

Corrigés des TD du Chapitre 10

Exercice 1

a. La loi $*$ est clairement interne et commutative.

$\forall (x, y, z) \in \mathbb{R}^3$, on a :

- $(x * y) * z = x * y + z - (x * y)z = x + y - xy + z - (x + y - xy)z = x + y + z - xy - xz - yz + xyz$.
- $x * (y * z) = x + y * z - x(y * z) = x + y + z - yz - x(y + z - yz) = x + y + z - yz - xy - xz + xyz$.

Donc $(x * y) * z = x * (y * z)$ et la loi $*$ est associative.

De plus, $\forall x \in \mathbb{R}$, on a $x * 0 = 0 * x = x + 0 - 0 = x$ donc 0 est élément neutre de la loi $*$.

Enfin, $\forall x \in \mathbb{R}$, supposons que x admet un symétrique x' pour $*$. Alors, on a $x * x' = 0$, soit :

$$x + x' - xx' = 0 \Leftrightarrow (x - 1)x' = x.$$

Si $x \neq 1$, alors x admet $x' = \frac{x}{x-1}$ pour symétrique, mais $\forall x \in \mathbb{R}$, $x * 1 = x + 1 - x = 1 \neq 0$ donc 1 n'admet pas de symétrique par $*$ (c'est un élément absorbant) et finalement :

$(\mathbb{R}, *)$ n'est pas un groupe.

b. $\forall n \in \mathbb{N}^*$, posons $x_n = x * x * \dots * x$ (avec n facteurs). On a :

$$x_2 = x * x = x + x - x^2 = 2x - x^2 = 1 - (1 - x)^2$$

$$x_3 = x * x * x = x + x * x - x(x * x) = x + 2x - x^2 - x(2x - x^2) = x^3 - 3x^2 + 3x = 1 - (1 - x)^3$$

Conjeturons que $\forall n \in \mathbb{N}^*$, $x_n = 1 - (1 - x)^n$ et prouvons-le par récurrence.

Initialisation : Pour $n = 1$, on a $x_n = x = 1 - (1 - x)^1$ donc la formule est vraie (d'après ce qui précède elle l'est aussi aux rangs 2 et 3).

Hérédité : Supposons la formule vraie au rang n . On veut prouver que $x_{n+1} = 1 - (1 - x)^{n+1}$. On a :

$$\begin{aligned} x_{n+1} &= x * x * \dots * x * x \quad (\text{avec } n+1 \text{ facteurs}) \\ &= x_n * x = x_n + x - x_n x \\ &= 1 - (1 - x)^n + x - [1 - (1 - x)^n]x \quad (\text{par hypothèse de récurrence}) \\ &= 1 - (1 - x)^n + x - x + x(1 - x)^n = 1 - (1 - x)(1 - x)^n \\ &= 1 - (1 - x)^{n+1} \end{aligned}$$

Donc la formule est vraie au rang $n + 1$.

Ainsi, la propriété est initialisée et héréditaire donc elle est vraie $\forall n \in \mathbb{N}^*$, soit :

$$\underbrace{x * x * \dots * x}_{n \text{ facteurs}} = 1 - (1 - x)^n$$

Exercice 2

1) Appelons e l'élément neutre de G . Comme G_1 et G_2 sont des sous-groupes de G , $e \in G_1$ et $e \in G_2$.

- $\forall (x_1, x_2) \in G_1 \times G_2$ et $\forall (y_1, y_2) \in G_1 \times G_2$, on a $x_1 y_1 \in G_1$ et $x_2 y_2 \in G_2$ car G_1 et G_2 sont stables par la loi, donc $(x_1, x_2) \otimes (y_1, y_2) = (x_1 y_1, x_2 y_2) \in G_1 \times G_2$ et la loi \otimes est interne dans $G_1 \times G_2$.
- $\forall (x_1, x_2) \in G_1 \times G_2$, $\forall (y_1, y_2) \in G_1 \times G_2$ et $\forall (z_1, z_2) \in G_1 \times G_2$, on a, avec l'associativité de \cdot dans G :

$$\begin{aligned} [(x_1, x_2) \otimes (y_1, y_2)] \otimes (z_1, z_2) &= (x_1 y_1, x_2 y_2) \otimes (z_1, z_2) = ((x_1 y_1) z_1, (x_2 y_2) z_2) = (x_1 y_1 z_1, x_2 y_2 z_2) \\ (x_1, x_2) \otimes [(y_1, y_2) \otimes (z_1, z_2)] &= (x_1, x_2) \otimes (y_1 z_1, y_2 z_2) = (x_1 (y_1 z_1), x_2 (y_2 z_2)) = (x_1 y_1 z_1, x_2 y_2 z_2) \end{aligned}$$

Donc $[(x_1, x_2) \otimes (y_1, y_2)] \otimes (z_1, z_2) = (x_1, x_2) \otimes [(y_1, y_2) \otimes (z_1, z_2)]$ et \otimes est associative.

- Comme $e \in G_1$ et $e \in G_2$, on a $(e, e) \in G_1 \times G_2$.

De plus, $\forall (x_1, x_2) \in G_1 \times G_2$, $(x_1, x_2) \otimes (e, e) = (x_1 e, x_2 e) = (x_1, x_2)$ et $(e, e) \otimes (x_1, x_2) = (e x_1, e x_2) = (x_1, x_2)$ donc (e, e) est élément neutre pour \otimes .

- $\forall (x_1, x_2) \in G_1 \times G_2$, soient x_1^{-1} et x_2^{-1} les symétriques respectifs de x_1 et x_2 dans G . Comme G_1 et G_2 sont des sous-groupes de G , $x_1^{-1} \in G_1$ et $x_2^{-1} \in G_2$ et :

$$\begin{aligned} (x_1, x_2) \otimes (x_1^{-1}, x_2^{-1}) &= (x_1 x_1^{-1}, x_2 x_2^{-1}) = (e, e) \\ (x_1^{-1}, x_2^{-1}) \otimes (x_1, x_2) &= (x_1^{-1} x_1, x_2^{-1} x_2) = (e, e) \end{aligned}$$

Donc (x_1, x_2) admet $(x_1^{-1}, x_2^{-1}) \in G_1 \times G_2$ pour symétrique par \otimes .

Finalement :

$(G_1 \times G_2, \otimes)$ est un groupe.

2) On a $G_1 \cap G_2 \subset G$ et comme $e \in G_1$ et $e \in G_2$, on a $e \in G_1 \cap G_2$.

De plus, $\forall x \in G_1 \cap G_2$ et $\forall y \in G_1 \cap G_2$, on a :

$$\left. \begin{array}{l} y \in G_1 \Rightarrow y^{-1} \in G_1 \text{ et } x \in G_1 \text{ donc } xy^{-1} \in G_1 \\ y \in G_2 \Rightarrow y^{-1} \in G_2 \text{ et } x \in G_2 \text{ donc } xy^{-1} \in G_2 \end{array} \right\} \Rightarrow xy^{-1} \in G_1 \cap G_2.$$

Donc :

$G_1 \cap G_2$ est un sous-groupe de G .

3) Posons $H = \bigcap_{i \in I} G_i$. On a $H \subset G$ et comme $\forall i \in I$, $e \in G_i$, on a $e \in H$.

De plus, $\forall (x, y) \in H^2$, on a $\forall i \in I$, $y \in G_i \Rightarrow y^{-1} \in G_i$ donc $\forall i \in I$, $xy^{-1} \in G_i$ et ainsi, $xy^{-1} \in H$.

Donc :

$\bigcap_{i \in I} G_i$ est un sous-groupe de G .

4) Appelons \mathcal{A} l'ensemble des sous-groupes de G contenant A . Comme G est un groupe (donc un sous-groupe de G) et contient A , on a $G \in \mathcal{A}$ donc \mathcal{A} est non vide.

Posons alors $G_A = \bigcap_{H \in \mathcal{A}} H$, l'intersection de tous les sous-groupes de G contenant A .

D'après la question précédente, G_A est un sous-groupe de G .

De plus, comme $\forall H \in \mathcal{A}, A \subset H$, on a $A \subset G_A$ et $\forall K \in \mathcal{A}, G_A = \bigcap_{H \in \mathcal{A}} H \subset K$.

Finalement :

L'intersection de tous les sous-groupes de G contenant A est le plus petit sous-groupe de G contenant A .

5) On veut prouver que :

$$G_1 \cup G_2 \text{ est un sous-groupe de } G \Leftrightarrow G_1 \subset G_2 \text{ ou } G_2 \subset G_1.$$

(\Leftarrow) Ce sens est trivial.

En effet, si $G_1 \subset G_2$ alors $G_1 \cup G_2 = G_2$ est bien un sous-groupe de G et si $G_2 \subset G_1$ alors $G_1 \cup G_2 = G_1$ est bien un sous-groupe de G .

(\Rightarrow) Supposons que $G_1 \cup G_2$ est un sous-groupe de G et que $G_1 \not\subset G_2$. Il faut alors prouver que $G_2 \subset G_1$.

Comme $G_1 \not\subset G_2$, il existe $a \in G_1$ tel que $a \notin G_2$ (on a alors $a \in G_1 \cup G_2$).

Alors $\forall x \in G_2$, on a $x \in G_1 \cup G_2$.

Comme $a \in G_1 \cup G_2$ et $G_1 \cup G_2$ est un sous-groupe de G , $xa \in G_1 \cup G_2$, c'est-à-dire $xa \in G_1$ ou $xa \in G_2$.

Mais, si $xa \in G_2$, alors comme $x^{-1} \in G_2$, on a $x^{-1}xa \in G_2$ soit $a \in G_2$, ce qui contredit l'hypothèse $a \notin G_2$.

Donc, $xa \in G_1$ et, comme $a \in G_1$, $xaa^{-1} \in G_1$, soit $x \in G_1$.

Ainsi, $\forall x \in G_2, x \in G_1$, c'est-à-dire $G_2 \subset G_1$.

Finalement, si $G_1 \cup G_2$ est un sous-groupe de G , alors soit $G_1 \subset G_2$, soit $G_2 \subset G_1$.

6) On pose $G_1G_2 = \{x_1x_2 \mid x_1 \in G_1, x_2 \in G_2\}$ et $G_2G_1 = \{x_2x_1 \mid x_1 \in G_1, x_2 \in G_2\}$ et on veut prouver que :

$$G_1G_2 \text{ est un sous-groupe de } G \Leftrightarrow G_1G_2 = G_2G_1.$$

Comme G est un groupe, on a clairement dans tous les cas : $G_1G_2 \subset G$, $G_2G_1 \subset G$ et $e = ee \in G_1G_2$.

(\Rightarrow) Si G_1G_2 est un sous-groupe de G , alors :

- $\forall x \in G_2G_1$, on a $x = x_2x_1$ avec $x_1 \in G_1$ et $x_2 \in G_2$.

Alors, $x^{-1} = x_1^{-1}x_2^{-1}$ avec $x_1^{-1} \in G_1$ et $x_2^{-1} \in G_2$ donc $x^{-1} \in G_1G_2$. Mais G_1G_2 est un sous-groupe de G donc $(x^{-1})^{-1} \in G_1G_2$, soit $x \in G_1G_2$. Ainsi, $\underline{G_2G_1 \subset G_1G_2}$.

- $\forall x \in G_1G_2$, on a $x^{-1} \in G_1G_2$ car G_1G_2 est un sous-groupe de G donc $x^{-1} = y_1y_2$ avec $y_1 \in G_1$ et $y_2 \in G_2$. Alors, $x = (x^{-1})^{-1} = (y_1y_2)^{-1} = y_2^{-1}y_1^{-1}$ avec $y_1^{-1} \in G_1$ et $y_2^{-1} \in G_2$ donc $x \in G_2G_1$.

Ainsi, $\underline{G_1G_2 \subset G_2G_1}$.

Finalement, on a bien :

$$\underline{G_1G_2 = G_2G_1}.$$

(\Leftrightarrow) Si $G_1G_2 = G_2G_1$, alors on a vu que l'on a déjà $e \in G_1G_2$.

$\forall x \in G_1G_2, \forall y \in G_1G_2$, on a $x = x_1x_2$ et $y = y_1y_2$ avec $x_1 \in G_1, x_2 \in G_2, y_1 \in G_1$ et $y_2 \in G_2$ donc :

$$xy^{-1} = x_1x_2y_2^{-1}y_1^{-1}.$$

Mais, $y_2^{-1} \in G_2$ donc $x_2y_2^{-1} \in G_2$ et $y_1^{-1} \in G_1$ donc $x_2y_2^{-1}y_1^{-1} \in G_2G_1$.

Comme $G_1G_2 = G_2G_1$, $x_2y_2^{-1}y_1^{-1} \in G_1G_2$ et il existe $z_1 \in G_1$ et $z_2 \in G_2$ tels que $x_2y_2^{-1}y_1^{-1} = z_1z_2$.

Alors $xy^{-1} = x_1x_2y_2^{-1}y_1^{-1} = x_1z_1z_2 = (x_1z_1)z_2$ avec $x_1z_1 \in G_1$ et $z_2 \in G_2$, ce qui prouve que $xy^{-1} \in G_1G_2$.

Ainsi :

G_1G_2 est un sous-groupe de G .

Exercice 3

Appelons e le neutre de G et x et y les deux autres éléments de G .

On a ainsi, $G = \{e, x, y\}$ avec $x \neq e, y \neq e$ et $x \neq y$.

Pour simplifier, nous noterons la loi $*$ multiplicativement (par exemple $x * y = xy$).

Dresser la table de G revient à déterminer tous les produits de deux éléments de G , sachant que la loi est interne (donc tous les produits valent soit e , soit x , soit y). La loi n'étant a priori pas commutative, il y a 9 produits à déterminer : $e^2, ex, ey, xe, ye, x^2, y^2, xy$ et yx .

Enfin, il ne faut pas oublier non plus que chacun des trois éléments de G admet un symétrique.

On a alors :

- $xe = ex = x, e^2 = e$ et $ye = ey = y$.
- Evaluons xy . Comme on l'a vu $xy = x, y$ ou e .
 - Si $xy = x$, alors $x^{-1}xy = x^{-1}x$ soit $y = e$ ce qui est faux.
 - Si $xy = y$, alors $xyy^{-1} = yy^{-1}$ soit $x = e$ ce qui est faux.

Donc, $xy = e$.

- Evaluons yx . On a $xy = e$ donc $x^{-1}xy = x^{-1}e$ soit $y = x^{-1}$ et y est le symétrique de x , donc $yx = e$.
- Evaluons x^2 .
 - Si $x^2 = x$, alors en multipliant par x^{-1} on obtient $x = e$ ce qui est faux.
 - Si $x^2 = e$, alors en multipliant par x^{-1} on obtient $x = x^{-1} = y$ ce qui est faux.

Donc, $x^2 = y$.

- On montre de la même façon que $y^2 = x$.

Finalement, on obtient la table :

*	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Soit maintenant H un sous groupe de G . On a alors forcément, $e \in H$.

Si $x \in H$, alors comme H est stable par $*$, on a $x * x = x^2 = y \in H$. Donc, si $x \in H$ alors $H = G$.

De la même façon, on montre que si $y \in H$ alors $H = G$.

Finalement :

Les sous-groupes de G sont $\{e\}$ et G .

Un exemple de groupe à trois éléments est l'ensemble des rotations conservant globalement un triangle équilatéral muni de la loi \circ .

En effet, si on appelle O le centre d'un triangle équilatéral ABC , O doit être invariant par les rotations qui conservent globalement ABC , donc doit en être le centre. De plus, le sommet A doit avoir l'un des trois sommets pour image. Il y a ainsi trois rotations qui conservent globalement ABC :

- l'identité ;
- la rotation r de centre O et d'angle $\frac{2\pi}{3}$;
- la rotation de centre O et d'angle $\frac{4\pi}{3}$, qui n'est autre que $r \circ r = r^2$.

Alors :

$G = \{\text{id}, r, r^2\}$

Exercice 4

Posons $f : x \mapsto axa^{-1}$.

- Comme $a \in G$, $a^{-1} \in G$ et $\forall x \in G$, $f(x) = axa^{-1} \in G$ (car la loi est interne). Donc, f est à images dans G .
- $\forall (x, x') \in G^2$, on a $f(xx') = axx'a^{-1} = ax(a^{-1}x'a^{-1}) = (axa^{-1})(ax'a^{-1}) = f(x)f(x')$ donc f est un morphisme de G dans G , soit un endomorphisme de G .
- $\forall (x, x') \in G^2$, $f(x) = f(x') \Leftrightarrow axa^{-1} = ax'a^{-1} \Leftrightarrow a^{-1}(axa^{-1})a = a^{-1}(ax'a^{-1})a \Leftrightarrow x = x'$ donc f est injective.
- $\forall y \in G$, on a $f(x) = y \Leftrightarrow axa^{-1} = y \Leftrightarrow a^{-1}(axa^{-1})a = a^{-1}ya \Leftrightarrow x = a^{-1}ya$ et, il est clair que $f(a^{-1}ya) = y$ donc f est surjective.
- Comme f est injective et surjective, elle est bijective et d'après le point précédent, $f^{-1} : y \mapsto a^{-1}ya$.

Finalement :

$x \mapsto axa^{-1}$ est un automorphisme de G et de réciproque $x \mapsto a^{-1}xa$.

Exercice 5

Ici, il convient de reformuler précisément les choses (attention, la loi $+$ n'est pas forcément commutative). On note 1 le neutre de H .

On a $f : G \rightarrow H$, $b \in H$ tel que $f(a) = b$ avec $a \in G$ et :

- $f^{-1}(\{b\}) = \{x \in G \mid f(x) = b\} \subset G$ donc :

$$x \in f^{-1}(\{b\}) \Leftrightarrow f(x) = b.$$

- $a + \ker f = \{x \in G \mid x = a + x_0, x_0 \in \ker f\} \subset G$ donc :

$$x \in a + \ker f \Leftrightarrow x = a + x_0 \text{ avec } x_0 \in \ker f \Leftrightarrow -a + x \in \ker f \Leftrightarrow f(-a + x) = 1.$$

- $\ker f + a = \{x \in G \mid x = x_0 + a, x_0 \in \ker f\} \subset G$ donc :

$$x \in \ker f + a \Leftrightarrow x = x_0 + a \text{ avec } x_0 \in \ker f \Leftrightarrow x - a \in \ker f \Leftrightarrow f(x - a) = 1.$$

Remarquons par ailleurs que f est un morphisme de groupes de $(G, +)$ dans (H, \cdot) donc $\forall x \in G$:

- $f(-a + x) = f(-a)f(x) = f(a)^{-1}f(x) = b^{-1}f(x)$;
- $f(x - a) = f(x)f(-a) = f(x)f(a)^{-1} = f(x)b^{-1}$.

Enfin, on veut prouver que $f^{-1}(\{b\}) = a + \ker f = \ker f + a$, c'est-à-dire que, $\forall x \in G$:

$$x \in f^{-1}(\{b\}) \Leftrightarrow x \in a + \ker f \Leftrightarrow x \in \ker f + a.$$

Nous n'avons a priori rien fait ici que reformuler les hypothèses, et pourtant c'est fini !

En effet, d'une part :

$$x \in f^{-1}(\{b\}) \Leftrightarrow f(x) = b \Leftrightarrow b^{-1}f(x) = b^{-1}b = 1 \Leftrightarrow f(-a + x) = 1 \Leftrightarrow x \in a + \ker f.$$

Donc $f^{-1}(\{b\}) = a + \ker f$.

Et d'autre part :

$$x \in f^{-1}(\{b\}) \Leftrightarrow f(x) = b \Leftrightarrow f(x)b^{-1} = bb^{-1} = 1 \Leftrightarrow f(x - a) = 1 \Leftrightarrow x \in \ker f + a.$$

Donc $f^{-1}(\{b\}) = \ker f + a$.

Ainsi :

$$f^{-1}(\{b\}) = a + \ker f = \ker f + a$$

Remarque : Les raisonnements équivalences évitent ceux par double inclusion.

Exercice 6

Cet exemple est classique.

L'élément neutre de A pour la multiplication est la fonction constante $1_A : [-1; 1] \rightarrow \mathbb{R} ; x \mapsto 1$. Or, toutes les fonctions de B sont nulles sur $[-1; 0]$ donc $1_A \notin B$ et :

$$B \text{ n'est pas un sous-anneau de } A.$$

Montrons que c'est néanmoins un anneau.

L'ensemble A muni de l'addition et du produit usuels des fonctions est un anneau et $B \subset A$.

- L'élément neutre de A pour l'addition est la fonction nulle sur $[-1; 1]$, notée 0_A . Il est clair que cette fonction est dans B . De plus, $\forall (f, g) \in B^2$, $f - g \in A$ et $\forall x \in [-1; 0]$, $f(x) = g(x) = 0$ donc :

$$(f - g)(x) = f(x) - g(x) = 0.$$

Ainsi, $f - g \in B$ donc $(B, +)$ est un sous-groupe de $(A, +)$, donc un groupe commutatif.

- $\forall (f, g) \in B^2$, la fonction fg est dans A et $\forall x \in [-1; 0]$, $f(x) = g(x) = 0$ donc $(fg)(x) = f(x)g(x) = 0$.

Ainsi, $fg \in B$ donc B est stable par le produit.

- Le produit étant associatif et distributif sur l'addition dans A , il l'est dans B .

- Enfin, la fonction $1_B : [-1;1] \rightarrow \mathbb{R} ; x \mapsto \begin{cases} 0 & \text{si } x \in [-1;0] \\ 1 & \text{si } x \in]0;1] \end{cases}$ est dans B et il est clair que $\forall f \in B$, $1_B f = f 1_B = f$. Ainsi, la multiplication possède un élément neutre dans B (différent de la fonction nulle).

Finalement :

B est un anneau.

Exercice 7

Dans $\mathcal{P}(E)$, les lois Δ et \cap sont clairement internes. Pour prouver que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau, il faut donc prouver que :

- (1) $(\mathcal{P}(E), \Delta)$ est un groupe commutatif ;
- (2) \cap est associative ;
- (3) \cap possède un élément neutre différent de celui de Δ ;
- (4) \cap est distributive à droite et à gauche par rapport à Δ .

Remarquons déjà que le point (2) est acquis (c'est du cours) et que la loi \cap est commutative, donc il suffit de prouver la distributivité à droite (ou à gauche) pour prouver (4).

(1) Pour prouver que $(\mathcal{P}(E), \Delta)$ est un groupe commutatif, il faut prouver que la loi Δ est associative, commutative, admet un élément neutre et que tout élément de $\mathcal{P}(E)$ admet un symétrique par Δ .

- Soient A et B deux parties de E . On a $A \Delta B = (A \setminus B) \cup (B \setminus A)$ et $B \Delta A = (B \setminus A) \cup (A \setminus B)$. Comme \cup est commutative, la loi Δ l'est aussi.
- Soient A, B et C trois parties de E . Introduisons les notations suivantes :

$$I = A \cap B \cap C$$

$$I_A = (B \cap C) \setminus I$$

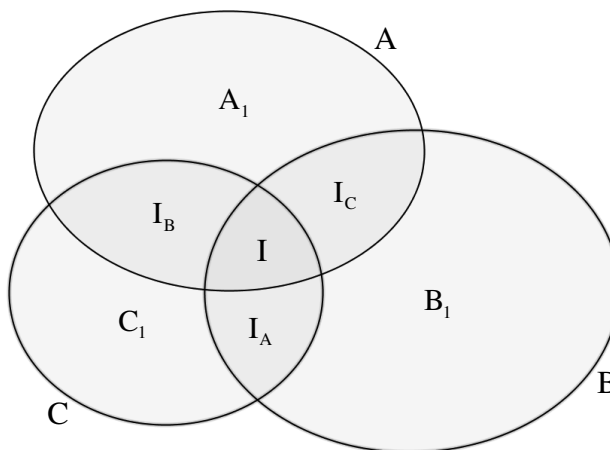
$$I_B = (A \cap C) \setminus I$$

$$I_C = (A \cap B) \setminus I$$

$$A_1 = A \setminus (I \cup I_B \cup I_C)$$

$$B_1 = B \setminus (I \cup I_A \cup I_C)$$

$$C_1 = C \setminus (I \cup I_A \cup I_B)$$



On a alors $A \setminus B = A_1 \cup I_B$ et $B \setminus A = B_1 \cup I_A$ donc $A \Delta B = (A \setminus B) \cup (B \setminus A) = A_1 \cup I_B \cup B_1 \cup I_A$.

Et $(A \Delta B) \setminus C = A_1 \cup B_1$ et $C \setminus (A \Delta B) = C_1 \cup I$ donc :

$$(A \Delta B) \Delta C = [(A \Delta B) \setminus C] \cup [C \setminus (A \Delta B)] = A_1 \cup B_1 \cup C_1 \cup I.$$

De même, $B \Delta C = B_1 \cup I_C \cup C_1 \cup I_B$, $(B \Delta C) \setminus A = B_1 \cup C_1$ et $A \setminus (B \Delta C) = A_1 \cup I$ donc :

$$A \Delta (B \Delta C) = A_1 \cup B_1 \cup C_1 \cup I.$$

Ainsi, $(A \Delta B) \Delta C = A \Delta (B \Delta C)$ et la loi Δ est associative.

- Soit A une partie de E . On a $A \setminus \emptyset = A$ et $\emptyset \setminus A = \emptyset$ donc $A \Delta \emptyset = \emptyset \Delta A = A$ et \emptyset est élément neutre pour Δ .
- Soit A une partie de E . On peut remarquer directement que $A \setminus A = \emptyset$ donc $A \Delta A = \emptyset$ et ainsi, A admet un symétrique par Δ : elle-même.

Finalement, $(\mathcal{P}(E), \Delta)$ est un groupe commutatif.

(2) Ce point est acquis (c'est du cours) : la loi \cap est associative.

(3) On sait aussi que \cap possède un élément neutre : E , qui est bien différent de celui de Δ (\emptyset).

(4) La loi \cap est commutative, donc il suffit de prouver la distributivité à droite.

Soient A, B et C trois parties de E . Comme \cap est distributive sur \cup , on a :

$$(A \Delta B) \cap C = [(A \setminus B) \cup (B \setminus A)] \cap C = [(A \setminus B) \cap C] \cup [(B \setminus A) \cap C].$$

En reprenant les notations utilisées pour l'associativité de Δ , on a :

$$\begin{aligned} (A \setminus B) \cap C &= (A_1 \cup I_B) \cap C = (A_1 \cap C) \cup (I_B \cap C) = \emptyset \cup I_B = I_B \\ (B \setminus A) \cap C &= (B_1 \cup I_A) \cap C = (B_1 \cap C) \cup (I_A \cap C) = \emptyset \cup I_A = I_A \end{aligned}$$

Donc $(A \Delta B) \cap C = I_B \cup I_A$.

Par ailleurs, $(A \cap C) \Delta (B \cap C) = (I_B \cup I) \Delta (I_A \cup I) = [(I_B \cup I) \setminus (I_A \cup I)] \cup [(I_A \cup I) \setminus (I_B \cup I)] = I_B \cup I_A$ donc :

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

et \cap est distributive sur Δ .

Finalement :

$(\mathcal{P}(E), \Delta, \cap)$ est un anneau commutatif, de neutres \emptyset et E pour Δ et \cap respectivement, et dont toute partie est son propre symétrique pour Δ .

Cherchons les inversibles pour \cap .

Si A est une partie de E admettant un symétrique A' pour \cap , on a $A \cap A' = E$, ce qui implique entre autres que $E \subset A$. Mais comme $A \subset E$, on obtient $A = E$.

On a clairement $E \cap E = E$ donc :

Le seul inversible pour \cap est E .

Soient A et B deux parties de E . Supposons que $A \cap B = \emptyset$ (l'équivalent de $ab = 0$ en notations additives et multiplicatives classiques). Il est clair alors que $A \cap B = \emptyset$, n'implique pas $A = \emptyset$ ou $B = \emptyset$ donc :

$(\mathcal{P}(E), \Delta, \cap)$ n'est pas intègre.

Soit E un ensemble. Dans $\mathcal{P}(E)$, on pose $A \Delta B = (A \setminus B) \cup (B \setminus A)$ (la différence symétrique de A et B).

Montrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau. En préciser le neutre et les inversibles (et leur inverse) pour chacune des deux lois. Cet anneau est-il intègre ?

Exercice 8

Soient $a \in A$ non nul. Comme A est stable par produit, $\forall x \in A \setminus \{0\}$, $ax \in A$.

De plus, comme A est intègre, $ax = 0 \Rightarrow a = 0$ ou $x = 0$, ce qui revient à : $a \neq 0$ et $x \neq 0 \Rightarrow ax \neq 0$.

On peut alors définir :

$$f : A \setminus \{0\} \rightarrow A \setminus \{0\}; x \mapsto ax.$$

Soit $(x, x') \in A^2$ tel que $f(x) = f(x')$. On a alors $ax = ax' \Leftrightarrow ax - ax' = 0 \Leftrightarrow a(x - x') = 0$.

Mais A est intègre et $a \neq 0$ donc $a(x - x') = 0 \Rightarrow x - x' = 0$, soit $x = x'$.

Ainsi, f est injective.

Mais A est fini, donc $A \setminus \{0\}$ aussi et on sait que toute injection d'un ensemble fini dans lui-même (de même cardinal !) est bijective. Ainsi, f est bijective.

Ceci implique que tout élément de $A \setminus \{0\}$ admet un antécédent (unique) par f , en particulier 1.

Autrement dit, il existe $a' \in A$ tel que $f(a') = 1$, ou encore, il existe $a' \in A$ tel que $aa' = 1$.

Comme A est commutatif, on alors $aa' = a'a = 1$, ce qui prouve que a admet un symétrique pour le produit.

Comme on a raisonné pour a non nul quelconque, on en déduit que tout élément non nul de A admet un symétrique pour le produit, donc que :

A est un corps.

Exercice 9

Remarquons déjà que pour $\mathbb{E} = \mathbb{Z}$ ou \mathbb{Q} , $\mathbb{E}[\sqrt{2}] \subset \mathbb{R}$ donc pour montrer que $\mathbb{E}[\sqrt{2}]$ est un anneau intègre ou un corps (suivant que $\mathbb{E} = \mathbb{Z}$ ou \mathbb{Q}), il suffit de montrer que c'est un sous-anneau ou sous-corps de \mathbb{R} .

De plus, comme $\sqrt{2}^2 = 2 \in \mathbb{N}$, on a, pour tout polynôme P à coefficients dans \mathbb{E} , $P(\sqrt{2}) = a + b\sqrt{2}$ avec a et b dans \mathbb{E} . Ainsi, pour $\mathbb{E} = \mathbb{Z}$ ou \mathbb{Q} , on a :

$$\mathbb{E}[\sqrt{2}] = \{a + b\sqrt{2} \mid (a, b) \in \mathbb{E}^2\}.$$

Enfin, dans les deux cas, l'écriture $a + b\sqrt{2}$ est unique du fait de l'irrationalité de $\sqrt{2}$.

En effet, si $a + b\sqrt{2} = a' + b'\sqrt{2}$, alors si $b \neq b'$, on a $\sqrt{2} = \frac{a' - a}{b - b'} \in \mathbb{Q}$ ce qui est absurde. Ainsi, $b = b'$ qui implique immédiatement $a = a'$.

1) Posons $A = \mathbb{Z}[\sqrt{2}]$.

$\forall (x, x') \in A^2$, il existe $(a, b, a', b') \in \mathbb{Z}^4$ tel que $x = a + b\sqrt{2}$ et $x' = a' + b'\sqrt{2}$. Alors :

- $x - x' = (a - a') + (b - b')\sqrt{2}$ avec $a - a' \in \mathbb{Z}$ et $b - b' \in \mathbb{Z}$ donc $x - x' \in A$.

Alors, comme $0 = 0 + 0\sqrt{2} \in A$, A est un sous-groupe de $(\mathbb{R}, +)$.

- $xx' = (aa' + 2bb') + (ba' + ab')\sqrt{2}$ avec $aa' + 2bb' \in \mathbb{Z}$ et $ba' + ab' \in \mathbb{Z}$ donc $xx' \in A$.

Ainsi, A est stable par la multiplication.

- $1 = 1 + 0\sqrt{2} \in A$.

Donc A est un sous-anneau de \mathbb{R} et ainsi :

$$A = \mathbb{Z}[\sqrt{2}] \text{ est un anneau int\grave{e}gre.}$$

Soit maintenant, $x = a + b\sqrt{2} \neq 0$ inversible dans $\mathbb{Z}[\sqrt{2}]$, son inverse est alors $\frac{1}{x} \in \mathbb{Z}[\sqrt{2}]$.

On a forc\^ement $a - b\sqrt{2} \neq 0$, car sinon, si $b = 0$, on aurait $x = a = 0$ et si $b \neq 0$, on aurait $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ ce qui, dans les deux cas, est absurde.

$$\text{Alors, } \frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2}.$$

Donc, x est inversible si et seulement si $N = \frac{a}{a^2 - 2b^2}$ et $M = \frac{b}{a^2 - 2b^2}$ sont entiers.

Alors, $aN - 2bM = 1$ donc, d'apr\^es le th\^eor\^eme de B\^ezout, $\text{PGCD}(a, b) = 1$.

Mais, comme N et M sont entiers, l'entier $a^2 - 2b^2$ est un diviseur commun \`a a et b donc vaut 1 ou -1 .

Consid\^erons ces deux cas :

- Si $a^2 - 2b^2 = 1$, alors $(a - b)(a + b) = a^2 - b^2 = b^2 + 1$ donc $a - b \mid b^2 + 1$ et $a + b \mid b^2 + 1$. Alors :
 - si $b = 0$, on a $a^2 = 1$;
 - si $b \neq 0$, on a $2b = (a + b) - (a - b)$ donc $2b \mid b^2 + 1$.

Mais $b \mid 2b$ donc $b \mid b^2 + 1$ et comme $b \mid b^2$, on obtient $b \mid 1$, soit $b = \pm 1$.

Alors, $b^2 = 1$ donc $a^2 = 2b^2 + 1 = 3$ ce qui est impossible car a est entier.

Donc, dans ce premier cas, on a forc\^ement $b = 0$ et $a^2 = 1$, soit $x = 1$ ou $x = -1$.

R\^eciproquement, il est clair que dans les deux cas $\frac{1}{x} = x \in \mathbb{Z}[\sqrt{2}]$.

- Si $a^2 - 2b^2 = -1$, alors $b \neq 0$ (car sinon $a^2 = -1$) et comme plus haut, $(a - b)(a + b) = b^2 - 1$ donc $a - b \mid b^2 - 1$ et $a + b \mid b^2 - 1$.

Alors, toujours comme ci-dessus, on obtient $2b \mid b^2 - 1$, puis $b \mid b^2 - 1$, puis $b \mid -1$ donc $b = \pm 1$.

De $a^2 - 2b^2 = -1$, on tire $a^2 = 1$ donc $a = \pm 1$.

Donc, dans ce second cas, on a $b = \pm 1$ et $a = \pm 1$, soit $x = 1 + \sqrt{2}$ ou $x = 1 - \sqrt{2}$ ou $x = -1 + \sqrt{2}$ ou $x = -1 - \sqrt{2}$.

R\^eciproquement, on a $\frac{1}{1 + \sqrt{2}} = \frac{1 - \sqrt{2}}{1 - 2} = -1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ et $\frac{1}{1 - \sqrt{2}} = \frac{1 + \sqrt{2}}{1 - 2} = -1 - \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ donc

$1 + \sqrt{2}$ et $-1 + \sqrt{2}$ sont inverses l'un de l'autre dans $\mathbb{Z}[\sqrt{2}]$ et il en va de m\^eme pour $1 - \sqrt{2}$ et $-1 - \sqrt{2}$.

Finalement :

$$\text{Les inversibles de } \mathbb{Z}[\sqrt{2}] \text{ sont } -1, 1, 1 + \sqrt{2}, -1 + \sqrt{2}, 1 - \sqrt{2} \text{ et } -1 - \sqrt{2}.$$

2) Posons $K = \mathbb{Q}[\sqrt{2}]$.

$\forall (x, x') \in K^2$, il existe $(a, b, a', b') \in \mathbb{Q}^4$ tel que $x = a + b\sqrt{2}$ et $x' = a' + b'\sqrt{2}$.

Alors :

- $x - x' = (a - a') + (b - b')\sqrt{2}$ avec $a - a' \in \mathbb{Q}$ et $b - b' \in \mathbb{Q}$ donc $x - x' \in \mathbb{K}$.

Alors, comme $0 = 0 + 0\sqrt{2} \in \mathbb{K}$, \mathbb{K} est un sous-groupe de $(\mathbb{R}, +)$.

- Pour $x \neq 0$ et $x' \neq 0$, on a $a' - b'\sqrt{2} \neq 0$ (on le montre comme plus haut). Alors :

$$\frac{x}{x'} = \frac{a + b\sqrt{2}}{a' + b'\sqrt{2}} = \frac{(a + b\sqrt{2})(a' - b'\sqrt{2})}{(a' + b'\sqrt{2})(a' - b'\sqrt{2})} = \frac{aa' - 2bb'}{a'^2 - 2b'^2} + \frac{a'b - ab'}{a'^2 - 2b'^2} \sqrt{2}$$

avec $\frac{aa' - 2bb'}{a'^2 - 2b'^2} \in \mathbb{Q}$ et $\frac{a'b - ab'}{a'^2 - 2b'^2} \in \mathbb{Q}$ donc $xx' \in \mathbb{K}^*$.

Ainsi, comme $1 = 1 + 0\sqrt{2} \in \mathbb{K}^*$, \mathbb{K}^* est un sous-groupe de (\mathbb{R}^*, \times) .

Donc \mathbb{K} est un sous-corps de \mathbb{R} et ainsi :

$$\mathbb{K} = \mathbb{Q}[\sqrt{2}] \text{ est un corps.}$$

Exercice 10

1) Soit \mathbb{K} est un sous-corps de \mathbb{R} , il contient \mathbb{Q} . Pour prouver que $\mathbb{Q} \subset \mathbb{K}$, procédons par étapes :

- Prouvons que $\mathbb{N} \subset \mathbb{K}$ ce qui revient à montrer que $\forall n \in \mathbb{N}, n \in \mathbb{K}$. On procède par récurrence.

Initialisation : \mathbb{K} est un sous-corps de \mathbb{R} donc il contient 0 et la propriété est vraie pour $n = 0$.

Hérédité : Supposons la propriété vraie au rang n .

\mathbb{K} est un sous-corps de \mathbb{R} donc il contient 1 et, par hypothèse de récurrence, $n \in \mathbb{K}$.

Comme \mathbb{K} est stable par l'addition, $n + 1 \in \mathbb{K}$ donc la propriété est vraie au rang $n + 1$.

Ainsi, la propriété est initialisée et héréditaire donc elle est vraie $\forall n \in \mathbb{N}$ et $\mathbb{N} \subset \mathbb{K}$.

- Prouvons que $\mathbb{Z} \subset \mathbb{K}$. Comme $(\mathbb{K}, +)$ est un groupe, $\forall x \in \mathbb{K}, -x \in \mathbb{K}$.

On a vu que $\forall n \in \mathbb{N}, n \in \mathbb{K}$ donc $-n \in \mathbb{K}$ et ainsi, $\forall n \in \mathbb{Z}, n \in \mathbb{K}$, soit $\mathbb{Z} \subset \mathbb{K}$.

- Comme \mathbb{K} est un sous-corps de \mathbb{R} , (\mathbb{K}^*, \times) est un groupe donc $\forall (x, y) \in \mathbb{K} \times \mathbb{K}^*, \frac{x}{y} \in \mathbb{K}$.

En particulier, $\forall (p, q) \in \mathbb{Z} \times \mathbb{N}^* \subset \mathbb{K} \times \mathbb{K}^*, \frac{p}{q} \in \mathbb{K}$ et ainsi :

$$\mathbb{Q} \subset \mathbb{K}.$$

2) Remarquons déjà que si \mathbb{K} est un sous-corps de \mathbb{R} , alors, comme \mathbb{K} est stable par produit, $\forall a \in \mathbb{K}, a\mathbb{Q} \subset \mathbb{K}$ (où $a\mathbb{Q}$ est l'ensemble des nombres de la forme ar avec $r \in \mathbb{Q}$).

En supposant qu'il en existe, soit alors \mathbb{K} un sous-corps de \mathbb{R} contenant $\sqrt{2}$ et $\sqrt{3}$.

Le corps \mathbb{K} contient au moins 0, 1, $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{2}\sqrt{3} = \sqrt{6}$ (car \mathbb{K} est stable par produit). Alors, d'après ce qui précède, \mathbb{K} contient \mathbb{Q} , $\mathbb{Q}\sqrt{2}$, $\mathbb{Q}\sqrt{3}$ et $\mathbb{Q}\sqrt{6}$.

Mais \mathbb{K} est stable par addition, donc il contient tous les nombres de la forme $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ avec a, b, c et d rationnels.

Posons alors :

$$\mathbb{K}_0 = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid (a, b, c, d) \in \mathbb{Q}^4\}.$$

Ce qui précède montre que :

$$\underline{K_0 \subset K}.$$

En remarquant que $\sqrt{2}\sqrt{6} = \sqrt{12} = 2\sqrt{3}$ et $\sqrt{3}\sqrt{6} = \sqrt{18} = 3\sqrt{2}$, on montre facilement (comme dans l'exercice précédent) que K_0 est un sous-anneau de \mathbb{R} .

De plus, si $x \in K_0 \setminus \{0\}$, on a $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ avec $(a, b, c, d) \in \mathbb{Q}^4$ et :

$$\begin{aligned} \frac{1}{x} &= \frac{1}{b\sqrt{2} + c\sqrt{3} + a + d\sqrt{6}} = \frac{(b\sqrt{2} + c\sqrt{3}) - (a + d\sqrt{6})}{(b\sqrt{2} + c\sqrt{3})^2 - (a + d\sqrt{6})^2} = \frac{b\sqrt{2} + c\sqrt{3} - a - d\sqrt{6}}{(2b^2 + 3c^2 - a^2 - 6d^2) + 2\sqrt{6}(bc - ad)} \\ &= \frac{[b\sqrt{2} + c\sqrt{3} - a - d\sqrt{6}][(2b^2 + 3c^2 - a^2 - 6d^2) - 2\sqrt{6}(bc - ad)]}{(2b^2 + 3c^2 - a^2 - 6d^2)^2 - 24(bc - ad)^2} \end{aligned}$$

Et comme $(2b^2 + 3c^2 - a^2 - 6d^2)^2 - 24(bc - ad)^2 \in \mathbb{Q}$, on a bien $x^{-1} \in K_0$, ce qui prouve que :

$$\underline{K_0 \text{ est un corps}}.$$

Il faut remarquer ici que pour mener à bien le calcul précédent, il faut quand même vérifier que :

$$x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \neq 0 \Rightarrow b\sqrt{2} + c\sqrt{3} - a - d\sqrt{6} \neq 0 \text{ et } (2b^2 + 3c^2 - a^2 - 6d^2) - 2\sqrt{6}(bc - ad) \neq 0.$$

En posant $y = b\sqrt{2} + c\sqrt{3} - a - d\sqrt{6}$ et $z = (2b^2 + 3c^2 - a^2 - 6d^2) - 2\sqrt{6}(bc - ad)$, on veut donc prouver que :

$$(x \neq 0 \Rightarrow y \neq 0 \text{ et } z \neq 0) \text{ soit } (y = 0 \text{ ou } z = 0 \Rightarrow x = 0)$$

- Supposons que $y = 0$.

$$\text{Remarquons que } xy = (b\sqrt{2} + c\sqrt{3})^2 - (a + d\sqrt{6})^2 = (2b^2 + 3c^2 - a^2 - 6d^2) + 2\sqrt{6}(bc - ad).$$

Alors $xy = 0$ donc $bc = ad$ (sinon $\sqrt{6}$ serait rationnel). On peut alors écrire :

$$ay = a(b\sqrt{2} + c\sqrt{3}) - a^2 - ad\sqrt{6} = a(b\sqrt{2} + c\sqrt{3}) - a^2 - bc\sqrt{6} = -(a - b\sqrt{2})(a - c\sqrt{3}) = 0.$$

Donc $a = b\sqrt{2}$ ou $a = c\sqrt{3}$. Mais, avec $y = b\sqrt{2} + c\sqrt{3} - a - d\sqrt{6} = 0$, on peut compléter en :

$$(a = b\sqrt{2} \text{ et } c = d\sqrt{2}) \text{ ou } (a = c\sqrt{3} \text{ et } b = d\sqrt{3}).$$

Evaluons ces deux cas :

- si $a = b\sqrt{2}$ et $c = d\sqrt{2}$ alors $b = d = 0$ (sinon $\sqrt{2}$ serait rationnel) donc $a = b = c = d = 0$;
- si $a = c\sqrt{3}$ et $b = d\sqrt{3}$ alors $c = d = 0$ (sinon $\sqrt{3}$ serait rationnel) donc $a = b = c = d = 0$.

Finalement, dans les deux cas, on obtient $a = b = c = d = 0$ et donc $x = 0$.

- Supposons que $z = 0$.

Alors $bc = ad$ (sinon $\sqrt{6}$ serait rationnel), ce qui implique que $2b^2 + 3c^2 - a^2 - 6d^2 = 0$ et donc que $xy = 0$.

Mais alors soit $x = 0$, soit $y = 0$ et on a vu que qu'alors $x = 0$. Donc, dans les deux cas $x = 0$.

Ainsi, on a bien, $x \neq 0 \Rightarrow y \neq 0$ et $z \neq 0$.

Finalement, on a prouvé qu'il existe un sous-corps de \mathbb{R} contenant $\sqrt{2}$ et $\sqrt{3}$: K_0 et que si K est un sous-corps de \mathbb{R} contenant $\sqrt{2}$ et $\sqrt{3}$, alors $K_0 \subset K$, donc :

$$\boxed{\text{Le plus petit (au sens de l'inclusion) sous-corps de } \mathbb{R} \text{ contenant } \sqrt{2} \text{ et } \sqrt{3} \text{ est } K_0.}$$

Remarque : Comme dans l'exercice précédent, on note ce corps $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

Exercice 11

a. On a $\sum_{k=0}^n (3k^2 + 2k + 2) = 3 \sum_{k=0}^n k^2 + 2 \sum_{k=0}^n k + \sum_{k=0}^n 2 = 3 \frac{n(n+1)(2n+1)}{6} + 2 \frac{n(n+1)}{2} + 2(n+1) = \frac{n+1}{2} (2n^2 + 3n + 4)$.

Donc :

$$\begin{aligned} \sum_{k=7}^{73} (3k^2 + 2k + 2) &= \sum_{k=0}^{73} (3k^2 + 2k + 2) - \sum_{k=0}^6 (3k^2 + 2k + 2) \\ &= \frac{74}{2} (2 \times 74^2 + 3 \times 74 + 4) - \frac{7}{2} (2 \times 6^2 + 3 \times 6 + 4) \\ &= 413257 \end{aligned}$$

b. On a $\sum_{k=1}^n (-1)^k \binom{n}{k} = \sum_{k=0}^n \binom{n}{k} (-1)^k - (-1)^0 \binom{n}{0} = (-1+1)^n - 1$, soit :

$$\sum_{k=1}^n (-1)^k \binom{n}{k} = -1$$

Si $n=0$, $\sum_{k=0}^0 k \binom{0}{k} = 0$ et si $n \geq 1$:

$$\sum_{k=0}^n k \binom{n}{k} = \sum_{k=1}^n k \binom{n}{k} = \sum_{k=1}^n k \frac{n!}{(n-k)!k!} = \sum_{k=1}^n n \frac{(n-1)!}{(n-k)!(k-1)!} = n \sum_{k=1}^n \binom{n-1}{k-1} = n \sum_{k=0}^{n-1} \binom{n-1}{k} = n2^{n-1}.$$

Dans les deux cas :

$$\sum_{k=0}^n k \binom{n}{k} = n2^{n-1}$$

Si $n=0$, $\sum_{k=0}^0 k^2 \binom{0}{k} = 0$, si $n=1$, $\sum_{k=0}^1 k^2 \binom{1}{k} = 0+1=1$ et si $n \geq 2$:

$$\begin{aligned} \sum_{k=0}^n k^2 \binom{n}{k} &= \sum_{k=0}^n (k^2 - k) \binom{n}{k} + \sum_{k=0}^n k \binom{n}{k} = \sum_{k=2}^n k(k-1) \frac{n!}{(n-k)!k!} + n2^{n-1} \\ &= \sum_{k=2}^n n(n-1) \frac{(n-2)!}{(n-2-(k-2))!(k-2)!} + n2^{n-1} = n(n-1) \sum_{k=2}^n \binom{n-2}{k-2} + n2^{n-1} \\ &= n(n-1) \sum_{k=0}^{n-2} \binom{n-2}{k} + n2^{n-1} = n(n-1)2^{n-2} + n2^{n-1} = [n(n-1) + 2n]2^{n-2} = n(n+1)2^{n-2} \end{aligned}$$

Dans les trois cas :

$$\sum_{k=0}^n k^2 \binom{n}{k} = n(n+1)2^{n-2}$$

c. $\sum_{j=1}^n \sum_{i=1}^n 2^j i = \left(\sum_{j=1}^n 2^j \right) \left(\sum_{i=1}^n i \right) = 2 \frac{2^n - 1}{2 - 1} \frac{n(n+1)}{2}$ soit :

$$\sum_{j=1}^n \sum_{i=1}^n 2^j i = n(n+1)(2^n - 1)$$

$$\begin{aligned} \sum_{j=1}^n \sum_{i=1}^n (i+j)2^{i+j} &= \sum_{j=1}^n \left(2^j \sum_{i=1}^n (i+j)2^i \right) = \sum_{j=1}^n \left(2^j \sum_{i=1}^n i2^i + 2^j j \sum_{i=1}^n 2^i \right) = \sum_{j=1}^n \left(2^j \sum_{i=1}^n i2^i \right) + \sum_{j=1}^n \left(2^j j \sum_{i=1}^n 2^i \right) \\ &= \left(\sum_{j=1}^n 2^j \right) \left(\sum_{i=1}^n i2^i \right) + \left(\sum_{i=1}^n 2^i \right) \left(\sum_{j=1}^n j2^j \right) = 2 \left(\sum_{i=1}^n 2^i \right) \left(\sum_{i=1}^n i2^i \right) \end{aligned}$$

Or, $\sum_{i=1}^n 2^i = 2(2^n - 1)$ et si on pose $S_n = \sum_{i=1}^n i2^i$, on a :

$$\begin{aligned} S_n &= \sum_{i=1}^n (i+1)2^i - \sum_{i=1}^n 2^i = \frac{1}{2} \sum_{i=1}^n (i+1)2^{i+1} - \sum_{i=1}^n 2^i = \frac{1}{2} \sum_{i=2}^{n+1} i2^i - \sum_{i=1}^n 2^i \\ &= \frac{1}{2} \left[(n+1)2^{n+1} + S_n - 2 \right] - 2(2^n - 1) = \frac{1}{2} S_n + (n-1)2^n + 1 \end{aligned}$$

Donc $S_n = (n-1)2^{n+1} + 2$ d'où $\sum_{j=1}^n \sum_{i=1}^n (i+j)2^{i+j} = 2 \left[2(2^n - 1) \right] \left[(n-1)2^{n+1} + 2 \right]$ soit :

$$\boxed{\sum_{j=1}^n \sum_{i=1}^n (i+j)2^{i+j} = 8(2^n - 1) \left[(n-1)2^n + 1 \right]}$$

d. $\sum_{1 \leq i, j \leq n} ij = \sum_{j=1}^n \sum_{i=1}^n ij = \sum_{j=1}^n \left(j \sum_{i=1}^n i \right) = \left(\sum_{j=1}^n j \right) \left(\sum_{i=1}^n i \right) = \left(\sum_{i=1}^n i \right)^2$ donc :

$$\boxed{\sum_{1 \leq i, j \leq n} ij = \frac{n^2(n+1)^2}{4}}$$

$$\begin{aligned} \sum_{1 \leq i \leq j \leq n} ij &= \sum_{j=1}^n \sum_{i=1}^j ij = \sum_{j=1}^n \left(j \sum_{i=1}^j i \right) = \sum_{j=1}^n j \frac{j(j+1)}{2} = \frac{1}{2} \left(\sum_{j=1}^n j^3 + \sum_{j=1}^n j^2 \right) = \frac{1}{2} \left(\frac{n^2(n+1)^2}{4} + \frac{n(n+1)(2n+1)}{6} \right) \\ &= \frac{n(n+1)}{24} [3n(n+1) + 2(2n+1)] = \frac{n(n+1)}{24} [3n^2 + 7n + 2] \end{aligned}$$

Soit, en factorisant :

$$\boxed{\sum_{1 \leq i \leq j \leq n} ij = \frac{n(n+1)(n+2)(3n+1)}{24}}$$

e. $\sum_{k=1}^n \sum_{i=1}^k \frac{i}{k} = \sum_{k=1}^n \left(\frac{1}{k} \sum_{i=1}^k i \right) = \sum_{k=1}^n \left(\frac{1}{k} \frac{k(k+1)}{2} \right) = \frac{1}{2} \sum_{k=1}^n (k+1) = \frac{1}{2} \left(\sum_{k=1}^n k + \sum_{k=1}^n 1 \right) = \frac{1}{2} \left(\frac{n(n+1)}{2} + n \right) = \frac{n(n+1) + 2n}{4}$.

Soit :

$$\boxed{\sum_{k=1}^n \sum_{i=1}^k \frac{i}{k} = \frac{n(n+3)}{4}}$$

$$\begin{aligned}
 S &= \sum_{k=1}^n \sum_{i=1}^k \frac{k}{i} = \sum_{i=1}^n \frac{1}{i} + \sum_{i=1}^2 \frac{2}{i} + \sum_{i=1}^3 \frac{3}{i} + \dots + \sum_{i=1}^{n-1} \frac{n-1}{i} + \sum_{i=1}^n \frac{n}{i} \\
 &= \binom{1}{1} + \binom{2}{1} + \binom{2}{2} + \binom{3}{1} + \binom{3}{2} + \binom{3}{3} + \dots + \binom{n-1}{1} + \binom{n-1}{2} + \binom{n-1}{3} + \dots + \binom{n-1}{n-1} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \dots + \binom{n}{n} \\
 &= \left(\frac{1}{1} + \frac{2}{1} + \frac{3}{1} + \dots + \frac{n-1}{1} + \frac{n}{1} \right) + \left(\frac{2}{2} + \frac{3}{2} + \frac{n-1}{2} + \frac{n}{2} \right) + \left(\frac{3}{3} + \dots + \frac{n-1}{3} + \frac{n}{3} \right) + \dots + \left(\frac{n-1}{n-1} + \frac{n}{n} \right) + \left(\frac{n}{n} \right) \\
 &= \sum_{i=1}^n i + \frac{1}{2} \sum_{i=2}^n i + \frac{1}{3} \sum_{i=3}^n i + \dots + \frac{1}{n-1} \sum_{i=n-1}^n i + 1 \\
 &= \sum_{i=1}^n i + \frac{1}{2} \left(\sum_{i=1}^n i - \sum_{i=1}^1 i \right) + \frac{1}{3} \left(\sum_{i=1}^n i - \sum_{i=1}^2 i \right) + \dots + \frac{1}{n-1} \left(\sum_{i=1}^n i - \sum_{i=1}^{n-2} i \right) + \frac{1}{n} \left(\sum_{i=1}^n i - \sum_{i=1}^{n-1} i \right) \\
 &= \sum_{i=1}^n i + \frac{1}{2} \sum_{i=1}^n i + \frac{1}{3} \sum_{i=1}^n i + \dots + \frac{1}{n-1} \sum_{i=1}^n i + \frac{1}{n} \sum_{i=1}^n i - \frac{1}{2} \sum_{i=1}^1 i - \frac{1}{3} \sum_{i=1}^2 i - \dots - \frac{1}{n-1} \sum_{i=1}^{n-2} i - \frac{1}{n} \sum_{i=1}^{n-1} i \\
 &= \sum_{i=1}^n i \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n-1} + \frac{1}{n} \right) - \sum_{k=2}^n \left(\frac{1}{k} \sum_{i=1}^{k-1} i \right) \\
 &= \frac{n(n+1)}{2} S_n - \sum_{k=2}^n \left(\frac{1}{k} \frac{(k-1)k}{2} \right) = \frac{n(n+1)}{2} S_n - \frac{1}{2} \sum_{k=2}^n (k-1) = \frac{n(n+1)}{2} S_n - \frac{1}{2} \sum_{k=1}^{n-1} k
 \end{aligned}$$

Soit :

$$\boxed{\sum_{k=1}^n \sum_{i=1}^k \frac{k}{i} = \frac{n(n+1)}{2} S_n - \frac{(n-1)n}{4}}$$

$$\text{f. } \prod_{k=2}^n \left(1 - \frac{1}{k} \right) = \prod_{k=2}^n \frac{k-1}{k} = \frac{\prod_{k=2}^n (k-1)}{\prod_{k=2}^n k} = \frac{\prod_{k=1}^{n-1} k}{\prod_{k=1}^n k} = \frac{(n-1)!}{n!}$$

Soit :

$$\boxed{\prod_{k=2}^n \left(1 - \frac{1}{k} \right) = \frac{1}{n}}$$

$$\begin{aligned}
 \prod_{k=2}^n \left(1 - \frac{1}{k^2} \right) &= \prod_{k=2}^n \frac{k^2-1}{k^2} = \frac{\prod_{k=2}^n (k^2-1)}{\prod_{k=2}^n k^2} = \frac{\prod_{k=2}^n [(k-1)(k+1)]}{\left(\prod_{k=2}^n k \right)^2} \\
 &= \frac{\left(\prod_{k=2}^n (k-1) \right) \left(\prod_{k=2}^n (k+1) \right)}{\left(\prod_{k=2}^n k \right)^2} = \frac{\left(\prod_{k=1}^{n-1} k \right) \left(\prod_{k=3}^{n+1} k \right)}{\left(\prod_{k=1}^n k \right)^2} = \frac{(n-1)! \frac{1}{2} (n+1)!}{(n!)^2}
 \end{aligned}$$

Soit :

$$\boxed{\prod_{k=2}^n \left(1 - \frac{1}{k^2} \right) = \frac{n+1}{2n}}$$

g. $\prod_{k=2}^n 2^{k^2} = 2^{\sum_{k=2}^n k^2} = 2^{\sum_{k=1}^n k^2 - 1}$ soit :

$$\prod_{k=2}^n 2^{k^2} = 2^{\frac{n(n+1)(2n+1)}{6} - 1}$$

Exercice 12

1) On a $p \geq 2$, $a \in \mathbb{Z}^*$ et $a \wedge p = 1$.

$\forall n \in \mathbb{N}$, on pose $a^n = q_n p + r_n$ avec $0 \leq r_n < p$ la division euclidienne de a^n par p .

On a alors $\forall n \in \mathbb{N}$, $r_n \in \llbracket 0; p-1 \rrbracket$ donc $\{r_0, r_1, \dots, r_p\} \subset \llbracket 0; p-1 \rrbracket$.

Or, $\text{Card} \llbracket 0; p-1 \rrbracket = p$, donc les $p+1$ restes r_0, r_1, \dots, r_p ne peuvent être distincts deux à deux et ainsi, il existe deux entiers k et k' de $\llbracket 0; p-1 \rrbracket$ tels $k < k'$ et $r_k = r_{k'}$, avec k le plus petit possible.

Posons $T = k' - k > 0$. On a alors $r_{k+T} = r_{k'} = r_k$ donc :

$$\begin{cases} a^{k+T} = q_{k+T} p + r_{k+T} = q_{k+T} p + r_k \\ a^k = q_k p + r_k \end{cases} \Rightarrow a^{k+T} - a^k = a^k (a^T - 1) = (q_{k+T} - q_k) p.$$

Ceci prouve que p divise $a^k (a^T - 1)$.

Mais $a \wedge p = 1$ donc a et p n'ont aucun facteur premier commun d'où $a^k \wedge p = 1$.

Le théorème de Gauss permet alors de conclure que $p \mid a^T - 1$ et il existe un entier m tel que $a^T = mp + 1$.

Alors, $\forall n \in \mathbb{N}$, on a :

$$a^{n+T} = a^n a^T = (q_n p + r_n)(mp + 1) = [q_n (mp + 1) + r_n m] p + r_n = Q p + r_n.$$

Or, $Q = q_n (mp + 1) + r_n m$ est un entier et $0 \leq r_n < p$ donc l'écriture ci-dessus est la division euclidienne de a^{n+T} par p (car elle est unique) et ainsi :

$$r_{n+T} = r_n.$$

Ceci prouve que :

La suite $(r_n)_{n \in \mathbb{N}}$ est T -périodique.

2) Avec les notations de la question précédente et en prenant $p = 5$ et $a = 3$, on cherche r_{2010} . On a :

- $3^0 = 1$ donc $r_0 = 1$.
- $3^1 = 3$ donc $r_1 = 3$;
- $3^2 = 9 = 5 + 4$ donc $r_2 = 4$;
- $3^3 = 27 = 5 \times 5 + 2$ donc $r_3 = 2$;
- $3^4 = 81 = 16 \times 5 + 1$ donc $r_4 = 1$.

D'après la question précédente, la suite $(r_n)_{n \in \mathbb{N}}$ est 4-périodique.

Or, $2010 = 4 \times 502 + 2$ donc $r_{2010} = r_{4 \times 502 + 2} = r_2 = 4$ et ainsi :

Le reste de la division euclidienne de 3^{2010} par 5 est 4.

3) On procède comme ci-dessus avec $p = 13$ et :

- Pour $a = 3$, on appelle $(r_n)_{n \in \mathbb{N}}$ la suite des restes. Avec $3^3 = 27 = 2 \times 13 + 1$, on trouve $r_3 = r_0 = 1$ donc $(r_n)_{n \in \mathbb{N}}$ est 3-périodique et comme $126 = 3 \times 42$, on a $r_{126} = r_0 = 1$.
- Pour $a = 5$, on appelle $(s_n)_{n \in \mathbb{N}}$ la suite des restes. Avec $5^4 = 625 = 48 \times 13 + 1$, on trouve $s_4 = s_0 = 1$ donc $(s_n)_{n \in \mathbb{N}}$ est 4-périodique et comme $126 = 4 \times 31 + 2$, on a $s_{126} = s_2 = 12$.

On a alors $3^{126} = 13q + 1$ et $5^{126} = 13q' + 12$ donc $3^{126} + 5^{126} = 13q + 1 + 13q' + 12 = 13(q + q' + 1) = 13Q$ avec $Q = q + q' + 1$ entier, donc :

$$3^{126} + 5^{126} \text{ est divisible par } 13.$$

Remarque : Evidemment, cet exercice va beaucoup plus vite avec les congruences !

Exercice 13

On sait qu'un sous-anneau est un sous-groupe pour l'addition et que les sous-groupes \mathbb{Z} sont de la forme $n\mathbb{Z}$. De plus, un sous-anneau de \mathbb{Z} doit contenir 1. Or, $n\mathbb{Z}$ e contient 1 que si $n = 1$ donc :

$$\mathbb{Z} \text{ est le seul sous-anneau de } \mathbb{Z}.$$

Exercice 14

$$1) \forall k \in \llbracket 1; p-1 \rrbracket, \text{ on a } \binom{p}{k} = \frac{p!}{k!(p-k)!}, \text{ soit } p! = k!(p-k)! \binom{p}{k}.$$

$$\text{Or, } \binom{p}{k} \text{ est entier donc } k!(p-k)! \binom{p}{k} \text{ aussi et comme } p \text{ divise } p!, \text{ il divise } k!(p-k)! \binom{p}{k}.$$

Mais $k!(p-k)! = 1 \times 2 \times \dots \times k \times 1 \times 2 \times \dots \times (p-k)$ si p , qui est premier divise $k!(p-k)!$, il diviserait l'un ou l'autre des facteurs de $k!(p-k)!$ (c'est une conséquence directe du théorème de Gauss).

Or, $0 < k < p$ donc $0 < p-k < p$, ce qui veut dire que tous les facteurs de $k!(p-k)!$ donnés plus haut sont strictement inférieurs à p et donc p ne peut en diviser aucun. Ainsi, p ne divise pas $k!(p-k)!$.

Alors, par le théorème de Gauss, on peut conclure que :

$$\binom{p}{k} \text{ est divisible par } p.$$

2) Montrons par récurrence sur n que $\forall n \in \mathbb{N}^*$, $n^p - n$ est divisible par p .

Initialisation : Pour $n = 1$, on a $n^p - n = 1^p - 1 = 0$ et p divise 0 donc la propriété est vraie.

Hérédité : Supposons la propriété vraie au rang n .

On veut prouver que p divise $(n+1)^p - (n+1)$.

On a :

$$(n+1)^p - (n+1) = \sum_{k=0}^p \binom{p}{k} n^k - n - 1 = 1 + \sum_{k=1}^{p-1} \binom{p}{k} n^k + n^p - n - 1 = \sum_{k=1}^{p-1} \binom{p}{k} n^k + n^p - n.$$

Or, d'après la question 1, p divise tous les $\binom{p}{k}$ pour $1 \leq k \leq p-1$ donc p divise $\sum_{k=1}^{p-1} \binom{p}{k} n^k$.

De plus, par hypothèse de récurrence, p divise $n^p - n$ donc p divise $(n+1)^p - (n+1)$ et la propriété est vraie au rang $n+1$.

Ainsi, la propriété est initialisée et héréditaire donc elle est vraie $\forall n \in \mathbb{N}^*$.

