

F4 Éléments de construction

(Ex1) Supposons par l'absurde que $f: \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$ est un morphisme de groupes, on a alors $f(\bar{0}) = \bar{0}$ et $f(\bar{1}) \in \{\bar{0}, \bar{1}, \bar{2}\}$. Si $f(\bar{1}) = \bar{0}$ alors le morphisme est trivial, on cherche un morphisme non trivial.

Si $f(\bar{1}) = \bar{1}$, alors $f(\bar{1} + \bar{1}) = f(\bar{0}) = \bar{0} = f(\bar{1}) + f(\bar{1}) = \bar{2}$, impossible.

Si $f(\bar{1}) = \bar{2}$, alors $f(\bar{1} + \bar{1}) = f(\bar{0}) = \bar{0} = f(\bar{1}) + f(\bar{1}) = \bar{2} + \bar{2} = \bar{1}$, impossible.

Donc il n'y a pas de morphisme non trivial de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$.

Une raison plus simple sera mise en évidence à l'exercice 3. On peut dire aussi que si f est non trivial, l'inverse et de $f \in \mathbb{Z}/3\mathbb{Z}$. Cela est impossible car 2+3.

(Ex2) Comme $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique engendré par $\bar{1}$,

pour définir un morphisme $f: \mathbb{Z}/n\mathbb{Z} \rightarrow (G, *)$ avec G groupe, il suffit de donner l'image de $\bar{1}$, ensuite on aura par cyclicité $f(\bar{k}) = f(\underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{\text{de } k \text{ fois}}) = \underbrace{f(\bar{1}) * f(\bar{1}) * \dots * f(\bar{1})}_{\text{de } k \text{ fois}}$.

Si $G = \mathbb{Z}/15\mathbb{Z}$ et si $f(\bar{1}) = \bar{3}$ alors $f(\bar{k}) = \underbrace{\bar{3} + \bar{3} + \dots + \bar{3}}_{\text{de } k \text{ fois}} = \bar{3k}$

Alors f est bien défini car $f(\bar{k} + 15\bar{l}) = \bar{3k} + 15\bar{l} = \bar{3k} = f(\bar{k})$.

Il s'agit alors d'un morphisme car $f(\bar{k}_1 + \bar{k}_2) = \bar{3(k}_1 + \bar{k}_2) = \bar{3k}_1 + \bar{3k}_2$

$= f(\bar{k}_1) + f(\bar{k}_2)$. On a $\text{Im } f = \{\bar{3k} \in \mathbb{Z}/15\mathbb{Z} \mid k \in \mathbb{Z}\} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}\}$

et $\text{Ker } f = \{\bar{5k} \in \mathbb{Z}/15\mathbb{Z} \mid \bar{3k} = \bar{0} \text{ dans } \mathbb{Z}/15\mathbb{Z}\} = \{\bar{k} \mid 15 \mid 3k\} =$
 $= \{\bar{k} \mid 5 \mid k\} = \{\bar{0}, \bar{5}\}$. Par conséquent f n'est ni injectif,

ni surjectif.

Réponse Il faut faire attention dans le cadre d'un groupe additif (la loi est abélienne et notée +) de noter aussi les inverses comme des opposés, donc x^{-1} devient $-x$. De toute manière dans $\mathbb{Z}/n\mathbb{Z}$ qui admet aussi une multiplication en tant qu'anneau, \bar{k} a une signification et \bar{k}^{-1} une autre (cette dernière possibilité n'apparaît que pour $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$, donc pour $k \mid n = 1$).

(ex3) Soit $x \in G$ et $\text{ord}(x) = m$. Alors $x^m = 1$ et $f(x^m) = f(x)^m = f(1) = 1$ (avec des notations multiplicatives pour les lois de G et H)
 Puisque $f(x)^m = 1$ on sait que $\text{ord}(f(x)) \mid m = \text{ord}(x)$, ce qui répond à la première question et renvoie aussi l'exercice 1 de la manière suivante : Si $f : \mathbb{Z}_{22} \rightarrow \mathbb{Z}_{32}$ est non trivial alors $\text{ord}(\bar{x}) = 2$ et $\text{ord}(f(\bar{x})) \mid 2$. Comme $\text{ord}(f(\bar{x})) \neq 1$, car on ne veut pas f trivial, c'est que $\text{ord}(f(\bar{x})) = 2$. On a l'ordre dont cherchons l'ordre du groupe \mathbb{Z}_{32} , c'est 3. Cela est impossible donc il n'y a pas de morphisme non trivial de \mathbb{Z}_{22} dans \mathbb{Z}_{32} .

Revenons à l'exercice 3 : si $|H| = n$ et $m \wedge n = 1$, on a que $\text{ord}(f(x))$ divise m et n (car $f(x) \in H$), c'est que $\text{ord}(f(x)) = 1$. Cela équivaut à $f(x) = 1$ donc à $x \in \ker f$.

(ex4) On a $|\mathbb{Z}_{30}^{\times}| = \varphi(30) = \varphi(2 \times 3 \times 5) = \varphi(2) \varphi(3) \varphi(5) = 1 \times 2 \times 4 = 8$ ce qui se voit aussi en enumérant les éléments de $\mathbb{Z}_{30}^{\times} = \{\bar{1}, \bar{7}, \bar{11}, \bar{13}, \bar{17} = -\bar{13}, \bar{19} = -\bar{11}, \bar{23} = -\bar{7}, \bar{29} = -\bar{1}\}$

On a $\bar{11}^2 = \bar{121} = \bar{1}$ donc $\text{ord}(\bar{11}) = 2$.

On peut calculer tous les ordres des éléments de $(\mathbb{Z}_{30}^{\times})^*$.

$\mathbb{Z}_{30}^{\times}^*$	$\bar{1}$	$\bar{7}$	$\bar{11}$	$\bar{13}$	$-\bar{13}$	$-\bar{11}$	$-\bar{7}$	$-\bar{1}$
ordre	1	4	2	4	4	2	4	2

on a que $\bar{7}^2 = -\bar{11}$ donc $\bar{7}^4 = \bar{1}$
 $(-\bar{7})^2 = -\bar{11}$ donc $(-\bar{7})^4 = \bar{1}$
 $\bar{13}^2 = -\bar{11}$ donc $\bar{13}^4 = \bar{1}$
 $(-\bar{13})^2 = -\bar{11}$ donc $(-\bar{13})^4 = \bar{1}$

On remarque que ce groupe n'est pas cyclique, car il n'y a pas d'élément d'ordre 8. Il s'agit plutôt d'un isomorphisme $\mathbb{Z}_{30}^{\times} \cong \mathbb{Z}_{22}^{\times} \times \mathbb{Z}_{32}^{\times} \times \mathbb{Z}_{52}^{\times} \cong (\mathbb{Z}_{22} \times \mathbb{Z}_{42}, +)$.

(x5)

En décomposant τ en cycles à supports disjoints on

obtient $\tau = (1562)(34)$. Alors $\tau^{-1} = (34)^{-1}(1562)^{-1} = (34)(1265)$

et $\tau^2 = (1562)^2(34)^2$ (car les cycles à supports disjoints commutent)

Donc $\tau^2 = (16)(25)$. L'écriture de τ n'est pas en cycles à

supports disjoints, donc on peut écrire $\tau = (1253)$

(cycle de longueur 4) et $\tau^2 = (15)(23)$.

Pour un cycle de longueur s , comme $c = (a_1 a_2 \dots a_s)$,

on a une écriture $c = (a_1 a_2)(a_2 a_3) \dots (a_{s-1} a_s)$ en produit de $s-1$ transpositions donc $\varepsilon(c) = (-1)^{s-1}$.

Par conséquent $\varepsilon(\tau^{-1}) = \varepsilon((34))\varepsilon((1265)) = (-1)^1(-1)^4 = (-1)^5 = 1$

et τ^{-2} est une permutation paire. De même $\varepsilon(\tau^2) = \varepsilon((16)(25)) = (-1)^2 = 1$ et ce sera toujours le cas pour $\varepsilon(\alpha^2) = \varepsilon(\alpha)^2 = 1$ pour n'importe quelle permutation α . Et aussi $\varepsilon(\tau^2) = \varepsilon(c)^2 = 1$ (ce qui colle avec $\varepsilon(\tau^2) = \varepsilon((15)(23)) = (-1)^2 = 1$).

Pour calculer $\tau^{-1}\tau\tau$ on peut appliquer le "principe de conjugaison".

Ce principe permet de calculer rapidement des expressions du type $\alpha c \alpha^{-1}$ pour $\alpha \in S_n$ et c un cycle. En effet, si $c = (a_1 \dots a_s)$ est un cycle de longueur s , on a $\alpha c \alpha^{-1} = (\alpha(a_1) \dots \alpha(a_s))$ c-à-d un cycle de longueur s comme c , mais où les éléments caractéristiques (a_i) sont remplacés par $\alpha(a_i)$. Cela se vérifie par calcul :

$$\alpha c \alpha^{-1}(\alpha(a_i)) = \alpha c(a_i) = \alpha(a_{i+1}) \text{ pour } i \text{ allant de } 1 \text{ à } s-1$$

(donc $\alpha c \alpha^{-1}$ agit de manière cyclique sur $\alpha(a_1), \dots, \alpha(a_{s-1})$) et $\alpha c \alpha^{-1}(\alpha(a_s)) = \alpha c(a_s) = \alpha(a_1)$ (et $\alpha(a_s)$ est envoyé sur $\alpha(a_1)$) et aussi $\alpha c \alpha^{-1}(b) = \alpha c^{-1}(b) = b$ pour $b \notin \alpha(a_i)$ (car alors $\alpha^{-1}(b) \notin a_i$).

Donc $\alpha c \alpha^{-1}$ agit comme le cycle $(\alpha(a_1) \dots \alpha(a_s))$ donc il l'est également.

Pour nous $\alpha = \tau^{-1}$, $c = \tau = (1253)$ donc $\tau^{-1}\tau\tau = (\tau^{-1}(1)\tau^{-1}(2)\tau^{-1}(5)\tau^{-1}(3)) = (2614)$
 $= (1426)$ ce qui se vérifie aussi par calcul direct.

(x6) On a comme ci-dessus $c = (12 \dots n) = (12)(23) \dots (m \dots n)$ donc $\varepsilon(12 \dots n) = (-1)^{n-1}$

Donc c est une permutation paire si n est impair.

(Ex7)

On a $\text{support}(S) = \{1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 16\}$ car

les éléments de 1 à 16 qui ne sont pas laissés fixes par S .

Les orbites sont $\{1, 13, 10, 9\}$, $\{2, 11, 7, 3, 16\}$, $\{4, 12, 5\}$, $\{6, 14\}$, $\{8\}$ et $\{15\}$ (il ne faut pas oublier les orbites à un seul élément).

La décomposition en cycles à supports disjoints est

$$S = (1 \ 13 \ 10 \ 9)(2 \ 11 \ 7 \ 3 \ 16)(4 \ 12 \ 5)(6 \ 14).$$

On sait que $\text{ord}(S) = \text{lcm}(\text{ord}(c_i))$ lorsque $S = c_1 \cdots c_n$ et la décomposition de S en cycles disjoints. Ceci puisque

$S^{\text{lcm}(\text{ord}(c_i))} = c_1^{\text{lcm}(\text{ord}(c_i))} \cdots c_n^{\text{lcm}(\text{ord}(c_i))} = 1$ vu que les c_i commutent. Et si $\ell = 1$ alors $c_1^\ell \cdots c_n^\ell = 1$ les cycles c_i^ℓ étant encore à supports disjoints. D'après l'unicité de la décomposition en cycles disjoints on aura alors $c_1^\ell = c_2^\ell = \cdots = c_n^\ell = 1$ donc $\text{ord}(c_i) | \ell$, $\forall i \in \{1, \dots, n\}$. Donc $\text{lcm}(\text{ord}(c_i)) | \ell$ et $\text{ord}(S)$ est bien $\text{lcm}(\text{ord}(c_i))$. On rappelle que $\text{ord}(c) = \text{long}(c)$ pour c un cycle.

$$\text{Ici } \text{ord}(S) = \text{lcm}(4, 5, 3, 2) = 60. \text{ Et } \epsilon(S) = (-1)^3(-1)^4(-1)^2(-1) = 1.$$

Donc $S \in A_{16}$ en tant que permutation paire.

(Ex8)

On a $\tau = (143)(265)$ et $\tau = (13)(46)$ donc $\tau = \tau^{-1}$.

On a $\tau^n = \tau^n \mod 6 \mid n$ car $\tau^n = \begin{cases} 1 & n \equiv 3 \pmod{6} \\ \tau & n \equiv 1 \pmod{3} \\ \tau^2 & n \equiv 2 \pmod{3} \end{cases}$ vu que $\text{ord}(\tau) = 3$

$$\text{et } \tau^n = \left\{ \begin{array}{ll} 1 & n \equiv 2 \pmod{6} \\ \tau & n \equiv 1 \pmod{2} \end{array} \right. \text{ et } \tau \neq \tau + \tau^2 \neq \tau.$$

(Ex9)

q1) On a $\pi = (1 \ 11 \ 3 \ 4)(5 \ 6)(7 \ 8 \ 9)$

$$\tau = (1 \ 3 \ 4 \ 11)(2 \ 6 \ 7 \ 8 \ 10)(5 \ 9) \text{ et}$$

$$\pi \tau = (1 \ 11 \ 3 \ 4)(5 \ 6)(7 \ 8 \ 9)(1 \ 3 \ 4 \ 11)(2 \ 6 \ 7 \ 8 \ 10)(5 \ 9) = (143)(25796810)$$

Composez dans le bon sens, en appliquant la permutation de droite vers le gauche)

q2) On a $\text{ord}(\pi) = \text{lcm}(4, 2, 3) = 12$, $\text{ord}(\tau) = \text{lcm}(4, 5, 2) = 20$, $\text{ord}(\pi \tau) = \text{lcm}(3, 2) = 21$.

q3) On a $|S_{11}| = 11!$

q4) On n'a pas $13 | 11!$ donc aucun élément de S_{11} n'est d'ordre 13. On cherche c_1, \dots, c_r tq $\ell(c_1) + \ell(c_2) + \dots + \ell(c_r) \leq 11$ et $\text{lcm}(\ell(c_1), \dots, \ell(c_r)) = 30 = 2 \times 3 \times 5$ (où $\ell(c)$ désigne la longueur du cycle c) et donc n ordre. Dans ce cas les seules possibilités sont $n=3$ et $\ell(c_1)=2$, $\ell(c_2)=3$, $\ell(c_3)=5$ ou bien $n=2$, $\ell(c_1)=6$, $\ell(c_2)=5$, donc on a bien des éléments d'ordre 30 dans S_{11} , par exemple

$$\tau_1 = (12)(3 \ 4 \ 5)(6 \ 7 \ 8 \ 9 \ 10) \text{ ou } \tau_2 = (123 \ 4 \ 5 \ 6)(7 \ 8 \ 9 \ 10 \ 11).$$

ex 10

q1) En effet $\sigma = \underbrace{(\tau_2)}_{\tau_2} \underbrace{(\tau_3)}_{\tau_3} \underbrace{(3 \ 11 \ 7 \ 9 \ 4)}_{\tau_5}$ et $\text{ord}(\sigma) = \text{lcm}(2, 3, 5) = 30$, $\varepsilon(\sigma) = -1$

Cet exemple peut servir à l'exercice 9, comme élément d'ordre 30 dans S_{11} .

q2) On a $H = \langle \tau_2, \tau_3, \tau_5 \rangle$ et les τ_i commutent car ils sont à supports disjoints.

Donc $H = \{ \tau_2^n \tau_3^m \tau_5^t \mid n, m, t \in \mathbb{Z} \}$ car que H contient tous les produits possibles des τ_i et de leurs puissances et H est commutatif.

q3) On a $\varphi((n_1, s_1, t_1) + (n_2, s_2, t_2)) = \varphi((n_1+n_2, s_1+s_2, t_1+t_2)) =$
 $= \tau_2^{n_1+n_2} \tau_3^{s_1+s_2} \tau_5^{t_1+t_2} = \tau_2^{n_1} \tau_3^{s_1} \tau_5^{t_1} \tau_2^{n_2} \tau_3^{s_2} \tau_5^{t_2} =$
 $= \varphi((n_1, s_1, t_1)) \varphi((n_2, s_2, t_2))$ donc φ est un morphisme.

On a φ surjectif d'après q2).

On a $\ker \varphi = \{ (n, s, t) \mid \tau_2^n \tau_3^s \tau_5^t = 1 \} = \{ (n, s, t) \mid \tau_2^n = \tau_3^s = \tau_5^t = 1 \}$
 $= \{ (n, s, t) \mid 2|n, 3|s, 5|t \} = \{ (2k) \times (3l) \times (5m) \}$.

On a $\tau_2^n \tau_3^s \tau_5^t = \tau_2^{n'} \tau_3^{s'} \tau_5^{t'} \quad \text{mi } n \in \mathbb{N}[2], s \in \mathbb{N}[3], t \in \mathbb{N}[5]$
 donc on a 2 choix pour τ_2^n , 3 choix pour τ_3^s , 5 choix pour τ_5^t
 d'où $|H| = 30$. Et $\text{ord}(\sigma) = 30$ donc $H = \langle \sigma \rangle$.

Il y a donc $\varphi(30) = \varphi(2) \varphi(3) \varphi(5) = 1 \times 2 \times 4 = 8$ générateurs distincts dans H comme dans tout groupe cyclique de cardinal 30 (en particulier \mathbb{Z}_{30} pour lequel on sait que $\langle \bar{k} \rangle = \mathbb{Z}_{30}$ mi $\bar{k} \in \mathbb{Z}_{30}^\times$ et $|\mathbb{Z}_{30}^\times| \subset \varphi(30)$).