Anneaux et arithmétique (ANAR)
TD 6 : Corps finis

Salim Rostam

2021–2022 (S6)

1 Groupe multiplicatif

Exercice 1. Soit k un corps et G un sous-groupe fini de $k^\times$. Le but de cet exercice est de montrer que G est cyclique. Soit n l'ordre de G.

1) Montrer que si n est premier alors G est cyclique.

On suppose maintenant que $n = ab$ avec $1 < a, b$ premiers entre eux. On considère l'application $f : G \to G$ donnée par $x \mapsto x^a$.

2) Justifier que f est bien à valeurs dans G.
3) Montrer que f est un morphisme de groupes.
4) Montrer que $\#\ker f \leq a$ et $\#\mathrm{im}\, f \leq b$.
5) Montrer que $\#\ker f \#\mathrm{im}\, f = n$.
6) En déduire par récurrence que G possède un élément d'ordre a et un élément d'ordre b.
7) En déduire que G est cyclique.
8) En déduire que si k est fini alors $k^\times$ est cyclique.

Exercice 2.
1) Soit k un corps et soit $P \in k[X]$.
   a) Montrer que si P est est irréductible de degré ≥ 2 alors P ne possède pas de racine dans k.
   b) Montrer que la réciproque est vraie si on suppose de plus $\deg P \leq 3$.
   c) Le polynôme $X^4 + 4 \in \mathbb{Q}[X]$ est-il irréductible ?
2) Pour $q \in \{8, 9\}$, construire un corps à q éléments, donner une $\mathbb{F}_p$-base, donner un générateur du groupe multiplicatif (cf. Exercice 1) et écrire son inverse dans la base précédente.

Exercice 3. Soit q une puissance d'un nombre premier. On note $\mathbb{F}_q^{\times 2}$ les carrés de $\mathbb{F}_q^\times$, c'est-à-dire l'ensemble des x^2 pour $x \in \mathbb{F}_q^\times$.

1) Si q est pair, montrer que $\mathbb{F}_q^{\times 2} = \mathbb{F}_q^\times$.

On supposera maintenant q impair.

2) Montrer que $\#\mathbb{F}_q^{\times 2} = \frac{q-1}{2}$.
3) a) Soit $x \in \mathbb{F}_q^\times$. Montrer que $x \in \mathbb{F}_q^{\times 2}$ si et seulement si $x^{\frac{q-1}{2}} = 1$.

b) En déduire que -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q = 1 \pmod 4$.

c) En déduire qu'il y a une infinité de nombres premiers de la forme $4n+1$. *Indication* : pour $n \in \mathbb{N}$, considérer $n!^2 + 1$.

4) Soient $a, b \in \mathbb{F}_q^\times$ et $c \in \mathbb{F}_q$. Montrer que l'équation $ax^2 + by^2 = c$ admet (au moins) une solution $(x, y) \in \mathbb{F}_p^2$. *Indication* : on a $by^2 = c - ax^2$.

2 Extensions de corps

Exercice 4. Soit k un corps fini et soit p la caractéristique de k.

1) Rappeler pourquoi p est un nombre premier.
2) Rappeler pourquoi $\#k = p^d$ pour $d \geq 1$.
3) On suppose que k contient un corps k' de cardinal $p^{d'}$ pour $d' \geq 1$.
   a) Montrer que $d' \mid d$.
   b) Montrer que pour tout $x \in k'$ on a $x^{p^{d'}} = x$.
   c) En déduire qu'un tel sous-corps k' est unique.
   d) Montrer qu'un tel sous-corps k' existe.
4) Déterminer le treillis des sous-corps de $\mathbb{F}_{4096}$.

Exercice 5. Soit k un corps fini de caractéristique p.

1) Rappeler pourquoi l'application $x \mapsto x^p$ est un automorphisme de k.
2) Soit $P \in \mathbb{F}_p[X]$ irréductible de degré d et supposons que k contienne une racine α de P.
   a) Soit n le plus petit entier ≥ 1 tel que $\alpha = \alpha^{p^n}$. Montrer que tous les éléments de $\mathbb{F}_p(\alpha)$ sont racines de $X^{p^n} - X$ et en déduire que $n = d$.
   b) Montrer que les α^{p^n} pour $0 \leq n < d$ sont racines de P.
   c) En déduire que P est scindé sur k.

On a montré le résultat suivant : sur les corps finis, un corps de rupture (d'un polynôme irréductible) est un corps de décomposition.

Exercice 6. Soit p un nombre premier. Pour $d \geq 1$ on note $I(d)$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré d et $i(d)$ leur nombre.

1) Soit $n \geq 1$. On veut montrer que $X^{p^n} - X = \prod_{d|n} \prod_{P \in I(d)} P$.
   a) Montrer que $X^{p^n} - X \in \mathbb{F}_p[X]$ est sans facteur carré.
   b) Si $d \mid n$ et $P \in I(d)$, montrer que les éléments du corps $\mathbb{F}_p[X]/(P)$ sont tous racines de $X^{p^n} - X$. *Indication* : on pourra utiliser l'Exercice 4.
   c) Si P est un facteur irréductible unitaire de $X^{p^n} - X$ sur $\mathbb{F}_p[X]$, montrer que $\deg(P) \mid n$. *Indication* : idem.
2) Soit $n \geq 2$.
   a) Déduire que $p^n = \sum_{d|n} d\, i(d)$.
   b) En déduire que $\frac{p^n - p^{\lfloor n/2 \rfloor + 1}}{n} \leq i(n) \leq \frac{p^n}{n}$ puis que $i(n) > 0$.

c) En déduire que $i(n) > 0$ et qu'un polynôme unitaire de degré n choisi uniformément dans $\mathbb{F}_p[X]$ a pour n grand une probabilité de $\frac{1}{n}$ d'être irréductible.

Exercice 7. *On rappelle le résultat suivant du TD 4 : si k est un corps et $P \in k[X]$, il existe un sur-corps K de k dans lequel P est scindé.* Soit p un nombre premier et $n \geq 1$. Soit K un sur-corps de $\mathbb{F}_p[X]$ tel que $X^{p^n} - X$ est scindé. On considère le sous-ensemble $k \coloneqq \{x \in K : x^{p^n} = x\}$.

1) Montrer que k est un corps.
2) Montrer que $\#k \leq p^n$.
3) Montrer que $\#k = p^n$.
4) En utilisant l'Exercice 1, retrouver le résultat de l'Exercice 6 : il existe un polynôme irréductible (unitaire) de degré n sur $\mathbb{F}_p$.

Exercice 8. *On rappelle le résultat suivant du TD 4 : si k un corps, il existe un sur-corps K de k algébriquement clos.* Soit p un nombre premier et soit K un sur-corps algébriquement clos de $\mathbb{F}_p$.

1) Le corps K peut-il être fini ?
2) Montrer que K possède un unique sous-corps de cardinal p^n pour tout $n \geq 1$.

On considère le sous-ensemble $k \coloneqq \cup_{n \geq 1} \mathbb{F}_{p^{n!}}$ de K.

3) Montrer que k est un corps.
4) Montrer que k est algébriquement clos.
5) Montrer que k est le plus petit corps algébriquement clos contenu dans K.

3 En pratique

Exercice 9. Soit q une puissance d'un nombre premier.

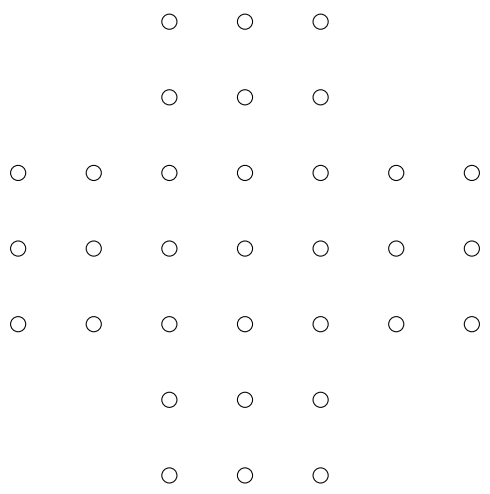
1) Factoriser le polynôme $X^q - X \in \mathbb{F}_q[X]$.
2) Soit $M \in \mathrm{M}_n(\mathbb{F}_q)$. Montrer que M est diagonalisable si et seulement si $M^q = M$.

Exercice 10. On est en face de quatre ampoules $A_1, \ldots, A_4$ et de quatre interrupteurs $I_1, \ldots, I_4$. Agir sur un interrupteur change l'état d'une ampoule (allumée devient éteinte et réciproquement). Les interrupteurs ont les actions suivantes :

— I_1 change l'état de toutes les ampoules ;
— I_2 change l'état de toutes les ampoules sauf A_2 ;
— I_3 change l'état des ampoules A_1 et A_2 ;
— I_4 change l'état des ampoules A_1 et A_4.

Initialement, les ampoules A_1, A_4 sont allumées et A_2, A_3 sont éteintes. Comment agir sur les interrupteurs pour que toutes les ampoules soient allumées en même temps ?

Exercice 11. Le solitaire se joue sur un plateau en forme de croix à 33 emplacements :



On indexe les emplacements par le sous-ensemble de $\mathbb{Z}^2$ correspondant, l'emplacement central correspondant à la position $(0,0)$. Chaque emplacement peut contenir une bille, et s'identifie donc avec un sous-ensemble $\mathcal{C}$ (« configuration ») de $\mathbb{Z}^2$. À partir d'une configuration $\mathcal{C}$ on peut faire sauter une bille au-dessus d'une autre bille β horizontalement ou verticalement (si l'emplacement d'arrivée est vide), en ensuite on enlève la bille β du plateau. Autrement dit, si $(a,b),(a+1,b) \in \mathcal{C}$ et $(a+2,b) \notin \mathcal{C}$ alors on peut obtenir la configuration

$$\widetilde{\mathcal{C}} \coloneqq \Big(\mathcal{C} \setminus \{(a,b),(a+1,b)\}\Big) \sqcup \{(a+2,b)\},$$

et idem verticalement. Le jeu consiste habituellement à partir d'une position $\mathcal{C}_{x_0}$ où les billes sont placées partout sauf en $x_0 \in \mathbb{Z}^2$, le but étant d'arriver à la position $\mathcal{C}'_{x_0}$ où tous les emplacements sont vides sauf celui en x_0.

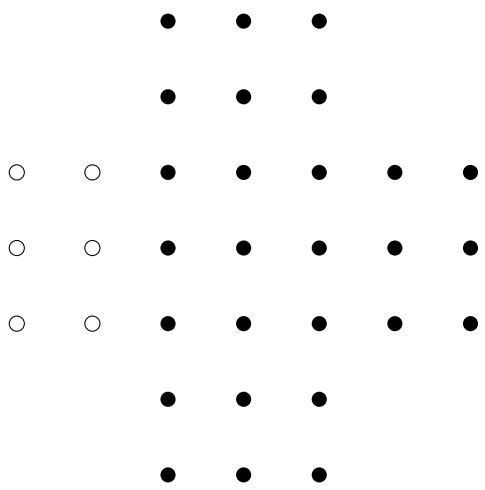
Soit k un corps tel que $X^2 - X - 1$ possède une racine j dans k. Si $\mathcal{C}$ est une configuration de billes, on définit les éléments de k suivants :

$$A_{\mathcal{C}} \coloneqq \sum_{(a,b)\in\mathcal{C}} j^{a+b}, \qquad\qquad B_{\mathcal{C}} \coloneqq \sum_{(a,b)\in\mathcal{C}} j^{a-b}.$$

1) Déterminer $(A_{\mathcal{C}}, B_{\mathcal{C}})$ pour $\mathcal{C} = \mathcal{C}'_{(a,b)}$.
2) Montrer que si $\mathcal{C}$ et $\mathcal{C}'$ sont deux configurations disjointes alors $X_{\mathcal{C}\sqcup\mathcal{C}'} = X_{\mathcal{C}} + X_{\mathcal{C}'}$ pour $X \in \{A,B\}$.
3) Montrer que la quantité (A,B) est conservée par les « sauts de billes ».

On suppose maintenant que $k = \mathbb{F}_4$.

4) L'hypothèse sur le polynôme $X^2 - X - 1$ est-elle vérifiée ? Montrer que j engendre $\mathbb{F}_4^\times$.
5) Déterminer $(A_{\mathcal{C}}, B_{\mathcal{C}})$ où $\mathcal{C}$ est la configuration où tous les emplacements sont occupés. *Indication* : c'est là que la forme particulière du plateau de jeu intervient !
6) Même question avec $\mathcal{C} = \mathcal{C}_{x_0}$.
7) On suppose que partant de la position $\mathcal{C}_{(0,0)}$ on est arrivé à une position de la forme $\mathcal{C}'_{(a,b)}$.
   a) Montrer que $a, b \in 3\mathbb{Z}$.
   b) Que peuvent valoir a, b ?
8) Montrer qu'en partant de la configuration $\mathcal{C}$ suivante :



il est impossible d'arriver à une configuration avec une unique bille.