Colles MP*

Jad ABOU YASSIN

15 Septembre 2022
Structures algébriques

Table des matières

Questions de cours et applications **2**
Exercice 1 - Étude de $\mathbb{Z}/6\mathbb{Z}$ 2
Exercice 2 - Morphismes 3
Exercice 3 - Étude d'une permutation de $\mathcal{S}_{12}$ 4

Exercices **5**
Exercice 4 - (*) Élévation à la puissance n dans un groupe fini 5
Exercice 5 - (*) Groupe multiplicatif d'un corps fini 5
Exercice 6 - (**) Sous-groupes d'un groupe infini 6
Exercice 7 - (**) Un sous-groupe maximal de $\mathfrak{S}_n$ 6
Exercice 8 - (**) Élément d'ordre 2 dans un groupe de cardinal pair 7
Exercice 9 - (**) Un sous-groupe de $GL_3(\mathbb{R})$ engendré par deux éléments . . 8
Exercice 10 - (***) Exposant d'un groupe 9

Questions de cours et applications

Exercice 1 - Étude de $\mathbb{Z}/6\mathbb{Z}$ Soit $G = \mathbb{Z}/6\mathbb{Z}$.

1. Quel est le cardinal de G ? Quels sont ses éléments ?
2. $(G, +)$ est-il un groupe ? $(G, \times)$ est-il un groupe ?
3. Quels sont les ordres des éléments de G ?
4. G est-il cyclique ?
5. $(G, +, \times)$ est-il un anneau ?
6. Qui sont les inversibles de l'anneau G, ensemble noté $G^\times$?
7. $(G^\times, \times)$ est-il un groupe ?
8. $(G^\times, \times)$ est-il cyclique ?
9. Quel est l'inverse de $\bar{5}$ dans $G^\times$?
10. $(G^\times, \times)$ est-il isomorphe à un groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ pour un certain n ?

Solution :

1. $G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ est de cardinal 6.
2. $(G, +)$ est un groupe via la loi $\bar{k} + \bar{l} = \overline{k+l}$. Le neutre est $\bar{0}$ et l'inverse de $\bar{k}$ est $\overline{-k} = \overline{6-k}$. $(G, \times)$ n'est pas un groupe car $\bar{0}$ n'a pas d'inverse (c'est un élément absorbant).
3. $\bar{0}$ est d'ordre 1 (élément neutre), $\bar{1}$ est d'ordre 6, $\bar{2}$ est d'ordre 3, $\bar{3}$ est d'ordre 2, $\bar{4}$ est d'ordre 3 et $\bar{5}$ est d'ordre 6.
4. Oui, G est de cardinal 6 et admet un élément d'ordre 6. Donc G est engendré par $\bar{1}$ (ou $\bar{5} = -\bar{1}$)
5. Oui. $(G, +)$ est un groupe abélien et la multiplication est bien associative et distributive sur l'addition.
6. Les inversibles de G sont $\bar{1}$ et $\bar{5}$. (Soit on calcule les puissances successives de chaque élément, soit on utilise un résultat du cours sur la nature des inversibles de $\mathbb{Z}/n\mathbb{Z}$, qui sont les $\bar{k}$ où k est premier avec n.)
7. Oui. De manière générale, l'ensemble des inversibles d'un anneau est un groupe.
8. Oui. Dans ce cas précis, il s'agit d'un groupe à deux éléments, donc est cyclique. Mais de manière générale, le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Attention : ce n'est pas vrai pour un anneau quelconque !
9. $\bar{5}$ est son propre inverse dans $G^\times$
10. Oui, $G^\times$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ car c'est un groupe cyclique d'ordre 2.

Exercice 2 - Morphismes

1. Soit $\varphi : A \to B$ un morphisme de groupes. L'image de φ est-elle un sous-groupe de B ? Et son noyau est-il un sous-groupe de A ?
2. Soit $\varphi : A \to B$ un morphisme de groupes. Si φ est bijective, est-ce que φ^{-1} est un morphisme de groupes de B vers A ?
3. Combien de morphismes de groupes y a-t-il entre $\mathbb{Z}$ et $\mathbb{Z}$? Combien de morphismes d'anneaux y a-t-il entre $\mathbb{Z}$ et $\mathbb{Z}$?
4. Si $\varphi : A \to B$ est un morphisme de groupes injectif, est-ce que $\varphi : A \to \varphi(A) \subset B$ est un isomorphisme de groupes ?
5. Si $\varphi : A \to B$ est un morphisme de groupes surjectif, est-ce que $\varphi : \ker(\varphi) \to B$ est un isomorphisme de groupes ?

Solution :

1. Oui et oui, c'est du cours.

   Remarque : C'est hors programme pour l'instant, mais on a mieux que ça comme résultat. Tout sous-groupe de B est l'image d'un certain morphisme de groupes (l'injection $H \hookrightarrow B$), mais il existe des sous-groupes de A qui ne sont pas des noyaux de morphismes.
2. Oui. C'est du cours encore une fois, mais c'est une propriété importante qu'on a tendance à prendre pour évident. Il n'y a *a priori* aucune raison pour que l'inverse (en tant qu'application entre deux ensembles) d'un morphisme de groupes bijectif soit lui aussi un morphisme de groupes. Un résultat du cours nous assure que si (et il faut savoir le redémontrer !)
3. Un morphisme de groupes partant de $\mathbb{Z}$ est uniquement déterminé par l'image de 1. Ainsi, l'ensemble des morphismes de groupes de $\mathbb{Z}$ dans lui-même (qu'on appelle les endomorphismes de $\mathbb{Z}$) est en bijection avec $\mathbb{Z}$. Un morphisme d'anneau envoie, par définition, 0 sur 0 et 1 sur 1. Comme il s'agit également d'un morphisme de groupes, par ce qui précède, ceci détermine entièrement ce morphisme : il s'agit de l'identité. Il n'y a donc qu'un seul morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{Z}$.
4. Oui. C'est une bijection ensembliste (restreindre une application injective à son image la rend bijective), qui est un morphisme de groupes car $\varphi(A)$ est un sous-groupe de B. Donc c'est une bijection.
5. Non. Ça ne marche pas dans ce sens, simplement parce que $\ker(\varphi)$ est par définition l'ensemble des éléments qui s'envoient sur le neutre de B ! En restreignant φ à son noyau, on l'a transformée en l'application constante égale au neutre.

Exercice 3 - Étude d'une permutation de $\mathcal{S}_{12}$

1. Rappeler le cardinal de $\mathfrak{S}_{12}$, s'il s'agit d'un groupe (pour quelle loi ?) et s'il est abélien.

   On pose :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 5 & 1 & 3 & 8 & 6 & 2 & 12 & 9 & 11 & 10 & 7 \end{pmatrix}$$

2. Que vaut $\sigma(4)$? $\sigma^{-1}(12)$? $\sigma^2(10)$?
3. Quel est le support de σ ?
4. Décomposer σ en produit de cycles à support disjoints.
5. Quel est l'ordre d'un k-cycle de $\mathfrak{S}_{12}$? Quel est l'ordre de σ ? Quel est son type cyclique ?
6. Quelle est la signature d'un k-cycle ? Quel est la signature de σ ?
7. Retrouver la signature de σ en écrivant σ comme un produit de transpositions. Pourquoi est-ce qu'on peut le faire ?
8. Calculer $\tau\sigma\tau^{-1}$ où $\tau = (4 \quad 2 \quad 10)(5 \quad 7)$ (vous pouvez écrire le résultat sous la forme que vous voulez, en produit de cycles à support disjoints, en produit de transposition, ...)

Solution :

1. $\mathfrak{S}_{12}$ est de cardinal 12! (pour info, ça fait 479001600). Il s'agit d'un groupe qui n'est pas abélien (par exemple, $(1 \quad 2)(2 \quad 3) = (1 \quad 3)$ mais $(2 \quad 3)(1 \quad 2) = (1 \quad 3 \quad 2)$)
2. $\sigma(4) = 3$. $\sigma^{-1}(12) = 8$. $\sigma^2(10) = 10$
3. Les seuls points fixes de σ sont 6 et 9, donc le support de σ est l'ensemble $[\![1, 12]\!] \setminus \{6, 9\}$
4. $\sigma = (1 \quad 4 \quad 3)(2 \quad 5 \quad 8 \quad 12 \quad 7)(10 \quad 11)$
5. L'ordre d'un k-cycle est k. σ étant écrit comme produit de cycles à supports disjoints, l'ordre de σ est le ppcm des ordres de chaque cycle : donc σ est d'ordre $2 \times 3 \times 5 = 30$. Le type cyclique de σ est alors $(2, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0)$

   Remarque : Pour ce genre de questions, il ne faut pas essayer de calculer les puissances de σ jusqu'à retomber sur l'identité !!
6. Un k-cycle est de signature $(-1)^{k+1}$. La signature étant un morphisme de groupes $\mathfrak{S}_{12} \to (\{-1, 1\}, \times)$, la signature de σ est $1 \times (-1) \times 1 = -1$.
7. On peut le faire car $\mathfrak{S}_{12}$ est engendré par les transpositions. On a :

$$\sigma = (1 \quad 4)(4 \quad 3)(2 \quad 5)(5 \quad 8)(8 \quad 12)(12 \quad 7)(10 \quad 11)$$

   qui est un produit de 7 transpositions, donc σ est bien de signature -1 car 7 est impair.

8. Conjuguer un cycle $(i_1 \quad i_2 \dots i_k)$ par une permutation τ donne le cycle $(\tau(i_1) \quad \tau(i_2) \dots \tau(i_k))$. Ainsi :

$$\tau\sigma\tau^{-1} = (1 \quad 2 \quad 3)(10 \quad 7 \quad 8 \quad 12 \quad 5)(4 \quad 11)$$

Exercices

Exercice 4 - (*) Élévation à la puissance n dans un groupe fini Soit G un groupe fini, et n un entier naturel premier à $|G|$. Montrer que l'application

$$\begin{array}{rccc} \varphi : & G & \to & G \\ & x & \mapsto & x^n \end{array}$$

est une bijection de G sur lui-même.
Indication : *On pourra utiliser une relation de* Bézout

Solution : Comme G est fini, il suffit de montrer la surjectivité de cette application pour conclure. Soit $y \in G$. Comme n et $|G|$ sont premiers entre eux, par le théorème de Bézout, il existe des entiers $k, l \in \mathbb{Z}$ tels que $kn + l|G| = 1$. Ainsi, $y = y^1 = y^{kn+l|G|} = (y^k)^n (y^{|G|})^l = (y^k)^n = \varphi(y^k)$. Ainsi, y est dans l'image de φ, qui est donc surjective. Donc $\boxed{\varphi \text{ est une bijection de } G}$.

Exercice 5 - (*) Groupe multiplicatif d'un corps fini Soit $\mathbb{K}$ un corps fini de cardinal q. On note e l'exposant du groupe $\mathbb{K}^*$, c'est-à-dire $e = \text{ppcm}(\{\text{ord}(x) \ ; \ x \in \mathbb{K}^*\})$.

1. En utilisant le fait que le nombre de racines d'un polynôme de $\mathbb{K}[X]$ est inférieur à son degré, montrer que $q - 1 \leq e$
2. En admettant qu'il existe un élément $x \in \mathbb{K}^*$ dont l'ordre est l'exposant du groupe (c'est un résultat vrai pour tout groupe abélien fini), montrer que $\mathbb{K}^*$ est un groupe cyclique.

Solution :

1. Par définition de e, on a pour tout $x \in \mathbb{K}^*$, $x^e = 1$. Ainsi, le polynôme $X^e - 1 \in \mathbb{K}[X]$ possède tous les éléments de $\mathbb{K}^*$ comme racine, qui est de cardinal $q - 1$, donc $\boxed{q - 1 \leq e}$.
2. Si $x \in \mathbb{K}^*$, alors $x^{q-1} = 1$ (car $|\mathbb{K}^*| = q - 1$), donc l'ordre de x divise $q - 1$. Ceci étant vrai pour tout $x \in \mathbb{K}^*$, le ppcm de leurs ordres divise encore $q - 1$, donc $e | q - 1$. Par la question précédente, $e = q - 1$. Ainsi, en admettant l'existence d'un élément d'ordre e, cet élément engendre $\mathbb{K}^*$, $\boxed{\text{qui est donc cyclique}}$.

Exercice 6 - (**) Sous-groupes d'un groupe infini Soit G un groupe infini.

1. On suppose qu'il existe dans G un élément d'ordre infini, montrer que G a une infinité de sous-groupes. Pouvez-vous donner un exemple d'un tel groupe ?
2. On suppose que tous les éléments de G sont d'ordre fini. En utilisant le fait que pour tout $g \in G$, $g \in \langle g \rangle$, montrer que G a une infinité de sous-groupes. Pouvez-vous donner un exemple d'un tel groupe ?

   Indication : (Orale) Essayer d'expliquer dans un premier temps pourquoi la réunion de tous les sous-groupes cycliques de G est égale à G, puis essayer de voir ce qui se passe si tous les sous-groupes cycliques de G sont finis.

Remarque : On a démontré le résultat suivant : si G est un groupe infini, alors G possède une infinité de sous-groupes.

Solution :

1. Soit $g \in G$ un élément d'ordre infini. Si $n \in \mathbb{N}$, on considère le sous-groupe $G_n = \langle g^n \rangle$. Ce sont des sous-groupes de G deux à deux distincts. En effet, si $n > m$, alors $g^m \notin G_n$ mais $g^m \in G_m$. En effet, si $g^m \in G_n$, alors il existe $k \in \mathbb{Z}$ tel que $g^m = g^{nk}$, c'est-à-dire que $m = nk$ (car G_n est monogène infini), donc que n divise m. Ceci n'est pas possible car $n > m$. Donc $\boxed{G \text{ a une infinité de sous-groupes}}$.
2. Soit $\mathcal{SGC}$ l'ensemble des sous-groupes cycliques de G. Comme

$$G = \bigcup_{g \in G} \{g\} \subset \bigcup_{g \in G} \langle g \rangle \subset \bigcup_{H \in \mathcal{SGC}} H \subset G$$

   toutes ces inclusions sont des égalités. En particulier, G est réunion de tous ses sous-groupes cycliques, qui sont tous finis par hypothèse. Nécessairement, $\mathcal{SGC}$ est de cardinal infini, car une réunion finie d'ensembles finis est finie. $\boxed{\text{Donc } G \text{ possède une infinité de sous-groupes}}$.

Exercice 7 - (**) Un sous-groupe maximal de $\mathfrak{S}_n$ Soit $G = \{\sigma \in \mathfrak{S}_n \ ; \ \sigma(n) = n\}$

1. Montrer que G est un sous-groupe de $\mathfrak{S}_n$
2. Montrer que $\{(1 \quad 2), \ldots, (1 \quad n)\}$ est une partie génératrice de $\mathfrak{S}_n$.

3. Montrer que G est maximal pour l'inclusion, c'est-à-dire que pour tout sous-groupe H de $\mathfrak{S}_n$ qui contient G, on a $H = G$ ou $H = \mathfrak{S}_n$
   Indication : *Remarquer que* $(1 \quad 2), \dots, (1 \quad n{-}1)$ *sont dans* G*, donc dans* H*, puis essayer de montrer que si* $G \subsetneq H$*, alors* $(1 \quad n)$ *est dans* H

   Solution :

   (a) L'inclusion $\mathfrak{S}_{n-1} \to \mathfrak{S}_n$ est un morphisme de groupes, dont l'image est G, qui est donc un $\boxed{\text{sous-groupe de } \mathfrak{S}_n}$. (Sinon, on peut aussi le faire à la main)

   (b) C'est fait en $\boxed{\text{TD, exercice 1.25.a)}}$. Il s'agit d'une récurrence sur n dont en voici une idée pour l'hérédité : Soit $\sigma = (n{+}1 \quad i_2 \quad \dots \quad i_k)\sigma' \in \mathfrak{S}_{n+1}$ avec $n{+}1$ qui n'est pas dans le support de σ'. On réécrit $\sigma = (n{+}1 \quad i_2)(i_2 \quad \dots \quad i_k)\sigma' = (n{+}1 \quad i_2)\sigma''$. Par hypothèse de récurrence, σ'' s'écrit comme un produit de transposition de la forme $(1 \quad i)$ où $1 \leq i \leq n$, et $(n{+}1 \quad i_2) = (1 \quad i_2)(1 \quad n{+}1)(1 \quad i_2)$. Ceci conclut l'hérédité.

   (c) Soit H un sous-groupe de $\mathfrak{S}_n$ qui contient G et différent de G. Montrons que $H = \mathfrak{S}_n$. Il existe dans H un élément ne fixant pas n (car $H \setminus G \neq \emptyset$) qu'on note $\sigma = (n \quad m \quad i_3 \quad \dots \quad i_k)\sigma'$ où n n'est pas dans le support de σ' et $m \in [\![1, n{-}1]\!]$ (notation obtenue en considérant la décomposition de σ en cycles à supports disjoints). On peut réécrire $\sigma = (n \quad m)(m \quad i_3 \quad \dots \quad i_k)\sigma' = (n \quad m)\sigma''$ où n est fixé par σ'', donc $\sigma'' \in G \subset H$, donc $(n \quad m) \in H$. En conjuguant par la transposition $(1 \quad m) \in G \subset H$, on obtient que la transposition $(1 \quad n) \in H$, donc H contient un système générateur de $\mathfrak{S}_n$ par la question précédente, donc $\boxed{H = \mathfrak{S}_n}$.

Exercice 8 - (**) Élément d'ordre 2 dans un groupe de cardinal pair Soit G un groupe de cardinal pair. Montrer qu'il existe dans G un élément d'ordre 2.
Indication : *(Orale) Essayez de regrouper les éléments* x *et* x^{-1} *et comptez !*

Solution : On construit un ensemble A de la manière suivante : initialement, $A = \{e\}$. On choisi un élément x_1 de G quelconque différent de e, puis on ajoute x_1 et x_1^{-1} à A. Ensuite, on choisi un élément quelconque x_2 de $G \setminus A$ et on ajoute x_2 et x_2^{-1} à A. On continue ainsi jusqu'à ce que l'ensemble $G \setminus A$ soit vide, ce qui se fait en un nombre fini d'étapes car G est fini. On a alors $G = A$. Comme A est de cardinal pair (car G l'est) et qu'il était de cardinal 1 (impair) initialement, il y a eu un moment où le cardinal de A n'a été augmenté que de 1. C'est-à-dire qu'il existe i un numéro d'étape tel que l'ajout de x_i et x_i^{-1} à A n'a fait augmenter le cardinal de A que de 1. Or, ni x_i ni x_i^{-1} n'étaient pas déjà présents dans A par construction. Donc cela signifie que $x_i = x_i^{-1}$, et que

donc $\boxed{x_i \text{ est d'ordre } 2}$.

Exercice 9 - (**) Un sous-groupe de $GL_3(\mathbb{R})$ engendré par deux éléments Soient A et B deux matrices de $\mathcal{M}_3(\mathbb{R})$ définies par :

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

1. Montrer que A et B sont dans $GL_3(\mathbb{R})$
2. Calculer A^2, B^2, B^3, AB, BA et AB^2.
   Remarque : Ce n'est pas aussi long que ce qu'on pense
3. Décrire le sous-groupe G de $GL_3(\mathbb{R})$ engendré par A et B.
4. G est-il isomorphe à un groupe symétrique ? Si oui, donner un isomorphisme. Si non, justifier pourquoi il n'existe pas d'isomorphisme entre G et un groupe symétrique.
   Indication : $\mathfrak{S}_n$ *admet-il un système de générateurs à deux éléments ? Est-ce que cela suffit pour avoir un isomorphisme ?*

Solution :

1. On calcule les déterminants de A et B, par exemple en développant par rapport à la première ligne. On obtient $\det(A) = -1$ et $\det(B) = 1$. Les deux sont non nuls, donc A et B sont inversibles.
2. $$B^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}; \quad \begin{cases} B^3 = I_3 \\ A^2 = I_3 \end{cases}; \quad AB = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}; \quad BA = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = AB^2$$
3. On remarque que AB et BA s'écrivent sous la forme $A^k B^l$ pour $k, l \in \mathbb{N}$. Ainsi, tout élément du sous-groupe de $GL_3(\mathbb{R})$ engendré par A et B s'écrit sous la forme $A^n B^m$ pour $n, m \in \mathbb{N}$. Or, $A^2 = I_3$ et $B^3 = I_3$, donc on a :
   $$G = \{I_3, A, B, B^2, AB, AB^2\}$$
4. Soit $\varphi : G \to \mathfrak{S}_n$ un isomorphisme de groupes. Tout d'abord, G est de cardinal 6 et le seul groupe symétrique de cardinal 6 est $\mathfrak{S}_3$. S'il y a un isomorphisme entre G et un groupe symétrique, c'est donc nécessairement $\mathfrak{S}_3$, donc $n = 3$. Un isomorphisme préserve les ordres :

si G_1, G_2 sont deux groupes isomorphes par $\varphi : G_1 \to G_2$ et $x \in G_1$, alors l'ordre de x est égal à l'ordre de $\varphi(x)$. Or, A est d'ordre 2 dans G et B est d'ordre 3 dans G. Un système de générateurs de $\mathfrak{S}_3$ est donné par $\tau = (1 \quad 2)$ et $\sigma = (1 \quad 2 \quad 3)$, et τ est d'ordre 2 et σ d'ordre 3 dans $\mathfrak{S}_3$. En procédant de même que dans les questions précédentes (ou bien en utilisant un résultat vu en TD), on obtient que $\mathfrak{S}_3 = \{id, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\}$. Posons : $\varphi(A) = \tau$ et $\varphi(B) = \sigma$, ce qui précède montre qu'il s'agit d'un isomorphisme de groupes.

Remarque : Ce n'est pas l'isomorphisme « naturel »entre $\mathfrak{S}_3$ et G, dû à notre choix de τ. De manière plus générale, il existe toujours un isomorphisme φ de $\mathfrak{S}_n$ vers un sous-groupe de $GL_n(\mathbb{R})$, appelé sous-groupe des matrices de permutation, donné par $\varphi(\sigma) = [e_{\sigma(1)}|\dots|e_{\sigma(n)}]$ où $(e_1, \dots, e_n)$ sont les vecteurs colonnes de la base canonique de $\mathbb{R}^n$. Dans notre cas, A représente la transposition $\tau' = (2 \quad 3)$

Exercice 10 - (***) Exposant d'un groupe Soit G un groupe fini. On définit l'exposant de G comme étant l'entier $e = \text{ppcm}\,(\{\text{ord}(g)\ ;\ g \in G\})$.

1. On suppose que G est abélien.
   (a) Montrer que pour tous $x, y \in G$, si $\text{ord}(x) \wedge \text{ord}(y) = 1$, alors $\text{ord}(xy) = \text{ord}(x)\text{ord}(y)$.
   (b) Soit $g \in G$ d'ordre maximal noté n. Après avoir justifié l'existence d'un tel élément, montrer que pour tout $h \in G$ d'ordre noté m, pour tout nombre premier p, la p-valuation de n est supérieure à celle de m (c'est-à-dire que n est divisible par p plus de fois que m l'est).
   Indication : Factoriser n et m par p autant que possible et essayer d'appliquer la question précédente à des puissances de g et h bien choisies.
   (c) Montrer qu'il existe dans G un élément dont l'ordre est e.
   Indication : (Orale) Que signifie la question précédente en terme de divisibilité des ordres de h et g ? Qu'est-ce qu'un ppcm ?
2. Le résultat est-il vrai si G n'est pas abélien ?
   Indication : (Orale) Essayer d'abord sur des petits exemples avant de vous lancer dans des choses compliquées ! Quels petits groupes non abéliens connaissez-vous ?
3. Le résultat est-il vrai si G est abélien infini en supposant que $\{\text{ord}(g)\ ;\ g \in G\}$ soit borné ? Avez-vous un exemple d'un tel groupe ?
   Indication : (Orale) Qu'est-ce qui ne marche pas dans la preuve de la question 1 dans le cas infini ? Notre hypothèse supplémentaire peut-elle nous aider ?
   Remarque : Si le candidat n'a pas d'exemple, ce n'est pas grave.
4. Peut-on simplement supposer que G soit abélien infini avec tous ses éléments d'ordre fini ?

Solution

1. (a) Soit n l'ordre de x et m l'ordre de y. Comme G est abélien, on a $(xy)^{nm} = x^{nm}y^{nm} = (x^n)^m(y^m)^n = ee = 1$, donc $k = \text{ord}(xy)|nm$. Supposons par l'absurde que $k \neq nm$. On a alors $(xy)^k = e = x^k y^k$, donc $x^{-k} = y^k$. En particulier, $y^k, x^k \in \langle x\rangle \cap \langle y\rangle$. Or, par le théorème de Lagrange, le sous-groupe $\langle x\rangle \cap \langle y\rangle$ est d'ordre divisant n et m, donc d'ordre 1 car $n \wedge m = 1$. Ainsi, $x^k = y^k = 1$, donc $k|n$ et $k|m$. Ceci est absurde car n et m sont premiers entre eux. Donc $\boxed{k = nm}$.

   (b) Soit $g \in G$ tel que $\text{ord}(g) = \max(\{\text{ord}(x)\ ;\ x \in G\})$ (qui existe car G est fini). Notons n l'ordre de g. Soit h un élément de G d'ordre noté m. Soit p un nombre premier. On écrit $n = p^\alpha r$ et $m = p^\beta s$ où $\alpha, \beta \in \mathbb{N}$ et $p \not| r, s$. Montrons que $\beta \leq \alpha$. L'élément g^{p^α} est d'ordre r et l'élément h^s est d'ordre p^β. Comme $p \not| r$, p^β et r sont premiers entre eux. En appliquant la question précédente à ces éléments, on obtient que l'élément $g^{p^\alpha}h^s$ est d'ordre $p^\beta r$. Par définition de g, $p^\beta r \leq n = p^\alpha r$. Ainsi, $\boxed{\beta \leq \alpha}$.

   (c) En gardant le même g que dans la question précédente, on a que pour tout $h \in G$ et pour tout p premier, la p-valuation de $\text{ord}(h)$ est inférieure à celle de $\text{ord}(g)$, ce qui signifie que l'ordre de h divise l'ordre de g (par le théorème fondamental de l'arithmétique). Ainsi, l'ordre de tout élément de G divise l'ordre de g, donc le ppcm des ordres de tous les éléments de G, qui est e, divise l'ordre de G. La relation de divisibilité inverse est évidente (car g est un élément de G). Donc $\boxed{g \text{ est d'ordre } e}$.

2. $\mathfrak{S}_3$ est un groupe d'ordre 6 qui possède un élément d'ordre 1 (le neutre), trois éléments d'ordre 2 (les transpositions) et 2 éléments d'ordre 3 (les 3-cycles). Ainsi, l'exposant de $\mathfrak{S}_3$ est $2 \times 3 = 6$, mais il n'y a pas d'éléments d'ordre 6 dans $\mathfrak{S}_3$. $\boxed{\text{Le résultat est donc faux si } G \text{ n'est pas abélien}}$.

3. La seule fois où la finitude de G intervient est pour pouvoir considérer le ppcm et le max de l'ensemble des ordres des éléments de G. Si on suppose que cet ensemble est borné (c'est-à-dire fini, car borné dans $\mathbb{N}$), alors la preuve fonctionne toujours (il suffit de la recopier !). $\boxed{\text{Le résultat est donc vrai dans ce cas}}$. Un exemple de tel groupe est $\boxed{(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}}$, l'ensemble des suites à valeurs dans $\mathbb{Z}/2\mathbb{Z}$ muni de l'addition terme à terme (groupe produit). Tous les éléments sont d'ordre 2.

4. On considère $\mathbb{U}$ l'ensemble des racines de l'unité. Il s'agit d'un groupe (cf TD, exercice 1.10). Tout élément de $\mathbb{U}$ est d'ordre fini, car c'est une racine n-ième de l'unité pour un certain $n \in \mathbb{N}$, et l'ensemble des ordres des éléments de $\mathbb{U}$ n'est pas borné, donc l'énoncé n'a soit pas de sens si on considère qu'on ne peut pas définir le ppcm d'une partie infinie de $\mathbb{N}$, soit faux si on considère que ce dernier vaut $+\infty$.

   Dans tous les cas, $\boxed{\text{on ne peut pas simplement supposer que tous les éléments de } G \text{ soient d'ordre fini}}$.