Ecole Polytechnique Fédérale de Lausanne

Sciences de l'information

Série 8

Olivier Cloux

8.1

1. Ce groupe n'est pas commutatif, car il n'existe pas d'élément symétrique pour les éléments différents de 0.

2. Ce groupe est commutatif. En effet, il répond à tous les critères :
   - L'addition est associative, aussi avec des entiers.
   - L'élément neutre est $e = 0$ car $a + 0 = a \ \forall a \in \mathbb{Z}$
   - Le symétrique est $-a$, car $a + (-a) = 0 = e \ \forall a \in \mathbb{Z}$
   - $a + b = b + a \ \forall a, b \in \mathbb{Z}$

3. Notre élément neutre est $e = 1$, car $a \cdot 1 = a \ \forall a \in \mathbb{Z}$.
   Malheureusement, il n'y a pas d'élément inverse pour 0. En effet, $0 \cdot a = 0 \neq 1 = e \ \forall a \in \mathbb{Z}$ Donc ce groupe n'est pas commutatif

4. Soient A et B deux angles de matrices de rotations.
$$\begin{pmatrix} \cos(A) & -\sin(A) \\ \sin(A) & \cos(A) \end{pmatrix} \cdot \begin{pmatrix} \cos(B) & -\sin(B) \\ \sin(B) & \cos(B) \end{pmatrix}$$
$$= \begin{pmatrix} \cos(A)\cos(B) - \sin(A)\sin(B) & -\cos(A)\sin(B) - \sin(A)\cos(B) \\ \sin(A)\cos(B) + \cos(A)\sin(B) & -\sin(A)\sin(B) + \cos(A)\cos(B) \end{pmatrix}$$
$$= \begin{pmatrix} \cos(A+B) & -\sin(A+B) \\ \sin(A+B) & \cos(A+B) \end{pmatrix}$$
   (selon les lois d'addition trigonométriques). Nous voyons bien que cela correspond aussi à une matrice de rotation. Cela nous indique qu'appliquer deux matrices de rotation à la suite revient à additionner les angles de rotation. Regardons si cela correspond aux critères d'un groupe commutatif :
   - Associativité : Appliquer trois matrices de rotations à la suite, respectivement $(A+(B+C))$ ou $(A+B)+C$ revient dans tous les cas à additionner les angles A, B, C (nous savons que l'addition est associative). Donc l'associativité est respectée.

- Notons $E = 0$ l'élément (angle) neutre. Faire une rotation de $A + E$ degrés $= A + 0 = A$ degrés, pour tout A. D'ailleurs, prendre un angle de 0 donnera la matrice I_2, donc multiplier une matrice quelconque[1] par la matrice identité ne changer pas notre matrice quelconque
- L'élément symétrique à A est $-A$. En effet, $A + (-A) = 0 = E$. Cela donnera par ailleurs la matrice I_2, donc aucune rotation.
- Pour finir, faire une rotation de A puis B degrés ou B puis A degrés donne toujours $A + B = B + A$ degrés. Dons la commutativité est respectée.

Tous ces éléments nous permettent de conclure que nous sommes en présence d'un magnifique groupe commutatif.

8.2

1. $\mathbb{Z}/mZ^*$ représente l'ensemble des éléments inversibles de $\mathbb{Z}/m\mathbb{Z}$. Les éléments inversibles sont ceux qui sont inférieurs à m et premiers avec lui. Dans le cas de 15, il y a 8 éléments, qui sont :

$$[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}$$

2.

$(\mathbb{Z}/15\mathbb{Z}^*, \cdot)$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

3. Notons que dans $(\mathbb{Z}/15\mathbb{Z}^*, \cdot)$ l'élément neutre est $[1]_{15}$. Nous allons donc aller au cas par cas :
   - $[1]_{15}$: sa période est simplement 1, car $([1]_{15})^1 = [1]_{15}$
   - $[2]_{15}$: il est facile de voir que sa période est 4, car $([2]_{15})^4 = [16]_{15} = [1]_{15}$
   - $[4]_{15}$: dans la même idée que pour 2, sa période est 2, car $([4]_{15})^2 = [16]_{15} = [1]_{15}$
   - $[7]_{15}$: il faut ici essayer différents k : après quelques essais, nous trouvons $k = 4$, car $([7]_{15})^4 = [2041]_{15} = [1]_{15}$
   - $[8]_{15}$: pareil ici : il faut simplement essayer différents k ; après quelques essaie infructueux, nous trouvons finalement $k = 4$, car $([8]_{15})^4 = [4096]_{15} = [1]_{15}$
   - $[11]_{15}$: nous avons vu dans le tableau de multiplication que $([11]_{15})^2 = [1]_{15}$, donc la période $k = 2$.
   - $[13]_{15}$: comme pour 7 et 8, nous essayons quelques chiffres. À nouveau, c'est 4 qui est la solution ($13^4 = 28561,\ 13^4 \mod 15 = 1$)
   - $[14]_{15}$: ici nous regardons encore dans le tableau pour voir que $14^2 \mod 15 = 1$, donc la période $k = 2$

4. Pour qu'un isomorphisme soit possible, il faut que les deux groupes aient la même cardinalité. Ainsi, le seul k possible est 8, car alors le nombre d'éléments dans chaque ensemble sera le même (8)
   Nous regardons donc s'il existe un isomorphisme entre $(\mathbb{Z}/15\mathbb{Z}^*, \cdot)$ et $(\mathbb{Z}/8\mathbb{Z}, +)$. Nous devons

[1] de bonne taille

pour cela comparer la table de multiplication (vue au dessus, au point 2.) et la table d'addition, ci dessous :

$(\mathbb{Z}/8\mathbb{Z},+)$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$(\mathbb{Z}/15\mathbb{Z}^*,\cdot)$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Le but serait alors de réarranger les lignes et colonnes de la multiplication de manière à ce que, en renommant les éléments, nous obtenions les même que dans l'addition (ou inversement, évidemment).
Un gros problème se pose à nous ici. Nous voyons que dans la diagonale de l'addition, nous avons 4 éléments distincts (0,2,4,6). Or, dans la diagonale de la multiplication, nous n'avons que deux éléments (1 et 4). Comme déplacer les colonnes/lignes conservera les éléments dans la diagonale (ne fera que les "réarranger"), nous aurons toujours 2 éléments distincts. Il n'y a aucun renommage qui permette de changer cela.

En conclusion : comme il n'y a qu'un seul k possible, et que ce k ne permet aucun isomorphisme, alors il n'existe aucun k tel que ces deux groupes soient isomorphes.

8.3

1. Rappelons nous tout d'abord la table du xor :

$\bigoplus$	0	1
0	0	1
1	1	0

Cela nous permet de comprendre la chose de manière instinctive. Donné un symbole binaire, le faire xor avec un 1 change le symbole, et le faire xor avec un 0 le laissera tel quel. Examinons maintenant les critères :

- Associativité : Appliquer une séquence binaire sur une autre séquence binaire se fera comme dit au dessus : appliquer un 1 changera le symbole, appliquer un 0 le gardera intact. De plus, modifier ou non un symbole n'a aucun effet sur les autres symboles de la séquence. Prenons donc une chaîne a de longueur 1 (nous pourrons par la suite généraliser, car nous savons que ce qui s'applique à un symbole s'applique à n). Si nous lui appliquons un symbole b (qui le changera ou non) puis un autre c (qui le re-modifiera ou non), nous aurons un symbole identique (ou non) à celui de départ. Si en revanche, nous prenons faisons $d = b \bigoplus c$, nous obtiendrons, en fonction des deux symboles, un d qui modifiera ou pas a (j'espère que vous me suivez). Puis $a \bigoplus d$ re-modifiera a, mais toujours en fonction de b et c. Prenons une exemple concret : si $b = c = 1$, alors $d = 0$, donc $a \bigoplus d = a$. De même que $(a \bigoplus b) \bigoplus c = \overline{a} \bigoplus c = a$. Donc l'associativité est respectée.
- L'élément (la chaîne) neutre est $E = \{0\}^n$ (une chaîne de même longueur que A, composée uniquement de 0). En effet, comme $a \bigoplus 0 = a$, n'avoir que des 0 ne modifiera pas du tout la chaîne A.
- L'élément symétrique de A est... A lui même. En effet, nous voyons dans le tableau que $a \bigoplus a = 0$ pour $a = \{1, 0\}$. Donc faire une chaîne xor elle-même met tous les éléments à 0, donc nous auront une chaîne de longueur n composée de 0 uniquement (ce qui est E).
- Finalement, nous n'avons qu'à regarder le tableau pour comprendre que la commutativité est respectée. La diagonale est triviale (faire $1 \bigoplus 1$ ou $1 \bigoplus 1$ ne change pour ainsi dire rien,

et faire $1 \bigoplus 0$ ou $0 \bigoplus 1$ est également similaire (nous le voyons dans la table du xor.)

2. Notons tous nos tableaux, pour $n = 2$:

$(A, \bigoplus)$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

$(\mathbb{Z}/4\mathbb{Z})$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}/2\mathbb{Z})^2$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Cela nous permet déjà d'affirmer que notre second tableau est tout à fait différent des autres, donc il ne peut pas exister d'isomorphisme avec les autres. En effet, sa diagonale contient 2 éléments (0 et 2) alors que les deux autres n'ont qu'un seul élément dans la diagonale. Nous avons montré précédemment que swapper des colonnes (donc des lignes aussi) gardera toujours la valeur des diagonales, en ne faisant que les déplacer sur cette même diagonale. Il n'y a donc pas de renommage possible, donc pas d'isomorphisme.

Restent donc les cas 1 et 3. Il est intéressant de constater que les deux tableaux sont les mêmes. Même en prenant un n plus grand, les tableaux resteraient identiques. Cela s'explique simplement, car les deux représentent la même opération. Il s'agit dans les deux cas d'une addition bit à bit sans retenue. A aura une longueur de n, et $(\mathbb{Z}/2\mathbb{Z})^n$ représente n symboles, soit 1 soit 0 (car plus petit que 2). Dans les deux cas, faire (1 et 1) ou (0 et 0) donne 0, alors que (1 et 0) ou (0 et 1) donne 1. Les opérations sur un symbole n'influences pas les autres ; tout cela mit ensemble démontre qu'il s'agit d'une simple réécriture du groupe. il existe donc un isomorphisme, qui renvoie un élément sur lui-même.