Factorisation des polynômes

VI.1 En utilisant le corollaire (**??**), déterminer tous les polynômes irréductibles de degré inférieur à 4 sur $\mathbf{F}_2$.

VI.2

1. Soit p un nombre premier, $q_1 = p^{n_1}$, $q = q_1^n$. Soient $P = X^q - X$, Q un diviseur de P de degré d irréductible sur le corps $\mathbf{F_{p^{q_1}}}$; montrer que d divise n (même démonstration que pour la remarque **??**, 4.).
2. Déterminer tous les polynômes irréductibles de degré inférieur ou égal à 2 sur $\mathbf{F}_4$ (appliquer 1. et l'exercice).

VI.3 On considère le polynôme $Q(X) = X^9 - X + 1$ sur $\mathbf{F}_3$.

(a) Montrer que le polynôme Q n'a pas de racines dans $\mathbf{F_3}, \mathbf{F_9}$.

(b) Montrer que $\mathbf{F_{27}} \simeq \frac{\mathbf{F_3[X]}}{\mathbf{(X^3-X-1)}}$.

(c) Montrer que toute racine $\alpha \in \mathbf{F_{27}}$ du polynôme $X^3 - X - 1$ est une racine du polynôme Q.

(d) Déterminer toutes les racines de Q dans $\mathbf{F_{27}}$.

(e) Factoriser le polynôme Q sur le corps $\mathbf{F_3}$.

VI.4 Soit $P \in \mathbf{F_p[X]}$ un polynôme irréductible de degré d; $q = p^n$. Montrer que les conditions suivantes sont équivalentes :

(a) Le polynôme P est réductible sur $\mathbf{F_q}$.

(b) Le polynôme P possède une racine dans un corps $\mathbf{F_{p^{rn}}}$ avec $r \leq d/2$.

VI.5 A quelle condition un polynôme P à coefficients dans $\mathbf{F}_p$ de degré n est-il irréductible sur $\mathbf{F}_{p^m}$? Dans le cas où P est irréductible sur $\mathbf{F}_p$, on donnera des précisions sur les degrés des facteurs irréductibles de P sur $\mathbf{F}_{p^m}$. En particulier pour $n = 5$, donner m minimal tel que tout polynôme de degré 5 à coefficients dans $\mathbf{F}_p$ soit totalement décomposé (resp. possède une racine) sur $\mathbf{F}_{p^m}$.

VI.6 Montrer que $X^4 + 1$ est irréductible sur $\mathbf{Z}$ et réductible modulo tout nombre premier p. (montrer que pour tout nombre premier impair p, le polynôme $X^4 + 1$ a une racine dans le corps $\mathbf{F_{p^2}}$ et appliquer l'exercice).

VI.7 Soit $P(X) = X^4 - 10X^3 + 21X^2 - 10X + 11$.

(a) Décomposer P en facteurs irréductibles modulo 2,3.

(b) Montrer que P est irréductible sur $\mathbf{Q}$.

Corps finis

VI.8

(a) Quels sont les ordres (multiplicatifs) des éléments de $\mathbf{F}_{\mathbf{23}}^*$?

(b) Calculer 5^2 et 5^{11} modulo 23.

(c) En déduire que la classe de 5 modulo 23 engendre le groupe $\mathbf{F}_{\mathbf{23}}^*$

VI.9 Soit $P[X]$ un polynôme unitaire de degré n sur un corps K. On note $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires des racines α_i $(1 \leq i \leq n)$ de P, et

$$N_s = \sum_{i=1}^{n} \alpha_i^s.$$

On rappelle que pour $1 \leq s \leq n$,

$$N_s = P_s(\sigma_1, \ldots, \sigma_s)$$

où P_s est un polynôme en s variables.

(a) Calculer P_1, P_2, P_3.

(b) Soit $\mathbf{F_q}$ le corps fini à q éléments avec $q = p^r$, p nombre premier. On pose

$$\psi(i) = \sum_{x \in \mathbf{F_q}} x^i$$

Montrer que

- $\psi(i) = -1 \bmod p \quad$ si $\quad q - 1 \mid i$
- $\psi(i) = 0$ sinon.

VI.10 Soit p un nombre premier, $q = p^n$, $\mathbf{F}_q$ le corps à q éléments. Soit $a \in \mathbf{F}_q^*$, q_a le polynôme minimal de a sur le corps $\mathbf{F}_p$.

(a) Que peut-on dire du degré de q_a ?

(b) Montrer que q_a est aussi le polynôme minimal de a^p.

(c) On suppose que q_a est de degré n ; montrer que les racines de q_a sont alors :

$$a, a^p, a^{p^2}, \ldots, a^{p^{n-1}}.$$

VI.11 On note $(0, 1, 2)$ les éléments du corps $\mathbf{F}_3$.

(a) Montrer que

$$\mathbf{F}_9 \simeq \frac{\mathbf{F}_3[X]}{(X^2+1)}.$$

On notera x la classe de X dans le quotient.

(b) Montrer que l' élément $a = 2x+1$ est primitif (*i.e.* engendre le groupe multiplicatif $\mathbf{F}_9^*$) ; trouver son polynôme minimal (sur le corps $\mathbf{F}_3$).

(c) Factoriser le polynôme $X^9 - X$ dans $\mathbf{F}_3[X]$ et identifier les facteurs irréductibles primitifs.

VI.12 En utilisant la proposition (**??**), justifier, pour n divisant n', l'écriture $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^{n'}}$.

VI.13 Montrer les isomorphismes suivants et donner un générateur du groupe des inversibles des corps en question :

(i) $\mathbf{F}_4 \simeq \mathbf{F}_2[X]/(X^2+X+1)$;

(ii) $\mathbf{F}_8 \simeq \mathbf{F}_2[X]/(X^3+X+1)$;

(iii) $\mathbf{F}_9 \simeq \mathbf{F}_3[X]/(X^2+X-1)$.

VI.14 Montrer l'existence d'une infinité de nombres premiers p tels que

(a) $p \equiv 1 \mod 8$ (on pensera à utiliser l'exercice (**??**)) ;

(a) $p \equiv 3 \mod 4$;

(b) $p \equiv 5 \mod 6$;

(c) $p \equiv 5 \mod 8$.

(La méthode est la même que pour le corollaire **??** : on suppose par l'absurde que l'ensemble en question est fini ; on aboutit alors à une contradiction en notant n le plus grand élément de cet ensemble et en considérant l'entier $N = 2(n!) - 1$ pour (a), $N = n! - 1$ pour (b)) et $N = (2.3.5.7.11...n)^2 + 4$ pour (c). On utilisera de plus pour (c) l'exercice **??**.

Problèmes

Problème VI.1

1. Le nombre 2 est-il un carré dans $\mathbf{F}_5$? Montrer que $X^2 + X + 1$ est irréductible sur $\mathbf{F}_5$.

2. Soit $P(X) \in \mathbf{F}_5[X]$ un polynôme unitaire irréductible de degré deux . Montrer que le quotient
$$\frac{\mathbf{F}_5[X]}{(P(X))}$$
est isomorphe au corps $\mathbf{F}_{25}$ et que P a deux racines dans $\mathbf{F}_{25}$.

3. On note α une racine de $X^2 + X + 1$ dans $\mathbf{F}_{25}$. Montrer que tout $\beta \in \mathbf{F}_{25}$ peut s'écrire $a\alpha + b$ avec a et b dans $\mathbf{F}_5$.

4. Soit $P = X^5 - X + 1$. Montrer que pour tout $\beta \in \mathbf{F}_{25}$, on a $P(\beta) \neq 0$.

5. En déduire que P est irréductible sur $\mathbf{F}_5$. P est-il irréductible sur $\mathbf{Q}$?

6. Soit $Q = X^9 - X + 1$. Q a-t-il une racine dans $\mathbf{F}_3$, $\mathbf{F}_9$, $\mathbf{F}_{27}$? Est-il irréductible sur $\mathbf{F}_3$?