

Feuille 3 : Groupes

Exercice 1. Résoudre dans \mathbb{Z} les systèmes de congruences suivants :

$$\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{11} \end{cases}, \quad \begin{cases} x \equiv 4 \pmod{21} \\ x \equiv 10 \pmod{33} \end{cases} \text{ et } \begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{6} \end{cases}.$$

Exercice 2. Soit $G = \{e, x, y, z, t\}$ un ensemble muni d'une loi de composition interne $*$, dont la table de multiplication est donnée par

*	e	x	y	z	t
e	e	x	y	z	t
x	x	e	t	y	z
y	y	z	e	t	x
z	z	t	x	e	y
t	t	y	z	x	e

La loi $*$ est-elle commutative ? Est-ce une loi de groupe ?

Exercice 3. Soit G un groupe d'ordre 2. Ecrire sa table de multiplication.

Exercice 4. Quelles sont les structures de groupes possibles sur un ensemble à 3 éléments ? Et à 4 éléments ?

Exercice 5. Soit G un groupe tel que $g^2 = 1$ pour tout $g \in G$. Montrer que G est abélien.

Exercice 6. Soit G un groupe. Soit $x, y \in G$ tels que $yx = xy^2$ et $xy = yx^2$. Montrer que $x = y = 1$.

Exercice 7. Soit $n \in \mathbb{N}^*$. On note $\mathcal{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$.

1. Montrer que \mathcal{U}_n est un sous-groupe de (\mathbb{C}^*, \times) .
2. Montrer que \mathcal{U}_n est un groupe cyclique d'ordre n .
3. Montrer que m divise n si et seulement si $\mathcal{U}_m \subseteq \mathcal{U}_n$.

Exercice 8. Trouver tous les ordres des éléments des groupes $(\mathbb{Z}/12\mathbb{Z}, +)$ et $((\mathbb{Z}/12\mathbb{Z})^*, \cdot)$.

Exercice 9. Soit G un groupe abélien. Montrer que l'ensemble $H = \{x \in G \mid \text{ord}(x) \text{ est fini}\}$ est un sous-groupe de G .

Exercice 10. Montrer que $\{e^{2ir\pi} \mid r \in \mathbb{Q}\}$ muni de la multiplication est un groupe infini dans lequel tout élément est d'ordre fini.

Exercice 11. Soit G un groupe d'ordre 35. Montrer que G possède un élément d'ordre 5 et un élément d'ordre 7.

Exercice 12. On note $\mathcal{M}_2(\mathbb{Z})$ et $SL_2(\mathbb{Z})$ respectivement l'ensemble des matrices 2×2 à coefficients entiers et l'ensemble de celles qui sont de déterminant 1.

1. Montrer que $SL_2(\mathbb{Z})$ est un groupe multiplicatif d'ordre infini. Est-il commutatif?

2. Soient $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Déterminer l'ordre de A , B et AB .

Exercice 13. Soit G un groupe. Montrer que si deux éléments x et y de G commutent et sont d'ordre a et b premier entre eux, alors l'ordre de xy est ab .

Exercice 14. Montrer que le groupe multiplicatif de $\mathbb{Z}/13\mathbb{Z}$ est cyclique.

Un groupe est :

- Un ensemble G
- Une loi $G \times G \xrightarrow{*} G$

qui vérifie :

- $*$ est associative

$\forall x, y, z \in G$

$$(a * b) * c = a * (b * c)$$

- \exists un élément neutre e tq $\forall a \in G$

$$a * e = e * a = a$$

- $\forall a \exists y$ un inverse, $a * b = b * a = e$

neutre \neq inverse

Ex2:

*	e	x	y	z	t
e	e	x	y	z	t
x	x	e	t	y	z
y	y	z	e	t	x
z	z	t	x	e	y
t	t	y	z	x	e

Dans élément neutre : e

$$e * e = e$$

$$e * x = x$$

$$e * y = y$$

Inverse : $a * b$
 $= b * a = e$

associativité : On teste l'associativité x, z, t

$$(x * z) * t = y * t = x$$

$$x * (z * t) = x * y = t$$

Dans $(x * z) * t = x * (z * t)$

Dans \star n'est pas associatif

$$(x \star x) \star y = e \star y = y$$

$$x \star (x \star y) = x +$$

$$= z$$

Clare loi : $G * G \rightarrow G$ est commutative
si $a + b = b + a \quad \forall a, b \in G$

Ex 3 : $G = \{x, y\}$

x	y	
x	x	y
y	y	x

2 possibilités : élément neutre = x

$$x \star (x \star x)$$

:

$$y \star (y \star y) = ? \quad (y \star y) \star y$$

$$= y \star x = y \quad = x \star y = y$$

x	y	
x	y	x
y	x	y

élément neutre = y

$$G = \{e, a\}$$

	e	a
e	e	a
a	a	e

Ex 4

$$G = \{e, x, y\}$$

	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

On suppose

	e	x
e	e	x
x	x	y
y	y	y

$$\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$$

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

	0	2	1
0	0	2	1
2	2	1	0
1	1	0	2

Ex 3 : Order 4

$$G = \{e, x, y, z\}$$

	e	x	y	z
e	e	x	y	z
x	x			
y	y			
z	z			

	e	x	y	z
e	e	x	y	z
x	x	e		
y	y		z	
z	z		y	e

Diagram illustrating a group homomorphism from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{Z}/4\mathbb{Z}$. The top row shows elements e, x, y, z with arrows indicating their mapping to re, ou, e respectively. The bottom row shows the group multiplication table for $\mathbb{Z}/4\mathbb{Z}$.

	e	x	y	z
e	e	x	y	z
x	x	y	z	e
y	y	z	e	x
z	z	e	x	y

Diagram illustrating a group homomorphism from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{Z}/4\mathbb{Z}$. The top row shows elements e, x, y, z with arrows indicating their mapping to re, ou, e respectively. The bottom row shows the group multiplication table for $\mathbb{Z}/4\mathbb{Z}$.

	e	x	y	z
e	e	x	y	z
x	x	z	e	y
y	y	e	z	xe
z	z	y	xe	e

$G_1, G_2, G_3 \rightarrow \mathbb{Z}/4\mathbb{Z}$

$$\begin{aligned}
 G & \quad e \leftrightarrow 0 \\
 & \quad x \leftrightarrow 2 \\
 & \quad y \leftrightarrow 1 \quad \left(\begin{array}{l} ou \\ y \leftrightarrow 2 \\ z \leftrightarrow 1 \end{array} \right) \\
 & \quad z \leftrightarrow 2
 \end{aligned}$$

$$G_3 : \begin{array}{l} e \leftrightarrow 0 \\ x \leftrightarrow 2 \end{array}$$

$$y \leftrightarrow 1$$

$$z \leftrightarrow 3$$

	0	1	2	3
0	0 0	1	2	3
1	1 1	2	3	0
2	2 2	3	0	1
3	3 3	0	1	2

$$G_4 : \begin{array}{l} e \leftrightarrow 0 \\ x \leftrightarrow 2 \end{array}$$

$$y \leftrightarrow 1$$

$$z \leftrightarrow 3$$

$$G_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad (0, 0) \quad (1, 0) \quad (0, 1) \quad (1, 1)$$

	(0, 0)	(1, 0)	(0, 1)	(1, 1)
(0, 0)	0, 0	1, 0	0, 1	1, 1
(1, 0)	1, 0	0, 0	1, 1	0, 1
(0, 1)	0, 1	1, 1	0, 0	1, 0
(1, 1)	1, 1	0, 1	1, 0	0, 0

13/10/3

Ex 6, 7, 8, 12, ex 1.3

$$f : (G, *) \longrightarrow (H, \cdot)$$

- $f(e_G) = e_H$ e : neutre
- $f(g_1 * g_2) = f(g_1) \cdot f(g_2) \quad \forall g_1, g_2 \in G$
- $f(g^{-1}) = (f(g))^{-1} \quad \forall g \in G$

Ex 1:

$$(S) \quad \begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{6} \end{cases}$$

On choisit 2 lignes

$$(S') : \begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{6} \end{cases}$$

6 et 11 premiers entre eux

$$11 = 1 \times 6 + 5 \qquad 1 = 6 - 5 = 6 - (11 - 6)$$

$$6 = 1 \times 5 + 1 \longrightarrow = 2 \times 2 - 11$$

$$5 = 5 \times 1 + 0$$

$$\text{Solutions de } S: x_p = 2 \times 6 \times 4 - 5 \times 11$$

$$= -7$$

$$\text{ppcm}(6, 11) = 66$$

x solution de (S')

$$\Leftrightarrow x \equiv -7 \pmod{66}$$

$$(S) \Leftrightarrow \begin{cases} x \equiv 3 \pmod{7} \\ x \equiv -7 \pmod{66} \end{cases}$$

⋮
⋮
⋮

$$(S) \Leftrightarrow x \equiv 52 \pmod{1129}$$

Ex 6 :

Soit G un groupe

$$(G, *) , x, y \in G$$

$$\textcircled{1} yx = xy^2 \Leftrightarrow y \times x = x \times y \times y$$

$$\textcircled{2} xey = yxe^2 \Leftrightarrow x \times ey = y \times xe \times x$$

Un groupe est :

- Un ensemble G
- Une loi $G \times G \xrightarrow{*} G$
- qui vérifie :
 - $*$ est associative
 - $\forall x, y, z \in G$
 - $(a * b) * c = a * (b * c)$
 - \exists un élément neutre e tq $\forall a \in G$
 - $a * e = e * a = a$
 - $\forall a \exists y$ un inverse, $a * b = b * a = e$
neutre \neq inverse

Montrer que $x = y = 1$:

$$y \textcircled{1} = xey = y^2$$

On multiplie par $(yx)^{-1}$

On a :

$$(yx)^{-1} yx = (yx)^{-1} yx xey$$

$$\text{donc } \textcircled{3} e_G = ey$$

$$\textcircled{1} yx = xey$$

$$\text{donc } g \textcircled{2} = y$$

On multiplie par y^{-1}

$$\circ xe = e_G$$

$$\text{donc } \textcircled{3} \text{ donc } e_G = y$$

Ex : $\mathbb{Z} \subset (\mathbb{R}, +)$ non nul
 $\mathbb{Z}^* \subset (\mathbb{R}^*, \times)$: (\mathbb{Z}^*, \times) pas un groupe
 $\mathbb{Q}^* \subset (\mathbb{R}^*, \times) \rightarrow (\mathbb{Q}^*, \times)$ un groupe

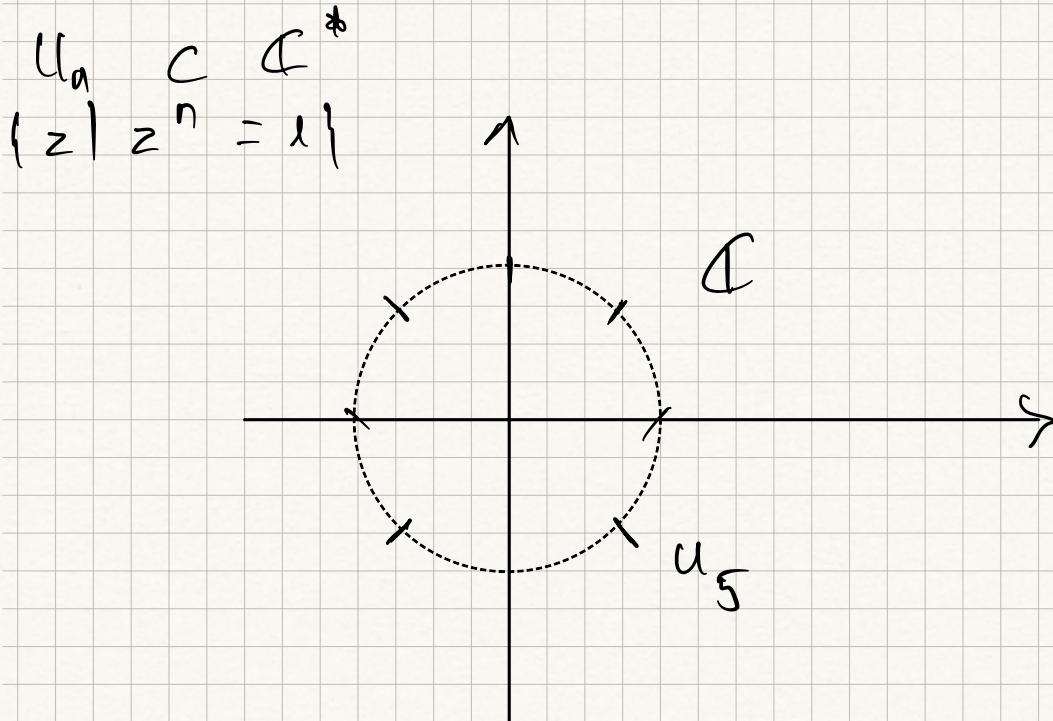
H : C (G, *)

est un sous-groupe si

- $e_G \in H$
- si $h_1, h_2 \in H$, $h_1 * h_2 \in H$
- si $h \in H$, $h^{-1} \in H$

Si on remplit les conditions alors $(H, *)$ est un groupe

Ex : (\mathbb{C}^*, \times)



1) Mq U_n est un sous-groupe de (\mathbb{C}^*, \times)

(\mathbb{C}^*, \times)

Un groupe est :

- Un ensemble G
- Une loi $G \times G \xrightarrow{*} G$

qui vérifie :

- $*$ est associative.

$\forall x, y, z \in G$

$$(a * b) * c = a * (b * c)$$

- \exists un élément neutre e tq $\forall a \in G$

$$a * e = e * a = a$$

- $\forall a \in G \exists y \in G$ tel que $a * y = y * a = e$

neutre \neq inverse

$$\begin{aligned} U_0 &\subset \mathbb{C}^* \\ \{z \mid z^n = 1\} \end{aligned}$$

$U_n \subset \mathbb{C}$ de (\mathbb{C}^*, \times) si :

$x \in \mathbb{H}$ pour tout $x, y \in \mathbb{H}$, on a $x * y \in \mathbb{H}$

x pour tout $x \in \mathbb{H}$, on a $x^{-1} \in \mathbb{H}$

$\forall n \in \mathbb{N} \subset (\mathbb{C}^*, \times)$

o est ce que $1 \in U_n$

neutre pour x

$1^n = 1$ donc $1 \in U_n$

$$U_2 = \{z \mid z^2 = 1\}$$

$$U_3 = \{1, -1\}$$

$$U_4 = \left\{ \begin{matrix} 1, -1, i, -i \\ k=0 \quad k=2 \quad k=1 \quad k=3 \end{matrix} \right\}$$

$$U_n = \left\{ e^{\frac{2i\pi k}{n}} \mid k = \{0, \dots, n-1\} \right\}$$

o Si $z_1, z_2 \in U_n$, on calcule

$$(z_1 * z_2)^n = z_1^n * z_2^n = 1 * 1 = 1$$

donc $z_1 * z_2 \in U_n$

o Si $z \in U_n$, $\left(\frac{1}{z}\right)^n = \frac{1}{z^n} = 1$ donc $\frac{1}{z} \in U_n$

donc $(U_{n, \times})$ est un sous-groupe de (\mathbb{C}^*, \times)

$$2\varphi_{ap}(\mathbb{Z}/n\mathbb{Z}, +) \cong (U_n, \times)$$

by $\xi \in U_n, U_n = \langle \xi \rangle$

by $\xi \in U_n, U_n = \langle \xi \rangle$

$$\xi = e^{\frac{2i\pi}{n}}$$

$$\begin{aligned} \text{Si } z \in U_n, \exists k \in \mathbb{Z} \text{ tq } \\ z = e^{\frac{2ik\pi}{n}} = (e^{\frac{2i\pi}{n}})^k \\ = \xi^k \end{aligned}$$

donc $U_n = \langle \xi \rangle$

donc U_n est cyclique et

$|U_n| = n$ donc U_n cyclique $f(-\bar{a}) = e^{\frac{2i(-\bar{a})\pi}{n}}$
d'ordre n

$$ap(\mathbb{Z}/n\mathbb{Z}, +) \xrightarrow{\cong} (U_n, \times)$$

$$\bar{k} \longmapsto e^{\frac{2ik\pi}{n}}$$

$$f(0) = e^{\frac{2i \cdot 0 \pi}{n}} = 1$$

$$\begin{aligned} f(\bar{a} + \bar{b}) &= e^{\frac{2i(a+b)\pi}{n}} \\ &= e^{\frac{2ia\pi}{n}} \times e^{\frac{2ib\pi}{n}} \\ &= f(\bar{a}) \times f(\bar{b}) \end{aligned}$$

$$\begin{aligned} f(-\bar{a}) &= e^{\frac{2i(-\bar{a})\pi}{n}} \\ &= e^{-\frac{2i\bar{a}\pi}{n}} \\ &= \frac{1}{e^{\frac{2i\bar{a}\pi}{n}}} = \frac{1}{f(\bar{a})} \end{aligned}$$

donc f morphisme de groupes
+ une bijection

donc $(\mathbb{Z}/n\mathbb{Z}, +)$ et (U_n, \times)

sont isomorphes

donc (U_n, \times) est un groupe
cyclique d'ordre n

$\exists y \in \mathbb{Q}$ si et seulement si $U_m \subseteq U_n$
 $\Leftrightarrow m \mid n$

(2) Si $m \mid n$, $\exists l \in \mathbb{N}^*$
 tq $n = lm \Leftrightarrow \frac{l}{m} = \frac{n}{n}$

$$\text{alors } U_m = \left\{ e^{\frac{2ik\pi}{n}} \mid k = 0, \dots, m-1 \right\}$$

$$= \left\{ e^{\frac{2ik\pi + l\pi}{n}} \mid k = 0, \dots, m-1 \right\}$$

$$\subset \left\{ e^{\frac{2ik'\pi}{n}} \mid k' = 0, \dots, n-1 \right\}$$

||
 U_n

$$\Rightarrow U_m \subset U_n$$

$\Rightarrow (U_m, \times)$ est un sous groupe de (U_n, \times)

$$\text{dans } m = |U_m| \quad |U_m| = n$$

Méthode alternativel

Si $U_m \subsetneq U_n$
 alors $e^{\frac{2i\pi}{m}} \in U_n$
 donc $\left(e^{\frac{2i\pi}{m}}\right)^n = e^{2i\pi \left(\frac{n}{m}\right)}$

||
 1

$$\text{dans } \frac{n}{m} \in \mathbb{Z}$$

$$\text{dans } m \mid n$$

Ex 8:

a) Calculer l'ordre de chaque élément de $(\mathbb{Z}/12\mathbb{Z}, +)$

b) $(\mathbb{Z}/12\mathbb{Z})^*, \times$

$x \in (G, \times)$ l'ordre de x

$$\begin{aligned} \text{ord}(x) &= \text{ord } \langle x \rangle \\ &= |\langle x \rangle| \end{aligned}$$

$$= \{e, x, x+x, x+x+\dots+x, x^{-1}\}$$

$$\underbrace{x^{-1} * \dots * x^{-1}}_{k \text{ fois}}, \dots \quad \left. \right\} \quad \underbrace{\dots}_{k \text{ fois}}$$

tel que $\underbrace{x * \dots * x}_n = e_G$

élément	ordre
$\bar{0}$	1
$\bar{1}$	12
$\bar{2}$	6
$\bar{3}$	4
$\bar{4}$	3
$\bar{5}$	12
$\bar{6}$	2
$\bar{7}$	12

$$\begin{aligned} 0 \text{ et } \bar{0} \\ \underbrace{\bar{0} * \dots * \bar{0}}_{1 \text{ fois}} = \bar{0} \leftarrow \text{tautologie} \\ \bar{12}^{12} = 0 \end{aligned}$$

$$\bar{0}^{12} : 0 \bmod 12$$

$$\begin{aligned} \bar{0} + \bar{0} \\ \text{et } \bar{0} \end{aligned}$$

$$\bar{0} + \bar{0} = 0$$

$\bar{8}$	3
$\bar{9}$	4
$\bar{10}$	6
$\bar{11}$	9

$$\bar{8} + \bar{8} = \bar{16} = \bar{4} \neq \bar{0}$$

$$3 \times \bar{8} = \bar{24} = \bar{0}$$

$$\text{ord}(\bar{8}) = 3$$

$$2 \times \bar{9} = \bar{18} = \bar{6} \neq \bar{0}$$

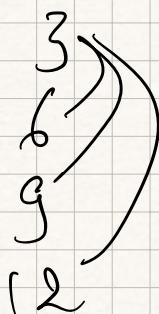
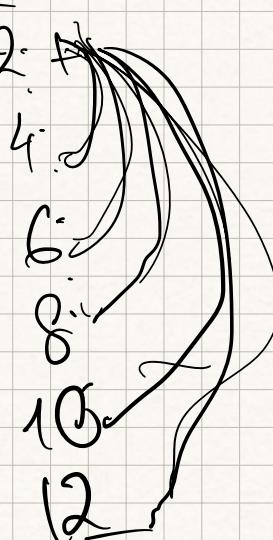
$$3 \times \bar{9} = \bar{27} = \bar{3} \neq \bar{0}$$

$$\text{ord}(\bar{9}) = 4$$

$$\begin{array}{c} \bar{10}, \bar{20}, \dots, \bar{50} \\ \neq \bar{0} \end{array}$$

dans

$$\begin{aligned} \frac{1}{2} + \frac{1}{1} &= \frac{1+1}{2+1} = \frac{2}{3} \\ \frac{2}{2+1} &= \frac{2}{3} \end{aligned}$$



$$6 \times \bar{10} = \bar{0}$$

$$\text{dans } \text{ord}(\bar{10}) = 6$$

$$\text{ord}(\bar{k}) \times \bar{k} = \bar{0}$$

$$\Rightarrow \text{ord}(\bar{k}) \times k = l_n$$

dans l_n divisible par k et par n

dans $\text{ppcm}(k, n) \mid \text{ord}(\bar{k}) \times k$

dans l'autre sens, comme $\text{ord}(\bar{k})$ est le plus petit entier tel que $\text{ord}(\bar{k}) \times k$ multiple de n

$$\text{ord}(\bar{k}) \times k = \text{ppcm}(k, n)$$

by $((\mathbb{Z}/12\mathbb{Z})^*, \times)$

élément

ordre

$\bar{0}$	
$\bar{1}$	
$\bar{2}$	
$\bar{3}$	
$\bar{4}$	
$\bar{5}$	
$\bar{6}$	
$\bar{7}$	
$\bar{8}$	
$\bar{9}$	
$\bar{10}$	
$\bar{11}$	

• : multiplication

* : élément inversible

avec 12 : nbr

premier avec 12

nbr inversible

dans

$\mathbb{Z}/12\mathbb{Z}$

$$(\bar{5})^2 = \bar{5^2} = \bar{25} = \bar{1}$$

$$(\bar{7})^2 = \bar{49} = \bar{1}$$

$$(\bar{11})^2 = \bar{121} = \bar{1}$$

des éléments de $((\mathbb{Z}/12\mathbb{Z})^*, \times)$ sont $\{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

$\bar{1}$ neutre car $\forall k \in \mathbb{Z}$

$$\bar{k} \times \bar{1} = \bar{k}$$

$\phi(n)$

• $\phi(p) = p-1$ si p premier

• $\phi(mn) = \phi(m)\phi(n)$

Si m et n premiers entre eux

$$|((\mathbb{Z}/12\mathbb{Z})^*)| = \phi(12) = \phi(4 \times 3) \\ = \phi(4) \times \phi(3)$$

$$\phi(4) = \phi(2^2) = 2^2 - 2^{2-1} = 2^2 - 2^1 = 2$$

$$\phi(3) = \phi(3^1) = 3^1 - 3^{1-1} = 3 - 1 = 2$$

$$\phi(12) = 2 \times 2 = 4$$

dans $\mathbb{Z}/4\mathbb{Z}$: $\overline{0}, \overline{1}, \overline{2}, \overline{3}$

\uparrow \uparrow
 inversible

$\phi(p) = p-1$

$3-1$
 $= 2$

dans $\phi(4) = 2$, $\phi(12) = 4$

dans $\text{ord}(k, n) = \frac{\text{ppcm}(k, n)}{k}$

$$= \frac{n}{\text{pgcd}(k, n)}$$

$$\phi(p^n) = (p-1)p^{n-1}$$

Ex 12

$$M_2(\mathbb{Z}), \quad SL_2(\mathbb{Z}) \subset M_2(\mathbb{Z})$$

$$\begin{matrix} \det \\ \downarrow \\ \mathbb{Z} \end{matrix} \quad \begin{matrix} \text{matrice de} \\ \text{determinant} \\ = 1 \end{matrix}$$

$Mg(SL_2(\mathbb{Z}), \circ)$ est un groupe
↑ produit matrice usuel

On vérifie, si $M, N \in SL_2(\mathbb{Z})$, ($\det(M) = \det(N) = 1$)
alors $\det(M \cdot N) = \det(M) \times \det(N) = 1$
donc $M \cdot N \in SL_2(\mathbb{Z})$

donc $\circ : SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z})$
bien défini

◦ neutre : $Id \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$

$\forall M \in SL_2(\mathbb{Z})$

$M \cdot Id = Id \cdot M = M$

◦ Si $M \in SL_2(\mathbb{Z})$, alors $\det(M) = 1 \neq 0$

donc $\exists M^{-1}$ matrice à coefficients variables
tq $M \cdot M^{-1} = M^{-1} \cdot M = id$

On peut exprimer les coef de M^{-1} comme des
fracțion de dénominateur $\det(M) = 1$ donc M^{-1} à coef entiers
 $N_1, M_2, M_3 \in SL_2(\mathbb{Z})$

$$(M_1 \cdot M_2) \cdot M_3 = M_1 (M_2 + M_3)$$

car la multiplication matricielle est associative
en général

donc $SL_2(\mathbb{Z})$ est un groupe

$$M_{1k} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \quad k \in \mathbb{Z}$$

$\forall k \neq k'$, $M_{1k} \neq M'_{1k'}$,
et $\forall k \in \mathbb{Z}$ $\det(M_{1k}) = 1$ donc $M_{1k} \in SL_2(\mathbb{Z})$

$SL_2(\mathbb{Z})$ contient un sous-ensemble infini
 $\{M_{1k} \mid k \in \mathbb{Z}\}$ dont est d'ordre ∞

$$M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad N = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$$

$$\det(M) = \det(N) = 1$$

On calcule

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = MN$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix} = NM$$

$$MN \neq NM$$

dans $(SL_2(\mathbb{Z}), \circ)$ pas abélien

Ex

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

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

$$A^4 = \text{Id}$$

↑ A est d'ordre 4

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

$$B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ordre $B = 3$

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

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

ordre de $AB = \infty$

$$M_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \quad k \in \mathbb{Z}$$

Si on avait $AB = BA$, $(AB)^n$ serait égal à $A^n B^n$ et pour $n = 12$ on aurait

$$\begin{aligned}
 (AB)^{12} &= A^{4 \times 3} B^{3 \times 4} \\
 &= (A^4)^3 (B^3)^4 \\
 &\equiv \text{Id}
 \end{aligned}$$

Feuille 3

Exercice 8

Trouver tous les ordres des éléments des groupes $(\mathbb{Z}/12\mathbb{Z}, +)$ et $((\mathbb{Z}/12\mathbb{Z})^*, \times)$.

Les éléments du groupe $(\mathbb{Z}/12\mathbb{Z}, +)$, sont :

- $\bar{0}$, c'est l'élément neutre de $(\mathbb{Z}/12\mathbb{Z}, +)$, on a donc $\bar{0}$ est d'ordre 1,
- $\bar{1}$. Pour $n \in \mathbb{Z}$, on a $n(\bar{1}) = \bar{n}$, donc $n(\bar{1}) \neq \bar{0}$, si $1 \leq n < 12$, et $12\bar{1} = \bar{0}$, on en déduit que $\bar{1}$ est d'ordre 12.
- $\bar{2}$ vérifie $n \times \bar{2} = \overline{2 \times n}$, d'où $n \times \bar{2} \neq \bar{0}$, pour $1 \leq n < 6$, et $6 \times \bar{2} = \bar{12} = \bar{0}$.
- De même, $\bar{3}$ est d'ordre 4 (car $4 \times \bar{3} = \bar{12} = \bar{0}$)
- De même, $\bar{4}$ est d'ordre 3.
- on calcule, $2 \times \bar{5} = \bar{10} = \bar{2}$, $3 \times \bar{5} = \bar{15} = \bar{3}$, $4 \times \bar{5} = \bar{20} = \bar{8}$, $5 \times \bar{5} = \bar{25} = \bar{1}$, $6 \times \bar{5} = \bar{30} = \bar{6}$, $7 \times \bar{5} = \bar{35} = \bar{1}$, $8 \times \bar{5} = \bar{40} = \bar{4}$, $9 \times \bar{5} = \bar{45} = \bar{9}$, $10 \times \bar{5} = \bar{50} = \bar{2}$, $11 \times \bar{5} = \bar{55} = \bar{7}$, et $12 \times \bar{5} = \bar{60} = \bar{0}$. Donc, $\bar{5}$ est d'ordre 12. Pour s'épargner les calculs, on aurait pu citer le cours, et observer que 5 et 12 sont premiers entre eux, et donc que 5 est d'ordre 12 dans $(\mathbb{Z}/12\mathbb{Z}, +)$.
- on a $2 \times \bar{6} = \bar{12} = \bar{0}$, et $\bar{6} \neq \bar{0}$, donc $\bar{6}$ est d'ordre 2 dans $(\mathbb{Z}/12\mathbb{Z}, +)$.
- 7 est premier avec 12, donc $\bar{7}$ est d'ordre 12 dans $(\mathbb{Z}/12\mathbb{Z}, +)$.
- on a $2 \times \bar{8} = \bar{16} = \bar{4}$ et $3 \times \bar{8} = \bar{24} = \bar{0}$, donc $\bar{8}$ est d'ordre 3 dans $(\mathbb{Z}/12\mathbb{Z}, +)$.
- $2 \times \bar{9} = \bar{18} = \bar{6}$, $3 \times \bar{9} = \bar{27} = \bar{3}$, $4 \times \bar{9} = \bar{36} = \bar{0}$, donc $\bar{9}$ est d'ordre 4 dans $(\mathbb{Z}/12\mathbb{Z}, +)$.
- On vérifie que $6 \times \bar{10} = \bar{0}$, et que $n \times \bar{10} \neq \bar{0}$ pour $1 \leq n < 5$, et on en déduit que $\bar{10}$ est d'ordre 6 dans $(\mathbb{Z}/12\mathbb{Z}, +)$.

- 11 et 12 sont premiers entre eux, donc $\bar{11}$ est d'ordre 12 dans $(\mathbb{Z}/12\mathbb{Z}, +)$.

On aurait aussi pu utiliser la formule générale : pour $a \neq 0$, l'ordre de \bar{a} dans $(\mathbb{Z}/n\mathbb{Z}, +)$ est $\frac{n}{\text{pgcd}(a, n)}$. (C'est un bon exercice que de montrer cette formule).

On s'intéresse maintenant aux éléments de $((\mathbb{Z}/12\mathbb{Z})^*, \times)$. Ceux-ci sont exactement les classes \bar{a} , des entiers $a \in \mathbb{Z}$ vérifiant $\text{pgcd}(a, 12) = 1$. Autrement dit, les éléments de $((\mathbb{Z}/12\mathbb{Z})^*, \times)$ sont $\bar{1}, \bar{5}, \bar{7}, \bar{11}$, on calcule leurs ordres :

- $\bar{1}$ est l'élément neutre de $((\mathbb{Z}/12\mathbb{Z})^*, \times)$, il est donc d'ordre 1 dans $((\mathbb{Z}/12\mathbb{Z})^*, \times)$.
- $\bar{5}^2 = \bar{25} = \bar{1}$, donc $\bar{5}$ est d'ordre 2 dans $((\mathbb{Z}/12\mathbb{Z})^*, \times)$.
- $\bar{7}^2 = \bar{49} = \bar{1}$, donc $\bar{7}$ est d'ordre 2 dans $((\mathbb{Z}/12\mathbb{Z})^*, \times)$.
- $\bar{11}^2 = \bar{121} = \bar{1}$, donc $\bar{11}$ est d'ordre 2 dans $((\mathbb{Z}/12\mathbb{Z})^*, \times)$.

Exercice 12

On note $\mathcal{M}_2(\mathbb{Z})$ et $\text{SL}_2(\mathbb{Z})$ respectivement l'ensemble des matrices 2×2 à coefficients entiers et l'ensemble de celles qui sont de déterminant 1.

1. Montrer que $\text{SL}_2(\mathbb{Z})$ est un groupe multiplicatif d'ordre infini. Est-il commutatif ?

2. Soient

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

Déterminer l'ordre de A , B , et AB

1. Montrons que $\text{SL}_2(\mathbb{Z})$ est un groupe pour la multiplication de matrices. Si $M, N \in \text{SL}_2(\mathbb{Z})$ sont deux matrices de déterminant 1 leur produit $M \cdot N$, vérifie

$$\det(M \cdot N) = \det(M) \det(N) = 1$$

En particulier, le produit matriciel est bien défini sur $\text{SL}_2(\mathbb{Z})$, i.e. on a une loi

$$\text{SL}_2(\mathbb{Z}) \times \text{SL}_2(\mathbb{Z}) \xrightarrow{\cdot} \text{SL}_2(\mathbb{Z})$$

Vérifions que $(\text{SL}_2(\mathbb{Z}), \cdot)$ vérifie les axiomes d'un groupe.

- La matrice $\text{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est dans $\text{SL}_2(\mathbb{Z})$ et est un élément neutre pour la multiplication de matrices, i.e. pour tout $M \in \text{SL}_2(\mathbb{Z})$, $M \cdot \text{Id} = \text{Id} \cdot M = M$
- Si $M \in \text{SL}_2(\mathbb{Z})$, alors $\det(M) = 1 \neq 0$, donc il existe une matrice inverse M^{-1} telle que $M \cdot M^{-1} = M^{-1} \cdot M = \text{Id}$. De plus, Les coefficients de M^{-1} peuvent s'écrire comme des fractions de dénominateurs $\det(M) = 1$, donc sont à coefficients dans \mathbb{Z} . Finalement, on a $\det(M^{-1}) = \frac{1}{\det(M)} = 1$, d'où $M^{-1} \in \text{SL}_2(\mathbb{Z})$, et M admet un inverse dans $\text{SL}_2(\mathbb{Z})$.

- Si M_1, M_2, M_3 sont trois éléments de $\mathrm{SL}_2(\mathbb{Z})$, alors l'associativité du produit matriciel (on la suppose connue) donne immédiatement

$$(M_1 \cdot M_2) \cdot M_3 = M_1 \cdot (M_2 \cdot M_3)$$

Et donc, le produit matriciel est associatif aussi lorsqu'on le restreint à $\mathrm{SL}_2(\mathbb{Z})$.

On en déduit que $(\mathrm{SL}_2(\mathbb{Z}), \cdot)$ est un groupe. A partir de maintenant, on notera simplement MN pour désigner le produit $M \cdot N$. Pour voir que $\mathrm{SL}_2(\mathbb{Z})$ est d'ordre infini, il suffit de trouver une infinité d'éléments distincts de $\mathrm{SL}_2(\mathbb{Z})$. Par exemple, pour $k \in \mathbb{Z}$ un entier relatif quelconque, on peut considérer la matrice

$$M_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

Alors, $\det(M_k) = 1$ quelque soit k , et si $k \neq k'$, $M_k \neq M_{k'}$. On en déduit que $\mathrm{SL}_2(\mathbb{Z})$ contient une infinité d'éléments distincts, c'est donc un groupe d'ordre infini.

Montrons que le groupe $(\mathrm{SL}_2(\mathbb{Z}), \cdot)$ n'est pas commutatif. On pose

$$M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \text{ et } N = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

On a $\det(M) = \det(N) = 1$, et donc $M, N \in \mathrm{SL}_2(\mathbb{Z})$. On calcule

$$MN = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = NM$$

On en déduit que le groupe $(\mathrm{SL}_2(\mathbb{Z}), \cdot)$ n'est pas commutatif.

2.

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

On calcule :

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, A^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, A^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

On en déduit que A est d'ordre 4. On calcule :

$$B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

On en déduit que B est d'ordre 3. On calcule

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, (AB)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, (AB)^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \therefore$$

On va montrer par récurrence que pour $n \geq 1$, $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. On a déjà montré la formule pour $n = 1$ en calculant AB . Soit $n \geq 1$, supposons que $(AB)^n = (AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ on calcule

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

On en déduit la formule pour $(AB)^n$. En particulier, pour tout $n \geq 1$, $(AB)^n \neq \text{Id}$. On en déduit que AB est d'ordre infini.

