

Corrigé de la feuille d'exercices n°5

Exercices obligatoires : 1 ; 2 ; 3 ; 4 ; 8 ; 10

1. Exercices importants

Exercice 1.

1. Soit $n, m \in \mathbb{Z}$. Montrer que $m|n$ (m divise n) si, et seulement si $n\mathbb{Z} \subset m\mathbb{Z}$.
2. a) Décrire les ensembles $3\mathbb{Z} \cap 4\mathbb{Z}$, $6\mathbb{Z} \cap 9\mathbb{Z}$, $4\mathbb{Z} \cap 8\mathbb{Z}$;
b) Plus généralement, caractériser le sous-groupe $n\mathbb{Z} \cap m\mathbb{Z}$ pour $n, m \in \mathbb{N}$.
3. Soit $n, m \in \mathbb{Z}$.
a) Montrer que

$$n\mathbb{Z} + m\mathbb{Z} = \{nu + mv \mid u, v \in \mathbb{Z}\}$$
 est un sous-groupe de $\mathbb{Z}$;
b) Caractériser ce sous-groupe.

Correction.

1. Soit $n, m \in \mathbb{Z}$.
 - $(\Rightarrow)$. On suppose $m|n$. Alors il existe $p \in \mathbb{Z}$ tel que $n = mp$.
Soit $k \in n\mathbb{Z}$. Alors il existe $q \in \mathbb{Z}$ tel que $k = nq$. Par suite,

$$k = nq = (mp)q = m(pq) \in m\mathbb{Z},$$
 donc $n\mathbb{Z} \subset m\mathbb{Z}$.
 - $(\Leftarrow)$. On suppose $n\mathbb{Z} \subset m\mathbb{Z}$. Alors, comme $n = n.1 \in n\mathbb{Z}$, n appartient à $m\mathbb{Z}$. Donc il existe $p \in \mathbb{Z}$ tel que $n = mp$ i.e. $m|n$.
2. a) On a :
 - $3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$
 - $6\mathbb{Z} \cap 9\mathbb{Z} = 18\mathbb{Z}$
 - $4\mathbb{Z} \cap 8\mathbb{Z} = 8\mathbb{Z}$
- b) Soit $n, m \in \mathbb{Z}$. Alors $n\mathbb{Z} \cap m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ comme intersection de sous-groupes de $\mathbb{Z}$. Ainsi, il existe $M \in \mathbb{Z}$ tel que $n\mathbb{Z} \cap m\mathbb{Z} = M\mathbb{Z}$.
Montrons que $M = \text{ppcm}(n, m)$. Soit k un multiple commun de n et m . Alors $n|k$ et $m|k$ donc $k \in n\mathbb{Z} \cap m\mathbb{Z} = M\mathbb{Z}$. Par suite $M|k$. Il en résulte que $M = \text{ppcm}(n, m)$.
Remarque : on a utilisé le résultat suivant (démontré en sup) : Soit $n, m \in \mathbb{Z}$ et $M \in \mathbb{N}$. Alors $M = \text{ppcm}(n, m)$ si, et seulement si, pour tout multiple commun k de n et m , $M|k$.

3. Soit $n, m \in \mathbb{Z}$.

a) On considère

$$n\mathbb{Z} + m\mathbb{Z} = \{nu + mv \mid u, v \in \mathbb{Z}\}.$$

i) On a $0 = n.0 + m.0 \in n\mathbb{Z} + m\mathbb{Z}$

ii) Soit $x, y \in n\mathbb{Z} + m\mathbb{Z}$. Alors il existe $u, v, p, q \in \mathbb{Z}$ tels que $x = nu + mv$ et $y = np + mq$. Montrons que $x + (-y) \in n\mathbb{Z} + m\mathbb{Z}$. On a :

$$x - y = nu + mv - (np + mq) = n(p - u) + m(v - q) \in n\mathbb{Z} + m\mathbb{Z}.$$

Donc $n\mathbb{Z} + m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

b) Comme $n\mathbb{Z} + m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, alors il est de la forme $d\mathbb{Z}$ avec $d \in \mathbb{N}$. Montrons que $d = \text{pgcd}(n, m)$.

D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $nu + mv = \text{pgcd}(n, m)$, donc $\text{pgcd}(n, m) \in n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. Par suite, $d \mid \text{pgcd}(n, m)$. De plus $n = n.1 + m.0$ et $m = n.0 + m.1$, donc $n, m \in n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, donc $d \mid n$ et $d \mid m$. Ainsi, d est un diviseur commun positif de n, m qui est inférieur ou égal à $\text{pgcd}(n, m)$ (car d positif et $d \mid \text{pgcd}(n, m)$) donc $d = \text{pgcd}(n, m)$.

Exercice 2. Théorème de Lagrange

Soit $(G, \cdot)$ un groupe fini et H un sous-groupe de G .

1. Montrer que pour tout $a \in G$, H et $aH = \{ah \mid h \in H\}$ ont le même nombre d'éléments.
2. Soient $a, b \in G$. Démontrer que $aH = bH$ ou $aH \cap bH = \emptyset$.
3. En déduire que le cardinal de H divise le cardinal de G .

Correction.

1. Soit $f : H \rightarrow aH$ définie par $f(h) = ah$. Il s'agit clairement d'une surjection de H sur aH . De plus, si $ah_1 = ah_2$, alors $h_1 = h_2$ car a est inversible, et donc f est aussi injective. f est donc une bijection de H sur aH ; ces deux ensembles ont le même nombre d'éléments.
2. Supposons que $aH \cap bH \neq \emptyset$ et prouvons que $aH = bH$. Par symétrie, il suffit de prouver que $aH \subset bH$. Soit $x \in aH \cap bH$, $x = ah_1 = bh_2$. Prenons $y = ah \in aH$. Alors $a = bh_2h_1^{-1}$ et donc $y = bh_2h_1^{-1}h \in bH$.
3. La réunion des ensembles aH est clairement égale à G (si $x \in G$, il est dans xH). On ne garde que les aH deux à deux disjoints et par les deux questions précédentes, on réalise ainsi une partition de G avec des ensembles qui ont tous le même cardinal, à savoir le cardinal de H . Si k est le nombre d'ensembles nécessaires pour réaliser cette partition, on a

$$k\text{card}(H) = \text{card}(G)$$

et donc le cardinal de H divise celui de G .

2. Exercices basiques

a. Ordre d'un élément dans un groupe

Exercice 3.

Quel est l'ordre de $\bar{9}$ dans $\mathbb{Z}/12\mathbb{Z}$?

Correction.

On a (tenant compte du fait que la loi est notée additivement) :

$$2 \times \bar{9} = \bar{6}, \quad 3 \times \bar{9} = \bar{3}, \quad 4 \times \bar{9} = 0.$$

$\bar{9}$ est donc d'ordre 4.

Exercice 4.

Soit G un groupe et $x \in G$ d'ordre n . Quel est l'ordre de x^2 ?

Correction.

D'abord, on remarque que x^2 est d'ordre fini, car $(x^2)^n = (x^n)^2 = e^2 = e$. De plus, son ordre que nous allons noter d divise n . Distinguons alors deux cas :

- Si n est pair et s'écrit $2p$, alors $(x^2)^p = x^n = e$, et donc l'ordre de x^2 divise p . De plus, si l'ordre de x^2 est inférieur strict à p , on a $x^{2d} = e$ avec $1 \leq 2d < n$, ce qui contredit la définition de l'ordre de x . Donc, si n est pair, l'ordre de x est $n/2$.
- Si n est impair, alors on a $x^{2d} = e$ et donc $n|2d$. Mais comme n est premier avec 2, on a $n|d$. Puisqu'on avait déjà remarqué que $d|n$, on en déduit que $d = n$. En résumé, si n est impair, l'ordre de x^2 est n .

Exercice 5.

Soit G un groupe dont tous les éléments (sauf l'élément neutre) sont d'ordre au plus deux. Démontrer que G est abélien.

Correction.

Pour tous $x, y \in G$, on a $x^2 y^2 = e = xyxy$ soit en simplifiant à gauche par x et à droite par y , $xy = yx$.

3. Exercices d'entraînement

a. Ordre d'un élément dans un groupe

Exercice 6.

Soit G un groupe de cardinal $2n$.

1. Démontrer que la relation $\mathcal{R}$ définie sur G par

$$x\mathcal{R}y \iff x = y \text{ ou } x = y^{-1}$$

est une relation d'équivalence sur G .

2. En déduire que G admet des éléments d'ordre deux.

Correction.

1. La relation est clairement réflexive et symétrique. De plus, si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors

- si $x = y$ et $y = z$, on a $x = z$;
- si $x = y$ et $y = z^{-1}$, on a $x = z^{-1}$;
- si $x = y^{-1}$ et $y = z$, on a $x = z^{-1}$;
- si $x = y^{-1}$ et $y = z^{-1}$, on a $x = z$.

Dans tous les cas, on a $x\mathcal{R}z$ et la relation est transitive.

2. Une classe d'équivalence comporte

- ou bien un seul élément, si $x = x^{-1}$;
- ou bien deux éléments, si $x \neq x^{-1}$; les éléments sont alors x et x^{-1} .

Il y a au moins une classe d'équivalence avec un seul élément : la classe de l'élément neutre. De plus, les classes d'équivalence forment une partition de G , et G est de cardinal pair. Il doit donc y avoir une autre classe de cardinal 1 (sinon le cardinal de G serait impair). Cette autre classe de cardinal 1 donne un élément x égal à son inverse.

Exercice 7.

Soient G et H deux groupes.

1. Montrer que si g est un élément d'ordre p de G et h un élément d'ordre q de H , alors (g, h) est d'ordre $\text{ppcm}(p, q)$ dans $G \times H$.
2. On suppose que G et H sont cycliques. Démontrer que $G \times H$ est cyclique si et seulement si les ordres de G et H sont premiers entre eux.

Correction.

1. On a $(g, h)^n = (g^n, h^n) = (e, e)$ si et seulement si on a à la fois $p|n$ et $q|n$, donc si et seulement si $\text{ppcm}(p, q)|n$. Ainsi, l'ordre de (g, h) est bien le ppcm de p et q .
2. Soit p l'ordre de G et q l'ordre de H . Si $p \wedge q = 1$, si x est un générateur de G (d'ordre p donc) et si y est un générateur de H (d'ordre q donc), alors (x, y) est d'ordre $\text{ppcm}(p, q) = pq$. Puisque $G \times H$ est de cardinal pq , c'est bien un groupe cyclique. Réciproquement si $G \times H$ est cyclique, soit (g, h) un générateur de $G \times H$. Alors g est un générateur de G et h est un générateur de H . Leur ordre respectif est donc p (resp. q), et par la première question, (g, h) est d'ordre $\text{ppcm}(p, q)$. Puisqu'on sait qu'il est d'ordre pq , on a bien $\text{ppcm}(p, q) = pq$ qui implique que p et q sont premiers entre eux.

Exercice 8.

Soit G un groupe admettant un nombre fini de sous-groupes.

1. Démontrer que tout élément de G est d'ordre fini.
2. En déduire que G est fini.

Correction.

1. Supposons que G admette un élément x d'ordre infini et notons H le sous-groupe engendré par x . Alors H est isomorphe à $(\mathbb{Z}, +)$, qui contient une infinité de sous-groupes. On en déduit que H , et donc G , contiennent aussi une infinité de sous-groupes (les sous-groupes engendrés par les x^n , $n \geq 1$, qui ne sont pas deux à deux égaux).
2. Pour $x \in G$, notons H_x le sous-groupe engendré par x . Alors on a $G = \bigcup_{x \in G} H_x$. Mais puisque G contient seulement un nombre fini de sous-groupes, il y a un nombre fini de H_x différents, notons-les $H_{x_1}, \dots, H_{x_p}$, d'où $G = \bigcup_{i=1}^p H_{x_i}$. Mais chacun des H_{x_i} est fini d'après la question précédente. Donc G est fini.

Exercice 9.

Soit $G = (\mathbb{Z}/20\mathbb{Z})^*$ le groupe des éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$.

1. Donner la liste de tous les éléments de G .
2. Pour tout $a \in G$, déterminer le sous groupe $\langle a \rangle$ engendré par a .
3. Déterminer un ensemble minimal de générateurs de $(G, \cdot)$.
4. $(G, \cdot)$ est-il un groupe cyclique ?
5. Déterminer tous les sous-groupes de G et, pour chaque sous-groupe, préciser un ensemble de générateurs.
6. Parmi les sous-groupes de $(G, \cdot)$, lesquels sont isomorphes à un groupe additif $(\mathbb{Z}/m\mathbb{Z}, +)$?

Correction.

1. Rappelons que par le théorème de Bézout, n est inversible dans $(\mathbb{Z}/20\mathbb{Z}, \cdot)$ si et seulement si n est premier avec 20. On a donc $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$.
2. On prend un élément et toutes ses puissances, jusqu'à obtenir l'élément neutre 1. On obtient

$$\begin{aligned}\langle 1 \rangle &= \{1\} \\ \langle 3 \rangle &= \{1, 3, 7, 9\} \\ \langle 7 \rangle &= \{1, 3, 7, 9\} \\ \langle 9 \rangle &= \{1, 9\} \\ \langle 11 \rangle &= \{1, 11\} \\ \langle 13 \rangle &= \{1, 9, 13, 17\} \\ \langle 17 \rangle &= \{1, 9, 13, 17\} \\ \langle 19 \rangle &= \{1, 19\}\end{aligned}$$

3. On vient de voir qu'on ne peut pas engendrer le groupe avec un seul élément. Essayons

avec deux éléments. C'est facile à voir. Si on prend par exemple 3 et 11, le groupe engendré comprend au moins $\langle 3 \rangle$ et $\langle 11 \rangle$, c'est-à-dire au moins 5 éléments. Comme son ordre doit diviser l'ordre du groupe, il contient au moins 8 éléments, c'est-à-dire que c'est G tout entier. Autrement dit, on a prouvé que $\langle 3, 11 \rangle = G$ et donc $\{3, 11\}$ est un ensemble minimal de générateurs de G .

4. Aucun élément de G n'engendre seul le groupe. G n'est pas cyclique.
5. Les sous-groupes de G sont d'ordre 1, 2, 4 ou 8. Dans G , il y a un élément d'ordre 1, 4 éléments d'ordre 4 et 3 éléments d'ordre 2. Si on combine deux éléments d'ordre 4 qui n'engendrent pas le même sous-groupe, ou un élément d'ordre 4 avec un élément d'ordre 2 qui n'est pas dans le sous-groupe engendré (comme à la question 3), on obtiendra G tout entier. Reste à voir les sous-groupes engendrés par les éléments d'ordre 2 : on a

$$\langle 11, 19 \rangle = \{1, 11, 19, 9\}$$

$$\langle 3, 11 \rangle = \langle 3, 13 \rangle = \langle 3, 19 \rangle = \langle 11, 13 \rangle = \langle 13, 19 \rangle = G.$$

6. Parmi les sous-groupes de G , ceux de la deuxième question sont cycliques, donc isomorphes à $\mathbb{Z}/m\mathbb{Z}$ où $m = 1, 2, 4$ suivant le cas. Le sous-groupe $\langle 11, 19 \rangle$ n'est pas cyclique, car il n'est pas engendré par un seul élément. De même, G n'est pas cyclique.

4. Exercices d'approfondissement

a. Ordre d'un élément dans un groupe

Exercice 10.

Soit G un groupe abélien, x et y deux éléments de G d'ordres respectifs p et q .

1. On suppose que p et q sont premiers entre eux. Démontrer que xy est d'ordre pq .
2. Importance des hypothèses - 1 : Si $H = GL_2(\mathbb{R})$, $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, vérifier que A et B sont d'ordre fini, mais que AB n'est pas d'ordre fini.
3. Importance des hypothèses - 2 : Si p et q ne sont pas supposés premiers entre eux, démontrer que le produit xy n'est pas nécessairement d'ordre pq , ou d'ordre $\text{ppcm}(p, q)$.
4. Une application :
 - (a) Soit d un diviseur de p . Démontrer qu'il existe un élément d'ordre d dans G .
 - (b) En déduire que G admet des éléments d'ordre $\text{ppcm}(p, q)$.
 - (c) On suppose de plus que G est fini. Démontrer que G admet un élément dont l'ordre est le ppcm de l'ordre des éléments de G .

Correction.

1. Notons d l'ordre de xy . Remarquons que $(xy)^{pq} = (x^p)^q(y^q)^p = e$, et donc $d|pq$. De plus, puisque $(xy)^d = e$, on en déduit que $x^d = y^{-d}$. Il vient alors

$$x^{dq} = (y^{-d})^q = (y^q)^{-r} = e.$$

Ainsi, $p|dq$ et puisque p et q sont premiers entre eux, on en déduit que $p|d$. De la même façon, on a $q|d$ et en utilisant à nouveau que p et q sont premiers entre eux, on conclut que $pq|d$. Ainsi, on a bien que $d = pq$.

2. On vérifie facilement que A est d'ordre 4, que B est d'ordre 3 et que

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

On prouve alors par récurrence que, pour tout $n \geq 1$,

$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

AB n'est pas d'ordre fini, et donc l'hypothèse que G est commutatif est importante.

3. Si x est un élément d'ordre $n \geq 2$ dans un groupe G , son inverse x^{-1} est aussi d'ordre n , et pourtant le produit xx^{-1} est d'ordre 1, et non d'ordre n ou n^2 !
4. Une application :
- (a) Considérons $a = x^{p/d}$. Alors on a $a^d = x^p = e$. D'autre part, si $a^r = e$, alors $x^{rp/d} = e$ et donc rp/d est un multiple de p . En particulier r/d est un entier, ce qui signifie que $d|r$. a est donc bien d'ordre d .
- (b) Décomposons p et q en facteurs premiers (pour avoir les mêmes facteurs, on s'autorise des exposants nuls) :

$$p = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad q = p_1^{\beta_1} \cdots p_r^{\beta_r}.$$

On sait qu'alors

$$\text{ppcm}(p, q) = p_1^{\max(\alpha_1, \beta_1)} \cdots p_r^{\max(\alpha_r, \beta_r)}.$$

Par la question précédente, il est possible, pour chaque $i = 1, \dots, r$, de fabriquer un élément a_i d'ordre $p_i^{\max(\alpha_i, \beta_i)}$ (on le fabrique à partir de x si $\alpha_i \geq \beta_i$, à partir de y sinon). En utilisant le résultat de la première question et une simple récurrence, le produit $a_1 \dots a_r$ est bien d'ordre $\text{ppcm}(p, q)$.

- (c) Notons $x_1, \dots, x_r$ les éléments de G , d'ordres respectifs $q_1, \dots, q_r$. Alors d'après la question précédente, il existe un élément d'ordre $\text{ppcm}(q_1, q_2)$. Puis appliquant une nouvelle fois la question précédente, il existe un élément d'ordre $\text{ppcm}(\text{ppcm}(q_1, q_2), q_3) = \text{ppcm}(q_1, q_2, q_3)$. Par une récurrence facile, on construit un élément d'ordre le ppcm que $q_1, \dots, q_r$.

Exercice 11.

Soit G un groupe cyclique et soit H un sous-groupe de G . Démontrer que H est cyclique.

Correction.

Soit a un générateur de G . L'ensemble des entiers $p \geq 1$ tels que $a^p \in H$ est non-vide (puisque $a^{\text{card}(G)} = e \in H$). Il contient un plus petit élément que nous noterons n . On va alors prouver que H est le groupe engendré par a^n . Il est d'abord évident que le sous-groupe engendré par a^n est contenu dans H . Réciproquement, soit $x \in H$. x s'écrit $x = a^p$, et il suffit de prouver que

$p = kn$. Effectuons la division euclidienne de p par n : $p = qn + r$ avec $0 \leq r < n$. Mais alors :

$$a^p = (a^n)^q a^r \implies a^r = a^p (a^n)^{-q} \in H.$$

Par minimalité de n , ceci n'est possible que si $r = 0$, donc que si p est un multiple de n . Remarquons la proximité entre cette démonstration et celle des sous-groupes de $\mathbb{Z}$.

Exercice 12.

1. Soit G un groupe et H, K deux sous-groupes de G d'ordre des entiers premiers. Démontrer que $H = K$ ou que $H \cap K = \{e\}$.
2. Démontrer que dans un groupe d'ordre 35, il existe un élément d'ordre 5 et un élément d'ordre 7.

Correction.

1. Soit p l'ordre de H , qui est premier. Puisque un élément de H a un ordre qui divise p , cet ordre ne peut être égal que à 1, si c'est l'élément neutre, ou à p . Autrement dit, tout élément de H autre que l'élément neutre génère H . Il en est de même pour tout élément de K . Ainsi, si $H \cap K$ contient un élément x différent de e , il contient toutes les puissances de x , donc H et K , et $H = K$.
2. Soit G un tel groupe. Ses éléments peuvent être d'ordre 1, 5, 7 ou 35. Si G admet un élément d'ordre 35 (ie G est cyclique), que l'on appelle a , alors a^5 est d'ordre 7 et a^7 est d'ordre 5. Supposons donc que G n'est pas cyclique et qu'il n'admet pas d'éléments d'ordre 7. Alors tous ses éléments, sauf l'élément neutre, sont d'ordre 5, et G est réunion de sous-groupes d'ordre 5. D'après la première question, l'intersection de deux de sous-groupes, quand ils sont distincts, est restreinte à $\{e\}$. Notons $G_1, \dots, G_n$ ces sous-groupes distincts. Alors chaque G_i s'écrit $G_i = \{e\} \cup H_i$, et les $H_1, \dots, H_n$ sont deux à deux disjoints. Autrement dit,

$$G = \{e\} \cup H_1 \cup \dots \cup H_n$$

est une partition de G . Comme chaque H_i est de cardinal 4, ceci implique que $35 = 4n + 1$. Mais alors 34 serait un multiple de 4, ce qui n'est pas le cas. Le raisonnement est similaire si on suppose que G n'admet pas d'éléments d'ordre 5. On aurait alors $35 = 6m + 1$ pour un entier m , ce qui n'est pas le cas puisque 34 n'est pas un multiple de 6.