Sorbonne Université – Master de Physique et Applications

Symétries en Physique – Contrôle Continu – Corrigé

Jeudi 5 mars 2020

Durée 2h. Documents de cours autorisés, calculatrices et téléphones interdits.

1 Groupe multiplicatif des entiers modulo n *[20 points]*

Si le groupe $\mathbb{Z}_n$ est l'ensemble $\{0, 1, 2, ..., n-1\}$ muni de l'opération *addition modulo* n, on peut également « multiplier » les éléments de $\mathbb{Z}_n$. On n'obtient pas alors un groupe puisque, par exemple, 0 n'a pas d'inverse.

Cependant, si l'on se restreint aux éléments possédant un inverse (multiplicatif), on obtient un groupe, appelé « groupe des unités », noté U_n. Ce groupe U_n est donc un sous-ensemble de $\mathbb{Z}_n$ muni de l'opération *multiplication modulo* n, et ses éléments sont premiers avec n (c'est-à-dire qu'ils ne possèdent aucun diviseur commun autre que 1 [théorème de Bezout]).

Par exemple : $U_{14} = \{1, 3, 5, 9, 11, 13\}$ pour lequel on vérifie aisément que la multiplication de deux éléments appartient bien à U_{14} (par exemple, $3 * 9 = 27 = 13 \ (mod\ 14)$).

1. Généralités

   (a) Montrer que U_n, $n \geq 1$, est bien un groupe pour l'opération *multiplication modulo* n.

   Il y a quatre choses à montrer :

   1. L'opération *multiplication modulo* n est une loi de composition interne : Soient a et b deux éléments de U_n, alors ils possèdent par définition un inverse a^{-1} et b^{-1}, et :

$$\left(b^{-1}a^{-1}\right)(ab) = b^{-1}\left(a^{-1}a\right)b = b^{-1}b = 1$$
$$(ab)\left(b^{-1}a^{-1}\right) = a\left(bb^{-1}\right)a^{-1} = aa^{-1} = 1$$

   qui montre que ab possède bien un inverse dans U_n.
   2. La multiplication usuelle étant associative, l'associativité de la loi de groupe est automatiquement vérifiée.
   3. Chaque élément possède un inverse par définition de U_n.
   4. L'élément identité est 1, d'inverse 1 appartenant à U_n.

   (b) U_n est-il abélien ?

   La multiplication usuelle étant commutative, le groupe U_n est abélien.

(c) Si n est un nombre premier, quel est l'ordre de U_n ?

Un élément de U_n étant un entier compris entre 0 et n qui ne possède pas de diviseur commun avec n, les seuls éléments de U_n lorsque n est premier sont : $\{1, 2, ..., n-1\}$. D'où : $|U_n| = n - 1$.

2. Groupe U_{16}

(a) Faire la liste des éléments de U_{16}

$$U_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\}$$

Qu'on a construit en enlevant de $\mathbb{Z}_{16}$ le nombre 0 (car ne possèdant pas d'inverse) et les nombres pairs (car multiples de 2, le seul diviseur primaire de $16 = 2^4$).

(b) Quels sont les ordres possibles des différents éléments de U_{16} ? (justifier)

Comme il y a 8 éléments dans U_{16}, un des théorèmes de Lagrange nous indique que les seuls ordres possibles des éléments de U_{16} sont les entiers qui divisent 8, soit :

$$1, 2, 4, 8$$

(c) A quel groupe, parmi les trois suivants, le groupe U_{16} est-il isomorphe ? (justifier)

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_4 \quad et \quad \mathbb{Z}_8$$

Attention, chacun des 3 groupes proposés possède bien 8 éléments ! Par contre, l'ordre des éléments dans chacun de ces groupes n'est pas le même. Dans le groupe $\mathbb{Z}_p$, l'ordre des éléments est au plus p, et il y a au moins un des éléments qui a p pour ordre.
Ainsi, dans $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, il n'y a que des éléments d'ordre au plus 2. Dans le groupe $\mathbb{Z}_2 \times \mathbb{Z}_4$, l'ordre des éléments est au plus égal à 4 et au moins un des éléments a un ordre égal à 4, et pour $\mathbb{Z}_8$, il y a au moins un élément d'ordre 8.

Qu'en est-il ici ? Par exemple, prenons « 3 », le deuxième élément de U_{16} :

$$3^2 = 9,\ 3^3 = 27 = 11\ (mod\ 16)\,,\ 3^4 = 81 = 1\ (mod\ 16)$$

Ainsi, 3 est d'ordre 4 (ce qui élimine de facto le groupe $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$).
Voyons s'il y a des éléments d'ordre 8.

$$5^2 = 25 = 9 \ (mod\ 16)$$
$$7^2 = 49 = 1 \ (mod\ 16)$$
$$9^2 = 81 = 1 \ (mod\ 16)$$
$$11^2 = 121 = 9 \ (mod\ 16)$$
$$13^2 = 169 = 9 \ (mod\ 16)$$
$$15^2 = 225 = 1 \ (mod\ 16)$$

qui montrent que 7**,** 9 **et** 15 **sont d'ordre 2, et que** 5**,** 11 **et** 13 **sont d'ordre 4.**

Puisqu'il n'y a pas d'élément d'ordre 8 et qu'il n'y a que des éléments d'ordre 1 (l'élément « 1 »), 2 ou 4, le groupe isomorphe à U_{16} **est** $\mathbb{Z}_2 \times \mathbb{Z}_4$**.**

3. Groupe U_{20}

(a) Faire la liste des éléments de U_{20}.

$$U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

où on a enlevé de $\mathbb{Z}_{20}$ **le nombre** 0 **(car ne possèdant pas d'inverse), les multiples de 2 et les multiples de 5 puisque étant les diviseurs de** $20 = 2^2 * 5$**.**

(b) Faire la liste des éléments du sous-groupe $\langle 19 \rangle$ généré par 19.

Le sous-groupe $\langle 19 \rangle$ **de** U_{20} **est formé des puissances de** 19 **appartenant à** U_{20}**. Comme** $19^2 = 361 = 1 \ (mod\ 20)$**, ce sous-groupe ne contient que 2 éléments :**

$$\langle 19 \rangle = \{1, 19\}$$

(c) Déterminer les classes de U_{20} suivant $\langle 19 \rangle$. On les notera sous la forme « $\overline{N}$ » avec N le plus petit nombre entier de chaque classe.

Puisque $|U_{20}| = 8$ **et que** $|\langle 19 \rangle| = 2$**, un des théorèmes de Lagrange nous indique qu'il y a** $8/2 = 4$ **classes d'équivalence de** U_{20} **suivant** $\langle 19 \rangle$**, chacune contenant le même nombre d'élément (2).**
Une première classe est le sous-groupe lui-même :

$$\overline{1} = \langle 19 \rangle = \{1, 19\}$$

Pour obtenir une autre classe, il suffit de prendre un élément de U_{20} **n'appartenant pas à** $\langle 19 \rangle$ **et de le multiplier par les éléments de** $\langle 19 \rangle$**.**
Par exemple, $3 * \langle 19 \rangle = \{3, 57\} = \{3, 17 \ (mod\ 20)\}$**. La deuxième classe de** U_{20} **suivant** $\langle 19 \rangle$ **est donc**

$$\overline{3} = \{3, 17\}$$

Puis : $7 * \langle 19 \rangle = \{7, 133\} = \{7, 13 \ (mod\ 20)\}$

$$\overline{7} = \{7, 13\}$$

et enfin

$$\overline{9} = \{9, 11\}$$

Attention, seul $\overline{1} = \langle 19 \rangle = \{1, 19\}$ est un sous-groupe de U_{20}.

(d) Calculer $\overline{3} * \overline{9}$ dans U_{20}.

La multiplication de deux classes fonctionne de la façon suivante : prendre un élément de chaque classe (n'importe lequel !), les multiplier et voir à quelle classe appartient le résultat. Ici, prenons par exemple 3 dans $\overline{3}$ et 11 dans $\overline{9}$, on obtient $33 = 13 \ (mod\ 20)$, qui appartient à la classe $\overline{7}$, d'où :

$$\overline{3} * \overline{9} = \overline{7}$$

(e) Calculer $\overline{3}^{\,-1}$ dans U_{20}.

Pour le calcul d'un inverse, il suffit de regarder ce que donne la mutiplication d'un élément de chaque classe par un élément de $\overline{3}$, et détecter lequel donne un nombre appartenant à $\overline{1}$.
Ici, on a de façon évidente $3 * 7 = 21 = 1 \ (mod\ 20)$, d'où $\overline{3} * \overline{7} = \overline{1}$:

$$\overline{3}^{\,-1} = \overline{7}$$

(f) Calculer $\overline{9}^{\,3}$ dans U_{20}.

Comme précédemment, il suffit de choisir l'un des éléments de $\overline{9}$, de lui faire l'opération requise, ici mettre au cube, et de voir à quelle classe appartient le résultat. Prenons 11 par exemple : $11^2 = 121$ et $11^3 = 121 * 11 = 1331 = 11 \ (mod\ 20)$ appartenant à $\overline{9}$. D'où :

$$\overline{9}^3 = \overline{9}$$

(g) Construire la table de Cayley du groupe quotient $U_{20}/\langle 19 \rangle$.

Le groupe quotient $U_{20}/\langle 19 \rangle$ est, par définition, le groupe à 4 éléments formé des classes d'équivalence de U_{20} suivant $\langle 19 \rangle$, c'est-à-dire

$$U_{20}/\langle 19 \rangle = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$$

On utilise alors le même principe qu'à la question précédente pour construire

la table de multiplication de ce groupe. On obtient :

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{1}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{1}$	$\overline{9}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{7}$	$\overline{3}$	$\overline{1}$

qui est symétrique par rapport à la diagonale comme pour tout groupe abélien.

(h) Ce groupe quotient est-il isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_2$ ou à $\mathbb{Z}_4$? (justifier)

Puisque qu'au moins un élément (et même deux : $\overline{3}$ et $\overline{7}$) est d'ordre 4, cela ne peut être que $\mathbb{Z}_4$.

2 Représentations irréductibles du groupe dihédral *[20 points]*

Soit n un entier supérieur ou égal à 2. On note C_n le groupe cyclique d'ordre n et D_{2n} le groupe dihédral d'ordre $2n$:

$$C_n = \left\{I, r, r^2, ..., r^{n-1}\right\}$$
$$D_{2n} = \left\{I, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\right\}$$

avec

$$r^n = I \ , \ s^2 = I \ , \ srsr = I \tag{1}$$

NB : les éléments r et s peuvent être vus comme, respectivement, une rotation d'angle $2\pi/n$ et une symétrie de réflection.

1. Le groupe C_n est-il abélien ? En déduire le nombre et la dimension de ses représentations irréductibles inéquivalentes.

   Les rotations commutant entre elles, le groupe C_n est abélien. Il en résulte que toutes les représentations irréductibles (« irreps ») de C_n sont de dimension 1. La relation fondamentale entre les dimensions des irreps ρ_j, le nombre N_{irrep} d'irreps inéquivalentes et la dimension du groupe

   $$\sum_{j=1}^{N_{irrep}} |\mathbf{dim}\,(\rho_j)|^2 = |C_n| = n$$

   conduit alors à

   $$\sum_{j=1}^{N_{irrep}} |\mathbf{dim}\,(\rho_j)|^2 = \sum_{j=1}^{N_{irrep}} 1 = N_{irrep} = n$$

   c'est-à-dire qu'il y a n irreps de dimension 1.

2. Montrer que $sr^p s = r^{-p}$ pour $0 \leq p \leq n-1$, et en déduire que les éléments r^p et r^{n-p} sont conjugués dans D_{2n}.

   On a

   $$sr^2 s = srssrs = \left(r^{-1}\right)^2 = r^{-2}$$

   puisque $s^2 = I$.

   En généralisant :

   $$sr^p s = (srs)^p = \left(r^{-1}\right)^p = r^{-p} = r^{n-p}$$

   puisque $r^{-p} = r^{-p} * I = r^{-p} * r^n = r^{n-p}$.

   Ensuite, on applique la définition : dans un groupe, deux éléments a et b sont conjugués s'il existe un élément g tel que $a = gbg^{-1}$.
   Ici, c'est bien le cas entre r^p et r^{n-p} avec $g = s = s^{-1}$.

3. Montrer que r^p et $r^{p'}$ sont conjugués dans D_{2n} si et seulement si $p - p' = 0 \ (mod\, n)$ ou $p + p' = 0 \ (mod\, n)$.

Regardons la conjugaison de r^p et $r^{p'}$ par l'intermédiaire de chaque élément g de D_{2n}. Puisqu'un élément quelconque de D_{2n} est forcément du type r^q (d'inverse r^{-q}) ou sr^q(d'inverse $r^{-q}s^{-1} = r^{-q}s$), avec $0 \leq q \leq n-1$, il suffit de vérifier la relation de conjugaison pour ces deux cas génériques :

$$r^{p'} = r^q r^p \left(r^q\right)^{-1} = r^{q+p-q} = r^p \qquad \longrightarrow \qquad p' = p \ (mod\, n)$$

$$r^{p'} = \left(sr^q\right) r^p \left(sr^q\right)^{-1} = sr^q r^p r^{-q} s = sr^p s = r^{-p} \qquad \longrightarrow \qquad p' = -p \ (mod\, n)$$

4. En déduire que les classes de conjugaison des rotations dans D_{2n} sont au nombre de $\frac{n+1}{2}$ si n est impair et $\frac{n}{2} + 1$ si n est pair. Donner également la liste de ces classes de conjugaison.

Du fait que les rotations r^p et r^{n-p} sont conjugués dans D_{2n} et que l'identité I forme une classe de conjugaison à elle seule, on obtient $(n-1)/2$ paires de rotations conjuguées lorsque n est impair :

$$n \textbf{ impair } : \{I\}, \left\{r, r^{n-1}\right\}, \left\{r^2, r^{n-2}\right\}, ..., \left\{r^{(n-1)/2}, r^{(n+1)/2}\right\}$$

Pour n pair, il y a le cas particulier de la rotation $r^{n/2}$ qui est conjuguée à elle-même, d'où seulement $\frac{n}{2} - 1$ paires de rotations distinctes conjuguées :

$$n \textbf{ pair } : \{I\}, \left\{r, r^{n-1}\right\}, \left\{r^2, r^{n-2}\right\}, ..., \left\{r^{n/2-1}, r^{n/2+1}\right\} \left\{r^{n/2}\right\}$$

Au final, le décompte des classes donne bien le résultat recherché : $\frac{n+1}{2}$ classes si n est impair et $\frac{n}{2} + 1$ classes si n est pair.

5. Déterminer les classes de conjugaison des symétries sr^p dans D_{2n} selon que n est pair ou impair.

Pour que sr^p soit conjuguée à $sr^{p'}$, il faut et il suffit qu'il existe un entier q tel que

$$sr^{p'} = \left(sr^q\right) sr^p \left(sr^q\right)^{-1} = sr^q sr^p r^{-q} s = sr^q sr^{p-q} s = sr^q r^{q-p} = sr^{2q-p} \qquad \longrightarrow \qquad p+p' = 2q \ (mod\, n)$$

(par l'intermédiaire d'une symétrie $g = sr^q$), ou

$$sr^{p'} = \left(r^q\right) sr^p \left(r^q\right)^{-1} = r^q sr^{p-q} = sr^{p-2q} \qquad \longrightarrow \qquad p - p' = 2q \ (mod\, n)$$

(par l'intermédiaire d'une rotation $g = r^q$, et où on a utilisé la relation de la question 2 : $r^q s = sr^{-q}$).

Si n est impair, la quantité $2q \ (mod\, n)$ peut redonner tous les nombres pairs

et impairs voulus pour $p \pm p'$ et il existe donc bien un tel nombre q pour chaque couple (p, p') de symétries conjuguées. Il y a donc une seule classe de conjugaison :

$$n \textbf{ impair } : \left\{s, sr, sr^2, ..., sr^{n-1}\right\}$$

Si n est pair, ce n'est plus le cas et les symétries se rangent dans deux classes, différant par une puissance simple de r :

$$n \textbf{ pair } : \left\{s, sr^2, sr^4, ..., sr^{n-2}\right\}, \left\{sr, sr^3, sr^5, ..., sr^{n-1}\right\}$$

6. Soit $\rho : D_{2n} \longrightarrow \mathbb{C}^*$ une représentation unidimensionnelle de D_{2n}, et soient les nombres $a = \rho(r)$ et $b = \rho(s)$.

   (a) Déduire de (1) les conditions auxquelles obéissent les nombres a et b.

   Par définition d'une représentation, on a

   $$\forall A, B,\ \rho(AB) = \rho(A)\,\rho(B)$$

   et

   $$\rho(I) = 1$$

   d'où ici

   $$\begin{aligned} \rho(r^n) &= (\rho(r))^n = a^n = 1 \\ \rho\left(s^2\right) &= (\rho(s))^2 = b^2 = 1 \\ \rho(srsr) &= \rho(s)\,\rho(r)\,\rho(s)\,\rho(r) = baba = b^2a^2 = 1 \end{aligned}$$

   Les deux dernières égalités donnant

   $$a^2 = 1$$

   Les conditions $b^2 = 1$ et $a^2 = 1$ conduisent alors aux quatre possibilités suivantes pour le couple (a, b) :

   $$\begin{aligned} a &= \pm 1 \\ b &= \pm 1 \end{aligned}$$

   Remarque : quelle que soit la représentation (irréductible de dimension 1) considérée, la donnée des nombres a et b suffit à complétement la caractériser (puisque tout élément de D_{2n} peut s'écrire comme un produit de s et d'une puissance de r). Il s'en suit qu'il y a au plus 4 irreps de dimension 1 de D_{2n}.

   (b) Montrer que $a = 1$ et $b = \pm 1$ si n est impair, et en déduire qu'il n'y a alors que deux représentations de dimension 1 pour n impair (notées ρ_1 pour la représentation triviale et ρ_1' pour l'autre).

La relation $a^n = 1$ combinée à $a = \pm 1$ implique que $a = 1$ si n est impair. On en déduit qu'i n'y a que deux possibilités pour une irrep de dimension 1 : $a = 1$ et $b = \pm 1$:

$$\begin{array}{lll} \rho_1 & \textit{telle que} : & \rho_1(r) = 1 = \rho_1(s) \\ \rho_1' & \textit{telle que} : & \rho_1'(r) = 1\ ,\ \rho_1'(s) = -1 \end{array}$$

L'irrep ρ_1 est la représentation identité : à chaque élément de D_{2n}, elle associe le nombre 1.
L'irrep ρ_1' est la représentation signature : à chaque élément de D_{2n}, elle associe soit le nombre 1 (rotations) soit le nombre -1 (symétries avec s). cf. la question suivante.

(c) *BONUS : Que valent $\rho_1'(r^p)$ et $\rho_1'(sr^p)$ pour $0 \leq p \leq n-1$? (pour n* impair)

$$\rho_1'(r^p) = (\rho_1'(r))^p = 1^p = 1$$
$$\rho_1'(sr^p) = \rho_1'(s)\,\rho_1'(r^p) = -1 * 1 = -1$$

(d) Montrer que $a = \pm 1$ et $b = \pm 1$ si n est pair, et en déduire deux autres représentations de dimension 1 pour n pair (notées ρ_2 et ρ_2').

Si n est pair, la relation $a^n = 1$ ne nous dit rien de plus par rapport à la valeur de a. On a donc les quatre possibilités $(a = \pm 1, b = \pm 1)$.
Les deux cas $(a = +1, b = \pm 1)$ correspondent aux deux irreps précédentes : ρ_1 et ρ_1'.
Les deux autres cas $(a = -1, b = \pm 1)$ donnent deux autres irreps de dimension 1, celles définies par :

$$\begin{array}{lll} \rho_2 & \textit{telle que} : & \rho_2(r) = -1\ ,\ \rho_2(s) = 1 \\ \rho_2' & \textit{telle que} : & \rho_2'(r) = -1 = \rho_2'(s) \end{array}$$

(e) *BONUS : Que valent $\rho_2(r^p)$, $\rho_2(sr^p)$, $\rho_2'(r^p)$ et $\rho_2'(sr^p)$ pour $0 \leq p \leq n-1$? (pour n* pair)

$$\rho_2(r^p) = (\rho_2(r))^p = (-1)^p$$
$$\rho_2(sr^p) = \rho_2(s)\,\rho_2(r^p) = (-1)^p$$

$$\rho_2'(r^p) = (\rho_2'(r))^p = (-1)^p$$
$$\rho_2'(sr^p) = \rho_2'(s)\,\rho_2'(r^p) = (-1)^{p+1}$$

7. On peut montrer que les autres représentations irréductibles inéquivalentes de D_{2n} sont toutes de dimensions 2.

Remarque : cela se justifie de diverses manières, en utilisant par exemple une représentation induite de C_n vers D_{2n}, ou bien en invoquant la propriété suivante

« Soit $\rho : G \longrightarrow GL(E)$ une représentation irréductible de G, et H un sous-groupe abélien de G, alors $dim(E) \leq |G| / |H|$ »

appliquée à $G = D_{2n}$ (de dimension $2n$) et $H = C_n$ (de dimension n) et qui implique que les irreps de D_{2n} sont nécessairement de dimension inférieure à 2, c'est-à-dire 1 ou 2.

(a) En utilisant un théorème fondamental liant leurs dimensions à l'ordre du groupe, déterminer leur nombre pour n pair puis pour n impair.

Comme à la question 1, on utilise la relation fondamentale entre les dimensions des irreps ρ_j, le nombre N_{irrep} d'irreps inéquivalentes et la dimension du groupe

$$\sum_{j=1}^{N_{irrep}} |\mathbf{dim}(\rho_j)|^2 = |D_{2n}| = 2n$$

sachant qu'ici $\mathbf{dim}(\rho_j)$ est égal à 1 ou 2.

Dans le cas où n est impair, on sait (cf les questions précédentes) qu'il y a 2 irreps de dimension 1. Le nombre N_{irrep2} d'irreps de dimension 2 est donc déduit de l'équation

$$1^2 + 1^2 + \sum_{j=1}^{N_{irrep2}} 2^2 = |D_{2n}| = 2n$$

c'est-à-dire

$$N_{irrep2} = \frac{2n-2}{4} = \frac{n-1}{2}$$

Dans le cas où n est pair, il y a 4 irreps de dimension 1. Le nombre N'_{irrep2} d'irreps de dimension 2 est donc déduit de l'équation

$$1^2 + 1^2 + 1^2 + 1^2 + \sum_{j=1}^{N'_{irrep2}} 2^2 = |D_{2n}| = 2n$$

c'est-à-dire

$$N'_{irrep2} = \frac{2n-4}{4} = \frac{n}{2} - 1$$

(b) En déduire le nombre total de classes de conjugaison de D_{2n} pour n pair puis pour n impair. Vérifier que ces résultats sont bien cohérents avec les réponses aux questions 4

et 5.

Le nombre de classes de conjugaison étant égal au nombre d'irreps non-équivalentes, on en déduit qu'il y a $2 + N_{irrep2} = \frac{n+3}{2}$ classes de conjugaison de D_{2n} pour n impair, et $4 + N'_{irrep2} = \frac{n}{2} + 3$ classes de conjugaison pour n pair.

Ces résultats sont bien entendu conformes avec les résultats des questions 4 et 5 où l'on a vu que les classes de conjugaison étaient au nombre de $\frac{n+1}{2}+1 = \frac{n+3}{2}$ ($\frac{n+1}{2}$ classes de rotation et 1 regroupant les symétries-réflections) si n était impair, et $\frac{n}{2} + 1 + 2 = \frac{n}{2} + 3$ ($\frac{n}{2} + 1$ classes de rotation et 2 regroupant les symétries-réflections) si n était pair.