Feuille 1

Exercice 1. [Ordre d'un élément / Groupe diédral, Dummit-Foot, page 27, exercice 1]
Calculer l'orde de tous les éléments des groupes :

a) D_6

b) D_8

Éléments de solution 1.

a) Considérons le groupe

$$D_6 = \langle r, s \,|\, r^3 = s^2 = \mathrm{id}, rs = sr^{-1} \rangle$$

Nous avons

$$D_6 = \{\mathrm{id}, r, r^2, s, sr, sr^2\}$$

L'ordre de id est 1.

L'ordre de r est 3 (en effet $r^2 \neq \mathrm{id}$, $r^3 = \mathrm{id}$).

L'ordre de r^2 est 3 (en effet $(r^2)^3 = r^6 = (r^3)^2 = \mathrm{id}^2 = \mathrm{id}$).

L'ordre de s est 2 (en effet $s^2 = \mathrm{id}$).

L'ordre de sr est 2 (en effet $(sr)^2 = srsr = s(rs)r = s(sr^{-1})r = s^2\mathrm{id} = s^2 = \mathrm{id}$).

L'ordre de sr^2 est 2 (en effet $(sr^2)^2 = sr^2sr^2 = sr^2(sr^{-1})r^3 = sr^2(rs)\mathrm{id} = sr^3s = s\mathrm{id}s = s^2 = \mathrm{id}$).

b) Considérons le groupe

$$D_8 = \langle r, s \,|\, r^4 = s^2 = \mathrm{id}, rs = sr^{-1} \rangle$$

Nous avons

$$D_8 = \{\mathrm{id}, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

L'ordre de id est 1.

L'ordre de r est 4 (en effet $r^2 \neq \mathrm{id}$, $r^3 \neq \mathrm{id}$ $r^4 = \mathrm{id}$).

L'ordre de r^2 est 2 (en effet $(r^2)^2 = r^4 = \mathrm{id}$).

L'ordre de r^3 est 4 (en effet $(r^3)^4 = (r^4)^3 = \mathrm{id}^3 = \mathrm{id}$).

L'ordre de s est 2 (en effet $s^2 = \mathrm{id}$).

L'ordre de sr est 2 (en effet $(sr)^2 = srsr = s(rs)r = s(sr^{-1})r = s^2 = \mathrm{id}$).

L'ordre de sr^2 est 2 (en effet $(sr^2)^2 = sr^2sr^2 = sr(rs)r^2 = sr(sr^{-1})r^2 = srsr = \mathrm{id}$).

L'ordre de sr^3 est 2 (en effet $(sr^3)^2 = sr^3sr^3 = sr^2(rs)r^3 = sr^2(sr^{-1})r^3 = sr^2sr^2 = \mathrm{id}$).

Exercice 2. [Sous-groupes cycliques / Groupe diédral, Dummit-Foot, page 60, exercice 11]
Trouver tous les sous-groupes cycliques de D_8.

Trouver un sous-groupe propre de D_8 qui n'est pas cyclique.

Éléments de solution 2.

Les sous-groupes cycliques de D_8 sont :

$$\langle \mathrm{id} \rangle = \{\mathrm{id}\} \qquad \langle s \rangle = \{\mathrm{id}, s\}$$
$$\langle r \rangle = \langle r^3 \rangle = \{\mathrm{id}, r, r^2, r^3\} \qquad \langle sr \rangle = \{\mathrm{id}, sr\}$$
$$\langle r^2 \rangle = \{\mathrm{id}, r^2\} \qquad \langle sr^2 \rangle = \{\mathrm{id}, sr^2\}$$
$$\langle sr^3 \rangle = \{\mathrm{id}, sr^3\}$$

Le groupe $\langle r^2, s \rangle = \{\mathrm{id}, r^2, s, sr^2\}$ est un sous-groupe propre de D_8 (il ne contient pas r) qui n'est pas cyclique (il ne peut pas être engendré par un seul élément).

Exercice 3. [Ordre d'un élément / Groupe diédral, Dummit-Foot, page 27, exercice 3]
Utiliser les générateurs et les relations de la présentation $\mathrm{D}_{2n} =< r, s \mid r^n = s^2 = 1, rs = sr^{-1} >$ pour montrer que chaque élément de D_{2n} qui n'est pas une puissance de r est d'ordre 2. En déduire que D_{2n} est engendré par les deux éléments s et sr, tous les deux d'ordre 2.

Éléments de solution 3.

Considérons le groupe $\mathrm{D}_{2n} =< r, s \mid r^n = s^2 = 1, rs = sr^{-1} >$.

Les éléments de D_{2n} qui ne sont pas une puissance de r sont de la forme sr^k. En effet un élément de D_{2n} qui n'est pas une puissance de r est de la forme $r^k s$ ou sr^ℓ. De plus pour tout $k \geq 1$ nous avons $r^k s = sr^{-k}$. C'est vrai pour $k = 1$ (présentation du groupe D_{2n}). Supposons que $r^k s = sr^{-k}$. Alors $r^{k+1}s = rr^k s$ mais par hypothèse de récurrence $r^k s = sr^{-k}$ donc $r^{k+1}s = rsr^{-k}$. D'après la présentation de D_{2n} nous avons $rs = sr^{-1}$ donc $r^{k+1}s = sr^{-1}r^{-k} = sr^{-(k+1)}$.

Déterminons l'ordre de sr^k. Nous avons

$$(sr^k) = sr^k sr^k = s(r^k s)r^k = s(sr^{-k})r^k = s^2 = \mathrm{id}.$$

Puisque $sr^k \neq \mathrm{id}$ l'ordre de sr^k est 2.

Le groupe D_{2n} est engendré par s et sr ; en effet le groupe D_{2n} est engendré par s et r et $r = s^2 r = s(sr)$. D'après ce qui précède sr est d'ordre 2 et par définition s est d'ordre 2.

Exercice 4. [Groupe diédral, Dummit-Foot, page 52, exercice 7]
Soit n un entier ≥ 3. Montrer que :

a) le centre du groupe diédral $Z(\mathrm{D}_{2n}) = \{1\}$, si n est impair ;

b) $Z(\mathrm{D}_{2n}) = \{1, r^k\}$, si $n = 2k$ est pair.

Éléments de solution 4.

Exercice 5. [Groupes de matrices / Ordre d'un élément, Dummit-Foot, page 35, exercices 1 et 2]

a) Soit $\mathbb{F}_2$ le corps fini de deux éléments. Montrer que l'ordre de $\mathrm{GL}_2(\mathbb{F}_2)$ est égal à 6.

b) Donner les éléments de $\mathrm{GL}_2(\mathbb{F}_2)$ et calculer l'ordre de chaque élément.

Éléments de solution 5.

a) Soit $\mathbb{F}_2$ le corps fini de deux éléments. Montrons que l'ordre de $\mathrm{GL}_2(\mathbb{F}_2)$ est égal à 6.

Le groupe $M_2(\mathbb{F}_2)$ est d'ordre $2^4 = 16$; en effet un élément de $M_2(\mathbb{F}_2)$ s'écrit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec a, b, c et d dans $\mathbb{F}_2$.

L'ordre de $\mathrm{GL}_2(\mathbb{F}_2)$ vaut

$$|\mathrm{GL}_2(\mathbb{F}_2)| = |M_2(\mathbb{F}_2)| - \#\big\{A \in M_2(\mathbb{F}_2) \mid \det A = 0\big\}$$

i.e.

$$|\mathrm{GL}_2(\mathbb{F}_2)| = 16 - \#\big\{A \in M_2(\mathbb{F}_2) \mid \det A = 0\big\}$$

Déterminons $\big\{A \in M_2(\mathbb{F}_2) \mid \det A = 0\big\}$: soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{F}_2)$. Alors $\det A = 0$ si et seulement si $ad = bc$. Nous avons l'alternative suivante :

- ou bien $a = 0$, alors
  - ou bien $b = 0$ et c, d sont libres ce qui donne quatre matrices ;
  - ou bien $b = 1$ et $c = 0$, d est libre ce qui conduit à deux matrices ;
- ou bien $a = 1$, alors
  - ou bien $d = 1$ et $b = c = 1$, ce qui donne une matrice ;
  - ou bien $d = 0$ et alors soit $b = 0$ et c est libre ce qui conduit à deux matrices, soit $b = 1$ et $c = 0$ ce qui conduit à une matrice.

Ainsi $\#\big\{A \in M_2(\mathbb{F}_2) \mid \det A = 0\big\} = 4 + 2 + 1 + 2 + 1 = 10$. Par conséquent $|\mathrm{GL}_2(\mathbb{F}_2)| = 16 - 10 = 6$.

b) Les éléments de $\mathrm{GL}_2(\mathbb{F}_2)$ sont :

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

L'ordre de $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ est 2.

L'ordre de $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ est 3.

L'ordre de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est 2.

L'ordre de $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ est 3.

L'ordre de $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ est 2.

L'ordre de $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est 1.

Exercice 6. [Groupes de matrices / Ordre d'un élément, Dummit-Foot, page 35 exercice 11]
Soient F un corps et $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$ le groupe de Heisenberg de F. Soient

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

des éléments de $H(F)$.

a) Calculer le produit XY et en déduire que $H(F)$ est fermé sous la multiplication de matrices. Montrer que $H(F)$ n'est pas abélien.

b) Donner une formule pour l'inverse X^{-1} et en déduire que $H(F)$ est fermé sous l'inverse.

c) Montrer que $H(F)$ est un groupe d'ordre $|F|^3$.

d) Trouver l'ordre de chaque élément du groupe $H\left(\mathbb{Z}/2\mathbb{Z}\right)$.

d) Montrer que chaque élément non-trivial de $H(\mathbb{R})$ est d'ordre infini.

Éléments de solution 6.

Considérons un corps F et $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$ le groupe de Heisenberg de F.
Soient

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

des éléments de $H(F)$.

a) Nous avons

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}$$

en particulier XY appartient à $H(F)$. Le groupe $H(F)$ est donc fermé sous la multiplication de matrices ;

Soient

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Alors

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

et

$$BA = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

En particulier $AB \neq BA$ et $H(F)$ n'est pas abélien.

b) Donner une formule pour l'inverse X^{-1} et en déduire que $H(F)$ est fermé sous l'inverse.

Soit $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ un élément de $H(F)$. Alors $X^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$ En particulier X^{-1} appartient à $H(F)$ et $H(F)$ est fermé sous l'inverse.

c) Montrons que $H(F)$ est un groupe d'ordre $|F|^3$.

Soit $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ un élément de $H(F)$; notons que a, b et c sont des éléments libres de F. Il s'en suit que $|H(F)| = |F|^3$.

d) Les éléments du groupe $H(\mathbb{Z}/2\mathbb{Z})$ sont

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

Nous pouvons vérifier que

- $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ est d'ordre 1.
- $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ est d'ordre 2.
- $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ est d'ordre 2.
- $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ est d'ordre 2.
- $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ est d'ordre 4.
- $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ est d'ordre 2.
- $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ est d'ordre 2.
- $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ est d'ordre 4.

d) Montrons que chaque élément non-trivial de $H(\mathbb{R})$ est d'ordre infini.

Soit $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ un élément de $H(\mathbb{R})$. Alors (récurrence) $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb+\ell ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$.

En particulier $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \mathrm{id}$ si et seulement si $\begin{cases} na = 0 \\ nb + \ell ac = 0 \\ nc = 0 \end{cases}$ autrement dit si et seulement si $a = b = c = 0$.

Exercice 7. [Groupes de matrices / Ordre d'un élément, Dummit-Foot, page 64 exemple]
Montrer que les élémentsle groupe $\mathrm{SL}_2(\mathbb{Z})$.

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

du groupe $\mathrm{SL}_2(\mathbb{Z})$ sont d'ordre fini mais que XY ne l'est pas.

Éléments de solution 7.
Considérons dans $\mathrm{SL}_2(\mathbb{Z})$ les éléments

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

D'une part $X^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ et d'autre part $-\mathrm{id}$ est d'ordre 2. Par suite X est d'ordre 4.

Nous avons $Y^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ puis $Y^3 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \mathrm{id}$.

Remarquons que $XY = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Par récurrence nous obtenons donc $(XY)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$; en particulier XY est d'ordre infini.

Exercice 8. Soit G un groupe abélien fini d'exposant e. Montrer que G contient un élément d'ordre e.

Éléments de solution 8.

Exercice 9. [Groupes de matrices / Groupe diédral / Morphismes, Dummit-Foot, page 41 exercice 25]
Soit $n \in \mathbb{N}^*$. Soient r et s les générateurs usuels de D_{2n}. Posons $\theta = 2\pi/n$. Montrer que l'application $\phi\colon \mathrm{D}_{2n} \to \mathrm{GL}_2(\mathbb{R})$ définie sur les générateurs par

$$\phi(r) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \quad \text{et} \quad \phi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

définit un morphisme injectif de D_{2n} dans $\mathrm{GL}_2(\mathbb{R})$.

Éléments de solution 9.

Exercice 10. [Groupes de matrices / Groupe des quaternions / Morphismes, Dummit-Foot, page 41 exercice 26]
Soient i et j les générateurs usuels de $Q_8 =< i, j \mid i^4 = 1, i^2 = j^2, iji = j >$. Montrer que l'application $\phi\colon Q_8 \mapsto \mathrm{GL}_2(\mathbb{C})$ définie sur les générateurs par

$$\phi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \quad \text{et} \quad \phi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

définit un morphisme injectif de Q_8 dans $\mathrm{GL}_2(\mathbb{C})$.

Éléments de solution 10.

Exercice 11. [Morphismes, Dummit-Foot, page 60 exercice 19]

a) Pour tout groupe G, montrer que l'on a une bijection entre les groupes $\mathrm{Hom}_{\mathrm{gp}}\Big(\mathbb{Z}, \mathrm{G}\Big)$ et G. Lorsque G est abélien, montrer qu'il s'agit d'un isomorphisme de groupes.

b) Déterminer

$$\mathrm{Hom}_{\mathrm{gp}}\Big(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}\Big), \qquad \mathrm{Hom}_{\mathrm{gp}}\Big(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}\Big), \qquad \mathrm{Hom}_{\mathrm{gp}}\Big(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\Big).$$

Plus généralement, expliciter une bijection entre $\mathrm{Hom}_{\mathrm{gp}}\left(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}\right)$ et l'ensemble des éléments de G d'ordre divisant n.

Éléments de solution 11.

a) Pour tout groupe G, montrons que l'on a une bijection entre les groupes $\mathrm{Hom}_{\mathrm{gp}}(\mathbb{Z}, \mathrm{G})$ et G. Lorsque G est abélien, montrons qu'il s'agit d'un isomorphisme de groupes.

Considérons

$$\begin{array}{rcl} \psi\colon \mathrm{G} & \to & \mathrm{Hom}(\mathbb{Z}, \mathrm{G}) \\ g & \mapsto & \psi_g\colon \mathbb{Z} \to \mathrm{G} \\ & & 1 \mapsto g. \end{array}$$

On constate que ψ réalise une bijection entre G et $\mathrm{Hom}(\mathbb{Z}, \mathrm{G})$.

Soit G un groupe abélien. Considérons

$$\begin{array}{rcl} \varphi\colon (\mathrm{G}, *) & \to & (\mathrm{Hom}(\mathbb{Z}, \mathrm{G}), \circ) \\ g & \mapsto & \psi_g\colon \mathbb{Z} \to \mathrm{G} \\ & & 1 \mapsto g. \end{array}$$

Soient g_1 et g_2 dans G ; alors

$$\varphi(g_1 * g_2)(k) = \varphi_{g_1 * g_2}(k) = (g_1 * g_2)^k$$

et

$$(\varphi_{g_1} \circ \varphi_{g_2})(k) = \varphi_{g_1}(k) * \varphi_{g_2}(k) = g_1^k * g_2^k.$$

Le groupe G étant abélien nous avons $(g_1 * g_2)^k = g_1^k * g_2^k$ d'où $\varphi(g_1 * g_2) = \varphi_{g_1} \circ \varphi_{g_2}$. Autrement dit φ est un isomorphisme de groupes.

b) Déterminons $\mathrm{Hom}_{\mathrm{gp}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$.

Soit $\varphi \in \mathrm{Hom}_{\mathrm{gp}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$; alors

$$\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}, \qquad \overline{1} \mapsto a$$

Nous avons d'une part $\varphi(\overline{n}) = n\varphi(\overline{1}) = na$ et d'autre part $\varphi(\overline{n}) = 0$. Il s'en suit que $na = 0$ et donc que $a = 0$. En d'autres termes φ est le morphisme trivial.

Déterminons $\mathrm{Hom}_{\mathrm{gp}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right)$.

Soit $\varphi \in \mathrm{Hom}_{\mathrm{gp}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right)$; alors

$$\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \qquad \overline{1} \mapsto \overline{a}$$

Nous avons d'une part $\varphi(\overline{n}) = n\varphi(\overline{1}) = n\overline{a}$ et d'autre part $\varphi(\overline{n}) = \overline{0}$ d'où $n\overline{a} = \overline{0}$. Il s'en suit que m divise na et $\frac{m}{\mathrm{pgcd}(m,n)}$ divise a.

Autre rédaction possible : l'ensemble $\mathrm{Hom}_{\mathrm{gp}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right)$ des morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ est un groupe abélien pour l'addition naturelle des morphismes. Posons $m' = \frac{m}{\mathrm{pgcd}(m,n)}$. Si $p\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ désigne la surjection canonique, la correspondance associant à tout $f \in \mathrm{Hom}_{\mathrm{gp}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right)$ l'élément $f \circ p(1)$ induit un isomorphisme de groupes entre $\mathrm{Hom}_{\mathrm{gp}}\left(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}\right)$ et le sous-groupe $m'\mathbb{Z}/m\mathbb{Z}$ du groupe additif $\mathbb{Z}/m\mathbb{Z}$ lequel est isomorphe à $\mathbb{Z}/\mathrm{pgcd}(m,n)\mathbb{Z}$.

Explicitons une bijection entre $\mathrm{Hom}_{\mathrm{gp}}\left(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}\right)$ et l'ensemble des éléments de G d'ordre divisant n.

L'application canonique

$$\mathbb{Z}/n\mathbb{Z} \to \mathrm{G} \qquad \overline{1} \mapsto \varphi(\overline{1})$$

est une bijection entre $\mathrm{Hom}_{\mathrm{gp}}\left(\mathbb{Z}/n\mathbb{Z}, \mathrm{G}\right)$ et l'ensemble des éléments de G d'ordre divisant n. En effet d'une part $\varphi(\overline{n}) = \varphi(\overline{1})^n$ et d'autre part $\varphi(\overline{n}) = e_{\mathrm{G}}$. Par conséquent $\varphi(\overline{1})^n = e_{\mathrm{G}}$, *i.e.* l'ordre de $\varphi(\overline{1})$ divise n.

Exercice 12. [Morphismes de réduction]

a) Soit d un diviseur de n. Montrer que le morphisme *de réduction*

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/d\mathbb{Z} \\ x \mod n = [x]_n & \mapsto & x \mod d = [x]_d \end{array}$$

est bien défini et surjectif. Quel est son noyau ?

b) Si m et n sont deux entiers premiers entre eux, montrer que le morphisme de réduction $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est un isomorphisme (*lemme chinois*).

c) Quel est le noyau du morphisme de réduction $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$? En déduire une condition nécessaire pour que ce morphisme soit un isomorphisme. Montrer que son image est isomorphe à $\mathbb{Z}/\mathrm{ppcm}(m,n)\mathbb{Z}$.
Montrer qu'un élément $(x \mod m, y \mod n)$ est dans son image si et seulement si on a

$$x \equiv y \mod \mathrm{pgcd}(n,m).$$

d) On considère le morphisme de réduction $\phi\colon \mathbb{Z}/35\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Déterminer la préimage de $([1]_7, [3]_5)$.

e) Résoudre dans $\mathbb{Z}$:

$$\begin{cases} x \equiv 1\ [45] \\ x \equiv 3\ [6] \end{cases}, \quad \begin{cases} x \equiv 4\ [45] \\ x \equiv 1\ [6] \end{cases}$$

Éléments de solution 12.

Exercice 13.

a) Soient G et H des anneaux. Montrer que $(\mathrm{G} \times \mathrm{H})^* = \mathrm{G}^* \times \mathrm{H}^*$.

b) Soient $x \in \mathrm{G}$ et $y \in \mathrm{H}$ d'ordre fini. Montrer que l'ordre de $(x,y) \in \mathrm{G} \times \mathrm{H}$ est égal au $\mathrm{ppcm}(o(x), o(y))$.

c) Calculer l'ordre de $\overline{526}$ dans $\left(\mathbb{Z}/561\mathbb{Z}\right)^*$.

Éléments de solution 13.

Exercice 14. [Sous-groupes finis, sous-groupes de type fini]

a) Montrer que les sous-groupes finis de $\mathbb{C}^*$ sont cycliques.

b) Quels sont les sous-groupes finis de $\mathbb{R}^*$?

c) Montrer qu'un sous-groupe de $(\mathbb{Q}, +)$ engendré par un nombre fini d'éléments est monogène.

d) Soit p un nombre premier. Montrer que

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b},\ a \in \mathbb{Z} \text{ et } b \text{ premier à } p \right\} \quad (\text{ "}\mathbb{Z} \text{ localisé en } p\text{"})$$

est un sous-groupe de $(\mathbb{Q}, +)$ qui n'est pas de type fini.

Éléments de solution 14.

a) Montrons que les sous-groupes finis de $\mathbb{C}^*$ sont cycliques.

Soit H un sous-groupe de $\mathbb{C}^*$. Si $z = \rho \mathrm{e}^{\mathbf{i}\theta}$ appartient à H, alors $|\mathrm{H}| = \infty$ sauf si $\rho = 1$. Ainsi si H est un sous-groupe fini de $\mathbb{C}^*$ et si nous notons n son ordre, alors

$$\mathrm{H} = \left\{ \mathrm{e}^{\mathbf{i}\theta_1}, \mathrm{e}^{\mathbf{i}\theta_2}, \ldots, \mathrm{e}^{\mathbf{i}\theta_n} \right\}.$$

Le théorème de Lagrange assure que pour tout g dans H l'ordre de g divise n d'où $(\mathrm{e}^{\mathbf{i}\theta_j})^n = \mathrm{id}$ pour tout $1 \leq j \leq n$. Il s'en suit que $n\theta_j = 2k\pi$, $k \in \mathbb{Z}$, pour tout $1 \leq j \leq n$. Par suite $\mathrm{H} = \langle \mathrm{e}^{\frac{2\mathbf{i}\pi}{n}} \rangle$.

b) Déterminons les sous-groupes finis de $\mathbb{R}^*$.

Soit G un sous-groupe fini de $\mathbb{R}^*$. Notons n l'ordre de G. Pour tout $g \in \mathrm{G}$ nous avons $g^n = 1$ d'où $|g^n| = 1$ et $|g|^n = 1$. Nous en déduisons que pour tout $g \in \mathrm{G}$ nous avons $|g| = 1$, c'est-à-dire g appartient à $\{-1, 1\}$. Il en résulte que les sous-groupes finis de $\mathbb{R}^*$ sont $\{1\}$ et $\{-1, 1\}$.

c) Montrons qu'un sous-groupe de $(\mathbb{Q}, +)$ engendré par un nombre fini d'éléments est monogène.

Supposons que G soit un sous-groupe de $(\mathbb{Q}, +)$ engendré par deux éléments $\frac{p_1}{q_1}$ et $\frac{p_2}{q_2}$, *i.e.* $\mathrm{G} = \langle \frac{p_1}{q_1}, \frac{p_2}{q_2} \rangle$. Soit $g \in \mathrm{G}$; il s'écrit

$$a_1 \frac{p_1}{q_1} + a_2 \frac{p_2}{q_2} = \frac{a_1 p_1 q_2 + a_2 p_2 q_1}{q_1 q_2} = \frac{k\mathrm{pgcd}(p_1 q_2, q_1 p_2)}{q_1 q_2}$$

Ainsi $\mathrm{G} \simeq \frac{k\mathrm{pgcd}(p_1 q_2, q_1 p_2)}{q_1 q_2} \mathbb{Z}$; en particulier G est monogène.

Un raisonnement analogue permet de conclure lorsque G est engendré par n éléments.

d) Soit p un nombre premier. Montrons que

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b},\ a \in \mathbb{Z} \text{ et } b \text{ premier à } p \right\} \quad (\text{ "}\mathbb{Z} \text{ localisé en } p\text{"})$$

est un sous-groupe de $(\mathbb{Q}, +)$ qui n'est pas de type fini.

Raisonnons par l'absurde : supposons que $\mathbb{Z}_{(p)}$ est de type fini. Alors d'après c) $\mathbb{Z}_{(p)}$ est monogène, *i.e.* $\mathbb{Z}_{(p)} = \langle \frac{a}{b} \rangle$.

Si $p = 2$, alors $\frac{a}{3b}$ appartient à $\mathbb{Z}_{(p)}$ mais $\frac{a}{3b}$ n'appartient pas à $\langle \frac{a}{b} \rangle$: contradiction.

Si $p \neq 2$, alors $\frac{a}{2b}$ appartient à $\mathbb{Z}_{(p)}$ mais $\frac{a}{2b}$ n'appartient pas à $\langle \frac{a}{b} \rangle$: contradiction.

Par conséquent $\mathbb{Z}_{(p)}$ n'est pas de type fini.

Exercice 15. [Automorphismes de $\mathbb{Z}/n\mathbb{Z}$, Perrin, Cours d'Algèbre, pages 24-26 ; Serre, Cours d'arithmétique, PUF, Paris (1970), pages 12-13]

Soient n un entier ≥ 2. Si s est un élément de $\mathbb{Z}$ notons $\overline{s}$ son image dans $\mathbb{Z}/n\mathbb{Z}$.

a) Montrer que les propriétés suivantes sont équivalentes :

1) s est premier avec n,
2) $\overline{s}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$,
3) $\overline{s}$ appartient au groupe $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

b) Montrer que $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ et $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ sont isomorphes.

c) Démontrer le

Lemme chinois. *Si p et q sont premiers entre eux, alors*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

d) Précisons maintenant la structure de $(\mathbb{Z}/n\mathbb{Z})^*$ suivant la décomposition en facteurs premiers de n. Soit n un entier, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ et les α_i dans $\mathbb{N}^*$. Montrer que $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{r} \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)^*$.

Si d divise n, désignons par C_d l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. Soit Φ_d l'ensemble des générateurs de C_d. Comme tout élément de $\mathbb{Z}/n\mathbb{Z}$ engendre l'un des C_d le groupe $\mathbb{Z}/n\mathbb{Z}$ est réunion disjointe des Φ_d et

$$n = \#\left(\mathbb{Z}/n\mathbb{Z}\right) = \sum_{d|n} \#\Phi_d = \sum_{d|n} \varphi(d).$$

e) Soit H un groupe d'ordre fini n. Supposons que pour tout diviseur d de n

$$\#\{g \in \mathrm{H} \,|\, g^d = 1\} \leq d.$$

Montrer que H est cyclique.

f) Reste à déterminer la structure des $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^*$ pour p premier. Soit p un nombre premier. Montrer que

$$\left(\mathbb{Z}/p\mathbb{Z}\right)^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

Éléments de solution 15.

a) D'après Bezout on a

$$\begin{aligned} s \text{ et } n \text{ sont premiers entre eux} &\iff \text{il existe } \lambda,\, \mu \in \mathbb{Z} \text{ tels que } \lambda s + \mu n = 1 \\ &\iff \text{il existe } \lambda \in \mathbb{Z} \text{ tel que } \overline{\lambda}\overline{s} = \overline{1} \text{ dans } \mathbb{Z}/n\mathbb{Z} \\ &\iff \overline{s} \in \left(\mathbb{Z}/n\mathbb{Z}\right)^* \end{aligned}$$

D'autre part si λ appartient à $\mathbb{Z}$, alors

$$\begin{aligned} \overline{\lambda}\overline{s} = \overline{1} &\iff \lambda\overline{s} = \overline{1} \\ &\iff \underbrace{\overline{s} + \overline{s} + \ldots + \overline{s}}_{\lambda \text{ fois}} = \overline{1} \\ &\iff \overline{1} \in \langle \overline{s} \rangle \\ &\iff \langle \overline{s} \rangle = \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

Définition. On appelle fonction d'Euler et on note $\varphi(n)$ le nombre d'entiers m tels que

$$\begin{cases} 1 \leq m \leq n \\ m \text{ premier avec } n \end{cases}$$

D'après a) on a l'égalité

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$$

Par ailleurs si p est premier il est clair que

$$\begin{cases} \varphi(p) = p - 1 \\ \varphi(p^\alpha) = p^{\alpha-1}(p-1) \text{ pour un certain } \alpha \in \mathbb{N}^* \end{cases}$$

b) Soit ψ un élément de $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$. Alors $\psi(1)$ est un générateur de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$ donc $\psi(1)$ appartient à $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ (cf a)). On peut vérifier que

$$\tau \colon \psi \mapsto \psi(1)$$

est un homomorphisme.

Soit σ défini sur $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ par $\sigma(s)x = sx$. Comme $s(x+y) = sx + sy$ on a : $\sigma(s)$ est un endomorphisme de $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$. C'est un automorphisme puisque, s étant inversible, $sx = 0$ entraîne $x = 0$.

On peut vérifier que σ et τ sont réciproques l'un de l'autre.

En particulier $\mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right)$ est un groupe abélien de cardinal $\varphi(n)$.

c) Démontrons le Lemme chinois. Soit $\overline{n}$, resp. $\widehat{n}$, resp. $\dot{n}$ la classe de n modulo pq, resp. p, resp. q. Considérons l'homomorphisme

$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \qquad \overline{n} \mapsto (\widehat{n}, \dot{n})$$

Il est injectif car $\mathrm{pgcd}(p,q) = 1$. On conclut grâce à l'égalité $\left|\mathbb{Z}/pq\mathbb{Z}\right| = \left|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}\right|$.

d) La première assertion de d) résulte du Lemme chinois.

En passant aux éléments inversibles on obtient la seconde assertion d).

Il en résulte la troisième assertion d).

e) Soit d un diviseur de n. S'il existe $g \in \mathrm{H}$ d'ordre d, alors le sous-groupe $\langle g \rangle = \{1, g, g^2, \ldots, g^{d-1}\}$ engendré par g est cyclique d'ordre d. Étant donnée l'hypothèse tout élément h de H tel que $h^d = 1$ appartient à $\langle h \rangle$. En particulier les seuls éléments de H d'ordre d sont les générateurs de $\langle g \rangle$ et il y en a $\varphi(d)$. Si c'était 0 pour une valeur de d, alors $n = \sum_{d|n} \varphi(d)$ impliquerait $|\mathrm{H}| < n$: contradiction. En particulier il existe g dans H d'ordre n et $\mathrm{H} = \langle g \rangle$.

f) On applique le e) à $\mathrm{H} = \left(\mathbb{Z}/p\mathbb{Z}\right)^*$ et $n = p - 1$. Il est en effet clair que l'équation $x^d = 1$ qui est de degré d a au plus d solutions dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 16.

Soit E un ensemble muni d'une loi de composition associative, avec un élément neutre e, et telle que tout élément de E possède un inverse à gauche.

Montrer que tout élément de E possède un inverse à droite qui coïncide avec son inverse à gauche. En déduire que E est un groupe.

Éléments de solution 16.

Soit g un élément de E. Par hypothèse g possède un inverse à gauche, *i.e.* il existe h dans E tel que $hg = e$. De même il existe k dans E tel que $kh = e$. Alors

$$g = (kh)g = k(hg) = k$$

et $gh = kh = e$: h est donc aussi inverse à droite de g. Tout élément de E admet donc un inverse à droite et à gauche, il s'en suit que E est un groupe.

Exercice 17.

Soit G un groupe tel que $g^2 = e$ pour tout g dans G. Montrer que G est abélien.

Éléments de solution 17.

Pour tous g, h dans G on a $(gh)^2 = e$, soit $ghgh = e$, d'où $(ghgh)(hg) = hg$. Mais $(ghgh)(hg) = ghgh^2g$. Or h appartient à G donc $h^2 = e$ et $ghgh^2g = ghg^2$. Puisque g est dans G on a $g^2 = e$ et $ghg^2 = gh$. Ainsi $(ghgh)(hg) = hg$ se réécrit $gh = hg$.

Exercice 18.

Soit G un groupe et soit H un sous-ensemble fini non vide de G stable pour la loi de composition du groupe G.

a) Montrer que H est un sous-groupe de G.

b) Trouver un exemple de groupe G et d'un sous-ensemble non vide de G stable pour la loi de composition du groupe G qui ne soit pas un sous-groupe de G.

Éléments de solution 18.

a) Considérons un élément h de H. Puisque H est fini et h^n appartient à H pour tout entier n, il existe deux entiers $k > m \geq 0$ tels que $h^k = h^m$. Or h admet un inverse dans G donc $h^{k-m} = e$. Mais H est stable par multiplication d'où e appartient à H et $h^{-1} = h^{k-m-1}$ appartient à H. Il en résulte que H est stable par inverse et donc que H est un sous-groupe de G.

b) Si $\mathrm{G} = (\mathbb{Z}, +)$ et $\mathrm{H} = \mathbb{N}$, alors H est un sous-ensemble non vide de G stable pour la loi de composition du groupe G qui n'est pas un sous-groupe de G.

Exercice 19.

Soit G un groupe fini.

a) Montrer que des éléments conjugués dans G sont de même ordre.

b) Deux éléments de même ordre dans G sont-ils toujours conjugués ?

c) Trouver tous les groupes abéliens finis G pour lesquels la question précédente a une réponse positive. Un exemple non abélien ?

Éléments de solution 19.

a) Soient g, h dans G et n dans $\mathbb{N}$. On a $(hgh^{-1})^n = hg^nh^{-1}$. Ainsi $(hgh^{-1})^n = e$ si et seulement si $hg^nh^{-1} = e$ si et seulement si $g^n = h^{-1}eh$ autrement dit si et seulement si $g^n = e$.

b) Deux éléments de même ordre dans un groupe fini ne sont pas toujours conjugués. Considérons par exemple le groupe $\mathbb{Z}/3\mathbb{Z}$; il contient deux éléments d'ordre 3 qui ne sont pas conjugués.

c) Soit G un groupe abélien fini. Les classes de conjugaison de G sont réduites à un élément. La question précédente a une réponse positive si et seulement si tous les éléments de G ont des ordres distincts. Or si un groupe contient un élément g d'ordre $n \geq 3$, alors il admet d'autres éléments d'ordre n, par exemple g^{-1}. Ainsi les seuls groupes abéliens qui conviennent sont le groupe trivial et le groupe $\mathbb{Z}/2\mathbb{Z}$.

Si G est le groupe des permutations $\mathcal{S}_3$, alors les éléments d'ordre 2 sont les transpositions (1 2), (1 3) et (2 3) qui sont conjuguées et les éléments d'ordre 3 sont les 3-cyles (1 2 3) et (1 3 2) qui sont également conjugués. Le groupe $\mathrm{G} = \mathcal{S}_3$ est donc un groupe fini non abélien tel que deux éléments de même ordre dans G sont toujours conjugués.

Exercice 20.

Soit $\varphi\colon \mathrm{G}_1 \to \mathrm{G}_2$ un morphisme de groupes. Soit g un élément de G_1 d'ordre fini.
Montrer que l'ordre de $\varphi(g)$ divise l'ordre de g.

Éléments de solution 20.

Soit n l'ordre de g. On a $g^n = e$ donc $\varphi(g)^n = \varphi(g^n) = \varphi(e) = e$, autrement dit l'ordre de $\varphi(g)$ divise n.

Exercice 21.

Soit G un groupe de type fini.

a) Un sous-groupe H de G est-il nécessairement de type fini ?

b) Même question en supposant de plus que G/H est fini.

Éléments de solution 21.

a) Soit G est un groupe de type fini ; G peut contenir un sous-groupe H qui n'est pas de type fini.

Considérons le sous-groupe G de $\mathrm{GL}(2,\mathbb{Q})$ engendré par les matrices

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Soit H le sous-groupe de G formé des matrices de G avec des 1 sur la diagonale. Raisonnons par l'absurde : supposons que H soit de type fini. Alors il existe un entier $N \geq 1$ tel que H soit contenu dans le sous-groupe de $\mathrm{GL}(2,\mathbb{Q})$ formé des matrices de la forme

$$\begin{pmatrix} 1 & \frac{a}{N} \\ 0 & 1 \end{pmatrix}$$

Or $A^{-N}BA^N = \begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix}$: contradiction ($2^N > N$). Ainsi H n'est pas de type fini alors que G l'est.

Considérons par exemple le groupe libre G sur deux générateurs a et b. Soit H le sous-groupe engendré par tous les éléments de la forme ab^n avec $n \in \mathbb{N}$. Raisonnons par l'absurde : supposons que H soit de type fini. Alors il existe un entier N tel que dans tout mot de H le nombre de b consécutifs soit toujours strictement inférieur à N. Or ab^N appartient à H : contradiction. Le sous-groupe H de G n'est donc pas de type fini.

b) Supposons G/H fini. On peut trouver un nombre fini d'éléments $\mathrm{G}_1 = e$, G_2, …, g_n de G tels que $\mathrm{G}/\mathrm{H} = \{g_1\mathrm{H}, g_2\mathrm{H}, \ldots, g_n\mathrm{H}\}$. Comme G est de type fini, il existe h_1, h_2, …, h_m dans G tels que : tout élément de G s'écrit comme un produit de h_i. Alors pour tous i, j il existe $1 \leq k \leq n$ et $h_{i,j} \in H$ tels que $h_i g_j = g_k h_{i,j}$.

Montrons que les $h_{i,j}$ engendrent H. Considérons un élément h dans H. Il existe i_1, i_2, …, i_r tels que $h = h_{i_1} h_{i_2} \ldots h_{i_r}$. De plus $h_{i_r} = h_{i_r} e = h_{i_r} \mathrm{G}_1 = g_{k_r} h_{i_r,1}$. D'où

$$h = h_{i_1} h_{i_2} \ldots h_{i_{r-1}} g_{k_r} h_{i_r,1}.$$

De même $h_{i_{r-1}} g_{k_r} = g_{k_{r-1}} h_{i_{r-1},k_r}$ donc

$$h = h_{i_1} h_{i_2} \ldots h_{i_{r-2}} g_{k_{r-1}} h_{i_{r-1},k_r} h_{i_r,1}.$$

Par récurrence on obtient

$$h = g_{k_1} h_{i_1,k_2} \dots h_{i_{r-1},k_r} h_{i_r,1}.$$

Enfin h et les $h_{i,j}$ appartiennent à H donc g_{k_1} est dans H et $k_1 = 1$. Par suite

$$h = h_{i_1,k_2} \dots h_{i_{r-1},k_r} h_{i_r,1}.$$

Exercice 22.

a) Déterminer les classes de conjugaison dans $\mathcal{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Éléments de solution 22.

a) Soit $c = (a_1 \ \dots \ a_k)$ un k-cycle de $\mathcal{S}_n$. Pour tout $\sigma \in \mathcal{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathcal{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \dots \leq m_r \qquad\qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ la classe de conjugaison dans $\mathcal{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathcal{S}_n$, la classe de conjugaison de σ dans $\mathcal{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathcal{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1 \ \dots \ a_{2k+1}) \qquad\qquad c' = (a'_1 \ \dots \ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1 \ a'_1) \dots (a_{2k+1} \ a'_{2k+1})$$

on a pour tout $\tau \in \mathcal{S}_n$

$$\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$$

et les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i \ j)\sigma(i \ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathcal{S}_n$.

Exercice 23.

Soit n un entier. Rappelons que $\mathcal{A}_n$ est le sous-groupe de $\mathcal{S}_n$ formé par les permutations paires.

a) Montrer que le produit de deux transpositions distinctes de $\mathcal{S}_n$ est un 3-cycle ou un produit de deux 3-cycles. En déduire que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles de $\mathcal{S}_n$.

b) i) Montrer que pour $n \geq 3$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles (1 2 3), …, (1 2 n). En déduire que $\mathcal{A}_n$ est pour $n \geq 3$ stable par tout automorphisme ϕ de $\mathcal{S}_n$ ($\mathcal{A}_n$ est donc un sous-groupe caractéristique de $\mathcal{S}_n$).

ii) Montrer que $\mathcal{A}_n$ est engendré
— si n est impair ≥ 5 par (1 2 3) et (3 4 … n) ;
— si n est pair ≥ 4 par (1 2 3) et (1 2)(3 4 … n).

c) Montrer que pour $n \geq 5$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des permutations de $\mathcal{S}_n$ de la forme $(a \ b)(c \ d)$ avec a, b, c, d deux à deux distincts.

Éléments de solution 23.

a) Soient $i < j < k < l$. On a

$$(i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l)$$

Or $(i\ j)(j\ k) = (i\ j\ k)$ donc

$$(i\ j)(k\ l) = (i\ j\ k)(j\ k\ l).$$

Tout élément σ de $\mathcal{A}_n$ est le produit d'un nombre pair de transpositions donc un produit de 3-cycles. Le sous-groupe de $\mathcal{A}_n$ engendré par les 3-cycles contient donc $\mathcal{A}_n$, c'est donc $\mathcal{A}_n$.

b) i) Soient i, j et k des éléments de $\{1, \ldots, n\}$ tels que $i < j < k$. On a

$$(i\ j\ k) = (1\ 2\ i)(2\ j\ k)(1\ 2\ i)^{-1}$$

et

$$(2\ j\ k) = (1\ 2\ j)(1\ 2\ k)(1\ 2\ j)^{-1}$$

donc $\mathcal{A}_n \subset \langle (1\ 2\ 3), \ldots, (1\ 2\ n)\rangle$. Il en résulte que

$$\mathcal{A}_n = \langle (1\ 2\ 3), \ldots, (1\ 2\ n)\rangle.$$

Soient ϕ un automorphisme de $\mathcal{S}_n$ et σ un 3-cycle. L'ordre de $\phi(\sigma)$ est 3. Donc $\phi(\sigma)$ est un produit de 3-cycles car son ordre est le ppcm des longueurs des cycles qui interviennent dans sa décomposition en cycles. Le groupe $\mathcal{A}_n$ est donc caractéristique dans $\mathcal{S}_n$.

ii) Pour $i \geq 4$ et $n \geq 4$ on a

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

Par ailleurs si $n \geq 5$ est impair, $(3\ 4\ \ldots\ n)$ est une permutation paire car c'est un cycle de longueur impaire $n-2$. Ainsi pour $n \geq 5$ impair on a

$$\mathcal{A}_n = \langle (1\ 2\ 3), (3\ 4\ \ldots\ n)\rangle$$

On a

$$(1\ 2)^{\alpha}(1\ 2\ i)(1\ 2)^{\alpha} = \begin{cases} (1\ 2\ i) \text{ pour } \alpha \text{ pair} \\ (1\ 2\ i)^{-1} \text{ pour } \alpha \text{ impair} \end{cases}$$

Donc puisque pour $i \geq 4$ et $n \geq 4$

$$(1\ 2\ i) = (3\ 4\ \ldots\ n)^{i-3}(1\ 2\ 3)(3\ 4\ \ldots\ n)^{-3+i}.$$

alors pour $i \geq 4$ impair et $n \geq 4$

$$(1\ 2\ i) = [(1\ 2)(3\ 4\ \ldots\ n)]^{i-3}(1\ 2\ 3)[(1\ 2)(3\ 4\ \ldots\ n)]^{-3+i}.$$

Et pour $i \geq 4$ pair et $n \geq 4$

$$(1\ 2\ i) = \big[\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{i-3}(1\ 2\ 3)\big((1\ 2)(3\ 4\ \ldots\ n)\big)^{-3+i}\big]^{-1}.$$

Or si $n \geq 4$ est pair $(1\ 2)(3\ 4\ \ldots\ n)$ est une pemutation paire. Par conséquent le groupe $\mathcal{A}_n$ est engendré par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \ldots\ n)$.

c) Il suffit de montrer que tout 3-cycle $(i\ j\ k)$ (avec $i < j < k$) est produit de permutations de la forme $(a\ b)(c\ d)$ où a, b, c et d sont deux à deux distincts. Puisque $n \geq 5$ il existe ℓ et m dans $\{1, 2, \ldots, n\}$ tels que i, j, k, ℓ et m soient 2 à 2 distincts. Or on a

$$(i\ j\ k) = (m\ \ell)(j\ k)(m\ \ell)(i\ k)$$

d'où le résultat.

Exercice 24. [Étude du groupe $\mathrm{O}(p,q)$, Caldero, Germoni, Histoires hédonistes de groupes et géométries, tome 1]

Soit n un entier naturel. L'ensemble des matrices symétriques définies positives de taille $n \times n$ est

$$\begin{aligned} \mathrm{S}^{++}(n,\mathbb{R}) &= \left\{ S \in \mathrm{GL}(n,\mathbb{R}) \,|\, \begin{cases} {}^{\mathrm{t}}S = S \\ \forall\, x \in \mathbb{R}^n \smallsetminus \{0\} \quad {}^{\mathrm{t}}xSx > 0 \end{cases} \right\} \\ &= \left\{ P\,{}^{\mathrm{t}}P \in \mathrm{M}(n,\mathbb{R}) \,|\, P \in \mathrm{GL}(n,\mathbb{R}) \right\} \end{aligned}$$

Cet ensemble forme un système homogène (*i.e.* un espace sur lequel un groupe agit de façon transitive).

Rappelons le théorème de décomposition polaire : la multiplication matricielle induit l'homéomorphisme

$$\mathrm{O}(n,\mathbb{R}) \times \mathrm{S}^{++}(n,\mathbb{R}) \xrightarrow{\sim} \mathrm{GL}(n,\mathbb{R}), \qquad (O,S) \mapsto OS$$

Soient p et q deux entiers naturels. Désignons par $\mathrm{O}(p,q)$ le sous-groupe de $\mathrm{GL}(p+q,\mathbb{R})$ formé des isométries de la forme quadratique standard sur $\mathbb{R}^{p+q}$ de signature (p,q) c'est-à-dire

$$x_1^2 + x_2^2 + \ldots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \ldots - x_{p+q}^2$$

dont la matrice dans la base canonique est

$$I_{p,q} = \left(\begin{array}{cccc|cccc} 1 & 0 & \ldots & 0 & & & & \\ 0 & \ddots & \ddots & \vdots & & & & \\ \vdots & \ddots & \ddots & 0 & & 0 & & \\ 0 & \ldots & 0 & 1 & & & & \\ \hline & & & & -1 & 0 & \ldots & 0 \\ & 0 & & & 0 & \ddots & \ddots & \vdots \\ & & & & \vdots & \ddots & \ddots & 0 \\ & & & & 0 & \ldots & 0 & -1 \end{array}\right)$$

Soient p et q deux entiers naturels distincts. Montrer que le groupe $\mathrm{O}(p,q)$ est homéomorphe à $\mathrm{O}(p) \times \mathrm{O}(q) \times \mathbb{R}^{pq}$.

Éléments de solution 24.

Soit $M \in \mathrm{O}(p,q) \subset \mathrm{GL}(n,\mathbb{R})$ avec $n = p+q$. La décomposition polaire assure l'existence de deux matrices $O \in \mathrm{O}(n,\mathbb{R})$ et $S \in \mathrm{S}^{++}(n,\mathbb{R})$ telles que $M = OS$.

Montrons que O et S appartiennent à $\mathrm{O}(p,q)$. Remarquons que pour cela il suffit de montrer que S appartient à $\mathrm{O}(p,q)$.

Posons $T = {}^tMM$. On peut vérifier que $S^2 = T$. Montrons que $\mathrm{O}(p,q)$ est stable par transposition :

$$\begin{aligned} M \in \mathrm{O}(p,q) &\Rightarrow MI_{p,q}{}^tM = I_{p,q} \\ &\Rightarrow {}^tM^{-1} I_{p,q} M^{-1} = I_{p,q} \\ &\Rightarrow {}^tM^{-1} \in \mathrm{O}(p,q) \\ &\Rightarrow {}^tM \in \mathrm{O}(p,q) \end{aligned}$$

On en déduit que $T = {}^tMM \in \mathrm{O}(p,q)$ et donc que $S^2 \in \mathrm{O}(p,q)$. Puisque T est, comme S, définie positive, on peut écrire $T = \exp U$ pour $U \in \mathrm{S}(n,\mathbb{R})$ bien choisie. On a alors

$$\begin{aligned} T \in \mathrm{O}(p,q) &\Leftrightarrow TI_{p,q}{}^tT = I_{p,q} \\ &\Leftrightarrow {}^tT = I_{p,q}T^{-1}I_{p,q}^{-1} \\ &\Leftrightarrow {}^t\exp(U) = I_{p,q}(\exp U)^{-1}I_{p,q}^{-1} \\ &\Leftrightarrow \exp({}^tU) = I_{p,q}\exp(-U)I_{p,q}^{-1} \\ &\Leftrightarrow \exp({}^tU) = \exp(-I_{p,q}UI_{p,q}^{-1}) \\ &\Leftrightarrow {}^tU = U = -I_{p,q}UI_{p,q}^{-1} \quad (\exp\colon \mathrm{S}(n,\mathbb{R}) \to \mathrm{S}^{++}(n,\mathbb{R}) \text{ est bijective}) \\ &\Leftrightarrow UI_{p,q} + I_{p,q}U = 0 \\ &\Leftrightarrow \frac{U}{2}I_{p,q} + I_{p,q}\frac{U}{2} = 0 \\ &\Leftrightarrow \frac{{}^tU}{2} = -I_{p,q}\frac{U}{2}I_{p,q}^{-1} \end{aligned}$$

$$\begin{aligned} T \in \mathrm{O}(p,q) &\Leftrightarrow \exp\left(\frac{{}^tU}{2}\right) = \exp\left(-I_{p,q}\frac{U}{2}I_{p,q}^{-1}\right) \\ &\Leftrightarrow {}^t\exp\left(\frac{{}^tU}{2}\right) = I_{p,q}\exp\left(\frac{U}{2}\right)^{-1}I_{p,q}^{-1} \end{aligned}$$

Or $\exp\left(\frac{U}{2}\right)$ appartient à $\mathrm{S}(n,\mathbb{R})$ et $\exp^2\left(\frac{U}{2}\right) = \exp U = T$. Par suite $\exp\left(\frac{U}{2}\right) = S$ et $SI_{p,q}{}^{\mathrm{t}}S = I_{p,q}$, *i.e.* S appartient à $\mathrm{O}(p,q)$. Enfin $O \in \mathrm{O}(p,q)$. Ainsi la décomposition polaire $M = OS \mapsto (O,S)$ induit une bijection continue

$$\mathrm{O}(p,q) \simeq \big(\mathrm{O}(p,q) \cap \mathrm{O}(n)\big) \times \big(\mathrm{O}(p,q) \cap \mathrm{S}^{++}(n,\mathbb{R})\big).$$

« Étude »de $\mathrm{O}(p,q) \cap \mathrm{O}(n)$: soit $O \in \mathrm{O}(p,q) \cap \mathrm{O}(n)$; on découpe O en blocs

$$0 = \left(\begin{array}{c|c} A & C \\ \hline B & D \end{array}\right) \in \mathrm{O}(p,q) \Leftrightarrow \left\{\begin{array}{l} {}^{\mathrm{t}}AA - {}^{\mathrm{t}}BB = I_p \\ {}^{\mathrm{t}}AC - {}^{\mathrm{t}}BD = 0 \\ {}^{\mathrm{t}}CA - {}^{\mathrm{t}}DB = 0 \\ {}^{\mathrm{t}}CC - {}^{\mathrm{t}}DD = -I_q \end{array}\right.$$

En effet

$$\begin{array}{rcl} \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix} & = & \begin{pmatrix} {}^{\mathrm{t}}A & {}^{\mathrm{t}}B \\ {}^{\mathrm{t}}C & {}^{\mathrm{t}}D \end{pmatrix} \begin{pmatrix} I_p & 0 \\ 0 & I_q \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \\ & = & \begin{pmatrix} {}^{\mathrm{t}}A & {}^{\mathrm{t}}B \\ {}^{\mathrm{t}}C & {}^{\mathrm{t}}D \end{pmatrix} \begin{pmatrix} A & C \\ -B & -D \end{pmatrix} \\ & = & \begin{pmatrix} {}^{\mathrm{t}}AA - {}^{\mathrm{t}}BB & {}^{\mathrm{t}}AC - {}^{\mathrm{t}}BD \\ {}^{\mathrm{t}}CA - {}^{\mathrm{t}}DB & {}^{\mathrm{t}}CC - {}^{\mathrm{t}}DD \end{pmatrix} \end{array}$$

D'autre part on a

$$O \in \mathrm{O}(n) \Longleftrightarrow \left\{\begin{array}{l} {}^{\mathrm{t}}AA + {}^{\mathrm{t}}BB = I_p \\ {}^{\mathrm{t}}AC + {}^{\mathrm{t}}BD = 0 \\ {}^{\mathrm{t}}CA + {}^{\mathrm{t}}DB = 0 \\ {}^{\mathrm{t}}CC + {}^{\mathrm{t}}DD = I_q \end{array}\right.$$

car

$$\begin{array}{rcl} \begin{pmatrix} I_p & 0 \\ 0 & I_q \end{pmatrix} & = & \begin{pmatrix} {}^{\mathrm{t}}A & {}^{\mathrm{t}}B \\ {}^{\mathrm{t}}C & {}^{\mathrm{t}}D \end{pmatrix} \begin{pmatrix} A & C \\ B & D \end{pmatrix} \\ & = & \begin{pmatrix} {}^{\mathrm{t}}AA + {}^{\mathrm{t}}BB & {}^{\mathrm{t}}AC + {}^{\mathrm{t}}BD \\ {}^{\mathrm{t}}CA + {}^{\mathrm{t}}DB & {}^{\mathrm{t}}CC + {}^{\mathrm{t}}DD \end{pmatrix} \end{array}$$

À partir de ${}^{\mathrm{t}}BB = 0$ on obtient $\mathrm{Tr}\,{}^{\mathrm{t}}BB = 0$. Si on écrit B sous la forme $B = (b_{ij})$ il vient $\sum_{i,j} b_{i,j}^2 = 0$ puis $B = 0$. De même $C = 0$. Par conséquent $A \in \mathrm{O}(p)$ et $D \in \mathrm{O}(q)$. Ainsi

$$\mathrm{O}(p,q) \cap \mathrm{O}(n) = \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \mid A \in \mathrm{O}(p),\, D \in \mathrm{O}(q) \right\} \simeq \mathrm{O}(p) \times \mathrm{O}(q).$$

Pour la seconde intersection on utilise que

- $\exp\colon \mathrm{S}(n,\mathbb{R}) \to \mathrm{S}^{++}(n,\mathbb{R})$ est un homéomorphisme
- $\exp\colon L = \big\{U \in \mathrm{M}(n,\mathbb{R}) \,|\, UI_{p,q} + I_{p,q}U = 0\big\} \to \mathrm{O}(p,q)$

On en déduit l'homéomorphisme

$$\mathrm{S}(n,\mathbb{R}) \cap L \simeq \mathrm{S}^{++}(n,\mathbb{R}) \cap \mathrm{O}(p,q).$$

Or $\mathrm{S}(n,\mathbb{R})$ est un espace vectoriel de dimension $\frac{n(n+1)}{2}$ et on peut vérifier que

$$\dim\big(\mathrm{S}(n,\mathbb{R}) \cap L\big) = pq$$

d'où $\mathrm{O}(p,q) \cap \mathrm{S}^{++}(n,\mathbb{R}) \simeq \mathbb{R}^{pq}$.

Finalement on a l'homéomorphisme

$$\mathrm{O}(p,q) \simeq \mathrm{O}(p) \times \mathrm{O}(q) \times \mathbb{R}^{pq}.$$

Exercice 25. [Sous-groupes additifs de $\mathbb{R}$, Francinou, Giunella, Nicolas, exercices de mathématiques, oraux x-ens, analyse 1, page 29]

Soit G un sous-groupe de $(\mathbb{R},+)$ non réduit à $\{0\}$. Montrer que G est ou bien dense dans $\mathbb{R}$, ou bien monogène, *i.e.* de la forme $a\mathbb{Z}$ avec $a > 0$ (donc discret).

Éléments de solution 25.

Si G est monogène, *i.e.* si $\mathrm{G} = a\mathbb{Z}$, avec $a > 0$, alors a est le plus petit élément strictement positif de G. Si G est dense dans $\mathbb{R}$, alors $G \cap \mathbb{R}_+^*$ n'a pas de plus petit élément mais une borne inférieure non nulle. On introduit donc

$$\mathrm{G}_+ = \mathrm{G} \cap \mathbb{R}_+^* \qquad\qquad a = \inf \mathrm{G}_+$$

Le réel $a \geq 0$ est bien défini car G_+ est non vide et minoré. En effet il existe un élément g dans G non nul donc x ou $-x$ est dans G_+ qui est minoré par 0.

On va distinguer le cas $a > 0$ du cas $a = 0$.

- Supposons $a > 0$. Montrons que a appartient à G puis que $\mathrm{G} = a\mathbb{Z}$.

  Raisonnons par l'absurde : supposons que a n'appartienne pas à G. Puisque $a > 0$, on a $2a > a$. Il existe g dans G_+ tel que $g < 2a$. Comme a n'appartient pas à G, on a les inégalités $a < g < 2a$. Il existe alors h dans G_+ tel que $h < g$. On a $a < h < g < 2a$ car a n'appartient pas à G. De plus comme G et h appatiennent à G, la différence $g - h$ appartient à G et on a même $g - h$ appartient à G_+. D'une part $a < h$ donc $a - h < 0$ et $2a - h < a$, d'autre part $g < 2a$ donc $g - h < 2a - h$. Par conséquent $g - h < a$: contradiction avec la définition de a. Par suite a appartient à G. Ainsi le groupe $a\mathbb{Z}$ engendré par a est inclus dans G.

  Réciproquement soit g un élément de G. Posons $k = E\left(\frac{g}{a}\right) \in \mathbb{Z}$. Puisque G est un groupe le réel $g - ak$ appartient à G. Comme $k \leq \frac{x}{a} < k+1$ on a $0 \leq g - ak < a = \min \mathrm{G}_+$. Nécessairement $g - ak = 0$ et $g = ak \in a\mathbb{Z}$. Il en résulte que $\mathrm{G} = a\mathbb{Z}$.
- Supposons que $a = 0$. Montrons qu'alors G est dense dans $\mathbb{R}$, autrement dit que G rencontre tout intervalle ouvert de $\mathbb{R}$. Soit $I =]a, b[$ un intervalle ouvert de $\mathbb{R}$. Comme $a = 0$ il existe $g \in G$ tel que $0 < g < b - a$. Le sous-groupe $g\mathbb{Z}$ engendré par g est inclus dans G et intersecte I (sinon il existerait $k \in \mathbb{Z}$ tel que $I \subset]kg, (k+1)g[$ ce qui contredirait l'inégalité $g < b - a$). Il s'en suit que G est dense dans $\mathbb{R}$.

Exercice 26.

Quels sont les éléments d'ordre 3 du groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

Éléments de solution 26.

On cherche $(\overline{x}, \overline{y}) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ tel que $3 = o(\overline{x}, \overline{y}) = \mathrm{ppcm}(o(\overline{x}), o(\overline{y}))$, *i.e.* tel que

- $o(\overline{x}) = 1$ et $o(\overline{y}) = 3$;
- $o(\overline{x}) = 3$ et $o(\overline{y}) = 1$;
- $o(\overline{x}) = 3$ et $o(\overline{y}) = 3$.

Par ailleurs

- $o(\overline{x}) = 3$ si et seulement si $\overline{x} \in \{\overline{1}, \overline{2}\}$,
- $o(\overline{x}) = 1$ si et seulement si $\overline{x} = \overline{0}$,
- $o(\overline{y}) = 3$ si et seulement si $\overline{y} \in \{\overline{2}, \overline{4}\}$,
- $o(\overline{y}) = 1$ si et seulement si $\overline{y} = \overline{0}$.

Il en résulte que les éléments d'ordre 3 de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ sont

$$(\overline{0}, \overline{2}), \qquad (\overline{0}, \overline{4}), \qquad (\overline{1}, \overline{0}), \qquad (\overline{2}, \overline{0}), \qquad (\overline{1}, \overline{2}), \qquad (\overline{1}, \overline{4}), \qquad (\overline{2}, \overline{2}), \qquad (\overline{2}, \overline{4}).$$

Exercice 27.

Étudier le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Éléments de solution 27.

La table de multiplication de $\mathrm{G} = \mathrm{Aut}\left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) = \{e, a_1, a_2, a_3\}$ est :

- $\forall i \; ea_i = a_i$;
- $\forall\, i \; a_i^2 = e$;
- $\forall\, i \; \forall\, j \neq i \; a_i a_j = a_k$ où $k \neq i$, $k \neq j$, où $i, j, k \in \{1, 2, 3\}$.

Tout automorphisme f de G laisse fixe e. Il permute donc les autres éléments a_1, a_2 et a_3.

Réciproquement pour toute permutation f de ces trois éléments, en posant $f(e) = e$, on obtient une bijection de G sur G qui respecte la table de multiplication ci-dessus. C'est donc un automorphisme.

Ainsi Aut(G) est d'ordre $3! = 6$ et isomorphe au groupe $\mathcal{S}_3$ des permutations de $\{1, 2, 3\}$.

Exercice 28.

Montrer que les groupes $\mathbb{R}/\mathbb{Z}$ et $\mathcal{U} = \left\{z \in \mathbb{C} \,|\, |z| = 1\right\}$ sont isomorphes.

Éléments de solution 28.

Puisque $\mathbb{R}$ est abélien, le sous-groupe $\mathbb{Z}$ est distingué. Notons

$$p\colon \mathbb{R} \to \mathbb{R}/\mathbb{Z}, \qquad\qquad x \mapsto \overline{x}$$

le morphisme canonique.

L'application $f\colon \mathbb{R} \to \mathcal{U},\ x \mapsto \exp(2\mathbf{i}\pi x)$ est un morphisme surjectif. De plus $\ker f = \{x \in \mathbb{R} \mid \exp(2\mathbf{i}\pi x) = 1\} = \mathbb{Z}$. Il existe donc un isomorphisme $\overline{f}\colon \mathbb{R}/\mathbb{Z} \to \mathcal{U}$ tel que $f = \overline{f} \circ p$.

Exercice 29.

Donner un exemple de groupe et de sous-groupes dont la réunion n'est pas un sous-groupe.

Éléments de solution 29. Dans $\mathbb{Z}$ la réunion des sous-groupes $2\mathbb{Z}$ et $3\mathbb{Z}$ n'est pas un groupe. En effet la somme $2 + 3 = 5$ d'un élément de $2\mathbb{Z}$ et d'un élément de $3\mathbb{Z}$ n'est ni multiple de 2, ni multiple de 3.

Exercice 30.

Soient G un groupe fini, H et K deux sous-groupes de G d'ordre h et k respectivement.

Si h et k sont premiers entre eux, que peut-on dire de $\mathrm{H} \cap \mathrm{K}$?

Éléments de solution 30.

$\mathrm{H} \cap \mathrm{K}$ est un sous-groupe de H et un sous-groupe de K. D'après le théorème de Lagrange l'ordre de $\mathrm{H} \cap \mathrm{K}$ divise h et divise k donc vaut 1. Autrement dit $\mathrm{H} \cap \mathrm{K} = \{e\}$.

Exercice 31.

Quel est le cardinal de $\mathrm{Aut}\left(\mathbb{Z}/4\mathbb{Z}\right)$? Et le cardinal de $(\mathbb{F}_4)^\times$?

Éléments de solution 31.

Le groupe $\mathrm{Aut}\left(\mathbb{Z}/4\mathbb{Z}\right)$ s'identifie à $\left(\mathbb{Z}/4\mathbb{Z}\right)^\times = \{\overline{1}, \overline{3}\}$, il est donc de cardinal 2.

$(\mathbb{F}_4)^\times$ est de cardinal 3 car tous les éléments non nuls sont inversibles dans un corps.

Exercice 32.

Dans les groupes suivants, donner un exemple d'élément d'ordre 4 s'il en existe, sinon donner un argument pour justifier qu'il n'y en a pas :

(a) le groupe linéaire $\mathrm{GL}_2(\mathbb{R})$;
(b) le groupe alterné $\mathcal{A}_8$;
(c) le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}_3(\mathbb{R})$ des rotations de $\mathbb{R}^3$ préservant un tétraèdre régulier T ;
(d) un groupe d'ordre 16 quelconque (attention il s'agit de déterminer si *tout* sous-groupe d'ordre 16 admet un élément d'ordre 4).

Éléments de solution 32.

(a) La rotation d'angle $\pi/2$ est un exemple d'élément d'ordre 4 dans $\mathrm{GL}_2(\mathbb{R})$, sa matrice est $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
(b) $(1\,2\,3\,4)(5\,6)$ est un exemple d'élément d'ordre 4 dans $\mathcal{A}_8$.
(c) Le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}_3(\mathbb{R})$ ne contient pas d'élément d'ordre 4. Il contient douze éléments dont huit d'ordre 3, trois d'ordre 2 et l'identité.

Autre justification possible : $\mathrm{Isom}^+(T) \subset \mathrm{SO}_3(\mathbb{R})$ est isomorphe à $\mathcal{A}_4$ et $\mathcal{A}_4$ ne contient pas d'élément d'ordre 4 (les 4-cycles ne sont pas de signature 1).
(d) Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe d'ordre 16 qui contient le neutre d'ordre 1 et des éléments d'ordre 2.

Exercice 33.

(1) Soit G un groupe abélien. Soient a et b deux éléments de G d'ordres finis premiers entre eux. Montrer que $\mathrm{ordre}(ab) = \mathrm{ordre}(a)\mathrm{ordre}(b)$.
(2) Soit G un groupe abélien fini et soit m le maximum parmi les ordres des éléments de G, m est appelé l'exposant de G. Montrer que l'ordre de tout élément de G divise m.
(3) Soient $\Bbbk$ un corps et $\mathrm{G} \subset \Bbbk^*$ un sous-groupe fini du groupe multiplicatif $\Bbbk^*$. Montrer que G est cyclique. [Indication : on peut considérer les racines du polynôme $X^m - 1 \in \Bbbk[X]$ où m est l'exposant de G.]
(4) Qu'en déduire pour le groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ avec p premier ? Qu'en déduire pour le groupe $\mathbb{C}^*$?

Éléments de solution 33.

(1) Posons m = ordre de a et n = ordre de b. On a $(ab)^{mn} = (a^m)^n(b^n)^m = 1$ donc mn est un multiple de d = ordre de (ab).

Par ailleurs on a $(ab)^d = 1$. Alors $a^d = b^{-d}$ sont de même ordre p divisant à la fois m et n (car $a^d \in \langle a\rangle$ et $b^{-d} \in \langle b\rangle$), donc $p = 1$. Autrement dit $a^d = b^{-d} = 1$ (dans un groupe le neutre est l'unique élément d'ordre 1). Ainsi d est un multiple commun de m et n donc un multiple de ppcm(m,n)$= mn$. Il en résulte que $d = mn$.

(2) Soit $x \in$ G réalisant l'ordre maximal m. Raisonnons par l'absurde : supposons qu'il existe $y \in$ G dont l'ordre q ne divise pas m. Il existe alors un premier p et des entiers $b > a$ tels que

$$m = p^a m' \qquad\qquad q = p^b q'$$

avec m', n' premiers avec p. D'après (1) l'ordre de $y^{q'}x^{p^a}$ est $p^b m' > m$: contradiction.

(3) D'après (2) tous les éléments de G sont des racines de $X^m - 1$. Or un polynôme de degré m sur un corps a au plus m racines et les m éléments du groupe $\langle x\rangle$ engendré par x fournissent déjà m racines. Il s'en suit que G $= \langle x\rangle$. En particulier G est cyclique.

(4) Pour tout premier p le groupe $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ est cyclique.

Tout sous-groupe fini de $\mathbb{C}^*$ est un groupe cyclique engendré par une racine de l'unité.

Exercice 34.

(1) Soient $n \geq 1$ et k deux entiers. Montrer l'équivalence des assertions suivantes :
(i) $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ engendre $\mathbb{Z}/n\mathbb{Z}$;
(ii) n et k sont premiers entre eux ;
(iii) $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.

(2) Montrer que $\big(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ\big) \simeq \big((\mathbb{Z}/n\mathbb{Z})^*, \times\big)$.

Éléments de solution 34.

(1) Soient $n \geq 1$ et k deux entiers. Montrons que $(i) \Longleftrightarrow (iii)$. Si $\overline{k}$ engendre $\mathbb{Z}/n\mathbb{Z}$ alors il existe $a \geq 1$ tel que

$$\underbrace{\overline{k} + \overline{k} + \ldots + \overline{k}}_{a \text{ fois}} = \overline{1}$$

et donc $\overline{a}$ est l'inverse de $\overline{k}$ modulo n.

Réciproquement si $\overline{k}$ est inversible modulo n on peut choisir d'écrire l'inverse sous la forme $\overline{a}$ avec $a \geq 1$.

Montrons que $(ii) \Longleftrightarrow (iii)$.

L'égalité $\overline{a}\overline{k} = \overline{1}$ équivaut à l'existence d'un $u \in \mathbb{Z}$ tel que $ak + un = 1$. Par Bezout ceci équivaut à k et n premiers entre eux.

(2) Montrons que $\big(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ\big) \simeq \big((\mathbb{Z}/n\mathbb{Z})^*, \times\big)$.

Puisque $\mathbb{Z}/n\mathbb{Z}$ est cyclique, un morphisme φ est entièrement déterminé par l'image d'un générateur, donc en particulier par l'image de $\overline{1}$.

φ est un automorphisme si et seulement $\varphi(\overline{1})$ est aussi un générateur de $\mathbb{Z}/n\mathbb{Z}$.

Par la question précédente on associe donc à chaque $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ un élément inversible $\overline{a} = \varphi(\overline{1}) \in (\mathbb{Z}/n\mathbb{Z})^*$.

Montrons qu'en fait φ est l'homothétie de rapport $\overline{a}$. On peut supposer $a \geq 1$. Pour tout $0 \leq x \leq n-1$ on écrit

$$\varphi(\overline{x}) = \varphi(\underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{x \text{ fois}}) = \underbrace{\varphi(\overline{1}) + \varphi(\overline{1}) + \ldots + \varphi(\overline{1})}_{x \text{ fois}} = \underbrace{\overline{a} + \overline{a} + \ldots + \overline{a}}_{x \text{ fois}} = \overline{ax}.$$

Ceci implique que la bijection

$$\varphi \in \mathrm{Aut}\Big(\mathbb{Z}/n\mathbb{Z}\Big) \mapsto \varphi(\overline{1}) \in \Big(\mathbb{Z}/n\mathbb{Z}\Big)^*$$

est un morphisme de groupes donc un isomorphisme.

Exercice 35.

Soit G un groupe abélien infini. Montrer que l'ensemble T des éléments d'ordre fini de G est un sous-groupe de G.

Si $\mathrm{T} = \{e\}$, on dit que G est sans torsion.

Montrer que G/T est sans torsion.

Éléments de solution 35.

Puisque $o(e) = 1$, on a $e \in \mathrm{T}$. Soient x, $y \in \mathrm{T}$ d'ordres k, $m \in \mathbb{N}^*$. On a $(xy)^{km} = (x^k)^m(y^m)^k = e$ donc $xy \in \mathrm{T}$. Comme $o(x) = o(x^{-1})$, on a $x^{-1} \in \mathrm{T}$. Ainsi T est un sous-groupe de G.

Considérons l'application canonique $\varphi\colon \mathrm{G} \to \mathrm{G}/\mathrm{T}$. Soit $a \in \mathrm{G}/\mathrm{T}$ d'ordre fini $s \in \mathbb{N}^*$. Il existe $x \in \mathrm{G}$ tel que $a = \varphi(x)$. On a

$$\varphi(x^s) = a^s = e$$

donc $x^s \in \mathrm{T} = \ker\varphi$. Il existe donc $r \in \mathbb{N}^*$ tel que $x^{sr} = (x^s)^r = e$ ce qui prouve que $x \in \mathrm{T}$ et donc que $a = \varphi(x) = e$. Par suite G/T est sans torsion.

Exercice 36. Soient $p < q$ deux nombres premiers tels que p divise $q - 1$. Donner un exemple de groupe non-abélien G d'ordre pq constitué de matrices triangulaires dans $\mathrm{GL}_2\big(\mathbb{Z}/q\mathbb{Z}\big)$.

Éléments de solution 36. Soient $p < q$ deux nombres premiers tels que p divise $q-1$. On a : $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$. Soit a un générateur de $\mathbb{F}_q^*$. Posons $\mathrm{H} = \langle a^k\rangle$ où k est tel que $kp = q-1$. Alors

$$\left\{\begin{pmatrix} b & c \\ 0 & b \end{pmatrix} \mid b \in \mathrm{H},\, c \in \mathbb{F}_q\right\}$$

est un groupe d'ordre pq.

Exercice 37. Le groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^*$ est-il cyclique ? Si oui, donner un générateur, et si non, donner un court argument.

Éléments de solution 37. Le groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^*$ est cyclique car c'est le groupe multiplicatif du corps fini $\mathbb{Z}/11\mathbb{Z}$.

La classe de 2 est un générateur. En effet $2^5 = 32 \equiv -1 \bmod 11$ donc 2 est bien d'ordre 10 dans $(\mathbb{Z}/11\mathbb{Z})^*$.

Exercice 38. Montrer que $\mathrm{GL}_2(\mathbb{F}_2)$ est isomorphe à $\mathcal{S}_3$.

Éléments de solution 38. Commençons par remarquer que $|\mathcal{S}_3| = |\mathrm{GL}_2(\mathbb{F}_2)| = 6$. Chaque élément $A \in \mathrm{GL}_2(\mathbb{F}_2)$ correspond à une bijection linéaire de $(\mathbb{F}_2)^2$, et donc à une permutation des trois vecteurs non nuls $v_1 = (1,0)$, $v_2 = (0,1)$ et $v_3 = (1,1)$. Autrement dit il existe $\sigma_A \in \mathcal{S}_3$ telle que $A(v_i) = v_{\sigma_A(i)}$. L'application qui à $A \in \mathrm{GL}_2(\mathbb{F}_2)$ fait correspondre $\sigma_A \in \mathcal{S}_3$ est l'isomorphisme recherché.

Exercice 39.

(1) Montrer que $(\mathbb{Z}, +)$ n'est pas isomorphe à $(\mathbb{Z}^2, +)$ et que $(\mathbb{Q}, +)$ n'est pas isomorphe à $(\mathbb{Q}^2, +)$.
(2) Montrer que le groupe abélien $(\mathbb{Q}, +)$ n'est pas de type fini.
(3) Soit G un groupe de $(\mathbb{C}^*, \cdot)$ dont chaque élément est d'ordre fini. Est-il vrai que G est forcément fini ? de type fini ?
(4) Montrer que les sous-groupes de $(\mathbb{R}, +)$ sont soit de la forme $a\mathbb{Z}$, soit denses.
(5) Que dire de $\mathbb{Z}[\sqrt{2}]$?

Éléments de solution 39.

(1) Soit $\varphi\colon \mathbb{Z} \to \mathbb{Z}^2$ un morphisme. Posons $\varphi(1) = (a, b)$. Pour tout $n \in \mathbb{Z}$ on a

$$\varphi(n) = (na, nb).$$

L'image de φ est donc contenue dans une droite et φ n'est pas surjectif.

Pour tous $\frac{a}{b}$, $\frac{c}{d} \in \mathbb{Q} \setminus \{0\}$ il existe m, $n \in \mathbb{Z} \setminus \{0\}$ tel que

$$m\frac{a}{b} + n\frac{c}{d} = 0$$

(prendre $m = -bc$ et $n = ad$). Mais cette propriété n'est pas vraie dans $\mathbb{Q}^2$: considérer par exemple $(1,0)$ et $(0,1)$. Par suite $\mathbb{Q}$ et $\mathbb{Q}^2$ ne sont pas isomorphes.

(2) Soit $\mathrm{G} = \langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots \frac{a_k}{b_k}\rangle$ un sous-groupe de $\mathbb{Q}$ de type fini. Tout élément de G peut s'écrire comme une fraction avec dénominateur égal au produit des b_i. En particulier G ne peut pas coïncider avec $\mathbb{Q}$.

(3) Soit G le groupe des racines de l'unité. On a

- G est un groupe de $(\mathbb{C}^*, \cdot)$ dont chaque élément est d'ordre fini ;
- G n'est pas fini ;
- G n'est pas de type fini.

(4) Soit G un sous-groupe de $\mathbb{R}$. Si G est trivial, alors $G = 0\mathbb{Z}$ et il n'y a rien à montrer. Supposons donc G non trivial. Posons $a = \inf\{x \in G \mid x > 0\}$.
- Supposons $a = 0$. Considérons $I =]x, x + \varepsilon[$ un intervalle ouvert. L'intervalle I contient un élément de G : par hypothèse il existe $y \in]0, \varepsilon/2[$ et l'un des multiples ny, $n \in \mathbb{Z}$, convient. Le groupe G est donc dense dans $\mathbb{R}$.
- Supposons $a > 0$. Dans ce cas l'inf est atteint, *i.e.* $a \in G$. Soit $x \in G$. On écrit $x = na + r$ avec n entier et $0 \leq r < a$. Mais alors $r = x - na \in G$; par minimalité de a on obtient que $r = 0$. Par suite $x \in a\mathbb{Z}$ et $G = a\mathbb{Z}$.

(5) Si le groupe $\mathbb{Z}[\sqrt{2}]$ était de la forme $a\mathbb{Z}$, alors 1 et $\sqrt{2}$ seraient tous les deux multiples entiers de a, donc a puis $\sqrt{2}$ seraient rationnels : contradiction. Le groupe $\mathbb{Z}[\sqrt{2}]$ est donc dense dans $\mathbb{R}$.

Exercice 40.

a) Soit G un sous-groupe fini de $\mathbb{C}^*$. Montrer que $G = \mathbb{U}_n$ où $n = [G : 1]$.
b) Soient m, $n \in \mathbb{N}^*$. Déterminer le sous-groupe de $\mathbb{C}^*$ engendré par $\mathbb{U}_m$ et $\mathbb{U}_n$.
c) Soient n, p, $q \in \mathbb{N}^*$. À quelle condition a-t-on $\mathbb{U}_n \simeq \mathbb{U}_p \times \mathbb{U}_q$?
d) Pour un tel choix montrer que $\mathrm{Aut}(\mathbb{U}_n) \simeq \mathrm{Aut}(\mathbb{U}_p) \times \mathrm{Aut}(\mathbb{U}_q)$.

Éléments de solution 40.

a) Soit G un sous-groupe fini de $\mathbb{C}^*$. Montrons que $G = \mathbb{U}_n$ où $n = [G : 1]$.
Soit G un sous-groupe fini de $\mathbb{C}^*$. D'après le théorème de Lagrange on a $z^{[G:1]} = 1$ pour tout $z \in G$. Par suite G est contenu dans $\mathbb{U}_n$. Comme $[G : 1] = [\mathbb{U}_n : 1] = n$ on obtient que $G = \mathbb{U}_n$.

b) Soient m, $n \in \mathbb{N}^*$. Déterminons le sous-groupe de $\mathbb{C}^*$ engendré par $\mathbb{U}_m$ et $\mathbb{U}_n$.
Posons $M = \mathrm{ppcm}(m, n)$. Puisque n divise M, la condition $z^n = 1$ implique $z^M = 1$. Il en résulte que $\mathbb{U}_n \subset \mathbb{U}_M$ et de même que $\mathbb{U}_m \subset \mathbb{U}_M$. Le sous-groupe $H = \mathbb{U}_n\mathbb{U}_m$, engendré par $\mathbb{U}_n$ et $\mathbb{U}_m$ est donc inclus dans $\mathbb{U}_M$ et est fini. L'inclusion $H \subset \mathbb{U}_M$ assure que $[H : 1] | M$. Le théorème de Lagrange assure que les ordres n et m de $\mathbb{U}_n$ et $\mathbb{U}_m$ divisent $[H : 1]$. Ainsi $M = \mathrm{ppcm}(n, m)$ divise $[H : 1]$. Finalement $M = [H : 1]$ et $H = \mathbb{U}_M$.

c) Soient $n, p, q \in \mathbb{N}^*$. Il est nécessaire que $p|n$ et $q|n$ afin que $\mathbb{U}_p$ et $\mathbb{U}_q$ soient des sous-groupes de $\mathbb{U}_n$. Comme $d \mapsto \mathbb{U}_d$ est un isomorphisme de l'ensemble ordonné des diviseurs de n sur l'ensemble ordonné des sous-groupes de $\mathbb{U}_n$ les conditions $\mathbb{U}_p \cap \mathbb{U}_q = \{1\}$ et $\mathbb{U}_p\mathbb{U}_q = \mathbb{U}_n$ équivalent à $\mathrm{pgcd}(p, q) = 1$ et $\mathrm{ppcm}(p, q) = n$ d'où $n = pq$.

d) Supposons que $n = pq$, n, p, $q \in \mathbb{N}^*$. Soit $\alpha \in \mathrm{Aut}(\mathbb{U}_n)$. Comme α est bijectif, $\alpha(\mathbb{U}_p)$ a le même ordre p que $\mathbb{U}_p$. Puisque $\mathbb{U}_p$ est le seul sous-groupe de $\mathbb{U}_n$ d'ordre p il est stable par α. Par restriction α induit un automorphisme β de $\mathbb{U}_p$. De même $\alpha(\mathbb{U}_q) = \mathbb{U}_q$ et par restriction α définit un élément γ de $\mathrm{Aut}(\mathbb{U}_q)$. On a donc une application

$$\phi\colon \mathrm{Aut}(\mathbb{U}_n) \to \mathrm{Aut}(\mathbb{U}_p) \times \mathrm{Aut}(\mathbb{U}_q), \qquad \alpha \mapsto (\beta, \gamma).$$

L'application ϕ est injective car tout élément de $\mathbb{U}_n$ est de la forme zz' avec $z \in \mathbb{U}_p$ et $z' \in \mathbb{U}_q$; de plus $\alpha(zz') = \beta(z)\gamma(z')$. L'application ϕ est surjective car la donnée de deux automorphismes β et γ de $\mathbb{U}_p$ et $\mathbb{U}_q$ détermine un automorphisme α de $\mathbb{U}_p \times \mathbb{U}_q = \mathbb{U}_n$ en posant $\alpha(z, z') = (\beta(z), \gamma(z'))$ (à vérifier). On a alors $\phi(\alpha) = (\beta, \gamma)$.

Enfin ϕ est un homomorphisme de groupes car la restriction de $\alpha_1 \circ \alpha_2$ au sous-groupe $\mathbb{U}_p$ est la composée $\beta_1 \circ \beta_2$ des restrictions de α_1 et α_2 et de même pour $\mathbb{U}_q$.

Exercice 41.

(1) Montrer que $\mathrm{GL}_n(\mathbb{C})$ est connexe par arcs.

(2) Montrer que $\mathrm{GL}_n(\mathbb{R})$ n'est pas connexe par arcs.

Éléments de solution 41.

(1) Montrons que $\mathrm{GL}_n(\mathbb{C})$ est connexe par arcs. Soient A et B deux éléments de $\mathrm{GL}_n(\mathbb{C})$. Considérons l'application $P\colon \mathrm{M}_n(\mathbb{C}) \to \mathbb{C}$ donnée par $P(z) = \det(zB + (1 - z)A)$. Par définition du déterminant cette application est un polynôme en z. De plus $P(0) = \det A \neq 0$. Ainsi P est un polynôme non nul. Notons z_1, z_2, …, z_r les racines de P. On a $P(0) = \det A \neq 0$ et $P(1) = \det B \neq 0$; par suite 0 et 1 ne font pas partie des z_k. Il existe donc une fonction continue $e\colon [0, 1] \to \mathbb{C} \setminus \{z_1, z_2, \ldots, z_r\}$ telle que $e(0) = 0$ et $e(1) = 1$. Considérons $c\colon [0, 1] \to \mathrm{M}_n(\mathbb{C})$

donnée par $c(t) = e(t)B + (1 - e(t))A$. Notons que c est à valeurs dans $\mathrm{GL}_n(\mathbb{C})$; en effet $\det c(t) = P(e(t)) \neq 0$ pour $t \in [0,1]$. De plus $c(0) = A$ et $c(1) = B$.

(2) L'ensemble $\mathrm{GL}_n(\mathbb{R})$ n'est pas connexe car on peut l'écrire comme union disjointe de deux ouverts non vides

$$U = \big\{A \in \mathrm{M}_n(\mathbb{R}) \mid \det A > 0\big\}$$

et

$$V = \big\{A \in \mathrm{M}_n(\mathbb{R}) \mid \det A < 0\big\}$$

Ce sont bien des ouverts (car, par exemple, U est l'image réciproque de l'ouvert $]0, +\infty[$ par l'application continue det).

On peut directement montrer que $\mathrm{GL}_n(\mathbb{R})$ n'est pas connexe par arcs. Considérons A, B dans $\mathrm{GL}_n(\mathbb{R})$ tels que $\det A > 0$ et $\det B < 0$. Raisonnons par l'absurde : supposons que $\mathrm{GL}_n(\mathbb{R})$ soit connexe par arcs. Il existe alors un chemin $c\colon [0,1] \to \mathrm{GL}_n(\mathbb{R})$ tel que $c(0) = A$ et $c(1) = B$. Par suite l'application $f\colon [0,1] \to \mathbb{R}$ donnée par $f = \det \circ c$ est continue. Ainsi $f(0)$ et $f(1)$ sont de signe opposé ; le théorème des valeurs intermédiaires implique l'existence de t_0 tel que $f(t_0) = 0$. La matrice $c(t_0)$ est alors de déterminant nul : contradiction.

Exercice 42. Montrer que $\mathrm{SO}_n(\mathbb{R})$ est connexe par arcs.

Éléments de solution 42. Montrons que $\mathrm{SO}_n(\mathbb{R})$ est connexe par arcs.

Soit $M \in \mathrm{SO}_n(\mathbb{R})$. Il existe $O \in \mathrm{O}_n(\mathbb{R})$ telle que

$$M = {}^{\mathrm{t}}O \,\mathrm{diag}(1, \ldots, 1, R(\theta_1), \ldots, R(\theta_s))\, O$$

où $R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$. La matrice $M_t = {}^{\mathrm{t}}O \,\mathrm{diag}(1, \ldots, 1, R(t\theta_1), \ldots, R(t\theta_s))\, O$ fournit alors un chemin $[0,1] \to \mathrm{SO}_n(\mathbb{R})$ tel que $M_0 = \mathrm{Id}$ et $M_1 = M$. Le groupe $\mathrm{SO}_n(\mathbb{R})$ est donc bien connexe par arcs.