## I
## Lois de composition interne

**1.** Les applications

$$\begin{array}{ccc} \mathbb{N}\times\mathbb{N} & \longrightarrow & \mathbb{N} \\ (x,y) & \longmapsto & x\wedge y \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathbb{N}\times\mathbb{N} & \longrightarrow & \mathbb{N} \\ (x,y) & \longmapsto & x\vee y \end{array}$$

sont-elles associatives ? commutatives ? Admettent-elles un élément neutre ?

**2.** Soient $E$, un ensemble et $X = \mathscr{A}(E,E)$, l'ensemble des applications de $E$ dans $E$. L'application

$$\begin{array}{ccc} X\times X & \longrightarrow & X \\ (f,g) & \longmapsto & f\circ g \end{array}$$

est une loi de composition interne. Est-elle associative ? commutative ? Admet-elle un élément neutre ?

## II
## Groupes

**3. Éléments conjugués**
Soit $(G,\star)$, un groupe.
**3.1** ✍ *Deux éléments $x$ et $y$ de $G$ sont dits **conjugués** lorsque*

$$\exists\, s\in G,\quad y = s\star x\star s^{-1}.$$

**3.2** On note $x\,\mathscr{R}\,y$ lorsque $x$ et $y$ sont conjugués. La relation de conjugaison $\mathscr{R}$ est une relation d'équivalence sur $G$.

**4. Centralisateur d'une partie**
Soient $(G,\star)$, un groupe et $A$, une partie de $G$.
**4.1** ✍ *Le **centralisateur** $Z(A)$ de la partie $A$ est défini par*

$$Z(A) = \big\{x\in G\ :\ \forall\, a\in A,\quad x\star a = a\star x\big\}.$$

**4.2** Le centralisateur de $A\subset G$ est un sous-groupe de $(G,\star)$.
**4.3** ✍ *Le **centre** du groupe $(G,\star)$ est le centralisateur de $G$.*
**4.4** Le centre de $G$ est un sous-groupe commutatif de $(G,\star)$.

**5. Sous-groupes distingués**
Soit $(G,\star)$, un groupe.
Pour tout sous-groupe $H$ de $(G,\star)$ et tout $a\in G$, on pose

$$aHa^{-1} = \big\{a\star x\star a^{-1},\ x\in H\big\}.$$

**5.1** Pour tout $a\in G$, l'application $\big[x\mapsto a\star x\star a^{-1}\big]$ est un automorphisme du groupe $(G,\star)$.
**5.2** L'ensemble $aHa^{-1}$ est un sous-groupe de $(G,\star)$.
**5.3** Si $aHa^{-1}=H$, alors $a^{-1}Ha = H$.
**5.4** ✍ *Le **normalisateur** $N(H)$ d'un sous-groupe $H$ est défini par*

$$N(H) = \big\{s\in G\ :\ sHs^{-1} = H\big\}.$$

**5.5** Le normalisateur d'un sous-groupe $H$ de $(G,\star)$ est un sous-groupe de $(G,\star)$.
**5.6** ✍ *Un sous-groupe $H$ est **distingué** lorsque*

$$\forall\, s\in G,\qquad sHs^{-1} = H.$$

**5.7** Un sous-groupe $H$ de $(G,\star)$ est distingué si, et seulement si,

$$\forall\, s\in G,\qquad sHs^{-1}\subset H.$$

**5.8** Tout sous-groupe d'un groupe abélien est distingué.
**5.9** Si $f : (G,\star)\to(H,\otimes)$ est un morphisme de groupes, alors $\operatorname{Ker} f$ est un sous-groupe distingué de $(G,\star)$.
Réciproquement, tout sous-groupe distingué est le noyau d'un morphisme de groupes. →**[19.3]**
**5.10** *Suite de* **[4]** – Le centre du groupe $(G,\star)$ est un sous-groupe distingué de $(G,\star)$.
**5.11** *Suite de* **[4]** – Le normalisateur $N(H)$ d'un sous-groupe $H$ de $(G,\star)$ est un sous-groupe distingué du centralisateur $Z(H)$.

### II.1 Parties génératrices

**6. Sous-groupe engendré par une partie**
Soient $(G,\star)$, un groupe et $A$, une partie de $G$. On note $\mathcal{G}$, l'ensemble des sous-groupes de $(G,\star)$ et on pose

$$\langle A\rangle = \bigcap_{\substack{H\in\mathcal{G}\\ A\subset H}} H.$$

Démontrer que $\langle A\rangle$ est un sous-groupe de $(G,\star)$.

**7.** Soient $f$, un morphisme du groupe $(G,\star)$ dans le groupe $(H,\otimes)$ et $A$, une partie de $G$.
**7.1** L'image directe $f_*(\langle A\rangle)$ est un sous-groupe de $(H,\otimes)$ qui contient $B = f_*(A)$, donc

$$\langle B\rangle\subset f_*(\langle A\rangle).$$

**7.2** L'image réciproque $f^*(\langle B\rangle)$ est un sous-groupe de $(G,\star)$ qui contient $A$, donc

$$\langle A\rangle\subset f^*(\langle B\rangle).$$

**7.3** Pour toute partie $A\subset G$,

$$f_*(\langle A\rangle) = \langle f_*(A)\rangle.$$

**8. Sous-groupe dérivé [5]**
Soit $(G,\star)$, un groupe.
**8.1** Pour toute partie $A\subset G$, le sous-groupe $H = \langle A\rangle$ est distingué si, et seulement si,

$$\forall\, a\in A,\ \forall\, s\in G,\quad s\star a\star s^{-1}\in H.$$

**8.2** ✍ *Le **sous-groupe dérivé** $D(G)$ est le sous-groupe de $G$ engendré par la partie*

$$A = \big\{x\star y\star x^{-1}\star y^{-1},\ (x,y)\in G\times G\big\}.$$

**8.3** Le sous-groupe dérivé $D(G)$ est un sous-groupe distingué de $(G,\star)$.

**9. Sous-groupe engendré par un élément**
Soient $(G,\star)$, un groupe et $x_0\in G$.
**9.1** Pour tout $x_0\in G$, l'application

$$\varphi_{x_0} = [n\mapsto x_0^n]$$

est un morphisme de groupes de $(\mathbb{Z},+)$ dans $(G,\star)$.
**9.2** L'ensemble

$$\langle x_0\rangle = \{x_0^n,\ n\in\mathbb{Z}\}$$

est un sous-groupe de $(G,\star)$.
**9.3** Soit $H$, un sous-groupe de $\langle x_0\rangle$. L'image réciproque de $H$ par $\varphi_{x_0}$ est un sous-groupe de $(\mathbb{Z},+)$.

**9.4** Un ensemble $H$ est un sous-groupe de $\langle x_0\rangle$ si, et seulement si, il existe un entier $k \in \mathbb{N}^*$ tel que

$$H = \langle x_0^k\rangle.$$

**9.5** On pose $m = \#\langle x_0\rangle$. Alors les éléments

$$e_G = x_0^0, \quad x_0 = x_0^1, \quad \ldots, \quad x_0^{m-1}$$

sont deux à deux distincts et

$$x_0^m \in \{x_0^k\,,\, 0 \leqslant k < m\}.$$

On a alors $x_0^m = e_G$. →**[16]**

**10. Sous-groupe engendré par deux éléments [6]**
Soient $(G,\star)$, un groupe et $x$, $y$, deux éléments de $G$.
**10.1** On suppose que $x \star y = y \star x$. Alors l'application

$$\left[(k,\ell) \mapsto x^k \star y^\ell\right]$$

est un morphisme de groupes de $(\mathbb{Z}^2,+)$ dans $(G,\star)$ dont l'image est le sous-groupe $\langle\{x,y\}\rangle$.
**10.2** On suppose que $x \star y \neq y \star x$. Alors un élément $z$ de $G$ appartient au sous-groupe $\langle\{x,y\}\rangle$ si, et seulement si, il existe un entier $n \geqslant 1$ et des entiers relatifs $m_1, m_2, \ldots, m_{2n}$ tels que

$$z = x^{m_1} \star y^{m_2} \star x^{m_3} \star y^{m_4} \star \cdots \star x^{m_{2n-1}} \star y^{m_{2n}}.$$

**10.3** On suppose que $x \star y = y^{-1} \star x$. Alors

$$y \star x = x \star y^{-1}, \quad y \star x^{-1} = x^{-1} \star y^{-1}, \quad x^{-1} \star y = y^{-1} \star x^{-1}.$$

On en déduit que

$$\forall\, m \in \mathbb{Z}, \quad y \star x^m = x^m \star y^{(-1)^m}$$

puis que

$$\forall\, (m,n) \in \mathbb{Z}^2, \quad y^n \star x^m = x^m \star y^{(-1)^m n}.$$

Un élément $z$ de $G$ appartient donc au sous-groupe $\langle\{x,y\}\rangle$ si, et seulement si, il existe deux entiers relatifs $m$ et $n$ tels que

$$z = x^m \star y^n.$$

**11.** Soient $H_1$ et $H_2$, deux sous-groupes de $(G,\star)$.
**11.1** On suppose que l'ensemble $H_1 \cup H_2$ est un sous-groupe de $(G,\star)$. Démontrer que :
— ou bien $H_1 \subset H_2$,
— ou bien $H_2 \subset H_1$.
**11.2** *Suite de* **[6]** – Démontrer que

$$H_1 = \bigcap_{\substack{H\in\mathcal{G}\\ H_1\subset H}} H$$

et que $\langle H_1 \cup H_2\rangle$ est un sous-groupe de $(G,\star)$ qui contient à la fois $H_1$ et $H_2$.
**12.** L'ensemble $\mathbb{U}$ des nombres complexes de module 1 est muni d'une structure de groupe pour la multiplication complexe.
**12.1** Pour tout $n \in \mathbb{N}^*$, l'ensemble $\mathbb{U}_n$ des racines $n$-ièmes de l'unité est un sous-groupe de $(\mathbb{U},\times)$.
**12.2** L'union des sous-groupes $\mathbb{U}_n$ pour $n \in \mathbb{N}^*$ est un sous-groupe de $(\mathbb{U},\times)$.

## II.2 Groupes finis

**13.** Le seul sous-groupe fini de $(\mathbb{C},+)$ est $\{0\}$.

**14.** Soit $G$, un sous-groupe fini de $(\mathbb{C}^*,\times)$ dont le cardinal est noté $n \in \mathbb{N}^*$.
**14.1** Soit $x_0 \in G$.
En étudiant l'ensemble

$$\langle x_0\rangle = \{x_0^k,\, k \in \mathbb{Z}\},$$

on montre que le module de $x_0$ est égal à 1.
L'application $[x \mapsto x_0 x]$ est une bijection de $G$ sur $G$, donc

$$\prod_{x\in G} x = \prod_{x\in G}(x_0 x)$$

et $x_0^n = 1$.
**14.2** Le sous-groupe $G$ est égal à $\mathbb{U}_n$.
**15. Un groupe produit**
Pour tout entier $n \geqslant 1$, on pose

$$\zeta_n = \exp\frac{2i\pi}{n}.$$

**15.1** Si les entiers $m$ et $n$ sont premiers entre eux, alors le couple $(\zeta_m,\zeta_n)$ engendre le groupe produit $\mathbb{U}_m \times \mathbb{U}_n$.
**15.2** On suppose que $d = m \wedge n \geqslant 2$. Alors **[9.5]** le cardinal de l'ensemble

$$\langle(\zeta_m,\zeta_n)\rangle = \big\{(\zeta_m^k,\zeta_n^k),\, k \in \mathbb{Z}\big\}$$

est égal à $m \vee n = \frac{mn}{d}$.
**16. Ordre d'un élément [9]**
Soit $(G,\star)$, un groupe fini.
**16.1** Pour tout $x \in G$, l'application $f_x = [n \mapsto x^n]$ est un morphisme de groupes de $(\mathbb{Z},+)$ dans $(G,\star)$.
**16.2** Le morphisme $f_x$ n'étant pas injectif, il existe un, et un seul, entier $a \geqslant 1$ tel que $\operatorname{Ker} f = a\mathbb{Z}$ et

$$\forall\, n \in \mathbb{Z}, \qquad x^n = e_G \iff a \mid n.$$

**16.3** ✍ *L'**ordre** de $x \in G$ est le plus petit $a \in \mathbb{N}^*$ tel que*

$$x^a = e_G.$$

**16.4** Si l'ordre de $x$ est égal à $a$, alors **[9.5]**

$$\#\{e_G, x, x^2, \ldots, x^{a-1}\} = a.$$

**16.5** Si l'ordre de $x$ est égal à $\#(G)$, alors $G = \langle x\rangle$.

**17.** Pour tout entier $n \geqslant 2$, l'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un groupe multiplicatif.
**17.1** Le groupe multiplicatif

$$(\mathbb{Z}/9\mathbb{Z})^\times = \{\pm1, \pm2, \pm4\}$$

est engendré par $\pm2$ **[9]** et isomorphe au groupe $(\mathbb{Z}/8\mathbb{Z},+)$.
**17.2** Les groupes multiplicatifs

$$(\mathbb{Z}/10\mathbb{Z})^\times = \{\pm1, \pm3\} \quad \text{et} \quad (\mathbb{Z}/12\mathbb{Z})^\times = \{\pm1, \pm5\}$$

sont respectivement engendrés par $\pm3$ et par $\pm5$. Ils sont isomorphes au groupe $(\mathbb{Z}/4\mathbb{Z},+)$.
**17.3** Le groupe multiplicatif

$$(\mathbb{Z}/16\mathbb{Z})^\times = \{\pm1, \pm3, \pm5, \pm7\}$$

est isomorphe au groupe produit

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \oplus).$$

Ce groupe d'ordre 8 ne contient aucun élément d'ordre 8 **[16]**.
**18. Classes à gauche modulo** $H$
Soit $H$, un sous-groupe du groupe $(G,\star)$.
**18.1** La relation $\mathscr{R}$ définie par

$$\forall\, x,y \in G, \quad x \mathscr{R} y \iff x^{-1} \star y \in H$$

est une relation d'équivalence.

**18.2** Pour tout $x \in G$, la classe d'équivalence de $x$ pour la relation $\mathscr{R}$ est égale à l'ensemble $xH$ défini par

$$xH = \{x \star u,\ u \in H\}.$$

**18.3** Quels que soient $a$ et $b$ dans $G$,

$$\begin{aligned} a \mathscr{R} b &\iff aH = bH \\ &\iff b^{-1} \star a \in H. \end{aligned}$$

**18.4** Soit $a \in G$. L'application $[x \mapsto a \star x]$ est une bijection de $H$ sur $aH$. (Préciser la bijection réciproque.) Est-ce un morphisme de groupes ?

**18.5** La classe $aH$ est un sous-groupe de $(G, \star)$ si, et seulement si, $a \in H$.

Autrement dit : la classe $aH$ est un sous-groupe de $(G, \star)$ si, et seulement si, $aH = H$.

**18.6** ✍ *L'**indice** du sous-groupe $H$ est le nombre, noté $|G : H|$, de classes d'équivalence de la relation $\mathscr{R}$.*

**18.7 Théorème de Lagrange**

Si l'ensemble $G$ est fini, alors

$$\forall\, x \in G, \quad \#(xH) = \#(H).$$

Comme les classes d'équivalence de $\mathscr{R}$ définissent une partition de $G$,

$$\#(G) = |G : H| \times \#(H)$$

donc l'ordre $\#(H)$ et l'indice $|G : H|$ du sous-groupe $H$ divisent l'ordre de $G$.

## II.3 Groupes quotients

**19. Groupe quotient [18]**

Soit $H$, un sous-groupe distingué [**5**] de $(G, \star)$.

**19.1** L'ensemble des classes d'équivalence modulo $H$

$$G/H = \{xH,\ x \in G\}$$

est muni d'une structure de groupe pour l'opération $\otimes$ définie par

$$\forall\, a, b \in G, \quad aH \otimes bH = (a \star b)H.$$

**19.2** Pour tout entier $n \in \mathbb{N}^*$, l'ensemble $n\mathbb{Z}$ est un sous-groupe distingué de $(\mathbb{Z}, +)$. Expliciter les éléments du groupe quotient $\mathbb{Z}/n\mathbb{Z}$.

**19.3 Projection canonique**

L'application $\pi : G \to G/H$ définie par

$$\forall\, x \in G, \quad \pi(x) = xH$$

est un morphisme de groupes. Ce morphisme est surjectif et $\operatorname{Ker} \pi = H$. De plus,

$$\#(G) = \#(G/H) \times \#(H).$$

**20.** On suppose que le groupe $(G, \star)$ admet un sous-groupe $H$ dont l'indice [**18.6**] est égal à 2.

**20.1** Si $x \in H$, alors $xH = H = Hx$.

**20.2** Si $x \in G \setminus H$, alors $xH = H^c = Hx$.

**20.3** Le sous-groupe $H$ est distingué [**5**].

## II.4 Actions de groupes

**21.** ✍ *Soient $(G, \star)$, un groupe et $X$, un ensemble. Une **action (à gauche)** du groupe $G$ sur l'ensemble $X$ est une application $\bullet$ de $G \times X$ dans $X$ qui vérifie les deux propriétés suivantes.*

1. *Pour tout $x \in X$,*
$$e_G \bullet x = x.$$
2. *Quels que soient $s$ et $t$ dans $G$,*
$$\forall\, x \in X, \quad s \bullet (t \bullet x) = (s \star t) \bullet x.$$

**22. Action d'un groupe sur lui-même**

Les trois applications suivantes sont des actions d'un groupe $(G, \star)$ sur l'ensemble $G$ lui-même.

**22.1 Translation à gauche**

$$\forall\, (s, x) \in G \times G, \quad s \bullet x = s \star x$$

**22.2 Translation à droite**

$$\forall\, (s, x) \in G \times G, \quad s \bullet x = x \star s^{-1}$$

**22.3 Conjugaison**

$$\forall\, (s, x) \in G \times G, \quad s \bullet x = s \star x \star s^{-1}$$

**23. Action sur les classes à gauche**

On note $G/H$, l'ensemble des classes à gauche de $G$ modulo un sous-groupe $H$ [**18**].

On définit une action du groupe $(G, \star)$ sur l'ensemble $G/H$ en posant

$$\forall\, (s, C) \in G \times G/H, \quad s \bullet C = (s \star x)H$$

pour tout $x \in G$ tel que $C = xH$.

**24. Stabilisateur**

On suppose donnée une action du groupe $(G, \star)$ sur l'ensemble $X$.

**24.1** ✍ *Le **stabilisateur** de $x \in X$ est l'ensemble $S_x$ défini par*

$$S_x = \{g \in G : g \bullet x = x\}.$$

**24.2** Le stabilisateur $S_x$ d'un élément quelconque $x \in X$ est un sous-groupe de $(G, \star)$.

**25.** On suppose donnée une action du groupe $(G, \star)$ sur l'ensemble $X$.

**25.1** ✍ *Pour tout élément $x \in X$, l'**orbite** de $x$ sous l'action de $G$ est l'ensemble*

$$\Omega_x = \{g \bullet x,\ g \in G\}.$$

**25.2** La relation $\mathscr{R}$ définie par

$$\forall\, x, y \in X, \quad x \mathscr{R} y \iff \exists\, g \in G, \quad y = g \bullet x$$

est une relation d'équivalence sur $X$.

**25.3** Tout élément $x$ de $X$ appartient à l'orbite $\Omega_x$.

**25.4** Soient $x$ et $y$ dans $X$, deux éléments tels que $\Omega_x \cap \Omega_y \neq \varnothing$. Alors $\Omega_x = \Omega_y$.

**25.5** Les orbites $\Omega_x$ sont les classes d'équivalence pour la relation d'équivalence $\mathscr{R}$.

$$\forall\, x, y \in X, \quad x \mathscr{R} y \iff \Omega_x = \Omega_y$$

**25.6** S'il existe $g \in G$ tel que $y = g \bullet x$, alors les stabilisateurs de $x$ et de $y$ [**24**] sont isomorphes :

$$S_y = g S_x g^{-1}.$$

**25.7** Soit $x \in X$. L'application de l'ensemble des classes à gauche

$$G/S_x = \{gS_x,\ g \in G\}$$

dans l'orbite $\Omega_x$ définie par

$$S_x g \longmapsto g \bullet x$$

est une bijection, donc

$$\#(G) = \#(\Omega_x) \times \#(S_x).$$