

Feuille de TD n°3

Exercice 1

Soit \mathbf{K} un corps et $P \in \mathbf{K}[X]$. Les assertions suivantes sont elles vraies ou fausses? On justifiera bien entendu la réponse.

1. Si P n'a pas de racine dans \mathbf{K} , alors P est irréductible dans $\mathbf{K}[X]$.
2. Si P est irréductible dans $\mathbf{K}[X]$, alors P n'a pas de racine dans \mathbf{K} .

Exercice 2

Soit \mathbf{K} un corps. On travaille dans $\mathbf{K}[X]$.

1. Soit n un entier naturel et d un diviseur de n . Montrer que $X^d - 1$ divise $X^n - 1$ (on pourra travailler dans l'anneau quotient $\mathbf{K}[X]/\langle X^d - 1 \rangle$).
2. Soit n un entier naturel. Soit d un entier naturel non nul et r le reste de la division euclidienne de n par d . Montrer que $X^r - 1$ est le reste de la division euclidienne de $X^n - 1$ par $X^d - 1$.
3. Soit m et n des entiers naturels, et $d = \text{pgcd}(m, n)$. Dédurre de ce qui précède que $X^d - 1$ est un pgcd de $X^m - 1$ et $X^n - 1$.

Exercice 3

1. Quels sont les polynômes irréductibles de $\mathbf{C}[X]$?
2. Quels sont les polynômes irréductibles de $\mathbf{R}[X]$?
3. Dans la suite de l'exercice, P désigne le polynôme $X^4 + 1$. Factoriser P en produit d'irréductibles dans $\mathbf{C}[X]$.
4. Factoriser P en produit d'irréductibles dans $\mathbf{R}[X]$.
5. Montrer que P ne peut pas se factoriser en produit de deux polynômes de degré 2 à coefficients rationnels.
6. En déduire que P est irréductible dans $\mathbf{Q}[X]$.

Exercice 4

Soit d un entier positif sans facteur carré, c'est-à-dire tel que pour tout nombre premier p , p^2 ne divise pas d .

1. Montrer que $\sqrt{d} \notin \mathbf{Q}$ et que le polynôme $X^2 - d$ est irréductible dans $\mathbf{Q}[X]$.
2. Soit $A = \{a + b\sqrt{d}, (a, b) \in \mathbf{Q}^2\}$; montrer que A est un sous-corps de \mathbf{R} isomorphe à $\mathbf{Q}[X]/\langle X^2 - d \rangle$. Si $(a, b) \in \mathbf{Q}^2 \setminus \{(0, 0)\}$, montrer que $a + b\sqrt{d}$ est inversible dans A et expliciter son inverse.

Exercice 5

Soit \mathbf{K} un corps et $P, Q \in \mathbf{K}[X]$.

1. Rappeler comment on peut utiliser l'algorithme d'Euclide pour déterminer $\Pi := \text{pgcd}(P, Q)$.

2. Soit \mathbf{L} un corps tel que \mathbf{K} est un sous-corps de \mathbf{L} . On a donc $\mathbf{K}[X] \subset \mathbf{L}[X]$. On suppose que Q divise P dans $\mathbf{K}[X]$. Montrer que Q divise P dans $\mathbf{L}[X]$.
3. Montrer que la réciproque est vraie (on pourra considérer une division euclidienne). Ainsi on pourra simplement dire « Q divise P » sans préciser si on voit P et Q comme des éléments de $\mathbf{K}[X]$ ou de $\mathbf{L}[X]$.
4. On voit P et Q comme des éléments de $\mathbf{L}[X]$. Montrer que leur pgcd est égal à Π . Ainsi on pourra parler du pgcd de P et Q sans préciser si l'on considère P et Q comme des éléments de $\mathbf{K}[X]$ ou comme des éléments de $\mathbf{L}[X]$.
5. Montrer que si P est irréductible dans $\mathbf{L}[X]$, alors P est irréductible dans $\mathbf{K}[X]$ (on pourra raisonner par contraposition). Montrer par des exemples que la réciproque est fautive. Ainsi, lorsque l'on parle d'irréductibilité, il est très important de préciser si l'on voit P comme un élément de $\mathbf{K}[X]$ ou comme un élément de $\mathbf{L}[X]$.

Exercice 6

Pour tout polynôme $P \in \mathbf{C}[X]$ non nul, on note $N_0(P)$ le nombre de racines de P comptées sans multiplicité. Par exemple $N_0(X^3) = 1$, $N_0(X^2(X-1)) = 2$. Le but de cet exercice est de démontrer le théorème suivant.

Théorème. Soit A, B, C des éléments de $\mathbf{C}[X]$ vérifiant $A + B = C$. On les suppose en outre premiers entre eux et non constants tous les trois. Alors on a l'inégalité

$$\max(\deg(A), \deg(B), \deg(C)) \leq N_0(ABC) - 1.$$

Ce théorème, dit de Mason-Stothers, a été démontré par Stothers en 1981 et indépendamment par Mason en 1983. Ce résultat a été à l'origine d'une célèbre (et toujours largement ouverte) conjecture d'arithmétique, la « conjecture abc ». La conjecture abc est un énoncé analogue au théorème de Mason-Stothers où \mathbf{Z} joue le rôle de $\mathbf{C}[X]$. La démonstration proposée dans cet exercice du théorème de Mason-Stothers est due à Noah Snyder, qui l'a trouvée à la fin des années 90 alors qu'il était encore au lycée. Nous verrons également comment le théorème de Mason-Stothers implique facilement le grand théorème de Fermat pour $\mathbf{C}[X]$ (le grand théorème de Fermat pour les entiers a été démontré par Wiles en 1994, mais la démonstration est infiniment moins élémentaire que dans le cas des polynômes!).

1. Montrer qu'on peut supposer qu'on a $\max(\deg(A), \deg(B), \deg(C)) = \deg(C)$.
2. Vérifier la relation $A'B - AB' = A'C - AC'$. En déduire que $\text{pgcd}(A, A') \text{pgcd}(B, B') \text{pgcd}(C, C')$ divise $A'B - AB'$ puis l'inégalité

$$\deg(\text{pgcd}(A, A')) + \deg(\text{pgcd}(B, B')) + \deg(\text{pgcd}(C, C')) \leq \deg(A) + \deg(B) - 1.$$

3. Soit $P \in \mathbf{C}[X]$ non nul. Montrer la relation

$$\deg(\text{pgcd}(P, P')) = \deg(P) - N_0(P).$$

4. Montrer qu'on a $N_0(ABC) = N_0(A) + N_0(B) + N_0(C)$.
5. Déduire de ce qui précède le théorème de Mason-Stothers.
6. Déduire du théorème de Mason-Stothers le grand théorème de Fermat pour $\mathbf{C}[X]$: soit $n \geq 3$ un entier, et A, B, C des polynômes de $\mathbf{C}[X]$ premiers entre eux et vérifiant $A^n + B^n + C^n = 0$; alors A, B et C sont des constantes (raisonner par l'absurde, et appliquer Mason-Stothers à A^n, B^n et C^n).

Exercice 7

Soit n et m des entiers strictement positifs. Montrer que les conditions suivantes sont équivalentes :

1. le groupe $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ est cyclique ;
2. les entiers n et m sont premiers entre eux.

Exercice 8

Soit p un nombre premier impair.

1. Quels éléments de $(\mathbf{Z}/p\mathbf{Z})^\times$ sont leur propre inverse ?
2. Dédire de la question précédente le théorème de Wilson : soit n un entier naturel supérieur à 3 ; alors n est premier si et seulement si on a $(n-1)! \equiv -1 \pmod{n}$.

Exercice 9

Choisir un petit nombre premier p (disons inférieur à 20) et répondre aux questions suivantes : quels sont les ordres possibles des éléments du groupe \mathbf{F}_p^\times ? Combien d'éléments de chaque ordre ce groupe possède-t-il ? Quels sont les éléments qui engendrent le groupe ? Recommencer avec un autre petit nombre premier. . .

Exercice 10

1. Soit $A = \mathbf{Z}/4\mathbf{Z}$. Déterminer A^\times ; A^\times est-il un groupe cyclique ? Mêmes questions avec $A = \mathbf{Z}/9\mathbf{Z}$.
2. Soit p un nombre premier. Soit $x = [1+p]_{p^2}$. Montrer que $x \in (\mathbf{Z}/p^2\mathbf{Z})^\times$. Montrer que l'ordre de x dans le groupe $(\mathbf{Z}/p^2\mathbf{Z})^\times$ est p .
3. Soit n un entier tel que $[n]_p \in (\mathbf{Z}/p\mathbf{Z})^\times$. On note r l'ordre de $[n]_p$ dans le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$. Montrer que $[n]_{p^2}$ est un élément de $(\mathbf{Z}/p^2\mathbf{Z})^\times$. Montrer que l'ordre de $[n]_{p^2}$ dans le groupe $(\mathbf{Z}/p^2\mathbf{Z})^\times$ est divisible par r .
4. Dédire de la question précédente que le groupe $(\mathbf{Z}/p^2\mathbf{Z})^\times$ possède un élément y dont l'ordre est divisible par $p-1$. En déduire que le groupe $(\mathbf{Z}/p^2\mathbf{Z})^\times$ possède un élément z dont l'ordre est $p-1$.
5. Soit G un groupe, g et h des éléments de G d'ordres finis respectivement égaux à n et m ; on suppose que g et h commutent et que n et m sont premiers entre eux ; montrer que gh est d'ordre mn .
6. Dédire des questions précédentes que le groupe $(\mathbf{Z}/p^2\mathbf{Z})^\times$ est un groupe cyclique.

Exercice 11

1. Soit p un nombre premier. On s'intéresse aux polynômes irréductibles sur \mathbf{F}_p . Expliciter une méthode effective pour déterminer la liste des polynômes irréductibles de degré 2 et 3 sur \mathbf{F}_p . Expliquer ensuite comment en déduire la liste des polynômes irréductibles de degré 4, puis 5 sur \mathbf{F}_p . Expliquer enfin une procédure générale permettant de déterminer de manière effective les polynômes irréductibles de degré n sur \mathbf{F}_p avec n quelconque.
2. Donner la liste des polynômes irréductibles unitaires de degré 2 et 3 sur $\mathbf{F}_3[X]$. Même question pour $\mathbf{F}_5[X]$.

- Donner la liste des polynômes irréductibles unitaires de degré 4 dans $\mathbf{F}_2[X]$, puis dans $\mathbf{F}_3[X]$, puis dans $\mathbf{F}_5[X]$.
- Pour $\mathbf{K} = \mathbf{F}_2, \mathbf{F}_3$ ou \mathbf{F}_5 et pour chacun des polynômes P déterminés ci-dessus, donner la liste des éléments de $\mathbf{K}[X]/\langle P \rangle$ (on notera α l'image de X dans le quotient), écrire les tables d'addition et de multiplication dans le corps $\mathbf{K}[X]/\langle P \rangle$, vérifier que le groupe $(\mathbf{K}[X]/\langle P \rangle)^\times$ est cyclique et en donner un générateur.
- Pour $\mathbf{K} = \mathbf{F}_2, \mathbf{F}_3$ ou \mathbf{F}_5 , et $d \in \{2, 3, 4\}$, et chaque couple (P, Q) de polynômes de $\mathbf{K}[X]$ irréductibles, unitaires, de degré d et distincts, exhiber un isomorphisme de $\mathbf{K}[X]/\langle P \rangle$ sur $\mathbf{K}[X]/\langle Q \rangle$.

La résolution complète de cet exercice est longue, surtout si l'on s'astreint à faire tous les calculs à la main ; il est conseillé d'en traiter une proportion suffisamment importante pour se sentir à l'aise avec les calculs explicites dans les corps finis.

Exercice 12

- Soit p un nombre premier. Montrer que les anneaux $\mathbf{Z}_{(p)}/p\mathbf{Z}_{(p)}$ et $\mathbf{Z}/p\mathbf{Z}$ sont isomorphes (cf. exercice 7.3 de la feuille 1 et 6 de la feuille 2).
- En déduire que si q est un nombre premier distinct de p alors les anneaux $\mathbf{Z}_{(p)}$ et $\mathbf{Z}_{(q)}$ ne sont pas isomorphes.
- Soit n un entier strictement positif. Montrer que les anneaux $\mathbf{Z}_{(p)}/p^n\mathbf{Z}_{(p)}$ et $\mathbf{Z}/p^n\mathbf{Z}$ sont isomorphes.

Exercice 13

- On considère les idéaux suivants de $\mathbf{Z}[X, Y]$:

$$\langle X, Y \rangle, \quad \langle 2X \rangle, \quad \langle X, Y, 2 \rangle, \quad \langle 2X, Y, 2 \rangle.$$

Ces idéaux sont-ils premiers (respectivement maximaux) ?

- Soit n un entier. À quelle condition sur n l'idéal $\langle n, X \rangle$ est-il un idéal premier (respectivement maximal) de $\mathbf{Z}[X]$? Même question avec l'idéal $\langle n \rangle$.
- Soit A un anneau et n un entier strictement positif. Soit \mathcal{I} un idéal de $A[X_1, \dots, X_n]$. On suppose qu'il existe un élément $P \in \mathcal{I}$ tel que $P - X_n \in A[X_1, \dots, X_{n-1}]$. Montrer que $A[X_1, \dots, X_n]/\mathcal{I}$ est naturellement isomorphe à un quotient de $A[X_1, \dots, X_{n-1}]$ que l'on décrira. Calculer le quotient $A[X, Y]/\langle X - Y^2, Y + 1 \rangle$ à l'aide du résultat précédent, puis en exhibant un morphisme surjectif de noyau convenable.

Exercice 14

Cet exercice s'intéresse aux éléments irréductibles de $\mathbf{Z}[i]$ et fait suite à l'exercice 10 de la feuille 2, dont on pourra admettre ici les résultats.

- Soit A un anneau intègre et $a \in A$ un élément irréductible. Montrer que les propriétés suivantes sont équivalentes :
 - l'idéal aA est premier ;
 - pour tout $(b, c) \in A^2$ tel que a divise bc , alors a divise b ou a divise c .

On admet (provisoirement) que tout élément irréductible de l'anneau $\mathbf{Z}[i]$ vérifie ces propriétés.

2. Soit z un élément irréductible de $\mathbf{Z}[i]$. Montrer qu'il existe un nombre premier p tel que z divise p dans $\mathbf{Z}[i]$. En déduire que les irréductibles de $\mathbf{Z}[i]$ sont exactement les éléments qui s'écrivent αp avec p nombre premier congru à 3 modulo 4 et $\alpha \in \{1, -1, i, -i\}$ ou $a + ib$ avec $a, b \in \mathbf{Z}$ et $a^2 + b^2$ premier. Vérifier *a posteriori* que pour tout élément irréductible z de $\mathbf{Z}[i]$, l'idéal $z\mathbf{Z}[i]$ est premier.
3. Décomposer en produit d'irréductibles dans $\mathbf{Z}[i]$ l'élément $-9 + 123i$. *Indication* : supposons la décomposition écrite ; que peut-on dire de la norme des éléments intervenant dans la décomposition ?

Exercice 15

Soit \mathbf{K} un corps. Soit A une \mathbf{K} -algèbre et $a \in A$. Soit $ev_a: \mathbf{K}[X] \rightarrow A$ le morphisme d'évaluation en a . On dit que a est transcendant sur \mathbf{K} si ev_a est injectif. Dans le cas contraire, a est dit algébrique sur \mathbf{K} , et le générateur unitaire de $\text{Ker}(ev_a)$ est appelé polynôme minimal de a (sur \mathbf{K}).

1. Soit $a \in A$. Vérifier que a est algébrique sur \mathbf{K} si et seulement si il existe $P \in \mathbf{K}[X] \setminus \{0\}$ tel que $P(a) = 0$.
2. Soit $a \in A$. Montrer que a est algébrique sur \mathbf{K} si et seulement si la \mathbf{K} -algèbre $\mathbf{K}[a]$ est un \mathbf{K} -espace vectoriel de dimension finie si et seulement si il existe $n \in \mathbf{N}$ tel que $\{a^i\}_{1 \leq i \leq n}$ est une base du \mathbf{K} -espace vectoriel $\mathbf{K}[a]$.
3. Soit $P \in \mathbf{K}[X] \setminus \{0\}$. On suppose dans cette question que $A = \mathbf{K}[X]/PK[X]$ et on note x l'image de X dans A . Montrer que tout élément de A est algébrique sur \mathbf{K} et que le polynôme minimal de x sur \mathbf{K} est P .
4. On suppose dans cette question que A est intègre. Soit $a \in A$ un élément algébrique sur \mathbf{K} . Montrer que le polynôme minimal de a sur \mathbf{K} est irréductible, et que $\mathbf{K}[a]$ est un sous-corps de A .
5. Soit a et b des éléments de A algébriques sur \mathbf{K} . Montrer qu'il existe $n \in \mathbf{N}$ tel que le sous \mathbf{K} -espace vectoriel de A engendré par $\{a^i b^j\}_{1 \leq i, j \leq n}$ est une sous- \mathbf{K} -algèbre de A . En déduire que l'ensemble des éléments de A qui sont algébriques sur \mathbf{K} est une sous- \mathbf{K} -algèbre de A .
6. On suppose dans cette question que A est un corps et que tout élément de A est algébrique sur \mathbf{K} . Soit B une A -algèbre et $b \in B$. Montrer que b est algébrique sur A si et seulement si b est algébrique sur \mathbf{K} .

Exercice 16

On rappelle une partie du théorème de structure des groupes abéliens finis.

Théorème. *Soit G un groupe abélien fini non trivial. Alors il existe un entier strictement positif r et un r -uplet (d_1, \dots, d_r) d'entiers supérieurs à 2 tels que pour tout $1 \leq i \leq r - 1$, d_i divise d_{i+1} et*

$$G \cong \prod_{i=1}^r \mathbf{Z}/d_i \mathbf{Z}.$$

Soit \mathbf{K} un corps fini. Dédurre du théorème ci-dessus que \mathbf{K}^\times est un groupe cyclique. *Indication* : supposons $r \geq 2$; que peut-on dire du nombre d'éléments de G dont l'ordre divise d_1 ?

Exercice 17

1. Soit $p \geq 2$ un entier, r et n des entiers strictement positifs. Montrer que $p^r - 1$ divise $p^n - 1$ si et seulement si r divise n .
2. Soit p un nombre premier et n un entier strictement positif.
 - (a) Soit r un diviseur positif de n et $P \in \mathbf{F}_p[X]$ un polynôme irréductible de degré r . Montrer que P divise $X^{p^n} - 1$.
 - (b) Soit r un entier strictement positif et $P \in \mathbf{F}_p[X]$ un polynôme irréductible de degré r . On suppose que P divise $X^{p^n} - X$. Montrer que r divise n . *Indication* : soit $\mathbf{K} = \mathbf{F}_p[X]/\langle P \rangle$; montrer que pour tout $x \in \mathbf{K}$, on a $x^{p^n} = x$.
 - (c) Pour tout entier strictement positif n , on note $\text{Irr}(p, n)$ l'ensemble des polynômes irréductibles unitaires de degré n sur \mathbf{F}_p . Montrer les relations

$$X^{p^n} - X = \prod_{\substack{r|n \\ P \in \text{Irr}(p,r)}} P$$

et

$$p^n = \sum_{r|n} r \text{Irr}(p, r).$$

En déduire l'encadrement

$$\frac{p^n - p^{\lfloor \frac{n}{2} \rfloor + 1}}{n} \leq \text{Irr}(p, n) \leq \frac{p^n}{n}.$$

En déduire que pour tout entier strictement positif n , l'ensemble $\text{Irr}(p, n)$ est non vide.

Exercice 18

Soit \mathbf{K} un corps, n et k des entiers strictement positifs avec $k \leq n$, E le \mathbf{K} -espace vectoriel \mathbf{K}^n et F un sous-espace vectoriel de E de dimension k . Soit $\pi: \mathbf{K}^n \rightarrow \mathbf{K}^{k-1}$ la projection sur les $k-1$ premières coordonnées. Montrer que $\pi|_F$ n'est pas injective. En déduire la borne de Singleton.

Exercice 19

Soit \mathcal{C} un code linéaire et H une matrice de contrôle de \mathcal{C} . Soit d l'unique entier strictement positif vérifiant la propriété suivante :

1. il existe d colonnes de H qui forment un système lié ;
2. tout sous-ensemble de colonnes de H de cardinal $d-1$ est un système libre

Montrer que d est la distance minimale de \mathcal{C} .

Exercice 20

1. Vérifier que la distance de Hamming est bien une distance.

2. Soit A un ensemble fini de cardinal q et $n \geq 1$ un entier. Soit $t \geq 1$ un entier. Montrer que le nombre d'éléments d'une boule de rayon t de A^n (pour la distance de Hamming) est

$$N(q, n, t) = \sum_{k=0}^t \binom{n}{k} (q-1)^k.$$

3. Soit $1 \leq k \leq n$ un entier et $A^k \cong \mathcal{C} \subset A^n$ un code. Soit $t \geq 1$ un entier. Montrer que \mathcal{C} est t -correcteur si et seulement si les boules de rayon t centrées en les éléments de \mathcal{C} sont deux à deux disjointes. Montrer que si \mathcal{C} est t -correcteur alors $N(q, n, t) \leq q^{n-k}$ (borne de Hamming).
4. Le code \mathcal{C} est dit *parfait* s'il existe un entier $t \geq 1$ tel que les boules de rayon t centrées en les éléments de \mathcal{C} forment une partition de A^n . Montrer qu'un tel entier t est alors unique et est le plus grand entier t' tel que \mathcal{C} est t' -correcteur. Montrer que le code \mathcal{C} est parfait si et seulement s'il existe un entier $t \geq 1$ tel que \mathcal{C} est t -correcteur et on a l'égalité

$$N(q, n, t) = q^{n-k}.$$

5. *Codes de Hamming binaires* : soit r un entier et $n = 2^r - 1$. Soit M une matrice à r colonnes et $2^r - 1$ lignes dont l'ensemble des lignes coïncide avec $\mathbf{F}_2^r \setminus \{0\}$. Soit

$$\mathcal{C} := \{x \in \mathbf{F}_2^n, \quad x \cdot M = 0\}.$$

Déterminer les paramètres de \mathcal{C} . Montrer que \mathcal{C} est 1-correcteur parfait.

6. Lister les éléments du code de Hamming binaire de paramètres $[7, 4, 3]$ (qui est historiquement l'un des premiers codes non triviaux introduits). Soit $y \in \mathbf{F}_2^7$ un mot transmis comprenant une erreur. Montrer que le syndrome de y est la ligne de M dont l'indice correspond à la position de l'erreur.
7. *Codes de Hamming q -aires* : soit \mathbf{K} un corps de cardinal q , r un entier. Soit $\mathcal{L} \subset \mathbf{K}^r$ une partie maximale de \mathbf{K}^r telle que deux éléments de \mathcal{L} ne sont pas colinéaires. Soit M la matrice à r colonnes dont l'ensemble des lignes coïncide avec \mathcal{L} . Explicitez le cas $q = 3, r = 2$. Soit

$$\mathcal{C} := \{x \in \mathbf{K}^n, \quad x \cdot M = 0\}.$$

Donner les paramètres de \mathcal{C} . Montrer que \mathcal{C} est 1-correcteur parfait.

Exercice 21

1. Soit \mathbf{K} un corps fini de cardinal q et α un générateur de \mathbf{K}^\times . Soit $2 \leq d \leq q-1$ un entier et \mathcal{I} l'idéal de $\mathbf{K}[X]$ engendré par le polynôme

$$g(X) := \prod_{i=1}^{d-1} (X - \alpha^i).$$

Montrer que \mathcal{I} définit un code cyclique sur \mathbf{K} de paramètres $[q-1, q-d, d]$ (donc de type MDS). Expliciter une base du code pour les paramètres suivants : $[3, 2, 2]$ et $[8, 7, 2]$.

2. Soit \mathbf{K} un corps, $\alpha \in \mathbf{K}^\times$ et n l'ordre multiplicatif de α . Soit $m(X)$ et $u(X)$ des éléments de $\mathbf{K}[X]$ de degré au plus $n-1$. Montrer que les deux propriétés suivantes sont équivalentes :

(a) on a $n \cdot m(X) = \sum_{i=0}^{n-1} u(\alpha^i) X^i$;

(b) on a $u(X) = \sum_{i=0}^{n-1} m(\alpha^{-i})X^i$.

3. Soit \mathbf{K} un corps de cardinal q et $2 \leq k \leq q-1$ un entier. Soit $\mathbf{K}[X]_{\leq k-1}$ l'ensemble des polynômes à coefficients dans \mathbf{K} de degré au plus $k-1$. Choisissons une énumération $\{x_i\}_{0 \leq i \leq q-2}$ des éléments de \mathbf{K}^\times . On considère l'application qui à $u \in \mathbf{K}[X]_{\leq k-1}$ associe $(u(x_i))_{0 \leq i \leq q-2}$. Montrer que son image est un code de paramètres $[q-1, k, q-k]$ (donc de type MDS). Comment ce code est-il relié à celui de la première question ?

Exercice 22

Soit \mathbf{K} un corps fini, n un entier positif tel que n et $q := \text{card}(\mathbf{K})$ sont premiers entre eux, r l'ordre de $[q]_n$ dans $(\mathbf{Z}/n\mathbf{Z})^\times$. Soit \mathbf{L} un corps à q^r éléments contenant \mathbf{K} et $\alpha \in \mathbf{L}^\times$ un élément d'ordre n . Pour toute partie Σ de $\mathbf{Z}/n\mathbf{Z}$, on note

$$g_\Sigma := \prod_{i \in \Sigma} (X - \alpha^i) \in \mathbf{L}[X]$$

1. On veut montrer que g_Σ est à coefficient dans \mathbf{K} si et seulement si Σ est stable par multiplication par q .
- (a) Soit A, B des anneaux et $\varphi: A \rightarrow B$ un morphisme. Soit I un ensemble fini, $(a_i)_{i \in I}$ des éléments de A . Écrivons

$$\prod_{i \in I} (X - a_i) = \sum_{k \geq 0} b_k X^k, \quad (b_k) \in A^{(\mathbf{N})}$$

Vérifier (sans calculs...) qu'on a

$$\prod_{i \in I} (X - \varphi(a_i)) = \sum_{k \geq 0} \varphi(b_k) X^k, \quad (b_k) \in A^{(\mathbf{N})}$$

- (b) Conclure en utilisant le morphisme $x \mapsto x^q$.
2. On suppose en outre qu'il existe $\nu \in \mathbf{Z}/n\mathbf{Z}$ et $2 \leq d \leq n$ un entier positif tels que

$$\{\nu + [i]_n\}_{0 \leq i \leq d-2} \subset \Sigma$$

On veut montrer que le code cyclique \mathcal{C} de $\mathbf{K}[X]/\langle X^n - 1 \rangle$ engendré par g est de distance minimale au moins d . Soit $P \in \mathbf{K}[X]$ un multiple de g de degré au plus $n-1$ et ayant *au plus* $d-1$ coefficients non nul. Traduire la condition que P est un multiple de g en un système linéaire d'inconnues les coefficients de P dont la matrice est une matrice de Vandermonde. Conclure que P est nul, puis conclure quant à la distance minimale de \mathcal{C} .

3. On suppose que $\mathbf{K} = \mathbf{F}_2$ et $n = 2^r - 1$. Soit

$$g := \prod_{i=0}^{r-1} (X - \alpha^{2^i}).$$

Vérifier que $g \in \mathbf{F}_2[X]$. Déterminer les paramètres du code cyclique engendré par g . Comparer avec les codes de Hamming binaires de l'exercice 20.

4. On suppose que $n = \frac{q^r - 1}{q - 1}$ et que n et $q - 1$ sont premiers entre eux. Soit

$$g =: \prod_{i=0}^{r-1} (X - \alpha^{q^i}).$$

Vérifier que $g \in \mathbf{K}[X]$. Déterminer les paramètres du code cyclique engendré par g ; on pourra comparer ce code avec le code de Hamming q -aire analogue de l'exercice 20.