Corrigé série 13

Exercice 1 (10 points)

a) On ne peut pas toujours diviser dans $\mathbb{Z}$. Par exemple, $\frac{1}{2} \notin \mathbb{Z}$.

b) On ne peut pas faire la division par $0 \in \mathbb{R}$. En effet, pour tout $r \in \mathbb{R}$, $\frac{r}{0}$ n'est pas défini.

c) Oui, on a affaire à une loi de composition. Pour deux polynômes $p(x), q(x) \in \mathbb{Q}[x]$, leur somme est $(p+q)(x) := p(x) + q(x)$, qui a des coefficients dans $\mathbb{Q}$. L'élément neutre est le polynôme nul, $p(x) = 0$.

d) Si on définit $r + \infty = \infty$ pour tout $r \in \mathbb{R}$, il est clair que l'on a affaire à une loi de composition. L'élément neutre est 0.

e) Comme dans la dernière partie, il est clair que l'on a affaire à une loi de composition. L'élément neutre est 0.

f) Il est encore claire que l'on a affaire à une loi de composition si l'on définit, par exemple, $\infty \cdot \infty = \infty$, $(-\infty) \cdot (-\infty) = \infty$ et $\infty \cdot (-\infty) = -\infty$. L'élément neutre est 1.

Exercice 2 (5 points)

Soit $E = \mathcal{P}(X)$ l'ensemble des parties $A \subset X$ qu'on munit de l'intersection. Si $A, B \subset X$, alors $A \cap B \subset X$ aussi. Donc l'intersection donne une loi de composition. L'élément neutre est X, comme $A \cap X = A$ pour tout $A \subset X$. X est le seul ensemble qui admet un inverse par rapport à cette loi de composition (l'inverse de X est lui-même).

Exercice 3 (10 points)

a) Non, $(\mathbb{R}_+^*, *)$ ne forme pas un groupe, car la division n'est pas associative. En général, pour $a, b, c > 0$, il n'est pas toujours vrai que $(a/b)/c = a/(b/c)$.

b) Oui, $(10\mathbb{Z}, +)$ forme un groupe, où $10\mathbb{Z} := \{10k \mid k \in \mathbb{Z}\}$. L'addition est associative. On a que $10k + 10m = 10(k+m) \in 10\mathbb{Z}$ pour tout $k, m \in \mathbb{Z}$. L'élément neutre est 0. Enfin, l'inverse de $10k$ est $-10k = 10(-k)$ pour tout $k \in \mathbb{Z}$. C'est donc un groupe puisque c'est un sous-groupe de $\mathbb{Z}$.

c) Si $k \in \mathbb{Z}$ est à la fois un multiple de 9 et de 12, alors k est divisible par p.p.m.c.$(9; 12) = 36$. Donc, on a $E = 36\mathbb{Z}$. C'est un groupe (sous l'addition), comme dans la dernière partie.

d) Il est facile de voir que $(E, +)$ est un sous-groupe de $(\mathbb{C}, +)$, où $E := \{a + bi \mid a, b \in \mathbb{Z}\}$. En effet, $-a - bi$ est l'inverse de $a + bi$, et $(a + bi) + (c + di) = (a + c) + (b + d)i \in E$ si $a, b, c, d \in \mathbb{Z}$. Donc, $(E, +)$ est un groupe.

e) Soit $E = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Alors, comme dans la dernière partie, on voit que $(E, +)$ est un sous-groupe de $(\mathbb{C}, +)$. Donc $(E, +)$ est bien un groupe.

f) Soit E comme dans la dernière partie. Alors, $(E, *)$ n'est pas un groupe. $0 = 0 + 0 \cdot \sqrt{2}$ n'a aucun inverse dans E.

g) Comme dans la dernière partie, on voit que $(E, *)$ n'est pas un groupe, comme $\sqrt{2}$ n'a aucun inverse dans E.

Exercice 4 (5 points)

On définit l'addition sur l'ensemble $\{0, 1\}$ comme suit : $0 + 0 = 0$, $1 + 1 = 0$ et $1 + 0 = 0 + 1 = 1$. Il s'agit bien d'un groupe abélien.

Exercice 5 (5 points)

Dans cette exercice, on utilise la même notation pour les éléments du groupe du matelas que dans le polycopié "Les groupes". La table de multiplication est donc la suivante. (Note que l'ordre de multiplication n'est pas important : le groupe du matelas est abélien.)

$*$	id	σ	τ	ρ
id	id	σ	τ	ρ
σ	σ	id	ρ	τ
τ	τ	ρ	id	σ
ρ	ρ	τ	σ	id

Exercice 6 (5 points)

Il s'agit bien d'une loi de composition, car un mélange de couleurs est encore une couleur. Cette loi est commutative. Cependant, elle n'est pas associative : si a, b, c sont trois couleurs distinctes, alors $(a * b) * c$ est composée à un quart de a, mais $a * (b * c)$ est composée à moitié de a.

Il n'existe pas une couleur c telle que $a * c = a$ pour toute couleur a. Donc, il n'existe pas un élément neutre, et donc l'ensemble de couleurs avec cette loi de composition n'est pas un groupe.

Exercice 7 (10 points)

a) **Faux.** Considère la loi de composition définie comme ci-dessous :

$$a * a = b$$
$$a * b = a$$
$$b * a = b$$
$$b * b = a$$

Alors, on a que

$$a * (b * a) = a * b = a$$

mais

$$(a * b) * a = a * a = b.$$

b) **Vrai.** On considère tous les cas possibles :

$$b * b * e$$
$$b * e * e$$
$$b * b * b$$
$$b * e * b$$
$$e * b * e$$
$$e * e * e$$
$$e * b * b$$
$$e * e * b$$

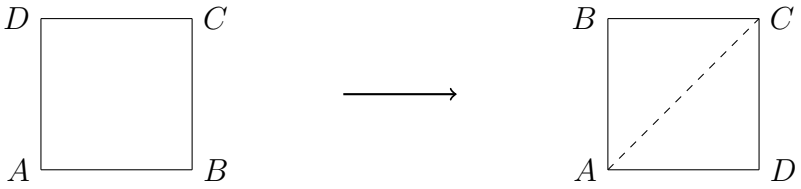
Quelle que soit la manière que l'on a de définir $b * e$ (soit e ou b), l'opération est associative, en utilisant le fait que e est un élément neutre ($e * e = e$, et $b * e = e * b = b$).

c) **Vrai.** Il faut que $a * e = e * a = a$ et $e * e = e$, comme e est l'élément neutre. Aussi, il faut définir $a * a = e$ pour que $\{a, e\}$ forme un groupe, comme il n'y a qu'un unique élément x tel que $x * a = a$. Cela montre qu'il n y a qu'une façon de définir la multiplication dans un groupe de deux éléments.

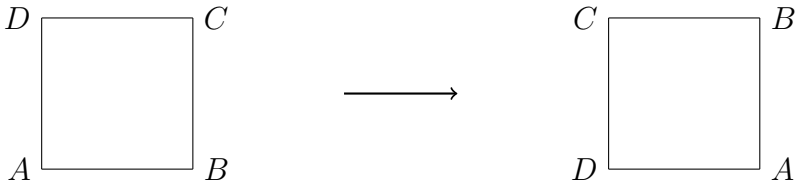
d) **Faux.** Par exemple, $2^{(3^2)} \neq (2^3)^2$.

Exercice 8 (5 points)

Il y a 8 isométries d'un carré dans le plan qui envoient les sommets aux sommets. Il y a 4 rotations (par des angles de 0, $\frac{\pi}{2}$, π et $\frac{3\pi}{2}$, respectivement) et 4 réflexions (à travers les quatre lignes de symétries du carré). Par exemple, une des réflexions est illustrée ci-dessous.



La rotation par un angle de $\frac{\pi}{2}$ est illustrée ci-dessous :



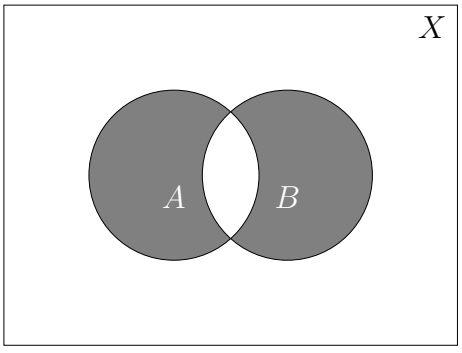
Il est facile de voir que ces isométries forment un groupe. Ce groupe n'est pas abélien. Par exemple, les deux éléments illustrés ci-dessus ne commutent pas.

Exercice 9 (10 points)

a) Avec un diagramme de Venn, comme ci-dessous, il est facile de voir que

$$A\Delta B = (A \cap (X - B)) \cup (B \cap (X - A)) = (A \cup B) - (A \cap B).$$

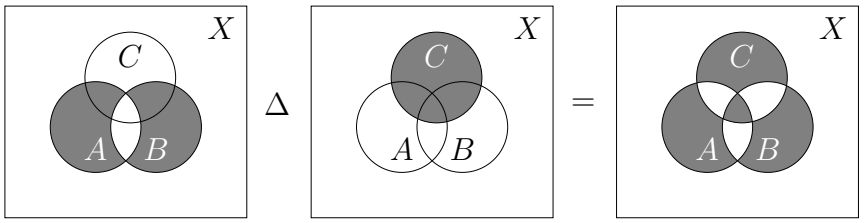
Sur la figure ci-dessous, la partie grise est $A\Delta B$, qui est aussi $(A \cup B) - (A \cap B)$. La partie grise à gauche est $A \cap (X - B)$; la partie grise à droite est $B \cap (X - A)$.



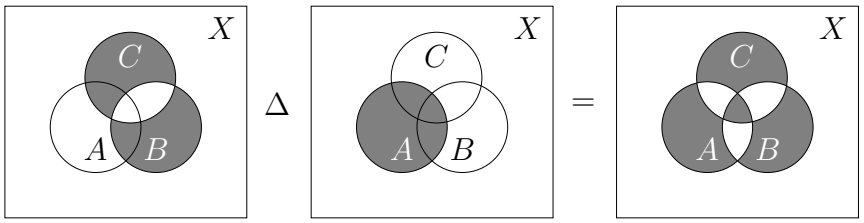
b) À nouveau, on utilise un diagramme de Venn. On veut voir que

$$(A\Delta B)\Delta C = A\Delta(B\Delta C).$$

Les diagrammes ci-dessous montrent $(A\Delta B)\Delta C$:



Les diagrammes ci-dessous montrent $A\Delta(B\Delta C)$:



Ce sont exactement le même. Donc,

$$(A\Delta B)\Delta C = A\Delta(B\Delta C).$$

c) Soit $X = \{a, b\}$. Alors, $\mathcal{P}(X)) = \{\emptyset; \{a\}; \{b\}; \{a; b\}\}$ et la table de la loi de composition Δ est la suivante :

Δ	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a, b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	$\emptyset$	$\{a\}$
$\{a, b\}$	$\{a, b\}$	$\{b\}$	$\{a\}$	$\emptyset$

d) L'élément neutre est $\emptyset$: pour tout $A \subset X$, on a

$$A\Delta\emptyset = (A \cup \emptyset) - (A \cap \emptyset) = A.$$

e) Chaque sous-ensemble $A \subset X$ est l'inverse de lui-même :

$$A\Delta A = (A \cup A) - (A \cap A) = \emptyset.$$

f) On a

$$A\Delta(X - A) = (A \cup (X - A)) - (A \cap (X - A)) = X - \emptyset = X.$$

Exercice 10 (10 points)

a) Un exemple d'un élément d'ordre deux est n'importe quel élément non-trivial du groupe du matelas. Un exemple d'un élément d'ordre infini est 1 dans le groupe $(\mathbb{Z}, +)$, car

$$1^n := \underbrace{1 + 1 + \cdots + 1}_{n \text{ fois}} = n \neq 0$$

pour tout $n \in \mathbb{N}$.

b) On suppose que $g^m = g^n = e$ pour entiers m, n. Soit $d = \text{p.g.d.c.}(m, n)$. Donc, $m = m'd$ et $n = n'd$ pour certains entiers m', n' avec $\text{p.g.d.c.}(m', n') = 1$. Il faut utiliser un peu de la théorie élémentaire des nombres : comme $\text{p.g.d.c.}(m', n') = 1$, il existe des entiers a, b tels que

$$am' + bn' = 1.$$

Donc,

$$g^d = g^{am'd+bn'd} = g^{am+bn} = (g^m)^a * (g^n)^b = e^a * e^b = e.$$

c) On suppose que $g^n = e$. Soit d l'ordre de g (clairement, $1 \leq d \leq n$). Par l'algorithme d'Euclide, on peut écrire $n = qd + r$ avec $q, r \in \mathbb{Z}$ et $0 \leq r < d$. Donc

$$e = g^n = g^{qd+r} = g^{qd} * g^r = g^r.$$

Comme d est le plus petit entier strictement positif tel que $g^d = e$, on voit qu'il faut que r soit 0. Ainsi, d divise n.

d) Soit $g \in G$. Considère l'ensemble $E = \{g, g^2, g^3, \ldots, g^{n+1}\}$ où $n = |G|$. Alors, par le principe des tiroirs, il existe des entiers $1 \leq a < b \leq n + 1$ tels que que $g^a = g^b$. Donc, $g^{b-a} = e$. Cela montre que l'ordre de g est fini.