Mathématiques pour l'informatique. L1 Informatique I23.

TD 6. Groupes [1]

EXERCICE 1. Démontrez qu'un magma unifère n'a qu'un élément neutre.

Solution. Par l'absurde, supposons qu'il existe deux éléments neutres e et e' dans un magma $(X, \diamond)$. Par définition si ϵ est un élément neutre alors

$$\forall x \in X \quad x \diamond \epsilon = \epsilon \diamond x = x. \tag{1}$$

On applique (1) à $x = e$ pour l'élément neutre $\epsilon := e'$ puis à $x = e'$ pour l'élément neutre $\epsilon := e$ pour obtenir respectivement :

$$\begin{aligned} e \diamond e' &= e' \diamond e = e \\ e' \diamond e &= e \diamond e' = e' \end{aligned}$$

et par transitivité de l'égalité, on en déduit $e = e'$.

EXERCICE 2. Soit X un ensemble et $\mathscr{P}(X)$ l'ensemble des parties de X. Démontrez que $(\mathscr{P}(X), \cup)$ est un magma. Ce magma est-il commutatif, associatif, unifère ? Même question pour $(\mathscr{P}(X), \cap)$.

Solution. Soit A et B deux éléments de $\mathscr{P}(X)$. De manière générale, la réunion hérite des propriétés du connecteur logique de disjonction *ou*. Si $x \in A \cup B$ alors $(x \in A) \vee (x \in B)$ or $A \subseteq X$ et $B \subseteq X$ donc $x \in X$ et $A \cup B \in \mathscr{P}(X)$. Pour les mêmes raisons, la réunion est commutative et associative. L'élément neutre est bien sûr l'ensemble vide $\varnothing$ puisque

$$\forall A \in \mathscr{P}(X) \quad A \cup \varnothing = \varnothing \cup A = A.$$

La preuve est similaire pour l'intersection qui hérite des propriétés du connecteur de conjonction *et*, mais cette fois l'élément neutre est l'ensemble X.

1. version du 20 avril 2023, 16 : 58

EXERCICE 3. Démontrez que l'intersection est distributive sur la réunion et réciproquement sur l'ensemble $\mathscr{P}(X)$ des parties d'un ensemble X.

Solution. C'est la conséquence directe de la distributivité du connecteur logique de conjonction *et* sur le connecteur logique de disjonction *ou* (et réciproquement). Montrons la distributivité de $\cap$ sur $\cup$, l'autre preuve est similaire. Montrons que $x \in A \cap (B \cup C) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$. On a

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow (x \in A) \wedge (x \in (B \cup C)) \\ &\Leftrightarrow (x \in A) \wedge \big((x \in B) \vee (x \in C)\big) \\ &\Leftrightarrow \big((x \in A) \wedge (x \in B)\big) \vee \big((x \in A) \wedge (x \in C)\big) \\ &\Leftrightarrow (x \in A \cap B) \vee (x \in A \cap C) \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

EXERCICE 4. Démontrez que si $(X, \diamond)$ est un monoïde, alors :

(1) Tout élément symétrisable à gauche (resp. à droite) est régulier à gauche (resp. à droite).

(2) Si un élément est symétrisable, son symétrique à gauche est égal à son symétrique à droite.

(3) Si un élément est symétrisable, son symétrique est unique.

(4) Le composé de deux éléments symétrisables est symétrisable.

Solution. Dans la suite on note e l'élément neutre du monoïde $(X, \diamond)$.

(1) Notons x' le symétrique à gauche de x. Soit $(s, t) \in X^2$ tels que $x \diamond s = x \diamond t$. On a

$$\begin{aligned} x' \diamond (x \diamond s) &= x' \diamond (x \diamond t) && \\ (x' \diamond x) \diamond s &= (x' \diamond x) \diamond t && \text{car } \diamond \text{ est associative} \\ e \diamond s &= e \diamond t && \text{car } x' \text{ symétrique à gauche de } x. \\ s &= t && \text{car } e \text{ est l'élément neutre pour } \diamond. \end{aligned}$$

La preuve est “symétrique” pour la régularité à droite.

(2) Notons x' (resp. x'') le symétrique à gauche (resp. à droite) de x. Par définition :

$$(x' \diamond x) = (x \diamond x'') = e. \tag{2}$$

On en déduit

$$\begin{aligned}
x' &= x' \diamond e && \text{car } e \text{ est l'élément neutre pour } \diamond \\
&= x' \diamond (x \diamond x'') && \text{d'après (2)} \\
&= (x' \diamond x) \diamond x'' && \text{car } \diamond \text{ est associative} \\
&= e \diamond x'' && \text{d'après (2)} \\
&= x'' && \text{car } e \text{ est l'élément neutre pour } \diamond
\end{aligned}$$

(3) Si x et x' sont deux symétriques de x, ils satisfont (2) et sont donc égaux.

(4) Soit x_1 et x_2 deux éléments de X de symétriques respectifs x_1' et x_2', ils sont uniques d'après (3), alors

$$\begin{aligned}
(x_1 \diamond x_2) \diamond (x_2' \diamond x_1') &= (x_1 \diamond (x_2 \diamond x_2')) \diamond x_1' && \text{car } \diamond \text{ est associative} \\
&= (x_1 \diamond e) \diamond x_1' && \text{car } x_2' \text{ est le symétrique de } x_2 \\
&= x_1 \diamond x_1' && \text{car } e \text{ est l'élément neutre pour } \diamond \\
&= e && \text{car } x_1' \text{ est le symétrique de } x_1
\end{aligned}$$

On procède de la même manière pour montrer que $(x_2' \diamond x_1') \diamond (x_1 \diamond x_2) = e$. Ceci prouve que $x_1 \diamond x_2$ admet $x_2' \diamond x_1'$ pour symétrique.

EXERCICE 5. Démontrez que si X et Y sont deux magmas, alors la bijection réciproque f^{-1} d'un morphisme bijectif $f : X \to Y$ est nécessairement un morphisme. Démontrez que si X et Y sont munis de relations binaires, alors la bijection réciproque f^{-1} d'un morphisme bijectif $f : X \to Y$ n'est *pas* nécessairement un morphisme. Indication : choisir l'égalité comme relation d'ordre sur X , une relation d'ordre $\leqslant$ sur Y et f un morphisme d'ensembles ordonnés.

Solution. Notons $(X, \star)$ et $(Y, \diamond)$ ces deux magmas. Il faut donc montrer que

$$\forall (y_1, y_2) \in Y \times Y \quad f^{-1}(y_1) \star f^{-1}(y_2) = f^{-1}(y_1 \diamond y_2).$$

Soit y_1 et y_2 deux éléments de Y, on note $x_1 := f^{-1}(y_1)$ et $x_2 := f^{-1}(y_2)$. Comme f est bijective, on a $f^{-1} \circ f = \mathrm{Id}_X$ (cf. ce théorème) et on en déduit que

$$\begin{aligned}
x_1 \star x_2 &= (f^{-1} \circ f)\big(x_1 \star x_2\big) \\
&= f^{-1}\big(f(x_1 \star x_2)\big) \\
&= f^{-1}\big(f(x_1) \diamond f(x_2)\big) && \text{car } f \text{ est un morphisme} \\
&= f^{-1}\big(y_1 \diamond y_2\big)
\end{aligned}$$

La bijection réciproque f^{-1} est donc bien un morphisme.

L'égalité est une relation d'ordre sur tout ensemble X, on considère donc $(X, =)$ et $(Y, \leqslant)$ où $\leqslant$ désigne une relation d'ordre sur Y. Si $f : X \to Y$ est une application bijective et croissante, on a $x = y \Rightarrow f(x) \leqslant f(y)$ mais pas nécessairement $f^{-1}(x) \leqslant f^{-1}(y) \Rightarrow x = y$, prendre par exemple l'application de $\mathbb{Z}^{\mathbb{Z}}$ définie par $n \mapsto n + 1$.

EXERCICE 6. Soit X, Y et Z trois ensembles structurés et $f : X \to Y$ et $g : Y \to Z$ deux morphismes.

(1) Démontrez que l'application $g \circ f$ est un morphisme de $X \to Z$.

(2) On suppose à présent que ces trois ensembles ont une structure de magma et que f et g sont des isomorphismes. Démontrez que $g \circ f$ est un isomorphisme de $X \to Z$.

Solution. **(1)** Montrons le pour des relations binaires $\mathscr{R}_X$, $\mathscr{R}_Y$ et $\mathscr{R}_Z$ sur ces ensembles respectivement. On a par hypothèse

$$\forall (x_1, x_2) \in X^2 \quad x_1 \mathrel{\mathscr{R}} x_2 \Rightarrow f(x_1) \mathrel{\mathscr{R}_Y} f(x_2) \tag{3}$$
$$\forall (y_1, y_2) \in Y^2 \quad y_1 \mathrel{\mathscr{R}_Y} y_2 \Rightarrow g(y_1) \mathrel{\mathscr{R}_Z} g(y_2) \tag{4}$$

Soit $(x_1, x_2) \in X^2$ tel que $x_1 \mathrel{\mathscr{R}} x_2$. D'après (3) on a $f(x_1) \mathrel{\mathscr{R}_Y} f(x_2)$ et on peut appliquer (4) au couple $(f(x_1), f(x_2))$ pour obtenir

$$\begin{aligned}
\forall (x_1, x_2) \in X^2 \quad x_1 \mathrel{\mathscr{R}} x_2 &\Rightarrow g(f(x_1)) \mathrel{\mathscr{R}_Z} g(f(x_2)) \\
&\Rightarrow (g \circ f)(x_1) \mathrel{\mathscr{R}_Z} (g \circ f)(x_2)
\end{aligned}$$

Montrons le à présent pour des lois de composition internes $+$, $\times$ et $\diamond$ respectivement. On a par hypothèse

$$\forall (x_1, x_2) \in X^2 \quad f(x_1 + x_2) = f(x_1) \times f(x_2) \tag{5}$$
$$\forall (y_1, y_2) \in Y^2 \quad g(y_1 \times y_2) = g(y_1) \diamond g(y_2) \tag{6}$$

Et pour tout couple $(x_1, x_2) \in X^2$, on a

$$\begin{aligned}(g \circ f)(x_1 + x_2) &= g(f(x_1 + x_2)) \\ &= g(f(x_1) \times f(x_2)) && \text{d'après (5)} \\ &= g(f(x_1)) \diamond g(f(x_2)) && \text{on applique (6) à } f(x_1) \times f(x_2) \\ &= (g \circ f)(x_1) \diamond (g \circ f)(x_2).\end{aligned}$$

(2) Supposons à présent que f et g soient des isomorphismes. Si f et g sont des bijections, nous savons que $g \circ f$ est une bijection et nous savons d'une part que $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ et que $f^{-1} \circ g^{-1}$ est un morphisme d'après l'exercice précédent, c'est donc bien un isomorphisme.

EXERCICE 7. On numérote les jours à l'aide des entiers relatifs, le jour 0 étant fixé au dimanche 4 mars 1962. On définit une relation binaire $\mathscr{R}$ sur $\mathbb{Z}$ par

$$x \mathscr{R} y \Leftrightarrow 7 \mid (y - x).$$

(1) Démontrez que $\mathscr{R}$ est une relation d'équivalence sur $\mathbb{Z}$.

(2) Quelles sont les différentes classes d'équivalence pour cette relation ?

(3) Soit φ la surjection canonique, on note dim $:= \varphi(0)$, lun $:= \varphi(1), \ldots$, sam $:= \varphi(6)$. Démontrez que $\mathscr{R}$ est compatible avec l'addition de $\mathbb{Z}$.

(4) Dressez la table d'addition de $\mathbb{Z}/\mathscr{R}$ pour la loi induite $+$

Solution. (1) La relation $\mathscr{R}$ est réflexive puisque $7 \mid 0$. Soit $(x, y) \in \mathbb{Z}^2$, si $7 \mid (y - x)$ alors $7 \mid (x - y)$, la relation $\mathscr{R}$ est donc symétrique. Soit $(x, y, z) \in \mathbb{Z}^3$, si $7 \mid (y - x)$ et $7 \mid (z - y)$ on en déduit l'existence de deux entiers a et b tels que $7a = y - x$ et $7b = z - y$ puis l'égalité

$$\begin{aligned}7b + 7a &= (z - y) + (y - x) \\ 7(b + a) &= z + ((-y) + y) - x && \text{car l'addition est associative dans } \mathbb{Z} \\ 7(b + a) &= z - x.\end{aligned}$$

Autrement dit que $7 \mid (z - x)$, ce qui prouve que $x \mathscr{R} z$.

(2) Les éléments de la classe de 0 sont les entiers relatifs x tels que $x \mathscr{R} 0$, c'est-à-dire ceux qui sont divisibles par 7 ou pour paraphraser, les multiples de 7 :

$$\overline{0} = \{7z \mid z \in \mathbb{Z}\}.$$

On a plus généralement pour $k \in [\![0, 6]\!]$:

$$\overline{k} = \{7z + k \mid z \in \mathbb{Z}\}.$$

Ces 7 ensembles sont deux-à-disjoints, en effet $7z + k = 7z + l$ entraîne $k = l$. D'autre part, en anticipant sur l'étude de la division euclidienne, il existe un unique $z \in \mathbb{Z}\backslash\{0\}$ et un unique $k \in [\![0, 6]\!]$ tels que $x = 7z + k$. Par conséquent, les ensembles $\overline{0}, \overline{1}, \ldots, \overline{6}$ sont toutes les classes d'équivalence de $\mathbb{Z}$ pour la relation $\mathscr{R}$.

+	DI	LU	MA	ME	JE	VE	SA
DI	DI	LU	MA	ME	JE	VE	SA
LU	LU	MA	ME	JE	VE	SA	DI
MA	MA	ME	JE	VE	SA	DI	LU
ME	ME	JE	VE	SA	DI	LU	MA
JE	JE	VE	SA	DI	LU	MA	ME
VE	VE	SA	DI	LU	MA	ME	JE
SA	SA	DI	LU	MA	ME	JE	VE

TABLE 1. Table d'addition de $\mathbb{Z}/7\mathbb{Z}$.

(3) Il faut donc prouver que

$$\forall (x, x', y, y') \in X^4 \quad (x \mathscr{R} x') \wedge (y \mathscr{R} y') \ \Rightarrow (x \diamond y) \mathscr{R} (x' \diamond y').$$

Ce qui se traduit ici par

$$\forall (x, x', y, y') \in X^4 \quad (7 \mid (x' - x)) \wedge (7 \mid (y' - y)) \ \Rightarrow 7 \mid \big((x' + y') - (x + y)\big).$$

Si $7 \mid (x' - x)$ et $7 \mid (y' - y)$, il existe $(k, l) \in \mathbb{N}^2$ tel que

$$7k = x' - x$$

$$7l = y' - y$$

Et en sommant on obtient $7(k + l) = x' + y' - (x + y)$, ce qui permet de conclure que la relation $\mathscr{R}$ est compatible avec l'addition dans $\mathbb{Z}$. L'ensemble quotient $\mathbb{Z}/\mathscr{R}$ peut donc être muni de la loi quotient additive héritée de celle de $\mathbb{Z}$.

(4) La table d'addition de $\mathbb{Z}/\mathscr{R}$ est présentée en table (1), avec l'association initiale entre les jours de la semaines et les classes modulo 7.

NB. Nous avons vu en cours que les seules relations d'équivalences $\mathscr{R}$ compatibles avec une loi de groupe $\diamond$ sont de la forme $x \mathscr{R} y \Leftrightarrow x^{-1} \diamond y \in H$ où H est un sous-groupe normal de G. Nous verrons en arithmétique que tous les sous-groupes de $(\mathbb{Z}, +)$ sont normaux car $(\mathbb{Z}, +)$ est commutatif et qu'ils sont de la forme $k\mathbb{Z}$ où $k \in \mathbb{Z}$, autrement dit ici $k = 7$ et $x \mathscr{R} y \Leftrightarrow (y - x \in 7\mathbb{Z})$ puisque le symétrique de x pour l'addition est $-x$.

EXERCICE 8. Soit $(X, \diamond)$ un magma et Y un ensemble et $f : X \to Y$ une bijection. Explicitez comment transporter la structure de magma de X sur Y à l'aide de f.

Solution. Il suffit de définir une loi $\star$ sur Y à l'aide de la bijection réciproque f^{-1} de f comme suit :

$$\forall (y, y') \in Y^2 \quad y \star y' := f(f^{-1}(y) \diamond f^{-1}(y')).$$

EXERCICE 9. ‡ Vérifiez que $(\mathbb{N}, +)$ est un monoïde commutatif.

(1) Démontrez que la relation binaire $\mathscr{R}$ définie sur $\mathbb{N} \times \mathbb{N}$ par

$$(n, m) \mathscr{R} (n', m') \Leftrightarrow n + m' = n' + m$$

est une relation d'équivalence.

(2) Démontrez que la loi de composition interne $\boxplus$ sur $\mathbb{N} \times \mathbb{N}$ définie par

$$(n, m) \boxplus (n', m') := (n + n', m + m')$$

est associative et commutative et montrez que la relation $\mathscr{R}$ est compatible avec $\boxplus$.

(3) On munit l'ensemble quotient $(\mathbb{N} \times \mathbb{N})/\mathscr{R}$ de la loi quotient $\boxplus$. Quel est son élément neutre ? Exhibez un symétrique pour tout élément $\overline{(n, m)}$ de $(\mathbb{N} \times \mathbb{N})/\mathscr{R}$.

(4) Démontrez que les couples $(n, 0)$ et $(0, m)$ pour tout entier n et tout entier m décrivent tous les représentants des classes d'équivalences de $\mathbb{N} \times \mathbb{N}$ pour la relation $\mathscr{R}$.

(5) Dessinez les classes d'équivalences $\overline{(0, 0)}$, $\overline{(1, 0)}$, $\overline{(2, 0)}$, $\overline{(3, 0)}$ et $\overline{(0, 1)}$, $\overline{(0, 2)}$, $\overline{(0, 3)}$ dans le plan discret $\mathbb{N} \times \mathbb{N}$.

(6) On définit $G := \{\overline{(n, 0)} \mid n \in \mathbb{N}\}$ sous-ensemble de $(\mathbb{N} \times \mathbb{N})/\mathscr{R}$. Démontrez que l'application $f : (\mathbb{N}, +) \to (G, \boxplus)$ définie par

$$f(n) := \overline{(n, 0)}$$

est un isomorphisme.

(7) Quel ensemble reconnaissez vous en $(\mathbb{N} \times \mathbb{N})/\mathscr{R}$?

Solution. L'ensemble $\mathbb{N}$ des entiers naturels est un monoïde puisque l'addition de deux entiers naturels est un entier naturel et on sait que $\forall (l, m, n) \in \mathbb{N}^3$ on a $n + m = m + n$ et $(l + m) + n = l + (m + n)$.

(1) Elle est trivialement réflexive et symétrique. Soit n, m, n', m', n'', m'' des entiers naturels tels que $(n, m) \mathscr{R} (n', m')$ et $(n', m') \mathscr{R} (n'', m'')$. On a donc

$$\begin{aligned} n + m' &= n' + m \\ n' + m'' &= n'' + m' \end{aligned}$$

On somme

$$\begin{aligned} (n + m') + (n' + m'') &= (n' + m) + (n'' + m') \\ n + (m' + n') + m'' &= n'' + (m' + n') + m \quad \text{(commut. et assoc. de +)} \\ n + m'' &= n'' + m \quad \text{(régularité de +)} \end{aligned}$$

et on conclut donc que $(n, m) \mathscr{R} (n'', m'')$ ce qui finit de prouver que la relation $\mathscr{R}$ est une relation d'équivalence.

(2) La commutativité et l'associativité de $\boxplus$ se déduisent immédiatement de la commutativité et de l'associativité de l'addition dans $\mathbb{N}$. Il reste à montrer que la relation $\mathscr{R}$ est compatible avec la loi $\boxplus$. Il faut donc montrer que

$$\begin{aligned} &\forall (n_1, m_1, n_1', m_1', n_2, m_2, n_2', m_2') \in \mathbb{N}^8 \\ &(n_1, m_1) \mathscr{R} (n_1', m_1') \wedge (n_2, m_2) \mathscr{R} (n_2', m_2') \\ &\qquad \Rightarrow ((n_1, m_1) \boxplus (n_2, m_2)) \mathscr{R} ((n_2, m_2) \boxplus (n_2', m_2')). \end{aligned}$$

La conjonction ci-dessus nous donne les deux identités suivantes :

$$\begin{aligned} n_1 + m_1' &= n_1' + m_1 \\ n_2 + m_2' &= n_2' + m_2 \end{aligned}$$

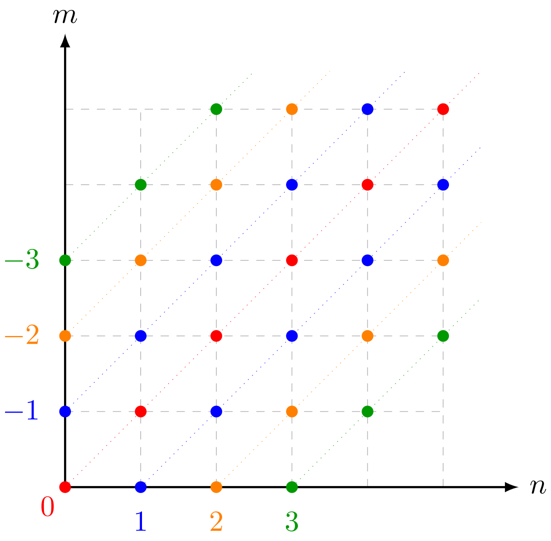

Figure 1. Quelques classes d'équivalences de la relation $\mathscr{R}$.

et en les additionnant

$$
\begin{aligned}
& (n_1 + m'_1) + (n_2 + m'_2) = (n'_1 + m_1) + (n'_2 + m_2) \\
\text{on commute : } \quad & (n_1 + n_2) + (m'_1 + m'_2) = (n'_1 + n'_2) + (m_1 + m_2)
\end{aligned}
$$

On en déduit donc que $(n_1 + n_2, m_1 + m_2) \ \mathscr{R} \ (n'_1 + n'_2, m'_1 + m'_2)$, soit

$$((n_1, m_1) \boxplus (n_2, m_2)) \ \mathscr{R} \ ((n_2, m_2) \boxplus (n'_2, m'_2))$$

(3) L'élément neutre pour la loi quotient est la classe d'équivalence $\overline{(0,0)}$ qui regroupe tous les couples du type (n, n) et le symétrique de la classe $\overline{(n,m)}$ est la classe $\overline{(m,n)}$, en effet $\overline{(n,m)} \boxplus \overline{(m,n)} = \overline{(n+m, m+n)} = \overline{(0,0)}$.

(4) Soit $(a, b) \in \mathbb{N} \times \mathbb{N}$. On a $a \geqslant b$ ou $a < b$. Dans le premier cas il existe un entier naturel n tel que $a + 0 = b + n$ et donc $(a, b) \ \mathscr{R} \ (n, 0)$, autrement dit $\overline{(a,b)} = \overline{(n,0)}$. Le raisonnement est le même dans l'autre cas avec un entier m tel que $a + m = b + 0$.

(5) Les classes d'équivalence sont représentées dans la figure (1) dans laquelle on a noté $n := \overline{(n,0)}$ et $-m := \overline{(0,m)}$.

(6) Démontrons tout d'abod qu'il s'agit d'un morphisme :

$$
\begin{aligned}
f(n + n') &= \overline{(n + n', 0)} \\
&= \overline{(n, 0) \boxplus (n', 0)} \\
&= \overline{(n, 0)} \boxplus \overline{(n', 0)} \\
&= f(n) \boxplus f(n')
\end{aligned}
$$

Il faut à présent montrer que le morphisme f est bijectif. Soit $\overline{(n,0)} \in G$. Il est clair que l'entier $n \in \mathbb{N}$ est un antécédent de la classe $\overline{(n,0)}$, donc f est surjective. D'autre part, si $f(n) = f(n')$ on a $\overline{(n,0)} = \overline{(n',0)}$ mais $\overline{(n,0)} = \{(n+k, k) \mid k \in \mathbb{N}$ et $\overline{(n',0)} = \{(n'+l, l) \mid l \in \mathbb{N}\}$, donc si $(n+k, k) \in \overline{(n',0)}$ alors il existe un entier naturel l tel que $(n + k, k) = (n' + l, l)$ et par conséquent $k = l$ et finalement $n = n'$.

(7) On reconnaît l'ensemble $\mathbb{Z}$ des entiers relatifs, les classes $\overline{(n,0)}$, $n \in \mathbb{N}$ décrivant les entiers positifs ou nuls et les classes $\overline{(0,m)}$, $m \in \mathbb{N} \backslash \{0\}$ décrivant les entiers "négatifs". Il s'agit d'une construction abstraite de l'ensemble Z qui n'a pour objectif que de montrer qu'il est constructible dans la théorie ZF.

EXERCICE 10. Démontrez qu'il existe une unique loi de groupe sur un singleton, explicitez cette loi. Même question pour une paire. Ces groupes sont-ils commutatifs ?

Solution. Supposons que $G := \{a\}$ et notons $\diamond$ la loi de composition interne sur G. On doit donc avoir $a \diamond a = a$, ce qui prouve d'une part que a l'élément neutre pour cette loi et par conséquent que a est son propre symétrique. La loi est trivialement commutative, elle est aussi associative :

$$
\begin{aligned}
(a \diamond a) \diamond a &= a \diamond a \\
&= a \diamond (a \diamond a)
\end{aligned}
$$

Si G est un groupe à deux éléments, on désigne par e son élément neutre et a l'autre élément : $G := \{a, e\}$. Il faut construire les 4 compositions possibles suivantes en s'assurant qu'elles satisfont une loi de groupe :

$$e \diamond e, \ \ e \diamond a, \ \ a \diamond e \text{ et } a \diamond a.$$

Pour les trois premières, il n'y a qu'une possibilité puisque e est l'élément neutre :

$$e \diamond e = e$$
$$e \diamond a = a \diamond e = a$$

Pour la dernière on ne peut avoir $a \diamond a = a$ sans quoi a serait neutre et égal à e et le groupe serait réduit à un élément, on a donc nécessairement $a \diamond a = e$ ce qui montre au passage que a est son propre symétrique. La commutativité est immédiate et pour l'associativité, il faut montrer que

$$\forall (x, y, z) \in G^3 \quad (x \diamond y) \diamond z = x \diamond (y \diamond z).$$

Il y a 8 combinaisons possibles pour le triplet (x, y, z) puisque $\#G = 2$ et qu'il y a 3 variables. Les identités suivantes les valident :

$$(x \diamond y) \diamond e = x \diamond y = x \diamond (y \diamond e)$$
$$(x \diamond e) \diamond a = x \diamond a = x \diamond (e \diamond a)$$
$$(e \diamond x) \diamond a = x \diamond a = e \diamond (x \diamond a)$$
$$(a \diamond a) \diamond a = e \diamond a = a \diamond e = a \diamond (a \diamond a)$$

EXERCICE 11. † Démontrez le théorème de caractérisation d'un sous-groupe du cours : Soit $(G, \diamond)$ un groupe et $H \subseteq G$, alors les 4 propositions suivantes sont équivalentes :

(1) H est un sous-groupe de G.

(2) H est stable et $e \in H$ et $\forall x \in H \ \ x^{-1} \in H$.

(3) H est stable et $H \neq \varnothing$ et $\forall x \in H \ \ x^{-1} \in H$.

(4) $H \neq \varnothing$ et $\forall (x, y) \in H \times H \ \ x \diamond y^{-1} \in H$.

Solution. Nous allons démontrer que (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2) : par définition H est stable pour $\diamond$ et cette proposition permet de conclure.

(2) $\Rightarrow$ (3) : c'est évident puisque $e \in H$.

(3) $\Rightarrow$ (4) : c'est évident puisque $y^{-1} \in H$ et que H est stable.

(4) $\Rightarrow$ (2) : puisque H n'est pas vide, il existe au moins un $x \in H$, on peut donc appliquer la deuxième partie de l'hypothèse sur le couple (x, x), soit $x \diamond x^{-1} = e \in H$. On peut à présent appliquer la deuxième partie de l'hypothèse au couple (e, x), soit $e \diamond x^{-1} = x^{-1} \in H$. Pour la stabilité, $x \diamond y = x \diamond (y^{-1})^{-1}$.

(2) $\Rightarrow$ (1) : l'ensemble H étant stable la loi $\diamond$ induite sur H est associative et admet e pour élément neutre et tout $x \in H$ admet pour symétrique x^{-1}.

EXERCICE 12. † Soit $(G, \diamond)$ un groupe.

(1) Montrez que l'ensemble noté $\mathfrak{S}(G)$ des bijections de l'ensemble G dans lui-même muni de la loi de composition des applications $\circ$ est un groupe.

(2) Montrez que le sous-ensemble $\text{Aut}(G)$ de $\mathfrak{S}(G)$ des *automorphismes* (morphismes bijectifs) muni de la loi induite est un sous-groupe de $(\mathfrak{S}(G), \circ)$.

Solution. (1) C'est une loi de composition interne puisque la composée de deux bijections est une bijection. On sait également que la composition des applications est associative (que ces applications soient bijectives ou non). L'application identité Id_G est évidemment bijective et fourni l'élément neutre de G pour la composition des applications car $\forall f \in \mathfrak{S}(G)$, $f \circ \text{Id}_G = \text{Id}_G \circ f = f$. Si f est une bijection, elle admet une bijection réciproque f^{-1} telle que $f \circ f^{-1} = f^{-1} \circ f = \text{Id}_G$. En revanche la loi $\circ$ n'est pas commutative.

(2) Si f est un automorphisme, on a donc

$$\forall (x, y) \in G^2 \quad f(x \diamond y) = f(x) \diamond f(y).$$

La composition de deux morphismes g et f est encore un morphisme (qu'ils soient bijectifs ou non), en effet soit $(x, y) \in G^2$,

$$\begin{aligned}(g \circ f)(x \diamond y) &= g(f(x) \diamond f(y)) \\ &= g(f(x)) \diamond g(f(y)) \\ &= (g \circ f)(x) \diamond (g \circ f)(y).\end{aligned}$$

Donc $\text{Aut}(G)$ est stable. D'autre part, l'élément neutre Id_G est trivialement un morphisme, on a donc $\text{Id}_G \in \text{Aut}(G)$. Soit f^{-1} la bijection réciproque d'un automorphisme $f \in \text{Aut}(G)$. Soit $(x', y') \in G^2$, comme f est bijective, il existe $(x, y) \in G^2$ tels que $f(x) = x'$ et $f(y) = y'$, soit

$f^{-1}(x') = x$ et $f^{-1}(y') = y$. On a donc

$$\begin{aligned}
f^{-1}(x' \diamond y') &= f^{-1}(f(x) \diamond f(y)) \\
&= f^{-1}(f(x \diamond y)) \quad \text{car } f \text{ est un morphisme} \\
&= (f^{-1} \circ f)(x \diamond y)) \\
&= \mathrm{Id}_G(x \diamond y) \\
&= x \diamond y \\
&= f^{-1}(x') \diamond f^{-1}(y')
\end{aligned}$$

Donc $f^{-1} \in \mathrm{Aut}(G)$ et la propriété (2) de l'exercice 11 permet de conclure que $(\mathrm{Aut}(G), \circ) \lhd (\mathfrak{S}(G), \circ)$.

EXERCICE 13. † Soit $(G, \diamond)$ un groupe.

(1) Démontrez que l'application $\varphi_a : G \to G$ définie par $x \mapsto \ a \diamond x \diamond a^{-1}$ est un automorphisme du groupe (dit *automorphisme intérieur* de G).

(2) Quel est l'automorphisme réciproque de φ_a ?

(3) Démontrez que l'application $\varphi : a \mapsto \varphi_a$ est un morphisme du groupe $(G, \diamond)$ dans le groupe $(\mathrm{Aut}(G), \circ)$.

(4) Vérifiez que $\mathrm{Ker}(\varphi) = Z(G)$.

Solution. (1) C'est un morphisme, en effet en notant e l'élément neutre pour $\diamond$, on a $a \diamond a^{-1} = e$ et on en déduit

$$\begin{aligned}
\varphi_a(x \diamond y) &= a \diamond x \diamond y \diamond a^{-1} \\
&= a \diamond x \diamond (a^{-1} \diamond a) \diamond y \diamond a^{-1} \\
&= (a \diamond x \diamond a^{-1}) \diamond (a \diamond y \diamond a^{-1}) \\
&= \varphi_a(x) \diamond \varphi_a(y).
\end{aligned}$$

Il est injectif, en effet

$$\varphi_a(x) = \varphi_a(y) \Leftrightarrow a \diamond x \diamond y \diamond a^{-1} = a \diamond y \diamond y \diamond a^{-1}$$

Il suffit de composer les deux membres de l'égalité à gauche par a^{-1} et à droite par a pour obtenir $x = y$. Il est également surjectif, soit $y \in G$, l'élément $x := \varphi_{a^{-1}}(y) = a^{-1} \diamond y \diamond a$ est un antécédent de y :

$$\begin{aligned}
\varphi_a(x) &= a \diamond (a^{-1} \diamond y \diamond a) \diamond a^{-1} \\
&= (a \diamond a^{-1}) \diamond y \diamond (a \diamond a^{-1}) \\
&= y.
\end{aligned}$$

Et nous savons que pour une loi de composition, un morphisme bijectif est un isomorphisme.

(2) On a $\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a^{-1}} \circ \varphi_a = \mathrm{Id}_G$, donc $\varphi_a^{-1} = \varphi_{a^{-1}}$.

(3) Soit $(a, b) \in G^2$. On a $\varphi(a \diamond b) = \varphi_{a \diamond b}$, or $\forall x \in G$,

$$\begin{aligned}
\varphi_{a \diamond b}(x) &= (a \diamond b) \diamond x \diamond (a \diamond b)^{-1} \\
&= (a \diamond b) \diamond x \diamond (b^{-1} \diamond a^{-1}) \\
&= a \diamond (b \diamond x \diamond b^{-1}) \diamond a^{-1} \\
&= \varphi_a(b \diamond x \diamond b^{-1}) \\
&= \varphi_a(\varphi_b(x)) \\
&= (\varphi_a \circ \varphi_b)(x)
\end{aligned}$$

Donc $\varphi(a \diamond b) = \varphi_a \circ \varphi_b$.

(4) Par définition $\mathrm{Ker}(\varphi) = \{a \in G \mid \varphi_a = \mathrm{Id}_G\}$. Mais $\varphi_a = \mathrm{Id}_G$ équivaut à ce que pour tout $x \in G$

$$\varphi_a(x) = x \ \Leftrightarrow \ a \diamond x \diamond a^{-1} = x \Leftrightarrow \ a \diamond x = x \diamond a.$$

Ce qui prouve que $\mathrm{Ker}(\varphi) = Z(G)$.

EXERCICE 14. Énumérez tous les éléments de $\mathfrak{S}_3$.

Solution. Nous savons que $\#\mathfrak{S}_3 = 3! = 6$ et ces permutations sont les suivantes :

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

EXERCICE 15. Soit n un entier tel que $n \geqslant 4$ et a, b, c et d quatre entiers distincts dans $[\![1,n]\!]$. Calculez le produit de transpositions $\sigma := (a\ b)(c\ d)(d\ a)$.

Solution. Par définition tout élément x ne faisant pas partie du support d'un p-cycle σ est laissé fixe, i.e. $\sigma(x) = x$, on se contente donc de calculer l'image des entiers a, b, c et d :

$$\begin{aligned}\sigma(a) &= (a\ b)(c\ d)(d\ a)(a)\\ &= (a\ b)(c\ d)(d)\\ &= (a\ b)(c)\\ &= c\end{aligned}$$

De la même façon on obtient $\sigma(b) = a$, $\sigma(c) = d$ et $\sigma(d) = b$. Donc

$$\sigma = \begin{pmatrix} a & b & c & d\\ c & a & d & b\end{pmatrix} = (a\ c\ d\ b)$$

EXERCICE 16. Démontrez que si σ est un p-cycle, alors $\sigma^p = \mathrm{Id}$. Quelle est l'inverse d'un p-cycle ?

Solution. Soit $\sigma := (i_i\ i_2\ \cdots\ i_p)$ un p-cycle. On considère le prédicat $P(k),\ k \in [\![1,p]\!]$ défini par

$$\forall j \in [\![1,p]\!] \quad \sigma^k(i_j) = \begin{cases} i_{j+k} & \text{si } j+k \leqslant p,\\ i_{j+k-p} & \text{sinon.}\end{cases} \tag{7}$$

Par définition d'un p-cycle σ, l'image d'un élément d'un cycle est l'élément suivant dans le cycle (circulairement) donc $P(1)$ est vrai. Il faut montrer à présent que

$$\forall k \in [\![1,p]\!] \quad P(k) \Rightarrow P(k+1).$$

Comme $\sigma^{k+1}(i_j) = \sigma(\sigma^k(i_j))$, il suffit d'appliquer l'hypothèse de récurrence (7) et d'avancer d'un élément dans le cycle pour conclure.

Par définition de l'écriture d'un p-cycle, l'image d'un élément est le suivant (circulairement) dont l'image réciproque d'un élément est le précédent, il suffit donc d'écrire les termes d'un p-cycle de droite à gauche pour obtenir son inverse : $\sigma^{-1} := (i_p, i_{p-1}, \ldots, i_2, i_1)$.

EXERCICE 17. Soit n un entier naturel. Montrez qu'une permutation $\sigma \in \mathfrak{S}_n$ différente de l'identité et involutive, c'est-à-dire telle que $\sigma^2 = \mathrm{Id}$, n'est pas nécessairement une transposition.

Solution. Prenons par exemple la permutation qui est le produit des deux transpositions $(1\ 3)$ et $(2\ 4)$:

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

Ce n'est pas une transposition et pourtant

$$\begin{aligned}\sigma^2 &= ((1\ 3)\,(2\ 4))^2\\ &= ((1\ 3)\,(2\ 4))\ ((1\ 3)\,(2\ 4))\\ &= (1\ 3)\ ((2\ 4)\,(1\ 3))\ (2\ 4) \quad \text{associativité}\\ &= (1\ 3)\ ((1\ 3)\,(2\ 4))\ (2\ 4) \quad \text{commutativité car supports disjoints}\\ &= (1\ 3)^2\,(2\ 4)^2 \quad \text{associativité}\\ &= \mathrm{Id} \quad \text{involution et neutre.}\end{aligned}$$

EXERCICE 18. † Démontrez que l'ordre d'une permutation est le PPCM des longueurs des cycles à supports disjoints de cette permutation.

Solution. Notons $\sigma := \sigma_1\,\sigma_2\cdots\sigma_k$ la décomposition de σ en produit de cycles à supports disjoints de longueurs respectives p_i. Notons que l'on parle de *la* décomposition, mais elle n'est unique qu'à l'ordre près des facteurs σ_i et uniquement si les cycles sont à supports *disjoints*. Notons $p := \text{PPCM}\{p_1, p_2, \ldots, p_k\}$ le PPCM des ordres p_i des cycles σ_i (on rappelle que l'ordre d'un p-cycle est égal à sa longueur p). On a

$$\forall i \in [\![1,k]\!] \quad \exists r_i \in \mathbb{N} \quad p_i\,r_i = p$$

et donc

$$\begin{aligned}\sigma^p &= (\sigma_1\,\sigma_2\cdots\sigma_k)^p\\ &= \sigma_1^p\,\sigma_2^p\cdots\sigma_k^p \quad \text{car les supports des } \sigma_i \text{ sont deux-à-deux disjoints!}\\ &= (\sigma^{p_1})^{r_1}\,(\sigma^{p_2})^{r_2}\cdots(\sigma^{p_k})^{r_k}\\ &= \mathrm{Id}\end{aligned}$$

D'après la définition de l'ordre d'une permutation, les seules puissances de cette permutation qui sont égales à l'identité sont nécessairement des multiples de cet ordre. Par définition du PPCM, p est le plus petit entier qui satisfait $\sigma^p = \mathrm{Id}$ ce qui achève la preuve.

EXERCICE 19. On considère la permutation σ suivante :

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

(1) Décomposez σ en produits de cycles à supports disjoints.
(2) Calculez la signature de σ.
(3) Décomposez σ en produit de transpositions.
(4) Calculez σ^{2021}.

Solution. **(1)** On détermine les cycles directement dans la matrice :

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

et on a donc $\sigma = (1\ 3\ 6\ 2\ 5)\,(4\ 7)$.
(2) La signature est donc $\varepsilon(\sigma) = (-1)^{7-2} = -1$ puisqu'il y a deux orbites. Attention au calcul de la signature, le nombre d'orbites n'est pas toujours égal au nombre de cycles, puisqu'une orbite de taille 1 n'est pas considérée comme un cycle.
(3) On connaît la décomposition d'un cycle en produit de transpositions et on obtient ici

$$\sigma = (1\ 3)\,(3\ 6)\,(6\ 2)\,(2\ 5)\,(4\ 7). \tag{8}$$

(4) Les cycles sont de longueurs 5 et 2, leur PPCM est égal à 10, l'ordre de la permutation est donc 10 et par conséquent $\sigma^{10} = \mathrm{Id}$. On a donc

$$\begin{aligned} \sigma^{2021} &= \sigma\,(\sigma^{10})^{202} \\ &= \sigma\,\mathrm{Id}^{202} \\ &= \sigma \end{aligned}$$

Attention à ne pas faire l'erreur de partir du produit de transpositions en (8) pour écrire que $\sigma^2 = \mathrm{Id}$ après avoir distribué l'exposant 2 à chaque transposition, ce qui est faux puisque leurs supports ne sont pas toujours disjoints, elles ne peuvent pas toutes commuter !

$$\begin{aligned} \sigma^2 &= \big((1\ 3)\,(3\ 6)\,(6\ 2)\,(2\ 5)(4\ 7)\big)\,\big((1\ 3)\,(3\ 6)\,(6\ 2)\,(2\ 5)\,(4\ 7)\big) \\ &\neq (1\ 3)^2\,(3\ 6)^2\,(6\ 2)^2\,(2\ 5)^2(4\ 7)^2 \end{aligned}$$

EXERCICE 20. Soit n et p deux entiers tels que $2 \leqslant p \leqslant n$. Combien le groupe $\mathfrak{S}_n$ possède-t-il de p-cycles ?

Solution. L'ensemble des p-uplets $(i_1\ i_2\ \ldots\ i_p)$ d'éléments distincts de $[\![1, n]\!]$ est en bijection avec l'ensemble des injections de $[\![1, p]\!]$ dans $[\![1, n]\!]$, il y en a donc $\frac{n!}{(n-p)!}$. Cependant, les p permutations circulaires d'un tel p-uplet codent le même p-cycle, il y en a donc finalement

$$\frac{n\,!}{p\,(n-p)\,!}$$

NB. Le nombre de p-cycle n'est *pas* le coefficient binomial $\binom{n}{p} = \frac{n\,!}{p\,!\,(n-p)\,!}$.

EXERCICE 21. Soit n un entier tel que $n \geqslant 1$. Calculez la signature de la permutation $\sigma \in \mathfrak{S}_n$ définie par $\sigma(k) := k + 1$ si $k < n$ et $\sigma(n) := 1$.

Solution. Il s'agit d'une permutation circulaire de l'identité, autrement dit du n-cycle $\sigma = (1\ 2\ 3 \ldots n-1\ n)$. Comme on sait qu'un n-cycle se décompose en un produit de $(n-1)$ transpositions, en l'occurrence ici :

$$\sigma = (1\ 2)\,(2\,3)\,(3\ 4)\ldots(n-1\ n),$$

que la signature d'une transposition est égale à -1 et que la signature d'un produit est le produit des signatures, on a $\varepsilon(\sigma) = (-1)^{n-1}$.

EXERCICE 22. Décrivez toutes les permutations des groupes $\mathfrak{S}_1$ et $\mathfrak{S}_2$. Montrez que ces groupes sont commutatifs.

Solution. Pour $\mathfrak{S}_1$ la seule permutation est l'identité et $\mathfrak{S}_2$ ne contient que l'identité et la transposition $(1\ 2)$. Par définition l'identité commute avec toute autre permutation et la transposition $(1\ 2)$ commute avec elle-même.

EXERCICE 23. Quelles sont les orbites de la permutation identité ?

Solution. Chaque élément est un point fixe de la permutation identité, il y a donc autant d'orbites que d'éléments de l'ensemble X sur lequel la permutation s'applique. Les orbites sont donc les singletons $\{x\}$ pour tout $x \in X$.

EXERCICE 24. Soit $\sigma \in \mathfrak{S}(X)$ et $\mathscr{O}$ une orbite suivant σ. Démontrez que la restriction de σ à $\mathscr{O}$ est une bijection.

Solution. Par définition, une orbite est une classe d'équivalence pour la relation $\mathscr{R}_\sigma$ définie par

$$x \mathscr{R}_\sigma y \Leftrightarrow \exists k \in \mathbb{Z} \quad y = \sigma^k(x). \tag{9}$$

Soit $y \in \mathscr{O}$, son antécédent $x := \sigma^{-1}(y)$ dans X existe et est unique puisque σ est une bijection et d'après (9), il appartient à $\mathscr{O}$ (en effet $k = -1$) et il reste unique dans $\mathscr{O}$ puisque la restriction de σ sur $\mathscr{O}$ coïncide avec σ sur $\mathscr{O}$.

EXERCICE 25. Vérifiez que la relation de conjugaison sur un groupe $(G, \diamond)$ est une relation d'équivalence.

Solution. Elle est bien réflexive puisque x est conjugué avec lui même $x = e \diamond x \diamond e$. Elle est symétrique puisque si $x' = a \diamond x \diamond a^{-1}$ alors $x' = a^{-1} \diamond x \diamond a$. Elle est également transitive puisque si $y = a \diamond x \diamond a^{-1}$ et $z = b \diamond y \diamond b^{-1}$, alors

$$\begin{aligned} z &= b \diamond (a \diamond x \diamond a^{-1}) \diamond b^{-1} \\ &= (b \diamond a) \diamond x \diamond (a^{-1} \diamond b^{-1}) \quad \text{car la loi est associative} \\ &= (b \diamond a) \diamond x \diamond (a^{-1} \diamond b^{-1}) \\ &= (b \diamond a) \diamond x \diamond (b \diamond a)^{-1} \end{aligned}$$

EXERCICE 26. Montrez que la classe de conjugaison de la permutation identique Id est réduite à Id quel que soit le groupe symétrique.

Solution. Soit n un entier naturel et $\mathfrak{S}_n$ le groupe symétrique à n éléments. Par définition, une permutation $\sigma \in \mathfrak{S}_n$ appartient à la classe de conjugaison de l'identité s'il existe $a \in \mathfrak{S}_n$ tel que

$$\begin{aligned} \sigma &= a \,\mathrm{Id}\, a^{-1} \\ &= a\, a^{-1} \\ &= \mathrm{Id} \end{aligned}$$

EXERCICE 27. Montrez que les transpositions $(1\ 2)$ et $(1\ 3)$ sont conjuguées dans $\mathfrak{S}_3$.

Solution. Il faut trouver une permutation ρ de $\mathfrak{S}_3$ telle que

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

Il suffit de remplacer 2 par 3, ce qui est réalisé par la transposition $\rho := (2\ 3)$. On a $(1\ 3) = (2\ 3)\,(1\ 2)\,(2\ 3)$ puisque le symétrique d'une transposition est la transposition elle-même.

EXERCICE 28. Énumérez toutes les partitions de l'entier $n = 5$.

Solution. Il y en a 7 (cf. Table 2) :

$$\begin{aligned} 5 &= 5 \\ &= 4 + 1 \\ &= 3 + 2 \\ &= 3 + 1 + 1 \\ &= 2 + 2 + 1 \\ &= 2 + 1 + 1 + 1 \\ &= 1 + 1 + 1 + 1 + 1 \end{aligned}$$

EXERCICE 29. † Le *"Le roi des Nains"* est un jeu de cartes qui ne comporte que trois couleurs (les *nains*, les *gobelins* et les *chevaliers*) avec 13 cartes par couleur et qui se joue en 7 donnes. La règle du jeu (la *quête*) change à *chaque* donne. Pour 3 joueurs, on distribue 13 cartes à chaque joueur, on tire au hasard une tuile "quête" qui propose deux règles du jeu, et c'est le joueur qui a le 5 chevalier dans sa main qui en choisit une. Lors d'une donne, le joueur avec le 5 chevalier a le choix entre les deux quêtes suivantes :

(1) Un joueur qui aura ramassé le même nombre de plis qu'un autre joueur gagnera 5 points.

(2) Un joueur qui aura ramassé un nombre de plis différents des autres joueurs gagnera 5 points.

Les deux évènements sont-ils équiprobables ou est-il préférable de choisir une quête plutôt que l'autre ?

Solution. Il faut étudier les différentes répartitions des plis possibles et compter celles qui satisfont les conditions de la première quête et celles qui satisfont celles de la seconde. Le nombre de répartitions différentes est lié aux partitions d'un entier. La relation de récurrence qui nous fournit le nombre $p(n,k)$ de partitions de l'entier n en k parties

$$p(n,k) := \begin{cases} p(n-1,k-1)+p(n-k,k) & \text{si } 1<k<n, \\ 1 & \text{si } k=1 \text{ ou } k=n, \\ 0 & \text{si } n<k. \end{cases} \tag{10}$$

nous permet de construire la table suivante :

$n\backslash k$	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1												
2	1	1											
3	1	1	1										
4	1	2	1	1									
5	1	2	2	1	1								
6	1	3	3	2	1	1							
7	1	3	4	3	2	1	1						
8	1	4	5	5	3	2	1	1					
9	1	4	7	6	5	3	2	1	1				
10	1	5	8	9	7	5	3	2	1	1			
11	1	5	10	11	10	7	5	3	2	1	1		
12	1	6	12	15	13	11	7	5	3	2	1	1	
13	**1**	**6**	**14**	18	18	14	11	7	5	3	2	1	1

Table 2. Nombre de partitions d'un entier n en k parties.

Pour la valeur 13 on a les décompositions suivantes :

$$\begin{array}{lll} 13=0+0+13 & 13=0+1+12 & 13=0+2+11 \\ 13=0+3+10 & 13=0+4+9 & 13=0+5+8 \\ 13=0+6+7 & 13=1+1+11 & 13=1+2+10 \\ 13=1+3+9 & 13=1+4+8 & 13=1+5+7 \\ 13=1+6+6 & 13=2+2+9 & 13=2+3+8 \\ 13=2+4+7 & 13=2+5+6 & 13=3+3+7 \\ 13=3+4+6 & 13=3+5+5 & 13=4+4+5 \end{array}$$

Notons que les deux quêtes sont complémentaires. En effet, 13 n'est pas divisible par 3, il ne peut donc y avoir que deux types de répartitions, celles où exactement deux joueurs ont le même nombre de plis et celles où tous les joueurs ont un nombre différent de plis. Il y en a respectivement 7 et $21-7=14$, autrement dit il y a deux fois plus de chances de gagner 5 points en choisissant la deuxième quête.

EXERCICE 30. Déterminez les classes de conjugaison des groupes $\mathfrak{S}_3$ et $\mathfrak{S}_4$.

Solution. On commence par le groupe $\mathfrak{S}_3$ qui en contient 3 dont l'identité $\{\mathrm{Id}\}$. La seconde contient les trois transpositions $(1\ 2)$, $(1\ 3)$ et $(2\ 3)$ (cf. exercice 27 pour comprendre l'origine du résultat). La dernière est formée des deux 3-cycles $(1\ 2\ 3)$ et $(3\ 1\ 2)$.
Le groupe $\mathfrak{S}_4$ en contient 5 dont l'identité $\{\mathrm{Id}\}$. La deuxième est formée des six transpositions $(1\ 2)$, $(1\ 3)$, $(1\ 4)$, $(2\ 3)$, $(2\ 4)$ et $(3\ 4)$. La troisième est formée des huit 3-cycles (d'ordre 3) $(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(2\ 3\ 4)$ et $(2\ 4\ 3)$. La quatrième est formée des six 4-cycles $(1\ 2\ 3\ 4)$, $(1\ 2\ 4\ 3)$, $(1\ 3\ 2\ 4)$, $(1\ 3\ 4\ 2)$, $(1\ 4\ 2\ 3)$ et $(1\ 4\ 3\ 2)$. Enfin la cinquième est formée des trois produits de deux transpositions à supports disjoints $(1\ 2)\,(3\ 4)$, $(1\ 3)\,(2\ 4)$ et $(1\ 4)\,(2\ 3)$.