Feuille d'exercices 2

Remarque: Tous les exercices ne seront pas traités en séance de TD, j'indiquerai au fur et à mesure sur la page du forum (http://cours-jussieu-nombres.monforum.com/cours-et-td-2007-vf6.html) les exercices que nous aurons abordés.

Corps finis

Exercice 1. *Montrer les isomorphismes suivant 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) $\mathbf{F}_{16} \simeq \mathbf{F}_2[X]/(X^4+X+1)$ *; donner dans cet isomorphisme l'image de* $\mathbf{F}_4 \subset \mathbf{F}_{16}$ *et en déduire* $\mathbf{F}_{16} \simeq \mathbf{F}_2[X,Y]/(Y^2+Y+1, X^2+X+Y)$.

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

Exercice 2. *On dira d'une extension de corps* $k \subset \bar{k}$ *qu'elle est une clôture algébrique si:*
(a) tout élément $x \in \bar{k}$ *est algébrique sur* k*, i.e. il existe une polynôme* $P \in k[X]$ *tel que* $P(x)=0$*;*
(b) tout polynôme $P \in \bar{k}[X]$ *est totalement décomposé dans* $\bar{k}$.
Pour tout n *divisant* n' *on fixe une injection* $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^{n'}}$*. Montrez alors que* $\bar{\mathbb{F}}_p := \bigcup_{n>1} \mathbb{F}_{p^{n!}}$ *est une cloture algébrique de* $\mathbf{F}_p$.

Exercice 3. *(i) Donner tous les polynômes irréductibles de degré inférieur à* 4 *sur* $\mathbf{F}_2$.
(ii) Quelle est la factorisation sur $\mathbb{F}_4$ *d'un polynôme de* $\mathbb{F}_2[X]$ *irréductible de degré* 4*?*
(iii) Déduire des questions précédentes, le nombre de polynômes irréductibles de degré 2 *sur* $\mathbf{F}_4$.
(iv) Expliciter les polynômes irréductibles de degré 2 *sur* $\mathbb{F}_4$.

Exercice 4. *Polynômes irréductibles sur* $\mathbb{F}_q$*. soient* $A(n,q)$ *l'ensemble des polynômes irréductibles unitaires de degré* n *sur* $\mathbb{F}_q$ *et* $I(n,q)$ *le cardinal de cet ensemble.*

(a) Montrer que si $d|n$ *alors si* $P \in A(d,q)$ *on a* P *qui divise* $X^{q^n}-X$.

(b) Montrer que si $P \in A(d,n)$ *divise* $X^{q^n}-X$ *alors* d *divise* n.

(c) En déduire la formule

$$\sum_{d|n} dI(d,q) = q^n,$$

puis en appliquant la formule d'inversion de Moebius

$$I(n,q) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d}) q^d.$$

(d) Montrer que pour tout $n \geq 1$*,* $I(n,q) \geq 1$ *et trouver un équivalent de* $I(n,q)$ *quand* n *tend vers* $+\infty$.

Exercice 5. *(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 $P(\beta) \neq 0$. En déduire que P est irréductible sur $\mathbf{F}_5$. P est-il irréductible sur $\mathbf{Q}$?*

Exercice 6. *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 $\mathbb{F}_3, \mathbb{F}_9$.*

(b) *Montrer que $\mathbb{F}_{27} \simeq \frac{\mathbb{F}_3[X]}{(X^3 - X - 1)}$.*

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

(d) *Déterminer toutes le racines de Q dans $\mathbb{F}_{27}$.*

(e) *Factoriser le polynôme Q sur le corps $\mathbb{F}_3$.*

Exercice 7. *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 $\mathbf{F}_{p^m}$.*

Exercice 8. *(i) Montrer que X^4+1 est irréductible sur $\mathbb{Z}$ et réductible modulo tout nombre premier p. (Indication : montrer que pour tout nombre premier impair p, le polynôme $X^4 + 1$ a une racine dans le corps $\mathbb{F}_{p^2}$.*

(ii) Soit n un entier ne s'écrivant pas sous la forme p^α ou $2p^\alpha$ avec p premier impair. On sait que le n-ième polynôme cyclotomique Φ_n est irréductible sur $\mathbb{Z}$. Montrer en utilisant la question (ii) de l'exercice sur la théorie de Galois des corps finis, que Φ_n est réductible modulo tout nombre premier.

Exercice 9. *Soit $P(X) = X^4 - 10X^3 + 21X^2 - 10X + 11$*

(a) *Décomposer P en facteurs irréductibles modulo 2,3,5.*

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

Exercice 10. *Soient p et l deux nombres premiers impairs. On suppose que p engendre $(\mathbb{Z}/l\mathbb{Z})^*$ et que $l \equiv 2 \mod 3$. On note $P(X) = X^{l+1} - X + p$. On veut montrer que P est irréductible sur $\mathbb{Z}$.*

(i) *Montrer que P n'a pas de racine rationnelle.*

(ii) *On raisonne par l'absurde et on suppose $P = QR$ avec $Q, R \in \mathbb{Z}[X]$ unitaire et de degré au moins 2. Montrer que $\bar{P} = X(X-1)\bar{\Phi}_l$ est la décomposition en polynômes irréductibles de $\bar{P}$ sur $\mathbf{F}_p$; en déduire alors que $\bar{Q} = \bar{\Phi}_l$ et $\bar{R} = X(X-1)$.*

(iii) *En passant modulo 2, en déduire une contradiction. Comme exemple on propose le polynôme $X^{72} - X + 47$.*

Exercice 11. *Montrer l'existence d'une infinité de nombres premiers p tels que*

(a) $p \equiv 3 \mod 4$; (b) $p \equiv 1 \mod 4$;
(c) $p \equiv 1 \mod 2^m$; (d) $p \equiv 5 \mod 6$;
(e) $p \equiv 5 \mod 8$; (f) $p \equiv 1 \mod 6$;
(g) $p \equiv -1 \mod 12$; (h) $p \equiv -1 \mod 10$.

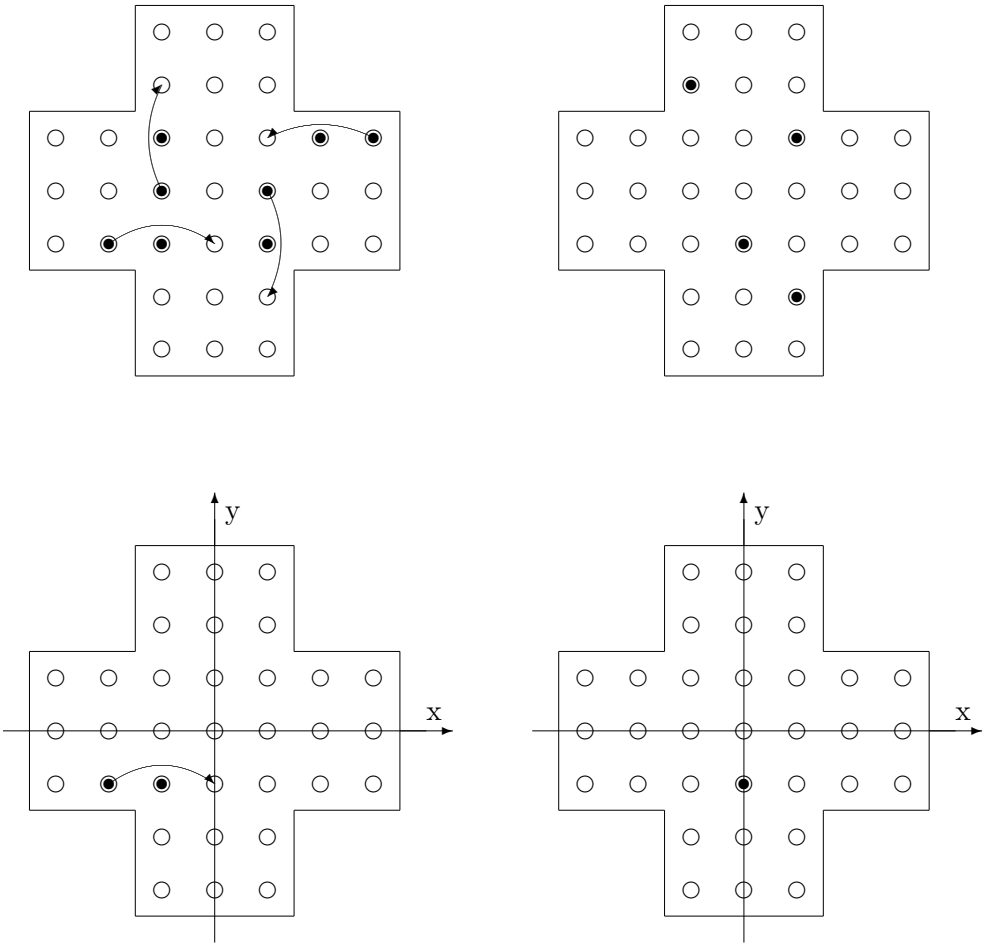
Indication: on cherchera à faire des lemmes du genre: si p divise $a^2 + qb^2$ et p premier avec b, alors $-q$ est un carré modulo p et donc d'après la loi de réciprocité quadratique p est congru à ? modulo q.

Exercice 12. *Le jeu du solitaire se joue sur un plateau disposant de 33 réceptacles (cercle vide) dans lesquels il peut y avoir des billes notés avec un cercle plein. A chaque étape on peut faire passer une bille au dessus d'une autre sur un axe vertical ou horizontal, pourvu que le réceptacle suivant soit vide, comme dans la figure suivante*

Soit alors O placé au centre du plateau et un repère (O, x, y) comme dans la figure suivante et pour une configuration $\mathcal{C}$ quelconque de billes sur le plateau on introduit

$$\alpha_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x+y} \in \mathbb{F}_4 \quad \beta_{\mathcal{C}} := \sum_{(x,y)\in\mathcal{C}} j^{x-y} \in \mathbb{F}_4$$

où j est un générateur de $\mathbb{F}_4^\times$.

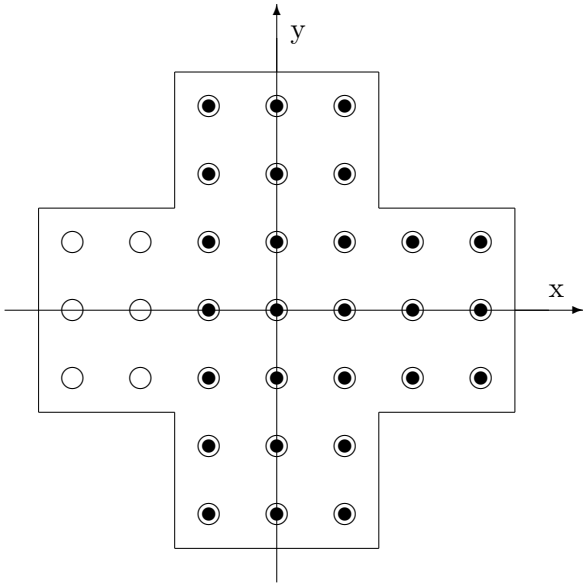


(1) Montrer que (α, β) est un invariant du jeu.

(2) Habituellement le jeu consiste à partir d'une configuration où l'on place des billes dans tous les réceptacles sauf un seul disons (x_0, y_0) et à arriver à la configuration où tous les réceptacles sont vides sauf celui (x_0, y_0). Montrer qu'effectivement les deux configurations précédentes, possèdent les mêmes invariants (α, β).

(3) Partant de la configuration suivante, montrer qu'il est impossible d'arriver à une configuration où il n'y aurait qu'une seule bille sur le plateau.

Exercice 13. *Soit n un entier tel que pour tout p premier sauf éventuellement un nombre fini, n est un carré modulo p. Montrer que n est un carré dans $\mathbb{N}$.*


y
x