Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Codes algébriques – Solutions de l'interrogation 1

01/03/2024

Exercice 1. Questions courtes (30 min).

Répondre aux questions suivantes en justifiant vos réponses.

Question 1.– Soit σ la permutation de $[1,6] := \{1,2,3,4,5,6\}$ donnée par

i	1	2	3	4	5	6
$\sigma(i)$	2	1	4	5	6	3

La permutation σ induit-elle un automorphisme du code binaire $\mathcal{C}$ engendré par la matrice

$$\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} ?$$

Question 2.– Soit $\mathcal{I}$ l'idéal de $\mathbb{F}_2[x]/(x^6-1)$ engendré par le polynôme $a(x) = x(x+1)^2$. Donner une matrice génératrice du code cyclique associé à l'idéal $\mathcal{I}$.

Question 3.– Quel est le polynôme générateur du dual du code cyclique binaire de longueur 7 engendré par $g(x) = x^3 + x^2 + 1$?

Question 4.– Existe t-il un code cyclique de longueur 14 et de dimension 5 sur $\mathbb{F}_3$?

Solutions de l'Exercice 1.

Solution Q1. On vérifie si les permutations des vecteurs d'une base du code $\mathcal{C}$ sont également dans le code. Observons que $\mathcal{C}$ contient exactement 4 mots de code :

$$(0,0,0,0,0,0),$$
$$(1,0,1,1,1,0),$$
$$(0,1,0,1,1,1),$$
$$\text{et } (1,1,1,0,0,1).$$

Comme vecteurs de la base, on choisit les deux lignes de la matrice $\boldsymbol{G}$. On observe que la permutation de $(1,0,1,1,1,0)$ donne $(0,1,0,1,1,1)$ qui est un mot du code. En revanche, la premutation de $(0,1,0,1,1,1)$ donne $(1,0,1,0,1,1)$ qui n'est pas un mot du code. Donc la premutation σ n'induit pas d'automorphisme de $\mathcal{C}$.

Solution Q2. On calcule d'abord le pgcd entre $a(x)$ et x^6-1. On sait que $x+1 = x-1$ divise x^6-1. Par ailleurs, x est premier avec x^6-1 car $x \times x^5 - (x^6-1) = 1$. Par conséquent, ce pgcd est

$$g(x) = (x+1)^2 = x^2+1\,.$$

C'est le polynôme générateur du code associé à l'idéal $\mathcal{I}$. Une matrice génératrice du code est donc

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Solution Q3. Le polynôme générateur du dual d'un code cyclique engendré par $g(x)$ est le polynôme réciproque $\overline{h}(x)$ de l'unique polynôme $h(x)$ qui vérifie $g(x)h(x) = x^7 - 1$ dans $\mathbb{F}_2[x]$.

Calculons donc d'abord $h(x)$; un calcul donne

$$x^7 - 1 = x^7 + 1 = (x^3 + x^2 + 1)(x^4 + x^3 + x^2 + 1)$$

donc $h(x) = x^4 + x^3 + x^2 + 1$ puis $\overline{h}(x) = x^4 + x^2 + x + 1$.

Solution Q4. Pour déterminer s'il existe un code cyclique de longueur $n = 14$ et de dimension $k = 5$ sur $\mathbb{F}_q$ avec $q = 3$, on déterminer les classes cyclotomiques sur $\mathbb{F}_q$ modulo n, qui permettront ensuite de décrire les degrés des polynômes générateurs éventuels :

1. $C_0 = \{0\}$,
2. $C_1 = \{1, 3, 9, 13, 11, 5\}$
3. $C_2 = \{2, 6, 4, 12, 8, 10\}$
4. $C_7 = \{7\}$

Par conséquent, $x^{14} - 1$ se factorise en un produit de 4 polynômes irréductibles : deux de degré 1 et deux de degré 6. Les diviseurs de $x^{14} - 1$ ont donc degré 0, 1, 2, 6, 7, 8, 12, 13 ou 14. Cela signifie que les codes cycliques associés à ces divisieurs ont dimension 14, 13, 12, 8, 7, 6, 2, 1 et 0 ; aucun n'a dimension 5.

Exercice 2. Construction de codes cycliques (30 min).

Question 1.– Soit $P(x) = x^2 - x + 1 \in \mathbb{F}_5[x]$.

1. Démontrer que $P(x)$ est irréductible sur $\mathbb{F}_5$.
2. Soit α une racine de $P(x)$. Dans quelle extension de $\mathbb{F}_5$ se situe α ?
3. Démontrer que α est une racine primitive 6-ème de l'unité.

Question 2.– Déterminer une factorisation de $x^6 - 1$ en polynômes irréductibles.

Question 3.– Donner la liste des polynômes générateurs des codes cycliques de longueur 6 et de dimension 4 sur $\mathbb{F}_5$.

Solutions de l'Exercice 2.

Solution Q1.

1. Le polynôme $P(x)$ est de degré 2. Il est donc irréductible sur $\mathbb{F}_5$ si et seulement s'il n'admet pas de racine sur $\mathbb{F}_5$. Calculons $P(i)$ pour tout $i \in \mathbb{F}_5$. On a $P(0) = 1$, $P(1) = 1$, $P(2) = 3$, $P(3) = 2$ et $P(4) = 3$, donc $P(x)$ est bien irréductible sur $\mathbb{F}_5$.
2. La racine d'un polynôme de degré 2 est, ou bien dans $\mathbb{F}_5$, ou bien dans son extension quadratique. Comme on a déjà vu que $P(x)$ n'admettait pas de racine sur $\mathbb{F}_5$, on en déduit que $\alpha \in \mathbb{F}_{25}$.
3. Calculons α^2, α^3 et α^6. Si $\alpha^6 = 1$, et si α^2 et α^3 sont tous les deux différents de 1, alors on pourra en déduire que α est une racine 6-ème de l'unité, et que son ordre est 6 (donc elle sera primitive).

   On a :

   $$\alpha^2 = \alpha - 1 \neq 1$$
   $$\alpha^3 = \alpha \times \alpha^2 = \alpha(\alpha - 1) = \alpha^2 - \alpha = -1 \neq 1$$
   $$\alpha^6 = (\alpha^3)^2 = (-1)^2 = 1$$

   ce qui montre le résultat voulu.

Solution Q2. On aura besoin d'écrire les puissances de α sous forme polynomiale. Le calcul a déjà été entamé à la question précédente, mais poursuivons-le :

i	0	1	2	3	4	5
α^i	1	α	$\alpha - 1$	-1	$-\alpha$	$-\alpha + 1$

Maintenant, déterminons les classes cyclotomiques :

1. $C_0 = \{0\}$,
2. $C_1 = \{1, 5\}$,
3. $C_2 = \{2, 4\}$,

4. $C_3 = \{3\}$.

Par conséquent, les polynômes irréductibles de la factorisation de $x^6 - 1$ sont :

1. $M_0(x) = x - \alpha^0 = x - 1$
2. $M_1(x) = (x - \alpha)(x - \alpha^5) = x^2 - (\alpha + \alpha^5)x + \alpha^6 = x^2 - x + 1$,
3. $M_2(x) = (x - \alpha^2)(x - \alpha^4) = x^2 - (\alpha^2 + \alpha^4)x + \alpha^6 = x^2 + x + 1$,
4. $M_3(x) = x - \alpha^3 = x + 1$.

Solution Q3. Pour obtenir un code cyclique de dimension 4 et de longueur 6, il faut concevoir un diviseur de degré $6 - 4 = 2$ de $x^6 - 1$. Il y a exactement trois manières d'en obtenir :

1. $M_1(x) = x^2 - x + 1$,
2. $M_2(x) = x^2 + x + 1$,
3. $M_0(x)M_3(x) = (x - 1)(x + 1) = x^2 - 1$.

Exercice 3. Somme de codes cycliques (15 min).

Soient $\mathcal{A}$ et $\mathcal{B}$ deux codes linéaires de même longueur définis sur un même corps fini. On appelle **somme** de $\mathcal{A}$ et $\mathcal{B}$, notée $\mathcal{A} + \mathcal{B}$, l'espace vectoriel constitué des sommes d'éléments de $\mathcal{A}$ et de $\mathcal{B}$:

$$\mathcal{A} + \mathcal{B} = \{\boldsymbol{a} + \boldsymbol{b}, \boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B}\}.$$

Question 1.– Démontrer que si $\mathcal{A}$ et $\mathcal{B}$ sont deux codes cycliques, alors $\mathcal{A} + \mathcal{B}$ est également un code cyclique.

Question 2.– On suppose encore que $\mathcal{A}$ et $\mathcal{B}$ sont deux codes cycliques. Soit $a(x)$ le polynôme générateur de $\mathcal{A}$ et $b(x)$ le polynôme générateur de $\mathcal{B}$. Quel est le polynôme générateur de $\mathcal{A} + \mathcal{B}$?

Solutions de l'Exercice 3.

Solution Q1. Pour démontrer que $\mathcal{A} + \mathcal{B}$ est cyclique, on revient à la définition, et on démontre que la permutation cyclique de tout mot de $\mathcal{A} + \mathcal{B}$ reste dans $\mathcal{A} + \mathcal{B}$. Notons σ la permutation cyclique et considérons donc $\boldsymbol{a} \in \mathcal{A}$ et $\boldsymbol{b} \in \mathcal{B}$. Par linéarité on a alors :

$$\sigma(\boldsymbol{a} + \boldsymbol{b}) = \sigma(\boldsymbol{a}) + \sigma(\boldsymbol{b}).$$

Comme $\mathcal{A}$ est cyclique, on sait donc que $\sigma(\boldsymbol{a}) \in \mathcal{A}$. De même, $\sigma(\boldsymbol{b}) \in \mathcal{B}$. Par conséquent $\sigma(\boldsymbol{a} + \boldsymbol{b})$ s'écrit comme une somme d'éléments de $\mathcal{A}$ et de $\mathcal{B}$, il est donc dans $\mathcal{A} + \mathcal{B}$.

Observation. La propriété que l'on vient de démontrer provient en réalité d'un résultat plus général : la somme de deux idéaux est également un idéal.

Solution Q2. Adoptons ici le formalisme polynomial. On cherche à caractériser $g(x)$, le polynôme générateur de $\mathcal{A} + \mathcal{B}$, c'est-à-dire (voir théorème du cours) l'unique polynôme unitaire de $\mathcal{A} + \mathcal{B}$ qui divise tous les polynômes de $\mathcal{A} + \mathcal{B}$.

En particulier, $g(x)$ doit diviser tous les polynômes de $\mathcal{A} \subseteq \mathcal{A} + \mathcal{B}$ (donc doit diviser $a(x)$) et tous les polynômes de $\mathcal{B}$ (donc $b(x)$). Il divise donc le pgcd de $a(x)$ et $b(x)$, que l'on note $p(x)$. Montrons qu'en réalité, $g(x) = p(x)$.

Pour cela, il suffit de démontrer que $p(x)$ est dans le code $\mathcal{A} + \mathcal{B}$ (car le polynôme générateur d'un code divise tous les éléments du code). Utilisons l'identité de Bezout : il existe $u(x)$ et $v(x)$ tels que $p(x) = u(x)a(x) + v(x)b(x)$. Comme $a(x)$ engendre $\mathcal{A}$, le polynôme $u(x)a(x)$ est dans $\mathcal{A}$. De même $v(x)b(x) \in \mathcal{B}$. Par définition de la somme de deux codes, on en déduit que $p(x) \in \mathcal{A} + \mathcal{B}$.
