
M2 MEEF : TD2

Exercice 1

1. Soit $n \in \mathbb{N} - \{0, 1\}$. Montrer que tous les entiers suivants ne sont pas des nombres premiers : $n! + 2, \dots, n! + n$.
2. Donner 100 entiers consécutifs non premiers.

Exercice 2

On pose $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$.

- (a) Montrer que $SL_2(\mathbb{Z})$ est un sous-groupe du groupe des matrices inversibles à coefficients dans $\mathbb{Z}$.
- (b) On considère les deux matrices

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

Démontrer que A et B sont d'ordres finis mais que AB est d'ordre infini.

Exercice 3

1. Soient G un groupe, a et b deux éléments de G d'ordre fini tels que $ab = ba$ et $\langle a \rangle \cap \langle b \rangle = \{e\}$. Montrer que l'ordre de ab est égal au ppcm des ordres de a et b .
2. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 1 & 4 & 2 & 6 & 9 & 8 & 5 & 10 \end{pmatrix} \in S_{10}$.
 - (a) Décomposer σ en produit de cycles disjoints et en produit de transpositions.
 - (b) Déterminer l'ordre de σ .
 - (c) Calculer σ^{2026} .

Exercice 4

1. Déterminer les sous-groupes de $(\mathbb{Z}, +)$.
2. Déterminer les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ puis ceux de $\mathbb{Z}/7\mathbb{Z}$.
3. Déterminer les sous-groupes de $\{z \in \mathbb{C}, z^4 = 1\}$.

Exercice 5

Soit $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$.

- 1) Montrer que $\mathbb{Z}[i\sqrt{5}]$ est un sous-anneau de $(\mathbb{C}, +, \cdot)$
- 2) Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{5}]$.

Exercice 6

Répondre par vrai ou faux aux assertions suivantes, en donnant suivant les cas un court argument ou un contre-exemple :

1. Si G est un groupe cyclique, il existe $n \geq 1$ tel que G soit isomorphe à $\mathbb{Z}$ ou à $n\mathbb{Z}$
Réponse : Faux : $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ est un groupe fini, n'est donc pas en bijection avec un groupe infini.
2. Il existe un groupe d'ordre 6 qui ne contient aucun élément d'ordre 6
Réponse : Vrai : Le groupe symétrique S_3 n'a pas d'élément d'ordre 6.
3. Il existe un élément d'ordre 4 dans le groupe $GL(2, \mathbb{R})$
Réponse : Vrai : La matrice $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est d'ordre 4, car $A^2 = -I$, $A^3 = -A$ et $A^4 = I$.

Exercice 7

Quelles sont les assertions correctes ?

1. Si G est un groupe abélien, alors G est cyclique.
Réponse : Faux : Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est abélien mais n'a pas d'élément d'ordre 4. Tout élément différent de l'élément neutre de ce groupe est d'ordre 2.
2. Si G est un groupe cyclique, alors G est abélien.
Réponse : Vrai : En effet, si G est cyclique d'ordre p , avec p un nombre premier, alors tout élément différent de l'élément neutre de ce groupe est d'ordre p , par conséquent il engendre le groupe, donc ce groupe est cyclique.
3. Si G est d'ordre p , avec p un nombre premier, alors G est cyclique.
Réponse : Vrai : En effet, si G est cyclique alors il existe $g \in G$ tel que $G = \langle g \rangle$. Soient x et y élément de G , alors ils s'écrivent $x = g^n$ et $y = g^m$ avec m, n dans $\mathbb{Z}$. Tout élément différent de l'élément neutre
Ainsi $x.y = g^n.g^m = g^{n+m} = g^{m+n} = g^m.g^n = y.x$
4. Si G est d'ordre fini et cyclique, alors G est d'ordre premier.
Réponse : Faux : $G = \mathbb{Z}/6\mathbb{Z}$ est cyclique d'ordre 6 qui n'est pas un nombre premier.

Exercice 8

1. Il existe deux groupes d'ordre 4 non isomorphes : vrai ou faux ?
Réponse : Faux : $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ sont deux groupes d'ordre 4, qui ne sont pas isomorphes car $\mathbb{Z}/4\mathbb{Z}$ est cyclique alors que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne l'est pas.
2. Il existe exactement quatre éléments d'ordre 2 dans le groupe $\text{Isom}(\mathbb{R})$ des isométries du plan préservant un rectangle (non carré) R : vrai ou faux ?
Réponse : Faux : Il n'y en a que 3, le dernier élément est l'identité qui est d'ordre 1.
3. Le groupe symétrique S_{10} contient au moins un élément d'ordre 30 : vrai ou faux ?
Réponse : Vrai : si $\sigma = (12)(345)(678910)$, alors $\text{ordre}(\sigma) = \text{ppcm}(2,3,5) = 30$.
4. Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est un exemple de groupe fini, abélien et non cyclique : vrai ou faux ?
Réponse : Faux : $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est cyclique engendré par $(\bar{1}, \hat{1})$, où $\bar{1}$ est la classe de 1 dans $\mathbb{Z}/2\mathbb{Z}$ et $\hat{1}$ est la classe de 1 dans $\mathbb{Z}/3\mathbb{Z}$.

Exercice 9

Déterminer tous les sous-groupes d'ordre ≤ 5 .

Réponse : à isomorphisme près, on pour l'ordre 1 : $G = \{1\}$

pour l'ordre 2 : $G = \mathbb{Z}/2\mathbb{Z}$

pour l'ordre 3 : $G = \mathbb{Z}/3\mathbb{Z}$

pour l'ordre 4 : on a deux groupes (non isomorphes) $G = \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

pour l'ordre 5 : $G = \mathbb{Z}/5\mathbb{Z}$

Remarque : Si G est d'ordre p , avec p un nombre premier, alors G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$

Exercice 10

Montrer que dans un groupe G , toute partie non vide finie stable par la loi du groupe est un sous-groupe. Donner un contre-exemple à la propriété précédente dans le cas d'une partie infinie.

Réponse :

1) Notons par $\cdot$ la loi du groupe G . Soit H une telle partie. Il reste à montrer que tout $g \in H$ admet un inverse. On a la suite des g^k , $k \in \mathbb{N}$, par hypothèse $g^k \in H$

$$e = g^0, g, g^2, \dots, g^k \dots$$

Comme H est fini, la suite des g^k est finie, il existe alors $n > m$ tels que $g^n = g^m$, d'où $g^{n-m} = e$ i.e. $g \cdot g^{n-m-1} = e$, ainsi g admet un inverse, à savoir $g^{-1} = g^{n-m-1}$.

2) $\mathbb{N}$ est une partie (infinie) de $\mathbb{Z}$ stable par l'addition, mais n'est pas un sous-groupe, il manque les inverses.

Exercice 11

Montrer que :

- 1) $11 \mid 2^{123} + 3^{121}$
- 2) $7 \mid 3^{2n+1} + 2^{n+2}$

Réponse

- 1) On a $2^5 \equiv -1 \pmod{11}$, d'où $2^{10} \equiv 1 \pmod{11}$. On a aussi $3^5 \equiv 1 \pmod{11}$, alors $2^{123} + 3^{121} = (2^{10})^{12} \cdot 2^3 + (3^{10})^{12} \cdot 3 \equiv 2^3 + 3 \equiv 0 \pmod{11}$.
- 2) $3^{2n+1} + 2^{n+2} = (3^2)^n \cdot 3 + 2^n \cdot 4 \equiv 2^n(3 + 4) \equiv 0 \pmod{7}$.

Exercice 12

- 1) Déterminer $x_1, x_2 \in \mathbb{Z}$ tels que $\begin{cases} x_1 \equiv 1 \pmod{28} \\ x_1 \equiv 0 \pmod{19} \end{cases}$ et $\begin{cases} x_2 \equiv 0 \pmod{28} \\ x_2 \equiv 1 \pmod{19} \end{cases}$
- 2) Déterminer $x \in \mathbb{Z}$ tel que $\begin{cases} x \equiv 13 \pmod{28} \\ x \equiv 9 \pmod{19} \end{cases}$

Réponse

- 1) On a $28 \wedge 19 = 1$, d'où $19 \cdot 3 + (2) \cdot 28 = 1$. En posant $c_1 = 19u = 57$ et $c_2 = 28v = -56$, on obtient $\begin{cases} c_1 \equiv 1 \pmod{28} \\ c_1 \equiv 0 \pmod{19} \end{cases}$
Ainsi, $x_1 \equiv c_1 \pmod{28 \cdot 19 = 532}$ De même, $x_2 \equiv c_2 \pmod{28 \cdot 19 = 532}$.
- 2) Posons $b_1 = 13$ et $b_2 = 9$ alors

$$\begin{cases} x \equiv 13 \pmod{28} \\ x \equiv 9 \pmod{19} \end{cases} \iff x \equiv b_1 c_1 + b_2 c_2 \pmod{28 \cdot 19 = 532}$$

$$\text{i.e } x \equiv 13 \cdot 57 - 9 \cdot 56 = 237 \pmod{28 \cdot 19 = 532}.$$

Exercice 13

- 1) Déterminer le groupe des isométries d'un triangle dont les longueurs des côtés sont distinctes deux à deux.

Réponse : Soit T un triangle (non aplati) dont les longueurs des côtés sont distinctes deux à deux. Comme toute isométrie préservant T préserve l'ensemble des sommets et comme la distance entre deux sommets est conservée, les sommets sont nécessairement fixés, alors une telle isométrie est l'identité. Ainsi $Isom(T) = \{Id\}$.

2) Déterminer le groupe des isométries d'un rectangle.

Réponse :

Si $P = ABCD$ est un rectangle qui n'est pas un carré. On note O l'isobarycentre des sommets (c'est aussi l'intersection des diagonales). Une application r de $\text{Isom}^+(P)$ sera une rotation de centre O . Par conservation des distances, le segment $[OA]$ sera transformé en $[OA]$ ou $[OC]$, de sorte que $r(A) = A$ ou C . Si $r(A) = A$, alors $r = Id$, et si $r(A) = C$ alors r sera la symétrie s_O par rapport au point O . Les réciproques étant triviales, on a montré l'égalité $\text{Isom}^+(P) = \{Id, s_O\}$.

les mêmes arguments montrent que $\text{Isom}^-(P) = \{s_{\Delta_{AC}}, s_{\Delta_{BD}}\}$, où $s_{\Delta_{AC}}$ et $s_{\Delta_{BD}}$ sont les réflexions par rapport aux médiatrices Δ_{AB} et Δ_{BC} respectives des côtés $[AB]$ et $[BC]$. Ainsi, $\text{Isom}(P) = \{Id, s_O, s_{\Delta_{AC}}, s_{\Delta_{BD}}\}$.