1.6 Correction de quelques exercices

Exercice 1 :

Soit G un groupe dont l'opération est notée multiplicativement et $S \subset G$ une partie non vide de G. Démontrer que :

$$\langle S\rangle = \left\{ y \in G \text{ où } y = \prod_{i=0}^{n} x_i \text{ avec } (\forall n \in \mathbb{N}) \left((x_n \in S) \text{ ou } \left(x_n^{-1} \in S\right)\right)\right\}$$

Nous faisons cette démonstration en 2 temps.
Appelons $\Gamma(S) = \left\{ y \in G \text{ où } y = \prod_{i=0}^{n} x_i \text{ avec } (\forall n \in \mathbb{N}) \left((x_n \in S) \text{ ou } \left(x_n^{-1} \in S\right)\right)\right\}$. Il est aussi tout à fait possible d'écrire $\Gamma(S) = \{y \in G \text{ où } y = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \text{ avec } x_i \in S \text{ et } \varepsilon_i \in \{-1;+1\}\}$.
Nous allons montrer que $\Gamma(S) = \langle S\rangle$

— Montrons que $\Gamma(S) \subset \langle S\rangle$
Soit $y \in \Gamma(S)$. Alors :

$$y = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \text{ avec } x_i \in S \text{ et } \varepsilon_i \in \{-1;+1\}$$

Nous savons que $\langle S\rangle$ est le plus petit sous-groupe de G tel que $S \subset \langle S\rangle$.
Ainsi, comme, pour tout $i \in \{1,\ldots,n\}$, $x_i \in S$, alors $x_i \in \langle S\rangle$ et $x_n^{\varepsilon_n} \in \langle S\rangle$. La multiplication étant interne dans $\langle S\rangle$, nous avons $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \in \langle S\rangle$, c'est à dire $y \in \langle S\rangle$, et donc $\Gamma(S) \subset \langle S\rangle$

— Montrons que $\Gamma(S)$ est un sous-groupe de G
⋆ S étant non vide, soit $x \in S$. Alors $e = x \times x^{-1} \in \Gamma(S)$, et donc $\Gamma(S) \neq \emptyset$
⋆ Soient $y \in \Gamma(S)$ et $y' \in \Gamma(S)$, alors $y = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ et $y_1 = x_{1,1}^{\varepsilon_{1,1}} \cdots x_{1,m}^{\varepsilon_{1,m}}$ et

$$y'y^{-1} = \left(x_{1,1}^{\varepsilon_{1,1}} \cdots x_{1,m}^{\varepsilon_{1,m}}\right)\left(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}\right)^{-1} = \left(x_{1,1}^{\varepsilon_{1,1}} \cdots x_{1,m}^{\varepsilon_{1,m}}\right)\left(x_n^{-\varepsilon_n} \cdots x_1^{-\varepsilon_1}\right) = x_{1,1}^{\varepsilon_{1,1}} \cdots x_{1,m}^{\varepsilon_{1,m}} x_n^{\varepsilon"_n} \cdots x_1^{\varepsilon"_1}$$

où, pour tout i, $\varepsilon"_i = -\varepsilon_i \in \{-1;+1\}$ et $\varepsilon_{1,i} \in \{-1;+1\}$
Et donc $y'y^{-1} \in \Gamma(S)$

Nous en déduisons donc que $\Gamma(S)$ est un sous groupe de G, contenant S, et donc $\langle S\rangle \subset \Gamma(S)$

Ainsi, $\langle S\rangle = \Gamma(S)$

Exercice 5 :

Montrer que si $(G,\star)$ est un groupe et E un ensemble quelconque non vide, alors l'ensemble G^E des applications de E dans G muni de la loi $\perp$ définie par :

$$\left(\forall f \in G^E\right)\left(\forall g \in G^E\right)\left((f \perp g)(x) = f(x) \star g(x)\right)$$

est un groupe et que ce groupe est commutatif si $(G,\star)$ l'est.

Voilà un exercice intéressant !!

→ Il est clair que l'opération $\perp$ est une opération interne puisque si $f \in G^E$ et $g \in G^E$ alors $f \perp g \in G^E$

→ Etudions l'associativité. Soient $f \in G^E$, $g \in G^E$ et $h \in G^E$, alors, pour tout $x \in E$:

$$\begin{aligned}((f \perp g) \perp h)(x) = & \ (f \perp g)(x) \star h(x) \\ = & \ (f(x) \star g(x)) \star h(x) \\ = & \ (f(x) \star g(x)) \star h(x) \\ = & \ f(x) \star (g(x) \star h(x)) \text{ (associativité de la loi } \star) \\ = & \ f(x) \star ((g \perp h)(x)) \\ = & \ (f \perp (g \perp h))(x)\end{aligned}$$

Ainsi, pour tout $x \in E$, nous avons $((f \perp g) \perp h)(x) = (f \perp (g \perp h))(x)$ et donc

$$(f \perp g) \perp h = f \perp (g \perp h)$$

La loi $\perp$ est donc associative.

→ Soit $I : E \longrightarrow G$ telle que pour tout $x \in E$, $I(x) = e$ où e est l'élément neutre de $(G, \star)$. I est l'application constante qui à tout $x \in E$ fait correspondre l'élément neutre e de $(G, \star)$
Alors, nous avons $f \perp I = I \perp f = f$ et I est le neutre pour l'opération $\perp$ dans G^E.
En effet, pour tout $x \in E$:

$$(f \perp I)(x) = f(x) \star I(x) = f(x) \star e = f(x) = e \star f(x) = I(x) \star f(x) = (I \perp f)(x)$$

Donc I est le neutre pour la loi $\perp$

→ Soit $f \in G^E$; existe-t-il $g \in G^E$ tel que $f \perp g = g \perp f = I$.
Si nous posons, pour tout $x \in E$, $g(x) = [f(x)]^{-1}$. $g(x)$ est donc l'inverse de l'élément $f(x)$ pour la loi $\star$ dans G. Nous allons démontrer que g est le symétrique de f pour la loi $\perp$ dans G^E.
Pour tout $x \in E$, nous avons :

$$(f \perp g)(x) = f(x) \star g(x) = f(x) \star [f(x)]^{-1} = e = I(x)$$

Nous avons donc $f \perp g = I$. Nous démontrerions de la même manière que $g \perp f = I$.
g est donc le symétrique de f pour la loi $\perp$ dans G^E.

Nous venons de montrer que $\left(G^E, \perp\right)$ est un groupe.

Supposons $(G, \star)$ commutatif

Alors, très simplement, pour tout $f \in G^E$, tout $g \in G^E$ et tout $x \in E$, nous avons :

$$(f \perp g)(x) = \underbrace{f(x) \star g(x) = g(x) \star f(x)}_{\text{Commutativité}} = (g \perp f)(x)$$

Ainsi, si $(G, \star)$ est commutatif, alors, pour tout $f \in G^E$, tout $g \in G^E$, nous avons $f \perp g = g \perp f$ et ainsi $\left(G^E, \perp\right)$ est un groupe commutatif

Exercice 6 :

On considère l'ensemble $G =]-1, +1[$ muni de la loi $\star$ définie par :

$$x \star y = \frac{x+y}{1+xy}$$

Démontrer que $(G, \star)$ est un groupe commutatif.

⇒ **Dans un premier temps, avons nous, pour tout $x \in]-1, +1[$ et tout $y \in]-1, +1[$, $1 + xy \neq 0$?**
Soient donc $x \in]-1, +1[$ et $y \in]-1, +1[$, alors $|x| < 1$ et $|y| < 1$, et donc $|xy| = |x|\,|y| < 1$, c'est à dire $-1 < xy < +1$ et donc $1 + xy > 0$, ce qui montre que $\dfrac{x+y}{1+xy}$ est défini lorsque $x \in]-1, +1[$ et $y \in]-1, +1[$

⇒ **Démontrons que pour tout $x \in]-1, +1[$ et tout $y \in]-1, +1[$, nous avons $x \star y = \dfrac{x+y}{1+xy} \in]-1, +1[$**
C'est à dire que nous allons démontrer que la loi $\star$ est interne. Nous avons :

$$\frac{x+y}{1+xy} \in]-1, +1[\iff \left|\frac{x+y}{1+xy}\right| < 1 \iff \left|\frac{x+y}{1+xy}\right|^2 < 1$$

Or, $\left|\dfrac{x+y}{1+xy}\right|^2 = \dfrac{|x+y|^2}{|1+xy|^2} = \dfrac{(x+y)^2}{(1+xy)^2}$.

Donc montrer que $\left|\dfrac{x+y}{1+xy}\right| < 1$, c'est montrer que $\dfrac{(x+y)^2}{(1+xy)^2} < 1 \iff (x+y)^2 < (1+xy)^2$.

Or,

$$(x+y)^2 - (1+xy)^2 = x^2 + y^2 + 2xy - 1 - x^2y^2 - 2xy = x^2 + y^2 - 1 - x^2y^2 = x^2\left(1 - y^2\right) + y^2 - 1 = \left(y^2 - 1\right)\left(1 - x^2\right)$$

Comme $|x| < 1$ et $|y| < 1$, nous avons $x^2 < 1$ et $y^2 < 1$ et donc $\left(y^2 - 1\right)\left(1 - x^2\right) < 0$ dont nous déduisons que $(x+y)^2 < (1+xy)^2$.

En conclusion, pour tout $x \in]-1,+1[$ et tout $y \in]-1,+1[$, nous avons $x \star y = \dfrac{x+y}{1+xy} \in]-1,+1[$ et la loi $\star$ est donc interne.

$\Rightarrow$ **La loi $\star$ est commutative**
Evidemment, cette commutativité provient de celles de la multiplication et de l'addition.

$\Rightarrow$ **La loi $\star$ est associative**
Soient $x \in]-1,+1[$, $y \in]-1,+1[$ et $z \in]-1,+1[$, il faut montrer que $x \star (y \star z) = (x \star y) \star z$.
Faisons les calculs :

$\triangleright$

$$\begin{aligned} x \star (y \star z) = &\ x \star \left(\frac{z+y}{1+zy}\right) \\ = &\ \frac{x + \frac{z+y}{1+zy}}{1 + x\frac{z+y}{1+zy}} \\ = &\ \frac{x+y+z+xyz}{1+xy+yz+xz} \end{aligned}$$

$\triangleright$

$$\begin{aligned} (x \star y) \star z = &\ \left(\frac{x+y}{1+xy}\right) \star z \\ = &\ \frac{\frac{x+y}{1+xy} + z}{1 + z\frac{x+y}{1+xy}} \\ = &\ \frac{x+y+z+xyz}{1+xy+yz+xz} \end{aligned}$$

Nous avons bien $x \star (y \star z) = (x \star y) \star z$ et la loi $\star$ est associative.

$\Rightarrow$ **Existence d'un élément neutre**
Si la loi $\star$ admet un neutre $e \in]-1,+1[$, nous avons, pour tout $x \in]-1,+1[$, $x \star e = e \star x = x$

$\triangleright$ Il est clair que nous avons $x \star 0 = 0 \star x = x$

$\triangleright$ Réciproquement, si e est l'élément neutre, nous avons :

$$\frac{x+e}{1+xe} = x \Longleftrightarrow x + e = x + ex^2 \Longleftrightarrow ex^2 - e = 0 \Longleftrightarrow e\left(x^2-1\right) = 0$$

Comme $x \neq \pm 1$, $x^2 - 1 \neq 0$ et donc $e = 0$

$\Rightarrow$ **Tout $x \in]-1,+1[$ admet-il un symétrique pour la loi $\star$?**
Soit $x \in]-1,+1[$. S'il existe un symétrique $y \in]-1,+1[$ de x pour la loi $\star$, ce symétrique vérifie $x \star y = 0$. Nous avons alors :

$$\frac{x+y}{1+xy} = 0 \Longleftrightarrow y = -x$$

Ainsi, tout $x \in]-1,+1[$ admet un symétrique pour la loi $\star$ qui est $y = -x$

Nous venons de montrer que $(G,\star)$ est un groupe commutatif.

Exercice 7 :

Soit G un groupe dont l'opération est notée multiplicativement d'élément neutre 1.

1. *Montrer que G est commutatif si, et seulement si, pour tout $a \in G$ et tout $b \in G$, nous avons $(ab)^2 = a^2b^2$*

   $\Rightarrow$ **Supposons G commutatif**
   Alors, nous avons :

   $$(ab)^2 = (ab) \times (ab) = a\,(ba)\,b = a\,(ab)\,b = (aa)\,(bb) = a^2b^2$$

   $\Rightarrow$ **Supposons que $(ab)^2 = a^2b^2$**
   Montrons que G est un groupe commutatif. Soient $x \in G$ et $y \in G$; alors :

   $$(xy)^2 = (xy)\,(xy) = x^2y^2 = (xx)\,(yy)$$

   C'est à dire $xyxy = xxyy$

Comme tout élément d'un groupe est régulier, nous avons les implications :

$$xyxy = xxyy \Longrightarrow yxy = xyy \Longrightarrow yx = xy$$

Nous venons de montrer la commutativité de G

2. *Montrer que G est commutatif si, et seulement si, pour tout $a \in G$ et tout $b \in G$, nous avons $(ab)^{-1} = a^{-1}b^{-1}$*

   Tout d'abord, il faut remarquer que nous avons toujours, dans tout groupe *(commutatif ou non)*, pour tout $a \in G$ et tout $b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$

   $\Rightarrow$ **Supposons G commutatif**
   Alors nous avons $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$
   Ce que nous voulions.

   $\Rightarrow$ **Supposons maintenant que pour tout $a \in G$ et tout $b \in G$, nous avons $(ab)^{-1} = a^{-1}b^{-1}$**
   Montrons que G est commutatif. Soient $x \in G$ et $y \in G$, alors :

$$(xy)(xy)^{-1} = 1 \Longleftrightarrow (xy)\left(y^{-1}x^{-1}\right) = 1 \Longleftrightarrow (xy)\left(x^{-1}y^{-1}\right) = 1$$

   Multiplions à droite par y. Alors :

$$(xy)\left(x^{-1}y^{-1}\right) = 1 \Longleftrightarrow (xy)\,x^{-1} = y$$

   Multiplions toujours à droite par x, cette fois-ci. Alors :

$$(xy)\,x^{-1} = y \Longleftrightarrow xy = yx$$

   Le groupe G est donc bien commutatif

Exercice 8 :

Montrer que l'ensemble $\mathrm{SL}_n(R)$ des matrices carrées réelles d'ordre n de déterminant égal à 1 est un sous-groupe de $\mathrm{GL}_n(R)$.

Bien entendu, nous avons $\mathrm{SL}_n(R) \subset \mathrm{GL}_n(R)$; nous allons montrer que $\mathrm{SL}_n(R)$ est un sous-groupe de $\mathrm{GL}_n(R)$

- ▷ Tout d'abord $\mathrm{SL}_n(R) \neq \emptyset$ puisque la matrice identité I_n qui a pour déterminant 1 et est donc dans $\mathrm{SL}_n(R)$
- ▷ Soient, maintenant $A \in \mathrm{SL}_n(R)$ et $B \in \mathrm{SL}_n(R)$.
  Alors B est inversible et $\det B^{-1} = \det B = 1$ et donc :

$$\det\left(AB^{-1}\right) = \det A \times \det B^{-1} = 1$$

  Donc $\left(AB^{-1}\right) \in \mathrm{SL}_n(R)$

Donc, $\mathrm{SL}_n(R)$ est un sous-groupe de $\mathrm{GL}_n(R)$.

Exercice 9 :

Montrer que l'ensemble G des matrices réelles de $\mathcal{M}_2(\mathbb{R})$ de la forme $M_{(a,b)} = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ avec $a^2 \neq b^2$ est un groupe multiplicatif. Est-il commutatif ?

Ré-écrivons G :

$$G = \left\{M_{(a,b)} \in \mathcal{M}_2(\mathbb{R}) \text{ telles que } M_{(a,b)} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \text{ où } a^2 - b^2 \neq 0\right\}$$

$\Rightarrow$ Tout d'abord, $G \neq \emptyset$ puisque $\mathrm{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$

$\Rightarrow$ Puis, remarquons que toute matrice $M_{(a,b)} \in G$ est inversible puisque $\det M_{(a,b)} = a^2 - b^2 \neq 0$. Il nous est même possible de calculer $\left(M_{(a,b)}\right)^{-1}$:

$$\left(M_{(a,b)}\right)^{-1} = \frac{1}{a^2-b^2}\begin{pmatrix} a & -b \\ -b & a \end{pmatrix} = M_{\left(\frac{a}{a^2-b^2}, \frac{-b}{a^2-b^2}\right)}$$

Et donc $\left(M_{(a,b)}\right)^{-1} \in G$

$\Rightarrow$ Ensuite, toute matrice $M_{(a,b)} \in G$ peut s'écrire :

$$M_{(a,b)} = a\mathrm{I}_2 + bJ \text{ où } J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

En remarquant que $J^2 = -\mathrm{I}_2$, nous avons, pour 2 matrices $M_{(a,b)} \in G$ et $M_{(c,d)} \in G$:

$$\begin{array}{rl} M_{(a,b)} \times M_{(c,d)} = & (a\mathrm{I}_2 + bJ) \times (c\mathrm{I}_2 + dJ) \\ = & ac\mathrm{I}_2 + adJ + bcJ - bd\mathrm{I}_2 \\ = & (ac-bd)\,\mathrm{I}_2 + (ad+bc)\,J \\ = & M_{(ac-bd, bc+ad)} \end{array}$$

Ce qui montre que l'opération de multiplication des matrices est interne dans G et commutative.

$\Rightarrow$ Ainsi, G muni de la multiplication des matrices est un groupe commutatif

Exercice 10 :

Soit H une partie finie non vide d'un groupe $(G, \star)$. Montrer que H est un sous-groupe de $(G, \star)$ si, et seulement si, il est stable pour la loi $\star$

$\Rightarrow$ **Si H est un sous-groupe de** $(G, \star)$ il est alors évident qu'il est stable pour la loi $\star$

$\Rightarrow$ **Supposons que H sous-ensemble fini de $(G, \star)$ soit stable pour la loi $\star$**

La démonstration se fera en plusieurs temps.

$\rightarrow$ H étant non vide, soit $a \in H$. Nous connaissons bien l'application δ_a définie par :

$$\begin{cases} \delta_a : H & \longrightarrow & G \\ \quad\quad x & \longmapsto & \delta_a(x) = x \star a \end{cases}$$

Nous savons, comme H est stable pour la loi $\star$ que, pour tout $x \in H$, $\delta_a(x) \in H$ et donc $\delta_a(H) \subset H$

D'autre part, nous avons démontré que les applications du type δ_a sont injectives.

Donc $\delta_a : H \longrightarrow H$ est injective et comme H est de cardinal fini, l'application δ_a est bijective et donc, en fait, $\delta_a(H) = H$

$\rightarrow$ Comme δ_a est bijective, il existe $u \in H$ tel que $\delta_a(u) = u \star a = a$. Cet élément $u \in H$ n'est autre que l'élément neutre e du groupe $(G, \star)$.

Nous venons donc de montrer que le neutre de $(G, \star)$ est dans H

$\rightarrow$ Comme $e \in H$, et que δ_a est bijective, il existe $u \in H$ tel que $\delta_a(u) = u \star a = e$. Cet élément $u \in H$ n'est autre que l'élément symétrique a^{-1} de a dans $(G, \star)$.

Nous venons donc de montrer que si $a_i n H$, alors $a^{-1} \in H$

En conclusion, $(H, \star)$ est bien un sous-groupe de$(G, \star)$

Exercice 11 :

Soit G un groupe dont l'opération est notée multiplicativement. Soient H et K deux sous-groupes de G. On définit les sous-ensembles HK et KH de G par :

$$HK = \{hk \text{ où } h \in H \text{ et } k \in K\} \text{ et } KH = \{kh \text{ où } h \in H \text{ et } k \in K\}$$

Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$

$\Rightarrow$ **Supposons que HK soit un sous-groupe de G**

Nous allons montrer que $HK = KH$

→ Démontrons que $HK \subset KH$
Soit $g \in HK$.
HK étant un sous-groupe, $g^{-1} \in HK$; il existe alors $h \in H$ et $k \in K$ tels que $g^{-1} = hk$ et donc $g = k^{-1}h^{-1}$.
K et H étant 2 sous-groupes $k^{-1} \in K$ et $h^{-1} \in H$ et donc $g \in KH$. D'où nous pouvons conclure que $HK \subset KH$

→ Nous démontrerions, de la même manière que $KH \subset HK$

→ Donc, de $HK \subset KH$ et $KH \subset HK$, nous déduisons $KH = HK$

⇒ **Supposons** $HK = KH$
Démontrons que HK est un sous-groupe de G.

→ Dans un premier temps, nous avons $HK \neq \emptyset$ car $1 \in HK$.
En effet, H et K étant 2 sous-groupes de G, alors $1 \in H$ et $1 \in K$ et comme $1 = 1 \times 1$, nous avons $1 \in HK$

→ Soient $u \in HK$ et $v \in HK$. Montrons que $uv^{-1} \in HK$
Comme $u \in HK$ et $v \in HK$, il existe alors $h_u \in H$, $h_v \in H$, $k_u \in K$ et $k_v \in K$ tels que $u = h_u k_u$ et $v = h_v k_v$ et donc $u^{-1} = k_v^{-1}h_v^{-1}$.D'où

$$uv^{-1} = h_u k_u k_v^{-1} h_v^{-1} = h_u \left(k_u k_v^{-1}\right) h_v^{-1}$$

K étant un groupe, nous avons $\left(k_u k_v^{-1}\right) \in K$ et donc $h_u \left(k_u k_v^{-1}\right) \in HK$ et comme $HK = KH$, il existe $h_1 \in H$ et $k_1 \in K$ tels que $h_u \left(k_u k_v^{-1}\right) = k_1 h_1$; d'où :

$$uv^{-1} = h_u \left(k_u k_v^{-1}\right) h_v^{-1} = (k_1 h_1) h_v^{-1} = k_1 \left(h_1 h_v^{-1}\right)$$

Comme $\left(h_1 h_v^{-1}\right) \in H$, nous avons $k_1 \left(h_1 h_v^{-1}\right) \in KH$; comme, par hypothèse, nous avons $HK = KH$, nous avons aussi $k_1 \left(h_1 h_v^{-1}\right) \in HK$, c'est à dire $uv^{-1} \in HK$

→ Ainsi, si $HK = KH$, alors HK et KH sont des sous-groupes de G

Que se passe-t-il si le groupe G est commutatif ?

Exercice 12 :

Soit G un groupe dont l'opération est notée multiplicativement. Montrer que, pour tout $a \in G$ et tout $b \in G$

1. *a et a^{-1} ont même ordre*
   ▷ Supposons que a soit d'ordre n ; alors, $a^n = e$
   - ⋆ En multipliant à droite par a^{-1}, nous obtenons $a^{n-1} = a^{-1}$
   - ⋆ Puis, en itérant cette opération, nous avons $a^{n-p} = \left(a^{-1}\right)^p$
   - ⋆ Et lorsque $p = n$, nous obtenons $e = \left(a^{-1}\right)^n$

   D'où nous tirons que a^{-1} a même ordre que a

   ▷ Une autre façon de démontrer consiste à dire que si a est d'ordre n, $\text{Card}\left(\langle a \rangle\right) = n$. Or, $\langle a \rangle = \langle a^{-1} \rangle$ et donc $\text{Card}\left(\langle a^{-1} \rangle\right) = n$
2. *a et bab^{-1} ont même ordre*

   Soit n l'ordre de a, c'est à dire $a^n = e$. Alors :

$$\begin{aligned}\left(bab^{-1}\right)^n &= \underbrace{\left(bab^{-1}\right)\left(bab^{-1}\right)\cdots\left(bab^{-1}\right)}_{n \text{ fois}} \\ &= ba\left(b^{-1}b\right)a\left(b^{-1}b\right)a\left(b^{-1}\cdots b\right)a\left(b^{-1}b\right)ab^{-1} \\ &= ba^nb^{-1} \\ &= ba^nb^{-1} = e\end{aligned}$$

   Donc $\left(bab^{-1}\right)^n = e$ et l'ordre de bab^{-1} est donc encore n.
3. *ab et ba ont même ordre*

Soit n l'ordre de ab, c'est à dire $(ab)^n = e$. Alors :

$$\begin{aligned} e = & \ (ab)^n \\ = & \ \underbrace{(ab)(ab)\cdots(ab)}_{n \text{ fois}} \\ = & \ a(ba)(ba)(ba)\cdots(ba)(ba)b \\ = & \ a(ba)^{n-1}b \end{aligned}$$

En composant à gauche par b, nous obtenons :

$$e = a(ba)^{n-1}b \Longleftrightarrow b = ba(ba)^{n-1}b \Longleftrightarrow b = (ba)^n b$$

Une loi de groupe étant régulière, nous pouvons « simplifier » par b et nous obtenons $(ba)^n = e$.
En conclusion, ab et ba ont même ordre

Exercice 22 :

Soient G un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G. On suppose que, pour tout $i \in I$ et tout $j \in I$, il existe un élément $k \in I$ tel que $H_i \subset H_k$ et $H_j \subset H_k$.
Montrer que $\bigcup\limits_{i\in I} H_i$ est un sous-groupe de G

$\Rightarrow$ En appelant e l'élément neutre de G, alors $e \in \bigcap\limits_{i\in I} H_i$ et donc $e \in \bigcup\limits_{i\in I} H_i$; ainsi, $e \in \bigcup\limits_{i\in I} H_i \neq \emptyset$

$\Rightarrow$ Soient $x \in \bigcup\limits_{i\in I} H_i$ et $y \in \bigcup\limits_{i\in I} H_i$; nous allons montrer que $xy^{-1} \in \bigcap\limits_{i\in I} H_i$

- ⋆ Il existe $i_0 \in I$ tel que $x \in H_{i_0}$; de même, il existe $j_0 \in I$ tel que $x \in H_{j_0}$
- ⋆ D'après l'hypothèse, il existe $k \in I$ tel que $H_{i_0} \subset H_k$ et $H_{j_0} \subset H_k$; par cette inclusion, nous avons $x \in H_k$ et $y \in H_k$
- ⋆ H_k étant un groupe, nous avons $xy^{-1} \in H_k$, et donc $xy^{-1} \in \bigcap\limits_{i\in I} H_i$

$\Rightarrow$ $\bigcup\limits_{i\in I} H_i$ est donc un sous-groupe de G

Exercice 23 :

Soit G un groupe non commutatif de centre $Z(G)$. On désigne par $Aut(G)$ l'ensemble des automorphismes de G et $Int(G)$ l'ensemble des automorphismes intérieurs de G.

1. (a) *Démontrer que $(Aut(G), \circ)$ est un groupe*

   En fait, un automorphisme est un isomorphisme particulier. C'est un isomorphisme qui va de G dans G. Nous allons donc utiliser, dès que nous le pourrons, les propriétés des isomorphismes vues en L_0

   $\Rightarrow$ Premièrement, $Aut(G) \neq \emptyset$ puisque Id_G, l'application identique de G est un homomorphisme bijectif de G ; c'est l'élément neutre pour la composition des applications

   $\Rightarrow$ Ensuite, si nous composons 2 homomorphismes, nous obtenons un homomorphisme, et si nous composons 2 bijections, nous obtenons aussi une bijection. La composition de 2 automorphismes de G est donc un automorphisme de G. La loi $\circ$ est donc interne.

   $\Rightarrow$ Si $f \in Aut(G)$, alors f est bijective et donc f^{-1} existe. En L_0, nous avons démontré que si $f : G \longrightarrow H$ est un isomorphisme de groupe, il en est de même de $f^{-1} : H \longrightarrow G$. Donc, si f est un automorphisme, f^{-1} en est un aussi

   Nous venons de démontrer que $(Aut(G), \circ)$ est un groupe

   En fait, $(Aut(G), \circ)$ est un sous-groupe du groupe $\mathfrak{S}(G)$ des permutations de G, ces permutations pouvant être des homomorphismes ou non

   (b) *Démontrer que $(Int(G), \circ)$ est un sous-groupe de $(Aut(G), \circ)$*

   Nous avons défini en L_0, ce qu'était un automorphisme intérieur et démontré, en L_0, que c'était des automorphismes. Nous avons donc $(Int(G), \circ) \subset (Aut(G), \circ)$

   Nous reprendrons la notation de L_0 en utilisant une opération multiplicative.

   $\Rightarrow$ Tout d'abord, $Int(G) \neq \emptyset$, puisque $f_e = \mathrm{Id}_G$

$\Rightarrow$ Soient $f_a \in Int(G)$ et $f_b \in Int(G)$, alors, pour tout $x \in G$, nous avons :

$$f_a \circ f_b(x) = f_a[f_b(x)] = f_a\left[bxb^{-1}\right] = abxb^{-1}a^{-1} = abx(ab)^{-1} = f_{ab}(x)$$

La composition des automorphismes intérieurs est donc interne et nous avons $f_a \circ f_b = f_{ab}$

$\Rightarrow$ Un automorphisme intérieur est une bijection, et nous avons $(f_a)^{-1} = f_{a^{-1}}$

Donc $(Int(G), \circ)$ est un sous-groupe de $(Aut(G), \circ)$

2. *Nous allons démontrer que G opère sur luimême par les automorphismes intérieurs.*
Soit $\Phi : G \longrightarrow Int(G)$ défini par :

$$\left\{\begin{array}{rcl} \Phi : G & \longrightarrow & Int(G) \\ a & \longmapsto & \Phi(a) = f_a \end{array}\right. \quad \text{où} \quad \left\{\begin{array}{rcl} f_a : G & \longrightarrow & G \\ x & \longmapsto & f_a(x) = axa^{-1} \end{array}\right.$$

Il faut démontrer que Φ est un homomorphisme

Pas très difficile ; nous allons beaucoup utiliser la question précédente. Soient donc $a \in G$ et $b \in G$, alors :

$$\Phi(ab) = f_{ab} = f_a \circ f_b = \Phi(a) \circ \Phi(b)$$

Φ est bien un homomorphisme de groupe

3. *Démontrer que $Int(G)$ est isomorphe à $G/Z(G)$*

C'est, en fait le but de l'exercice !!

Nous allons utiliser la proposition 1.3.3 de décomposition canonique d'un homomorphisme qui affirme que $G/\ker\Phi$ et $\Phi(G) = Int(G)$ sont isomorphes.

Nous devons donc démontrer que $\ker\Phi = Z(G)$.

$\rightarrow$ Nous allons montrer que $Z(G) \subset \ker\Phi$

Soit $a \in Z(G)$. Il faut donc montrer que $\Phi(a) = \mathrm{Id}_G$ et alors, $a \in \ker\Phi$

Pour tout $x \in G$:

$$\Phi(a)(x) = f_a(x) = axa^{-1} \overset{a\in Z(G)}{=} aa^{-1}x = x = \mathrm{Id}_G(x)$$

Ainsi, pour tout $x \in G$, $\Phi(a)(x) = x$ et, donc, pour tout $a \in Z(G)$, nous avons $\Phi(a) = \mathrm{Id}_G$ et donc $a \in \ker\Phi$, c'est à dire $Z(G) \subset \ker\Phi$

$\rightarrow$ Réciproquement, démontrons que $\ker\Phi \subset Z(G)$

Soit $a \in \ker\Phi$, alors, $\Phi(a) = \mathrm{Id}_G$ et donc, pour tout $x \in G$ $\Phi(a)(x) = x$, c'est à dire :

$$\Phi(a)(x) = x \Longleftrightarrow f_a(x) = x \Longleftrightarrow axa^{-1} = x \Longleftrightarrow ax = xa$$

Ainsi, pur tout $x \in G$, nous avons $ax = xa$ et donc $a \in Z(G)$, et donc $\ker\Phi \subset Z(G)$

En conclusion $\ker\Phi = Z(G)$ et d'après 1.3.3, nous avons démontré que $G/\ker\Phi$ et $\Phi(G) = Int(G)$ sont isomorphes.

Ce que nous voulions

Quelques compléments

$\Rightarrow$ Dans l'opération $\Phi : G \longrightarrow Int(G)$, l'orbite de $x \in G$ est donnée par :

$$\mathcal{O}(x) = \{y \in G \text{ tel que } \exists a \in G \text{ tel que } y = f_a(x)\} = \left\{y \in G \text{ tel que } \exists a \in G \text{ tel que } y = axa^{-1}\right\}$$

La relation $\mathcal{R}$ définie sur G par $x\mathcal{R}y$ si et seulement si il existe $a \in G$ tel que $y = axa^{-1}$ peut être aussi définie par

$$x\mathcal{R}y \Longleftrightarrow y \in \mathcal{O}(x)$$

C'est, bien entendu, une relation d'équivalence

$\Rightarrow$ f_a étant un automorphisme de G, pour tout $a \in G$, et tout sous-groupe $H \subset G$, nous avons $f_a(H)$ qui est un sous-groupe de G. Si $H' = f_a(H)$, on dit que les sous-groupes H et H' sont conjugués.

Exercice 24 :

1. *Trouver tous les groupes d'ordre 4*

   Soit G un tel groupe ; on pose $G = \{e, a, b, c\}$ avec e élément neutre de G.
   Nous chosissons $a \in G$; bien entendu, $a \neq e$
   Puisque $\langle a \rangle$ est un sous-groupe de G, l'ordre de a divise 4
   $\rightarrow$ Cet ordre ne peut pas être 1, sinon $a = e$, ce qui est impossible
   $\rightarrow$ Si l'ordre de a est 4, alors G est cyclique, engendré par a et $G = \{e, a, a^2, a^3\}$.
   (On peut remarquer que $H = \{e, a^2\}$ est un sous-groupe de G)
   $\rightarrow$ Si l'ordre de a est 2, alors $a^2 = e$, et nous avons $ab = ba = c$ et $ac = ca = b$. Il n'y a pas d'autre solution, puisque si $ab = b$, alors $a = e$, ce qui est impossible.
   $\star$ Nous obtenons alors la table de multiplcation de G

$\curvearrowright$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

   $\star$ Considérons le groupe produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow G$ telle que :

   $$\varphi[(0,0)] = e \quad \varphi[(1,0)] = a \quad \varphi[(0,1)] = b \quad \varphi[(1,1)] = c$$

   Il est facile *(et fastidieux)* de démontrer que φ est un isomorphisme de groupe
   $\rightarrow$ il n'existe donc que 2 types de groupes à 4 éléments :
   $\star$ Soit G est un groupe cyclique isimorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$
   $\star$ Soit G est isomorphe au groupe produit $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ appelé **Groupe de Klein**

2. *Soit G un groupe d'ordre $2n$ et d'élément neutre e.*
   On suppose qu'il existe 2 sous-groupes de G, différents, H_1 et H_2 d'ordre n et tels que $H_1 \cap H_2 = \{e\}$

   (a) *Montrer que $n = 2$, c'est à dire que G est un groupe à 4 éléments*

   $\Rightarrow$ Supposons que $n < 2$, c'est à dire $n = 1$; alors G est un groupe d'ordre 2 ; supposons $G = \{e, a\}$. Les seuls sous-groupes de G sont G ou $\{e\}$, les seules possibilités que nous ayions est $H_1 = H_2 = \{e\}$, ce qui est en contradiction avec le fait que $H_1 \neq H_2$
   Nous avons donc $n \geqslant 2$
   $\Rightarrow$ Supposons, maintenant que $n \geqslant 2$
   Nous avons Card $(H_1 \cup H_2) = 2n - 1$, et il existe donc $\alpha \in G$ tel que $\alpha \notin H_1$ et $\alpha \notin H_2$
   Nous avons $\alpha^{-1} = \alpha$
   En effet, supposons le contraire, c'est à dire $\alpha^{-1} \neq \alpha$, alors, en regardant les cardinaux, nous avons $\alpha^{-1} \in H_1$ ou $\alpha^{-1} \in H_2$
   Si $\alpha^{-1} \in H_1$, alors $\alpha^{-1} \times \alpha = e$ et, des propriétés de composition interne dans un groupe, nous aurions $\alpha \in H_1$, ce qui est impossible.
   $\Rightarrow$ Supposons maintenant $n > 2$, c'est à dire $n \geqslant 3$
   Comme Card $H_1 = n$, il existe des éléments $\beta_1 \in H_1$, $\gamma_1 \in H_1$, $\beta_2 \in H_2$, $\gamma_2 \in H_2$ tels que $\beta_1 \neq e$, $\gamma_1 \neq e$, $\beta_2 \neq e$ et $\gamma_2 \neq e$
   $\triangleright$ Nous avons $\beta_1 \times \beta_2 = \alpha$, car si nous avions $\beta_1 \times \beta_2 \in H_1$, alors, nous devons avoir $\beta_2 \in H_1$, ce qui est impossible puisque $\beta_2 \in H_2$ et $H_1 = H_2 = \{e\}$
   $\triangleright$ Pour les mêmes raisons, nous avons $\gamma_1 \times \beta_2 = \alpha$
   $\triangleright$ Donc, nous avons $\beta_1 \times \beta_2 = \gamma_1 \times \beta_2 = \alpha$, c'est à dire $\beta_1 = \gamma_1$, ce qui est impossible.
   $\triangleright$ Il y a donc une contradiction et l'hypothèse $n \geqslant 3$ est fausse et donc $n < 3$
   En conclusion, $n = 2$
   G est donc un groupe à 4 éléments

   (b) *Montrer que la structure de G est entièrement déterminée et en donner la table de multiplication*

   G étant un groupe à 4 éléments est cyclique ou isomorphe au groupe de Klein.

Nous avons donc $G = \{e, h_1, h_2, \alpha\}$ où $H_1 = \{e, h_1\}$ et $H_2 = \{e, h_2\}$, et donc, d'après les questions précédentes, $h_1^2 = e$ et $h_2^2 = e$, et, toujours d'après l'étude précédente, $h_1h_2 = \alpha$ et $\alpha^2 = e$.
C'est donc le groupe de Klein dont la table de multiplication est donnée dans la question précédente.
Il y a donc 3 sous-groupes d'ordre 2 : $H_1 = \{e, h_1\}$, $H_2 = \{e, h_2\}$ et $H_3 = \{e, \alpha\}$

Exercice 25 :

Soit G un groupe cyclique d'ordre n et de générateur a

1. *Montrer que tout sous-groupe de G est cyclique*

   Soit $H \subset G$ un sous-groupe de G
   Soit $n_0 \in \mathbb{N}^*$ le plus petit entier strictement positif tel que $a^{n_0} \in H$.
   Le sous-groupe $\langle a^{n_0} \rangle$ engendré par a^{n_0} est un sous-groupe de H.
   Soit $x \in H$ un élément quelconque de H ; comme $x \in G$, il existe alors $m \in \mathbb{N}^*$ tel que $x = a^m$.
   Nous effectuons la division euclidienne de m par n_0

   $$m = qn_0 + r \text{ où } 0 \leqslant r < n_0$$

   Alors, $x = a^m = a^{qn_0+r} = (a^{n_0})^q \times a^r$. Nous avons $a^m \in H$ par définition ; puis nous avons $(a^{n_0})^q \in \langle a^{n_0} \rangle$, c'est à dire, puisque $\langle a^{n_0} \rangle \subset H$, $(a^{n_0})^q \in H$, et donc $a^r \in H$. Nous ne pouvons pas avoir $0 < r < n_0$, car c'est en contradiction avec le fait que n_0 est le plus petit entier strictement positif tel que $a^{n_0} \in H$. Donc $r = 0$.
   Ainsi, tout $x \in H$ est du type $x = (a^{n_0})^q$ et donc $x \in \langle a^{n_0} \rangle$, ce qui veut dire que $H \subset \langle a^{n_0} \rangle$
   Et donc, $H = \langle a^{n_0} \rangle$ et est donc un groupe cyclique.

2. *Soit $m \in \mathbb{N}^*$. Montrer que $a^m = e$ si et seulement si n divise m*

   $\Rightarrow$ Si n divise m, il existe alors $k \in \mathbb{N}^*$ tel que $m = kn$, et alors $a^m = a^{kn} = (a^n)^k = e^k = e$
   $\Rightarrow$ Réciproquement, supposons $a^m = e$.
   Alors $m \geqslant n$, puisque si $m < n$, alors, a ne peut être générateur de G.
   Faisons la division euclidenne de m par n : $m = kn + r$ avec $0 \leqslant r < n$; alors $a^m = a^{kn+r} = a^{kn}a^r = (a^n)^k \times a^r = a^r = e$. Et la seule possibilité est que $r = 0$ et donc n divise m

3. *Soit p un entier quelconque tel que $1 \leqslant p \leqslant n$ et $\langle a^p \rangle$ le sous-groupe de G engendré par a^p*

   (a) *Montrer que nous avons $\langle a^p \rangle = \langle a^q \rangle$ où q est le pgcd de n et p*

   Soit donc q le pgcd de n et p
   $\rightarrow$ Il existe donc $k_1 \in \mathbb{N}$ tel que $p = k_1q$.
   Alors $a^p = a^{k_1q} = (a^q)^{k_1}$ et donc $a^p \in \langle a^q \rangle$; d'où $\langle a^p \rangle \subset \langle a^q \rangle$
   $\rightarrow$ D'après le théorème de Bezout, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $q = un + vp$, et donc $a^q = a^{un+vp} = a^{un} \times a^{vp} = (a^n)^u \times (a^p)^v = (a^p)^v$, et donc $a^q \in \langle a^p \rangle$ et donc $\langle a^q \rangle \subset \langle a^p \rangle$
   $\rightarrow$ D'où $\langle a^p \rangle = \langle a^q \rangle$
   Ce que nous voulions

   (b) *Démontrer que $\langle a^p \rangle = G$ si et seulement si n et p sont premiers entre eux.*

   Si n et p sont premiers entre eux, alors le pgcd de n et p est 1, et d'après la question qui précède, $\langle a^p \rangle = \langle a \rangle = G$

Nous avons démontré 2 résultats importants :

1. Tout sous groupe d'un groupe cyclique est cyclique
2. Si n est l'ordre d'un groupe cyclique G généré par a, alors pour tout entier p tel que p soit premier avec n, a^p engendre G

Exercice 26 :

Soient G_1 et G_2 2 groupes et nous considérons leur produit direct $G_1 \times G_2$. Nous appelons e_1 l'élément neutre de G_1 et e_2, celui de G_2
On consdère $a_1 \in G_1$ d'ordre n_1 et $a_2 \in G_2$ d'ordre n_2

1. *Montrer que l'ordre de l'élément $(a_1, a_2) \in G_1 \times G_2$ est le ppcm de n_1 et de n_2*

   C'est, cette fois-ci, assez facile.
   Soit $q \in \mathbb{N}^*$ tel que $(a_1, a_2)^q = (e_1, e_2)$, ceci veut dire que $(a_1^q, a_2^q) = (e_1, e_2) \Longleftrightarrow a_1^q = e_1$ et $a_2^q = e_2$
   Et nous avons ces égalités si et seulement si q est un ùultiple commun à n_1 et n_2
   L'ordre de (a_1, a_2) est donc bien le ppcm de n_1 et de n_2
2. *On suppose G_1 cyclique d'ordre n_1 et G_2 cyclique d'ordre n_2. Démontrer que si n_1 et n_2 sont premiers entre eux, alors $G_1 \times G_2$ est cyclique d'ordre $n_1 n_2$*

   Si G_1 est cyclique d'ordre n_1 et G_2 cyclique d'ordre n_2, alors Card $[G_1 \times G_2] = n_1 n_2$.
   Si a_1 d'ordre n_1 engendre G_1 et a_2 d'ordre n_2 engendre G_2, alors, d'après la question précédente, l'ordre de (a_1, a_2) est le ppcm de n_1 et de n_2, et, ici, comme n_1 et n_2 sont premiers entre eux, ce ppcm est $n_1 n_2$
   Comme Card $[G_1 \times G_2] = n_1 n_2$, $G_1 \times G_2$ est cyclique d'ordre $n_1 n_2$.

Exercice 27 :

Montrer que les conditions suivantes sont équivalentes :

1. *G est un groupe cyclique d'ordre premier*
2. *G est un groupe abélien simple*

1. Supposons que G soit un groupe cyclique d'ordre premier
   - ▷ Tout d'abord, G étant cyclique, est abélien
   - ▷ Soit $p \geqslant 2$ l'ordre de G ; il y a donc au moins 2 éléments. Soit $x \neq e$ un autre élément générateur de G. Alors $\langle x \rangle$ est le sous-groupe engendré par x et l'ordre de $\langle x \rangle$ divise p, l'ordre de G. Comme p est premier, l'ordre de $\langle x \rangle$ est 1 ou p, c'est à dire $\langle x \rangle = \{e\}$ ou $\langle x \rangle = G$

   G est donc un groupe simple.
2. Supposons que G soit un groupe abélien simple
   Soit $x \in G$ tel que $x \neq e$. Alors $\langle x \rangle$ est un sous-groupe de G. G étant simple, $\langle x \rangle = G$, c'est à dire que G est monogène, autrement dit :

   $$G = \{x^n \text{ avec } n \in \mathbb{Z}\}$$

   - ▷ Ainsi, si G est infini, alors G est isomorphe à $\mathbb{Z}$ et s'il est d'ordre fini n, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$
   - ▷ G est sûrement d'ordre fini.
     En effet, soit $f : \mathbb{Z} \longrightarrow G$, définie par :

     $$\begin{cases} f : \mathbb{Z} & \longrightarrow & G \\ \quad n & \longmapsto & f(n) = x^n \end{cases}$$

     f est un homomorphisme de $\mathbb{Z}$ dans G, et si G est monogène, f est un isomorphisme de $\mathbb{Z}$ dans G. Pour $m \in \mathbb{N}^*$, $m\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ et $f(m\mathbb{Z})$ est un sous-groupe de G, différent de G et de $\{e\}$.
     Ce qui est impossible. Donc G est fini et d'ordre n
   - ▷ n est un nombre premier
     En effet, supposons le contraire, et posons $n = pq$.
     Alors, x^n est un élément d'ordre q, et le sous-groupe $\langle x^p \rangle$ est un sous-groupe de G d'ordre q, différent de G et de $\{e\}$, ce qui est impossible.
     Donc n est premier.

   G est donc un groupe cyclique d'ordre n premier.

Exercice 28 :

Soient G_1 et G_2 2 groupes et $G_1 \times G_2$ leur produit direct.. On appelle ϖ_1 la projection de $G_1 \times G_2$ sur G_1 et ϖ_2 la projection de $G_1 \times G_2$ sur G_2.
Soit G un groupe quelconque $u_1 : G \longrightarrow G_1$ un homomorphisme de groupe et $u_2 : G \longrightarrow G_2$ un second homomorphisme de groupe.
Démontrer qu'il existe un homomorphisme $h : G \longrightarrow G_1 \times G_2$ et un seul tel que $u_1 = \varpi_1 \circ h$ et $u_2 = \varpi_2 \circ h$

Commençons par faire un diagramme pour visualiser le problème :

$$\begin{tikzcd} G \arrow[r, "u_1"] \arrow[d, "u_2"'] \arrow[dr, "h"] & G_1 \\ G_2 & G_1 \times G_2 \arrow[l, "\varpi_2"] \arrow[u, "\varpi_1"'] \end{tikzcd}$$

Rigoureusement, il n'y a pas de grandes mathématiques dans cet exercice. Il suffit de poser, pour $x \in G$, $h(x) = (u_1(x), u_2(x))$; l'unicité de h est liée à la définition même de h.
Nous avons, bien entendu, $\varpi_1 \circ h(x) = \varpi_1(u_1(x), u_2(x)) = u_1(x)$, et donc $u_1 = \varpi_1 \circ h$. De la même manière, nous avons $u_2 = \varpi_2 \circ h$