Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Codes algébriques – Solutions feuille de TD 3

09/02/2024

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

`https://lvzl.fr/teaching/2023-24/ca.html`

(⋆) exercice fondamental (⋆⋆) pour s'entraîner (⋆⋆⋆) pour aller plus loin 💻 sur machine

Exercice 1. (⋆) Calcul de classes cyclotomiques.

Question 1.– Pour $q = 3$ et $n = 11$, déterminer la classe cyclotomique de $b = 1$ modulo n sur $\mathbb{F}_q$.

Question 2.– Déterminer toutes les classes cyclotomiques modulo 15 sur $\mathbb{F}_2$.

Question 3.– Vrai ou faux ? Fixons q et n premiers entre eux.

1. Une classe cyclotomique modulo n sur $\mathbb{F}_q$ est également une classe cyclotomique modulo n sur $\mathbb{F}_{q^2}$.
2. Une classe cyclotomique modulo n sur $\mathbb{F}_{q^2}$ est également une classe cyclotomique modulo n sur $\mathbb{F}_q$.
3. Une classe cyclotomique modulo n sur $\mathbb{F}_q$ peut être partitionnée en classes cyclotomique modulo n sur $\mathbb{F}_{q^2}$.

Question 4.– Supposons que $n = q^2 - 1$. Déterminer toutes les classes cyclotomiques modulo n sur $\mathbb{F}_q$.

Solutions de l'Exercice 1.

Solution Q1. La classe cyclotomique de b modulo n sur $\mathbb{F}_q$ est l'ensemble $C_b = \{b, qb, \dots, q^{s-1}b\}$ où s est tel que $bq^s \equiv b \mod n$.

Ici, on a donc

$$C_b = \{1, 3, 9, 5, 4\}.$$

Solution Q2. Les classes cyclotomiques modulo 15 sur $\mathbb{F}_2$ sont :

— $C_0 = \{0\}$
— $C_1 = \{1, 2, 4, 8\}$
— $C_3 = \{3, 6, 12, 9\}$
— $C_5 = \{5, 10\}$
— $C_7 = \{7, 14, 13, 11\}$

Solution Q3.

1. Une classe cyclotomique modulo n sur $\mathbb{F}_q$ est de la forme $C_b = \{b, qb, \dots, q^{s-1}b\}$ où s est tel que $bq^s \equiv b \mod n$, tandis qu'une classe cyclotomique modulo n sur $\mathbb{F}_{q^2}$ est de la forme $C'_b = \{b, q^2b, \dots, q^{2(s'-1)}b\}$ où s' est tel que $bq^{2s'} \equiv b \mod n$.

   Ces ensembles ne sont donc généralement pas égaux. Par exemple, dans la question 2 on a $C_1 = \{1, 2, 4, 8\}$ et $C'_1 = \{1, 4\}$ pour la classe de 1 modulo 15 sur $\mathbb{F}_4$.

   Réponse plus avancée. En revanche, on peut noter que $C_b = C'_b$ lorsque l'entier s est impair ; par exemple, $C'_0 = C_0$, et pour l'exemple de la question 1, on a $C'_1 = \{1, 9, 4, 3, 5\} = C_1$. Ce résultat peut se démontrer. Notons $C_b = \{b, bq, \dots, bq^{s-1}\}$. Alors, pour s impair l'application $i \mapsto 2i \mod s$ est une bijection de $\{0, \dots, s-1\}$. Par conséquent$C_b = \{b, bq^2, \dots, bq^{2(s-1) \bmod s}\} = C'_b$.
2. On a répondu à cette question dans le point précédent.

3. C'est vrai. On peut toujours écrire :

$$C_b = \{b, bq, \dots, bq^{s-1}\} = \{b, bq^2, \dots, bq^{2(s-1) \mod s}\} \cup \{bq, bq^3, \dots, bq^{2(s-1)+1 \mod s}\} = C'_b \cup C'_{bq}$$

avec, ou bien une union disjointe, ou bien une égalité entre ces deux sous-ensembles (voir remarque précédente).

Solution Q4. On suppose que $n = q^2 - 1$, et on cherche à caractériser toutes les classes cyclotomiques C_b modulo n sur $\mathbb{F}_q$. Soit $b \in \{0, \dots, q^2 - 2\}$.

Rappelons qu'une classe cylctomique s'écrit $C_b = \{b, bq, \dots, bq^{s-1}\}$ où q est le plus petit entier strictement positif tel que $bq^s \equiv b \mod n$. Cherchons les valeurs possibles de s. Comme $n = q^2 - 1$, on a :

$$bq^s \equiv b \mod n \quad \iff \quad q^2 - 1 \text{ divise } b(q^s - 1)$$

Il y a donc deux possibilités.

1. Si b est un multiple de $q+1$, alors $q^2 - 1$ divise $b(q-1)$ donc $s = 1$. Puis on déduit que $C_b = \{b\}$.
2. Sinon, $q^2 - 1$ ne divise pas $b(q-1)$ mais il divise naturellement $b(q^2 - 1)$. Donc, $s = 2$ et $C_b = \{b, bq\}$.

Exercice 2. ($\star\star$) Divisiblité de polynômes.

Question 1.– Soient a et b deux entiers strictement positifs, et K un corps. Démontrer l'équivalence suivante :

$$x^a - 1 \text{ divise } x^b - 1 \text{ dans } K[x] \iff a \text{ divise } b \text{ dans } \mathbb{Z}.$$

Question 2.– Dans cette question on pose $K = \mathbb{F}_q$ et on fixe un entier n premier avec q. On note m l'ordre de q dans $(\mathbb{Z}/m\mathbb{Z})^\times$.

1. Déduire de la question précédente que $x^n - 1$ divise $x^{q^m - 1} - 1$.
2. Montrer que, pour tout $1 \leq s < m$, le polynôme $x^n - 1$ ne divise pas $x^{q^s - 1} - 1$.

Solutions de l'Exercice 2.

Solution Q1. Soient a, b deux entiers strictement positifs.

($\Leftarrow$) Supposons que a divise b dans $\mathbb{Z}$. Alors on a $b = ka$ pour un entier $k \geq 1$, et ainsi

$$x^b - 1 = x^{ka} - 1 = (x^a)^k - 1 = (x^a - 1)((x^a)^{k-1} + (x^a)^{k-2} + \dots x^a + 1)$$

Donc $x^a - 1$ divise $x^b - 1$.

($\Rightarrow$) Supposons que $x^a - 1$ divise $x^b - 1$ dans $K[x]$. Effectuons la division euclidienne de b par a : on a $b = at + r$ avec $0 \leq r < a$ et $t \in \mathbb{N}$. Alors,

$$x^b - 1 = x^{at+r} - 1 = x^{at+r} - x^r + x^r - 1 = x^r(x^{at} - 1) + x^r - 1\,.$$

Comme $x^a - 1$ divise $x^{at} - 1$ (vu précédemment), il divise donc également $x^b - 1 - x^r(x^{at} - 1) = x^r - 1$. Mais $r < a$ donc nécessairement $x^r - 1 = 0$, ce qui implique $r = 0$ puis $b = at$.

Solution Q2.

1. C'est une conséquence directe du fait que n divise $q^m - 1$ (car m est l'ordre multiplicatif de q modulo n), et de la question précédente.
2. Si $x^n - 1$ divise $x^{q^s - 1} - 1$, alors d'après la question 1, l'entier n divise $q^s - 1$, ce qui est impossible pour $s < m$ (par minimalité de m, l'ordre de q modulo n)

Exercice 3. ($\star\star$) Factorisation de $x^n - 1$ par les classes cyclotomiques.

Dans cet exercice, on pose $q = 3$ et $n = 8$.

Question 1.– Déterminer les classes cyclotomiques modulo n sur $\mathbb{F}_q$.

Question 2.– Déterminer le corps de décomposition de $x^n - 1$, c'est-à-dire la plus petite extension de $\mathbb{F}_3$ qui contient toutes les racines de $x^n - 1$.

Question 3.–

1. Montrer que $x^2 + 1$ est irréductible sur $\mathbb{F}_3$.
2. Soit β une racine de $x^2 + 1$ dans $\mathbb{F}_9$. L'élément β est-il une racine primitive 8-ème de l'unité ?

Question 4.–

1. Montrer que $x^2 + x - 1$ est irréductible sur $\mathbb{F}_3$.
2. Soit α une racine de $x^2 + x - 1$ dans $\mathbb{F}_9$. L'élément α est-il une racine primitive n-ème de l'unité ?

Question 5.– En utilisant la question 1 et la question 4, factoriser $x^n - 1$ dans $\mathbb{F}_3$.

Solutions de l'Exercice 3.

Solution Q1. On a

— $C_0 = \{0\}$
— $C_1 = \{1, 3\}$
— $C_2 = \{2, 6\}$
— $C_4 = \{4\}$
— $C_5 = \{5, 7\}$

Solution Q2. Le corps de décomposition de $x^n - 1$ est $\mathbb{F}_{q^m}$, où m est le cardinal de C_1. Donc, ici, $\mathbb{F}_{3^2} = \mathbb{F}_9$.

Solution Q3.

1. Pour vérifier qu'un polynôme de degré 2 est irréductible, il suffit de montrer qu'il n'admet pas de racine. Soit $P(x) = x^2 + 1 \in \mathbb{F}_3[x]$. On a $P(0) = 1$, $P(1) = 2$ et $P(2) = 2$, donc $P(x)$ n'admet aucune racine sur $\mathbb{F}_3$. Il est bien irréductible.
2. Soit $\beta \in \mathbb{F}_9$ tel que $\beta^2 + 1 = 0$. On a $\beta^4 = (\beta^2)^2 = (-1)^2 = 1$. Donc β n'est pas d'ordre 8, il n'est donc pas une racine **primitive** 8-ème de l'unité.

Solution Q4.

1. Soit $F(x) = x^2 + x - 1 \in \mathbb{F}_3[x]$. On a $F(0) = 2$, $F(1) = 1$ et $F(2) = 2$, donc $F(x)$ n'admet aucune racine sur $\mathbb{F}_3$. Il est bien irréductible.
2. Soit $\alpha \in \mathbb{F}_9$ tel que $\alpha^2 + \alpha - 1 = 0$. On a $\alpha^4 = (\alpha^2)^2 = (1 - \alpha)^2 = \alpha^2 + \alpha + 1 = -1 \neq 1$. Par ailleurs, $\alpha^8 = (\alpha^4)^2 = 1$. Donc l'ordre de α est exactement 8, et α est donc une racine **primitive** 8-ème de l'unité.

Solution Q5. On a trouvé une racine primitive n-ème de l'unité. On peut donc maintenant associer à chaque classe cyclotomique un diviseur irréductible de $x^n - 1$.

Pour rendre les calculs plus aisés, exprimons les puissances de α sous une forme "polynomiale" (il est conseillé de faire les calculs) :

α^i	1	α	α^2	α^3	α^4	α^5	α^6	α^7
	1	α	$-\alpha + 1$	$-\alpha - 1$	-1	$-\alpha$	$\alpha - 1$	$\alpha + 1$

— Pour $C_0 = \{0\}$, on obtient le diviseur
$$M_0(x) = x - \alpha^0 = x - 1$$
— Pour $C_1 = \{1, 3\}$, on obtient le diviseur
$$M_1(x) = (x - \alpha^1)(x - \alpha^3) = x^2 - (\alpha + \alpha^3)x + \alpha^4 x^2 + x - 1$$
— Pour $C_2 = \{2, 6\}$, on obtient le diviseur
$$M_2(x) = (x - \alpha^2)(x - \alpha^6) = x^2 - (\alpha^2 + \alpha^6) + \alpha^8 = x^2 + 1$$
— Pour $C_4 = \{4\}$, on obtient le diviseur
$$M_4(x) = x - \alpha^4 = x + 1$$
— Pour $C_5 = \{5, 7\}$, on obtient le diviseur
$$M_5(x) = (x - \alpha^5)(x - \alpha^7) = x^2 - (\alpha^5 + \alpha^7) + \alpha^{12} = x^2 - x - 1$$

La factorisation de $x^8 - 1$ en irréductibles de $\mathbb{F}_3[x]$ est donc :

$$(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1)\,.$$

Exercice 4. ($\star\star$) Classification des codes cycliques pour $q = 2$ et $n = 17$.

Question 1.– Déterminer les classes cyclotomiques modulo $n = 17$ sur $\mathbb{F}_2$.

Question 2.– Sans factoriser $x^n - 1$, en déduire le nombre de codes cycliques binaires de longueur 17, ainsi que leur dimension.

Solutions de l'Exercice 4.

Solution Q1. Les classes cyclotomiques modulo 17 sur $\mathbb{F}_2$ sont :

- $C_0 = \{0\}$
- $C_1 = \{1, 2, 4, 8, 16, 15, 13, 9\}$
- $C_3 = \{3, 6, 12, 7, 14, 11, 5, 10\}$

Solution Q2. Il y a 3 classes cyclotomiques, donc $x^{17} - 1$ admet 3 diviseurs irréductibles. Un code cyclique correspond donc à un produit (potentiellement vide) de ces trois diviseurs irréductibles. Il y a $2^3 = 8$ produits possibles, donc 8 codes cycliques binaires de longueur 17.

La dimension d'un code cyclique est $n - \deg(g)$, où g est le degré de son polynôme générateur. Ce degré est égal au cardinal de la réunion de classes cyclotomiques associée au polynôme.

Ici, on observe que les classes cyclotomiques ont cardinal 1, 8 et 8. Ainsi, les degrés des polynômes générateurs sont :

- $0 \times 1 + 0 \times 8 + 0 \times 8 = 0$, ce qui donne un code de dimension $17 - 0 = 17$;
- $0 \times 1 + 0 \times 8 + 1 \times 8 = 8$, ce qui donne un code de dimension $17 - 8 = 9$;
- $0 \times 1 + 1 \times 8 + 0 \times 8 = 8$, ce qui donne un code de dimension $17 - 8 = 9$;
- $0 \times 1 + 1 \times 8 + 1 \times 8 = 16$, ce qui donne un code de dimension $17 - 16 = 1$;
- $1 \times 1 + 0 \times 8 + 0 \times 8 = 1$, ce qui donne un code de dimension $17 - 1 = 16$;
- $1 \times 1 + 0 \times 8 + 1 \times 8 = 9$, ce qui donne un code de dimension $17 - 9 = 8$;
- $1 \times 1 + 1 \times 8 + 0 \times 8 = 9$, ce qui donne un code de dimension $17 - 9 = 8$;
- $1 \times 1 + 1 \times 8 + 1 \times 8 = 17$, ce qui donne un code de dimension $17 - 17 = 0$.

Exercice 5. ($\star\star$) Liste des codes cycliques pour $q = 2$ et $n = 7$.

Question 1.– Donner la liste de tous les codes cycliques binaires de longueur 7. On décrira ces codes par leur polynôme générateur, et on donnera leur dimension.

Solutions de l'Exercice 5.

Solution Q1. On reprend la méthode générale pour trouver tous les codes cycliques de longueur 7 sur $\mathbb{F}_2$.

Première étape : calcul des classes cyclotomiques. On a ici $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}$ et $C_3 = \{3, 5, 6\}$.

Deuxième étape : calcul d'une racine primitive de l'unité. Ce type de racine est à chercher parmi des racines de polynômes irréductibles de degré $m = \mathrm{ord}_7(2) = |C_1| = 3$. Or, un polynôme de degré 3 est irréductible s'il n'admet pas de racine. Sur $\mathbb{F}_2$, cela impose que le nombre de coefficients non-nuls du polynôme soit impair. En degré $m = 3$, le polynôme $P(x) = x^3 + x + 1$ convient (par exemple). On pose donc $\alpha \in \mathbb{F}_8$ telle que $\alpha^3 = \alpha + 1$ et on vérifie aisément que son ordre est 7 (il n'y a pas grand chose à vérifier, car 7 est premier...).

Troisème étape : calcul des diviseurs irréductibles de $x^n - 1$. Ces polynômes $M_b(x)$ ont pour racines les $\alpha^i, i \in C_b$. Pour les calculer précisément, on aura besoin de déterminer la forme polynomiale des α^i :

α^i	1	α	α^2	α^3	α^4	α^5	α^6
	1	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$

Puis on obtient les polynômes :

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

Quatrième étape : calcul des polynômes générateurs des codes cycliques. Pour cela, on effectue tous les produits possibles des $M_j(x)$:

1. le produit vide, qui donne le polynôme générateur $g_1(x) = 1$, donc le code cyclique de dimension $k = n - 0 = 7$ (c'est le code "plein")
2. $g_2(x) = M_0(x) = x + 1$, qui donne le code cyclique de dimension $k = 6$ (le code de parité)
3. $g_3(x) = M_1(x) = x^3 + x + 1$, qui donne un code cyclique de dimension $k = 4$
4. $g_4(x) = M_3(x) = x^3 + x^2 + 1$, qui donne un code cyclique de dimension $k = 4$
5. $g_5(x) = M_0(x)M_1(x) = x^4 + x^3 + x^2 + 1$, qui donne un code cyclique de dimension $k = 3$
6. $g_6(x) = M_0(x)M_3(x) = x^4 + x^2 + x + 1$, qui donne un code cyclique de dimension $k = 3$
7. $g_7(x) = M_1(x)M_3(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1$, qui donne un code cyclique de dimension $k = 1$ (le code de répétition)
8. $g_8(x) = M_0(x)M_1(x)M_3(x) = x^7 - 1 \equiv 0 \mod (x^7 - 1)$, qui donne un code cyclique de dimension $k = 0$ (le code nul)
