10.14 Quelques exercices corrigés

10.14.1 Premières définitions

Exercice 1 :

1. *On considère les 4 matrices :*

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

L'ensemble de ces 4 matrices, muni de la multiplication, forme-t-il un groupe ?

Nous appelons $\mathrm{I}_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$; c'est la matrice identité et, clairement $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}=-\mathrm{I}_2$.

Si $R_1=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ et $R_2=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$, nous avons $R_1=-R_2$ et $R_1R_2=\mathrm{I}_2$, $R_1^2=R_2^2=-\mathrm{I}_2$.

D'où le tableau :

$\times$	I_2	$-\mathrm{I}_2$	R_1	R_2
I_2	I_2	$-\mathrm{I}_2$	R_1	R_2
$-\mathrm{I}_2$	$-\mathrm{I}_2$	I_2	R_2	R_1
R_1	R_1	R_2	$-\mathrm{I}_2$	I_2
R_2	R_2	R_1	I_2	$-\mathrm{I}_2$

L'ensemble de ces 4 matrices muni de la multiplication des matrices est donc un groupe fini. Ce groupe est même commutatif.

R_1 est une rotation du plan d'angle $-\dfrac{\pi}{2}$, alors que R_2 est une rotation du plan d'angle $\dfrac{\pi}{2}$

2. *Dans cette question, j représente une racine cubique de 1 : $j=\dfrac{-1+i\sqrt{3}}{2}$*
On considère les 4 matrices suivantes :

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\quad\begin{pmatrix}j&0\\0&j^2\end{pmatrix}\quad\begin{pmatrix}j^2&0\\0&j\end{pmatrix}\quad\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

L'ensemble de ces 4 matrices, muni de la multiplication, forme-t-il un groupe ?

Pour commencer, il faut remarquer que $1+j+j^2=0$

Pour nous simplifier la vie, nous posons $\mathrm{I}_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $A=\begin{pmatrix}j&0\\0&j^2\end{pmatrix}$, $B=\begin{pmatrix}j^2&0\\0&j\end{pmatrix}$ et $S=\begin{pmatrix}0&1\\1&0\end{pmatrix}$

Comme tout à l'heure, I_2 est l'élément neutre de la multiplication des matrices, et nous avons $S^2=\mathrm{I}_2$

Par calcul, nous montrons que $AB=BA=\mathrm{I}_2$, $A^2=B$ et $B^2=A$, mais nous avons $AS=\begin{pmatrix}0&j\\j^2&0\end{pmatrix}$ qui n'est pas un élément de l'ensemble considéré.

Ce n'est donc pas un groupe puisque la multiplication n'est pas interne.

Exercice 2 :

Soit G un groupe de neutre e, tel que pour tout $x\in G$, $x^2=e$. Montrer que G est commutatif

Soient $x\in G$ et $y\in G$; il faut donc montrer que $xy=yx$.
La seule hypothèse que nous ayions est : $(xy)^2=e$. Or, $(xy)^2=xyxy=e$
En composant à droite par y, nous obtenons :

$$xyxyy=ey\iff xyxy^2=y\iff xyx=y$$

En composant maintenant à gauche par x, nous obtenons :

$$xyx=y\iff xxyx=xy\iff x^2yx=xy\iff yx=xy$$

On vient donc de montrer que si, pour tout $x\in G$, $x^2=e$, alors $xy=yx$

Exercice 4 :

Soient $(G_1,*)$, $(G_2,\top)$ 2 groupes ; on suppose $(G_2,\top)$ commutatif. Soit $\mathrm{Hom}(G_1,G_2)$ l'ensemble des homomorphismes de groupes de G_1 dans G_2.
On définit, dans $\mathrm{Hom}(G_1,G_2)$, la loi $\diamond$ par $(f\diamond g)(x)=f(x)\top g(x)$
La loi $\diamond$ définit-elle une loi de groupe sur $\mathrm{Hom}(G_1,G_2)$? Comment la structure de $(G_2,\top)$ intervient-elle ?

1. **Montrons que c'est une loi de composition interne**
   Il faut donc montrer que si $f\in\mathrm{Hom}(G_1,G_2)$ et $g\in\mathrm{Hom}(G_1,G_2)$, alors $f\diamond g\in\mathrm{Hom}(G_1,G_2)$
   Il faut donc démontrer que, pour tout $x\in G_1$ et tout $y\in G_2$, $f\diamond g(x*y)=(f\diamond g)(x)\top(f\diamond g)(y)$.
   Soient donc $x\in G_1$ et $y\in G_1$:

$$\begin{array}{rcl} f\diamond g(x*y) = & f(x*y)\top g(x*y) & \\ = & (f(x)\top f(y))\top(g(x)\top g(y)) & \\ = & (f(x)\top g(x))\top(f(y)\top g(y)) & \text{(associativité dans } (G_2,\top) \text{ et commutativité de } (G_2,\top)) \\ = & ((f\diamond g)(x))\top((f\diamond g)(y)) & \end{array}$$

   $f\diamond g$ est donc un homomorphisme et $f\diamond g\in\mathrm{Hom}(G_1,G_2)$
   La structure de $(G_2,\top)$ intervient dans le fait où c'est un groupe commutatif
2. **Montrons que l'opération $\diamond$ est associative**
   Il faut donc montrer que, pour tout $f\in\mathrm{Hom}(G_1,G_2)$, tout $g\in\mathrm{Hom}(G_1,G_2)$ et tout $h\in\mathrm{Hom}(G_1,G_2)$, nous avons
   $$f\diamond(g\diamond h)=(f\diamond g)\diamond h$$
   Soit donc $x\in G_1$:

$$\begin{array}{rcl} f\diamond(g\diamond h)(x) = & f(x)\top(g\diamond h)(x) & \\ = & f(x)\top(g(x)\top h(x)) & \\ = & (f(x)\top g(x))\top h(x) & (\text{ associativité dans } (G_2,\top)) \\ = & (f\diamond g)(x)\top h(x) & \\ = & ((f\diamond g)\diamond h)(x) & \end{array}$$

   Nous avons donc, pour tout $x\in G$, $f\diamond(g\diamond h)(x)=((f\diamond g)\diamond h)(x)$, c'est à dire que nous avons $f\diamond(g\diamond h)=(f\diamond g)\diamond h$
   La loi $\diamond$ est donc associative.
3. **Recherche d'un élément neutre pour la loi $\diamond$**
   Il faut donc trouver $\mathcal{N}\in\mathrm{Hom}(G_1,G_2)$ tel que, pour tout $f\in\mathrm{Hom}(G_1,G_2)$, $f\diamond\mathcal{N}=\mathcal{N}\diamond f=f$.
   Si cet homomorphisme $\mathcal{N}$ existe, alors, pour tout $x\in G_1$, nous avons :
   $$f\diamond\mathcal{N}(x)=f(x)\top\mathcal{N}(x)=f(x)$$
   Ainsi, pour tout $x\in G_1$, nous avons $\mathcal{N}(x)=e_2$ où e_2 est le neutre de $(G_2,\top)$.
   Il est facile de démontrer que $\mathcal{N}\in\mathrm{Hom}(G_1,G_2)$.
   La loi $\diamond$ admet donc un élément neutre qui est l'homomorphisme constant $\mathcal{N}$ défini par :
   $$\left\{\begin{array}{rcl} \mathcal{N}:G_1 & \longrightarrow & G_2 \\ x & \longmapsto & \mathcal{N}(x)=e_2 \end{array}\right.$$
4. **Recherche de symétrique**
   Soit $f\in\mathrm{Hom}(G_1,G_2)$. Existe-t-il $f_s\in\mathrm{Hom}(G_1,G_2)$ telle que $f\diamond f_s=f_s\diamond f=\mathcal{N}$?
   C'est à dire que nous devrions avoir, pour tout $x\in G_1$ $f\diamond f_s(x)=\mathcal{N}(x)=e_2$.
   En ré-écrivant cette égalité, nous avons :
   $$f\diamond f_s(x)=f(x)\top f_s(x)=e_2$$
   Ainsi, $f_s(x)=[f(x)]^{-1}=f\left(x^{-1}\right)$, puisque f est un homomorphisme de groupe
   Démontrons que f_s est un homomorphisme, c'est à dire $f_s\in\mathrm{Hom}(G_1,G_2)$.

Pour tout $x \in G_1$ et tout $y \in G_2$, nous avons :

$$\begin{array}{rcl} f_s(x*y) = & f\left((x*y)^{-1}\right) & \\ = & f\left(y^{-1}*x^{-1}\right) & \\ = & f\left(y^{-1}\right) \top f\left(x^{-1}\right) & \\ = & f\left(x^{-1}\right) \top f\left(y^{-1}\right) & \text{par commutativité dans } (G_2, \top) \\ = & f_s(x) \top f_s(y) & \end{array}$$

Donc $f_s \in \text{Hom}(G_1, G_2)$

5. **L'opération $\diamond$ est-elle commutative ?**
Autrement dit, est ce que, pour tout $f \in \text{Hom}(G_1, G_2)$ et tout $g \in \text{Hom}(G_1, G_2)$, avons nous $f \diamond g = g \diamond f$?
Soit $x \in G_1$; alors :

$$\begin{array}{rcl} f \diamond g(x) = & f(x) \top g(x) & \\ = & g(x) \top f(x) & \text{(commutativité de } (G_2, \top)) \\ = & g \diamond f(x) & \end{array}$$

Ainsi, pour tout $x \in G_1$, $f \diamond g(x) = g \diamond f(x)$ et donc $f \diamond g = g \diamond f$

Il est évident que la structure du groupe $(G_2, \top)$ joue un rôle majeur, et en particulier la commutativité de ce groupe

Exercice 5 :

1. *S_3 est le groupe des permutations d'un ensemble à 3 éléments. Avons nous $(S_3, \circ)$ isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$?*

Il est clair que $(S_3, \circ)$ ne peut être isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$. En effet, $(\mathbb{Z}/6\mathbb{Z}, +)$ est un groupe commutatif, alors que $(S_3, \circ)$ ne l'est pas.

En effet, soient $\sigma_1 \in S_3$ et $\sigma_2 \in S_3$ définies par :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix} \qquad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix}$$

Regardons maintenant les compositions $\sigma_1 \circ \sigma_2$ et $\sigma_2 \circ \sigma_1$:

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix}$$

Nous avons donc $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$

2. *Dans $\mathbb{Z}/16\mathbb{Z}$, on considère l'ensemble $H = \{1, 3, 9, 11\}$. Vérifier que H est un groupe multiplicatif. Rechercher tous les homomorphismes de $(\mathbb{Z}/4\mathbb{Z}, +)$ dans $(H, \times)$. Parmi ces homomorphismes, quels sont les isomorphismes ?*

⇒ **Faisons la table de multiplication de $(H, \times)$**

$\times$	1	3	9	11
1	1	3	9	11
3	3	9	11	1
9	9	11	1	3
11	11	1	3	9

⇒ **Recherchons les homomorphismes de $(\mathbb{Z}/4\mathbb{Z}, +)$ dans $(H, \times)$**
Nous appellerons φ un homomorphisme quelconque
⋆ Tout d'abord, l'image du neutre de $(\mathbb{Z}/4\mathbb{Z}, +)$ est le neutre de $(H, \times)$, nous devons avoir $\varphi(0) = 1$

⋆ Puis, $\varphi(2) = \varphi(1+1) = (\varphi(1))^2$, ainsi que $\varphi(3) = (\varphi(1))^3$. Le choix de $\varphi(1)$ est donc important

⇒ Les homomorphismes sont donc :

⋆ L'homomorphisme constant, qui à tout $n \in (\mathbb{Z}/4\mathbb{Z}, +)$ fait correspondre $\varphi(n) = 1$; de manière claire, ce n'est pas un isomorphisme.

⋆ Soit $\varphi_1 : (\mathbb{Z}/4\mathbb{Z}, +) \longrightarrow (H, \times)$ défini par :

$$\varphi_1(0) = 1 \quad \varphi_1(1) = 3 \quad \varphi_1(2) = 9 \quad \varphi_1(3) = 11$$

C'est un isomorphisme

⋆ Soit $\varphi_2 : (\mathbb{Z}/4\mathbb{Z}, +) \longrightarrow (H, \times)$ défini par :

$$\varphi_2(0) = 1 \quad \varphi_2(1) = 9 \quad \varphi_2(2) = 1 \quad \varphi_2(3) = 9$$

Ce n'est clairement pas un isomorphisme, mais l'image de φ_2 est $\{1, 9\}$ qui est un sous-groupe de $(H, \times)$

⋆ Soit $\varphi_3 : (\mathbb{Z}/4\mathbb{Z}, +) \longrightarrow (H, \times)$ défini par :

$$\varphi_3(0) = 1 \quad \varphi_3(1) = 11 \quad \varphi_3(2) = 9 \quad \varphi_3(3) = 3$$

C'est un isomorphisme

10.14.2 Sous-groupes

Exercice 7 :

Soit $(G, *)$ un groupe. Le centre de $(G, *)$ est l'ensemble $Z(G)$ des éléments de G qui commutent avec tous les éléments de G, autrement dit : $Z(G) = \{x \in G \text{ tels que pour tout } y \in G \; x * y = y * x\}$
Il faut montrer que $Z(G)$ est un sous-groupe de $(G, *)$

1. Premièrement, $Z(G) \neq \emptyset$, puisque si $e \in G$ est le neutre, pour tout $x \in G$, nous avons $x * e = e * x$, et donc, $e \in Z(G)$
2. Secondement, montrons que si $x \in Z(G)$ et $y \in Z(G)$, alors $x * y \in Z(G)$

   Comme $x \in Z(G)$, alors, pour tout $T \in G$, nous avons $x * T = T * x$; de même pour y. Il faut donc montrer que, pour tout $T \in G$, $(x * y) * T = T * (x * y)$

   $$\begin{array}{rll} (x*y)*T = & x*(y*T) & \text{par associativité de la loi } * \\ = & x*(T*y) & \text{car } y \in Z(G) \\ = & (x*T)*y & \text{par associativité de la loi } * \\ = & (T*x)*y & \text{car } x \in Z(G) \\ = & T*(x*y) & \text{par associativité de la loi } * \end{array}$$

   Nous avons donc $(x * y) * T = T * (x * y)$
3. En troisième lieu, montrons, maintenant, que si $x \in Z(G)$, alors $x^{-1} \in Z(G)$

   Il faut donc montrer que, pour tout $T \in G$, nous avons $x^{-1} * T = T * x^{-1}$
   Posons $z = x^{-1} * T$; en composant à gauche par x, nous avons : $x * z = x * \left(x^{-1} * T\right)$.
   Par associativité, nous avons : $x * z = \left(x * x^{-1}\right) * T = e * T = T$
   Comme $x \in Z(G)$, nous avons $x * z = z * x$, ce qui fait que $T = z * x$
   Maintenant, en composant à droite par x^{-1}, nous obtenons : $T * x^{-1} = (z * x) * x^{-1} = z * \left(x * x^{-1}\right) = z * e = z$
   Nous avons donc $x^{-1} * T = z = T * x^{-1}$, ce qui montre que $x^{-1} \in Z(G)$
   Ce que nous voulions

$Z(G)$ est donc un sous-groupe de $(G, *)$

Exercice 8 :

$\mathrm{M}_2(\mathbb{R})$ est l'ensemble des matrices carrées d'ordre 2 à coefficients réels.
On considère les matrices $g(a,b) = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ avec $a \in \mathbb{R}$ et $b \in \mathbb{R}$
Soit $G = \{g(a,b)$ avec $a \in \mathbb{R}, b \in \mathbb{R}$ et $|a| \neq |b|\}$. Démontrer que G est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$

1. Tout d'abord, on démontre que $G \subset \mathrm{GL}_2(\mathbb{R})$
   Il suffit, pour cela de calculer le déterminant de $g(a,b)$. Clairement, $\det g(a,b) = a^2 - b^2 \neq 0$
2. D'autre part, la multiplication est interne ; nous avons, en effet :
$$g(a,b) \times g(c,d) = g(ac+bd, ad+bc)$$
3. D'autre part, l'inverse de $g(a,b)$ est aussi un élément de G. En effet :
$$(g(a,b))^{-1} = \frac{1}{a^2-b^2}\begin{pmatrix} a & -b \\ -b & a \end{pmatrix} = g\left(\frac{a}{a^2-b^2}, \frac{-b}{a^2-b^2}\right)$$

Exercice 9 :

1. *Comment considérer $\mathcal{S}_3$ comme sous groupe de $\mathcal{S}_4$?*

   Soit $X = \{x_1, x_2, x_3, x_4\}$ un ensemble à 4 éléments et $\mathcal{S}_4$ son groupe de permutations.
   Soit $X_3 = \{x_1, x_2, x_3\}$ un sous-ensemble de X à 3 éléments. On peut écrire $X = X_3 \cup \{x_4\}$ et nous considérons les permutations de $\mathcal{S}_4$ qui laissent $\{x_4\}$ invariant. Soit $\mathcal{U} \subset \mathcal{S}_4$ cet ensemble. Il est facile de montrer que $(\mathcal{U}, \circ)$ est un sous-groupe de $(\mathcal{S}_4, \circ)$ de cardinal 6, et donc isomorphe à $\mathcal{S}_3$
   Donc, considérer $\mathcal{S}_3$ comme sous groupe de $\mathcal{S}_4$, c'est plutôt considérer que $\mathcal{S}_3$ est isomorphe à un sous groupe de $\mathcal{S}_4$.
2. *Plus généralement, soit X un sous-ensemble d'un ensemble Y fini. Pouvons nous considérer $\mathcal{S}_X$ comme sous groupe de $\mathcal{S}_Y$?*

   La méthode est la même.
   Si $X = \{x_1, x_2, \cdots, x_n\}$ et $X_m = \{x_1, x_2, \cdots, x_m\}$ avec $m \leqslant n$, nous avons $X = X_m \cap \{x_{m+1}, x_{m+2}, \cdots, x_n\}$, et nous considérons l'ensemble $\mathcal{U}$ des permutations laissant $\{x_{m+1}, x_{m+2}, \cdots, x_n\}$ invariant.
   Comme précédemment, $(\mathcal{U}, \circ)$ est un sous-groupe de $(\mathcal{S}_n, \circ)$ de cardinal $m!$, et donc isomorphe à $\mathcal{S}_m$
   Donc, considérer $\mathcal{S}_m$ comme sous groupe de $\mathcal{S}_n$, c'est plutôt considérer que $\mathcal{S}_m$ est isomorphe à un sous groupe $(\mathcal{U}, \circ)$ de $\mathcal{S}_n$

10.14.3 Relations d'équivalence

Exercice 13 :

Soient H et K deux sous-groupes finis d'un groupe G d'élément neutre e. Si H et K sont d'ordres premiers entre eux, montrer que $H \cap K = \{e\}$.

Soient H et K deux sous-groupes d'un groupe G, d'ordres premiers entre eux.
Alors $H \cap K$ est un sous-groupe de H, et aussi un sous-groupe de K.
Par le théorème de Lagrange, l'ordre de $H \cap K$ divise à la fois l'ordre de H et celui de K.
C'est donc un diviseur commun à l'ordre de H et à l'ordre de K. Comme ils sont premiers entre eux, on en déduit que $H \cap K$ est d'ordre 1, c'est-à-dire $H \cap K = \{e\}$.

Exercice 14 :

$\mathrm{GL}_n(\mathbb{R})$ est l'ensemble des matrices inversibles de dimension n et à coefficients réels. $\mathrm{GL}_n^+(\mathbb{R})$ est le sous groupe des matrices de déterminants strictement positifs. Montrer que $\mathrm{GL}_n^+(\mathbb{R})$ est d'indice 2 dans $\mathrm{GL}_n(\mathbb{R})$

Si nous considérons la relation d'équivalence modulo $\mathrm{GL}_n^+(\mathbb{R})$, il est évident qu'il n'y a que 2 classes d'équivalences : $\mathrm{GL}_n^+(\mathbb{R})$ et $\mathrm{GL}_n^-(\mathbb{R})$, l'ensemble des matrices de $\mathrm{GL}_n(\mathbb{R})$ de déterminant négatif.
L'indice de $\mathrm{GL}_n^+(\mathbb{R})$ dans $\mathrm{GL}_n(\mathbb{R})$ est donc 2

Exercice 15 :

Soit $n \in \mathbb{N}^*$ et on appelle $F_n = \left\{q = \dfrac{a}{n} \text{ où } a \in \mathbb{Z}\right\}$. Quel est l'indice $[F_n : \mathbb{Z}]$ de $\mathbb{Z}$ dans F_n

$\Rightarrow$ Il est évident que F_n est un sous-groupe de $(\mathbb{Q}, +)$

$\Rightarrow$ Montrons que $\mathbb{Z} \subset F_n$
Soit $m \in \mathbb{Z}$; alors $m = \dfrac{m \times n}{n}$, et en posant $a = mn$, nous avons bien $m \in F_n$ et donc $\mathbb{Z} \subset F_n$.
De plus, $(\mathbb{Z}, +)$ est un sous-groupe de $(F_n, +)$

$\Rightarrow$ Pour connaitre l'indice $[F_n : \mathbb{Z}]$, il faut connaître le nombre de classes d'équivalences modulo $\mathbb{Z}$ dans F_n.
Or, si $\mathfrak{R}$ est cette relation d'équivalence, nous avons :

$$\frac{a}{n}\mathfrak{R}\frac{b}{n} \iff \frac{a}{n} - \frac{b}{n} \in \mathbb{Z} \iff (\exists k \in \mathbb{Z})\left(\frac{a}{n} - \frac{b}{n} = k\right)$$

Ainsi $\dfrac{\dot{a}}{n} = \left\{\dfrac{a}{n} + k \text{ où } k \in \mathbb{Z}\right\}$

Il n'y a que n classes d'équivalence dans cette relation d'équivalence ; elle sont du type $\dfrac{\dot{a}}{n}$ avec $0 \leqslant a \leqslant n-1$

- ⋆ Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $0 \leqslant a < b \leqslant n-1$ alors $\dfrac{\dot{a}}{n} \cap \dfrac{\dot{b}}{n} = \emptyset$
  En effet, nous n'avons pas $\dfrac{a}{n}\mathfrak{R}\dfrac{b}{n}$.
  Si nous avions $\dfrac{a}{n}\mathfrak{R}\dfrac{b}{n}$, nous arriverions à une contradiction puisque $\dfrac{a}{n} - \dfrac{b}{n} = \dfrac{a-b}{n}$ et des inégalités $0 \leqslant a < b \leqslant n-1$, nous tirons $\dfrac{1-n}{n} \leqslant \dfrac{a-b}{n} \leqslant \dfrac{n-1}{n}$; ceci montre que $\dfrac{a}{n} - \dfrac{b}{n} \notin \mathbb{Z}$, ce qui est impossible sauf si $a - b = 0$, c'est à dire si $a = b$. Il y a donc contradiction.
- ⋆ Supposons $a \geqslant n$; faisons maintenant la division euclidienne de a par n.
  Nous avons $a = un + v$ avec $0 \leqslant v \leqslant n-1$ et donc $\dfrac{a}{n} = u + \dfrac{v}{n}$, et nous avons $\dfrac{a}{n}\mathfrak{R}\dfrac{v}{n}$
- ⋆ Il n'y a donc que n classes d'équivalence qui sont du type $\dfrac{\dot{a}}{n}$ où $0 \leqslant a \leqslant n-1$

L'indice $[F_n : \mathbb{Z}]$ de $\mathbb{Z}$ dans F_n est donc n

Exercice 16 :

1. *Montrer que $(\mathbb{R}/2\pi\mathbb{Z}, +)$ et $(\mathbb{U}, \times)$ sont isomorphes*

   Nous allons construire cet isomorphisme, et cet isomorphisme est immédiat. On l'appelle donc φ.
   Nous le définissons ainsi :

$$\left\{\begin{array}{rcl} \varphi : (\mathbb{R}/2\pi\mathbb{Z}, +) & \longrightarrow & (\mathbb{U}, \times) \\ \dot{x} & \longmapsto & \varphi(\dot{x}) = e^{ix} \end{array}\right.$$

   $\Rightarrow$ φ est un homomorphisme
   En effet, soient $\dot{x} \in \mathbb{R}/2\pi\mathbb{Z}$ et $\dot{y} \in \mathbb{R}/2\pi\mathbb{Z}$; alors :

$$\varphi(\dot{x} + \dot{y}) = \varphi\left(\dot{x + y}\right) = e^{i(x+y)} = e^{ix} \times e^{iy} = \varphi(\dot{x}) \times \varphi(\dot{y})$$

   φ est donc un homomorphisme

   $\Rightarrow$ φ est injective
   Nous allons utiliser 2 modes de démonstrations
   - ⋆ Tout d'abord, soit $\dot{x} \in \ker\varphi$; alors $\varphi(\dot{x}) = 1$ et donc $e^{ix} = 1$, c'est à dire $x = 2k\pi$ où $k \in \mathbb{Z}$, c'est à dire que $x \in \dot{0}$; ainsi, $\ker\varphi = \left\{\dot{0}\right\}$ et φ est injective.

⋆ Autre façon de faire qui est très proche en termes de démonstration :
Soient $\dot{x}$ et $\dot{y}$ tels que $\varphi(\dot{x}) = \varphi(\dot{y})$. Alors :

$$\varphi(\dot{x}) = \varphi(\dot{y}) \Longleftrightarrow e^{ix} = e^{iy} \Longleftrightarrow e^{i(x-y)} = 1 \Longleftrightarrow x - y = 2k\pi \Longleftrightarrow \dot{x} = \dot{y}$$

φ est donc bien injective
$\Rightarrow$ φ est surjective
Soit $z \in \mathbb{U}$, alors $z = e^{i \arg z}$, et il existe donc dans $\mathbb{R}/2\pi\mathbb{Z}$ $\dot{x} = \arg z$ tel que $\varphi(\dot{x}) = z$
φ est donc un isomorphisme et les deux groupes $(\mathbb{R}/2\pi\mathbb{Z}, +)$ et $(\mathbb{U}, \times)$ sont isomorphes. Il est possible de définir φ^{-1} par :

$$\begin{cases} \varphi^{-1} : (\mathbb{U}, \times) & \longrightarrow & (\mathbb{R}/2\pi\mathbb{Z}, +) \\ z & \longmapsto & \varphi^{-1}(z) = \arg z \end{cases}$$

2. *Montrer que $(\mathbb{R}/2\pi\mathbb{Z}, +)$ et $(\mathbb{R}/\mathbb{Z}, +)$ sont isomorphes*

Dans un premier temps, on peut remarquer que si $x \in [0; 2\pi[$, alors $\dfrac{x}{2\pi} \in [0; 1[$ d'où une idée d'homomorphisme ψ :

$$\begin{cases} \psi : (\mathbb{R}/2\pi\mathbb{Z}, +) & \longrightarrow & (\mathbb{R}/\mathbb{Z}, +) \\ x & \longmapsto & \psi(x) = \dfrac{\dot{x}}{2\pi} \end{cases}$$

$\Rightarrow$ ψ est un homomorphisme
En effet, soient $\dot{x} \in (\mathbb{R}/2\pi\mathbb{Z}, +)$ et $\dot{y} \in (\mathbb{R}/2\pi\mathbb{Z}, +)$, alors :

$$\psi(\dot{x} + \dot{y}) = \psi\left(x \dot{+} y\right) = \frac{x \dot{+} y}{2\pi} = \frac{\dot{x}}{2\pi} + \frac{\dot{y}}{2\pi} = \psi(\dot{x}) + \psi(\dot{y})$$

ψ est donc un homomorphisme
$\Rightarrow$ ψ est un homomorphisme injectif
En effet, soient $\dot{x} \in (\mathbb{R}/2\pi\mathbb{Z}, +)$ et $\dot{y} \in (\mathbb{R}/2\pi\mathbb{Z}, +)$ tels que $\psi(\dot{x}) = \psi(\dot{y})$, alors :

$$\psi(\dot{x}) = \psi(\dot{y}) \Longleftrightarrow \frac{\dot{x}}{2\pi} = \frac{\dot{y}}{2\pi} \Longleftrightarrow \frac{x}{2\pi} = \frac{y}{2\pi} + k \text{ où } k \in \mathbb{Z} \Longleftrightarrow x = y + 2k\pi \Longleftrightarrow \dot{x} = \dot{y} \text{ dans } (\mathbb{R}/2\pi\mathbb{Z}, +)$$

Et donc ψ est bien un homomorphisme injectif
$\Rightarrow$ ψ est un homomorphisme surjectif
Soit $\dot{y} \in (\mathbb{R}/\mathbb{Z}, +)$; existe-t-il $\dot{x} \in (\mathbb{R}/2\pi\mathbb{Z}, +)$ tel que $\psi(x) = \dot{y}$
Il suffit donc de poser $\dot{x} = 2\dot{\pi}y$ et alors $\psi(x) = \psi\left(2\dot{\pi}y\right) = \dfrac{2\dot{\pi}y}{2\pi} = \dot{y}$
ψ est donc un isomorphisme et les groupes $(\mathbb{R}/2\pi\mathbb{Z}, +)$ et $(\mathbb{R}/\mathbb{Z}, +)$ sont isomorphes.

3. *Montrer que $(\mathbb{R}/\mathbb{Z}, +)$ et $(\mathbb{U}, \times)$ sont isomorphes*

Il suffit de faire les compositions $(\mathbb{R}/\mathbb{Z}, +) \xrightarrow{\psi^{-1}} (\mathbb{R}/2\pi\mathbb{Z}, +) \xrightarrow{\varphi} (\mathbb{U}, \times)$.
Nous composons ainsi 2 isomorphimes et donc $\varphi \circ \psi^{-1} : (\mathbb{R}/\mathbb{Z}, +) \longrightarrow (\mathbb{U}, \times)$ est un isomorphisme de groupes.
Il est possible d'expliciter clairement $\varphi \circ \psi^{-1}$:

$$\begin{cases} \varphi \circ \psi^{-1} : (\mathbb{R}/\mathbb{Z}, +) & \longrightarrow & (\mathbb{U}, \times) \\ x & \longmapsto & \varphi \circ \psi^{-1}(x) = e^{2i\pi x} \end{cases}$$

Les groupes $(\mathbb{R}/\mathbb{Z}, +)$ et $(\mathbb{U}, \times)$ sont bien isomorphes

Exercice 17 :

Avons nous $(2(\mathbb{Z}/12\mathbb{Z}), +)$ isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$?

Dans un premier temps, nous allons étudier $(2(\mathbb{Z}/12\mathbb{Z}), +)$, et surtout en faire sa table d'addition.

Tout d'abord $2(\mathbb{Z}/12\mathbb{Z}) = \{0, 2, 4, 6, 8, 10\}$

+	0	2	4	6	8	10
0	0	2	4	6	8	10
2	2	4	6	8	10	0
4	4	6	8	10	0	2
6	6	8	10	0	2	4
8	8	10	0	2	4	6
10	10	0	2	4	6	8

S'il existe un isomorphisme $\varphi : (2(\mathbb{Z}/12\mathbb{Z}), +) \longrightarrow (\mathbb{Z}/6\mathbb{Z}, +)$, alors $\varphi(0) = 0$, et φ est entièrement déterminé par $\varphi(1)$

⋆ Premier homomorphisme :

$$\varphi(0) = 0 \quad \varphi(1) = 2 \quad \varphi(2) = 4 \quad \varphi(3) = 6 \quad \varphi(4) = 8 \quad \varphi(5) = 10$$

Cet homomorphisme est bien un isomorphisme

⋆ Second homomorphisme :

$$\varphi(0) = 0 \quad \varphi(1) = 4 \quad \varphi(2) = 8 \quad \varphi(3) = 0 \quad \varphi(4) = 4 \quad \varphi(5) = 8$$

Cet homomorphisme n'est pas un isomorphisme, et $\text{Im}\varphi = \{0, 4, 8, \}$ qui est un sous-groupe de $(2(\mathbb{Z}/12\mathbb{Z}), +)$

⋆ Troisième homomorphisme :

$$\varphi(0) = 0 \quad \varphi(1) = 6 \quad \varphi(2) = 0 \quad \varphi(3) = 6 \quad \varphi(4) = 0 \quad \varphi(5) = 6$$

Cet homomorphisme n'est pas un isomorphisme, et $\text{Im}\varphi = \{0, 6\}$ qui est un sous-groupe de $(2(\mathbb{Z}/12\mathbb{Z}), +)$

⋆ Quatrième homomorphisme :

$$\varphi(0) = 0 \quad \varphi(1) = 8 \quad \varphi(2) = 4 \quad \varphi(3) = 0 \quad \varphi(4) = 8 \quad \varphi(5) = 4$$

Cet homomorphisme n'est pas un isomorphisme, et $\text{Im}\varphi = \{0, 4, 8\}$ qui est un sous-groupe de $(2(\mathbb{Z}/12\mathbb{Z}), +)$

Nous avons 4 homomorphismes dont un seul est un isomorphisme.
En conclusion, $(2(\mathbb{Z}/12\mathbb{Z}), +)$ est isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$

Exercice 18 :

On considère $\text{SL}_2(\mathbb{R})$ le sous-groupe de $\text{GL}_2(\mathbb{R})$ formé des matrices de déterminant $+1$
On considère les sous-groupes H et K de $\text{SL}_2(\mathbb{R})$ engendrés respectivement par

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Déterminer les éléments des espaces quotients $\text{SL}_2(\mathbb{R})/H$ et $\text{SL}_2(\mathbb{R})/K$

⇒ **Détermination de $\text{SL}_2(\mathbb{R})/H$**

Appelons C la matrice $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ Par calculs, nous obtenons $C^2 = -\text{Id}_2$, $C^3 = -C$ et $C^4 = \text{Id}_2$, de telle sorte que nous montrons que H est un groupe à 4 éléments :

$$H = \{\text{Id}_2, C, -\text{Id}_2, -C\}$$

Pour une matrice $A \in \text{SL}_2(\mathbb{R})$ avec $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $ad - bc = 1$,

⋆ La classe à gauche de A notée AH est donnée par :

$$AH = \{A, AC, -A, -AC\} \text{ avec } AC = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$$

⋆ La classe à droite de A notée HA est donnée par :

$$AH = \{A, CA, -A, -CA\} \text{ avec } CA = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix}$$

⇒ **Détermination de** $\mathrm{SL}_2(\mathbb{R})/K$

Appelons D la matrice $D = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

Par calculs, et avec une démonstration par récurrence, nous démontrons que, pour tout $n \in \mathbb{Z}$, nous avons $D^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ et donc, le groupe K est défini par :

$$K = \{D^n \text{ avec } n \in \mathbb{Z}\}$$

⋆ La classe à gauche de A notée AK est donnée par :

$$AK = \{AD^n \text{ avec } n \in \mathbb{Z}\} \text{ et } AD^n = \begin{pmatrix} a & an+b \\ c & cn+d \end{pmatrix}$$

⋆ La classe à droite de A notée KA est donnée par :

$$AK = \{D^n A \text{ avec } n \in \mathbb{Z}\} \text{ avec } D^n A = \begin{pmatrix} a+nc & b+nd \\ c & d \end{pmatrix}$$

10.14.4 Sous-groupes distingués

Exercice 21 :

Montrer que l'ensemble $\mathrm{GL}_n^+(\mathbb{R})$ des matrices de $\mathrm{GL}_n(\mathbb{R})$ de déterminant strictement positif est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$ puis qu'il est distingué dans ce groupe.

Soit donc $\mathrm{GL}_n^+(\mathbb{R})$ l'ensemble des matrices de $\mathrm{GL}_n(\mathbb{R})$ de déterminant strictement positif.

⇒ $\mathrm{GL}_n^+(\mathbb{R})$ **est un sous-groupe de** $\mathrm{GL}_n(\mathbb{R})$

⋆ Il est évident que $\mathrm{GL}_n^+(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$ et que $\mathrm{GL}_n^+(\mathbb{R}) \neq \emptyset$ puisque la matrice identité d'ordre n notée Id_n est un élément de $\mathrm{GL}_n^+(\mathbb{R})$ puisque $\det \mathrm{Id}_n = 1$

⋆ D'autre part, pour $M \in \mathrm{GL}_n^+(\mathbb{R})$ et $N \in \mathrm{GL}_n^+(\mathbb{R})$, nous avons $MN^{-1} \in \mathrm{GL}_n^+(\mathbb{R})$; en effet :

$$\det\left(MN^{-1}\right) = \det M \times \det\left(N^{-1}\right) = \det M \times (\det N)^{-1} = \frac{\det M}{\det N}$$

Comme $\det M > 0$ et $\det N > 0$, nous avons $\det\left(MN^{-1}\right) > 0$ et donc $MN^{-1} \in \mathrm{GL}_n^+(\mathbb{R})$

Cela prouve que $\mathrm{GL}_n^+(\mathbb{R})$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$

⇒ **Montrons que** $\mathrm{GL}_n^+(\mathbb{R})$ **est distingué en** $\mathrm{GL}_n(\mathbb{R})$

Il faut donc montrer que pour tout $M \in \mathrm{GL}_n(\mathbb{R})$ et tout $N \in \mathrm{GL}_n^+(\mathbb{R})$, nous avons $MNM^{-1} \in \mathrm{GL}_n^+(\mathbb{R})$, c'est à dire qu'il faut démontrer que $\det MNM^{-1} > 0$; or :

$$\det MNM^{-1} = \det M \det N \det M^{-1} = \det M \det N (\det M)^{-1} = \det N > 0$$

$\mathrm{GL}_n^+(\mathbb{R})$ est donc distingué en $\mathrm{GL}_n(\mathbb{R})$

Exercice 22 :

Soit G un groupe ; $H_1 \triangleright G$ et $H_2 \triangleright G$ 2 sous-groupes distingués en G. Est-ce que $H_1 \cap H_2$ est un sous-groupe distingué en G ?

On appelle $H = H_1 \cap H_2$.

Soit $x \in H$; alors $x \in H_1$ et $x \in H_2$. Pour tout $z \in G$, $zxz^{-1} \in H_1$ car H_1 est distingué ; de même, et pour les mêmes raisons, $zxz^{-1} \in H_2$, et donc $zxz^{-1} \in H$ et H est donc distingué en G

Exercice 23 :

Soient G et G' deux groupes et $f : G \longrightarrow G'$ un morphisme de groupes.

1. *Soit $H' \rhd G'$ un sous-groupe distingué en G'. Démontrer que $f^{-1}(H')$ est distingué en G*

   Soient $g \in G$ et $u \in f^{-1}(H')$; il faut que nous démontrions que $gug^{-1} \in f^{-1}(H')$
   Soit $z = gug^{-1}$; alors, $f(z) = f\left(gug^{-1}\right) = f(g) f(u) f(g)^{-1}$. Par construction, $f(u) \in H'$, et H' étant distingué en G', nous avons $f(g) f(u) f(g)^{-1} \in H'$, c'est à dire $f(z) \in H'$, et donc $z \in f^{-1}(H')$.
   Ce que nous voulions

2. *Démontrer que si f est surjective, alors, pour tout sous groupe $H \rhd G$ distingué en G, alors, $f(H)$ est distingué en G'*

   Il faut donc démontrer que, pour tout $x \in G'$ et tout $y \in f(H)$, nous avons $xyx^{-1} \in f(H)$
   Soit donc $x \in G'$ et $y \in f(H)$
   — f étant surjective, il existe $g \in G$ tel que $f(g) = x$, et donc $f\left(g^{-1}\right) = f(g)^{-1} = x^{-1}$
   — Il existe aussi $h \in H$ tel que $f(h) = y$
   — Donc : $xyx^{-1} = f(g) f(h) f(g)^{-1} = f\left(ghg^{-1}\right)$
   H étant distingué, $ghg^{-1} \in H$, et donc $f\left(ghg^{-1}\right) \in f(H)$, c'est à dire $xyx^{-1} \in f(H)$
   $f(H)$ est bien distingué en G'

Exercice 24 :

Soit G un groupe et $\mathfrak{R}$ une relation d'équivalence sur G.
On suppose que cette relation $\mathfrak{R}$ est compatible avec la loi de groupe, c'est à dire :

$$(\forall x \in G)(\forall y \in G)(\forall x_1 \in G)(\forall y_1 \in G)((x\mathfrak{R}y \text{ et } x_1\mathfrak{R}y_1) \Longrightarrow (xx_1\mathfrak{R}yy_1))$$

Pour nous simplifier la vie, nous appelons e l'élément neutre de G

1. *On appelle H la classe de l'élément neutre. Montrer que H est un sous-groupe distingué de G*

   Nous avons donc $H = \{x \in G \text{ tels que } x\mathfrak{R}e\}$
   — H est un sous-groupe de G
   - Tout d'abord, H est non vide puisque $e \in H$
   - Soit $x \in H$ et $y \in H$; alors, par définition, $x\mathfrak{R}e$ et $y\mathfrak{R}e$; par compatibilité de la relation $\mathfrak{R}$ avec l'opération de groupe nous avons $xy\mathfrak{R}e$
     La multiplication est donc interne dans H
   - Soit $x \in H$, alors $x\mathfrak{R}e$; de la réflexivité de la relation d'équivalence $\mathfrak{R}$, nous avons $x^{-1}\mathfrak{R}x^{-1}$, et maintenant, par compatibilité de la relation $\mathfrak{R}$ avec l'opération de groupe nous avons $xx^{-1}\mathfrak{R}ex^{-1} \Longleftrightarrow x^{-1}\mathfrak{R}e$, c'est à dire que $x^{-1} \in H$

   H est donc un sous groupe de G
   — H est un sous-groupe distingué de G
   Soient $x \in G$ et $h \in H$; il faut donc montrer que $xhx^{-1} \in H$.
   Pour commencer, $h \in H \Longleftrightarrow h\mathfrak{R}e$ et, par réflexivité de $\mathfrak{R}$, nous avons $x\mathfrak{R}x$ et $x^{-1}\mathfrak{R}x^{-1}$.
   Doinc :

   $$\begin{array}{rl} h\mathfrak{R}e \Longrightarrow & xh\mathfrak{R}xe \Longleftrightarrow xh\mathfrak{R}x \text{ Par compatibilité de la relation avec les opérations de groupe} \\ \Longrightarrow & xhx^{-1}\mathfrak{R}xx^{-1} \Longleftrightarrow xhx^{-1}\mathfrak{R} \text{ Par compatibilité de la relation avec les opérations de groupe} \end{array}$$

   Nous avons donc $xhx^{-1} \in H$
   $H = \dot{e}$ est donc un sous-groupe distingué en G

2. *Montrer que $(\forall x \in G)(\forall y \in G)\left((x\mathfrak{R}y) \Longleftrightarrow \left(yx^{-1} \in H\right)\right)$*

   La démonstration est évidente, et nous procédons par équivalence.
   Soient donc $x \in G$ et $y \in G$ tels que $x\mathfrak{R}y$. Alors :

   $$\left((x\mathfrak{R}y) \text{ et } \left(x^{-1}\mathfrak{R}x^{-1}\right) \Longleftrightarrow \left(yx^{-1}\mathfrak{R}xx^{-1}\right) \Longleftrightarrow \left(yx^{-1}\mathfrak{R}e\right) \Longleftrightarrow \left(yx^{-1} \in H\right)\right)$$

3. *Plus généralement, pour H sous-groupe distingué de G, montrer que la relation d'équivalence sur G $x\mathfrak{R}y \Longleftrightarrow xy^{-1} \in H$ est compatible avec la loi de groupe de G*

   Soient $x \in G$, $y \in G$, $z \in G$ et $t \in G$ tels que $x\mathfrak{R}y$ et $z\mathfrak{R}t$; montrons que $zx\mathfrak{R}ty$
   — Premièrement, $x\mathfrak{R}y \Longleftrightarrow xy^{-1} \in H$ et $z\mathfrak{R}t \Longleftrightarrow zt^{-1} \in H$
   — Ensuite, H étant distingué en G, nous avons $zxy^{-1}z^{-1} \in H$
   — Le produit étant interne, $\left(zxy^{-1}z^{-1}\right)\left(zt^{-1}\right) \in H$. Or :

   $$\left(zxy^{-1}z^{-1}\right)\left(zt^{-1}\right) = zxy^{-1}\left(z^{-1}z\right)t^{-1} = zxy^{-1}t^{-1} = zx\,(ty)^{-1}$$

   Donc $= zx\,(ty)^{-1} \in H$ et nous avons donc $zx\mathfrak{R}ty$
   Ce que nous voulions

Exercice 25 :

Soit G un groupe, H sous-groupe distingué de G et K sous-groupe de H

1. *On appelle $HK = \{g \in G$ tel que $g = hk$ où $h \in H$ et $k \in K\}$*

   (a) *Montrer que $HK = KH$*

   — On montre que $HK \subset KH$
   Soit $x \in HK$; il existe alors $h \in H$ et $k \in K$ tels que $x = hk$. Or, $x = kk^{-1}hk$ et le groupe H étant distingué, $k^{-1}hk = h' \in H$. Donc, $x = kh' \in KH$.
   Ainsi, $HK \subset KH$
   — On montre que $KH \subset HK$
   On démontre, avec les mêmes arguments que $KH \subset HK$ en évrivant $y = kh = khk^{-1}k$
   Donc, $HK = KH$

   (b) *Montrer que HK est un sous groupe de G*

   - HK est clairement non vide puisque $e \in HK$
   - Soient $x \in HK$ et $y \in HK$.
     Alors, il existe $h \in H$ et $k \in K$ tels que $x = hk$; de même,il existe $h' \in H$ et $k' \in K$ tels que $y = h'k'$.

     $$xy = (hk)\,(h'k') = h\left(kh'k^{-1}\right)kk'$$

     H étant distingué, nous avons $kh'k^{-1} \in H$ et donc $h\left(kh'k^{-1}\right) \in H$.
     K étant un groupe, $kk' \in K$ et nous en déduisons que $xy \in HK$
     D'autre part, $x^{-1} = k^{-1}h^{-1} = \left(k^{-1}h^{-1}\right)kk^{-1} = \left(k^{-1}h^{-1}k\right)k^{-1}$.
     Comme H est distingué, $k^{-1}h^{-1}k \in H$ et K étant un groupe, $k^{-1} \in K$, et donc $x^{-1} \in HK$

   (c) *Montrer que si, de plus, K est distingué en G, alors HK est un sous groupe distingué de G*

   Soit $z \in HK$. Alors, il existe $h \in H$ et $k \in K$ tels que $z = hk$. Soit $u \in G$; alors : $uzu^{-1} = uhku^{-1} = uhu^{-1}uku^{-1}$
   H étant distingué, $uhu^{-1} \in H$ et $uku^{-1} \in K$ et donc $uzu^{-1} \in HK$ et HK est bien distingé

   (d) *Montrer que H est un sous-groupe distingué de KH*

   Soit $u \in KH$ et $h \in H$. Il faut montrer que $uhu^{-1} \in H$.
   Il existe $k \in H$ et $h \in H$ tels que $u = kh'$; et alors :

   $$uhu^{-1} = (kh')\,h\,(kh')^{-1} = (kh')\,hh'^{-1}k^{-1} = k\left(h'hh'^{-1}\right)k^{-1}$$

   De la structure de groupe de H, $h'hh'^{-1} \in H$, et du fait que H soit distingué en G, $k\left(h'hh'^{-1}\right)k^{-1} \in H$.

   Donc, H est un sous-groupe distingué de KH

2. *Montrer que $K \cap H$ est distingué en K*

   Soit $u \in K \cap H$ et $k \in K$. Alors : $kuk^{-1} \in K$
   H étant distingué en G, alors, comme $u \in H$, $kuk^{-1} \in H$ et donc $kuk^{-1} \in K \cap H$.
   Ce que nous voulions.

Exercice 26 :

Soit G un groupe et soient $x \in G$ et $y \in G$. On appelle commutateur de x et de y, l'élément de G :

$$[x,y] = xyx^{-1}y^{-1}$$

On appelle sous-groupe dérivé de G le sous-groupe de G, noté $\mathcal{D}(G)$, engendré par les commutateurs.

1. *Montrer que $\mathcal{D}(G)$ est un sous-groupe distingué de G*

   On peut vérifier que $e = [e,e] \in \mathcal{D}(G)$ et que $([x,y])^{-1} = [y,x]$
   Il suffit en suite de démontrer que pour tout $x \in G$, $y \in G$ et $z \in G$, $z[x,y]z^{-1} \in \mathcal{D}(G)$. Nous avons :

   $$\begin{array}{rcl} z[x,y]z^{-1} = & zxyx^{-1}y^{-1}z^{-1} \\ = & \left(zxz^{-1}\right)\left(zyz^{-1}\right)\left(zx^{-1}z^{-1}\right)\left(zy^{-1}z^{-1}\right) \end{array}$$

   Il faut remarquer, ici, que :

   $$\left(zxz^{-1}\right)^{-1} = \left(z\left(xz^{-1}\right)\right)^{-1} = \left(xz^{-1}\right)^{-1}z^{-1} = \left(zx^{-1}\right)z^{-1} = zx^{-1}z^{-1}$$

   De la même manière, nous démontrerions que $\left(zyz^{-1}\right)^{-1} = zy^{-1}z^{-1}$. Et donc :

   $$\begin{array}{rcl} z[x,y]z^{-1} = & \left(zxz^{-1}\right)\left(zyz^{-1}\right)\left[\left(zxz^{-1}\right)\right]^{-1}\left[\left(zyz^{-1}\right)\right]^{-1} \\ = & \left[zxz^{-1}, zyz^{-1}\right] \end{array}$$

   Ce que nous voulions
2. *Démontrer que $G/\mathcal{D}(G)$ est un groupe abélien*

   Soient $x \in G$ et $y \in G$; alors, $[x,y] \in \mathcal{D}(G)$, et donc $\dot{\overline{[x,y]}} = \dot{e}$
   Or, $\dot{\overline{[x,y]}} = \dot{\overline{(xy)(yx)^{-1}}}$, et donc :

   $$\dot{\overline{(xy)(yx)^{-1}}} = \dot{e} \Longleftrightarrow \dot{\overline{(xy)}}\dot{\overline{(yx)^{-1}}} = \dot{e} \Longleftrightarrow \dot{\overline{(xy)}} = \dot{\overline{(yx)}}$$

   Et, pour finir :

   $$\dot{x}\dot{y} = \dot{\overline{(xy)}} = \dot{\overline{(yx)}} = \dot{y}\dot{x}$$

   $G/\mathcal{D}(G)$ est donc un groupe abélien
3. *Soit $H \triangleright G$ un sous-groupe distingué de G. Montrer que G/H est abélien si et seulement si $\mathcal{D}(G) \subset H$*

   Nous allons procéder par équivalence. Soient $\dot{x} \in G/H$ et $\dot{y} \in G/H$.

   $$\begin{array}{rcl} G/H \text{ abélien} & \Longleftrightarrow & \dot{x}\dot{y} = \dot{y}\dot{x} \\ & \Longleftrightarrow & \dot{\overline{xy}} = \dot{\overline{yx}} \\ & \Longleftrightarrow & xy(yx)^{-1} \in H \\ & \Longleftrightarrow & xyx^{-1}y^{-1} \in H \\ & \Longleftrightarrow & [x,y] \in H \\ & \Longleftrightarrow & \mathcal{D}(G) \subset H \end{array}$$

   Ce que nous voulions

Exercice 27 :

Soit G un groupe et $A \subset G$, une partie de G. On note :
- *$N(A) = \{x \in G$ tels que $xA = Ax\}$. $N(A)$ est le* **normalisateur** *de A*
- *$C(A) = \{x \in G$ tels que pour tout $a \in A$ $ax = xa\}$. $C(A)$ est le* **centralisateur** *de A*

Pour simplifier, nous appelons e l'élément neutre de G

1. *Montrer que $N(A)$ est un sous-groupe de G*

— Tout d'abord, $N(A) \neq \emptyset$ puisque $e \in N(A)$: nous avons $A = eA = Ae$
— Soient $x \in N(A)$ et $y \in N(A)$; Il faut montrer que $xy \in N(A)$.
Nous avons $xA = Ax$ et $yA = Ay$; il faut donc montrer que $xyA = Axy$.
Soit $z \in xyA$; il existe donc $a \in A$ tel que $z = (xy)\,a$.
De l'associativité, nous avons : $z = (xy)\,a = x\,(ya)$. Comme $yA = Ay$, il existe $a_1 \in A$ tel que $ya = a_1 y$, et donc

$$z = (xy)\,a = x\,(ya) = x\,(a_1 y) = (xa_1)\,y$$

Toujours, parce que $xA = Ax$, il existe $a_2 \in A$ tel que $xa_1 = a_2 x$, et donc

$$z = (xy)\,a = x\,(ya) = x\,(a_1 y) = (xa_1)\,y = (a_2 x)\,y = a_2\,(xy)$$

On démontre ainsi que $z \in Axy$ et que donc $xyA \subset Axy$
On démontrerait, de même que $Axy \subset xyA$, et que donc $xyA = Axy$ et donc $xy \in N(A)$
— Soit $x \in N(A)$; il faut montrer que $x^{-1} \in N(A)$.
Nous avons $xA = Ax$; il faut donc montrer que $x^{-1}A = Ax^{-1}$.
Soit $z \in x^{-1}A$; il existe donc $a \in A$ tel que $z = x^{-1}a$. Or :

$$z = x^{-1}a = x^{-1}a\left(xx^{-1}\right) = x^{-1}\,(ax)\,x^{-1}$$

Comme $xA = Ax$, il existe $a_1 \in A$ tel que $ax = xa_1$, et donc :

$$z = x^{-1}a = x^{-1}a\left(xx^{-1}\right) = x^{-1}\,(ax)\,x^{-1} = x^{-1}\,(xa_1)\,x^{-1} = \left(x^{-1}x\right)a_1x^{-1} = a_1x^{-1}$$

Donc, $z \in Ax^{-1}$, et nous venons de montrer que $x^{-1}A \subset Ax^{-1}$
Nous démontrerions de la même manière que $Ax^{-1} \subset x^{-1}A$, et donc, si $x \in N(A)$, alors $x^{-1}A = Ax^{-1}$ et $x^{-1} \in N(A)$
On vient de montrer que $N(A)$ est un sous-groupe de G

2. *Montrer que $C(A)$ est un sous-groupe distingué de $N(A)$*
— On montre, tout d'abord que $C(A)$ est un sous-groupe de G
• Premièrement, $C(A) \neq \emptyset$ puisque $e \in C(A)$
• Soient $x \in C(A)$ et $y \in C(A)$; il faut montrer que $xy \in C(A)$
Soit $a \in A$; alors,

$$(xy)\,a = x\,(ya) = x\,(ay) = (xa)\,y = (ax)\,y = a\,(xy)$$

Donc xy commute avec tous les éléments de A, et donc $xy \in C(A)$
• Soient $x \in C(A)$; il faut montrer que $x^{-1} \in C(A)$
Soit $a \in A$; alors,

$$x^{-1}a = \left(x^{-1}a\right)\left(xx^{-1}\right) = x^{-1}\,(ax)\,x^{-1} = x^{-1}\,(xa)\,x^{-1} = \left(x^{-1}x\right)ax^{-1} = ax^{-1}$$

Donc $x^{-1} \in C(A)$
On vient donc de montrer que $C(A)$ est un sous-groupe de G
— On termine, par montrer que $C(A)$ est un sous-groupe distingué de $N(A)$
Soit $y \in N(A)$ et $c \in C(A)$; il faut donc montrer que $ycy^{-1} \in C(A)$
Soit $a \in A$; nous avons $\left(ycy^{-1}\right)a = (yc)\left(y^{-1}a\right)$.
Comme $y \in N(A)$, nous avons aussi $y^{-1} \in N(A)$ et il existe donc $a_1 \in A$ tel que $y^{-1}a = a_1y^{-1}$.
A ce moment, il faut faure remarquer que :

$$y^{-1}a = a_1y^{-1} \Longleftrightarrow a = ya_1y^{-1} \Longleftrightarrow ay = ya_1$$

En repremant $\left(ycy^{-1}\right)a = (yc)\left(y^{-1}a\right)$, nous avons :

$$\left(ycy^{-1}\right)a = (yc)\left(y^{-1}a\right) = (yc)\left(a_1y^{-1}\right) = y\,(ca_1)\,y^{-1} = y\,(a_1c)\,y^{-1} = (ya_1)\,cy^{-1} = aycy^{-1}$$

Donc $ycy^{-1} \in C(A)$ et $C(A)$ est un sous-groupe distingué de $N(A)$

3. *Démontrez que si $H \triangleright G$ est un sous-groupe distingué de G, alors $C(H)$ est aussi un sous-groupe distingué de G*

   D'après la question précédente, on sait que $C(H)$ est un sous-groupe de G. La différence avec la question précédente est de montrer que $C(H)$ est aussi un sous-groupe distingué de G avec l'hypothèse supplémentaire que $H \triangleright G$ est un sous-groupe distingué de G
   Soit $g \in G$ et $c \in C(H)$; il faut donc démontrer que $gcg^{-1} \in C(H)$.
   Soit donc $h \in H$. Alors :

$$\left(gcg^{-1}\right) h = \left(gcg^{-1}\right) h \left(gg^{-1}\right) = gc\left(g^{-1}hg\right) g^{-1}$$

   H est distingué en G, et donc $g^{-1}hg \in H$, et comme $c \in C(H)$, nous avons $c\left(g^{-1}hg\right) = \left(g^{-1}hg\right) c$.
   En remplaçant, nous avons :

$$\left(gcg^{-1}\right) h = gc\left(g^{-1}hg\right) g^{-1} = g\left(g^{-1}hg\right) cg^{-1} = \left(gg^{-1}\right) hgcg^{-1} = h\left(gcg^{-1}\right)$$

   Nous avons donc bien $gcg^{-1} \in C(H)$ et $C(H)$ est un sous-groupe distingué de G

10.14.5 Décomposition canonique d'un morphisme

Exercice 28 :

On considère une groupe G tel qu'il existe $n \in \mathbb{N}^*$ tel que $(\forall (x,y) \in G \times G)\left((xy)^n = x^n y^n\right)$
- *On note $G^{(n)} = \{y \in G$ tels que $\exists g \in G$ tel que $y = g^n\}$*
- *Et on note $G_{(n)} = \{x \in G$ tels que $x^n = e\}$ où e est le neutre de G.*

Vérifier que $G_{(n)}$ et $G^{(n)}$ sous des sous groupes distingués de G. Démontrez que $G/G_{(n)}$ est isomorphe à $G^{(n)}$

1. On montre que $G_{(n)}$ est un sous groupe distingué de G
   - $G_{(n)}$ est un sous groupe de G
     - $G_{(n)}$ est non vide puisque $e \in G_{(n)}$; en effet, $e^n = e$
     - Soit $x \in G_{(n)}$ et $y \in G_{(n)}$. Montrons que $xy^{-1} \in G_{(n)}$

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

     $G_{(n)}$ est donc un sous groupe de G
   - $G_{(n)}$ est distingué en G
     Soit $g \in G$ et $x \in G_{(n)}$. Montrons que $gxg^{-1} \in G_{(n)}$

$$\left(gxg^{-1}\right)^n = g^n\left(xg^{-1}\right)^n = g^n x^n\left(g^{-1}\right)^n = g^n\left(g^{-1}\right)^n = \left(gg^{-1}\right)^n = e$$

     Donc $gxg^{-1} \in G_{(n)}$

   $G_{(n)}$ est donc un sous groupe distingué de G
2. On montre que $G^{(n)}$ est un sous groupes distingués de G
   - $G^{(n)}$ est un sous groupe de G
     - $G^{(n)}$ est non vide puisque $e \in G_{(n)}$; en effet, $e^n = e$
     - Soit $x \in G^{(n)}$ et $y \in G^{(n)}$. Montrons que $xy^{-1} \in G^{(n)}$
       Il existe donc $g \in G$ et $g_1 \in G$ tels que $x = g^n$ et $y = g_1^n$. Donc :

$$xy^{-1} = g^n\left(g_1^{-1}\right)^n = \left(gg_1^{-1}\right)^n$$

       Il existe donc $u \in G$, $u = gg_1^{-1}$ tel que $xy^{-1} = u^n$. Donc, $xy^{-1} \in G^{(n)}$

     $G^{(n)}$ est donc un sous groupe de G
   - $G^{(n)}$ est distingué en G
     Soit $g \in G$ et $u \in G^{(n)}$. Montrons que $gug^{-1} \in G^{(n)}$
     Il existe $x \in G$ tel que $u = x^n$ et $gug^{-1} = gx^n g^{-1}$. Or,

$$\begin{array}{rcll}\left(gxg^{-1}\right)^n = & \left(gxg^{-1}\right)\left(gxg^{-1}\right)\cdots\left(gxg^{-1}\right) & n\text{fois} \\ = & gx\left(g^{-1}g\right)x\left(g^{-1}g\right)x\cdots\left(g^{-1}g\right)xg^{-1} & n\text{fois} \\ = & gx^n g^{-1} & \end{array}$$

Donc, $gug^{-1} = gx^n g^{-1} = \left(gxg^{-1}\right)^n$, et $gug^{-1} \in G^{(n)}$
$G^{(n)}$ est donc un sous groupe distingué de G

3. On montre que $G/G_{(n)}$ est isomorphe à $G^{(n)}$
On considère l'homomorphisme $f : G \longrightarrow G$ tel que $f(x) = x^n$. D'après le théorème de décomposition, $G/\ker f$ est isomorphe à $f(G)$. Or, ici :
— $\ker f = G_{(n)}$
— $f(G) = \text{Im} f = G^{(n)}$
Nous avons donc bien $G/G_{(n)}$ isomorphe à $G^{(n)}$

10.14.6 Groupes cycliques

Exercice 29 :

Soit G un groupe commutatif d'ordre n. On appelle $\mathcal{R}$ la relation :

$$(\forall x \in G)\,(\forall y \in G)\,(x\mathcal{R}y \Longleftrightarrow x \text{ et } y \text{ ont le même ordre})$$

$\mathcal{R}$ est une relation d'équivalence
On appelle $\psi(d)$ le nombre d'éléments d'ordre d de G. Montrer qu'alors on a : $n = \sum_{d|n} \psi(d)$

Montrer que $\mathcal{R}$ est une relation d'équivalence ne pose aucune difficulté. L'ensemble des classes d'équivalences $G/\mathcal{R}$ forme une partition de G. Si C_d est la classe d'équivalence :

$$C_d = \{x \in G \text{ tel que } x \text{ est d'ordre } d\}$$

Nous avons $\bigcup_{d|n} C_d = G$, et si $\psi(d) = \text{Card}\, C_d$, nous avons $\text{Card}\, G = n = \sum_{d|n} \psi(d)$

Exercice 30 :

Soit G un groupe cyclique d'ordre n, de générateur $g \in G$ et d'élément neutre $e \in G$.

1. *Montrer que, pour tout $k \in \mathbb{N}$, nous avons* $\text{Card}\,\langle g^k\rangle = \dfrac{n}{\text{pgcd}(n,k)}$ Nous allons procéder par petits pas.
   (a) Premier pas, c'est que $\langle g^k\rangle$ est le sous-groupe de G engendré par les puissances de g^k
   (b) Soit q le pgcd de n et k ; autrement dit $q = \text{pgcd}(n,k)$; nous avons $q \leqslant k$ et nous allons montrer que $\langle g^k\rangle = \langle g^q\rangle$
   → Il existe $q_1 \in \mathbb{N}$ tel que $k = qq_1$ et $q_2 \in \mathbb{N}$ tel que $n = qq_2$
   Alors $g^k = g^{qq_1} = (g^q)^{q_1}$ et donc g^k apparaît comme une puissance de de g^q et donc $g^k \in \langle g^q\rangle$ et donc $\langle g^k\rangle \subset \langle g^q\rangle$
   → D'après le théorème de Bezout, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $q = ku + nv$, et donc :
   $$g^q = g^{ku+nv} = g^{ku} \times g^{nv} = \left(g^k\right)^u \times (g^n)^v = \left(g^k\right)^u \text{ puisque } g^n = e$$
   Ainsi, nous avons $g^q = \left(g^k\right)^u$ et g^q apparaît donc comme une puissance de g^k.
   Nous en tirons donc $g^q \in \langle g^k\rangle$ et donc $\langle g^q\rangle \subset \langle g^k\rangle$
   → Ainsi, finalement $\langle g^q\rangle = \langle g^k\rangle$
   (c) Ainsi, $\langle g^k\rangle$ est d'ordre q_2 et nous avons donc :
   $$\text{Card}\,\langle g^k\rangle = q_2 = \frac{qq_2}{q} = \frac{n}{\text{pgcd}(n,k)}$$

2. *En déduire que si k et n sont premiers entre eux, alors $\langle g^k\rangle = G$*
   (a) Supposons que $\text{pgcd}(n,k) = 1$, alors $\text{Card}\,\langle g^k\rangle = \dfrac{n}{1} = n$ et donc $\langle g^k\rangle = G$
   (b) Réciproquement, supposons que k et n ne soient pas premiers entre eux, et soit $q = \text{pgcd}(n,k)$; alors, $q > 1$ et d'après la formule $\text{Card}\,\langle g^k\rangle = \dfrac{n}{\text{pgcd}(n,k)}$, nous avons $\text{Card}\,\langle g^k\rangle < n$ et donc, sûrement $\langle g^k\rangle \neq G$
   D'où le résultat

10.14.7 Groupes de permutations

Exercice 33 :

Cet exercice est très simple et d'applications directes vues en cours
Nous nous plaçons dans $\mathcal{S}_9$. Nous considérons les permutations suivantes :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 7 & 6 & 5 & 4 & 8 & 9 & 3 & 1 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 7 & 2 & 4 & 1 & 9 & 8 & 3 \end{pmatrix}$$

1. $\Rightarrow$ *Calculer $\sigma_1 \circ \sigma_2$,*

   On donne simplement le résultat :

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 8 & 9 & 7 & 5 & 2 & 1 & 3 & 6 \end{pmatrix}$$

   $\Rightarrow$ *Calculer $\sigma_2 \circ \sigma_1$,*

   A nouveau, un simple résultat :

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 9 & 1 & 4 & 2 & 8 & 3 & 7 & 5 \end{pmatrix}$$

   $\Rightarrow$ *Calculer σ_1^{-1}*

   Tout de suite, donc :

$$\sigma_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 9 & 1 & 8 & 5 & 4 & 3 & 2 & 6 & 7 \end{pmatrix}$$

   $\Rightarrow$ *Calculer σ_2^{-1}*

$$\sigma_2^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 4 & 9 & 5 & 1 & 2 & 3 & 8 & 7 \end{pmatrix}$$

2. *Décomposer σ_1 et σ_2 en produit de cycles à supports deux à deux disjoints*

   Très simple :
   $\Rightarrow$ $\sigma_1 = (1\,2\,7\,9)\,(3\,6\,8)\,(4\,5)$
   $\Rightarrow$ $\sigma_2 = (1\,5\,4\,2\,6)\,(3\,7\,9)$

3. *Donner une factorisation de σ_1 en produit de transpositions. Même question pour σ_2*

   $\Rightarrow$ $\sigma_1 = (1\,9)\,(1\,7)\,(1\,2)\,(3\,8)\,(3\,6)\,(4\,5)$
   $\Rightarrow$ $\sigma_2 = (1\,6)\,(1\,2)\,(1\,4)\,(1\,5)\,(3\,9)\,(3\,7)$

Exercice 34 :

Encore un exercice d'applications directes
Nous nous plaçons, cette fois ci dans $\mathcal{S}_7$. Nous considérons les cycles suivants :

$$c_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 7 & 6 & 1 & 5 & 4 & 3 \end{pmatrix} \qquad c_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 3 & 4 & 2 & 1 & 7 \end{pmatrix}$$

1. *Calculer $c_1 \circ c_2$ et $c_2 \circ c_1$*

$$c_1 \circ c_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 4 & 6 & 1 & 7 & 2 & 3 \end{pmatrix} \qquad c_2 \circ c_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 7 & 1 & 5 & 2 & 4 & 3 \end{pmatrix}$$

   On vérifie ici, la non-commutativité de la composition dans $\mathcal{S}_n$

2. *Calculer le carré $c_1^2 = c_1 \circ c_1$ de c_1. Est-ce un cycle ?*

$$c_1 \circ c_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 3 & 4 & 2 & 5 & 1 & 6 \end{pmatrix}$$

   c_1^2 n'est pas un cycle, mais un produit de cycles ; nous avons : $c_1^2 = (1\,7\,6)\,(2\,3\,4)$

Exercice 35 :

On appelle centre de $\mathcal{S}_n$ l'ensemble $Z(\mathcal{S}_n)$ des permutations qui commutent avec toutes les permutations de $\mathcal{S}_n$:

$$Z(\mathcal{S}_n) = \{\sigma \in \mathcal{S}_n \text{ tels que pour tout } s \in \mathcal{S}_n \text{ tel que } s \circ \sigma = \sigma \circ s\}$$

L'objet de cet exercice est de montrer que $Z(\mathcal{S}_n) = \{\mathrm{Id}_{\mathbb{N}_n}\}$ si $n \geqslant 3$.
Supposons donc $n \geqslant 3$ et soient $\sigma \in Z(\mathcal{S}_n)$, $i \in \mathbb{N}_n$, $j \in \mathbb{N}_n$ tels que $i \neq j$. On pose τ la transposition telle que $\tau(i) = j$

1. *Montrer que $(\tau\sigma)(i) = \sigma(j)$*

   Pas très difficile !!
   Comme $\sigma \in Z(\mathcal{S}_n)$, σ commute avec τ et nous avons alors $\sigma \circ \tau = \tau \circ \sigma$ et donc :

$$\tau[\sigma(i)] = (\tau\sigma)(i) = (\sigma\tau)(i) = \sigma[\tau(i)] = \sigma(j)$$

   Par la même démonstration, nous avons $\tau[\sigma(j)] = (\tau\sigma)(j) = \sigma(i)$

2. *En déduire $\sigma(i) \in \{i, j\}$*

   Par la question précédente,nous avons démontré que τ « échangeait » $\sigma(i)$ et $\sigma(j)$.
   D'autre part, σ est une bijection de $\mathcal{S}_n$ et est, entre autres, une injection, c'est à dire que, comme $i \neq j$, nous avons $\sigma(i) \neq \sigma(j)$, ce qui veut dire que $\sigma(i)$ et $\sigma(j)$ sont dans le support de τ et que donc $\sigma(i) \in \{i, j\}$

3. *Démontrer que $\sigma(i) = i$. Conclure.*

   Comme $n \geqslant 3$, il existe $k \in \mathbb{N}_n \setminus \{i, j\}$; c'est à dire que $k \neq i$ et $k \neq j$.
   Considérons la transposition $\tau_{i,k} = (i\,k)$ qui « échange » i et k.
   Par la question précédente, nous avons, à nouveau, $\sigma(i) \in \{i, k\}$ et donc $\sigma(i) \in \{i, j\} \cap \{i, k\}$.
   Comme les nombres i, j et k sont tous différents, alors $\sigma(i) = i$
   Ainsi, pour tout $i \in \mathbb{N}_n$, $\sigma(i) = i$, nous avons donc $\sigma = \mathrm{Id}_{\mathbb{N}_n}$ et donc $Z(\mathcal{S}_n) = \{\mathrm{Id}_{\mathbb{N}_n}\}$

4. *Que se passe-t-il si $n = 2$?*

   Nous venons de résoudre la question pour $n \geqslant 3$. $\mathcal{S}_2$ n'est composé que de 2 permutations : $\mathrm{Id}_{\mathbb{N}_2}$ et de la transposition $\tau_{1,2} = (1\,2)$.
   Bien entendu, ces permutations commutent et nous avons $Z(\mathcal{S}_2) = \{\mathrm{Id}_{\mathbb{N}_2}, \tau_{1,2}\}$

Exercice 36 :

Soit $\sigma \in \mathcal{S}_5$ défini par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

1. *Ecrire la décomposition de σ en produit de cycles de supports disjoints.*

   Pas difficile ; $\sigma = (1\,5\,3)\,(2\,4)$
   Dans la suite, nous appellerons $c = (1\,5\,3)$ et $\tau = (2\,4)$, et donc $\sigma = c\tau = \tau c$
   c est un cycle de longueur 3 et τ, un cycle de longueur 2
2. *Donner la liste des éléments de $\Gamma(\sigma)$ le sous-groupe engendré par σ*

   L'ordre de σ est le ppcm de l'ordre de c et de τ ; l'ordre de σ est donc de 6. Nous avons donc :

$$\Gamma(\sigma) = \left\{\mathrm{Id}_{\mathbb{N}_5}\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\right\}$$

   Plus précisément :

   ⋆ $\sigma = c\tau$
   ⋆ $\sigma^2 = c^2\tau^2 = c^2$
   ⋆ $\sigma^3 = c^3\tau^3 = \tau$
   ⋆ $\sigma^4 = c^4\tau^4 = c$
   ⋆ $\sigma^5 = c^5\tau^5 = c^2\tau$
   ⋆ $\sigma^6 = c^6\tau^6 = \mathrm{Id}_{\mathbb{N}_5}$

Exercice 37 :

Donner, si c'est possible, un exemple d'élément d'ordre 30 dans le groupe symétrique $\mathcal{S}_{10}$

Voilà un nouvel exercice d'application directe.
$\sigma = (1\,2\,3\,4\,5)\,(6\,7\,8)\,(9\,10)$ convient, car σ est de type 2, 3, 5, et donc son ordre est $\mathrm{PPCM}(2,3,5) = 30$

Exercice 38 :

Montrer que si c et c_1 sont deux cycles dans $\mathcal{S}_n$ de même longueur k, il existe $\sigma \in \mathcal{S}_n$ tel que $c_1 = \sigma \circ c \circ \sigma^{-1}$
La démonstration va se faire en 2 temps ; le premier est une redite de démonstrations ou d'exemple nécessaire pour le second temps qui répond à laq uestion posée
Nous nous situons toujours dans $\mathbb{N}_n$ et nous considérons toujours $\mathcal{S}_n$ l'ensemble des permutations de $\mathbb{N}_n$

1. Soit $c = (a_1\,a_2\,\cdots\,a_k)$ un cycle de longueur k. Pour chaque j tel que $1 \leqslant j \leqslant k$, nous avons $a_j \in \mathbb{N}_n$
   Nous allons montrer que, pour toute permutation $\sigma \in \mathcal{S}_n$, nous avons $\sigma \circ c \circ \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \cdots \sigma(a_k))$ qui est une permutation circulaire de longueur k aussi.

   Commençons par traiter un exemple pour $n = 7$
   ⋆ Soit $c = (2\,4\,6)$ qui peut aussi s'exprimer par :

$$c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 6 & 5 & 2 & 7 \end{pmatrix}$$

   c est un cycle de longueur 3
   ⋆ Soit $\sigma \in \mathcal{S}_7$ la permutation suivante : $\sigma = (2\,3\,4)\,(5\,6)$ qui peut aussi s'écrire :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 4 & 2 & 6 & 5 & 7 \end{pmatrix}$$

   Alors :

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 2 & 3 & 6 & 5 & 7 \end{pmatrix}$$

   Et :

$$\sigma \circ c \circ \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 5 & 2 & 4 & 3 & 6 & 7 \end{pmatrix} = (2\,5\,3)$$

   $\sigma \circ c \circ \sigma^{-1}$ est donc un cycle de longueur 3
   ⋆ Nous avons $\sigma \circ c \circ \sigma^{-1} = (2\,5\,3) = (\sigma(4)\ \sigma(6)\ \sigma(2)) = (\sigma(2)\ \sigma(4)\ \sigma(6))$

Retour à la démonstration

Soit donc $\sigma \in \mathcal{S}_n$ une permutation de $\mathbb{N}_n$

$\Rightarrow$ Soit $i \in \mathbb{N}_n$ tel que $i \notin \{\sigma(a_1), \sigma(a_2), \cdots \sigma(a_k)\}$.
Alors, $\sigma^{-1}(i) \notin \{a_1, a_2, \cdots, a_k\}$, puisque, sinon, $i = \sigma \circ \sigma^{-1}(i) \in \{\sigma(a_1), \sigma(a_2), \cdots \sigma(a_k)\}$, ce qui est contradictoire.
Ainsi, $\sigma^{-1}(i)$ n'appartient pas au support de c et donc $c\left(\sigma^{-1}(i)\right) = \sigma^{-1}(i)$ et donc

$$\sigma\left[c\left(\sigma^{-1}(i)\right)\right] = \sigma\left[\sigma^{-1}(i)\right] = i$$

Et donc i est invariant par $\sigma c \sigma^{-1}$

$\Rightarrow$ Soit, maintenant, $i \in \mathbb{N}_n$ tel que $i \in \{\sigma(a_1), \sigma(a_2), \cdots \sigma(a_k)\}$.
Il existe donc $j_0 \in \{1, 2, \cdots, k\}$ tel que $i = \sigma(a_{j_0})$, et σ étant une bijection, nous avons $i = \sigma(a_{j_0}) \Longleftrightarrow \sigma^{-1}(i) = a_{j_0}$.
Ainsi, si $1 \leqslant j_0 \leqslant k-1$:

$$\sigma \circ c \circ \sigma^{-1}(i) = \sigma[c(a_{j_0})] = \sigma(a_{j_0+1})$$

Et si $j_0 = k$,

$$\sigma \circ c \circ \sigma^{-1}(i) = \sigma[c(a_k)] = \sigma(a_1)$$

Et donc $\sigma \circ c \circ \sigma^{-1}$ est le cycle $\sigma \circ c \circ \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2) \cdots \sigma(a_{k-1})\ \sigma(a_k))$

2. Soit, maintenant $c_1 = (b_1\, b_2\, \cdots\, b_k)$ un cycle de longueur k où, pour tout i tel que $1 \leqslant i \leqslant k$, $b_i \in \mathbb{N}_n$. Il nous faut donc trouver $\sigma \in \mathcal{S}_n$ tel que $c_1 = \sigma \circ c \circ \sigma^{-1}$
$\Rightarrow$ Nous avons $c = (a_1\, a_2\, \cdots\, a_k)$, et d'après la question précédente,

$$\sigma \circ c \circ \sigma^{-1} = (\sigma(a_1)\ \sigma(a_2) \cdots \sigma(a_{k-1})\ \sigma(a_k))$$

$\Rightarrow$ Nous construisons donc une permutation $\sigma \in \mathcal{S}_n$ telle que :

$$\begin{cases} \sigma(a_i) = b_i \text{ si } 1 \leqslant i \leqslant k \\ \sigma(x) = x \text{ si } x \in \mathbb{N}_n \setminus \{a_1, a_2, \ldots, a_k\} \end{cases}$$

σ est bien une permutation de $\mathbb{N}_n$ (i.e. $\sigma \in \mathcal{S}_n$) et nous avons bien $c_1 = \sigma \circ c \circ \sigma^{-1}$
De plus nous avons support $(c_1) = \{b_1, \ldots, b_k\} = \{\sigma(a_1)\ \sigma(a_2) \cdots \sigma(a_{k-1})\ \sigma(a_k)\} = \sigma(\text{support}(c))$.

Exercice 39 :

Montrer que le produit de deux transpositions distinctes est un cycle de longueur 3 ou un produit de deux cycles de longueur 3.

1. Soit τ_1 la transposition $\tau_1 = (a\, b)$ et τ_2 la transposition $\tau_2 = (b\, c)$. Alors :
   - ⋆ Evaluons $\tau_1 \circ \tau_2$:
     - → $\tau_1 \circ \tau_2(a) = \tau_1(a) = b$
     - → $\tau_1 \circ \tau_2(b) = \tau_1(c) = c$
     - → $\tau_1 \circ \tau_2(c) = \tau_1(b) = a$

     Et donc $\tau_1 \circ \tau_2 = (a\, b\, c)$
   - ⋆ Pour aller plus loin, nous évaluons $\tau_2 \circ \tau_1$:
     - → $\tau_2 \circ \tau_1(a) = \tau_2(b) = c$
     - → $\tau_2 \circ \tau_1(b) = \tau_2(a) = a$
     - → $\tau_2 \circ \tau_1(c) = \tau_2(c) = b$

     Et donc $\tau_2 \circ \tau_1 = (a\, c\, b)$
2. Nous continuons, maintenant, en supposant que τ_1 et τ_2 n'aient aucun élément en commun.
   Soit donc τ_1 la transposition $\tau_1 = (a\, b)$ et τ_2 la transposition $\tau_2 = (c\, d)$.
   On considère la transposition $\mathcal{T} = (c\, b)$; remarquons que nous prenons un élément dans chaque support des tanspositions τ_1 et τ_2. En remarquant, en outre que $\mathcal{T}^2 = \mathcal{T} \circ \mathcal{T} = \text{Id}_{\mathbb{N}_n}$, nous avons :

$$\tau_1 \circ \tau_2 = \tau_1 \circ \mathcal{T} \circ \mathcal{T} \circ \tau_2 = (\tau_1 \circ \mathcal{T}) \circ (\mathcal{T} \circ \tau_2) = ((a\, b)\,(c\, b))\,((c\, b)\,(c\, d)) = (a\, b\, c)\,(c\, d\, b)$$

   Ainsi $\tau_1\tau_2 = (a\, b)\,(c\, d)$ est-il le produit de deux cycles de longueur 3.

10.14.8 Automorphisme d'un groupe

Exercice 40 :

Soit G un groupe. Démontrer que $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}(G)$

Soit $f \in \mathrm{Aut}(G)$. Il faut donc démontrer que, pour tout $\alpha_x \in \mathrm{Int}(G)$, nous avons $f \circ \alpha_x \circ f^{-1} \in \mathrm{Int}(G)$,
Soit $g \in G$, alors :

$$\begin{array}{rcl} f \circ \alpha_x \circ f^{-1}(g) = & f\left[\alpha_x\left(f^{-1}(g)\right)\right] & \\ = & f\left[xf^{-1}(g)\,x^{-1}\right] & \text{par définition de } \alpha_x \\ = & f(x)\,f\left(f^{-1}(g)\right)f\left(x^{-1}\right) & \text{parce que } f \text{ est un morphisme} \\ = & f(x)\,f\left(f^{-1}(g)\right)f(x)^{-1} & \text{toujours parce que } f \text{ est un morphisme} \\ = & f(x)\,gf(x)^{-1} & \text{parce que } f \text{ est un automorphisme} \\ = & \alpha_{f(x)}(g) & \end{array}$$

On vient donc de démontrer que pour tout $f \in \mathrm{Aut}(G)$ et tout $\alpha_x \in \mathrm{Int}(G)$, nous avons $f \circ \alpha_x \circ f^{-1} = \alpha_{f(x)}$ et que donc, $f \circ \alpha_x \circ f^{-1} \in \mathrm{Int}(G)$
$\mathrm{Int}(G)$ est donc un sous-groupe distingué de $\mathrm{Aut}(G)$

10.14.9 Groupe opérant dans un ensemble

Exercice 42 :

Soit G un groupe d'ordre 21 agissant sur un ensemble E à $n \geqslant 1$ éléments.

1. *Quel est le cardinal possible de chaque orbite ?*

   Ici, c'est une application directe de 10.12.6.
   Le cardinal est donc un diviseur de l'ordre de G. Les diviseurs de 21 étant $1, 3, 7, 21$, le carinal possible de chaque orbite est donc $1, 3, 7, 21$

2. *Notons N_i le nombre d'orbites à i éléments, pour $i \geqslant 1$. En utilisant la partition de E en orbites, trouver une relation entre les N_i.*

   La question était posée de telle manière que, par l'énoncé, l'étudiant ne devine pas le résultat de la question 1 !!
   Ainsi, il y a N_1 orbites à 1 élément, N_3 orbites à 3 éléments, N_7 orbites à 7 éléments et N_{21} orbites à 21 éléments.
   Les orbites formant une partition de E, nous avons :

$$n = N_1 + 3N_3 + 7N_7 + 21N_{21}$$

Exercice 43 :

Considérons le groupe spécial linéaire $\mathrm{SL}_2(\mathbb{R})$ des matrices de déterminant 1, c'est à dire :

$$\mathrm{SL}_2(\mathbb{R}) = \{M \in \mathrm{GL}_2(\mathbb{R}) \text{ tel que } \det M = 1\}$$

On considère le **demi-plan de Poincaré** *:*

$$\mathcal{H} = \{z \in \mathbb{C} \text{ tel que } \mathrm{Im}(z) > 0\}$$

$\mathbb{C}^{\mathcal{H}}$ désigne les applications de $\mathcal{H}$ dans $\mathbb{C}$

1. *On considère l'application $\Phi : \mathrm{SL}_2(\mathbb{R}) :\longrightarrow \mathbb{C}^{\mathcal{H}}$ définie par :*

$$\left\{\begin{array}{rcl} \Phi : \mathrm{SL}_2(\mathbb{R}) : & \longrightarrow & \mathbb{C}^{\mathcal{H}} \\ M & \longmapsto & \Phi(M) \end{array}\right.$$

où, si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\Phi(M)$ *est l'application définie par :*

$$\begin{cases} \Phi(M) : \mathcal{H} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \Phi(M)(z) = \dfrac{az+b}{cz+d} \end{cases}$$

Démontrer que Φ *définit une action de* $\mathrm{SL}_2(\mathbb{R})$ *sur* $\mathcal{H}$.

⇒ **Nous allons commencer par montrer que si** $z \in \mathcal{H}$**, alors** $\Phi(M)(z) \in \mathcal{H}$
Nous allons utiliser le fait que pour tout $a \in \mathbb{C}$, $a - \overline{a} = 2i \operatorname{Im}(a)$ qui est un imaginaire pur.
Soit donc $z \in \mathcal{H}$. Alors :

$$\begin{aligned} 2i \operatorname{Im}(\Phi(M)(z)) &= \Phi(M)(z) - \overline{\Phi(M)(z)} \\ &= \frac{az+b}{cz+d} - \frac{a\overline{z}+b}{c\overline{z}+d} \\ &= \frac{(az+b)(c\overline{z}+d) - (a\overline{z}+b)(cz+d)}{(cz+d)(c\overline{z}+d)} \\ &= \frac{\left(ac|z|^2 + adz + bc\overline{z} + bd\right) - \left(ac|z|^2 + bcz + da\overline{z} + db\right)}{|cz+d|^2} \\ &= \frac{(ad-bc)z - (ad-bc)\overline{z}}{|cz+d|^2} \\ &= \frac{z-\overline{z}}{|cz+d|^2} \text{ car } ad-bc = \det M = 1 \\ &= \frac{2i \operatorname{Im} z}{|cz+d|^2} \end{aligned}$$

Comme $\operatorname{Im} z > 0$, nous avons aussi $\operatorname{Im}(\Phi(M)(z)) > 0$, ce qui veut dire que si $z \in \mathcal{H}$, alors $\Phi(M)(z) \in \mathcal{H}$

⇒ **Nous allons montrer que, pour tout** $M \in \mathrm{SL}_2(\mathbb{R})$**,** $\Phi(M)$ **est une bijection de** $\mathcal{H}$

⋆ $\Phi(M)$ est une injection
Soient donc, $z_1 \in \mathcal{H}$ et $z_2 \in \mathcal{H}$ tels que $\Phi(M)(z_1) = \Phi(M)(z_2)$. Alors :

$$\begin{aligned} \Phi(M)(z_1) = \Phi(M)(z_2) &\iff \frac{az_1+b}{cz_1+d} = \frac{az_2+b}{cz_2+d} \\ &\iff (az_1+b)(cz_2+d) = (az_2+b)(cz_1+d) \\ &\iff acz_1z_2 + adz_1 + bcz_2 + bd = acz_1z_2adz_2 + bcz_1 + bd \\ &\iff adz_1 + bcz_2 = adz_2 + bcz_1 \\ &\iff (ad-bc)z_1 = (ad-bc)z_2 \\ &\iff z_1 = z_2 \end{aligned}$$

$\Phi(M)$ est donc bien injective

⋆ $\Phi(M)$ est une surjection
Soit $z_1 \in \mathcal{H}$; existe-t-il $z \in \mathcal{H}$ tel que $\Phi(M)(z) = z_1$
Si ce z existe, nous avons $z_1 = \dfrac{az+b}{cz+d}$ et donc :

$$\begin{aligned} z_1 = \frac{az+b}{cz+d} &\iff z_1(cz+d) = az+b \\ &\iff czz_1 + dz_1 = az+b \\ &\iff dz_1 - b = az - czz_1 \\ &\iff dz_1 - b = z(a - cz_1) \\ &\iff z = \frac{dz_1-b}{-cz_1+a} \end{aligned}$$

Nous avons $z = \Phi\left(\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\right)(z_1)$ et nous pouvons voir que

$$\det \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{vmatrix} d & -b \\ -c & a \end{vmatrix} = ad - bc = 1$$

Donc si $M=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in \mathrm{SL}_2(\mathbb{R})$, alors $M^{-1}=\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}\in \mathrm{SL}_2(\mathbb{R})$ et donc

$$z=\Phi\left(M^{-1}\right)(z_1)$$

Ce qui montre qu'en particulier, $z\in\mathcal{H}$

Ainsi $\Phi(M)$ est surjective.

$\Phi(M)$ étant injective et surjective, est donc bijective, et d'après les développements précédents, nous avons :

$$(\Phi(M))^{-1}=\Phi\left(M^{-1}\right)$$

⇒ **Si $\mathcal{S}_{\mathcal{H}}$ est l'ensemble des bijections de $\mathcal{H}$, on montre que $\Phi:\mathrm{SL}_2(\mathbb{R}):\longrightarrow\mathcal{S}_{\mathcal{H}}$ est un morphisme de groupe**

Il faut donc montrer que pour tout $M\in\mathrm{SL}_2(\mathbb{R})$ et tout $N\in\mathrm{SL}_2(\mathbb{R})$, $\Phi(MN)=\Phi(M)\circ\Phi(N)$

→ On pose $M=\begin{pmatrix}a_M & b_M\\ c_M & d_M\end{pmatrix}$ et $N=\begin{pmatrix}a_N & b_N\\ c_N & d_N\end{pmatrix}$.

Soit $z\in\mathcal{H}$; alors $\Phi(N)(z)=\dfrac{a_Nz+b_N}{c_Nz+d_N}$

Puis :

$$\begin{aligned}\Phi(M)[\Phi(N)(z)]&=\frac{a_M\Phi(N)(z)+b_M}{c_M\Phi(N)(z)+d_M}\\ &=\frac{a_M\left(\frac{a_Nz+b_N}{c_Nz+d_N}\right)+b_M}{c_M\left(\frac{a_Nz+b_N}{c_Nz+d_N}\right)+d_M}\\ &=\frac{a_M(a_Nz+b_N)+b_M(c_Nz+d_N)}{c_M(a_Nz+b_N)+d_M(c_Nz+d_N)}\\ &=\frac{(a_Ma_N+b_Mc_N)z+(a_Mb_N+b_Md_N)}{(a_Nc_M+d_Mc_N)z+(c_Mb_N+d_Md_N)}\end{aligned}$$

→ Remarquons que $MN=\begin{pmatrix}a_M & b_M\\ c_M & d_M\end{pmatrix}\times\begin{pmatrix}a_N & b_N\\ c_N & d_N\end{pmatrix}=\begin{pmatrix}a_Ma_N+b_Mc_N & a_Mb_N+b_Md_N\\ a_Nc_M+d_Nc_N & c_Mb_N+d_Md_N\end{pmatrix}$

Nous avons donc, pour tout $z\in\mathcal{H}$ $\Phi(M)\circ\Phi(N)(z)=\Phi(MN)(z)$

C'est à dire $\Phi(MN)=\Phi(M)\circ\Phi(N)$ et Φ est un homomorphisme du groupe $\mathrm{SL}_2(\mathbb{R})$ dans le groupe $\mathcal{S}_{\mathcal{H}}$ des premutations de $\mathcal{H}$

→ Nous avons donc, en particulier $(\Phi(M))^{-1}=\Phi\left(M^{-1}\right)$ et $\Phi(\mathrm{Id}_2)=\mathrm{Id}_{\mathcal{H}}$

2. *Quel est le stabilisateur F_i du nombre complexe i de $\mathcal{H}$?*

⇒ D'après la définition 10.12.4 de stabilisateur, nous devons rechercher les matrices $M\in\mathrm{SL}_2(\mathbb{R})$ telles que $\Phi(M)(i)=i$.

Dans le cours, il a été démontré que le stabilisateur est un sous-groupe de $\mathrm{SL}_2(\mathbb{R})$. Nous le vérifierons.

⇒ Nous avons donc :

$$\begin{aligned}\Phi(M)(i)=i\iff&\frac{ai+b}{ci+d}=i\\ \iff&ai+b=-c+id\\ \iff&(d-a)i=b+c\\ \iff&d-a=0\text{ et }b+c=0\\ \iff&a=d\text{ et }b=-c\end{aligned}$$

Et donc $F_i=\left\{M\in\mathrm{SL}_2(\mathbb{R})\text{ tel que }M=\begin{pmatrix}a & -b\\ b & a\end{pmatrix}\text{ avec }a^2+b^2=1\right\}=\mathrm{O}_2^+(\mathbb{R})$, c'est à dire que F_i est le groupe de rotations du plan.

3. *Montrer que l'action est transitive*

D'après la définition 10.12.7l faut donc démontrer que, pour tout $z\in\mathcal{H}$ et tout $z_1\in\mathcal{H}$, il existe $M\in\mathrm{SL}_2(\mathbb{R})$ telles que $\Phi(M)(z)=z_1$

→ Nous allons commencer par démontrer que pour tout $z\in\mathcal{H}$, il existe une matrice $M\in\mathrm{SL}_2(\mathbb{R})$ telles que $\Phi(M)(i)=z$

En posant $z = x + iy$ avec $y > 0$, nous devrions avoir $x + iy = \dfrac{ai+b}{ci+d}$. Il est clair que $a = y$, $b = x$, $c = 0$ et $d = 1$ sont des valeurs qui conviennent ; la matrice $M_1 = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$ est une matrice candidate sauf que sont déterminant est $y > 0$.

En divisant par $\sqrt{y}$ *(possible parce que $y > 0$)* la matrice $M = \begin{pmatrix} \frac{y}{\sqrt{y}} & \frac{x}{\sqrt{y}} \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix}$ dont le déterminant est 1 convient

→ Soit maintenant $z_1 \in \mathcal{H}$, il existe une matrice $N \in \mathrm{SL}_2(\mathbb{R})$ telles que $\Phi(N)(i) = z_1$

→ Soient $z \in \mathcal{H}$ et $z_1 \in \mathcal{H}$, alors :

$$z_1 = \Phi(N)(i) \iff z_1 = \Phi(N)\left(\Phi\left(M^{-1}\right)(z)\right) = \Phi\left(NM^{-1}\right)(z)$$

Donc pour tout $z \in \mathcal{H}$, il existe une matrice $A \in \mathrm{SL}_2(\mathbb{R})$ telles que $\Phi(A)(z) = z_1$

Exercice 44 :

Soit G un groupe opérant dans un ensemble quelconque X. Soient $x \in X$ et $y \in X$, 2 éléments de X dans la même orbite. Montrer que leurs stabilisateurs F_x et F_y sont conjugués dans G, c'est à dire qu'il existe $g \in G$ tel que $F_y = gF_xg^{-1}$

Nous appelons Φ l'action de G sur X
Comme $x \in X$ et $y \in X$ sont dans la même orbite, il existe $h \in G$ tel que $\Phi(h)(x) = y$
Soit maintenant $g \in G$. On a alors :

$$\begin{aligned} g \in F_y &\iff \Phi(g)(y) = y \\ &\iff \Phi(g)(\Phi(h)(x)) = \Phi(h)(x) \\ &\iff \Phi(gh)(x) = \Phi(h)(x) \\ &\iff [\Phi(h)]^{-1} \circ \Phi(gh)(x) = x \\ &\iff \Phi\left(h^{-1}gh\right)(x) = x \\ &\iff h^{-1}gh \in F_x \end{aligned}$$

Nous venons de démontrer qu'il existe $g \in G$ tel que $F_y = gF_xg^{-1}$ en ayant posé $g = h^{-1}$

10.14.10 Miscelleanous : pour aller plus loin

Exercice 46 :

Nous considérons les permutations suivantes :

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 4 & 7 & 3 & 2 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 & 7 & 8 & 6 & 5 \end{pmatrix} \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$$

1. *Décomposer les permutations a, b et c en produits de cycles et donner leur ordre*

   Assez simplement, nous avons :
   - ⋆ $a = (1\,5\,3\,4\,7)\,(2\,6)$
     a est le produit d'un cycle de longueur 5 et d'une transposition qui est un cycle de longueur 2. L'ordre de a est donc donné par le ppcm de 5 et 2, c'est à dire 10
   - ⋆ $b = (2\,4)\,(5\,7\,6\,8)$
     Par un raisonnement anologue à celui donné ci dessus, l'ordre de b est le ppcm de 2 et 4, c'est à dire 4
   - ⋆ $c = (1\,3\,8)\,(2\,7)\,(4\,9\,6\,5)$
     L'ordre de c est donc le ppcm de 3, 2 et 4, c'est à dire 12
2. *En plongeant a, b et c dans $\mathcal{S}_9$, calculez a^{201}, b^{198} et c^{1000}*
   - ⋆ Pour connaître a^{201}, il suffit de connaître la congruence de 201 modulo 10. Or, $201 \equiv 1\,[10]$ et donc $a^{201} = a$

⋆ De la même manière, $198 \equiv 2\,[4]$ et donc $b^{198} = b^2$.
Nous pouvons même aller plus loin. En effet :

$$b^2 = (2\,4)^2\,(5\,7\,6\,8)^2 = (5\,7\,6\,8)^2 = (5\,6)\,(7\,8)$$

⋆ Pour le calcul de c^{1000}, nous avons $1000 \equiv 4\,[12]$ et donc $c^{1000} = c^4$

$$c^4 = (1\,3\,8)^4\,(2\,7)^4\,(4\,9\,6\,5)^4 = (1\,3\,8)^4 = (1\,3\,8)$$

Car $(4\,9\,6\,5)$ étant d'ordre 4, $(4\,9\,6\,5)^4 = \mathrm{Id}_{\mathbb{N}_9}$ et $(1\,3\,8)$ est d'ordre 3 donc $(1\,3\,8)^4 = (1\,3\,8)$

Exercice 47 :

Soient n un entier plus grand ou égal à 2 et $\mathcal{S}_n$, le groupe symétrique de degré n.

1. *Démontrer que $\mathcal{S}_n$ est engendré par les transpositions $(1\,2)\,,(2\,3)\,,\ldots,(n-1\,n)$*

   Nous avons démontré en 10.10.11 que toute permutation $\sigma \in \mathcal{S}_n$ peut s'écrire sous forme de produit de transpositions.
   Il suffira donc de démontrer que toute transposition $\tau = (i\,j)$ avec $i \neq j$ peut s'écrire sous la forme de produit de transpositions de type $\tau_k = (k\,k+1)$ avec $1 \leqslant k \leqslant n-1$.
   Comme $\tau = (i\,j) = (j\,i)$, nous allons supposer $i < j$. Nous avons alors :

   $$(i\,j) = (i\,i+1)\,(i+1\,i+2)\cdots(j-2\,j-1)\,(j-1\,j)\,(j-2\,j-1)\cdots(i+1\,i+2)\,(i\,i+1)$$

   Pour bien comprendre ce qui a été écrit ci-dessus, vérifier par un cas pratique :

   $$(2\,7) = (2\,3)\,(3\,4)\,(4\,5)\,(5\,6)\,(6\,7)\,(5\,6)\,(4\,5)\,(3\,4)\,(2\,3)$$

2. *En déduire que $\mathcal{S}_n$ est engendré par les transpositions $(1\,2)\,,(1\,3)\,,\ldots,(1\,n)$*

   D'après la question précédente, si nous démontrons que toute transformation du type $\tau_k = (k\,k+1)$ avec $1 \leqslant k \leqslant n-1$ peut être engendrée par des transpositions du type $(1\,2)\,,(1\,3)\,,\ldots,(1\,n)$, nous aurons gagné. Or :

   $$(k\,k+1) = (1\,k)\,(1\,k+1)\,(1\,k)$$

   Nous avons donc gagné

3. *On pose $t = (1\,2)$ et $c = (1\,2\,3\cdots n)$; calculer c^k et $c^k t c^{-k}$ lorsque $1 \leqslant k \leqslant n-2$ et en déduire que t et c engendrent $\mathcal{S}_n$*

   ⇒ Si $n = 2$, alors $t = c = (1\,2)$ et nous avons $t^2 = c^2 = \mathrm{Id}_{\mathbb{N}_n}$
   ⇒ Supposons $n \geqslant 3$, et considérons donc $t = (1\,2)$ et $c = (1\,2\,3\cdots n)$ Soit k tel que $1 \leqslant k \leqslant n-1$
   ⋆ Nous avons :

   $$c = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix} \qquad c^2 = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-2 & n-1 & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 5 & \cdots & n & 1 & 2 \end{pmatrix}$$

   Et donc, plus généralement :

   $$c^k = \begin{pmatrix} 1 & 2 & \cdots & n-k & n-k+1 & \cdots & n \\ \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow \\ k+1 & k+2 & \cdots & n & 1 & \cdots & k \end{pmatrix}$$

   ⋆ Nous avons, pour le calcul de c^{-1} :

   $$c^{-1} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ n & 1 & 2 & \cdots & n-1 \end{pmatrix} \qquad c^{-2} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-2 & n-1 & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \downarrow \\ n-1 & n & 1 & \cdots & n-4 & n-3 & n-2 \end{pmatrix}$$

   Et donc, plus généralement :

   $$c^{-k} = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 & \cdots & n \\ \downarrow & \downarrow & \cdots & \downarrow & \downarrow & \cdots & \downarrow \\ n-k+1 & n-k+2 & \cdots & n & 1 & \cdots & n-kk \end{pmatrix}$$

Nous remarquons, très facilement que si $i \notin \{k+1, k+2\}$, alors $c^k t c^{-k}(i) = i$, que $c^k t c^{-k}(k+1) = k+2$ et $c^k t c^{-k}(k+2) = k+1$.
Nous avons donc $c^k t c^{-k} = (k+1\ k+2)$
Comme toutes les transpositions $\tau_k = (k+1\ k+2)$ s'expriment comme un produit de c, t et c^{-1}, et que les transpositions $(1\,2), (1\,3), \ldots, (1\,n)$ engendrent $\mathcal{S}_n$, il résulte que les transformations c et t engendrent $\mathcal{S}_n$

Exercice 48 :

Pour $n > 3$ on désigne par $\mathcal{B}_n$ le sous-groupe de A_n engendré par les cycles

$$(1\ 2\ 3), (1\ 2\ 4), \ldots, (1\ 2\ n)$$

Pour nous simplifier la vie, nous posons $c_k = (1\ 2\ k)$ avec $1 \leqslant k \leqslant n$

1. *Montrer que $\mathcal{B}_n$ est un sous-groupe du groupe alterné A_n*

   Nous allons démontrer que, pour tout $k \in \mathbb{N}$, $1 \leqslant k \leqslant n$ le cycle c_k est un élément de A_n, c'est à dire a une signature positive.
   - ⋆ Nous avons donc $c_k = (1\ 2\ k) = (1\ 2)(2\ k)$, c'est à dire que chaque cycle c_k est le produit de 2 transpositions
   - ⋆ Si $\varepsilon(c_k)$ est la signature du cycle c_k, la signature de chaque transposition est -1. Ainsi :

   $$\varepsilon(c_k) = \varepsilon((1\ 2)) \times \varepsilon((2\ k)) = (-1)^2 = 1$$

   Ainsi, pour tout k tel que $1 \leqslant k \leqslant n$ $c_k \in A_n$
   A_n étant un sous-groupe de $\mathcal{S}_n$, la composition des c_k, pour $1 \leqslant k \leqslant n$ est toujours dans A_n.
   Et donc $\mathcal{B}_n$ est un sous-groupe du groupe alterné A_n.
2. *Démontrer que si i et j sont deux entiers distincts ($i \neq j$) tels que $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant n$, les permutations $(1\ 2)(i\ j)$ et $(i\ j)(1\ 2)$ appartiennent à $\mathcal{B}_n$*

   Comme $i \neq j$, nous supposons $i < j$
   → Supposons que $i = 1$ et $j = 2$
   Alors $(1\ 2)(i\ j) = (1\ 2)(1\ 2) = \mathrm{Id}_{\mathbb{N}_n}$.
   De même, $(i\ j)(1\ 2) = (1\ 2)(1\ 2) = \mathrm{Id}_{\mathbb{N}_n}$
   Et donc les permutations $(1\ 2)(i\ j)$ et $(i\ j)(1\ 2)$ appartiennent à $\mathcal{B}_n$
   → Supposons maintenant $i = 1$ et $j > 2$
   Alors $(i\ j)(1\ 2) = (1\ j)(1\ 2) = (1\ 2\ j)$ et par définition, $(1\ 2\ j) \in \mathcal{B}_n$.
   Ensuite, $(1\ 2)(i\ j) = (1\ 2)(1\ j) = (1\ j\ 2)$. Or, $(1\ j\ 2) = (1\ 2\ j) \circ (1\ 2\ j) = (1\ 2\ j)^2$, et donc $(1\ j\ 2) \in \mathcal{B}_n$
   Nous en concluons que $(1\ 2)(1\ j)$ et $(1\ j)(1\ 2)$ appartiennent à $\mathcal{B}_n$
   → Supposons maintenant que $i > 1$, et donc $j > 2$; alors, comme les 2 permutations $(1\ 2)$ et $(i\ j)$ ont des supports d'intersection vide et commutent :

   $$(1\ 2)(i\ j) = (i\ j)(1\ 2)$$

   D'après des exercices précédents :

   $$(1\ 2)(i\ j) = (1\ 2\ i)(i\ j\ 2)$$

   Et nous avons :

   $$(i\ j\ 2) = (1\ 2\ j)(1\ 2\ j)(1\ 2\ i)$$

   D'où

   $$(1\ 2)(i\ j) = (1\ 2\ i)(1\ 2\ j)(1\ 2\ j)(1\ 2\ i) = c_i \circ c_j^2 \circ c_i$$

   Ce qui montre que si $1 < i < j$, alors les permutations $(1\ 2)(i\ j)$ et $(i\ j)(1\ 2)$ appartiennent à $\mathcal{B}_n$ comme composée de cycles de type c_k

3. *Montrer que $\mathcal{B}_n = A_n$*

   Soit $\sigma \in A_n$; alors la signature de σ est $\varepsilon(\sigma) = +1$.
   σ est la composition de transpositions *(cf théorème 10.10.11)* ; la signature d'une transposition étant -1, le nombre de ces transpositions est donc forcément pair, donc :

   $$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2p-1} \circ \tau_{2p}$$

   Soit τ_0 la transposition $\tau_0 = (1\ 2)$; alors, comme $\tau_0 \circ \tau_0 = \mathrm{Id}_{\mathbb{N}_n}$, nous pouvons écrire :

   $$\begin{array}{rl} \sigma = & \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2p-1} \circ \tau_{2p} \\ = & \tau_1 \circ (\tau_0 \circ \tau_0) \circ \tau_2 \circ \tau_3 \circ (\tau_0 \circ \tau_0) \circ \tau_4 \circ \cdots \circ \tau_{2p-1} \circ (\tau_0 \circ \tau_0) \circ \tau_{2p} \\ = & (\tau_1 \circ \tau_0) \circ (\tau_0 \circ \tau_2) \circ (\tau_3 \circ \tau_0) \circ \cdots \circ (\tau_{2p-1} \circ \tau_0) \circ (\tau_0) \circ \tau_{2p}) \end{array}$$

   D'après la question précédente, toutes les transpositions du type $\tau_0 \circ \tau_{2i}$ ou $\tau_{2i-1} \circ \tau_0$ avec $i \leqslant i \leqslant p$ sont des éléments de $\mathcal{B}_n$ et donc $\sigma \in \mathcal{B}_n$ comme composée d'éléments de $\mathcal{B}_n$

Exercice 50 :

On considère deux groupes $(G_1, \star)$ et $(G_2, \top)$, deux homomorphismes de groupes f et g définis sur G_1 à valeurs dans G_2 et on appelle H l'ensemble des éléments $x \in G_1$ tels que $f(x) = g(x)$.

1. *Montrer que H est un sous-groupe de $(G_1, \star)$.*
   ⇒ Tout d'abord $H \neq \emptyset$ puisque si e_1 est l'élément neutre de $(G_1, \star)$ et e_2, celui de $(G_2, \top)$, nous avons, propriété des homomorphismes, $f(e_1) = g(e_1) = e_2$
   ⇒ Soient $x \in H$ et $y \in H$, avons nous $x \star y^{-1} \in H$?
   Nous avons :

   $$\begin{array}{rl} f\left(x \star y^{-1}\right) = & f(x) \top f\left(y^{-1}\right) \\ = & f(x) \top (f(y))^{-1} \\ = & g(x) \top (g(y))^{-1} \\ = & g(x) \top (g(y))^{-1} \\ = & g(x) \top g\left(y^{-1}\right) \\ = & g\left(x \star y^{-1}\right) \end{array}$$

   Ainsi $x \star y^{-1} \in H$
   Et donc H est un sous-groupe de $(G_1, \star)$
2. *On désigne par h l'injection canonique de H dans G_1*

   (a) *Montrer que $f \circ h = g \circ h$.*

   Soit $x \in H$. L'injection canonique de H dans G_1 est telle que, pour tout $x \in H$, $h(x) = x$. Ainsi, pour tout $x \in H$,

   $$f \circ h(x) = f[h(x)] = f(x) = g(x) = g[h(x)] = g \circ h(x)$$

   Et nous avons bien $f \circ h = g \circ h$

   (b) *Montrer que si $(G_3, \diamond)$ est un groupe et h' un homomorphisme défini sur G_3 à valeurs dans G_1, tel que $f \circ h' = g \circ h'$, alors il existe un homomorphisme $\theta : G_3 \longrightarrow H$ défini sur G_3 à valeurs dans H, et un seul, tel que $h' = h \circ \theta$.*

   Si nous avons, par hypothèse $f \circ h' = g \circ h$, nous avons, pour tout $x \in G_3$,

   $$f \circ h'(x) = g \circ h'(x) \Longleftrightarrow f[h'(x)] = g[h'(x)]$$

   Et donc $h'(x) \in H$
   Soit donc $\theta : G_3 \longrightarrow H$ ainsi définie :

   $$\left\{ \begin{array}{rcl} \theta : G_3 & \longrightarrow & H \\ x & \longmapsto & \theta(x) = h'(x) \end{array} \right.$$

   θ, définie par h' est clairement un homomorphisme, et nous avons, pour tout $x \in G_3$, $h(\theta(x)) = \theta(x) = h'(x)$, et donc $h' = h \circ \theta$

Exercice 51 :

Soient $(G,\star)$ un groupe abélien, G_1 et G_2 deux sous-groupes de G tels que $G_1 \subset G_2$.
Soient $\varpi_1 : G \longrightarrow G/G_1$ et $\varpi_2 : G \longrightarrow G/G_2$ les homomorphismes canoniques de G sur G/G_1 et de G sur G/G_2

1. *Montrer qu'il existe un homomorphisme ρ défini sur G/G_1 à valeurs dans G/G_2 et un seul, tel que $\rho \circ \varpi_1 = \varpi_2$*

   → Soit $\dot{x} \in G/G_1$; il existe alors $x \in G$ tel que $\varpi_1(x) = \dot{x}$

   → Soit $x' \in G$ tel que $\varpi_1(x) = \varpi_1(x') = \dot{x}$. Ceci signifie donc que $x' \in \dot{x}$, c'est à dire, par la relation d'équivalence canonique, $x - x' \in G_1$, et comme $G_1 \subset G_2$, nous avons $x - x' \in G_2$ et donc $\varpi_1(x' - x) = \dot{e}$, c'est à dire $\varpi_2(x) = \varpi_2(x')$

   → Soit $\rho : G/G_1 \longrightarrow G/G_2$ définie par :

   $$\left\{\begin{array}{rcl} \rho : G/G_1 & \longrightarrow & G/G_2 \\ \dot{x} & \longmapsto & \rho(\dot{x}) = \varpi_2(x) \end{array}\right.$$

   Alors $\rho \circ \varpi_1(x) = \rho(\dot{x}) = \varpi_2(x)$ et donc $\rho \circ \varpi_1 = \varpi_2$

   → ρ est un homomorphisme de groupe
   En effet, soient $\dot{x} \in G/G_1$ et $\dot{y} \in G/G_1$. Il existe $x \in G$ et $y \in G$ tels que $\varpi_1(x) = \dot{x}$ et $\varpi_1(y) = \dot{y}$, et donc :

   $$\rho(\dot{x} \star \dot{y}) = \rho(\varpi_1(x) \star \varpi_1(y)) = \rho(\varpi_1(x \star y)) = \varpi_2(x \star y) = \varpi_2(x) \star \varpi_2(y) = \rho(\dot{x}) \star \rho(\dot{y})$$

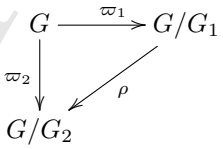
   ρ est donc bien un homomorphisme

   → ρ est unique
   Soit ρ' un second homomorphisme de groupe tel que $\rho' \circ \varpi_1 = \varpi_2$.
   Nous avons alors $\rho' \circ \varpi_1 = \rho \circ \varpi_1$
   Soit $\dot{x} \in G/G_1$; il existe alors $x \in G$ tel que $\varpi_1(x) = \dot{x}$. Alors :

   $$\rho(\dot{x}) = \rho(\varpi_1(x)) = \rho'(\varpi_1(x)) = \rho'(\dot{x})$$

   Et donc $\rho = \rho'$. Il y a donc unicité

   Nons avons donc le schéma :

2. *Montrer que ρ est surjectif et que son noyau est G_2/G_1*

   → ρ est surjective
   En effet, soit $\dot{y} \in G/G_2$; il existe donc $y \in G$ tel que $\varpi_2(y) = \dot{y}$.
   De l'égalité $\varpi_2 = \rho \circ \varpi_1$, nous déduisons

   $$\dot{y} = \varpi_2(y) = \rho \circ \varpi_1(y) = \rho[\varpi_1(y)]$$

   En posant $z = \varpi_1(y)$, nous avons $z \in G/G_1$ et $\dot{y} = \rho(z)$.
   ρ est donc bien surjective

   → Recherche de $\ker \rho$
   Soit $\dot{x} \in G/G_1$ tel que $\dot{x} \in \ker \rho$; alors $\rho(\dot{x}) = \dot{e}$. Il existe aussi $x \in G$ tel que $\varpi_1(x) = \dot{x}$
   Toujours de l'égalité $\varpi_2 = \rho \circ \varpi_1$, nous déduisons

   $$\dot{e} = \rho(\dot{x}) = \rho \circ \varpi_1(x) = \varpi_2(x)$$

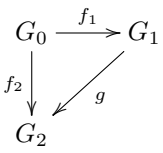
   Et donc $x \in G_2$ et donc $\dot{x} \in G_2/G_1$
   D'où $\ker \rho = G_2/G_1$

Exercice 52 :

Soient G_0, G_1, G_2 des groupes, $f_1 : G_0 \longrightarrow G_1$, un homomorphisme surjectif de G_0 sur G_1, et $f_2 : G_0 \longrightarrow G_2$, un homomorphisme de G_0 sur G_2, tels que $\ker f_1 \subset \ker f_2$

1. *Montrer qu'il existe un homomorphisme $g : G_1 \longrightarrow G_2$ défini sur G_1, à valeurs dans G_2, et un seul, tel que $f_2 = g \circ f_1$*

   En fait, nous devons démontrer que nous avons le schéma suivant :

   Nous allons noter $e_0 \in G_0$ l'élément neutre de G_0, $e_1 \in G_1$ l'élément neutre de G_1 et $e_2 \in G_2$ l'élément neutre de G_2.

   Soit $y \in G_1$; nous nous devons donc de définir $g(y)$

   - ⋆ f_1 étant surjective, il existe $x \in G_0$ tel que $y = f_1(x)$, et il semble naturel alors de poser $g(y) = f_2(x)$ et, dans ce cas, $f_2 = g \circ f_1$
   - ⋆ f_1 étant surjective, il peut exister $x' \in G_0$ tel que $y = f_1(x')$ avec, éventuellement $x \neq x'$... Et alors ? ?

     Posons nous d'abord la question sur ce que veut dire $f_1(x') = f_1(x)$.

     $$f_1(x') = f_1(x) \Longleftrightarrow f_1(x') \times (f_1(x))^{-1} = e_1 \Longleftrightarrow f_1\left(x'x^{-1}\right) = e_1$$

     Ce qui veut donc dire que $x'x^{-1} \in \ker f_1$

     Or, par hypothèse, $\ker f_1 \subset \ker f_2$ et donc $x'x^{-1} \in \ker f_2$.

     En reprenant la démonstration que nous avons faite pour f_1, nous déduisons que $f_2(x') = f_2(x)$ et donc $g(y)$ est entièrement et bien défini.
   - ⋆ Est ce que g est un homomorphisme de groupe ?

     Soient $y_1 \in G_1$ et $y_2 \in G_1$ et étudions $g(y_1y_2)$.

     Il existe donc $x_1 \in G_0$ et $x_2 \in G_0$ tels que $y_1 = f_1(x_1)$ et $y_2 = f_1(x_2)$ et donc $g(y_1) = f_2(x_1)$ et $g(y_2) = f_2(x_2)$

     $$g(y_1y_2) = g(f_1(x_1)\, f_1(x_2)) = g(f_1(x_1x_2)) = f_1(x_1)\, f_1(x_2) = g(y_1)\, g(y_2)$$

     g est donc bien un homomorphisme
   - ⋆ Y a-t-il unicité de g ?

     Soit donc $g' : G_1 \longrightarrow G_2$ un second homomorphisme tel que $f_2 = g' \circ f_1$

     Soit $y \in G_1$. Il existe $x \in G_0$ tel que $y = f_1(x)$, et nous avons alors :

     $$g'(y) = g'(f_1(x)) = g' \circ f_1(x) = f_2(x) = g \circ f_1(x) = g(f_1(x)) = g(y)$$

     Nous venons donc de démontrer que $g = g'$, c'est à dire que nous venons de démontrer l'unicité.

2. *Montrer que* $\ker g = f_1(\ker f_2)$

   $\Rightarrow$ Soit $y \in f_1(\ker f_2)$; alors, il existe $x \in \ker f_2$ tel que $y = f_1(x)$ et

   $$g(y) = g(f_1(x)) = f_2(x) = e_2$$

   Et donc, comme $g(y) = e_2$, nous avons $y \in \ker g$

   D'où $f_1(\ker f_2) \subset \ker g$

   $\Rightarrow$ Reciproquement soit $y \in \ker g$; alors $g(y) = e_2$ et donc, de $g(y) = g \circ f_1(x) = f_2(x) = e_2$ nous tirons que $x \in \ker f_2$, et comme $y = f_1(x)$, nous avons $y \in f_1(\ker f_2)$.

   Donc $\ker g \subset f_1(\ker f_2)$

   D'où $\ker g = f_1(\ker f_2)$

Exercice 53 :

Si $(G,+)$ est un groupe abélien, nous désignerons par $\mathrm{Hom}(\mathbb{Z},G)$ l'ensemble des homomorphismes de $\mathbb{Z}$ dans G.

1. *Montrer que tout homomorphisme f de $\mathbb{Z}$ dans G est complètement déterminé par la donnée de $f(1)$.*

   Soit $(G,+)$ un groupe abélien dont l'opération est notée additivement de neutre noté 0 et $f : \mathbb{Z} \longrightarrow G$ un homomorphisme de groupe
   - Alors $f(0) = 0$, et en utilisant les propriétés d'homomorphisme, pour tout $m \in \mathbb{Z}$ et tout $n \in \mathbb{Z}$ nous avons :
   $$f(m+n) = f(m) + f(n) \text{ et } f(0) = 0 \text{ et } f(-m) = -f(m)$$
   En particulier, $f(2) = f(1+1) = f(1) + f(1) = 2f(1)$
   - Très généralement, et par une récurrence facile, on montre que pour tout $n \in \mathbb{N}^*$ que $f(n) = nf(1)$
   - Supposons que, maintenant, $n \in \mathbb{Z}^-$; il existe alors $n' \in \mathbb{N}^*$ tel que $n = -n'$, et donc :
   $$f(n) = f(-n') = -f(n') = -[n'f(1)] = -n'f(1) = nf(1)$$

   Nous venons donc de montrer que pour tout $n \in \mathbb{Z}$, $f(n) = nf(1)$ et donc $f(1)$ détermine bien l'homomorphisme de groupe $f : \mathbb{Z} \longrightarrow G$

2. *On munit $\mathrm{Hom}(\mathbb{Z},G)$ de la loi de composition suivante :*

   Si $f \in \mathrm{Hom}(\mathbb{Z},G)$ et $g \in \mathrm{Hom}(\mathbb{Z},G)$, alors $f \oplus g$ est l'application de $\mathbb{Z}$ dans G définie en posant pour chaque entier rationnel $n \in \mathbb{Z}$,
   $$(f \oplus g)(n) = f(n) + g(n)$$

   Montrer que $\mathrm{Hom}(\mathbb{Z},G)$ devient ainsi un groupe abélien.

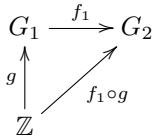
   Voici une question classique et des plus faciles
   - La loi $\oplus$ est une loi interne dans $\mathrm{Hom}(\mathbb{Z},G)$
   Soient $f \in \mathrm{Hom}(\mathbb{Z},G)$ et $g \in \mathrm{Hom}(\mathbb{Z},G)$, il faut montrer que $f \oplus g \in \mathrm{Hom}(\mathbb{Z},G)$
   Il faut donc montrer que $f \oplus g$ est un homomorphisme de groupe.
   Soient $m \in \mathbb{Z}$ et $n \in \mathbb{Z}$, alors :
   $$\begin{array}{rcl}(f \oplus g)(m+n) & = & f(m+n) + g(m+n) \\ & = & f(m) + f(n) + g(m) + g(n) \\ & = & f(m) + g(m) + f(n) + g(n) \text{ par commutativité dans } (G,+) \\ & = & (f \oplus g)(m) + (f \oplus g)(n)\end{array}$$
   Nous venons de montrer que $f \oplus g$ est un homomorphisme de groupe et que donc $f \oplus g \in \mathrm{Hom}(\mathbb{Z},G)$
   La loi $\oplus$ est donc interne dans $\mathrm{Hom}(\mathbb{Z},G)$
   - La loi $\oplus$ est associative
   Il faut donc montrer que, pour tout $f \in \mathrm{Hom}(\mathbb{Z},G)$, $g \in \mathrm{Hom}(\mathbb{Z},G)$ et $h \in \mathrm{Hom}(\mathbb{Z},G)$, nous avons
   $$(f \oplus g) \oplus h = f \oplus (g \oplus h)$$
   Soit donc $n \in \mathbb{Z}$; alors :
   $$\begin{array}{rcl}((f \oplus g) \oplus h)(n) & = & (f \oplus g)(n) + h(n) \\ & = & (f(n) + g(n)) + h(n) \\ & = & f(n) + (g(n) + h(n)) \text{ par associativité dans } (G,+) \\ & = & f(n) + (g \oplus h)(n) \\ & = & (f \oplus (g \oplus h))(n)\end{array}$$
   Et donc nous avons, dans $\mathrm{Hom}(\mathbb{Z},G)$, $(f \oplus g) \oplus h = f \oplus (g \oplus h)$.
   La loi $\oplus$ est donc associative.

- La loi $\oplus$ est commutative
  Il faut donc montrer que, pour tout $f \in \mathrm{Hom}(\mathbb{Z}, G)$ et tout $g \in \mathrm{Hom}(\mathbb{Z}, G)$ nous avons
  $$f \oplus g = g \oplus f$$
  Soit donc $n \in \mathbb{Z}$; alors :
  $$\begin{array}{rcl}(f \oplus g)(n) = & f(n) + g(n) & \\ = & g(n) + f(n) & \text{par la commutativité dans } (G, +) \\ = & (g \oplus f)(n) & \end{array}$$
  Et donc nous avons, dans $\mathrm{Hom}(\mathbb{Z}, G)$, $f \oplus g = g \oplus f$.
  La loi $\oplus$ est donc commutative.
- L'élément neutre de $\oplus$ dans $\mathrm{Hom}(\mathbb{Z}, G)$ est la fonction constante $\mathcal{O} : \mathbb{Z} \longrightarrow G$ telle que, pour tout $n \in \mathbb{Z}$, $\mathcal{O}(n) = 0$.
  En effet, pour tout $n \in \mathbb{Z}$, nous avons :
  $$(f \oplus \mathcal{O})(n) = f(n) + \mathcal{O}(n) = f(n) + 0 = f(n)$$
  Et donc $f \oplus \mathcal{O} = f$
  Par commutativité, nous avons de la même manière que $\mathcal{O} \oplus f = f$
  Et donc $f \oplus \mathcal{O} = \mathcal{O} \oplus f = f$
- Chaque élément $f \in \mathrm{Hom}(\mathbb{Z}, G)$ admet un symétrique noté $(-f)$ et défini pour tout $n \in \mathbb{Z}$ par $(-f)(n) = -f(n)$. En effet :
  $$(f \oplus (-f))(n) = f(n) + (-f)(n) = f(n) - f(n) = 0 = \mathcal{O}(n)$$
  Nous avons donc $f \oplus (-f) = \mathcal{O}$, et , par commutativité, $(-f) \oplus f = \mathcal{O}$

3. *Soient G_1, G_2 et G_3, trois groupes abéliens, $f_1 : G_1 \longrightarrow G_2$ un homomorphisme de G_1 dans G_2 et $f_2 : G_2 \longrightarrow G_3$ un homomorphisme de G_2 dans G_3.*
   On note f_1^* l'application de $\mathrm{Hom}(\mathbb{Z}, G_1)$ dans $\mathrm{Hom}(\mathbb{Z}, G_2)$ ainsi définie :
   $$\left\{\begin{array}{rcl} f_1^* : \mathrm{Hom}(\mathbb{Z}, G_1) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}, G_2) \\ g & \longmapsto & f_1^*(g) = f_1 \circ g \end{array}\right.$$
   On définit de manière analogue f_2^* par
   $$\left\{\begin{array}{rcl} f_2^* : \mathrm{Hom}(\mathbb{Z}, G_2) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}, G_3) \\ g & \longmapsto & f_2^*(g) = f_2 \circ g \end{array}\right.$$

   (a) *Montrer que f_1^* et f_2^* sont des homomorphismes.*

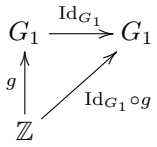
   Nous allons montrer seulement que f_1^* est un homomorphisme.
   Pour commencer, un schéma peut être instructif :

   Soit $g \in \mathrm{Hom}(\mathbb{Z}, G_1)$ et $g' \in \mathrm{Hom}(\mathbb{Z}, G_1)$; il faut donc montrer que
   $$f_1^*(g \oplus g') = f_1^*(g) \oplus f_1^*(g')$$
   Soit donc $n \in \mathbb{Z}$, et nous avons :
   $$\begin{array}{rcl}[f_1^*(g \oplus g')](n) = & [f_1 \circ (g \oplus g')](n) & \\ = & f_1[(g \oplus g')(n)] & \\ = & f_1[g(n) + g'(n)] & \\ = & f_1[g(n)] + f_1[g'(n)] & \\ = & f_1 \circ g(n) + f_1 \circ g'(n) & \\ = & f_1^*(g)(n) + f_1^*(g')(n) & \\ = & [f_1^*(g) \oplus f_1^*(g')](n) & \end{array}$$
   Nous avons donc $f_1^*(g \oplus g') = f_1^*(g) \oplus f_1^*(g')$ et f_1^* est donc un homomorphisme de groupes

(b) *Montrer que si $G_1 = G_2$, et si f_1 est l'identité de G_1 alors f_1^* est l'identité de* $\mathrm{Hom}(\mathbb{Z}, G_1)$.

Reprenons le schéma :



Il faudrait donc montrer que, pour tout $g \in \mathrm{Hom}(\mathbb{Z}, G_1)$, nous avons $f_1^*(g) = g$.
Soit $n \in \mathbb{Z}$, alors :

$$f_1^*(g)(n) = f_1 \circ g(n) = \mathrm{Id}_{G_1} \circ g(n) = g(n)$$

Nous avons bien $f_1^*(g) = g$ et donc $f_1^* = \mathrm{Id}_{\mathrm{Hom}(\mathbb{Z},G_1)}$

(c) *Montrer que $(f_2 \circ f_1)^* = f_2^* \circ f_1^*$*

Tout d'abord, il faut remarquer que $f_2 \circ f_1$ est un homomorphisme du groupe G_1 dans le groupe G_3.
Il nous faut démontrer que, pour tout $g \in \mathrm{Hom}(\mathbb{Z}, G_1)$, nous avons

$$(f_2 \circ f_1)^*(g) = (f_2^* \circ f_1^*)(g) = f_2^*[f_1^*(g)]$$

Soit $n \in \mathbb{Z}$; alors :

$$\begin{aligned}(f_2 \circ f_1)^*(g)(n) &= f_2 \circ f_1 \circ g(n)\\ &= f_2[f_1 \circ g(n)]\\ &= f_2[f_1^*(g)(n)]\\ &= f_2^*[f_1^*(g)](n)\end{aligned}$$

Et nous avons donc, pour tout $g \in \mathrm{Hom}(\mathbb{Z}, G_1)$, $(f_2 \circ f_1)^*(g) = f_2^*[f_1^*(g)] = (f_2^* \circ f_1^*)(g)$
D'où $(f_2 \circ f_1)^* = f_2^* \circ f_1^*$

(d) *Montrer que si f_1 est injectif alors f_1^* est injectif.*

Supposons f_1 injectif et montrons que f_1^* est injectif.
Il nous faut donc montrer l'implication suivante pour tout $g \in \mathrm{Hom}(\mathbb{Z}, G_1)$ et tout $g' \in \mathrm{Hom}(\mathbb{Z}, G_1)$:

$$f_1^*(g) = f_1^*(g') \Longrightarrow g = g'$$

Supposons donc que $f_1^*(g) = f_1^*(g')$, alors, pour tout $n \in \mathbb{Z}$

$$f_1^*(g)(n) = f_1^*(g')(n) \Longleftrightarrow f_1 \circ g(n) = f_1 \circ g'(n) \Longleftrightarrow f_1(g(n)) = f_1(g'(n))$$

De l'injectivité de f_1, nous déduisons, pour tout $n \in \mathbb{Z}$, $g(n) = g'(n)$, c'est à dire $g = g'$.
f_1^* est donc injectif

(e) *Montrer que si f_1 est surjectif alors f_1^* est surjectif.*

Supposons f_1 surjectif. Soit $h \in \mathrm{Hom}(\mathbb{Z}, G_2)$; existe-t-il $g \in \mathrm{Hom}(\mathbb{Z}, G_1)$ tel que $f_1^*(g) = h$?
Soit $h \in \mathrm{Hom}(\mathbb{Z}, G_2)$.
f_1 étant surjectif, il existe $x \in G_1$ tel que $f_1(x) = h(1)$
Les homomorphismes $g \in \mathrm{Hom}(\mathbb{Z}, G_1)$ sont entièrement déterminés par la donnée de $g(1)$. Il existe donc un et un seul endomorphisme $g \in \mathrm{Hom}(\mathbb{Z}, G_1)$ tel que $g(1) = x$.
Alors $f_1 \circ g(1) = f_1(x) = h(1)$. Les homomorphismes g et h sont entièrement déterminés.
Ainsi $f_1 \circ g = h$, c'est à dire $f_1^*(g) = h$ et f_1^* est surjectif

Exercice 55 :

Soient G un groupe abélien et $H \subset G$ un sous-groupe de G tel que le quotient G/H soit un groupe monogène infini.
Montrer qu'il existe un isomorphisme de $H \times (G/H)$ sur G.

Soit $x \in G$ tel que $\dot{x}$ engendre G/H, c'est à dire :

$$G/H = \{(\dot{x})^n \text{ avec } n \in \mathbb{Z}\}$$

On appelle $X = \Gamma(\{x\})$, le sous-groupe de G engendré par x

→ Soit $\varphi : G/H \longrightarrow X$ une application définie par :

$$\left\{\begin{array}{rcl} \varphi : G/H & \longrightarrow & X \\ (\dot{x})^n & \longmapsto & \varphi\left((\dot{x})^n\right) = x^n \end{array}\right.$$

Nous allons montrer que φ est un isomorphisme de groupe

⋆ φ est un homomorphisme de groupe
En effet :

$$\begin{array}{rcl} \varphi\left((\dot{x})^n \times (\dot{x})^m\right) = & \varphi\left(\dot{x^n} \times \dot{x^m}\right) \\ = & \varphi\left(x^n \dot{\times} x^m\right) \\ = & \varphi\left(\dot{x^{n+m}}\right) \\ = & x^{n+m} = x^n \times x^m \\ = & \varphi\left((\dot{x})^n\right) \times \varphi\left((\dot{x})^m\right) \end{array}$$

φ est donc bien un homomorphisme de groupe

⋆ φ est surjective
Soit $y \in X$; il existe donc $n \in \mathbb{Z}$ tel que $y = x^n$ et donc, comme $\dot{x^n} = \dot{x}^n$, nous avons $\varphi\left(\dot{x^n}\right) = \varphi\left((\dot{x})^n\right) = x^n = y$.
Donc $\varphi : G/H \longrightarrow X$ est bien une application surjective.

⋆ Montrons que φ est injective.
Soient donc $y \in G/H$ et $z \in G/H$ tels que $\varphi(y) = \varphi(z)$.
Il existe $m \in \mathbb{Z}$ et $n \in \mathbb{Z}$ tels que $(\dot{x})^n = y$ et $(\dot{x})^m = z$, et donc

$$\varphi(y) = \varphi(z) \Longleftrightarrow x^n = x^m \Longleftrightarrow x^{n-m} = e$$

En particulier, de $x^{n-m} = e$, nous tirons $\dot{x}^{n-m} = \dot{e}$.
Comme G/H est un groupe monogène infini, alors $n - m = 0 \Longleftrightarrow n = m$ et donc, $y = z$
φ est donc injective

Ainsi, φ est un isomorphisme de groupe.

De quel type sont donc les éléments $\dot{x} \in G/H$?
Nous avons $y \in \dot{x} \Longleftrightarrow y = xh$ avec $h \in H$. Du fait que G/H est monogène, toutes les classes de G/H sont du type $(\dot{x})^n$ avec $n \in \mathbb{Z}$ et alors $\dot{x^n} = \{y \in G \text{ avec } y = x^n h \text{ avec } h \in H\}$

→ Soit, maintenant $\psi : H \times X \longrightarrow G$ définie par :

$$\left\{\begin{array}{rcl} \psi : H \times X & \longrightarrow & G \\ (h, x^n) & \longmapsto & \psi\left[(h, x^n)\right] = hx^n \end{array}\right.$$

La structure de groupe de $H \times X$ est celle impliquée par les structures de groupe de H et de X

⋆ ψ est un homomorphisme de groupe
En effet

$$\psi\left[(h, x^n)\left(h', x^m\right)\right] = \psi\left[\left(hh', x^{n+m}\right)\right] = hh'x^{n+m} = hx^n h'x^m = \psi\left[(h, x^n)\right] \times \psi\left[(h', x^m)\right]$$

⋆ ψ est surjective
Soit $y \in G$; alors $\dot{y} \in G/H$ et, comme G/H est monogène infini, nous avons $\dot{y} = (\dot{x})^n$. Comme $y \in (\dot{x})^n$, il existe $h \in H$ tel que $y = x^n h$, c'est à dire :

$$y = x^n h = \psi\left[(h, x^n)\right]$$

ψ est donc surjective

⋆ ψ est injective
Soient $(h, x^n) \in H \times X$ et $(h', x^m) \in H \times X$ tels que $\psi\left[(h, x^n)\right] = \psi\left[(h', x^m)\right]$.
Alors $hx^n = h'x^m$, c'est à dire $x^n = h^{-1}h'x^m = \left(h^{-1}h'\right)x^m$; ainsi, $x^n \in (\dot{x})^m$, c'est à dire $(\dot{x})^n = (\dot{x})^m$ et donc $m = n$, et de $m = n$, on tire $h = h'$. Donc :

$$(h, x^n) = (h', x^m)$$

ψ est donc injective

Et ψ est un isomorphisme de $H \times X$ sur G

$\rightarrow$ Nous avons montré que G/H et X étaient isomorphes *(par l'isomorphisme φ).*
Comme $H \times X$ et G sont isomorphes, il est naturel de penser que $H \times G/H$ et G sont isomorphes.
Soit $\overline{\varphi} : H \times G/H \longrightarrow H \times X$ définie par :

$$\left\{ \begin{array}{rcl} \overline{\varphi} : H \times G/H & \longrightarrow & H \times X \\ (h, (\dot{x})^n) & \longmapsto & \overline{\varphi}\left[(h, (\dot{x})^n)\right] = (h, \varphi\left((\dot{x})^n\right)) = (h, x^n) \end{array} \right.$$

Il est facile de démontrer que $\overline{\varphi}$ est un isomorphisme de groupe. Nous avons donc :

$$H \times G/H \quad \stackrel{\overline{\varphi}}{\longrightarrow} \quad H \times X \quad \stackrel{\psi}{\longrightarrow} \quad G$$

Nous avons donc $\psi \circ \overline{\varphi} : H \times G/H \longrightarrow G$ qui est un isomorphisme comme composée de 2 isomorphismes.

Q.E.D.

Compléments

Nous avons dit qu'il était « facile de démontrer que $\overline{\varphi}$ est un isomorphisme de groupe ».
Nous vous proposons de le démontrer en élargissant le propos :
Soient G, H et K, 3 groupes et $\varphi : H \longrightarrow K$, un isomorphisme de groupes.
On construit $\overline{\varphi}$ de cette façon :

$$\left\{ \begin{array}{rcl} \overline{\varphi} : G \times H & \longrightarrow & G \times K \\ (g, h) & \longmapsto & \overline{\varphi}\left[(g, h)\right] = (g, \varphi\left(h\right)) \end{array} \right.$$

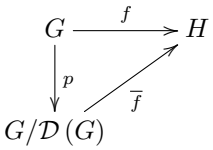
Montrer que $\overline{\varphi}$ est un isomorphisme de $G \times H$ sur $G \times K$

Exercice 56 :

Soient G un groupe d'élément neutre e.
On appelle sous-groupe dérivé de G, que l'on note $\mathcal{D}(G)$ le sous-groupe engendré par les éléments de la forme $[x, y] = xyx^{-1}y^{-1}$ où x et y sont des éléments de G.
Nous avons déjà démontré que $\mathcal{D}(G)$ est un sous-groupe distingué de G et que $G/\mathcal{D}(G)$ est un groupe abélien.

1. *Montrer que si f est un homomorphisme de G dans un groupe commutatif H, il existe un homomorphisme $\overline{f}$ de $G/\mathcal{D}(G)$ dans H, et un seul, tel que $f = \overline{f} \circ p$ où p désigne la surjection canonique de G sur $G/\mathcal{D}(G)$*

   En fait, nous souhaitons que le diagramme suivant soit commutatif :



   $\Rightarrow$ **Nous allons démontrer que, pour tout homomorphisme $f : G \longrightarrow H$ où H est un groupe commutatif, nous avons $\mathcal{D}(G) \subset \ker f$**
   Nous notons e', l'élément neutre de H
   En effet, soit $z \in \mathcal{D}(G)$; il existe alors $x \in G$ et $y \in G$ tels que $z = [x, y] = xyx^{-1}y^{-1}$, et nous avons :

$$\begin{array}{rcll} f(z) = & f\left(xyx^{-1}y^{-1}\right) & & \\ = & f(x) f(y) f(x)^{-1} f(y)^{-1} & \text{(propriétés des homomorphismes)} & \\ = & f(x) f(x)^{-1} f(y) f(y)^{-1} & \text{(par commutativité de H)} & \\ = & e' & & \end{array}$$

   Donc $z \in \ker f$ et donc $\mathcal{D}(G) \subset \ker f$

$\Rightarrow$ Soit $\dot{y} \in G/\mathcal{D}(G)$; on pose $\overline{f}(\dot{y}) = f(y)$. En réutilisant la proposition 10.7.5, on démontre facilement que $\overline{f}$ est un homomorphisme de groupe et nous avons, pour tout $y \in G$,

$$f(y) = \overline{f}(\dot{y}) = \overline{f} \circ p(\dot{y})$$

c'est à dire $f = \overline{f} \circ p$

2. *En déduire que si K est un sous-groupe distingué de G tel que G/K soit commutatif, alors $K \supset \mathcal{D}(G)$* [1]

On considère la projection canonique $s : G \longrightarrow G/K$; s est un homomorphisme de groupe de noyau K. D'après la question précédente, $\mathcal{D}(G) \subset \ker s$, c'est à dire $\mathcal{D}(G) \subset K$.
Ce que nous voulions.

3. *On définit par récurrence le sous-groupe $\mathcal{D}^n(G)$ en posant $\mathcal{D}^0(G) = G$ et pour tout entier naturel n, $\mathcal{D}^{n+1}(G) = \mathcal{D}(\mathcal{D}^n(G))$.*
Montrer que les conditions suivantes sont équivalentes :
   (a) *Il existe un entier naturel k tel que $\mathcal{D}^k(G) = \{e\}$*
   (b) *Il existe p sous-groupes $G_1, \dots G_p$ de G tels que $G_0 = G \supset G_1 \supset \cdots \supset G_p \supset G_{p+1} = \{e\}$ et pour tout entier q tel que $0 \leqslant q \leqslant p$,G_{q+1},est un sous-groupe distingué de G_q et G_q/G_{q+1} est un groupe commutatif.*

▷ **Supposons qu'il existe un entier naturel k tel que $\mathcal{D}^k(G) = \{e\}$**
$\mathcal{D}^{i+1}(G) = \mathcal{D}\left(\mathcal{D}^i(G)\right)$ est le sous groupe dérivé de $\mathcal{D}^i(G)$ et nous avons ainsi une suite de sous-groupes décroissante, c'est à dire $\mathcal{D}^{i+1}(G) \subset \mathcal{D}^i(G)$.
On a montré aussi que un sous-groupe dérivé est toujours distingué, donc $\mathcal{D}^{i+1}(G)$ est un sous-groupe distingué de $\mathcal{D}^i(G)$, et donc, l'ensemble des classes d'équivalence modulo $\mathcal{D}^{i+1}(G)$ qu'est $\mathcal{D}^{i+1}(G)/\mathcal{D}^i(G)$ est un groupe commutatif.
Nous avons donc prouvé l'existence de k sous-groupes $G_1, \dots G_k$ de G tels que $G_0 = G \supset G_1 \supset \cdots \supset G_{k-1} \supset G_k = \{e\}$ et pour tout entier q tel que $0 \leqslant q \leqslant k$,G_{q+1},est un sous-groupe distingué de G_q et G_q/G_{q+1} est un groupe commutatif.

▷ **Réciproquement, supposons qu'il existe p sous-groupes $G_1, \dots G_p$ de G tels que $G_0 = G \supset G_1 \supset \cdots \supset G_p \supset G_{p+1} = \{e\}$ et pour tout entier q tel que $0 \leqslant q \leqslant p$,G_{q+1} est un sous-groupe distingué de G_q et G_q/G_{q+1} est un groupe commutatif.**
☒ D'après l'hypothèse, G/G_1 est un groupe commutatif, G_1 est un sous-groupe distingué de G et donc, d'après la question 3 $\mathcal{D}(G) \subset G_1$
☒ Soit $q \in \mathbb{N}$ tel que $0 \leqslant q \leqslant p+1$, et supposons que, pour tout $k \in \mathbb{N}$ tel que $0 \leqslant k < q$, on ait $\mathcal{D}^k(G) \subset G_k$
Nous avons, en particulier, $\mathcal{D}^{q-1}(G) \subset G_{q-1}$

On énonce, ici, un résultat nécessaire, dont la démonstration est facile.

Lemme

Soient G un groupe, A et B 2 sous-groupe de G
Si $A \subset B$, alors $\mathcal{D}(A) \subset \mathcal{D}(B)$

Démonstration

Si $z \in \mathcal{D}(A)$, alors $z = [x, y] = xyx^{-1}y^{-1}$ où $x \in A$ et $y \in B$
Comme $A \subset B$, nous avons aussi $x \in B$ et $y \in B$ et donc $z \in \mathcal{D}(B)$.
D'où $\mathcal{D}(A) \subset \mathcal{D}(B)$

Donc, de $\mathcal{D}^{q-1}(G) \subset G_{q-1}$, nous déduisons que $\mathcal{D}\left(\mathcal{D}^{q-1}(G)\right) \subset \mathcal{D}(G_{q-1})$, c'est à dire $\mathcal{D}^q(G) \subset \mathcal{D}(G_{q-1})$
☒ Par hypothèse, G_q est un sous-groupe distingué de G_{q-1}, que G_{q-1}/G_q est un groupe commutatif ; donc, d'après la question 3 ci-dessus, $\mathcal{D}(G_{q-1}) \subset G_q$.
Ainsi, de $\mathcal{D}^q(G) \subset \mathcal{D}(G_{q-1})$ et $\mathcal{D}(G_{q-1}) \subset G_q$, nous tirons, que, pour tout $q \in \mathbb{N}$ tel que $0 \leqslant q \leqslant p+1$, nous avons $\mathcal{D}^q(G) \subset G_q$.
En particulier, nous avons $\mathcal{D}^{p+1}(G) \subset G_{p+1} = \{e\}$.
Il existe donc $k \in \mathbb{N}$ tel que $\mathcal{D}^k(G) = \{e\}$

1. Nous trouvons une autre et meilleure démonstration dans la question 3 de l'exercice 23

Exercice 57 :

Soit Gun groupe d'élément neutre e, ayant au moins deux éléments et dont les seuls sous-groupes sont $\{e\}$ et G. Montrer que G est cyclique d'ordre premier.

Soit donc G un groupe de cardinal au moins 2, c'est à dire Card $G \geqslant 2$
Soit donc $x \in G$ tel que $x \neq e$, et on considère $\langle x\rangle = \{x^n$ avec $n \in \mathbb{Z}\}$, le sous-groupe de G engendré par x.
Comme $\langle x\rangle \neq \{e\}$, nous avons $\langle x\rangle = G$, et G est donc un groupe monogène.

→ Supposons que G soit un groupe d'ordre infini.
Alors, d'après 10.8.6, G est isomorphe à $\mathbb{Z}$; or, $\mathbb{Z}$ admet des sous-groupes non triviaux le ssous-groupes $p\mathbb{Z}$ avec $p \in \mathbb{N}$, ce qui contredit l'hypothèse.
Donc G est d'ordre fini.
G est donc monogène fini, c'est à dire cyclique.

→ Où nous montrons que n, l'ordre de G est un nombre premier.
Nous avons donc $\langle x\rangle = \left\{e, x, x^2, \cdots, x^{n-1}\right\}$.
Soit $0 \leqslant k \leqslant n-1$, et considérons le sous-groupe $\left\langle x^k\right\rangle$ engendré par l'élément x^k.
Alors Card $\left(\left\langle x^k\right\rangle\right) = \dfrac{n}{\text{pgcd}\,(n,k)}$. Ord'après l'hypothèse, $\left\langle x^k\right\rangle = G$ et nous avons donc $n = \dfrac{n}{\text{pgcd}\,(n,k)}$, c'est à dire pgcd $(n,k) = 1$, et ceci, pour tout $0 \leqslant k \leqslant n-1$; donc n est premier.

Exercice 58 :

L'objectif de cet exercice est de démontrer que les seuls groupes d'ordre 6 à isomorphisme près sont $(\mathbb{Z}/6\mathbb{Z}, +)$ et $\mathcal{S}_3$.
Soit donc G un groupe d'ordre 6.

1. *Montrer que G possède au moins un élément d'ordre 3. On note x un tel élément.*

   → Supposons G groupe cyclique
   Alors, $G = \left\{e, x, x^2, x^3, x^4, x^5\right\}$, c'est à dire que G possède un élément d'ordre 6.
   Si nous considérons x^2, alors x^2 est un élément d'ordre 3 car nous avons $\left(x^2\right)^3 = e$ et $x^2 \neq e$

   → Supposons G groupe non cyclique
   Il n'y a donc aucun élément d'ordre 6, sinon, G serait cyclique.
   Soit $x \in G$ tel que $x \neq e$
   Alors $\langle x\rangle$ le sous groupe engendré par x ; alors, d'après le théorème de Lagrange, $\langle x\rangle$ est d'ordre 2 ou d'ordre 3, c'est à dire que x est d'ordre 2 ou d'ordre 3.

   → Supposons que tous les éléments de G soient d'ordre 2, c'est à dire que tout $x \in G$ est tel que $x^2 = e$; alors G est un groupe commutatif.
   Soient $a \in G$ et $b \in G$ avec $a \neq b$ et considérons $\langle a, b\rangle$ le sous-groupe engendré par a et b.
   Alors $\langle a, b\rangle = \{a, b, ab\}$ (puisque nous avons $ab = ba$.
   C'est donc un sous-groupe d'ordre 4, ce qui est impossible puisque 4 ne divise pas 6 *(théorème de Lagrange)*. Il existe donc, dans G, un élément d'ordre 3.

2. *Montrer que G possède au moins un élément d'ordre 2. On note y un tel élément.*

   On aurait pu penser la démonstration semblable à celle ci-dessus, il n'en est rien.

   → Supposons G groupe cyclique
   Alors, $G = \left\{e, x, x^2, x^3, x^4, x^5\right\}$, c'est à dire que G possède un élément d'ordre 6.
   Si nous considérons x^3, alors x^3 est un élément d'ordre 2 car nous avons $\left(x^3\right)^2 = x^6 = e$ et $x^3 \neq e$

   → Supposons G groupe non cyclique Il n'y a donc aucun élément d'ordre 6, sinon, G serait cyclique.
   Soit $x \in G$ tel que $x \neq e$
   Alors $\langle x\rangle$ est le sous groupe engendré par x ; alors, d'après le théorème de Lagrange, $\langle x\rangle$ est d'ordre 2 ou d'ordre 3, c'est à dire que x est d'ordre 2 ou d'ordre 3.

   → Supposons que tous les éléments de G soient d'ordre 3, c'est à dire que tout $x \in G$ est tel que $x^3 = e$.

Soient $a \in G$ et $b \in G$ deux éléments de G distincts et d'ordre 3.
Alors G contient $\left\{e, a, a^2, b, b^2\right\}$ qui sont des éléments deux à deux distincts.
Comme Card $G = 6$, il existe donc un autre élément $c \in G$, distincts des précédents, tel que $G = \left\{e, a, a^2, b, b^2, c\right\}$
De plus c est nécessairement d'ordre 3.

→ Mais, bien entendu, G doit aussi contenir c^2.
On vérifie par un calcul direct que c^2 est distinct de e, a, a^2, b, b^2, c. En effet :
- ⋆ c étant d'ordre 3, $c^2 \neq e$
- ⋆ Ensuite, nous ne pouvons avoir $c^2 = a$, puisque si nous l'avions, alors $c^4 = c = a^2$, ce qui est impossible, et donc $c^2 \neq a$; on démontre aussi $c^2 \neq b$
- ⋆ De même, il nous est impossible d'avoir $c^2 = a^2$, puisque si nous l'avions, nous aurions $\left(c^2\right)^2 = \left(a^2\right)^2 \iff c^4 = a^4 \iff c = a$

Ce qui est impossible.
Ainsi G possède au moins un élément d'ordre 2.

3. *Montrer que $G = \langle x, y\rangle$*

Le groupe G contient $\left\{e, x, x^2, y\right\}$ qui sont distincts deux à deux *(nous avons $y^2 = e$).*
On peut compléter cette liste en considérant xy et x^2y.
Nous avons xy et x^2y sont distincts des précédents ; en effet, les quelques calculs suivants le montrent :

→ Si $xy = x$, alors $x^2(xy) = x^2x \iff y = x^3 = e$, ce qui est impossible. De même, si $xy = y$, en multipliant à droite par y, nous avons $x = e$; ce qui est toujours impossible

→ Si $xy = x^2$, en multipliant à gauche par x^2, nous avons $x^2(xy) = x^2 \times x^2 \iff x^3y = x^4 \iff y = x$, ce qui est impossible

→ Si $x^2y = x$, toujours par multiplication, $y = x^2$; si $x^2y = y$, alors $x^2 = e$ et si $x^2y = y$, alors $y = e$, ce qui est impossible.

Ainsi $G = \left\{e, x, x^2, y, xy, x^2y\right\}$. En particulier nous avons $G = \langle x, y\rangle$.

4. *Montrer que si G est abélien, alors G est cyclique d'ordre 6.*

Supposons G groupe abélien.
Comme nous avons $xy = yx$ avec x d'ordre 3 et y d'ordre 2 . Remarquons que 2 et 3 sont premiers entre eux ; donc, le produit xy est d'ordre 6.
De Card $G = 6$, on déduit que G est cyclique et engendré par xy.
D'après le théorème de classification des groupes cycliques 10.8.7, G est isomorphe à $(\mathbb{Z}/6\mathbb{Z}, +)$.

5. *Si G n'est pas abélien, montrer que $yx = x^2y$. Ecrire la table de multiplication de G. Conclure que $G \cong \mathcal{S}_3$*

Supposons G groupe non abélien.
Nous avons alors $yx = x^2y$. En effet :

→ Si $yx = e$, alors, en composant à gauche par y, nous avons :

$$yx = e \iff y(yx) = y \times e \iff y^2x = y \iff x = y$$

Ce qui est impossible

→ Si $yx = x$, alors, en composant à droite par x^2, nous avons :

$$yx = x \iff (yx)x^2 = x \times x^2 \iff yx^3 = x^3 \iff y = e$$

Ce qui est impossible

→ Si $yx = x^2$, alors, en composant à droite par x^2, nous avons :

$$yx = x^2 \iff (yx)x^2 = x^2 \times x^2 \iff yx^3 = x^4 \iff y = x$$

Ce qui est impossible

→ Si $yx = y$, alors, en composant à gauche par y, nous avons :

$$yx = y \iff y(yx) = y \times y \iff y^2x = e \iff x = e$$

Ce qui est impossible

Nous en déduisons que $yx = xy$ ou $yx = x^2y$. Mais comme $G = \langle x, y\rangle$ est non abélien, on a nécessairement $yx = x^2y$.

Table de multiplication de $G = \langle x, y\rangle$

$\curvearrowright$	e	x	x^2	y	xy	x^2y
e	e	x	x^2	y	xy	x^2y
x	x	x^2	e	xy	x^2y	y
x^2	x^2	e	x	x^2y	y	xy
y	y	x^2y	xy	e	x^2	x
xy	xy	y	x^2y	x	e	x^2
x^2y	x^2y	xy	y	x^2	x	e

Est ce que $G = \langle x, y\rangle$ est isomorphe à $\mathcal{S}_3$?

$\mathcal{S}_3$ est le groupe des permutations de $\{1, 2, 3\}$

Nous avons d'abord les permutations circulaires :

$$\mathrm{Id}_{\mathbb{N}_3} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \quad c = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = (1\ \ 2\ \ 3) \quad c^2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = (1\ \ 3\ \ 2)$$

Puis les transpositions :

$$\tau_{\{1,2\}} = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} \quad \tau_{\{1,3\}} = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} \quad \tau_{\{3,2\}} = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

On peut remarquer que $\tau_{\{1,3\}} \circ \tau_{\{1,2\}} = c$

En créant un homomorphisme de groupe Φ entre $G = \langle x, y\rangle$ et $\mathcal{S}_3$ en posant $\Phi(x) = c$ et $\Phi(y) = \tau_{\{1,2\}}$, on démontre facilement que Φ est un isomorphisme.

A un isomorphisme près, il n'y a que 2 groupes à 6 éléments : $(\mathbb{Z}/6\mathbb{Z}, +)$ et $\mathcal{S}_3$

6. *Justifier que les groupes $(\mathbb{Z}/6\mathbb{Z}, +)$ et $\mathcal{S}_3$ ne sont pas isomorphes*

   Ils ne peuvent pas être isomorphes puisque, si $(\mathbb{Z}/6\mathbb{Z}, +)$ est commutatif, par contre $\mathcal{S}_3$ ne l'est pas.

Exercice 59 :

Soit Δ_4 un groupe diédral à 8 éléments, de générateurs r et s avec r d'ordre 4, s d'ordre 2 et $rsrs = e$. On pose $K = \langle s\rangle$ et $H = \langle s, r^2\rangle$. Montrer que K est distingué dans H, H est distingué dans Δ_4 mais K n'est pas distingué dans Δ_4.

Nous avons $\Delta_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.

Nous avons, par calculs :

- ⋆ $sr = r^3s$ puisque, partant de $rsrs = e$, en multipliant à gauche par r^3, nous obtenons :
$$r^3(rsrs) = r^3 \Longleftrightarrow srs = r^3$$
Puis, en multipliant à droite par s, nous obtenons $(srs)\,s = r^3s \Longleftrightarrow sr = r^3s$
- ⋆ De même, $rs = sr^3$. Nous partons toujours de $rsrs = e$, nous multiplions à gauche par r^3 pour obtenir $srs = r^3$, puis toujours à gauche par s et nous obtenons $rs = sr^3$
- ⋆ Par calculs semblables, nous obtenons $sr^2 = r^2s$

De manière générale, pour $k = 0, 1, 2, 3$, nous obtenons $r^ks = sr^{4-k}$

On pose $K = \langle s\rangle$ et $H = \langle s, r^2\rangle$.

⇒ **K est un sous-groupe distingué de H** Tel que défini, le sous-groupe est donc $K = \{1, s\}$ est donc d'ordre 2.

Déterminons les éléments de H.

- ⋆ r étant un élément d'ordre 4, l'élément r^2 est d'ordre 2
- ⋆ D'autre part, $sr^2 = r^2s$

Et donc $H = \{e, s, r^2, r^2s\}$, et l'ordre de H est donc 4 et $K \subset H$.

De l'identité Card $H = [H : K]$ Card K, nous déduisons que $[H : K] = 2$, et donc que K est un sous-groupe distingué de H

$\Rightarrow$ **H est un sous-groupe distingué de Δ_4**

De la même manière, l'indice de H dans Δ_4 est $\dfrac{\text{Card } \Delta_4}{\text{Card } H} = \dfrac{8}{4} = 2$ donc H est un sous-groupe distingué de Δ_4

$\Rightarrow$ **K n'est pas un sous-groupe distingué de Δ_4**

Il faut donc trouver un élément $X \in \Delta_4$ et un élément $x \in K$ tel que $XxX^{-1} \notin K$
Pour cela, considérons l'élément $s \in K$ et $r \in \Delta_4$. Alors :

$$rsr^{-1} = rsr^3 = r\,(rs) = r^2 s.$$

Or, $r^2 s \notin K$. Cela prouve que K n'est pas distingué dans Δ_4.

Prolongements

Considérons les isométries qui conservent un carré.

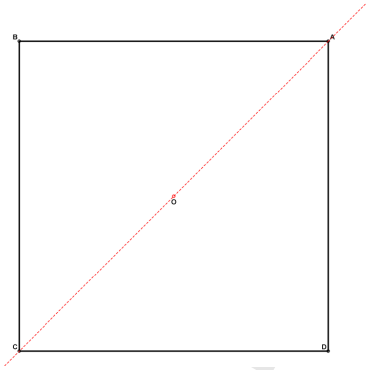


FIGURE 10.4 – Le carré

Si nous considérons la rotation de centre O et d'angle $+\dfrac{\pi}{2}$ et la symétrie s par rapport à la droite (AC), nous avons $r^4 = \text{Id}_P$ et $s^2 = \text{Id}_P$
Nous obtenons donc les permutations suivantes :

$$r = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix} = (A \quad B \quad C \quad D) \quad \text{et} \quad s = \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} = \tau_{\{B,D\}}$$

s apparaît donc comme une transposition et r comme une permutation circulaire. Nous avons aussi :

$$rs = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} = \tau_{\{B,A\}} \circ \tau_{\{C,D\}}$$

Et nous avons bien $rsrs = \text{Id}_P$ *(C'est, en fait, la symétrie orthogonale par rapport à la médiatrice du segment $[A, B]$)*
Les isométries laissant invariant un carré forment un groupe isomorphe à Δ_4. C'est, en fait, un sous-groupe de $\mathcal{S}_4$, groupe des permutations d'un ensemble à 4 éléments.
Faisons l'inventaire des transformations :

$$sr = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} = \tau_{\{A,D\}} \circ \tau_{\{B,C\}} \qquad sr^2 = \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix} = \tau_{\{A,C\}}$$

$$sr^3 = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} = \tau_{\{A,B\}} \circ \tau_{\{C,D\}} \qquad \text{On remarque que } sr^3 = rs$$

Géométriquement, sr est la symétrie orthogonale par rapport à la médiatrice du segment $[A, D]$, tandis que sr^2 la symétrie orthogonale par rapport à la diagonale (BD)

Exercice 60 :

Soient G un groupe d'ordre $n = pq$, avec $n \geqslant 2$, où p et q sont des nombres premiers, et e son élément neutre.

1. *Montrer que G a au moins un sous-groupe distinct de $\{e\}$ et de G.*

   Soit $x \in G$ tel que $x \neq e$.
   Alors, $\langle x \rangle$ est un sous-groupe de G dont l'ordre divise n. Ainsi, par hypothèses, Card $\langle x \rangle = 1$ ou Card $\langle x \rangle = p$ ou Card $\langle x \rangle = q$ ou Card $\langle x \rangle = n$, c'est à dire que x est d'ordre 1, p, q ou n
   - ⋆ Comme $x \neq e$, l'ordre ne peut être 1
   - ⋆ Si x est d'ordre p, alors $\langle x \rangle$ est bien distinct de $\{e\}$ et de G
   - ⋆ La réponse est la même si x est d'ordre q
   - ⋆ Si x est d'ordre n, alors G est cyclique et l'élément x^p est un élément d'ordre q, c'est à dire Card $\langle x^p \rangle = q$ et donc $\langle x^p \rangle$ est bien distinct de $\{e\}$ et de G

2. *Si H et H' sont deux sous-groupes propres de G tels que $H \neq H'$, montrer que $H \cap H' = \{e\}$.*

   Soient H et H', 2 sous-groupes propres de G tels que $H \neq H'$
   Ceci veut donc dire que $H \neq \{e\}$, $H' \neq \{e\}$, $H \neq G$ et $H' \neq G$; donc H et H' ont des ordres qui divisent $n = pq$
   Alors $H \cap H'$ est un sous-groupe de H dont l'ordre divise celui de H. Soit p l'ordre de H
   Si Card $H \cap H' = p$, alors $H \cap H' = H$, ce qui veut dire que $H \subset H'$, ce qui est impossible.
   Donc Card $H \cap H' = 1$, c'est à dire $H \cap H' = \{e\}$

3. *Soit H un sous-groupe de G. On appelle* **normalisateur** *de H l'ensemble $N(H)$ des éléments $x \in G$ tels que $xHx^{-1} = H$. Montrer que $N(H)$ est un sous-groupe de G.*

   Cette question a déjà été résolue

   Nous pouvons démontrer que, pour tout groupe quelconque G, si H est un sous-groupe de G, alors, pour tout $x \in G$, l'ensemble xHx^{-1} est un sous-groupe de G

   En effet, soit $x \in G$, fixé :
   - ⋆ $xHx^{-1} \neq \emptyset$ puisque $e \in xHx^{-1}$.
     Nous avons $e = xex^{-1} = xx^{-1}$. Comme $e \in H$, nous avons répondu à la question
   - ⋆ Soient $a \in xHx^{-1}$ et $b \in xHx^{-1}$; avons nous $ab \in xHx^{-1}$?
     Par hypothèses, il existe $h \in H$ et $h' \in H$ tels que $a = xhx^{-1}$ et $b = xh'x^{-1}$. Alors :

     $$ab = \left(xhx^{-1}\right)\left(xh'x^{-1}\right) = xh\left(x^{-1}x\right)h'x^{-1} = xhh'x^{-1}$$

     Nous avons bien $ab \in xHx^{-1}$
   - ⋆ Si $a \in xHx^{-1}$, avons nous $a^{-1} \in xHx^{-1}$?
     Comme tout à l'heure, il existe $h \in H$ tel que $a = xhx^{-1}$. Alors :

     $$a^{-1} = \left(xhx^{-1}\right)^{-1} = x\left(xh\right)^{-1} = x\left(h^{-1}x^{-1}\right) = xh^{-1}x^{-1}$$

     Nous avons donc $a^{-1} \in xHx^{-1}$

   xHx^{-1} est donc un sous-groupe de G appelé **sous-groupe conjugué de H**

   Redémontrons que $N(H)$ est un sous-groupe de G.
   → Tout d'abord, $N(H) \neq \emptyset$ puisque $e \in N(H)$; en effet, $eHe^{-1} = eHe = H$
   → Soient, maintenant $x \in N(H)$ et $y \in N(H)$, alors $xHx^{-1} = H$ et $yHy^{-1} = x$. Montrons que $xy \in N(H)$:

   $$xyH\left(xy\right)^{-1} = xyHy^{-1}x^{-1} = x\left(yHy^{-1}\right)x^{-1} = xHx^{-1} = H$$

   Donc $xy \in N(H)$
   → Soit $x \in N(H)$ et montrons que $x^{-1} \in N(H)$ Nous avons $xHx^{-1} = H$ et donc $x^{-1}\left(xHx^{-1}\right)x = x^{-1}Hx$, c'est à dire $\left(x^{-1}x\right)H\left(x^{-1}x\right) = x^{-1}Hx$ et donc $H = x^{-1}Hx$.
   Donc $x^{-1} \in N(H)$
   Donc $N(H)$ est un sous-groupe de G.
   Il faut faire remarquer que $H \subset N(H)$

4. *Déterminer $N(H)$ si H est un sous-groupe distingué de G, et montrer que si H n'est pas un sous-groupe distingué de G alors $N(H) = H$.*

→ Il est évident que si H est un sous-groupe distingué de G, $G = N(H)$
→ Supposons que H ne soit pas un sous-groupe distingué.
Alors $N(H) \neq G$. L'ordre de $N(H)$ est donc p ou q, nombre premier. Comme $H \subset N(H)$, l'ordre de H divise l'ordre de $N(H)$, les sous-groupes H et $N(H)$ sont de même ordre et donc $N(H) = H$

5. *On dit que deux sous-groupes H' et $H"$ de G sont conjugués, et on note $H'\mathcal{C}H"$, si et seulement si il existe un élément $x \in G$ tel que $H" = xH'x^{-1}$. Montrer que $\mathcal{C}$ est une relation d'équivalence sur l'ensemble des sous-groupes de G.*

Nous appelons $\mathfrak{H}$ l'ensemble des sous-groupes de G et nous allons montrer que $\mathcal{C}$ est une relation d'équivalence sur $\mathfrak{H}$
→ Elle est réflexive
En effet, soit $H \in \mathfrak{H}$
Alors, $eHe^{-1} = eHe = H$, et nous avons bien $H\mathcal{C}H$
→ Elle est symétrique
Soient $H \in \mathfrak{H}$ et $H' \in \mathfrak{H}$ tels que $H'\mathcal{C}H$.
Il existe alors $x \in G$ tel que $H = xH'x^{-1}$, et donc $H' = x^{-1}Hx$. Il existe donc $y \in G$, $y = x^{-1}$ tel que $H' = yHy^{-1}$ et donc nous avons $H\mathcal{C}H'$.
La relation est donc symétrique
→ Elle est transitive
Soient $H \in \mathfrak{H}$, $H' \in \mathfrak{H}$ et $H'' \in \mathfrak{H}$tels que $H\mathcal{C}H'$ et $H'\mathcal{C}H''$.
Il existe donc $x \in G$ tel que $H' = xHx^{-1}$ et $y \in G$ tel que $H'' = yH'y^{-1}$. Alors :

$$H'' = yH'y^{-1} \Longleftrightarrow H'' = y\left(xHx^{-1}\right)y^{-1} \Longleftrightarrow H'' = yxHx^{-1}y^{-1}$$

Il existe donc $z \in G$, $z = xy$ tel que $H'' = zHz^{-1}$ et donc nous avons $H\mathcal{C}H''$
La relation $\mathcal{C}$ est donc transitive
$\mathcal{C}$ est donc une relation d'équivalence sur $\mathfrak{H}$

6. *Soit H un sous-groupe de G d'ordre p. Déterminer le nombre d'éléments de la classe d'équivalence de H modulo $\mathcal{C}$*

⇒ Si H est distingué, alors, pour tout $x \in G$, $H = xHx^{-1}$ et H est le seul élément de sa classe d'équivalence
⇒ Si H n'est pas distingué en G, la classe de H modulo $\mathcal{C}$est l'ensemble des groupes conjugués de H.
Soit H_1 un sous-groupe conjugué de H. A quelles conditions sur $x \in G$ et $y \in G$, avons nous $H_1 = xHx^{-1} = yHy^{-1}$?

$$\begin{aligned} H_1 = xHx^{-1} = yHy^{-1} &\Longleftrightarrow y^{-1}\left(xHx^{-1}\right)y = H \\ &\Longleftrightarrow y^{-1}xxHx^{-1}y = H \\ &\Longleftrightarrow \left(y^{-1}x\right)H\left(y^{-1}x\right)^{-1} = H \end{aligned}$$

Ce qui veut dire que $y^{-1}x$ est un élément du normalisateur $N(H)$ de H ; autrement dit $y^{-1}x \in N(H)$.
Comme H n'est pas distingué, $N(H) = H$ et donc $y^{-1}x \in H$, et dans la relation d'équivalence modulo H, $\dot{x} = \dot{y}$, et donc $xHx^{-1} = yHy^{-1} \Longleftrightarrow \dot{x} = \dot{y}$
Le nombre de sous-groupes conjugués à H est donc le nombre de classes dans la relation d'équivalence à gauche modulo H.
C'est donc l'indice $[G : H]$, c'est à dire $\dfrac{n}{p} = \dfrac{pq}{p} = q$
Il y a donc q sous-groupes conjugués à H

7. *Démontrer que G a au moins un sous-groupe distingué différent de $\{e\}$ et de G.*

⇒ Si G est cyclique, bien entendu, G est commutatif et tous ses groupes sont distingués.
⇒ Supposons G non cyclique
→ G admet au moins un sous groupe propre, c'est à dire distinct de $\{e\}$ et de G. Appelons le H. Alors H est d'ordre p ou q. Supposons que H soit d'ordre p

→ Si H n'est pas distingué, il existe donc q sous-groupes de G qui lui sont conjugués.
Si nous appelons $H_1, H_2 \cdots, H_q$ les q sous-groupes conjugués, en soulignant que $H_1 = H$, puisque H est conjugué à lui-même.

Nous appelons $L = \bigcup_{i=1}^{q} H_i$

⋆ Bien entendu, Card H_i = Card $H = p$

⋆ Si $i \neq j$, alors $H_i \cap H_j = \{e\}$
Tout d'abord, nous avons, évidemment $e \in H_i \cap H_j$
D'autre part, H_i et H_j sont 2 sous-groupes conjugués de H, c'est à dire qu'il existe $a \in G$ et $b \in G$ tels que $H_i = aHa^{-1}$ et $H_j = bHb^{-1}$ et comme $H_i \neq H_j$, nous avons $ab^{-1} \notin H$
Soit $y \in H_i \cap H_j$, alors $y = ah_ia^{-1}$ et $y = bh_jb^{-1}$ avec $h_i \in H$ et $h_j \in H$. De $y = ah_ia^{-1} = bh_jb^{-1}$, nous tirons $H_j = b^{-1}ah_ia^{-1}b = gh_ig^{-1}$, c'est à dire $H = gHg^{-1}$.
Donc $g \in H$ et donc $b^{-1}a \in H$. Il y a contradiction et donc $H_i \cap H_j = \{e\}$

Et donc Card $L = q(p-1) + 1 = n - (q-1)$ et donc Card $L < n$

→ Nous avons donc $G \setminus L \neq \emptyset$ et soit donc $x \in G \setminus L$; nous avons $x \neq e$ puisque $e \in L$

→ On appelle $K = \langle x \rangle$ le sous groupe de G engendré par x. K est non trivial, et donc Card $K = q$ ou Card $K = p$.
G n'étant pas cyclique, nous n'avons pas Card $K = n$

→ On suppose que K n'est pas distingué en G

→ Si x est d'ordre p, la classe de K, modulo la relation d'équivalence $\mathcal{C}$, contient q sous-groupes $K_1, \cdots, K_q$ avec $K_1 = K$
Pour $1 \leqslant i \leqslant q$ et $1 \leqslant j \leqslant q$, nous avons $K_i \neq H_j$, car l'intersection des classes d'équivalences est vide
Posons $M = \bigcup_{j=1}^{q} K_j$; alors Card $(M \cup L) = q(p-1) + q(p-1) + 1 = 2n - 2q + 1 > n$, ce qui est impossible parce que nous devons avoir Card $(M \cup L) \leqslant$ Card $G = n$

→ Si x est d'ordre q, la classe de K, modulo la relation d'équivalence $\mathcal{C}$, contient p sous-groupes $K_1, \cdots, K_p$ avec $K_1 = K$
Pour $1 \leqslant i \leqslant p$ et $1 \leqslant j \leqslant q$, nous avons $K_i \neq H_j$, car l'intersection des classes d'équivalences est vide
Posons $M = \bigcup_{j=1}^{p} K_j$; alors Card $(M \cup L) = p(q-1) + q(p-1) + 1 = 2n - 2p + 1 > n$, ce qui est impossible parce que nous devons avoir Card $(M \cup L) \leqslant$ Card $G = n$

→ L'hypothèse où K n'est pas distingué est donc contradictoire.

Le sous-groupe K est donc distingué en G

Ainsi G contient au moins un sous-groupe distingué

OUF !!

Nous venons de montrer :

Tout groupe fini G d'ordre pq où p et q sont des nombres premiers possède au moins un sous-groupe distingé non trivial