Université Denis Diderot — Algèbre et géométrie
Licence L3 – Mathématiques-informatique — 2006–2007

Feuille d'exercices n°8

Dans cette feuille d'exercices, les anneaux sont supposés commutatifs.

Exercice n°1 :

Montrer que le polynôme $P = X^3 - X + 1 \in \mathbf{F}_3[X]$ est irréductible.

Exercice n°2 :

Soit $\mathbf{F}_q$ un corps fini à q éléments. Soit $P \in \mathbf{F}_q[X]$ un polynôme (unitaire) irréductible de degré d. On choisit $D/\mathbf{F}$ un corps de décomposition de P. On fixe x_0 un zéro de P dans K et on note $R \subset D$ le corps de rupture de P engendré par x_0. On veut montrer que R est un corps de décomposition de P.

a) Montrer que l'application $F\colon D \to D$ qui à x associe x^q est un automorphisme du corps D fixant $\mathbf{F}_q$.

b) Soit $x \in K$ un zéro de P. Montrer que $x^{q^d} = x$.

c) Montrer que pour tout x de K, on a $x^{q^d} = x$.

d) Montrer que $R = \left\{x \in K, x^{q^d} = x\right\}$.

e) Montrer que $D = R$.

Exercice n°3 :

a) On note $Q = X^2 + X + 1 \in \mathbf{F}_2[X]$. Montrer que Q est irréductible.

b) On note $\mathbf{F}_4$ le corps de rupture de Q sur $\mathbf{F}_2$ (on note α la racine de Q ainsi construite). On note $P = X^3 + X + 1 \in \mathbf{F}_4[X]$. Montrer que P est irréductible.

c) On note $\mathbf{F}_{64}$ le corps de rupture de P sur $\mathbf{F}_4$. Soit β une racine de Q dans $\mathbf{F}_{64}$. Quelle est le degré sur $\mathbf{F}_2$ du sous-corps de $\mathbf{F}_{64}$ engendré par β ?

d) Montrer que le degré de $\alpha + \beta$ sur $\mathbf{F}_2$ est 6.

e) Montrer que le polynôme minimal de $\alpha + \beta$ sur $\mathbf{F}_2$ est

$$\prod_{i \in \mathbf{Z}/6\mathbf{Z}} (X - \alpha^{2^i} - \beta^{2^i}) .$$

f) Déterminer le polynôme minimal de $\alpha + \beta$ sur $\mathbf{F}_2$.

Exercice n°4 :

Soit A un anneau. Soit f un élément de A engendrant un idéal premier. Soit d un entier naturel non nul. On considère l'anneau $B = A[T]/(T^d - f)$.

a) Construire un isomorphisme $A/(f) \xrightarrow{\sim} B/(T)$.

b) En déduire que l'idéal de B engendré par T est premier.

Exercice n°5 :

On note $\mathbf{Z}[i]$ le sous-anneau de $\mathbf{C}$ engendré par i. C'est l'anneau des entiers de Gauß.

a) Montrer que $\mathbf{Z}[i]$ est un anneau intègre.

b) Montrer que tout élément de $\mathbf{Z}[i]$ peut s'écrire de manière unique sous la forme $a+ib$ avec $(a, b) \in \mathbf{Z}^2$.

c) Construire un isomorphisme $\mathbf{Z}[X]/(X^2+1) \xrightarrow{\sim} \mathbf{Z}[i]$.

d) Montrer que si $b \in \mathbf{Z}[i] - \{0\}$ et $a \in \mathbf{Z}[i]$, il existe $(q, r) \in \mathbf{Z}[i]$ tels que $a = bq + r$ et $|r| < |b|$.

e) En déduire que $\mathbf{Z}[i]$ est un anneau principal.

f) Quel est le groupe des unités de $\mathbf{Z}[i]$?

g) Déterminer un générateur de l'idéal de $\mathbf{Z}[i]$ engendré par $3 + 4i$ et $1 + 3i$.

h) Soit p un nombre premier supérieur ou égal à 3. On veut montrer que les conditions suivantes sont équivalentes :

   (1) l'entier -1 est un carré modulo p ;

   (2) le polynôme $X^2 + 1$ n'est pas irréductible sur $\mathbf{F}_p$;

   (3) l'idéal engendré par p dans $\mathbf{Z}[i]$ n'est pas premier ;

   (4) l'entier p est somme de deux carrés ;

   (5) on a la congruence $p \equiv 1 (\text{mod. } 4)$.

   Montrer que les conditions (1), (2), (3) et (4) sont équivalentes et que (4) implique (5).

i) Supposons (5). Soit x un générateur du groupe multiplicatif $\mathbf{F}_p^\times$. Montrer que $x^{\frac{p-1}{4}}$ est une racine carrée de -1. En déduire que (5) implique (1).