Feuille d'exercices - Chapitre 18.

Vrai ou Faux :

1. L'ensemble des racines complexes de -1 est un groupe pour la multiplication.
2. L'ensemble des fonctions $\mathscr{C}^\infty$ de $[\,0\,;1\,]$ dans $\mathbb{R}$ est un groupe pour l'addition.
3. L'ensemble vide est un sous-groupe de $\mathbb{Z}$.
4. Le seul sous-groupe de $\mathbb{Z}$ contenant 1 est $\mathbb{Z}$.
5. Le seul sous-groupe de $\mathbb{Z}$ contenant 4 est $4\mathbb{Z}$.
6. Un groupe fini est abélien.
7. Un groupe d'ordre 4 est cyclique.
8. Un groupe d'ordre 7 est cyclique.
9. Un groupe cyclique a un cardinal premier.
10. La valeur absolue est un morphisme de groupes de $(\mathbb{R}^*,\times)$ dans $(\mathbb{R}_+^*,\times)$.
11. La fonction $x\mapsto 2022\ln(x)$ est un morphisme de groupes de $(\mathbb{R}_+^*,\times)$ dans $(\mathbb{R}^*,\times)$.
12. L'image d'un morphisme de groupes est un sous-groupe du groupe d'arrivée.
13. L'image d'un élément d'ordre n par un morphisme de groupes est un élément d'ordre n.
14. Pour tout élément x d'un anneau A, $(-1_A)\times x$ est le symétrique de x pour l'addition.
15. Les éléments non nuls d'un anneau intègre sont inversibles.
16. La conjugaison est un morphisme de corps de $\mathbb{C}$ dans $\mathbb{C}$.
17. L'application partie réelle est un morphisme de corps de $\mathbb{C}$ dans $\mathbb{R}$.
18. L'application $x\mapsto -x$ est un morphisme de corps de $\mathbb{R}$ dans $\mathbb{R}$.

1 Lois de composition internes

Exercice 1 : ✪ Soit E muni d'une loi de composition associative et commutative notée multiplicativement. Soit $(x,y)\in E^2$. On suppose que xy est symétrisable. Montrer que x et y le sont aussi.

Correction : Soit $z=(xy)^{-1}$. Alors $(xy)*z=z*(xy)=e$ (le neutre). La loi étant associative, $x*(yz)=e$ donc x est symétrisable à gauche donc est symétrisable puisque la loi est commutative. Par symétrie des rôles (x et y jouent le même rôle puisque la loi est commutative), y est symétrisable.

Exercice 2 : ✪ Soit E un ensemble non vide muni d'une loi de composition interne $*$. Un élément x de E est dit idempotent si $x*x=x$.

1. Montrer que si tout élément de E est régulier et si $*$ est distributive par rapport à elle-même, alors tout élément de E est idempotent.
2. Montrer que si tout élément de E est régulier et si $*$ est associative, alors E admet au plus un élément idempotent.

Correction :

1. Supposons donc que tout élément de E soit régulier que $*$ soit distributive par rapport à elle-même. Soit $x\in E$. $*$ étant distributive par rapport à elle-même, $x*(x*x)=(x*x)*(x*x)$ et $(x*x)$ est régulier donc $x=x*x$, x est idempotent.
2. Supposons que tout élément de E soit régulier et que $*$ soit associative. Supposons que E admette deux éléments idempotents x et y. On a donc : $x*y=(x*x)*y$ et la loi est associative donc $x*y=x*(x*y)$. x est régulier donc $y=x*y$. De même, $x*y=x*(y*y)=(x*y)*y$ et y est régulier donc $x=x*y$ donc $x=y$: il y a au plus un élément régulier.

Exercice 3 : ✪ On munit l'ensemble $\mathbb{Q}^2$ d'une loi définie par $(x_1,y_1)\otimes(x_2,y_2)=(x_1x_2,y_1x_2+y_2)$ pour tous couples (x_1,y_1) et (x_2,y_2) de $\mathbb{Q}^2$.

1. La loi $\otimes$ est-elle commutative ?
2. Montrer que $\otimes$ est associative et admet un élément neutre.
3. Étudier l'existence de symétriques.

Correction :

1. Non, elle n'est pas commutative puisque $(1,1)\otimes(0,0)=(0,0)$ et $(0,0)*(1,1)=(0,1)$.
2. Soient $(x_1,y_1),(x_2,y_2)$ et (x_3,y_3) trois éléments de $\mathbb{Q}^2$. Tout d'abord :

$$\begin{aligned}(x_1,y_1)\otimes((x_2,y_2)\otimes(x_3,y_3)) &= (x_1,y_1)\otimes(x_2x_3,y_2x_3+y_3)\\ &= (x_1x_2x_3,y_1(x_2x_3)+y_2x_3+y_3)\\ &= (x_1x_2x_3,y_1x_2x_3+y_2x_3+y_3)\end{aligned}$$

D'autre part :

$$\begin{aligned}((x_1,y_1)\otimes(x_2,y_2))\otimes(x_3,y_3) &= (x_1x_2,y_1x_2+y_2)\otimes(x_3,y_3)\\ &= (x_1x_2x_3,(y_1x_2+y_2)x_3+y_3)\\ &= (x_1x_2x_3,y_1x_2x_3+y_2x_3+y_3)\end{aligned}$$

La loi est donc bien associative. Soit $(a,b)\in\mathbb{Q}^2$.

$$\begin{aligned}(a,b)\text{ est un élément neutre} &\iff \forall(x,y)\in\mathbb{Q}^2,(x,y)\otimes(a,b)=(a,b)\otimes(x,y)=(x,y)\\ &\iff \forall(x,y)\in\mathbb{Q}^2,(xa,ay+b)=(ax,bx+y)=(x,y)\\ &\iff a=1 \quad\text{et}\quad \forall(x,y)\in\mathbb{Q}^2,ay+b=bx+y=y\\ &\iff a=0 \quad\text{et}\quad b=1\end{aligned}$$

$(0,1)$ est donc l'unique élément neutre (on peut aussi raisonner par analyse synthèse si on n'est pas à l'aise avec les équivalences).

3. Soit $(x,y)\in\mathbb{Q}^2$. Soit $(a,b)\in\mathbb{Q}^2$.

$$\begin{aligned}(a,b)\text{ est le symétrique de }(x,y) &\iff (x,y)\otimes(a,b)=(a,b)\otimes(x,y)=(1,0)\\ &\iff (xa,ay+b)=(ax,bx+y)=(1,0)\\ &\iff x\neq 0 \quad\text{et}\quad a=\frac{1}{x} \quad\text{et}\quad \frac{y}{x}+b=bx+y=0\\ &\iff x\neq 0 \quad\text{et}\quad a=\frac{1}{x} \quad\text{et}\quad b=-\frac{y}{x}\end{aligned}$$

Finalement, (x,y) admet un symétrique si et seulement si $x\neq 0$ et alors son symétrique est $\left(\frac{1}{x},-\frac{y}{x}\right)$.

Exercice 4 : ✪ Soit E un ensemble muni d'une loi $*$ associative. On suppose que E admet un élément neutre à gauche (i.e. : $\forall a\in E, e*a=a$) et que pour tout $a\in E$, il existe $b\in E$ tel que $b*a=e$.

1. Soit $a\in E$ tel que $a*a=a$. Montrer que $a=e$.
2. Soient $a\in E$ et $b\in E$ tel que $b*a=e$. Montrer que $a*b=e$.
3. Montrer que e est aussi élément neutre à droite (i.e. : $\forall a\in E, a*e=a$). E est alors muni d'une structure de groupe.

Correction :

1. En composant à gauche par l'élément b tel que $b*a=e$ (un tel élément existe par hypothèse), il vient : $b*(a*a)=b*a$. Or, la loi est associative donc $(b*a)*a=b*a$. Or, $b*a=e$ donc $e*a=b*a$, et $e*a=a$ et $b*a=e$ donc on obtient bien $a=e$.
2. Multiplions à gauche par c, l'élément vérifiant $c*b=e$, et la loi est associative (on peut enlever les parenthèses), ce qui donne : $c*b*a=c$ mais $c*b=e$ donc $e*a=c$. Enfin, $e*a=a$ donc $a=c$ c'est-à-dire que $a*b=e$.

3. Soit $a \in E$. Multiplions $a * e$ à gauche par b, l'élément de E tel que $b * a = e$, ce qui donne $b * a * e = e * e$ (la loi est associative). Or, e est neutre à gauche donc $e * e = e$ si bien que $b * (a * e) = b * a$. En multipliant à gauche par a (et en utilisant l'associativité de la loi), il vient : $(a * b) * (a * e) = (a * b) * a$. Or, $a * b = b * a = e$ si bien que $e*(a*e) = a*e$ et $(a*b)*a = e*a = a$ car e est neutre à gauche. On trouve enfin $a*e = a$ ce qui est le résultat voulu.

Exercice 5 : ✪

1. Soit $\mathbb{N}$ muni des deux lois internes $*$ et $\circ$ définies par $a * b = a + 2b, a \circ b = 2ab$. Sont-elles commutatives, associatives, distributives l'une par rapport à l'autre ?
2. Même question avec $a * b = a + b$ et $a \circ b = ab^2$.
3. Même question avec $a * b = a^2 + b^2$ et $a \circ b = a^2b^2$.

Correction :

1. La loi $\circ$ est commutative, mais $*$ ne l'est pas car $1 * 0 = 1 \neq 2 = 0 * 1$. Soit $(a, b, c) \in \mathbb{N}^3$.

$$\begin{aligned} a \circ (b \circ c) &= a \circ (2bc) \\ &= 2a(2bc) \\ &= 4abc \end{aligned}$$

tandis que

$$\begin{aligned} (a \circ b) \circ c &= (2ab) \circ c \\ &= 2(2ab)c \\ &= 4abc \end{aligned}$$

La loi $\circ$ est donc associative. De plus :

$$\begin{aligned} a * (b * c) &= a * (b + 2c) \\ &= a + 2(b + 2c) \\ &= a + 2b + 4c \end{aligned}$$

et

$$\begin{aligned} (a * b) * c &= (a + 2b) * c \\ &= a + 2b + 2c \end{aligned}$$

Attention, dire qu'on n'obtient pas la même chose est faux et insuffisant : par exemple, pour $a = b = c = 0$, on obtient la même chose, il faut un contre-exemple explicite. En remarque que, si $a = b = c = 1$, les deux quantités sont différentes : la loi $*$ n'est pas associative. Enfin, on a d'une part

$$\begin{aligned} a * (b \circ c) &= a * (2bc) \\ &= a + 2(2bc) \\ &= a + 4bc \end{aligned}$$

et

$$\begin{aligned} (a * b) \circ (a * c) &= (a + 2b) \circ (a + 2c) \\ &= 2(a + 2b)(a + 2c) \\ &= 2a^2 + 4ab + 4ac + 8bc \end{aligned}$$

Idem, il faut un contre-exemple explicite : avec $a = b = c = 1$, on trouve des résultats distincts : la loi $*$ n'est pas distributive par rapport à $\circ$. De plus :

$$\begin{aligned} a \circ (b * c) &= a \circ (b + 2c) \\ &= 2a(b + 2c) \\ &= 2ab + 4ac \end{aligned}$$

et

$$\begin{aligned} (a \circ b) * (a \circ c) &= (2ab) * (2ac) \\ &= 2ab + 2(2ac) \\ &= 2ab + 4ac \end{aligned}$$

La loi $\circ$ est distributive par rapport à la loi $*$.

2. La loi $*$ n'est rien d'autre que la somme, qui est donc commutative et associative. La loi $\circ$ n'est pas commutative car $1 \circ 2 = 4 \neq 2 \circ 1 = 2$. Soit $(a, b, c) \in \mathbb{N}^3$.

$$\begin{aligned} a \circ (b \circ c) &= a \circ (bc^2) \\ &= a(bc^2)^2 \\ &= ab^2c^4 \end{aligned}$$

tandis que

$$\begin{aligned} (a \circ b) \circ c &= (ab^2) \circ c \\ &= (ab^2)c^2 \\ &= ab^2c^2 \end{aligned}$$

Là aussi, il faut un contre-exemple explicite, par exemple $a = b = 1$ et $c = 2$: la loi $\circ$ n'est pas associative. Enfin, on a d'une part

$$\begin{aligned} a * (b \circ c) &= a * (bc^2) \\ &= a + bc^2 \end{aligned}$$

et

$$\begin{aligned} (a * b) \circ (a * c) &= (a + b) \circ (a + c) \\ &= (a + b)(a + c)^2 \end{aligned}$$

Là aussi, un contre-explicite : $a = 1, b = 0, c = 2$, la loi $*$ n'est pas distributive par rapport à la loi $\circ$. De plus :

$$\begin{aligned} a \circ (b * c) &= a \circ (b + c) \\ &= 2a(b + c) \\ &= 2ab + 2ac \end{aligned}$$

et

$$\begin{aligned} (a \circ b) * (a \circ c) &= (ab^2) * (ac^2) \\ &= ab^2 + ac^2 \end{aligned}$$

En prenant $a = 1, b = c = 3$, on trouve que la loi $\circ$ n'est pas distributive par rapport à la loi $*$.

3. Les lois $*$ et $\circ$ sont commutatives. Soit $(a, b, c) \in \mathbb{N}^3$.

$$\begin{aligned} a \circ (b \circ c) &= a \circ (b^2c^2) \\ &= a^2(b^2c^2)^2 \\ &= a^2b^4c^4 \end{aligned}$$

tandis que

$$\begin{aligned}(a\circ b)\circ c &= (a^2b^2)\circ c\\ &= (a^2b^2)^2c^2\\ &= a^4b^4c^2\end{aligned}$$

En prenant $a=b=1$ et $c=2$, on a un résultat distinct, la loi $\circ$ n'est pas associative. De plus,

$$\begin{aligned}a*(b*c) &= a*(b^2+c^2)\\ &= a^2+(b^2+c^2)^2\\ &= a^2+b^4+2b^2c^2+c^4\end{aligned}$$

tandis que

$$\begin{aligned}(a*b)*c &= (a^2+b^2)*c\\ &= (a^2+b^2)^2+c^2\\ &= a^4+2a^2b^2+b^4+c^2\end{aligned}$$

En prenant $a=b=0$ et $c=2$, on trouve que la loi $*$ n'est pas associative. Enfin, on a d'une part

$$\begin{aligned}a*(b\circ c) &= a*(b^2c^2)\\ &= a^2+(b^2c^2)^2\\ &= a^2+b^4c^4\end{aligned}$$

et

$$\begin{aligned}(a*b)\circ(a*c) &= (a^2+b^2)\circ(a^2+c^2)\\ &= (a^2+b^2)^2(a^2+c^2)^2\end{aligned}$$

En prenant $a=2$ et $b=c=0$, on trouve des résultats distincts : la loi $*$ n'est pas distributive par rapport à la loi $\circ$. Finalement :

$$\begin{aligned}a\circ(b*c) &= a\circ(b^2+c^2)\\ &= a^2(b^2+c^2)^2\\ &= a^2(b^4+2b^2c^2+c^4)\\ &= a^2b^4+2a^2b^2c^2+a^2c^4\end{aligned}$$

et

$$\begin{aligned}(a\circ b)*(a\circ c) &= (a^2b^2)*(a^2c^2)\\ &= (a^2b^2)^2+(a^2c^2)\\ &= a^4b^4+a^4c^4\end{aligned}$$

En prenant $b=0$ et $a=c=2$, on trouve que $\circ$ n'est pas non plus distributive par rapport à $*$.

Exercice 6 : ✪ Pour tous réels x et y, on pose $x\star y = x+y+xy^2$.

1. La loi $\star$ est-elle commutative ? associative ?
2. Montrer que $\star$ admet un élément neutre.
3. Montrer qu'aucun élément de $\mathbb{R}^*$ n'admet d'inverse pour $\star$.
4. Résoudre l'équation $x\star x = 3$.

Correction :

1. Elle n'est pas commutative car $1 \star 2 = 7$ et $2 \star 1 = 5$. Soit $(a, b, c) \in \mathbb{R}^3$.

$$\begin{aligned} a \star (b \star c) &= a \star (b + c + bc^2) \\ &= a + b + c + bc^2 + a(b + c + bc^2)^2 \end{aligned}$$

tandis que

$$\begin{aligned} (a \star b) \star c &= (a + b + ab^2) \star c \\ &= a + b + ab^2 + c + (a + b + ab^2)c^2 \end{aligned}$$

En prenant $a = 1, b = 1$ et $c = 2$, on trouve que la loi n'est pas associative.

2. Soit $e \in \mathbb{R}$.

$$\begin{aligned} e \text{ est un élément neutre} &\iff \forall x \in \mathbb{R}, x \star e = e \star x = x \\ &\iff \forall x \in \mathbb{R}, x + e + xe^2 = e + x + ex^2 = x \\ &\iff \forall x \in \mathbb{R}, e + xe^2 = e + ex^2 = 0 \end{aligned}$$

0 est solution évidente donc 0 est élément neutre (et c'est même le seul d'après le cours).

3. Soit $x \in \mathbb{R}^*$. Supposons que x admettre un inverse noté y. Alors $x \star y = y \star x = 0$ (le neutre) si bien que

$$x + y + xy^2 = y + x + yx^2 = 0$$

Dès lors, $x + y = -xy^2 = -yx^2$ donc, en particulier, $xy^2 = yx^2$. Puisque x est non nul, $y^2 = yx$. Si y est nul, alors y est le neutre donc $x \star y = x \neq 0$, ce qui est exclu, donc on peut simplifier par y si bien que $y = x$: x est son propre inverse, ce qui est absurde car $x \star x = 2x + x^3 = x(x^2 + 2)$ qui est non nul car $x \neq 0$ et $x^2 + 2 > 0$. En conclusion, un réel non nul n'est pas inversible.

4. Soit $x \in \mathbb{R}$.

$$\begin{aligned} x \star x = 3 &\iff 2x + x^3 = 3 \\ &\iff x^3 + 2x - 3 = 0 \end{aligned}$$

$x = 1$ est solution évidente : on peut donc factoriser le membre de gauche par $x - 1$: il existe (a, b, c) tel que

$$x^3 + 2x - 3 = (x - 1)(ax^2 + bx + c) = ax^3 + x^2(b - a) + x(c - b) - c$$

On trouve que $a = 1, c = 3$ et $b = 1$. Dès lors,

$$\begin{aligned} x \star x = 3 &\iff (x - 1)(x^2 + x + 3) = 0 \\ &\iff x = 1 \quad \text{ou} \quad x^2 + x + 3 = 0 \end{aligned}$$

Or, l'équation $x^2 + x + 3 = 0$ n'a pas de solution car son discriminant est strictement négatif. En conclusion, la seule solution de l'équation $x \star x = 3$ est $x = 1$.

Exercice 7 : ✪✪ Soit $*$ la loi de composition interne sur $\mathbb{Q}$ définie par $a * b = a + b + ab$.

1. Associativité, commutativité, élément neutre de $*$?
2. $*$ est-elle distributive par rapport à l'addition et la multiplication dans $\mathbb{Q}$?
3. Quels sont les éléments inversibles, réguliers, idempotents (i.e. les éléments x tels que $x * x = x$) ?
4. Résoudre les équations $7 * x = 3$, $x * (-5) = -1$, $x * x = 2$, $x * x = 3$.
5. Calculer, pour a inversible et $n \in \mathbb{Z}$, a^n (il s'agit des puissances au sens de la loi $*$).

Correction :

1. La loi $*$ est évidemment commutative. Soit $(a, b, c) \in \mathbb{Q}^3$. D'une part,

$$\begin{aligned} a * (b * c) &= a * (b + c + bc) \\ &= a + b + c + bc + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc \end{aligned}$$

et d'autre part,

$$\begin{aligned}(a*b)*c &= (a+b+ab)*c\\ &= a+b+ab+c+(a+b+ab)c\\ &= a+b+ab+c+ac+bc+abc\\ &= a*(b*c)\end{aligned}$$

La loi $*$ est donc associative. De plus, il est immédiat que 0 est un élément neutre car, pour tout $a \in \mathbb{Q}$, $a*0 = 0*a = a$.

2. Soit $(a,b,c) \in \mathbb{Q}^3$. D'une part :

$$\begin{aligned}a*(b+c) &= a+b+c+a(b+c)\\ &= a+b+c+ab+ac\end{aligned}$$

et, d'autre part :

$$(a*b)+(a*c) = a+b+ab+a+c+ac$$

En prenant $a = 1$ et $b = c = 0$, on voit que la loi $*$ n'est pas distributive par rapport à la somme. De plus :

$$a*(b\times c) = a+bc+abc$$

tandis que

$$(a*b)\times(a*c) = (a+b+ab)\times(a+c+ac)$$

En prenant $a = b = c = 1$, on voit que $*$ n'est pas distributive par rapport au produit.

3. Rappelons que 0 est le neutre de $*$ et que $*$ est commutative : dès lors, un élément est inversible si et seulement s'il est inversible à gauche ou à droite. Soit $x \in \mathbb{Q}$.

$$\begin{aligned}x \text{ est inversible} &\iff \exists y \in \mathbb{Q}, x*y = 0\\ &\iff \exists y \in \mathbb{Q}, x+y+xy = 0\\ &\iff \exists y \in \mathbb{Q}, y(1+x) = -x\end{aligned}$$

Il y a deux cas de figure : si $x \neq -1$, alors x est inversible et $y = \dfrac{-x}{1+x}$ est l'inverse de x, tandis que si $x = -1$, alors $x*y = -1+y-y = -1 \neq 0$ pour tout y, c'est-à-dire que -1 n'est pas inversible.

Cherchons à présent les éléments réguliers (idem, un élément est régulier si et seulement s'il est régulier à gauche ou à droite). On pourrait raisonner par équivalences, mais entre les équivalences et les implications, cela donnerait une rédaction délicate. Soit $x \in \mathbb{Q}$ et soit $(y,z) \in \mathbb{Q}^2$ tel que $y*x = z*x$. Alors $y+x+yx = z+x+zx$ donc $y(1+x) = z(1+x)$. Si $x \neq -1$, on peut simplifier par $1+x$ si bien que $y = z$: tout élément différent de -1 est régulier. De plus, d'après la question précédente, pour tous y et z, $y*(-1) = z*(-1) = -1$ donc -1 n'est pas régulier. Enfin, $x*x = 2x+x^2$. Par conséquent, x est idempotent si et seulement si $2x+x^2 = x$ si et seulement si $x+x^2 = x(x+1) = 0$. On en déduit que 0 et -1 sont les seuls éléments idempotents.

4. Soit $x \in \mathbb{Q}$.

$$\begin{aligned}7*x = 3 &\iff 7+x+7x = 3\\ &\iff 8x = -4\\ &\iff x = -1/2\end{aligned}$$

puis :

$$\begin{aligned}x*(-5) = -1 &\iff x-5-5x = -1\\ &\iff -4x = 4\\ &\iff x = -1\end{aligned}$$

puis :

$$\begin{aligned} x * x = 2 &\iff x + x + x^2 = 2 \\ &\iff x^2 + 2x - 2 = 0 \\ &\iff x = \frac{-2 \pm \sqrt{12}}{2} = -1 \pm \sqrt{3} \end{aligned}$$

Or, on est sur $\mathbb{Q}$ et $\sqrt{3}$ est irrationnel : l'équation n'a pas de solution. Enfin,

$$\begin{aligned} x * x = 3 &\iff x + x + x^2 = 3 \\ &\iff x^2 + 2x - 3 = 0 \\ &\iff x = 1 \quad \text{ou} \quad x = -3 \end{aligned}$$

5. On demande donc, si $n \geq 1$ (nous verrons les autres cas plus tard), de donner $\underbrace{a * \cdots * a}_{n \text{ fois}}$ (cette notation a du sens car la loi est associative). On a tout d'abord $a^1 = a$ puis $a^2 = a * a = 2a + a \times a$ (dans cette question, nous gardons la notation puissance pour la loi $*$, quand nous aurons un vrai produit, nous l'écrirons avec la loi $\times$ pour qu'il n'y ait aucune confusion). Ensuite,

$$\begin{aligned} a^3 &= a^2 * a \\ &= a^2 + a + a^2 \times a \\ &= (a + a + a \times a) + a + (a + a + a \times a) \times a \\ &= 3a + 3a \times a + a \times a \times a \end{aligned}$$

On reconnaît un binôme de Newton tronqué, à savoir $(a+1) \times \cdots \times (a+1)$ (n fois), mais il manque le 1. Prouvons donc que

$$a^n = \underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} - 1$$

Prouvons ce résultat par récurrence sur $n \geq 1$. Le résultat est vérifié aux rangs $1, 2, 3$. Soit $n \geq 3$. Supposons qu'il soit vrai au rang n et prouvons qu'il est toujours vrai au rang $n+1$. $a^{n+1} = a^n * a = a^n + a + a^n \times a$. Par hypothèse de récurrence :

$$\begin{aligned} a^{n+1} &= \left(\underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} - 1 \right) + a + \left(\underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} - 1 \right) \times a \\ &= \underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} - 1 + a + \underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} \times a - a \\ &= \underbrace{(a+1) \times \cdots \times (a+1)}_{n \text{ fois}} \times (1 + a) - 1 \\ &= \underbrace{(a+1) \times \cdots \times (a+1)}_{n+1 \text{ fois}} - 1 \end{aligned}$$

ce qui clôt la récurrence. Pour $n = 0$, a^0 est, par convention, égal au neutre, c'est-à-dire à 0 ici. Enfin, si $n < 0$, par définition, $a^n = \left(a^{-1}\right)^{-n}$ (toujours au sens de la loi $*$). En utilisant l'expression de l'inverse d'un élément (en particulier, $a^{-1} + 1 = 1/(1+a)$) et l'expression d'une puissance positive (car $-n > 0$), on trouve finalement :

$$a^n = \underbrace{\left(\frac{1}{1+a}\right) \times \cdots \times \left(\frac{1}{1+a}\right)}_{-n \text{ fois}}$$

Exercice 8 - L'addition parallèle : ✪✪ Il est bien connu (demandez à votre professeur de physique préféré) en électricité que si on met deux résistances R_1 et R_2 en parallèle, la résistance équivalente obtenue est $\dfrac{R_1 R_2}{R_1 + R_2}$. On se propose

dans cet exercice d'étudier quelques aspects de cette loi de composition interne.

On note // la loi de composition interne définie sur $\mathbb{R}_+^*$ par :

$$a//b = \frac{ab}{a+b}$$

1. Montrer que c'est bien une loi de composition interne.
2. Montrer qu'elle est associative et commutative.
3. Montrer que // n'a pas d'élément neutre.
4. Soit $x > 0$. Montrer que

$$\inf_{\substack{(y,z)\in\mathbb{R}^2 \\ y+z=x}} \left(ay^2 + bz^2\right) = (a//b)x^2$$

   Cette borne inférieure est-elle atteinte ? Si oui, en quel(s) (y, z) ?
5. ✪✪✪ Soient $n \geq 1$, $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_n)$ deux n-uplets de réels strictement positifs. Montrer que :

$$\sum_{i=1}^{n}(a_i//b_i) \leq \left(\sum_{i=1}^{n} a_i\right) // \left(\sum_{i=1}^{n} b_i\right)$$

   On pourra raisonner par récurrence prouver le résultat pour $n = 1$ et $n = 2$ (et s'armer de patience...).
6. Question bonus : donner une interprétation physique des résultats prouvés dans cet exercice.

Correction :

1. Immédiat : si a et b sont strictement positifs, $a//b$ l'est aussi.
2. La commutativité est évidente. Soit $(a, b, c) \in \left(\mathbb{R}_+^*\right)^3$. D'une part,

$$\begin{aligned} a//(b//c) &= a// \left(\frac{bc}{b+c}\right) \\ &= \frac{a \times \dfrac{bc}{b+c}}{a + \dfrac{bc}{b+c}} \\ &= \frac{abc}{b+c} \times \frac{b+c}{ab+ac+bc} \\ &= \frac{abc}{ab+ac+bc} \end{aligned}$$

   et d'autre part

$$\begin{aligned} (a//b)//c &= \left(\frac{ab}{a+b}\right)//c \\ &= \frac{\dfrac{ab}{a+b} \times c}{\dfrac{ab}{a+b} + c} \\ &= \frac{abc}{a+b} \times \frac{a+b}{ab+ac+bc} \\ &= \frac{abc}{ab+ac+bc} \end{aligned}$$

   La loi est bien associative.
3. Supposons par l'absurde que // admette un élément neutre x. Alors, pour tout $a > 0$, $a//x = a$ donc

$$\frac{ax}{a+x} = a$$

   Ainsi, $ax = a(a + x)$ donc $a^2 = 0$ ce qui est absurde car $a > 0$. Finalement, il n'y a pas d'élément neutre.

4. Soit $(y,z) \in \mathbb{R}^2$ tel que $y+z=x$. L'astuce est de voir qu'il n'y a en fait qu'une variable parmi y et z, l'autre est donnée automatiquement. Plus précisément, $z=x-y$. Par conséquent, on demande de prouver que :

$$\inf_{y\in\mathbb{R}} \left(ay^2+b(x-y)^2\right) = (a//b)x^2$$

et cela ne pose plus de difficulté : posons $\varphi(y)=ay^2+b(x-y)^2$. Alors

$$\varphi(y) = (a+b)y^2 - 2bxy + bx^2$$

On pourrait donner le tableau de variations de φ mais on reconnaît un trinôme du second degré de coefficient dominant strictement positif : on sait qu'il y a un minimum atteint en « -b/2a » (avec les notations ax^2+bx+c, pas les a et b de l'énoncé) donc, ici, en

$$\frac{2bx}{2(a+b)} = \frac{bx}{a+b}$$

et celui-ci vaut :

$$\begin{aligned}
\varphi\left(\frac{bx}{a+b}\right) &= (a+b)\left(\frac{bx}{a+b}\right)^2 - 2bx\times\frac{bx}{a+b} + bx^2 \\
&= \frac{b^2x^2}{a+b} - \frac{2b^2x^2}{a+b} + bx^2 \\
&= \frac{-b^2x^2}{a+b} + \frac{bx^2(a+b)}{a+b} \\
&= \frac{abx^2}{a+b} \\
&= (a//b)x^2
\end{aligned}$$

Il est de plus atteint uniquement pour $y=bx/(a+b)$ et $z=x-y=ax/(a+b)$.

5. Prouvons le résultat par récurrence sur n. Il n'y a rien à prouver pour $n=1$ puisque les deux termes de l'inégalité sont égaux à $a_1//b_1$. Prouvons le résultat pour $n=2$. Soient a_1,a_2,b_1,b_2 des réels strictement positifs. Notons

$$D = (a_1+a_2)//(b_1+b_2) - (a_1//b_1 + a_2//b_2)$$

Alors :

$$\begin{aligned}
D &= \frac{(a_1+a_2)(b_1+b_2)}{a_1+a_2+b_1+b_2} - \frac{a_1b_1}{a_1+b_1} - \frac{a_2b_2}{a_2+b_2} \\
&= \frac{(a_1+a_2)(b_1+b_2)(a_1+b_1)(a_2+b_2) - a_1b_1(a_1+a_2+b_1+b_2)(a_2+b_2) - a_2b_2(a_1+a_2+b_1+b_2)(a_1+b_1)}{(a_1+a_2+b_1+b_2)(a_1+b_1)(a_2+b_2)}
\end{aligned}$$

En faisant le calcul (c'est long...) on trouve que

$$\begin{aligned}
D &= \frac{{a_1}^2{b_2}^2 + {a_2}^2{b_1}^2 - 2a_1a_2b_1b_2}{(a_1+a_2+b_1+b_2)(a_1+b_1)(a_2+b_2)} \\
&= \frac{(a_1b_2+a_2b_1)^2}{(a_1+a_2+b_1+b_2)(a_1+b_1)(a_2+b_2)} \\
&\geq 0
\end{aligned}$$

si bien que

$$(a_1+a_2)//(b_1+b_2) \geq a_1//b_1 + a_2//b_2$$

Le résultat est donc vrai pour $n=2$. Soit $n\geq 1$, supposons le résultat vrai au rang n et prouvons qu'il est encore vrai au rang $n+1$. Soient donc $(a_1,\dots,a_{n+1})$ et $(b_1,\dots,b_{n+1})$ des familles de réels strictement positifs. Tout d'abord, notons

$$S_n = \sum_{i=1}^{n} a_i \qquad \text{et} \qquad T_n = \sum_{i=1}^{n} b_i$$

On en déduit que

$$\left(\sum_{i=1}^{n+1} a_i\right) // \left(\sum_{i=1}^{n+1} b_i\right) = (S_n + a_{n+1})//(T_n + b_{n+1})$$

D'après le cas $n = 2$, on en déduit que :

$$\left(\sum_{i=1}^{n+1} a_i\right) // \left(\sum_{i=1}^{n+1} b_i\right) \geq S_n//T_n + a_{n+1}//b_{n+1} = \left(\sum_{i=1}^{n} a_i\right) // \left(\sum_{i=1}^{n} b_i\right) + a_{n+1}//b_{n+1}$$

Il suffit d'appliquer l'hypothèse de récurrence pour conclure.

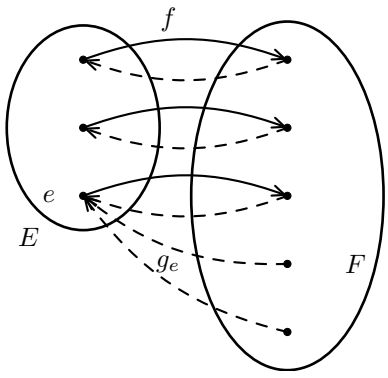
6. Pour la question 1 : la résistance équivalente est strictement positive. Pour la question 2 : la commutativité prouve que l'ordre des deux résistances ne change rien, et l'associativité prouve que si on met A et B en parallèle de C ou A en parallèle de B et C, cela ne change rien. La question 3 prouve qu'il n'est pas possible de mettre en parallèle d'une résistance R une autre résistance R' de manière à ce que la résistance totale soit encore R (i.e. soit inchangée) : quand on met une deuxième résistance en parallèle, cela change la résistance totale. Pour la question 4, on se souvient que $P = UI$ et $U = RI$ donc $P = RI^2$: si on a deux résistances R_1 et R_2 en parallèle et une intensité de I, d'après la loi des noeuds, il y a une intensité I_1 qui va chez R_1 et une intensité I_2 qui va chez R_2, avec $I_1 + I_2 = I$, et la répartition qui minimise la puissance est obtenue avec $I_1 = R_2 I/(R_1 + R_2)$, et cette puissance minimale est la même que celle obtenue avec la résistance équivalente $R_1//R_2$ (et l'intensité I). Enfin, pour la question 5, cela prouve que si on a des résistances $R_1, \dots, R_n$ et $\rho_1, \dots, \rho_n$, on a une résistance plus faible en mettant chaque R_i avec chaque ρ_i en parallèle, puis à mettre ces couples en séries, qu'en mettant toutes les R_i en série, les ρ_i en série également, et enfin en mettant ces deux familles de n résistances en série en parallèle.

Exercice 9 : ✪✪ Soient E et F deux ensembles non vides. Soit $f : E \to F$.

1. On suppose dans cette question que E n'est pas un singleton. Montrer que si f est injective mais non surjective, alors f admet plusieurs symétriques à gauche (pour la composition). Admet-elle un symétrique à droite ?
2. Montrer que si f est surjective mais non injective, alors f admet plusieurs symétriques à droite. Admet-elle un symétrique à gauche ?

Correction :

1. Faisons un dessin :



Si $e \in E$, notons g_e l'application définie comme suit :

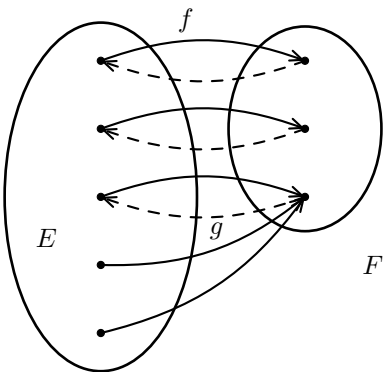
$$g_e : \begin{cases} F & \to & E \\ y & \mapsto & \begin{cases} f^{-1}(y) & \text{si } y \in f(E) \\ e & \text{sinon} \end{cases} \end{cases}$$

On prouve comme dans l'exercice 43 du chapitre 3 que $g_e \circ f = \mathrm{Id}_E$: g_e est un inverse de f à gauche. Puisque E n'est pas un singleton, il admet plusieurs éléments e donc f admet plusieurs inverses à gauche. Cependant, f n'admet

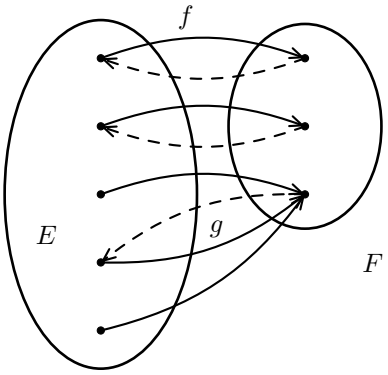
aucun inverse à droite car il n'existe aucune fonction $g : F \to E$ telle que $f \circ g = \mathrm{Id}_F$: en effet, si on prend $y \in F$ non atteint par f, il n'existe aucun $x \in E$ tel que $f(x) = y$ donc il n'existe aucune fonction g telle que $f(g(y)) = y$: il n'existe aucune fonction g telle que $f \circ g = \mathrm{Id}_F$, f n'est pas inversible à droite.

2. Soit

$$g : \begin{cases} F & \to & E \\ y & \mapsto & \textbf{un} \text{ antécédent de } y \text{ par } f \end{cases}$$



On prouve de même que dans l'exercice 43 du chapitre 3 que $f \circ g = \mathrm{Id}_F$ donc g est un inverse à droite de f. Il y a plusieurs inverses à droite car il suffit de changer la valeur de g en un y qui admet plusieurs antécédents, et donc en envoyant y sur un autre de ses antécédents, on obtient un autre inverse à droite.



Cependant, f n'admet aucun inverse à gauche : en effet, supposons qu'il existe $g : F \to E$ telle que $g \circ f = \mathrm{Id}_E$. Soient $x_1 \neq x_2$ tels que $f(x_1) = f(x_2)$ (possible car f non injective) donc $g \circ f(x_1) = g \circ f(x_2)$ ce qui est absurde car $g(f(x_1)) = x_1$ et $g(f(x_2)) = x_2$.

Exercice 10 : Soit E un ensemble à n éléments.

1. ✪ Dénombrer les lois de composition internes sur E.
2. ✪✪ Dénombrer les lois de composition internes commutatives sur E.
3. ✪✪✪ Dénombrer les lois de composition internes commutatives sur E admettant un élément neutre.

Correction :

1. Une loi de composition interne est une application de E^2 dans E donc un élément de $\left(E^2\right)^E$, ensemble à $(n^2)^n = n^{2n}$ éléments (cf. chapitre précédent, le cardinal de F^E est $\mathrm{card}(F)^{\mathrm{card}(E)}$).
2. Notons $E = \{x_1; \ldots; x_n\}$. Une loi de composition interne commutative est entièrement déterminée par l'image des (x_i, x_j) pour $i \leq j$, les autres sont déduits par commutativité (par exemple, si on connaît l'image de (x_1, x_2), on connaît automatiquement celle de (x_2, x_1)). Soit $(i, j) \in [\![1 ; n]\!]^2$. Il y a n choix possibles pour l'image d e(x_i, x_j) donc le cardinal recherché est (par principe multiplicatif)

$$\begin{aligned} S &= \prod_{i=1}^{n}\prod_{j=i}^{n} n \\ &= \prod_{i=1}^{n} n^{n-i+1} \\ &= \prod_{k=1}^{n} n^{k} \\ &= n^{\sum_{k=1}^{n} k} \\ &= n^{n(n+1)/2} \end{aligned}$$

On peut aussi voir le résultat de la façon suivante : on représente la loi par un tableau, avec, en position (i,j), l'image de (x_i, x_j). Alors il suffit de connaître les éléments au-dessus (au sens large) de la diagonale car la loi est commutative, on déduit les autres par symétrie : il faut connaître $n(n+1)/2$ images, n images possibles pour chaque, et on retrouve le même résultat.

3. Une telle loi est totalement déterminée, pour commencer, par le choix de l'élément neutre : n choix possibles. Notons x_e l'élément neutre. Alors les $x_i * x_e$ sont déjà connus puisqu'ils valent x_i. Par conséquent, comme dans la question précédente, une telle loi est totalement déterminée ensuite par les images des (x_i, x_j) avec $i \leq j$ et i et j distincts de e. Le raisonnement est le même qu'à la question précédente, si ce n'est qu'il faut déterminer n images de moins : $(x_1, x_e), (x_2, x_e) \ldots, (x_e, x_e), (x_e, x_{e+1}), \ldots, (x_e, x_n)$. Il y a donc $n^{n(n+1)/2-n} = n^{n(n-1)/2}$, qu'il ne faut pas oublier de multiplier par n (les n choix possibles pour l'élément neutre). Il y a donc $n^{n(n-1)/2+1}$ telles lois internes.

Exercice 11 : ✪✪✪ Soit E un ensemble fini muni d'une loi de composition interne associative notée multiplicativement. Montrer qu'il existe $x \in E$ tel que $x^2 = x$.

Correction : Soit $a \in E$. Les puissances de a sont en nombre infini alors que E est fini : d'après le principe des tiroirs, il existe une infinité de puissances égales. Soient par exemple n_1 et n_2 avec $n_2 \geq 2n_1$ (c'est possible car il existe une infinité de puissances égales, on prend donc une puissance n_1 quelconque parmi l'infinité de puissances égales, puis une autre supérieure à son double, ce qui est possible puisqu'il y en a une infinité, nous verrons pourquoi il est intéressant d'avoir $n_2 \geq 2n_1$ dans la suite) $a^{n_1} = a^{n_2}$. On cherche un entier k tel qu'en multipliant par a^k, une des deux puissances serait le double de l'autre, i.e. on cherche k tel que $n_2 + k = 2(n_1 + k)$. Alors $k = n_2 - 2n_1$ convient (d'où la nécessité d'avoir $n_2 \geq 2n_1$). Puisque $a^{n_2} = a^{n_1}$ alors $a^{n_2+k} = a^{n_1+k}$ (en multipliant par a^k) mais, par choix de k, on a $n_2 + k = 2(n_1 + k)$ si bien qu'en posant $x = a^{n_1+k}$, on a bien $x^2 = x$.

2 Groupes

2.1 Exemples explicites

Exercice 12 : ✪ Montrer que $\bigcup_{n\in\mathbb{N}^*} \mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$. Est-il égal à $\mathbb{U}$?

Correction : Rappelons (cf. cours) que, pour tout n, $\mathbb{U}_n$ est un sous-groupe de $\mathbb{U}$ (pour la loi $\times$). Attention, une union de sous-groupes n'est pas forcément un sous-groupe ! Notons cet ensemble G. Rappelons qu'un élément est dans G si et seulement s'il existe un $n \in \mathbb{N}^*$ tel que cet élément soit dans $\mathbb{U}_n$. Rappelons également que $\mathbb{U}_n$ est inclus dans $\mathbb{U}_m$ si et seulement si $n|m$.

1. G est une union d'ensembles inclus dans $\mathbb{U}$ donc est inclus dans $\mathbb{U}$.
2. $1 \in \mathbb{U}_1$ donc $1 \in G$: G est non vide.
3. Soient z_1 et z_2 deux éléments de G. Alors il existe n_1 et n_2 dans $\mathbb{N}^*$ tels que $z_1 \in \mathbb{U}_{n_1}$ et $z_2 \in \mathbb{U}_{n_2}$. L'idée est de trouver un même $\mathbb{U}_m$ tel que z_1 et z_2 appartiennent à $\mathbb{U}_m$. Soit $m = n_1 \vee n_2$. Alors n_1 et n_2 divisent m donc $\mathbb{U}_{n_1}$ et $\mathbb{U}_{n_2}$ sont inclus dans $\mathbb{U}_m$ si bien que z_1 et z_2 appartiennent à $\mathbb{U}_m$. Or, $\mathbb{U}_m$ est un groupe (pour la loi $\times$) donc $z_1 \times z_2 \in \mathbb{U}_m$ si bien que $z_1 \times z_2 \in G$: G est stable par produit.
4. Soit $z \in G$. Alors il existe $n \in \mathbb{N}^*$ tel que $z \in \mathbb{U}_n$ qui est un groupe donc $1/z \in \mathbb{U}_n$ et donc $1/z \in G$: G est stable par inverse.

En conclusion, G est un sous-groupe de $\mathbb{U}$ (et donc est un groupe pour la loi $\times$). Cependant, il existe des éléments de $\mathbb{U}$ qui ne sont pas des racines de l'unité, par exemple $e^{i\pi\sqrt{2}}$, cf. exercice 61 du chapitre 7, donc $G \neq \mathbb{U}$.

Exercice 13 : ✪ Soit n un entier naturel impair. On définit sur $\mathbb{R}$ la loi $*$ par :

$$\forall (x,y) \in \mathbb{R}^2, x * y = \sqrt[n]{x^n + y^n}$$

1. Montrer que $(\mathbb{R}, *)$ est un groupe abélien.
2. Soit $\varphi : x \mapsto x^n$. Montrer que φ est un isomorphisme de groupes de $(\mathbb{R}, *)$ dans $(\mathbb{R}, +)$.

Correction :

1. Précisons que, n étant impair, si $x \in \mathbb{R}$, $\sqrt[n]{x}^n = x$ (ce n'est pas vrai si n est pair et x négatif). Le fait que la loi soit interne et commutative est immédiat. Prouvons qu'elle est associative. Soit $(x,y,z) \in \mathbb{R}^2$. D'une part :

$$\begin{aligned} x * (y * z) &= x * \sqrt[n]{y^n + z^n} \\ &= \sqrt[n]{x^n + (\sqrt[n]{y^n + z^n})^n} \\ &= \sqrt[n]{x^n + y^n + z^n} \end{aligned}$$

   et d'autre part

$$\begin{aligned} (x * y) * z &= \sqrt[n]{x^n + y^n} * z \\ &= \sqrt[n]{(\sqrt[n]{x^n + y^n} + z^n)^n} \\ &= \sqrt[n]{x^n + y^n + z^n} \end{aligned}$$

   La loi est bien associative. Il est immédiat que 0 est élément neutre et que, pour tout x, $-x$ est le symétrique de x : $(\mathbb{R}, *)$ est bien un groupe abélien.
2. Soient x et y deux réels.

$$\begin{aligned} \varphi(x * y) &= (x * y)^n \\ &= (\sqrt[n]{x^n + y^n})^n \\ &= x^n + y^n \\ &= \varphi(x) + \varphi(y) \end{aligned}$$

   c'est-à-dire que φ est un morphisme de groupes entre $(\mathbb{R}, *)$ et $(\mathbb{R}, +)$. La bijectivité découle directement du théorème de la bijection.

Exercice 14 : ✪✪ Les ensembles suivants sont-ils des groupes ?

1. L'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ de la forme $x \mapsto ax + b$ avec $(a,b) \in \mathbb{R}^* \times \mathbb{R}$ muni de la composition.
2. $]-1\,;1[$ muni de la loi $\oplus$ définie par $x \oplus y = \dfrac{x+y}{1+xy}$.
3. $\mathbb{R}^2$ muni de la loi $\star$ définie par $(x_1, y_1) \star (x_2, y_2) = (x_1 + x_2, y_1 e^{x_2} + y_2 e^{x_1})$.

Correction :

1. On sait que $S_{\mathbb{R}}$ (l'ensemble des bijections de $\mathbb{R}$ dans $\mathbb{R}$) est un groupe pour la composition. Il suffit donc de prouver que cet ensemble (qu'on notera H) est un sous-groupe de $S_{\mathbb{R}}$.
   - Une fonction affine non constante étant une bijection de $\mathbb{R}$ dans $\mathbb{R}$, G est inclus dans $S_{\mathbb{R}}$.
   - Soient $f_1 : x \mapsto a_1 x + b$ et $f_2 : x \mapsto a_2 x + b_2$ avec a_1 et a_2 non nuls appartenant à G. Alors (attention, il faut examiner la stabilité par la loi du groupe, la composition, pas par le produit !), pour tout $x \in \mathbb{R}$:

$$\begin{aligned} f_1 \circ f_2(x) &= f_1(a_2 x + b_2) \\ &= a_1(a_2 x + b_2) + b_1 \\ &= a_1 a_2 x + a_1 b_1 + b_1 \end{aligned}$$

     et puisque $a_1 a_2 \neq 0$, $f_1 \circ f_2 \in G$: G est stable par composition.

- Soit $f : x \mapsto ax + b \in G$, avec donc $a \neq 0$. Soit $y \in \mathbb{R}$ et soit $x \in \mathbb{R}$ (méthode pour expliciter f^{-1} : résoudre l'équation, d'inconnue x, $f(x) = y$). Alors : $y = f(x) \iff x = \dfrac{y-b}{a}$. En d'autres termes, f^{-1} est la fonction $x \mapsto \dfrac{x}{a} - \dfrac{b}{a}$ (la variable est muette, l'appeler x ou y ne change rien) et puisque $1/a \neq 0$, on a bien $f^{-1} \in G$: G est stable par inverse (inverse au sens de la composition).

En conclusion, G est un sous-groupe de $S_{\mathbb{R}}$ donc est un groupe (pour la composition). Si on ne pense pas à $S_{\mathbb{R}}$, il faut prouver à la main que c'est un groupe donc préciser que la composition est associative, que $\mathrm{Id} : x \mapsto x \in G$ est un élément neutre (à droite et à gauche car la composition n'est pas commutative) et que, comme ci-dessus, tout élément f de G admet un inverse.

2. Dans cet exemple et le suivant, la loi n'est pas une loi connue : il faut tout montrer, on ne peut pas montrer que les ensembles sont des sous-groupes de groupes connus.
   - Prouvons que la loi $\oplus$ est interne, ce qui n'est pas immédiat à première vue. Soit $(x, y) \in]-1\,;1[^2$. Alors $|xy| < 1$ donc $1 + xy > 0$, d'où les équivalences suivantes :

$$\begin{aligned} -1 < x \oplus y < 1 &\iff -1 - xy < x + y < 1 + xy \\ &\iff -1 - xy < x + y \quad \text{et} \quad x + y < 1 + xy \\ &\iff -1 - y < x + xy \quad \text{et} \quad x - xy < 1 - y \\ &\iff -1(1 + y) < x(1 + y) \quad \text{et} \quad x(1 - y) < 1 - y \end{aligned}$$

     Or, $1 + y$ et $1 - y$ sont strictement positifs car $y \in]-1\,;1[$ donc on peut simplifier par $1 \pm y$ si bien qu'on arrive à $-1 < x$ et $x < 1$ ce qui est vrai : puisqu'on a travaillé par équivalences, l'assertion de départ est vraie aussi, c'est-à-dire que $x \oplus y \in]-1\,;1[$: $\oplus$ est bien une loi interne.
   - Prouvons que la loi est associative. Soit $(x, y, z) \in]-1\,;1[$. D'une part,

$$\begin{aligned} x \oplus (y \oplus z) &= x \oplus \frac{y+z}{1+yz} \\ &= \frac{x + \dfrac{y+z}{1+yz}}{1 + x \times \dfrac{y+z}{1+yz}} \\ &= \frac{x(1+yz) + y + z}{1+yz} \times \frac{1+yz}{(1+yz) + x(y+z)} \\ &= \frac{x + y + z + xyz}{1 + yz + xy + xz} \end{aligned}$$

     et d'autre part

$$\begin{aligned} (x \oplus y) \oplus z &= \frac{x+y}{1+xy} \oplus z \\ &= \frac{\dfrac{x+y}{1+xy} + z}{1 + \dfrac{x+y}{1+xy} \times z} \\ &= \frac{x + y + z(1+xy)}{1+xy} \times \frac{1+xy}{(1+xy) + z(x+y)} \\ &= \frac{x + y + z + xyz}{1 + yz + xy + xz} \end{aligned}$$

     si bien que la loi est associative.
   - Il est évident que 0 est un élément neutre et que, pour tout x, $-x$ est le symétrique de x.

   En conclusion, $(]-1\,;1[, \oplus)$ est un groupe.
3. Il est immédiat que la loi est interne.
   - Prouvons qu'elle est associative. Soient $(x_1, y_1), (x_2, y_2)$ et (x_3, y_3) trois éléments de $\mathbb{R}^2$. D'une part :

$$\begin{aligned}(x_1,y_1)\star((x_2,y_2)\star(x_3,y_3)) &= (x_1,y_1)\star(x_2+x_3,y_2e^{x_3}+y_3e^{x_2})\\ &= (x_1+x_2+x_3,y_1e^{x_2+x_3}+(y_2e^{x_3}+y_3e^{x_2})e^{x_1})\\ &= (x_1+x_2+x_3,y_1e^{x_2+x_3}+y_2e^{x_1+x_3}+y_3e^{x_1+x_2})\end{aligned}$$

et d'autre part

$$\begin{aligned}((x_1,y_1)\star(x_2,y_2))\star(x_3,y_3) &= (x_1+x_2,y_1e^{x_2}+y_2e^{x_1})\star(x_3,y_3)\\ &= (x_1+x_2+x_3,(y_1e^{x_2}+y_2e^{x_1})e^{x_3}+y_3e^{x_1+x_2})\\ &= (x_1+x_2+x_3,y_1e^{x_2+x_3}+y_2e^{x_1+x_3}+y_3e^{x_1+x_2})\end{aligned}$$

et donc la loi est bien associative.

- Il est immédiat que, pour tout $(x,y)\in\mathbb{R}^2, (x,y)\star(0,0)=(x,y)$ (la loi étant commutative, il suffit de prouver qu'un élément est neutre à droite ou à gauche pour prouver que c'est un neutre) est un élément neutre. Cherchons le symétrique de (x,y). Soit $(a,b)\in\mathbb{R}^2$.

$$\begin{aligned}(x,y)\star(a,b)=(0,0) &\iff (x+a,ye^a+be^x)=(0,0)\\ &\iff x+a=0 \quad \text{et} \quad ye^a+be^x=0\\ &= a=-x \quad \text{et} \quad ye^{-x}+be^x=0\\ &= a=-x \quad \text{et} \quad b=-ye^{-2x}\end{aligned}$$

Il en découle que $(-x,-ye^{-2x})$ est un inverse à droite de (x,y) donc, par commutativité de $\star$, un inverse de (x,y). Finalement, $(\mathbb{R}^2,\star)$ est bien un groupe.

Exercice 15 : ✪✪ Soit G l'ensemble suivant :

$$G=\left\{x+y\sqrt{3}\,|\,x\in\mathbb{N},y\in\mathbb{Z},x^2-3y^2=1\right\}$$

Montrer que G est un sous-groupe de $\mathbb{R}^{+*}$.

Correction : Il est sous-entendu que la loi est le produit puisque $(\mathbb{R}_+^*,\times)$ est un groupe.

- Prouvons tout d'abord, ce qui n'est pas si évident que ça car y peut être négatif, que G est inclus dans $\mathbb{R}_+^*$. Soit donc $x+y\sqrt{3}$ (avec x et y vérifiant les bonnes conditions) un élément de G. Alors $x^2=1+3y^2>3y^2$ et la racine carrée est strictement croissante donc

$$\sqrt{x^2}=x>\sqrt{3y^2}=|y|\sqrt{3}\geq -y\sqrt{3}$$

$\sqrt{x^2}=x$ puisque x est positif, et $|y|\geq\pm y$. Finalement, $x+y\sqrt{3}\in\mathbb{R}_+^*$, d'où l'inclusion voulue.
- $1=1+0\sqrt{3}$ avec $1\in\mathbb{N},0\in\mathbb{Z}$ et $1^2-3\times0^2=1$ donc $1\in G$: G est non vide.
- Prouvons que G est stable par produit. Soient $x_1+y_1\sqrt{3}$ et $x_2+y_2\sqrt{3}$ deux éléments de G. Alors

$$(x_1+y_1\sqrt{3})(x_2+y_2\sqrt{3})=X+Y\sqrt{3}$$

avec $X=x_1x_2+3y_1y_2$ et $Y=x_1y_2+x_2y_1$. Il est immédiat que $Y\in\mathbb{Z}$. De plus, $X\in\mathbb{Z}$: prouvons que $X\geq0$. De même que ci-dessus, $x_1>|y_1|\sqrt{3}$ et $x_2>|y_2|\sqrt{3}$ donc, par produit (les inégalités sont positives, d'où la nécessité de la valeur absolue), $x_1x_2>3|y_1y_2|\geq-3y_1y_2$ (toujours car $|y_1y_2|\geq\pm y_1y_2$) si bien que $X=x_1x_2+3y_1y_2\geq0$: on a bien $X\in\mathbb{N}$. Enfin :

$$\begin{aligned}X^2-3Y^2 &= (x_1x_2+3y_1y_2)^2-3(x_1y_2+x_2y_1)^2\\ &= {x_1}^2{x_2}^2+6x_1x_2y_2y_2+9{y_1}^2{y_2}^2-3({x_1}^2{y_2}^2+2x_1y_2x_2y_1+{x_2}^2{y_1}^2)\\ &= {x_1}^2{x_2}^2+9{y_1}^2{y_2}^2-3{x_1}^2{y_2}^2-3{x_2}^2{y_1}^2\\ &= {x_1}^2\left({x_2}^2-3{y_2}^2\right)-3{y_1}^2\left({x_2}^2-3{y_2}^2\right)\\ &= {x_1}^2\times1-3{y_1}^2\times1\\ &= 1\end{aligned}$$

Finalement, on a bien $(x_1+y_1\sqrt{3})(x_2+y_2\sqrt{3})=X+Y\sqrt{3}\in G$: G est stable par produit.

- Prouvons que G est stable par inverse. Soit $x+y\sqrt{3} \in G$. Tout d'abord, $x+y\sqrt{3} > 0$ comme on l'a déjà vu donc étudier son inverse a du sens. Avec la méthode de l'expression conjuguée :

$$\begin{aligned}\frac{1}{x+y\sqrt{3}} &= \frac{x-y\sqrt{3}}{(x+y\sqrt{3})(x-y\sqrt{3})} \\ &= \frac{x-y\sqrt{3}}{x^2-3y^2} \\ &= x-y\sqrt{3}\end{aligned}$$

  Or, $x \in \mathbb{N}$, $(-y) \in \mathbb{Z}$ et $x^2-3(-y^2) = x^2-3y^2 = 1$ si bien que

$$\frac{1}{x+y\sqrt{3}} = x-y\sqrt{3} \in G$$

  En d'autres termes, G est stable par inverse.

En conclusion, G est un sous-groupe de $\mathbb{R}_+^*$ (et, en particulier, G est un groupe pour la loi $\times$).

2.2 Calculs dans un groupe

Exercice 16 : ✪ Soit G un groupe. Soient $(a,b) \in G^2$ et $n \in \mathbb{N}^*$ tels que $(ab)^n = e$. Montrer que $(ba)^n = e$.

Correction : Évidemment, le groupe n'est pas supposé abélien sinon $ab = ba$ et alors le résultat est évident. Par définition,

$$\underbrace{(ab) \times \cdots \times (ab)}_{n \text{ fois}} = e$$

En particulier, la loi étant associative :

$$a \times \underbrace{(ba) \times \cdots \times (ba)}_{n-1 \text{ fois}} \times b = e$$

En multipliant par b à gauche :

$$ba \times \underbrace{(ba) \times \cdots \times (ba)}_{n-1 \text{ fois}} \times b = b$$

Dans un groupe, tout élément est régulier donc on peut « simplifier » par b (ou, de façon explicite, on multiplie par b^{-1} à droite) ce qui donne :

$$\underbrace{(ba) \times \cdots \times (ba)}_{n \text{ fois}} = e$$

ce qui est le résultat voulu.

Exercice 17 : ✪ Soit G un groupe tel que pour tout $(x,y) \in G^2, (xy)^2 = x^2y^2$. Montrer que G est commutatif.

Correction : Soit $(x,y) \in G^2$. Par hypothèse, $(xy) \times (xy) = x^2y^2$ c'est-à-dire (la loi étant associative donc on peut se passer de parenthèses) $xyxy = xxyy$. Dans un groupe, tout élément est régulier (ou alors, explicitement, en multipliant par x^{-1} à gauche et y^{-1} à droite) donc $yx = xy$: le groupe est abélien.

Exercice 18 : ✪ Soit G un groupe dont tous les éléments x vérifient $x^2 = e$. Montrer que G est abélien.

Correction : Soit $(x,y) \in G^2$. Par hypothèse, $(xy)^2 = xyxy = e$. Tout élément est par hypothèse son propre inverse donc, en multipliant par x à gauche et y à droite, il vient : $x^2yxy^2 = xy$ donc $yx = xy$: G est abélien.

Exercice 19 : ✪ Soit G un groupe (pas nécessairement abélien) de neutre e et soient a et b deux éléments de G.

1. Montrer que si $ab = b^2a$ et $b^5 = e$ alors $ab^3 = ba$ et $a^2b^2 = b^3a^2$.
2. Montrer que si $a^5 = e$ et $ab = ba^3$ alors $a^2b = ba$ et $ab^3 = b^3a^2$.

Correction :

1. On utilisera sans arrêt l'associativité de la loi : nous pourrons donc sans arrêt mettre des parenthèses où ça nous arrange, et les supprimer si cela nous arrange aussi. D'une part :

$$\begin{aligned} ab^3 &= (ab)b^2 \\ &= b^2ab^2 \\ &= b^2(ab)b \\ &= b^2(b^2a)b \\ &= b^2b^2(ab) \\ &= b^2b^2b^2a \\ &= b^5ba \\ &= eba \\ &= ba \end{aligned}$$

   D'autre part, en utilisant à présent le fait que $ab^3 = ba$:

$$\begin{aligned} a^2b^2 &= a(ab)b \\ &= a(b^2a)b \\ &= ab^2(ab) \\ &= ab^2(b^2a) \\ &= (ab^3)ba \\ &= (ba)ba \\ &= b(ab)a \\ &= b(b^2a)a \\ &= b^3a^2 \end{aligned}$$

2. De même :

$$\begin{aligned} a^2b &= a(ab) \\ &= a(ba^3) \\ &= (ab)a^3 \\ &= (ba^3)a^3 \\ &= ba^6 \\ &= baa^5 \\ &= bae \\ &= ba \end{aligned}$$

   et, en utilisant le fait que $a^2b = ba$:

$$\begin{aligned} ab^3 &= (ab)b^2 \\ &= (ba^3)b^2 \\ &= ba^2(ab)b \\ &= ba^2(ba^3)b \\ &= b(a^2b)a(a^2b) \\ &= b(ba)a(ba) \\ &= b^2(a^2b)a \\ &= b^2(ba)a \\ &= b^3a^2 \end{aligned}$$

2.3 Transport de structure

Exercice 20 : ✪ Soient G_1, G_2, H_1, H_2 quatre groupes. On suppose que G_1 et G_2 sont isomorphes, ainsi que H_1 et H_2. Montrer que les groupes $G_1 \times H_1$ et $G_2 \times H_2$ sont isomorphes.

Correction : Notons $\varphi : G_1 \to G_2$ un isomorphisme et $\psi : H_1 \to H_2$ un isomorphisme. Toutes les lois seront notées $*$ par souci de simplicité (nous n'allons par noter $*_{G_1}$ la loi de G_1 etc.), mais il faut bien garder à l'esprit que les lois n'ont aucune raison d'être les mêmes (il y a quatre lois distinctes : celle de G_1, celle de G_2, celle de H_1, celle de H_2, c'est un bon exercice de se demander à chaque fois à quel ensemble appartient quel objet). Soit $f : G_1 \to H_1 \mapsto G_2 \times H_2$ définie par :

$$\forall (a_1, b_1) \in G_1 \times H_1, f(a_1, b_1) = (\varphi(x_1), \psi(b_1))$$

Tout d'abord, φ étant à valeurs dans G_2 et ψ dans H_2, f va bien de $G_1 \times H_1$ dans $G_2 \times H_2$.

- Montrons que f est un morphisme de groupes (pour la loi produit, cf. cours). Soient (a_1, b_1) et (c_1, d_1) deux éléments de $G_1 \times H_1$. Par définition de la loi produit, $(a_1, b_1) \times (c_1, d_1) = (a_1 * c_1, b_1 * d_1)$ (une dernière fois, précisons que, dans la première coordonnée, $*$ désigne la loi de G_1 et, dans la deuxième coordonnée, $*$ désigne la loi de H_1, lois qui ne sont pas forcément les mêmes, et ce sera pareil pour les lois de G_2 et H_2 dans la suite). Dès lors :

$$\begin{aligned} f((a_1, b_1) \times (c_1, d_1)) &= f(a_1 * c_1, b_1 * d_1) \\ &= (\varphi(a_1 * c_1), \psi(b_1 * d_1)) \\ &= (\varphi(a_1) * \varphi(c_1), \psi(b_1) * \psi(d_1)) \quad \text{car } \varphi \text{ et } \psi \text{ sont des morphismes de groupes} \\ &= (\varphi(a_1), \psi(b_1)) \times (\varphi(c_1), \psi(d_1)) \\ &= f(a_1, b_1) \times f(c_1, d_1) \end{aligned}$$

  si bien que f est un morphisme de groupes.
- Soit $(a_1, b_1) \in \ker(f)$. Alors $f(a_1, b_1) = (e_2, \varepsilon_2)$ (où e_2 est le neutre de G_2 et ε_2 le neutre de H_2) mais, par définition, $f(a_1, b_1) = (\varphi(a_1), \psi(b_1))$ donc $\varphi(a_1) = e_2$ et idem pour l'autre, si bien que $a_1 \in \ker(\varphi) = \{e_1\}$ par injectivité de φ donc $a_1 = e_1$. De même, $b_1 = \varepsilon_1$ (le neutre de H) donc $\ker(f) = \{(e_1, \varepsilon_1)\}$, f est injective.
- Enfin, soit $(a_2, b_2) \in G_2 \times H_2$. φ étant surjective, il existe $a_1 \in G_1$ tel que $a_2 = \varphi(a_1)$ et idem il existe $b_1 \in H_1$ tel que $\psi(b_1) = b_2$ et donc $f(a_1, b_1) = (a_2, b_2)$: f est surjective donc bijective donc c'est un isomorphisme.

Exercice 21 : ✪ Soient $(G, \times)$ un groupe, E un ensemble (pas forcément un groupe) et $f : G \to E$ une bijection. On définit une loi de composition interne $*$ sur E par :

$$\forall (x, y) \in E^2, x * y = f\left(f^{-1}(x) \times f^{-1}(y)\right)$$

Montrer que $(E, \times)$ est un groupe isomorphe à $(G, \times)$.

Correction : On utilisera souvent le fait que, pour tout $y \in E$, $f(f^{-1}(y)) = y$ et que pour tout $g \in G$, $f^{-1}(f(g)) = g$.

- Montrons que la loi $*$ est associative. Soient y_1, y_2, y_3 trois éléments de E.

$$\begin{aligned} y_1 * (y_2 * y_3) &= y_1 * f\left(f^{-1}(y_2) \times f^{-1}(y_3)\right) \\ &= f\left(f^{-1}(y_1) \times f^{-1}\left(f\left(f^{-1}(y_2) \times f^{-1}(y_3)\right)\right)\right) \\ &= f\left(f^{-1}(y_1) \times \left(f^{-1}(y_2) \times f^{-1}(y_3)\right)\right) \end{aligned}$$

et

$$\begin{aligned} (y_1 * y_2) * y_3 &= f\left(f^{-1}(y_1) \times f^{-1}(y_2)\right) * y_3 \\ &= f\left(f^{-1}\left(f\left(f^{-1}(y_1) \times f^{-1}(y_2)\right)\right) \times f^{-1}(y_3)\right) \\ &= f\left(\left(f^{-1}(y_1) \times f^{-1}(y_2)\right) \times f^{-1}(y_3)\right) \end{aligned}$$

et ces deux quantités sont bien égales par associativité de la loi $\times$ puisque $(G, \times)$ est un groupe.

- Notons $\varepsilon = f(e)$ où e désigne évidemment le neutre de G. Montrons que e est un élément neutre dans E (attention, il faut regarder les deux sens car la loi n'est pas forcément commutative). Soit $y \in E$. D'une part, e étant le neutre de G,

$$\begin{aligned} y * \varepsilon &= f\left(f^{-1}(y) \times f^{-1}(\varepsilon)\right) \\ &= f\left(f^{-1}(y) \times e\right) \\ &= f\left(f^{-1}(y)\right) \\ &= y \end{aligned}$$

et, d'autre part, on montre de même que $\varepsilon * y = y$: ε est bien le neutre de G.

- Soit $y \in E$. Alors il existe $g \in G$ tel que $y = f(g)$. G étant un groupe, g admet un inverse qu'on note h (il y a assez de -1 comme ça dans cet exercice) et notons $x = f(h)$: montrons que x est l'inverse de y pour la loi $*$.

$$\begin{aligned} x * y &= f\left(f^{-1}(x) \times f^{-1}(g)\right) \\ &= f(h \times g) \\ &= f(e) \\ &= \varepsilon \end{aligned}$$

et idem pour $y * x$: x est l'inverse de y. Finalement, E est bien un groupe.

- Enfin, f est une bijection de G dans E. Pour montrer que c'est un isomorphisme, il suffit de prouver que c'est un morphisme de groupes entre G et E. Soient g et h deux éléments de G et notons $y = f(g)$ et $x = f(h)$, bien que :

$$\begin{aligned} f(g \times h) &= f\left(f^{-1}(y) \times f^{-1}(x)\right) \\ &= y * x \end{aligned}$$

par définition de la loi $*$: f est un morphisme, f est bijective donc f est un isomorphisme : G et E sont deux groupes isomorphes.

Exercice 22 : ✪ Soit $(E, \top)$ un groupe. Soit F un ensemble non vide muni d'une loi interne $\perp$. On suppose qu'il existe une bijection $f : E \to F$ telle que :

$$\forall (x, y) \in E^2, f(x \top y) = f(x) \perp f(y)$$

Montrer que $(F, \perp)$ est un groupe isomorphe à $(E, \top)$.

Correction : Il suffit de prouver que $(F, \perp)$ est un groupe : il sera automatiquement isomorphe à $(E, \top)$ puisque f est une bijection de E dans F et que, par définition, elle est compatible entre la loi $\top$ et la loi $\perp$. Idem que dans l'exercice précédent, f étant bijective, elle admet une bijection réciproque f^{-1}, et $f \circ f^{-1} = \mathrm{Id}_F$ et $f^{-1} \circ f = \mathrm{Id}_E$.

- Montrons que $\perp$ est associative. Soient a, b, c trois éléments de F. Notons $x = f^{-1}(a), y = f^{-1}(b)$ et $z = f^{-1}(c)$ leurs antécédents par f (donc des éléments de E). En utilisant la propriété de la fonction f et le fait que $\top$ est associative puisque $(E, \top)$ est un groupe :

$$\begin{aligned} a\perp(b\perp c) &= f(x)\perp(f(y)\perp f(z)) \\ &= f(x)\perp f(y\top z) \\ &= f(x\top(y\top z)) \\ &= f((x\top y)\top z) \\ &= f(x\top y)\perp f(z) \\ &= (f(x)\perp f(y))\perp f(z) \\ &= (a\perp b)\perp c \end{aligned}$$

c'est-à-dire que la loi $\perp$ est associative.

- Notons $\varepsilon = f(e)$ où e est l'élément neutre de $(E, \top)$. Soit $y \in F$ et notons $x \in E = f^{-1}(y)$. D'une part,

$$\begin{aligned} y\perp\varepsilon &= f(x)\perp f(e) \\ &= f(x\top e) \\ &= f(x) \\ &= y \end{aligned}$$

et on prouve de même que $\varepsilon\perp y = y$: ε est bien le neutre de F.

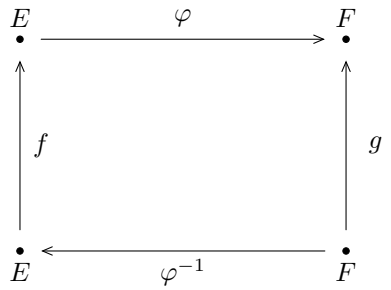
- Soit $a \in F$. Notons $x = f^{-1}(a)$ son unique antécédent par f. Soit $y \in E$ l'inverse de x, et soit enfin $b = f(y)$. Alors :

$$\begin{aligned} a\perp b &= f(a)\perp f(b) \\ &= f(a\top b) \\ &= f(e) \\ &= \varepsilon \end{aligned}$$

et on prouve de même que $b\perp a = \varepsilon$: a admet un inverse, F est bien un groupe et on a déjà dit pourquoi, dans ce cas, il est isomorphe à E.

Exercice 23 : ✪✪ Les deux questions sont indépendantes.

1. Montrer que si E et F sont deux ensembles équipotents (i.e. s'il existe une bijection de E dans F) alors S_E et S_F sont isomorphes. On pourra s'inspirer du dessin ci-contre.
2. Montrer que si un ensemble contient au moins 3 éléments, alors $Z(S_E) = \{\mathrm{Id}_E\}$, c'est-à-dire que Id_E est le seul élément qui commute avec tout le monde.



Correction : Rappelons que S_E est l'ensemble des bijections de E (on dit aussi l'ensemble des permutations, même si on garde plutôt le terme de permutation pour les ensembles finis) et que c'est un groupe pour la composition (cf. cours).

1. Notons donc φ une bijection de E dans F. Montrons que

$$c : \begin{cases} S_E & \to & S_F \\ f & \to & \varphi \circ f \circ \varphi^{-1} \end{cases}$$

est un isomorphisme entre S_E et S_F munis de la composition (φ^{-1} est bien définie puisque φ est bijective).

- Montrons tout d'abord que c est bien définie i.e. va bien de S_E dans S_F. Soit $f \in S_E$. Alors $\varphi^{-1} : F \to E$, $f : E \to E$ et $\varphi : E \to F$ donc $c(f)$ va bien de F dans F et est bijective car composée de bijections donc $c(f)$ est bien un élément de S_F.

- Montrons tout d'abord que c est un morphisme de groupes. Soient f_1 et f_2 deux éléments de S_E (i.e. deux bijections de E dans E). Alors (en utilisant l'associativité de la composition) :

$$\begin{aligned} c(f_1)\circ c(f_2) &= \left(\varphi\circ f_1\circ\varphi^{-1}\right)\circ\left(\varphi\circ f_2\circ\varphi^{-1}\right)\\ &= \varphi\circ f_1\circ(\varphi-1\circ\varphi)\circ f_2\circ\varphi-1\\ &= \varphi\circ f_1\circ(\mathrm{Id}_E)\circ f_2\circ\varphi-1\\ &= \varphi\circ(f_1\circ f_2)\circ\varphi-1\\ &= c(f_1\circ f_2) \end{aligned}$$

  si bien que c est bien un morphisme de groupes.
- Montrer que c est une bijection. Attention de ne pas confondre c qui va de E_E dans S_F avec $c(f)=\varphi\circ f\circ\varphi-1$ et de ne pas dire que c est bijective car est une composée de bijections, cela n'aurait aucun sens ! Soient $f\in S_E$ et $g\in S_F$. Alors, en composant à gauche par $\varphi-1$ et à droite par φ, on obtient : $c(f)=g \iff f=\varphi^{-1}\circ g\circ\varphi$. En d'autres termes, g admet un unique antécédent par c, c est bijective, c'est un isomorphisme de groupes, et en particulier les deux groupes sont isomorphes.

2. Soit $f\in S_E\backslash\{\mathrm{Id}_E\}$ et montrons que f n'appartient pas au centre de S_E donc que f ne commute pas avec tout le monde. Il suffit donc d'exhiber une bijection de E qui ne commute pas avec f. f n'étant pas l'identité, il existe $a\in E$ tel que $f(a)\neq a$. Notons $b=f(a)$: on a donc $a\neq b$ et $f(a)=b$. Il y a deux cas de figure : soit $f(b)=a$ (i.e. f « échange a et b ») soit $f(b)\neq a$. Supposons que $f(b)=a$. Puisque E a au moins trois éléments, soit $c\neq a,b$ et soit $g:E\to E$ la fonction qui échange a et c i.e. définie par :

$$\forall x\in E, g(x)=\begin{cases} x & \text{si } x\neq a,c\\ c & \text{si } x=a\\ a & \text{si } x=c\end{cases}$$

   Il est immédiat que g est bijective. Or, $f(g(b))=f(b)=a$ et $g(f(b))=g(a)=c$ donc f est g ne commutent pas. Supposons à présent que $f(b)\neq a$. Puisque $f(a)=b$ et f injective, on a également $f(b)\neq b$: notons $c=f(b)$ et donc $c\neq a,b$. Avec la même fonction g, il vient : $f(g(b))=f(b)=c$ et $g(f(b))=g(c)=a$ et on conclut de la même façon.

Exercice 24 : ✪✪ Soient $(G,.)$ un groupe et $a\in G$. On définit une nouvelle loi $*$ sur G par $x*y=xay$. Montrer que $(G,*)$ est un groupe isomorphe à $(G,.)$.

Correction : Intuitivement, on « fait une rotation de a » : les résultats de cet exercice sont intuitifs une fois que l'on a cette image en tête. Quand on parlera de la loi du groupe, on parlera de la loi . que l'on note multiplicativement : parfois (tout le temps), on écrira ab au lieu de $a.b$.

- Montrons que $*$ est associative. Soit $(x,y,z)\in G^3$. On va utiliser que la loi du groupe (notée multiplicativement) est associative.

$$\begin{aligned} x*(y*z) &= x*(yaz)\\ &= xa(yaz)\\ &= (xay)az\\ &= (x*y)az\\ &= (x*y)*z \end{aligned}$$

  La loi est bien associative.
- Notons a^{-1} l'inverse de a pour la loi du groupe et e le neutre de G (qui existent car G est un groupe). On montre aisément que, pour tout $x\in G$, $x*a^{-1}=a^{-1}*x=x$ donc a^{-1} est bien le neutre pour $*$.
- Pour tout $x\in G$, on cherche donc y tel que $xay=a^{-1}$. En multipliant par x^{-1} (l'inverse de x au sens de la loi du groupe, qui existe puisqu'on est sur un groupe justement) à gauche puis a^{-1}, on trouve que $y=a^{-1}x^{-1}a^{-1}$, et il est immédiat (en utilisant l'associativité de la loi du groupe) qu'on a bien $x*y=y*x=a^{-1}$, le neutre, donc $a^{-1}x^{-1}a^{-1}$ est le symétrique de x pour la loi $*$.
- En conclusion, $(G,*)$ est bien un groupe. Exhibons un isomorphisme de $(G,.)$ dans $(G,*)$. Montrons que $\varphi:x\mapsto a^{-1}x$ est un tel isomorphisme (la « rotation » dans le sens inverse). Soit $(x,y)\in G^2$. Alors (on utilise l'associativité de la loi du groupe) :

$$\begin{aligned}\varphi(xy) &= a^{-1}xy\\ &= a^{-1}xaa^{-1}y\\ &= \varphi(x)a\varphi(y)\\ &= \varphi(x)*\varphi(y)\end{aligned}$$

c'est-à-dire que φ est un morphisme de groupes. Il est évidemment bijectif : si $\varphi(x_1)=\varphi(x_2)$ alors $a^{-1}x_1 = a^{-1}x_2$ donc, en multipliant par a à gauche (ou car tout élément de G est régulier), $x_1 = x_2$ donc φ est injective, et pour tout $y \in G$, ay est un antécédent de y donc φ est bijective, c'est un isomorphisme.

2.4 Morphismes

Exercice 25 : ✪ Soit $n \geq 1$. Montrer que $z \mapsto z^n$ réalise un endomorphisme de groupe de $(\mathbb{C}^*, \times)$ (i.e. un morphisme de groupes de $(\mathbb{C}^*, \times)$ dans lui-même). Donner son image et son noyau.

Correction : Soit $(z_1, z_2) \in (\mathbb{C}^*)^2$. Notons f cette fonction. Alors

$$\begin{aligned}f(z_1 \times z_2) &= (z_1 \times z_2)^n\\ &= {z_1}^n \times {z_2}^n\\ &= f(z_1) \times f(z_2)\end{aligned}$$

c'est-à-dire que f est un morphisme de groupe de $(\mathbb{C}^*, \times)$ dans lui-même donc un endomorphisme de groupes. Puisque le neutre est 1, son noyau est $\ker(f) = \{z \in \mathbb{C}^* \mid f(z) = 1\}$ donc l'ensemble des n tels que $z^n = 1$, c'est-à-dire que $\ker(f) = \mathbb{U}_n$, l'ensemble des racines n-ièmes de l'unité. Son image est $\mathbb{C}^*$ tout entier : en effet, si $z \in \mathbb{C}^*$, alors (cf. chapitre 7), z a des racines n-ièmes (et même n distinctes pour être précis) donc au moins une : f est surjective.

Exercice 26 : ✪

1. Donner tous les morphismes de groupe de $\mathbb{Z}$ dans lui-même. En déduire le groupe des automorphismes de $\mathbb{Z}$ (i.e. des morphismes bijectifs de $\mathbb{Z}$ dans lui-même).
2. Donner tous les morphismes de groupe de $\mathbb{Q}$ dans lui-même.

Correction :

1. Analyse : soit f un morphisme de groupes de $\mathbb{Z}$ dans lui-même. Alors, pour tout $n \in \mathbb{N}^*$ (le 1 apparaît n fois)

$$\begin{aligned}f(n) &= f(1+\cdots 1)\\ &= f(1)+\cdots+f(1)\\ &= nf(1)\end{aligned}$$

Si on note $a = f(1)$, alors $f(n) = an$ pour tout $n \in \mathbb{N}$. On sait de plus que $f(0) = 0$ (un morphisme envoie le neutre sur le neutre) et, si $n < 0$, alors $-n \in \mathbb{N}^*$ donc $f(-n) = -na$ et $f(n-n) = f(0) = 0$ mais f est un morphisme donc

$$\begin{aligned}f(n-n) &= f(n)+f(-n)\\ &= -f(-n)\\ &= na\end{aligned}$$

En conclusion, $f(n) = na$ avec $a = f(1)$. Réciproquement, soit $a \in \mathbb{Z}$ et prouvons que $f : n \mapsto na$ est un morphisme de groupe de $\mathbb{Z}$ dans lui-même. Soient n_1 et n_2 dans $\mathbb{Z}$, alors

$$\begin{aligned}f(n_1+n_2) &= a(n_1+n_2)\\ &= an_1+an_2\\ &= f(n_1)+f(n_2)\end{aligned}$$

c'est-à-dire que f est un morphisme de groupes. En conclusion, les morphismes de groupes de $\mathbb{Z}$ dans lui-même sont les $n \mapsto an$, pour tout $a \in \mathbb{Z}$. Un tel morphisme est bijectif si et seulement si $a = 1$ donc l'unique automorphisme de $\mathbb{Z}$ est $n \mapsto n$ donc l'identité de $\mathbb{Z}$: le groupe des automorphismes de $\mathbb{Z}$ est $\{\mathrm{Id}_{\mathbb{Z}}\}$.

2. Notons $a = f(1)$. De même, $f(n) = an$ pour tout $n \in \mathbb{Z}$. Soit $n \in \mathbb{N}^*$. Puisque $1 = \dfrac{1}{n} + \cdots + \dfrac{1}{n}$ (n fois) donc
$$f(1) = f\left(\frac{1}{n}\right) + \cdots + f\left(\frac{1}{n}\right)$$
si bien que $f\left(\dfrac{1}{n}\right) = \dfrac{a}{n} = \dfrac{f(1)}{n}$. Soit à présent $r = p/q$ un rationnel avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. On montre de même que $f(p/q) = pf(1/q)$ et d'après ce qui précède, $f(1/q) = f(1)/q$ donc $f(p/q) = pf(1)/q$ donc $f(r) = rf(1)$. On montre réciproquement que toute fonction du type $r \mapsto ar$ convient. En conclusion, les morphismes de $\mathbb{Q}$ dans $\mathbb{Q}$ sont exactement les fonctions de la forme $r \mapsto ar$ avec $a \in \mathbb{Q}$.

Exercice 27 : ✪✪ Donner tous les morphismes de groupe de $\mathbb{Q}$ dans $\mathbb{Z}$.

Correction : De même que dans l'exercice précédent, on montre que $\varphi(r) = r\varphi(1)$ pour tout $r \in \mathbb{Q}$ (ou alors, tout simplement, on utilise l'exercice précédent en disant qu'un morphisme de $\mathbb{Q}$ dans $\mathbb{Z}$ est un morphisme de $\mathbb{Q}$ dans lui-même donc est de cette forme). En particulier, pour tout $n \in \mathbb{N}^*$, $\varphi(1/n) = \varphi(1)/n \xrightarrow[n\to+\infty]{} 0$ donc appartient à $]-1\,;1[$ pour n assez grand. Or, c'est un entier : on en déduit que $\varphi(1) = 0$, si bien que φ est la fonction nulle : la fonction nulle est donc l'unique morphisme de groupes de $\mathbb{Q}$ dans $\mathbb{Z}$.

Exercice 28 - Isomorphismes : ✪✪ Les groupes suivants sont-ils isomorphes ?

1. $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$.
2. $(\mathbb{Q}, +)$ et $(\mathbb{Q}_+^*, \times)$.
3. $(\mathbb{Q}, +)$ et $(\mathbb{Z}, +)$.
4. $(\mathbb{Q}_+^*, \times)$ et $(\mathbb{R}_+^*, \times)$.
5. $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$.

Correction :

1. L'exponentielle est un isomorphisme entre ces deux groupes (cf. cours). Les groupes suivants ne sont pas isomorphes : l'idée est toujours la même (cf. cours), trouver une équation dans un groupe, son analogue dans l'autre groupe, et montrer qu'elles n'ont pas le même nombre de solutions ce qui est absurde si les groupes sont isomorphes.
2. Intéressons-nous à l'équation $y^2 = 2$, qui n'a pas de solution dans $\mathbb{Q}_+^*$, alors que son analogue dans $\mathbb{Q}$, $x + x = \cdots$ en a. Supposons qu'il existe un isomorphisme φ entre les deux groupes. Notons a l'unique antécédent de 2 par φ (celui-ci existe et est unique par bijectivité). Alors,φ étant un morphisme :
$$\begin{aligned} 2 &= \varphi(a) \\ &= \varphi\left(\frac{a}{2} + \frac{a}{2}\right) \\ &= \varphi\left(\frac{a}{2}\right) \times \varphi\left(\frac{a}{2}\right) \\ &= \varphi\left(\frac{a}{2}\right)^2 \end{aligned}$$
si bien que $\varphi(a/2) = \sqrt{2}$ (c'est un nombre positif) ce qui est absurde car φ est à valeurs dans $\mathbb{Q}$.
3. On a déjà prouvé dans l'exercice précédent qu'ils ne sont pas isomorphes, car le seul morphisme entre de $\mathbb{Q}$ dans $\mathbb{Z}$ est le morphisme nul qui n'est pas bijectif, mais remontrons qu'ils ne sont pas isomorphes. S'ils sont isomorphes, soit $\varphi : \mathbb{Q} \to \mathbb{Z}$ un isomorphisme et soit n l'unique antécédent de 1. Alors
$$\begin{aligned} \varphi(n) &= \varphi(1 + \cdots + 1) \\ &= \varphi(1) + \cdots + \varphi(1) \\ &= n\varphi(1) \end{aligned}$$
mais $\varphi(n) = 1$ donc $\varphi(1) = 1/n$ ce qui est absurde si $n \neq \pm 1$ puisque φ est à valeurs dans $\mathbb{Z}$. Il en découle que $n = \pm 1$ donc l'unique antécédent de 1 est ± 1 mais alors $\varphi(\pm 1/2) = \pm 12$ (même raisonnement que d'habitude) ce qui est absurde puisque φ est à valeurs dans $\mathbb{Z}$: les deux groupes ne sont pas isomorphes.

4. Il n'existe de toute façon aucune bijection (morphisme ou non) entre les deux ensembles car l'un est dénombrable et pas l'autre, mais c'est plutôt au programme de deuxième année donc donnons une preuve au programme (et qui utilise les morphismes de groupes). Là encore, intéressons-nous à l'équation $x^2 = 2$. Supposons qu'il existe un isomorphisme de $\mathbb{R}_+^*$ dans $\mathbb{Q}_+^*$ et notons a l'antécédent de 2. Alors

$$\begin{aligned}\varphi(a) &= \varphi(\sqrt{a} \times \sqrt{a}) \\ &= \varphi(\sqrt{a}) \times \varphi(\sqrt{a}) \\ &= \varphi(\sqrt{a})^2\end{aligned}$$

   Or, $\varphi(a) = 2$ et φ est à valeurs positives donc $\varphi(\sqrt{a}) = \sqrt{2}$ ce qui est absurde car φ est à valeurs rationnelles : les deux groupes ne sont pas isomorphes.

5. Intéressons-nous cette fois à l'équation $x^2 = -1$ qui a des solutions sur $\mathbb{C}$ mais pas sur $\mathbb{R}$. Supposons qu'il existe un isomorphisme $\varphi : \mathbb{C} \to \mathbb{R}$. Notons a l'unique antécédent de -1. a étant un complexe non nul, il existe deux complexes opposés b_1 et b_2 dont le carré donne a. De même que ci-dessus, il en découle que

$$-1 = \varphi(a) = \varphi(b_1)^2$$

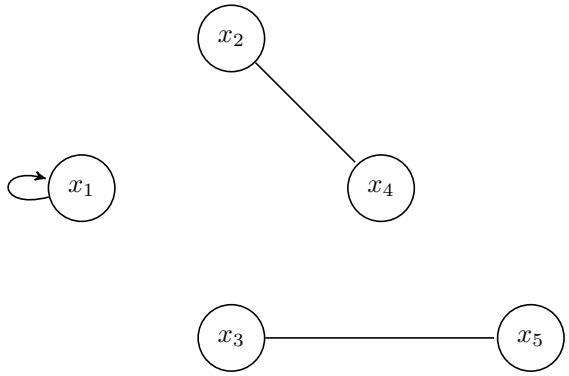
   ce qui est absurde car φ est à valeurs réelles : les deux groupes ne sont pas isomorphes.

Exercice 29 - Autour de l'inverse : ✪✪

1. Montrer par récurrence que, pour tout n, une involution sur un ensemble à $2n+1$ éléments admet au moins un point fixe.
2. Soit G un groupe. Montrer que $x \mapsto x^{-1}$ est un automorphisme de G (i.e. un morphisme bijectif de G dans lui-même) si et seulement si G est abélien.
3. On suppose dans cette question que G est un groupe fini et que f est un automorphisme de G involutif sans point fixe non trivial, c'est-à-dire : $\forall x \in G, f(x) = x \Rightarrow x = e$.
   (a) Montrer que $x \mapsto f(x)x^{-1}$ est une bijection de G dans G.
   (b) Montrer que pour tout $x \in G, f(x) = x^{-1}$.
   (c) En déduire que G est abélien et de cardinal impair.

Correction :

1. Montrons le résultat par récurrence. Soit H_n : « Toute involution sur un ensemble fini de cardinal $2n+1$ admet au moins un point fixe. » Si $n = 0$, on a un ensemble à un élément donc la seule involution est l'identité qui admet un point fixe donc H_0 est vraie. Soit $n \geq 0$, supposons que H_n soit vraie. Montrons que H_{n+1} est vraie. Soit E un ensemble de cardinal $2(n+1)+1 = 2n+3$ et soit f une involution de E. Soit a un élément de E. Si a est un point fixe c'est terminé. Sinon il existe b distinct de a tel que $b = f(a)$. Or, f est une involution donc $f(b) = a$. f est donc une involution de $E\backslash\{a, b\}$ qui est un ensemble à $2n+1$ éléments donc admet un point fixe par hypothèse de récurrence. Donc H_{n+1} est vraie donc H_n est vraie pour tout n par le principe de récurrence.
2. Notons cette fonction φ. Prouvons que c'est une bijection. Soient g_1 et g_2 tels que ${g_1}^{-1} = {g_2}^{-1}$. En passant à l'inverse, $g_1 = g_2$: φ est injective. Soit $y \in G$. Alors $\varphi\left(y^{-1}\right) = y$: y^{-1} est un antécédent de y donc φ est surjective donc bijective (on pouvait aussi dire que φ est involutive donc bijective). Prouvons donc que φ est un morphisme de groupes si et seulement si G est abélien. Supposons que φ soit un morphisme et soient a, b deux éléments de G. Alors $\varphi(ab) = \varphi(a)\varphi(b)$ c'est-à-dire que $(ab)^{-1} = a^{-1}b^{-1}$. Or, $a^{-1}b^{-1} = (ba)^{-1}$ (on change l'ordre quand on inverse) si bien que $(ab)^{-1} = (ba)^{-1}$. En passant à l'inverse, il vient : $ab = ba$, G est abélien. Réciproquement, si G est abélien, alors pour tous a et b dans G, $ab = ba$ donc, en passant à l'inverse, $(ab)^{-1} = a^{-1}b^{-1}$ c'est-à-dire que $\varphi(ab) = \varphi(a)\varphi(b)$: φ est un morphisme, d'où l'équivalence.
3. (a) Notons cette fonction φ. Soient a et b dans G tels que $f(a)a^{-1} = f(b)b^{-1}$. Alors, en multipliant par a à droite, $f(a) = f(b)b^{-1}a$, et en multipliant par $f(b)^{-1}$ à gauche, $f(b)^{-1}f(a) = b^{-1}a$. Or, f est un morphisme donc $f\left(b^{-1}a\right) = b^{-1}a$: $b^{-1}a$ est un point fixe de f, donc $b^{-1}a = e$ par hypothèse sur f, si bien que $a = b$: g est injective. Puisqu'elle est injective entre deux ensembles finis de même cardinal (d'un ensemble fini dans lui-même), c'est une bijection.
   (b) Soit $x \in G$. φ étant surjective, il existe $a \in G$ tel que $\varphi(a) = x$ donc $f(a) = ax$. En appliquant f (morphisme involutif), il vient : $a = f(a)f(x)$ si bien que $f(a) = af(x)^{-1}$ donc, finalement, $ax = af(x)^{-1}$ et tout élément est régulier (ou en multipliant à gauche par a^{-1}) donc $x = f(x)^{-1}$ si bien que $f(x) = x^{-1}$.
   (c) D'après la question 2, G est abélien. Prouvons que le cardinal de G est impair, ce qui se voit très bien sur un dessin en associant chaque élément et son image (rappelons que f est une involution avec un unique point fixe donc, à part le point fixe, les éléments sont regroupés par paires, ce qui donne un nombre impair) :



Supposons que G soit de cardinal pair qu'on note $2p$. Alors $G\backslash\{e\}$ est de cardinal $2p-1$, et la restriction de G à $E\backslash\{a\}$ est donc une involution sans point fixe ce qui est absurde d'après la question 1.

2.5 Groupes et combinatoire

Exercice 30 : ✪ Soit G un groupe fini et soient A, B deux parties de G telles que $\text{card}(A) + \text{card}(B) > \text{card}(G)$. Enfin, notons $AB = \{ab \,|\, a \in A, b \in B\}$.

1. Montrer que, pour tout $g \in G$, $A \cap \{gb^{-1} \,|\, b \in B\}$ est non vide.
2. Montrer que $G = AB$.

Correction :

1. Soit $g \in G$. Soit φ qui va de B dans $\{gb^{-1} \,|\, b \in B\}$ qui à b associe gb^{-1}. Montrons que φ est bijective. Elle est surjective par définition de l'ensemble $\{gb^{-1} \,|\, b \in B\}$. Montrons qu'elle est injective. Soient b_1 et b_2 dans B tels que $\varphi(b_1) = \varphi(b_2)$. Alors ${gb_1}^{-1} = {gb_2}^{-1}$. En multipliant par g^{-1} à gauche (ou, car dans un groupe, tout élément est régulier), il vient : ${b_1}^{-1} = {b_2}^{-1}$. En multipliant par b_1 à gauche, on trouve $e = b_1{b_2}^{-1}$ et en multipliant par b_2 à droite, on trouve $b_2 = b_1$: φ est injective donc bijective. On en déduit que $\{gb^{-1} \,|\, b \in B\}$ et B ont le même cardinal. Si A et $\{gb^{-1} \,|\, b \in B\}$ sont disjoints, le cardinal de l'union est la somme des cardinaux donc est égal à $\text{card}(A) + \text{card}(B) > \text{card}(G)$ ce qui est absurde puisque l'union est incluse dans G : les deux ensembles ne sont pas disjoints.
2. Soit $g \in G$. Soit a dans l'intersection (non vide d'après ce qui précède). Alors $a \in A$ et il existe $b \in B$ tel que $a = gb^{-1}$ donc, en multipliant par b à droite, on obtient : $g = ab$ donc $g \in AB$. En d'autres termes, $G \subset AB$ et l'inclusion réciproque étant évidente, on a l'égalité voulue.

Exercice 31 : ✪✪✪ Soit G un groupe et soient H et K deux sous-groupes de G. On pose $HK = \{hk \,|\, (h,k) \in H \times K\}$: c'est donc l'ensemble des produits d'un élément de H par un élément de K (dans cet ordre).

1. Montrer que HK est un sous-groupe de G si et seulement si $HK = KH$, KH étant défini de façon analogue.
2. (a) Soient h_1 et h_2 deux éléments de H et k_1 et k_2 deux éléments de K. Montrer que $h_1k_1 = h_2k_2$ si et seulement s'il existe $x \in H \cap K$ tel que $h_2 = h_1x$ et $k_2 = x^{-1}k_1$.
   (b) On suppose que G est fini. Montrer que $\text{card}(HK) \times \text{card}(H \cap K) = \text{card}(H) \times \text{card}(K)$.

Correction :

1. HK est évidemment non vide car H et K sont non vides (ce sont des sous-groupes de G). Plus précisément, $e \in H$ et $e \in K$ donc $e * e = e \in HK$. Ainsi, HK est un sous-groupe de G si et seulement si HK est stable par produit (i.e. la loi de G) et par inverse.

   Supposons que HK soit un sous-groupe de G, et soit $g \in HK$. HK étant un sous-groupe de G, il est stable par inverse donc $g^{-1} \in HK$. Il existe alors $h \in H$ et $k \in K$ tels que $g^{-1} = hk$ si bien que $g = k^{-1}h^{-1} \in KH$: on a l'inclusion $HK \subset KH$, et par symétrie des rôles, on a l'inclusion réciproque donc l'égalité.

   Réciproquement, supposons que $HK = KH$ (ce qui ne veut pas dire que $hk = kh$ pour tous $h \in H$ et $k \in K$!) et prouvons que HK est un sous-groupe de G. Soient x_1 et x_2 deux éléments de HK : il existe h_1 et h_2 dans H et k_1 et k_2 dans K tels que $x_1 = h_1k_1$ et $x_2 = h_2k_2$ et donc $x_1x_2 = h_1(k_1h_2)k_2$ (la loi est associative). Or, $KH = HK$ donc $k_1h_2 \in HK$: il existe $h_3 \in H$ et $k_3 \in K$ tels que $k_1h_2 = h_3k_3$ si bien que $x_1x_2 = (h_1h_3)(k_3k_1)$. Or, H et K sont stables par produit (la loi de G) donc $h_1h_3 \in H$ et idem pour k_3k_1, si bien que $x_1x_2 \in HK$: HK est stable par produit. De plus, ${x_1}^{-1} = {k_1}^{-1}{h_1}^{-1}$. De même, il existe $h_4 \in H$ et $k_4 \in K$ tels que ${k_1}^{-1}{h_1}^{-1} = h_4k_4$ donc ${x_1}^{-1} = h_4k_4 \in HK$: HK est stable par inverse, donc c'est un sous-groupe de G.

2. (a) Supposons qu'il existe un tel x. Alors $h_2 = h_1 x$ donc, en multipliant à gauche par ${h_1}^{-1}$, il vient : $x = {h_1}^{-1} h_2$. De plus, $k_2 = x^{-1} k_1$ donc, de même : $x^{-1} = k_2 {k_1}^{-1}$ donc $x = k_1 {k_2}^{-1}$ (ne pas oublier de changer l'ordre). Dès lors, ${h_1}^{-1} h_2 = k_1 {k_2}^{-1}$. En multipliant à gauche par h_1 et à droite par k_2, on trouve bien que $h_2 k_2 = h_1 k_2$. Réciproquement, supposons que $h_1 k_1 = h_2 k_2$ et notons $x = {h_1}^{-1} h_2$ (d'après ce qui précède, si un tel x existe, c'est lui). Puisque $h_1 k_1 = h_2 k_2$, alors en multipliant par ${h_1}^{-1}$ à gauche et ${k_2}^{-1}$ à droite, on trouve que ${h_1}^{-1} h_2 = k_1 {k_2}^{-1}$ c'est-à-dire que

$$x = {h_1}^{-1} h_2 = k_1 {k_2}^{-1}$$

On en déduit que $x \in H$ (car H est stable par produit et par inverse puisque c'est un sous-groupe) et que $x \in K$ (pour les mêmes raisons) donc que $x \in H \cap K$, et on a bien $h_2 = h_1 x$ (en multipliant à gauche par h_1) et $k_2 = x^{-1} k_1$ (en multipliant à droite par k_2 et à gauche par x^{-1}).

(b) Soit

$$\varphi : \begin{cases} H \times K & \to & HK \\ (h,k) & \mapsto & hk \end{cases}$$

Alors φ est surjective par définition mais n'est pas forcément injective. Plus précisément, on vient de voir que, si $g \in HK$ et si (h_1, k_1) est un antécédent de g par φ, alors (h_2, k_2) est un autre antécédent de g si et seulement s'il existe $x \in H \cap K$ tel que $h_2 = h_1 x$ et $k_2 = x^{-1} k_1$. En d'autres termes, si on note $A = \varphi{-}1(\{g\})$ l'ensemble des antécédents de g par φ, alors la fonction

$$\psi : \begin{cases} H \cap K & \to & A \\ x & \mapsto & (h_1 x, x^{-1} k_1) \end{cases}$$

est surjective, c'est-à-dire que tous les antécédents de g sont de cette forme. Il est assez simple de voir que ψ est injective (si $\psi(x_1) = \psi(x_2)$ alors $h_1 x_1 = h_1 x_2$ donc $x_1 = x_2$) donc bijective, si bien que $\text{card}(A) = \text{card}(H \cap K)$. En d'autres termes, tout élément g de G a exactement $\text{card}(H \cap K)$ antécédents, et le lemme des bergers appliqué à φ permet de conclure.

Exercice 32 : ✪✪✪ Soient G un groupe fini, H un groupe (pas forcément fini) et $f : G \to H$ un morphisme de groupes. Montrer que $\text{card}(G) = \text{card}(\ker(f)) \times \text{card}(\text{Im}(f))$.

Correction : Tout d'abord, $\ker(f)$ est inclus dans G donc est fini (une partie d'un ensemble fini est finie) et $\Im(f)$ est finie car $f : G \to \Im(f)$ est surjective (si E est fini et $f : E \to F$ est surjective alors F est fini, cf. chapitre précédent). On va raisonner comme dans l'exercice précédent. Soit $y \in \Im(f)$ et soit $x_1 \in G$ un antécédent de G. Soit enfin $x_2 \in G$. Alors (on note e le neutre de H et on utilise plusieurs fois le fait que f est un morphisme) :

$$\begin{aligned} x_2 \text{ est un antécédent de } y &\iff f(x_2) = y \\ &\iff f(x_2) = f(x_1) \\ &\iff f(x_2) f(x_1)^{-1} = e \\ &\iff f\left(x_2 * {x_1}^{-1}\right) = e \\ &\iff x_2 * {x_1}^{-1} \in \ker(f) \\ &\iff \exists x \in \ker(f), x_2 * {x_1}^{-1} = x \\ &\iff \exists x \in \ker(f), x_2 = x * x_1 \end{aligned}$$

Dès lors, si on note A l'ensemble des antécédents de y par f, l'application

$$\varphi : \begin{cases} \ker(f) & \to & A \\ x & \mapsto & x * x_1 \end{cases}$$

est surjective, et on montre comme ci-dessus qu'elle est injective donc bijective : $\text{card}(A) = \text{card}(\ker(f))$. On en déduit que tout élément de $\Im(f)$ admet exactement $\text{card}(\ker(f))$ antécédents, et on conclut à l'aide du lemme des bergers.

2.6 Quelques groupes classiques

Exercice 33 - Centre d'un groupe : ✪✪ Soit G un groupe. On rappelle que le centre de G est l'ensemble $Z(G) = \{x \in G \,|\, \forall y \in G, xy = yx\}$ c'est-à-dire l'ensemble des éléments qui commutent avec tout le monde.

1. Montrer que si $f : G \to G$ est un automorphisme, alors $f(Z(G)) = Z(G)$.
2. Soit H un sous-groupe de G. Y a-t-il une inclusion entre $Z(H)$ et $Z(G) \cap H$? Montrer, à l'aide de l'exercice 23, qu'il n'y a pas forcément égalité.

Correction :

1. Montrons le résultat par double inclusion. Soit $y \in f(Z(G))$ et prouvons que $y \in Z(G)$, c'est-à-dire qu'il faut prouver que y commute avec tout le monde. Soit donc $x \in G$, et prouvons que $xy = yx$. $y \in f(Z(G))$ donc il existe $a \in Z(G)$ tel que $y = f(a)$. f étant un automorphisme, elle est surjective donc il existe $b \in G$ tel que $x = f(b)$. f étant un morphisme, $yx = f(a)f(b) = f(ab)$. Or, $a \in Z(G)$ donc a commute avec b si bien que

$$\begin{aligned} yx &= f(ba) \\ &= f(b)f(a) \\ &= xy \end{aligned}$$

   c'est-à-dire que $y \in Z(G)$: d'où l'inclusion $f(Z(G)) \subset Z(G)$. Prouvons l'inclusion réciproque : soit $y \in Z(G)$. f étant surjective, il existe $x \in G$ tel que $y = f(x)$. Prouvons donc que $x \in Z(G)$ c'est-à-dire que x commute avec tout le monde. Soit $z \in G$. f étant un morphisme, $f(xz) = f(x)f(z) = yf(z)$. Or, $y \in Z(G)$ donc $yf(z) = f(z)y$ si bien que

$$\begin{aligned} f(xz) &= f(z)y \\ &= f(z)f(x) \\ &= f(zx) \end{aligned}$$

   et f est injective donc $xz = zx : x \in Z(G)$ et donc $y = f(x) \in f(Z(G))$, d'où l'inclusion réciproque, d'où l'égalité.
2. L'inclusion $Z(G) \cap H \subset Z(H)$ est immédiate : un élément de $Z(G) \cap H$ est un élément de H qui commute avec tous les éléments de G, donc il commute en particulier avec tous les éléments de H. Prouvons que l'inclusion réciproque est fausse en général. Il faut taper dans le non abélien pour que ça ait des chances de marcher, car dans un groupe abélien, le centre est le groupe tout entier. Plaçons-nous dans S_E avec E de cardinal au moins 3 si bien que, d'après l'exercice 23, $S_E = \{\mathrm{Id}_E\}$. Soient a et b deux éléments distincts de E et soit g la fonction qui échange a et b, c'est-à-dire que $g(x) = x$ pour tout $x \neq a, b$, $g(a) = b$ et $g(b) = a$. Alors $H = \{\mathrm{Id}_E; g\}$ est un sous-groupe de S_E (c'est le groupe engendré par g). En effet, il est non vide, stable par composition et stable par symétrique (car g est son propre symétrique, toujours pour la composition). H est abélien car le neutre (l'identité ici) commute avec tout le monde donc $Z(H) = H$ mais $Z(S_E) \cap H = \{\mathrm{Id}_E\}$: l'inclusion peut être stricte.

Exercice 34 - Sous-groupes distingués : ✪✪ Soit G un groupe et soit H un sous-groupe de G. Si $x \in G$, on note $xH = \{xh \,|\, h \in H\}$, et on définit de façon analogue Hx et xHx^{-1}.

1. Montrer que les trois conditions suivantes sont équivalentes :

   - $\forall x \in G, xH = Hx$.
   - $\forall x \in G, xHx^{-1} = H$.
   - $\forall x \in G, \forall h \in H, xhx^{-1} \in H$.

   On dit qu'un sous-groupe de G vérifiant ces conditions est un sous-groupe distingué de G.
2. Montrer que si G est commutatif, tout sous-groupe de G est distingué dans G.
3. Soit $f : G_1 \to G_2$ un morphisme de groupes. Montrer que $\ker(f)$ est distingué dans G_1.
4. Montrer que $Z(G)$, le centre de G, est distingué dans G.
5. On suppose dans cette question que G est fini et que H est un sous-groupe d'indice 2 de G, c'est-à-dire que $\mathrm{card}(H) = \mathrm{card}(G)/2$. Montrer que H est distingué dans G. On pourra commencer par prouver que si $x \notin H$, G est l'union disjointe de H et de xH.

Correction :

1. Si on les note $1, 2, 3$, prouvons que $1 \Rightarrow 2, 2 \Rightarrow 3$ et $3 \Rightarrow 1$.

   Supposons 1 et prouvons 2. Soit $x \in G$. Prouvons que $xHx^{-1} = H$ par double inclusion. Soit $h \in H$. Alors $hx \in Hx$ et $xH = Hx$ par hypothèse (ce qui ne veut pas dire que $xh = hx$!) donc il existe $h' \in H$ tel que $hx = xh'$ si bien que

(en multipliant par x^{-1} à droite) $h = xh'x-1 \in xHx^{-1}$. Réciproquement, soit $y \in xHx^{-1}$: il existe donc $h \in H$ tel que $y = xhx^{-1}$. De même, il existe h' tel que $xh = h'x$ si bien que $y = h'xx^{-1} = h' \in H$. D'où l'inclusion réciproque, d'où l'égalité.

L'implication $2 \Rightarrow 3$ étant évidente (c'est l'inclusion $xHx^{-1} \subset H$ qui est vraie par hypothèse), prouvons que $3 \Rightarrow 1$. Supposons donc 3 et prouvons 1 : soit $x \in G$, prouvons que $xH = Hx$. Soit $g \in xH$: il existe donc $h \in H$ tel que $g = xh$. En multipliant par x^{-1} à droite : $gx^{-1} = xhx^{-1}$ qui est un élément de H par hypothèse (on a supposé 3 vraie). Il existe donc $h' \in H$ tel que $gx^{-1} = h'$ donc $g = h'x \in HX$: d'où l'inclusion $xH \subset Hx$. L'inclusion réciproque est analogue et laissée en exercice.

2. Supposons G commutatif. Soit H un sous-groupe de G et prouvons la propriété 3 ci-dessus (c'est la seule qui ne demande pas de prouver deux inclusions, c'est la plus simple à manipuler). Soit $x \in G$ et soit $h \in H$. Le groupe étant abélien, $xhx^{-1} = hxx^{-1} = h \in H$, H est distingué.
3. Soit $x \in \ker(f)$ et soit $h \in \ker(f)$. f étant un morphisme, $f(xhx^{-1}) = f(x)f(h)f(x)^{-1}$. Or, $h \in \ker(f)$ donc $f(h) = e_2$ (le neutre de G_2) si bien que

$$\begin{aligned} f(xhx^{-1}) &= f(x)e_2f(x)^{-1} \\ &= f(x)f(x)^{-1} \\ &= e_2 \end{aligned}$$

c'est-à-dire que $xhx^{-1} \in \ker(f)$: le groupe est distingué.

4. Soit $x \in G$ et soit $h \in Z(G)$. Montrons que $xhx^{-1} \in Z(G)$, c'est-à-dire que xhx^{-1} commute avec tout le monde. Soit donc $y \in G$. Rappelons que $h \in Z(G)$ donc h commute avec tout le monde.

$$\begin{aligned} xhx^{-1}y &= xx^{-1}hy \\ &= ehy \\ &= hy \end{aligned}$$

et

$$\begin{aligned} yxhx^{-1} &= yhxx^{-1} \\ &= yh \\ &= hy \end{aligned}$$

puisque h et y commutent. Finalement, $xhx^{-1}y = yxhx^{-1}$ donc $xhx^{-1} \in Z(G)$, $Z(G)$ est distingué.

5. Pour commencer, soit $x \notin H$. Supposons qu'il existe $y \in H \cap xH$. Alors il existe $h \in H$ tel que $y = xh$ donc tel que $x = yh^{-1}$. Or, $y \in H$ et H est un sous-groupe de G donc stable par produit et par inverse : $x \in H$, ce qui est absurde. L'intersection est donc vide, l'union est disjointe. En particulier, $\text{card}(H \cup xH) = \text{card}(H) + \text{card}(xH)$. Or, l'application $h \mapsto xh$ est une bijection de H dans xH (surjective par définition, et injective car tout élément est régulier, donc si $xh_1 = xh_2$ alors $h_1 = h_2$) donc $\text{card}(xH) = \text{card}(H)$. On en déduit que $\text{card}(H \cup xH) = 2\text{card}(H) = \text{card}(G)$ donc $H \cup xH = G$.

Prouvons à présent que H est distingué. Soit $h \in H$ et soit $x \in G$, et prouvons que $xhx^{-1} \in H$. Si $x \in H$, c'est terminé puisque H est un sous-groupe de G. Sinon, d'après ce qui précède, $xhx^{-1} \in G = H \cup xH$. Supposons par l'absurde que $xhx^{-1} \in xH$: il existe $h' \in H$ tel que $xhx^{-1} = xh'$ donc (tout élément d'un groupe est régulier, ou en multipliant par x^{-1} à gauche) $hx^{-1} = h'$ si bien que $h'^{-1}h = x \in H$ ce qui est exclu. En conclusion, $xhx^{-1} \in H$, H est distingué.

Exercice 35 - Théorème de Cayley : ✪✪ Soit G un groupe. En considérant la fonction φ_g de G dans lui-même définie par $\varphi_g : x \mapsto gx$, montrer que G est isomorphe à un sous-groupe de S_G. En déduire que si G est un groupe à n éléments, alors G est isomorphe à un sous-groupe de S_n. On pourra utiliser l'exercice 23.

Correction : Prouvons que $f : g \mapsto \varphi_g$ est une injection de G dans S_G. Tout d'abord, f est bien à valeurs dans S_G puisque, pour tout g, φ_g est bijective comme on le montre de même que précédemment. Soient $g_1 \neq g_2$ deux éléments de g. Alors $\varphi_{g_1}(e) = g_1 \neq g_2 = \varphi_{g_2}(e)$: les deux fonctions φ_{g_1} et φ_{g_2} sont différentes en e donc ne sont pas la même fonction, c'est-à-dire que $f(g_1) \neq f(g_2)$: f est injective. Prouvons à présent que f est un morphisme de groupes. Soient g_1 et g_2 deux éléments (pas forcément distincts) de G. Soit $x \in G$. Par associativité de la loi sur G :

$$\begin{aligned}\varphi_{g_1g_2}(x) &= g_1g_2x\\ &= g_1(g_2x)\\ &= \varphi_{g_1}(g_2x)\\ &= \varphi_{g_1}\circ\varphi_{g_2}(x)\end{aligned}$$

et cette égalité est valable pour tout $x \in G$ donc $\varphi_{g_1g_2} = \varphi_{g_1g_2} \circ \varphi_{g_1g_2}$, c'est-à-dire que $f(g_1g_2) = f(g_1) \circ f(g_2)$: f est bien un morphisme de groupes, et puisque f est injective, c'est une bijection sur son image, c'est-à-dire que G et $\Im(f)$ sont isomorphes, ce qui est le résultat voulu puisque $\Im(f)$ est un sous-groupe de S_G (l'image d'un morphisme est un sous-groupe). Soit à présent G un groupe à n éléments. Alors G et $[\![\,1\,;\,n\,]\!]$ sont en bijection (car ont le même cardinal) donc, d'après l'exercice 23, S_G et S_n sont isomorphes, c'est-à-dire qu'il existe $\psi : S_G \to S_G$ isomorphisme, et $\psi \circ f$ est alors un morphisme injectif de G dans S_n et on conclut de la même façon.

Remarque : Ainsi, un groupe à 10 éléments est isomorphe à un sous-groupe de S_{10}. On pourrait se dire que, pour trouver tous les groupes à 10 éléments (à isomorphisme près), il suffit de trouver tous les sous-groupes de S_{10} à 10 éléments... Sauf que S_{10} est tellement énorme ($10! = 3628800$ éléments !) que ce n'est pas du tout réalisable en pratique !

2.7 Sous-groupes de $\mathbb{R}$

Exercice 36 : ✪✪

1. Montrer que $G = \{n + 2\pi p \,|\, (n,p) \in \mathbb{Z}^2\}$ est dense dans $\mathbb{R}$. On pourra utiliser le fait que π est irrationnel.
2. En déduire que l'ensemble $\{\cos(n) \,|\, n \in \mathbb{N}\}$ est dense dans $[\,-1\,;1\,]$.

1. Prouvons que G est un sous-groupe de $\mathbb{R}$ (pour la loi + évidemment).
   - $0 = 0 + 2\pi \times 0 \in \mathbb{Z}$: G est non vide.
   - Soient x_1 et x_2 deux éléments de G : il existe $(n_1, n_2, p_1, p_2) \in \mathbb{Z}^4$ tel que $x_1 = n_1 + 2\pi p_1$ et $x_2 = n_2 + 2\pi p_2$. Alors $x_1 + x_2 = (n_1 + n_2) + 2\pi(p_1 + p_2) \in G$ car $n_1 + n_2$ et $p_1 + p_2$ appartiennent à $\mathbb{Z}$: G est stable par somme.
   - De plus, $-x_1 = (-n_1) + 2\pi \times (-p_1) \in G$ car $-n_1$ et $-p_1$ appartiennent à $\mathbb{Z}$: G est stable par inverse.

   Finalement, G est un sous-groupe de $\mathbb{R}$. Pour prouver qu'il est dense, il suffit de prouver qu'il n'est pas de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}$. Raisonnons par l'absurde et supposons qu'il existe $\alpha \in \mathbb{R}$ tel que $G = \alpha\mathbb{Z}$. $1 = 1 + 2\pi \times 0 \in G$ donc il existe $k \in \mathbb{Z}$ tel que $1 = \alpha k$, et $2\pi = 0 + 2\pi \times 1 \in G$ donc il existe $n \in \mathbb{Z}$ tel que $2\pi = \alpha n$. Or, $\alpha k = 1$ donc k est non nul et $\alpha = 1/k$ si bien que $\pi = n/2k \in \mathbb{Q}$. Absurde : G n'est pas de la forme $\alpha\mathbb{Z}$ donc est dense dans $\mathbb{R}$.
2. Soient $x < y$ deux éléments de $[\,-1\,;1\,]$ et soit $z \in \,]\,x\,;y\,[$ (on peut prendre par exemple $(x+y)/2$). Soit enfin $a = \text{Arccos}(z)$. L'ensemble G étant dense dans $\mathbb{R}$, par caractérisation de la borne supérieure, il existe une suite $(x_k)_{k\in\mathbb{N}}$ d'éléments de G qui converge vers α. Or, la fonction cos est continue donc $\cos(x_k) \xrightarrow[k\to+\infty]{} \cos(\alpha) = z$ donc $\cos(x_k) \in \,]\,x\,;y\,[$ pour k assez grand. Or, pour tout k, il existe n_k et p_k dans $\mathbb{Z}$ tels que $x_k = n_k + 2\pi p_k$ et donc

$$\cos(x_k) = \cos(n_k) \in \{\cos(n) \,|\, n \in \mathbb{N}\}$$

   c'est-à-dire qu'il existe un élément de cet ensemble dans $]\,x\,;y\,[$, d'où la densité cherchée.

Exercice 37 : ✪✪✪ Montrer qu'il existe une puissance de 2 (positive ou négative) qui commence par votre date de naissance. Pour les puissances négatives, on dit qu'elles commencent au premier chiffre non nul (par exemple $1/4 = 0.25$ commence par un 2).

Correction : Essayons de traduire l'énoncé d'un point de vue mathématique. Notons d la date de naissance. Un nombre commence par d s'il s'écrit sous la forme $da_1a_2\ldots a_n$ où les a_i sont des entiers (par exemple, un nombre qui commence par 1022002 s'écrit sous la forme $1022002a_1a_2\ldots a_n$) donc s'il est compris entre un terme de la forme $d0\ldots0 = d \times 10^n$ et $d9\ldots9 = (d+1) \times 10^n - 1$ (un nombre commence par 1022002 s'il est compris entre 1022002 s'il est compris entre $102200200\ldots0$ et $102200300\ldots0$), donc s'il est supérieur ou égal à $b \times 10^n$ et strictement inférieur à $b \times 10^{n+1}$. D'où les équivalences suivantes (attention à la rédaction !) :

$$\begin{aligned}\text{Il existe une puissance de 2 qui commence par } d &\iff \exists (k,n) \in \mathbb{Z}^2, d \times 10^n \leq 2^k < (d+1) \times 10^n\\ &\iff \exists (k,n) \in \mathbb{Z}^2, n\ln(10) + \ln(d) \leq k\ln(2) < n\ln(10) + \ln(d+1)\\ &\iff \exists (k,n) \in \mathbb{Z}^2, \ln(d) \leq k\ln(2) - n\ln(10) < \ln(d+1)\\ &\iff \exists (k,n) \in \mathbb{Z}^2, \frac{\ln(d)}{\ln(10)} \leq k\frac{\ln(2)}{\ln(10)} - n < \frac{\ln(d+1)}{\ln(10)}\end{aligned}$$

Il suffit de prouver que $G = \left\{ k\frac{\ln(2)}{\ln(10)} - n \,|\, (k,n) \in \mathbb{Z}^2 \right\}$ est dense dans $\mathbb{R}$, ce qu'on fait de même que dans l'exercice précédent, en utilisant le fait que $\ln(2)/\ln(10)$ est irrationnel. En effet, s'il est rationnel, alors il existe a et b dans $\mathbb{N}^*$ (ce nombre est strictement positif) tels que $\ln(2)/\ln(10) = a/b$ donc $b\ln(2) = a\ln(10)$ si bien que $2^b = 10^a$. En particulier, puisque $a \geq 1$, 2^b est divisible par 5 ce qui est absurde, d'où la conclusion voulue. On voit que l'argument clef est que 2^b n'est pas une puissance de 10, donc cela marche avec n'importe quelle puissance à part les puissances de 10, pour lesquelles il est immédiat que cela ne fonctionne pas puisqu'une puissance de 10 s'écrit forcément $10000\ldots0$.

2.8 Un problème de groupes complet (découpé en trois exercices)

Exercice 38 - Produit semi-direct : ✪✪✪

1. Si G est un groupe, on note $\mathrm{Aut}(G)$ l'ensemble de ses automorphismes. Montrer que $(\mathrm{Aut}(G), \circ)$ est un groupe.
2. Soient H et K deux groupes et $\varphi : K \to \mathrm{Aut}(H)$ un morphisme de groupe. On munit $H \times K$ de la loi interne $*$ définie par :

$$(h_1, k_1) * (h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2)$$

   Montrer que $(H \times K, *)$ est un groupe. Ce groupe est appelé produit semi-direct de H et K relativement à φ et est noté $H \rtimes_\varphi K$ ou $H \rtimes K$ s'il n'y a aucune ambiguïté sur φ.
3. Expliquer pourquoi le produit semi-direct est une généralisation du produit direct.

Correction :

1. On sait que S_G, l'ensemble des bijections de G dans lui-même, est un groupe pour la loi $\circ$ (cf. cours). Il suffit donc de prouver que $\mathrm{Aut}(G)$ est un sous-groupe de S_G. Il est non vide car convient l'identité, est stable par composition car une composée de morphismes est un morphisme, et une composée de bijections est une bijections, donc une composée d'automorphismes est un automorphisme, et enfin il est stable par inverse puisque la réciproque d'un morphisme bijectif est un morphisme (toujours bijectif). On en déduit le résultat voulu.
2. Ici, par contre, il faut tout démontrer. Précisons que la notation $\varphi(k_1)(h_2)$ n'est pas fausse puisque $\varphi(k_1)$ est, par définition, un automorphisme de H donc est en particulier une fonction de H dans H, qu'on peut évaluer en un élément de H.
   - Prouvons que la loi est associative. Soient $(h_1, k_1), (h_2, k_2)$ et (h_3, k_3) trois éléments de $H \times K$. Tout d'abord :

$$\begin{aligned}(h_1, k_1) * ((h_2, k_2) * (h_3, k_3)) &= (h_1, k_1) * (h_2\varphi(k_2)(h_3), k_2k_3) \\ &= (h_1\varphi(k_1)\left[h_2\varphi(k_2)(h_3)\right], k_1(k_2k_3)) \\ &= (h_1\varphi(k_1)\left[h_2\varphi(k_2)(h_3)\right], k_1k_2k_3)\end{aligned}$$

     puisque la loi du groupe est associative (on peut donc enlever les parenthèses dans la deuxième coordonnée). De plus :

$$\begin{aligned}((h_1, k_1) * (h_2, k_2)) * (h_3, k_3) &= (h_1\varphi(k_1)(h_2), k_1k_2) * (h_3, k_3) \\ &= (h_1\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3), (k_1k_2)k_3) \\ &= (h_1\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3), k_1k_2k_3)\end{aligned}$$

     Les deuxièmes coordonnées étant les mêmes, il suffit de prouver que les premières coordonnées sont aussi égales, c'est-à-dire que :

$$h_1\varphi(k_1)\left[h_2\varphi(k_2)(h_3)\right] = h_1\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3)$$

     Il suffit donc de prouver que

$$\varphi(k_1)\left[h_2\varphi(k_2)(h_3)\right] = \varphi(k_1)(h_2)\varphi(k_1k_2)(h_3)$$

     Précisons que le membre de gauche est la fonction (plus précisément, l'automorphisme de H) $\varphi(k_1)$ qu'on évalue en $h_2\varphi(k_2)h_3$ qui est bien un élément de H. Puisque $\varphi(k_1)$ est un morphisme, on peut « casser » ce qu'il y a à l'intérieur, c'est-à-dire que

$$\varphi(k_1)\left[h_2\varphi(k_2)(h_3)\right] = \varphi(k_1)(h_2) \times \varphi(k_1)\left[\varphi(k_2)(h_3)\right]$$

     où l'on a noté $\times$ la loi du groupe G. En d'autres termes (rappelons que $\varphi(k_2)$ est un automorphisme de H donc en particulier une fonction) :

$$\varphi(k_1)\left[h_2\varphi(k_2)(h_3)\right] = \varphi(k_1)(h_2) \times \varphi(k_1) \circ \varphi(k_2)(h_3)$$

Or, φ est un morphisme de K dans $\mathrm{Aut}(H)$ donc $\varphi(k_1) \circ \varphi(k_2) = \varphi(k_1k_2)$ si bien que

$$\varphi(k_1)\left[h_2\varphi(k_2)(h_3)\right] = \varphi(k_1)(h_2) \times \varphi(k_1k_2)(h_3)$$

ce qui est le résultat voulu : la loi $*$ du produit semi-direct est associative.

- Prouvons qu'il y a un élément neutre. On cherche donc un élément (h_1, k_1) tel que, pour tout $(h, k) \in H \times K$, $(h, k) * (h_1, k_1) = (h_1, k_1) * (h, k) = (h, k)$. Or, si $(h, k) \in H \times K$,

$$(h_1, k_1) * (h, k) = (h_1\varphi(k_1)(h), k_1k)$$

donc on cherche h_1, k_1 tels que $h_1\varphi(k_1)(h) = h$ et $k_1k = k$: prenons $k_1 = e_K$ (le neutre de K) et $h_1 = e_H$ (le neutre de H). Dès lors, $k_1k = e_Kk = k$. De plus, φ étant un morphisme de K dans $\mathrm{Aut}(H)$, $\varphi(e_K)$ est le neutre de $\mathrm{Aut}(H)$ donc Id_H si bien que $\varphi(k_1)(h) = h$ et donc $h_1\varphi(k_1)(h) = h$. Finalement, on a bien $(e_H, e_K)*(h, k) = (h, k)$. Enfin,

$$(h, k) * (e_H, e_K) = (h\varphi(k)(e_H), ke_K)$$

Il est immédiat que $ke_K = k$. De plus, $\varphi(k)$ est un automorphisme de H donc $\varphi(k)(e_H) = e_H$ si bien qu'on a aussi $(h, k) * (e_H, e_K) = (h, k)$: (e_H, e_K) est un élément neutre.

- Prouvons enfin que tout élément admet un symétrique pour la loi $*$. Soit $(h, k) \in H \times K$. On cherche (h_1, k_1) tel que $(h, k) * (h_1, k_1) = (h_1, k_1) * (h, k) = (e_H, e_K)$. Or, on a :

$$(h, k) * (h_1, k_1) = (h\varphi(k)(h_1), kk_1) \qquad \text{et} \qquad (h_1, k_1) * (h, k) = (h_1\varphi(k_1)(h), k_1k)$$

Posons tout d'abord $k_1 = k^{-1}$ (K étant un sous-groupe de G, k admet un inverse dans K). Cherchons à présent h_1. On a $\varphi(k_1) = \varphi\left(k^{-1}\right)$ si bien qu'on veut avoir

$$h_1\varphi(k^{-1})(h) = e_H$$

Posons donc $h_1 = \left(\varphi(k^{-1})(h)\right)^{-1} = \varphi(k^{-1})\left(h^{-1}\right)$ puisqu'on a un morphisme (attention de ne pas simplifier les -1, l'un porte sur h et l'autre sur k). Prouvons donc que $(\varphi(k^{-1})(h^{-1}), k^{-1})$ convient. D'une part :

$$(h, k) * (\varphi(k^{-1})(h^{-1}), k^{-1}) = (h\varphi(k)\left[\varphi(k^{-1})(h^{-1})\right], kk^{-1})$$

Rappelons que $\varphi(k)$ et $\varphi(k^{-1})$ sont des fonctions donc cette égalité se réécrit :

$$(h, k) * (\varphi(k^{-1})(h^{-1}), k^{-1}) = (h\varphi(k) \circ \varphi(k^{-1})(h^{-1}), kk^{-1})$$

Or, φ est un morphisme donc $\varphi(k) \circ \varphi(k^{-1}) = \varphi(kk^{-1}) = \varphi(e_K) = \mathrm{Id}_H$ comme on l'a déjà vu, si bien que

$$\begin{aligned}(h, k) * (\varphi(k^{-1})(h^{-1}), k^{-1}) &= (hh^{-1}, kk^{-1}) \\ &= (e_H, e_K)\end{aligned}$$

Enfin :

$$(\varphi(k^{-1})(h^{-1}), k^{-1}) * (h, k) = (\varphi(k^{-1})(h^{-1})\varphi(k^{-1})(h), k^{-1}k)$$

$\varphi(k^{-1})$ est un morphisme (c'est un automorphisme de H),

$$\begin{aligned}(\varphi(k^{-1})(h^{-1}), k^{-1}) * (h, k) &= (\varphi(k^{-1})(h^{-1}h), k^{-1}k) \\ &= (\varphi(k^{-1})(e_H), e_K) \\ &= (e_H, e_K)\end{aligned}$$

ce qui permet de conclure.

En conclusion, on a bien un groupe.

3. Le produit direct n'est rien d'autre que le produit semi direct obtenu avec $\varphi : k \mapsto \mathrm{Id}_H$ donc est un cas particulier de produit semi-direct.

Exercice 39 - Un critère bien pratique : ✪✪✪ Soit G un groupe. On suppose que G admet deux sous-groupes H et K vérifiant les conditions suivantes :

- H est distingué dans K (cf. exercice 34)

- $H \cap K = \{e\}$.
- $G = HK$ (cf. exercice 31).

1. Montrer que pour tout $k_1 \in K$, $f_{k_1} : h \mapsto k_1 h {k_1}^{-1}$ est un automorphisme de H. On note cet automorphisme morphisme $\varphi(k_1)$.
2. Montrer que G est isomorphe au produit semi-direct $H \rtimes_\varphi K$ où φ est définie par :

$$\varphi : \begin{cases} K & \longrightarrow & \mathrm{Aut}(H) \\ k_1 & \longmapsto & \varphi(k_1) \end{cases}$$

On vérifiera bien que φ est un morphisme de groupes.

Correction :

1. Soit $k_1 \in K$. Soient h_1 et h_2 deux éléments de H.

$$\begin{aligned} f_{k_1}(h_1 h_2) &= k_1 h_1 h_2 {k_1}^{-1} \\ &= k_1 h_1 {k_1}^{-1} k_1 h_2 {k_1}^{-1} \\ &= f_{k_1}(h_1) f_{k_1}(h_2) \end{aligned}$$

donc f_{k_1} est bien un morphisme de groupes. Il va bien de H dans H car H est distingué (cf. exercice 34). Prouvons enfin qu'il est bijectif. Soient h_1 et h_2 tels que $f_{k_1}(h_1) = f_{k_1}(h_2)$. Alors $k_1 h_1 {k_1}^{-1} = k_1 h_2 {k_2}^{-1}$. Tout élément dans un groupe étant régulier, $h_1 = h_2$: f_{k_1} est injective. Enfin, si $h \in H$, alors on cherche h_1 tel que $k_1 h_1 {k_1}^{-1} = h$. Alors $h_1 = {k_1}^{-1} h k_1$ convient et appartient bien à H car H est distingué. En d'autres termes, c'est un antécédent de h donc f_{k_1} est surjective donc bijective : c'est bien un automorphisme de H.

2. Montrons tout d'abord que φ est un morphisme de groupes. Soient k_1 et k_2 deux éléments de K. Alors $\varphi(k_1 k_2) = f_{k_1 k_2}$ c'est-à-dire que c'est la fonction $h \mapsto k_1 k_2 h (k_1 k_2)^{-1} = k_1 k_2 h {k_2}^{-1} {k_1}^{-1}$. Or, pour tout $h \in H$,

$$\begin{aligned} \varphi(k_1) \circ \varphi(k_2)(h) &= \varphi(k_1)(k_2 h {k_2}^{-1}) \\ &= k_1 k_2 h {k_2}^{-1} {k_1}^{-1} \\ &= \varphi(k_1 k_2)(h) \end{aligned}$$

et ceci étant valable pour tout h, cela signifie que les deux fonctions $\varphi(k_1 k_2)$ et $\varphi(k_1) \circ \varphi(k_2)$ sont égales : φ est bien un morphisme de groupes. Soit enfin la fonction

$$\psi : \begin{cases} H \times K & \to & G \\ (h, k) & \mapsto & hk \end{cases}$$

et prouvons que ψ est un isomorphisme entre $(H \times K, *)$, c'est-à-dire le produit semi-direct $H \rtimes_\varphi K$, et G. Puisque $G = HK$, ψ est surjective. Prouvons que c'est un morphisme de groupes (cela nous permettra de prouver ensuite l'injectivité plus simplement, avec le critère du noyau). Soient (h_1, k_1) et (h_2, k_2) deux éléments de $H \times K$.

$$\begin{aligned} \psi((h_1, k_1) * (h_2, k_2)) &= \psi(h_1 \varphi(k_1)(h_2), k_1 k_2) \\ &= h_1 \varphi(k_1)(h_2) k_1 k_2 \end{aligned}$$

Or, $\varphi(k_1)(h_2) = k_1 h_2 {k_1}^{-1}$ si bien que :

$$\begin{aligned} \psi((h_1, k_1) * (h_2, k_2)) &= h_1 k_1 h_2 {k_1}^{-1} k_1 k_2 \\ &= h_1 k_1 h_2 k_2 \\ &= \psi(h_1, k_1) \psi(h_2, k_2) \end{aligned}$$

c'est-à-dire que ψ est bien un morphisme de groupes. Prouvons enfin qu'elle est injective. Soit $(h, k) \in \ker(\psi)$. Alors $hk = e$ si bien que $h = k^{-1}$. Or, $h \in H$ et $k^{-1} \in K$ donc h est égal à un élément de K donc il appartient aussi à K. Finalement, $h \in H \cap K = \{e\}$ si bien que $h = e$ et donc $k^{-1} = e$ donc $k = e$. On en déduit que $\ker(\psi) = \{(e, e)\}$ donc ψ est injective donc bijective : c'est un isomorphisme. Les deux groupes sont donc bien isomorphes.

Exercice 40 - Application à un certain type de groupes d'ordre 8 : ✪✪✪ On se donne dans cet exercice un groupe G à 8 éléments. On suppose qu'il existe $a \in G$ d'ordre 4 et $b \in G\backslash \mathrm{gr}(a)$ d'ordre 2. On pose enfin $H = \mathrm{gr}(a)$ et $K = \mathrm{gr}(b)$.

1. Montrer que H et K vérifient les conditions de l'exercice précédent. On pourra utiliser les exercices 31 et 34.
2. Rappeler pourquoi H est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ et K à $\mathbb{Z}/2\mathbb{Z}$. Dans la suite, quitte à raisonner comme dans l'exercice 20, on supposera donc que $H = \mathbb{Z}/4\mathbb{Z}$ et $K = \mathbb{Z}/2\mathbb{Z}$. On en déduit qu'il existe $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ tel que G soit isomorphe à $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.
3. En déduire qu'il existe exactement deux groupes non isomorphes vérifiant cette condition et donner leurs tables (on pourra utiliser l'exercice 68).

Remarque : Ici s'achève (presque) la recherche des groupes à 8 éléments (à isomorphisme près). Soit G un groupe d'ordre 8. L'ordre d'un élément de G divise 8 donc vaut $1, 2, 4$ ou 8. Plusieurs cas se présentent :

- Si G contient un élément d'ordre 8, alors G est cyclique et isomorphe à $\mathbb{Z}/8\mathbb{Z}$. On suppose dans la suite que G ne contient aucun élément d'ordre 8.
- Si G contient un élément a d'ordre 4 tel que $G\backslash \mathrm{gr}(a)$ contienne un élément d'ordre 2, alors G est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou un groupe non abélien qu'on note D_8 (et qu'on appelle le groupe diédral) d'après ce qui précède.
- Si G contient un élément a d'ordre 4 tel que $G\backslash \mathrm{gr}(a)$ ne contienne aucun élément d'ordre 2, alors G est isomorphe à $\mathbb{H}_8$ d'après le cours.
- Enfin, si G n'a que des éléments d'ordre 2 (hormis le neutre), G est abélien d'après l'exercice 18 et on peut montrer (mais ce n'est pas si simple que ça) que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

En conclusion, il n'existe que 5 groupes à 8 éléments à isomorphisme près : $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_8, $\mathbb{H}_8$ et $(\mathbb{Z}/2\mathbb{Z})^3$.

Correction :

1. H est d'ordre 4 donc est d'indice 2 dans G (c'est-à-dire que son cardinal est la moitié de celui de G). D'après l'exercice 34, il est distingué dans G. Puisque b est d'ordre 2, alors $K = \{e; b\}$ et $b \notin H$ par hypothèse donc $H \cap K = \{e\}$. Enfin, d'après l'exercice 31, puisque $H \cap K$ est de cardinal 1, alors $\mathrm{card}(HK) = \mathrm{card}(H) \times \mathrm{card}(K) = 8 = \mathrm{card}(G)$ si bien que $G = HK$: les groupes H et K vérifient bien les conditions de l'exercice précédent.
2. C'est du cours (enfin, au programme de deuxième année, pas de pression) : si x est d'ordre n, alors $\mathrm{gr}(x)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
3. D'après l'exercice 68, il y a deux endomorphismes de $\mathbb{Z}/4\mathbb{Z}$: l'identité, et la fonction f définie par : $f(\overline{0}) = \overline{0}, f(\overline{1}) = \overline{3}$, $f(\overline{2}) = \overline{2}$ et $f(\overline{3}) = \overline{1}$. Le morphisme $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ étant, justement, un morphisme, il envoie le neutre sur le neutre donc $\varphi(\overline{0}) = \mathrm{Id}_{\mathbb{Z}/4\mathbb{Z}}$ et, ensuite, il y a deux possibilités : soit $\varphi(\overline{1}) = \mathrm{Id}_E$, c'est-à-dire que φ est constante égale à Id_E, soit $\varphi(\overline{1}) = f$, l'autre automorphisme de $\mathbb{Z}/4\mathbb{Z}$. Il y a donc au plus deux groupes G (à isomorphisme près) vérifiant les conditions de l'exercice. Supposons que φ soit constante égale à $\mathrm{Id}_{\mathbb{Z}/4\mathbb{Z}}$. Alors le produit semi-direct $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ est en fait le produit direct (on peut appliquer la question 3 de l'exercice 38 ou le refaire à la main) c'est-à-dire que $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ muni de la loi produit c'est-à-dire que $(h_1, k_1) + (h_2, k_2) = (h_1 + h_2, k_1 + k_2)$ puisque $\varphi(k_1)(h_2) = \mathrm{Id}(h_2) = h_2$ (ici, la loi est notée additivement car on se place sur $\mathbb{Z}/4\mathbb{Z}$). On en déduit la table ci-dessous (rappelons que la première coordonnée est dans $\mathbb{Z}/4\mathbb{Z}$ et la deuxième dans $\mathbb{Z}/2\mathbb{Z}$ donc la première est prise modulo 4 et la deuxième modulo 2) :

$+$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{3},\overline{0})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$
$(\overline{2},\overline{0})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{2},\overline{1})$	$(\overline{2},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$
$(\overline{3},\overline{0})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$
$(\overline{3},\overline{1})$	$(\overline{3},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{2},\overline{0})$

Supposons à présent que φ soit l'autre morphisme de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$ c'est-à-dire que $\varphi(\overline{0}) = \mathrm{Id}_{\mathbb{Z}/4\mathbb{Z}}$ et $\varphi(\overline{1}) = f$ avec f la fonction vue précédemment. Donnons la table du groupe

$$G = \mathbb{Z}/4\mathbb{Z}\times = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

muni de la loi (encore une fois, la loi est notée additivement) :

$$(h_1, k_2) * (h_2, k_2) = (h_1 + \varphi(k_1)(h_2), k_1 + k_2)$$

Par exemple (rappelons que la première coordonnée est dans $\mathbb{Z}/4\mathbb{Z}$ et la deuxième dans $\mathbb{Z}/2\mathbb{Z}$ donc la première est prise modulo 4 et la deuxième modulo 2) :

$$\begin{aligned}(\overline{1},\overline{1}) * (\overline{1},\overline{1}) &= (\overline{1} + \varphi(\overline{1})(\overline{1}), \overline{1} + \overline{1}) \\ &= (\overline{1} + f(\overline{1}), \overline{0}) \\ &= (\overline{1} + \overline{3}, \overline{0}) \\ &= (\overline{0}, \overline{0})\end{aligned}$$

et idem pour les autres. D'où la table du groupe ci-dessous. Il y a donc au plus deux groupes : réciproquement, ce sont bien des groupes car on sait que les produits (directs ou semi-directs) sont des groupes, et ils sont non isomorphes car ils n'ont pas la même table (l'un est abélien et pas l'autre). Ouf !

$+$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{2},\overline{0})$
$(\overline{2},\overline{0})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{2},\overline{1})$	$(\overline{2},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{3},\overline{0})$
$(\overline{3},\overline{0})$	$(\overline{3},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{2},\overline{1})$
$(\overline{3},\overline{1})$	$(\overline{3},\overline{1})$	$(\overline{3},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{2},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$

3 Anneaux et corps

Exercice 41 : ✪ Montrer que l'ensemble des fonctions continues de $[\,0\,;1\,]$ dans $\mathbb{R}$ est un anneau (muni de l'addition et du produit des fonctions). Est-il intègre ?

Correction : Il suffit de prouver que c'est un sous-anneau de $\mathbb{R}^{[\,0\,;1\,]}$ (rappelons que si X est un ensemble quelconque et A un anneau, alors A^X est muni d'une structure d'anneau). L'ensemble $\mathscr{C}([\,0\,;1\,],\mathbb{R})$ est non vide (il contient la fonction nulle), stable par somme et par opposé (si f et g sont continues sur $[\,0\,;1\,]$, alors $f+g$ et $-f$ sont continues sur $[\,0\,;1\,]$) donc $\mathscr{C}([\,0\,;1\,],\mathbb{R})$ est un sous-groupe (pour l'addition) de $\mathbb{R}^{[\,0\,;1\,]}$. La fonction constante égale à 1 appartient évidemment à $\mathscr{C}([\,0\,;1\,],\mathbb{R})$ et cet ensemble est stable par produit : c'est donc un sous-anneau de $\mathbb{R}^{[\,0\,;1\,]}$ et en particulier c'est un anneau. Il n'est pas intègre car, si on note f la fonction nulle sur $[\,0\,;1/2\,]$ et égale à $x-1/2$ sur $[\,1/2\,;1\,]$, et g la fonction constante égale à 0 sur $[\,1/2\,;1\,]$ et égale à $1/2-x$ sur $[\,0\,;1/2\,]$, on a $f\times g=0$ alors que ni f ni g n'est la fonction nulle : l'anneau n'est pas intègre.

Exercice 42 : ✪ On considère l'anneau $A = \mathbb{R}^{[\,0\,;2\,]}$ muni de l'addition et du produit des fonctions (il n'est pas demandé de prouver que c'est effectivement un anneau). On note A_1 l'ensemble des éléments de A nuls sur $]\,1\,;2\,]$. Montrer que $(A_1,+,\times)$ est un anneau inclus dans A. Est-ce un sous-anneau de A ?

Correction : Il est non vide (contient la fonction nulle), stable par somme et par opposé donc c'est un sous-groupe de A (muni de la loi $+$). La multiplication est toujours associative et distributive par rapport à la somme. Enfin, la fonction φ constante égale à 1 sur $[\,0\,;1\,]$ et nulle sur $]\,1\,;2\,]$ (les fonctions ne sont pas forcément continues dans cet exercice) est un élément neutre sur A_1 : en effet, si $f\in A_1$, alors f est nulle sur $]\,1\,;2\,]$ donc, pour tout $x\in[\,0\,;2\,]$, soit $x\in[\,0\,;1\,]$, et alors $\varphi(x)=1$ si bien que $f(x)\times\varphi(x)=1$, et si $x\in]\,0\,;1\,]$, alors $f(x)=0$ donc $f(x)=f(x)\times\varphi(x)$: φ est neutre à droite donc neutre car le produit est commutatif. A_1 est bien un anneau inclus dans A mais ce n'est pas un sous-anneau puisque

le neutre n'est pas le même.

Exercice 43 : ✪ On note $\mathbb{Q}_i$ l'ensemble des rationnels dont le dénominateur (dans l'écriture irréductible) est impair. Montrer que $\mathbb{Q}_i$ est un anneau et donner ses éléments inversibles.

Correction : Montrons que c'est un sous-groupe de $\mathbb{Q}$ (pour la loi $+$). Il est non vide car contient $0 = 0/1$. Soient $r_1 = a_1/b_1$ et $r_2 = a_2/b_2$ (on écrit les rationnels sous forme irréductible) deux éléments de $\mathbb{Q}_i$: les entiers b_1 et b_2 sont donc impairs. Par conséquent, $-r_1 = -a_1/b_1 \in Q_i$, et

$$r_1 + r_2 \quad = \quad \frac{a_1b_2 + a_2b_1}{b_1b_2}$$

Le dénominateur de cette fraction, lorsqu'on la met sous forme irréductible, est un diviseur de b_1b_2 qui est impair (car produit de deux entiers impairs) donc est lui-même impair (les nombres impairs n'ont que des diviseurs impairs). On en déduit que $r_1 + r_2 \in \mathbb{Q}_i$: $\mathbb{Q}_i$ est stable par somme, c'est donc un sous-groupe de $\mathbb{Q}$. De plus, $1 = 1/1$ donc $1 \in \mathbb{Q}_i$. Enfin, $r_1r_2 = a_1a_2/b_1b_2$ qui appartient à $\mathbb{Q}_i$ pour la même raison que ci-dessus (que la fraction soit ou non irréductible) : $\mathbb{Q}_i$ est stable par produit, c'est donc un sous-anneau de $\mathbb{Q}$, en particulier c'est un anneau. r_1 est inversible si et seulement r_1 est non nul et $1/r_1 = b_1/a_1 \in \mathbb{Q}_i$ si et seulement si a_i est impair. En conclusion, les inversibles de $\mathbb{Q}_i$ sont exactement les rationnels qui s'écrivent (sous forme irréductible) comme quotient de deux entiers impairs (par exemple, $1/3$ mais pas $2/3$).

Exercice 44 : ✪ Soient A_1 et A_2 deux anneaux et $f : A_1 \to A_2$ un morphisme d'anneaux. Montrer que si A_2 a au moins deux éléments, $\ker(f)$ n'est pas un sous-anneau de A_1.

Correction : Un morphisme d'anneaux envoie 1_{A_1} sur $1_{A_2} \neq 0_{A_2}$ puisque A_2 a au moins deux éléments. Dès lors, 1_{A_1} n'appartient pas à $\ker(f)$ donc $\ker(f)$ n'est pas un sous-anneau de A_1.

Exercice 45 : ✪ Montrer que le centre d'un anneau A est un sous-anneau de A.

Correction : Nous n'avons pas défini le centre d'un anneau, mais cela n'est pas très difficile de deviner la définition : c'est l'ensemble des éléments de A qui commutent avec tout le monde (au sens de la multiplication : A est un groupe abélien muni de la loi $+$) i.e. $Z(A) = \{a \in A \,|\, \forall b \in A, ab = ba\}$.

- Pour tout $b \in A, 0 \times b = b \times 0 = 0$ donc $0 \in Z(A)$: $Z(A)$ est non vide.
- Soient a_1 et a_2 deux éléments de $Z(A)$. Soit $b \in A$. Par distributivité du produit sur la somme, $(a_1 + a_2)b = a_1b + a_2b$. Or, a_1 et a_2 sont dans $Z(A)$ donc $a_1b = ba_1$ et idem pour l'autre, si bien que $(a_1 + a_2)b = ba_1 + ba_2$, et encore par distributivité, on obtient $(a_1 + a_2)b = b(a_1 + a_2)$: $a_1 + a_2 \in Z(A)$, $Z(A)$ est stable par somme.
- $a_1b - a_1b = 0$ donc $ba_1 - a_1b = 0$ si bien que $-a_1b = -ba_1$: $-a_1 \in Z(A)$, $Z(A)$ est stable par passage à l'opposé : c'est un sous-groupe de A.
- $1 \in Z(A)$ car le neutre commute avec tout le monde.
- Enfin, soit $b \in A$. Puisque a_1 et a_2 appartiennent à $Z(A)$, on a successivement (par associativité du produit) : $a_1a_2b = a_1ba_2 = ba_1a_2$ donc $a_1a_2 \in Z(A)$, $Z(A)$ est stable par produit donc c'est un sous-anneau de A.

Exercice 46 : ✪ Soit A un anneau (pas forcément commutatif) et soient a et b deux éléments de A tels que ab soit nilpotent. Montrer que ba est nilpotent.

Correction : Il existe $n \geq 1$ tel que $(ab)^n = 1$. Attention, a et b ne commutent pas forcément donc on n'a pas forcément $(ab)^n = a^nb^n$. On a :

$$(ab)^n = (ab)(ab)(ab)(ab)\cdots(ab) = 0$$

avec ab multiplié par lui-même n fois. En multipliant par b à gauche et par a à droite, on a encore 0 puisque 0 est absorbant, si bien que (toujours par associativité du produit) :

$$b(ab)(ab)(ab)(ab)\cdots(ab)a = (ba) \times \cdots \times (ba) = 0$$

avec ba multiplié par lui-même $n + 1$ fois : en d'autres termes, $(ba)^{n+1} = 0$, ba est encore nilpotent.

Exercice 47 : ✪ Soit $k \in \mathbb{R}$. On munit $\mathbb{R}$ des deux lois de composition internes suivantes :

$$\forall (a, b) \in \mathbb{R}^2, \begin{cases} a\$b = a + b - k \\ \\ a \top b = ab - k(a + b) + k(k + 1) \end{cases}$$

Étudier la structure de $(\mathbb{R}, \$, \top)$.

Correction : Voyons si $(\mathbb{R}, \$)$ est un groupe abélien : si oui, on verra si $(\mathbb{R}, \$, \top)$ est un anneau, sinon on s'arrêtera là. Ici, rien n'est évident, on n'a pas des lois usuelles : il faut tout montrer à la main.

- La loi \$ est bien une loi interne, et il est immédiat qu'elle est commutative. Vérifions qu'elle est associative. Soit $(a,b,c) \in \mathbb{R}^3$. D'une part :

$$\begin{aligned} a\$(b\$c) &= a\$(b+c-k) \\ &= a+(b+c-k)-k \\ &= a+b+c-2k \end{aligned}$$

et d'autre part :

$$\begin{aligned} (a\$b)\$c &= (a+b-k)\$c \\ &= (a+b-k)+c-k \\ &= a+b+c-2k \end{aligned}$$

donc la loi \$ est bien associative.
- Il est immédiat que k est neutre pour la loi \$ et que, pour tout a, $2k-a$ est le symétrique de a pour la loi \$: il y a un neutre et tout élément admet un symétrique, $(\mathbb{R},\$)$ est bien un groupe abélien.
- Regardons si $(A,\$,\top)$ est un anneau : sinon, on s'arrête là, si oui, on verra ensuite si c'est un corps. Regardons si la loi $\top$ est associative. D'une part :

$$\begin{aligned} a\top(b\top c) &= a\top(bc-k(b+c)+k(k+1)) \\ &= a(bc-k(b+c)+k(k+1))-k(a+bc-k(b+c)+k(k+1))+k(k+1) \\ &= abc-ak(b+c)+ak(k+1)-ak-kbc+k^2(b+c)-k^2(k+1)+k(k+1) \\ &= abc-k(ab+ac+bc)+k^2(a+b+c)-k^3+k \end{aligned}$$

et d'autre part :

$$\begin{aligned} (a\top b)\top c &= (ab-k(a+b)+k(k+1))\top c \\ &= (ab-k(a+b)+k(k+1))c-k(ab-k(a+b)+k(k+1)+c)+k(k+1) \\ &= abc-kc(a+b)+ck(k+1)-kab+k^2(a+b)-k^2(k+1)-kc+k(k+1) \\ &= abc-k(ab+ac+bc)+k^2(a+b+c)-k^3+k \end{aligned}$$

et donc la loi $\top$ est associative. Regardons si elle est distributive par rapport à la loi \$. La loi $\top$ étant évidemment commutative, il suffit d'étudier la distributivité à gauche. D'une part :

$$\begin{aligned} a\top(b\$c) &= a\top(b+c-k) \\ &= a(b+c-k)-k(a+b+c-k)+k(k+1)\ \ lcl \\ &= ab+ac-k(2a+b+c)+2k^2+k \end{aligned}$$

et, d'autre part :

$$\begin{aligned} (a\top b)\$(a\top c) &= (ab-k(a+b)+k(k+1))\$(ac-k(a+c)+k(k+1)) \\ &= (ab-k(a+b)+k(k+1))+(ac-k(a+c)+k(k+1))-k \\ &= ab+ac-k(2a+b+c)+2k^2+k \end{aligned}$$

et donc $\top$ est distributive par rapport à \$. Cherchons si $\top$ admet un élément neutre. Soit $b \in \mathbb{R}$ (la loi est commutative, il suffit de chercher un neutre à gauche) :

$$\begin{aligned} b \text{ est neutre pour } \top &\iff \forall \in \mathbb{R}, a\top b = ab-k(a+b)+k(k+1) = a \\ &\iff \forall a \in \mathbb{R}, a(b-k)-kb+k^2+k = a \end{aligned}$$

Posons $b = k+1$. Alors on a bien, pour tout $a \in \mathbb{R}, a\top b = a$: $k+1$ est neutre pour la loi $\top$. Finalement, $(A,\$,\top)$ est un anneau commutatif.

- Cherchons si c'est un corps. Soit donc $a \neq k$ (le neutre de la première loi). On cherche b tel que $a \top b = k+1$ (idem, la loi est commutative, il suffit de chercher un inverse à droite). Soit $b \in \mathbb{R}$.

$$\begin{aligned} a \top b = k+1 &\iff ab - k(a+b) + k(k+1) = k+1 \\ &\iff ab - ka - kb + k^2 = 1 \\ &\iff b(a-k) = 1 + ka - k^2 \end{aligned}$$

  et puisque $a \neq k$, on en déduit que $\dfrac{1+ak-k^2}{a-k}$ est l'inverse de a pour la loi $\top$: $(\mathbb{R}, \$, \top)$ est un corps.

Exercice 48 : ✪ Montrer que $\mathbb{D}$ (l'ensemble des nombres décimaux) est un anneau (on pourra utiliser l'exercice 9 du chapitre 12). Est-ce un corps ? Mêmes question avec l'ensemble des nombres dyadiques.

Correction : Rappelons qu'un rationnel r est un décimal si et seulement s'il existe $k \in \mathbb{Z}$ et $n \in \mathbb{N}$ tel que $r = k/10^n$. Pour montrer que $\mathbb{D}$ est un anneau, il suffit de prouver que c'est un sous-anneau de $\mathbb{Q}$.

1. $0 = 0/10^1 \in \mathbb{D}$ donc $\mathbb{D}$ est non vide.
2. Soient r_1 et r_2 deux décimaux. Il existe alors $(k_1, k_2) \in \mathbb{Z}^2$ et $(n_1, n_2) \in \mathbb{N}^2$ tel que $r_1 = k_1/10^{n_1}$ et $r_2 = k_2/10^{n_2}$. Sans perte de généralité, supposons $n_1 \geq n_2$. Alors :

$$r_1 + r_2 = \frac{k_1 + k_2 10^{n_1 - n_2}}{10^{n_2}} \in \mathbb{D}$$

   $\mathbb{D}$ est donc stable par somme. De plus, $-n_1 = -k_1/10^{n_1} \in \mathbb{D}$: $\mathbb{D}$ est stable par opposé, c'est un sous-groupe de $\mathbb{Q}$ (muni de la loi + évidemment).
3. $1 = 1/10^0 \in \mathbb{D}$.
4. Enfin, $r_1 r_2 = k_1 k_2 / 10^{n_1+n_2} \in \mathbb{D}$: $\mathbb{D}$ est stable par produit, c'est un sous-anneau de $\mathbb{Q}$, et en particulier c'est un anneau. Ce n'est cependant pas un corps car $3 \in D$ mais $1/3 \notin \mathbb{D}$: rappelons (cf. exercice 9 du chapitre 12) qu'un rationnel est décimal si et seulement si les facteurs premiers de son dénominateur (quand on écrit la fraction sous forme irréductible) sont égaux à 2 et/ou 5, ce qui n'est pas le cas de 1/3 : $\mathbb{D}$ n'est donc pas un corps. Idem pour l'ensemble des nombres dyadiques en remplaçant 10 par 2 dans ce qui précède.

Exercice 49 : ✪

1. Montrer que $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \,|\, (a,b) \in \mathbb{Z}^2\right\}$ est un anneau intègre.
2. On définit sur $\mathbb{Z}\left[\sqrt{2}\right]$ une application N par $N(a+b\sqrt{2}) = a^2 - 2b^2$. Montrer que N est une application multiplicative i.e. vérifie $N(xy) = N(x)N(y)$ pour tous x et y.
3. En déduire que les éléments inversibles de $\mathbb{Z}\left[\sqrt{2}\right]$ sont exactement les éléments de la forme $a+b\sqrt{2}$ avec $a^2 - 2b^2 = \pm 1$. D'après l'exercice 15 du chapitre 1, il y a donc une infinité d'inversibles.

Correction :

1. Montrons que c'est un sous-anneau de $\mathbb{R}$.
   - $0 = 0 + \sqrt{2} \times 0$ donc $0 \in \mathbb{Z}[\sqrt{2}]$: $\mathbb{Z}[\sqrt{2}]$ est non vide.
   - Soient x_1 et x_2 deux éléments de $\mathbb{Z}[\sqrt{2}]$. Alors il existe a_1, b_1, a_2, b_2 dans $\mathbb{Z}$ tels que $x_1 = a_1 + b_1\sqrt{2}$ et $x_2 = a_2 + b_2\sqrt{2}$ si bien que $x_1 + x_2 = a_1 + a_2 + \sqrt{2}(b_1 + b_2)$. Or, $a_1 + a_2$ et $b_1 + b_2$ sont des éléments de $\mathbb{Z}$ donc $x_1 + x_2 \in \mathbb{Z}[\sqrt{2}]$: $\mathbb{Z}[\sqrt{2}]$ est stable par somme.
   - De plus, $-x_1 = -a - b\sqrt{2}$ et puisque $-a$ et $-b$ appartiennent à $\mathbb{Z}$, $-x_1 \in \mathbb{Z}[\sqrt{2}]$: $\mathbb{Z}[\sqrt{2}]$ est un sous-groupe de $\mathbb{R}$.
   - $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
   - Enfin, $x_1 x_2 = (a_1 a_2 + 2b_1 b_2) + \sqrt{2}(a_1 b_2 + a_2 b_1) \in \mathbb{Z}[\sqrt{2}]$: $\mathbb{Z}[\sqrt{2}]$ est stable par produit, c'est donc un sous-anneau de $\mathbb{R}$, et en particulier c'est un anneau. Il est intègre puisqu'il est inclus dans $\mathbb{R}$ qui est intègre.
2. Avec les mêmes notations que ci-dessus :

$$\begin{aligned} N(x_1x_2) &= (a_1a_2 + 2b_1b_2)^2 - 2(a_1b_2 + a_2b_1)^2 \\ &= {a_1}^2{a_2}^2 + 4{b_1}^2{b_2}^2 + 4a_1a_2b_1b_2 - 2{a_1}^2{b_2}^2 - 2{a_2}^2{b_1}^2 - 4a_1a_2b_1b_2 \\ &= {a_1}^2{a_2}^2 + 4{b_1}^2{b_2}^2 - 2{a_1}^2{b_2}^2 - 2{a_2}^2{b_1}^2 \end{aligned}$$

   et :

$$\begin{aligned} N(x_1)N(x_2) &= ({a_1}^2 - 2{b_1}^2)({a_2}^2 - 2{b_2}^2) \\ &= {a_1}^2{a_2}^2 + 4{b_1}^2{b_2}^2 - 2{a_1}^2{b_2}^2 - 2{a_2}^2{b_1}^2 \end{aligned}$$

N est bien multiplicative.

3. Supposons que $x = a+b\sqrt{2}$ soit inversible et notons son inverse $x'+y'\sqrt{2}$. Alors $N(xy) = N(1) = 1$ donc $N(x)N(y) = 1$. Or, $N(x) \in \mathbb{Z}$ donc $N(x) = a^2 - 2b^2 = \pm 1$. Réciproquement, supposons que $N(x) = \pm 1$. Notons $y = a - b\sqrt{2}$. Alors $xy = a^2 - 2b^2 = \pm 1$. Si $xy = 1$ alors y est un inverse de x, sinon $-y$ est un inverse de x. Dans tous les cas, x est inversible. D'où l'équivalence.

Exercice 50 : ✪

1. Montrer que le seul morphisme de corps de $\mathbb{Q}$ dans $\mathbb{Q}$ est l'identité.
2. Déterminer tous les automorphismes de corps de $\mathbb{Q}\left[\sqrt{2}\right]$.

Correction :

1. Découle de l'exercice 26 : les morphismes de groupes de $\mathbb{Q}$ dans lui-même sont exactement les fonctions de la forme $r \mapsto ar$ avec $a \in \mathbb{Q}$. Puisqu'un morphisme de corps vérifie $f(1) = 1$, la seule possibilité est d'avoir $a = 1$ donc que le morphisme soit l'identité.
2. Analyse : soit f un automorphisme de corps de $\mathbb{Q}[\sqrt{2}]$. Alors, de même que dans l'exercice 26, puisque $f(1) = 1$, alors $f(r) = r$ pour tout rationnel. Puisque f est un morphisme d'anneaux, $f(\sqrt{2}^2) = f(\sqrt{2})^2$, et puisque $f(2) = 2$, il vient : $f(\sqrt{2}) = \pm\sqrt{2}$. Puisque f est un morphisme d'anneau et que pour tout rationnel, $f(r) = r$, on trouve :

$$\forall (a,b) \in \mathbb{Q}^2, f(a + b\sqrt{2}) = a \pm \sqrt{2}$$

On en déduit que, si $f(\sqrt{2}) = \sqrt{2}$, f est l'identité de $\mathbb{Q}[\sqrt{2}]$, et si $f(\sqrt{2}) = -\sqrt{2}$, alors f est « la conjugaison sur $\mathbb{Q}[\sqrt{2}]$ », c'est-à-dire que, pour tous a et b dans $\mathbb{Q}$, $f(a + b\sqrt{2}) = a - b\sqrt{2}$. Synthèse : il est immédiat que ce sont des automorphismes de corps.

Exercice 51 : ✪

1. Montrer que $A = \{a + b\sqrt{3} \,|\, (a,b) \in \mathbb{Q}^2\}$ est un corps. Est-ce le cas de $B = \{a + b\sqrt{2} + c\sqrt{3} \,|\, (a,b,c) \in \mathbb{Q}^3\}$?
2. Montrer que A et $\mathbb{Q}\left[\sqrt{2}\right]$ ne sont pas isomorphes.

Correction :

1. On montre que c'est un corps de la même façon que dans le cours, où l'on a montré que $\mathbb{Q}[\sqrt{2}]$ est un corps. Ce Cependant, B n'est pas un corps car ce n'est pas un anneau puisqu'il n'est pas stable par produit : en effet, $\sqrt{2} \times \sqrt{3} = \sqrt{6} \notin B$.
2. Supposons qu'il existe un isomorphisme d'anneaux (et donc de corps) noté f entre A et $\mathbb{Q}[\sqrt{2}]$. De même que précédemment, $f(r) = r$ pour tout rationnel r. De même que dans l'exercice précédent, $f(\sqrt{3}) = \pm\sqrt{3}$ ce qui est absurde puisque $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

Exercice 52 : ✪

1. Montrer que $\mathbb{Q}[i] = \{a + ib \,|\, (a,b) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{C}$.
2. On définit de même $\mathbb{Q}[j]$ où $j = e^{2i\pi/3}$. Montrer que $\mathbb{Q}[j]$ est un corps non isomorphe à $\mathbb{Q}[i]$.

Correction :

1. Analogue aux exemples $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[\sqrt{3}]$.
2. Montrons que $\mathbb{Q}[j]$ est un sous-corps de $\mathbb{C}$. Le fait que ce soit un sous-groupe est immédiat. De plus, $1 = 1+0\times j \in \mathbb{Q}[j]$. Soient $x_1 = a_1 + b_1 j$ et $x_2 = a_2 + b_2 j$ deux éléments de $\mathbb{Q}[j]$ (avec a_1, a_2, b_1, b_2 rationnels, donc). On a :

$$x_1 x_2 = a_1 a_2 + b_1 b_2 j^2 + j(a_1 b_2 + a_2 b_1)$$

Puisque $1 + j + j^2 = 0$, $j^2 = -1 - j$ et donc :

$$x_1 x_2 = a_1 a_2 - b_1 b_2 + j(a_1 b_2 + a_2 b_1 - b_1 b_2) \in \mathbb{Q}[j]$$

$\mathbb{Q}[j]$ est stable par produit : c'est un sous-anneau de $\mathbb{C}$. Enfin, si $a + bj \neq 0$:

$$\begin{aligned}\frac{1}{a+bj} &= \frac{1}{a-b/2+bi\sqrt{3}/2}\\ &= \frac{a-b/2-i\sqrt{3}/2}{(a-b/2)+b^2\times 3/4}\\ &= \frac{a}{(a-b/2)+b^2\times 3/4}+\frac{b}{(a-b/2)+b^2\times 3/4}\times(-1/2-i\sqrt{3}/2)\\ &= \frac{a}{(a-b/2)+b^2\times 3/4}+\frac{b}{(a-b/2)+b^2\times 3/4}\times j^2\end{aligned}$$

Or, $1+j+j^2=0$ donc $j^2=-1-j$ ce qui permet de conclure comme ci-dessus en regroupant les termes : $1/(a+bj)\in\mathbb{Q}[j]$, $\mathbb{Q}[j]$ est un corps. On trouve de même que précédemment que si $\varphi:\mathbb{Q}[i]\to\mathbb{Q}[j]$ est un isomorphisme, alors $\varphi(r)=r$ pour tout rationnel, et donc $\varphi(i^2)=-1=\varphi(i)^2$ donc $\varphi(i)=\pm i$ ce qui est absurde puisque $\pm i\notin\mathbb{Q}[j]$: en effet, si $i\in\mathbb{Q}[j]$, il existe a et b rationnels tels que $i=a+bj$ donc

$$i=a-\frac{b}{2}+bi\frac{\sqrt{3}}{2}$$

Si $b\neq 0$, en identifiant les parties imaginaires, $\sqrt{3}=2/b\in\mathbb{Q}$ ce qui est absurde.

Exercice 53 - Anneau d'Eisenstein : ✪✪ On définit $\mathbb{Z}[j]$ de façon analogue à ci-dessus.

1. Vérifier que $\mathbb{Z}[j]$ est un anneau.
2. Soit $u\in\mathbb{Z}[j]$. Vérifier que u est inversible dans $\mathbb{Z}[j]$ si et seulement si $|u|=1$.
3. En déduire tous les inversibles de $\mathbb{Z}[j]$.

Correction :

1. Analogue à ce qui précède.
2. Tout d'abord, si $u\in\mathbb{Z}[j]$, il existe a et b entiers tels que $u=a+jb=a-b/2+ib\sqrt{3}/2$. Par conséquent :

$$\begin{aligned}|u|^2 &= (a-b/2)^2+3b^2/4\\ &= a^2-ab+b^2/4+3b^2/4\\ &= a^2-ab+b^2\end{aligned}$$

Si u est inversible, notons v son inverse. Alors $uv=1$ donc $u^2v^2=1$ si bien que $|u|^2\times|v|^2=1$. Or, on déduit de ce qui précède que $|u|^2$ et $|v|^2$ sont des entiers (et ils sont positifs par propriété d'un carré réel) donc $|u|^2=1$ si bien que $|u|=1$. Réciproquement, supposons que $|u|=1$. Alors, en mettant au carré, on trouve : $|u|^2=a^2-ab+b^2=1$. Posons

$$\begin{aligned}v &= \overline{u}\\ &= a-b/2-ib\sqrt{3}\\ &= a+bj^2\\ &= a+b(-1-j)\\ &= (a-b)-bj\in\mathbb{Z}[j]\end{aligned}$$

et $uv=|u|^2=1$: u est bien inversible, d'où l'équivalence.

3. On cherche donc les couples d'entiers (a,b) tels que $a^2-ab+b^2=1$. Soit $(a,b)\in\mathbb{Z}^2$.

$$a^2-ab+b^2=1\iff(a-b)^2=1-ab\qquad\text{et}\qquad a^2+b^2=1+ab$$

Par conséquent, si (analyse synthèse) le couple (a,b) convient, alors $1\pm ab\geq 0$ donc $1\geq\pm ab$ i.e. $1\geq|ab|$: il en découle que $ab=\pm1$ ou 0. De plus, puisque $ab\leq 1$, alors $a^2+b^2\leq 2$ donc $|a|$ et $|b|$ sont inférieurs ou égaux à 1 (sinon a^2 ou $b^2\geq 4$). On a donc les couples suivants : $(-1,1),(1,-1),(1,1),(-1,-1),(\pm1,0)$ et $(0,\pm1)$. En conclusion, les inversibles éventuels (rappelons qu'on est dans la phase analyse) sont :

$$\pm 1, \pm j, -1+j, 1-j, 1+j, -1-j$$

Synthèse : $j-1$ et $1-j$ ne sont pas de norme 1 donc ne sont pas des inversibles. Finalement, les inversibles de $\mathbb{Z}[j]$ sont $\pm 1, \pm j, 1+j = -j^2$ et $-1-j = j^2$.

Exercice 54 : ✪✪ Soit E un ensemble non vide quelconque.

1. Montrer que $(\mathscr{P}(E), \Delta)$ est un groupe abélien.
2. Montrer que $(\mathscr{P}(E), \Delta, \cap)$ est un anneau commutatif.
3. Est-ce que $(\mathscr{P}(E), \Delta, \cup)$ est un anneau ?
4. Soit F une partie de E. $\mathscr{P}(F)$ est-il un sous-anneau de $\mathscr{P}(E)$?
5. **Remake :** Ces résultats sont-ils encore vrais avec $\mathscr{P}_f(E)$, l'ensemble des parties finies de E, à la place de $\mathscr{P}(E)$?

Correction :

1. On sait que la différence symétrique est associative. Elle est de plus commutative (cf. chapitre 3). D'après l'exercice 13 du chapitre 3 (mais essayez de le redémontrer), l'ensemble vide est un élément neutre, et A est son propre symétrique (i.e. $A \Delta A = \varnothing$) : on a bien un groupe abélien.
2. L'intersection est commutative, associative et admet un élément neutre (E tout entier). Pour prouver qu'on a un anneau commutatif, il reste à prouver que l'intersection est distributive par rapport à la différence symétrique (et puisque l'intersection est commutative, il suffit de prouver qu'elle est distributive à gauche). Soient A, B, C trois parties de E. D'une part, en utilisant la distributivité de l'intersection sur l'union :

$$\begin{aligned} A \cap (B \Delta C) &= A \cap ((B \cap \overline{C}) \cup (\overline{B} \cap C)) \\ &= (A \cap (B \cap \overline{C})) \cup (A \cap (\overline{B} \cap C)) \end{aligned}$$

et d'autre part :

$$(A \cap B) \Delta (A \cap C) = (A \cap B \cap (\overline{A \cap C})) \cup ((\overline{A \cap B} \cap A \cap C))$$

Or,

$$\begin{aligned} (A \cap B) \cap (\overline{A \cap C}) &= (A \cap B) \cap (\overline{A} \cup \overline{C}) \\ &= (A \cap B \cap \overline{A}) \cup (A \cap B \cap \overline{C}) \\ &= \varnothing \cup (A \cap B \cap \overline{C}) \\ &= (A \cap B \cap \overline{C}) \end{aligned}$$

et on trouve de même que $(\overline{A \cap B} \cap A \cap C) = A \cap \overline{B} \cap C$: l'intersection est distributive par rapport à la différence symétrique, on a bien un anneau commutatif.
3. Non car le neutre des deux lois sont les mêmes : à chaque fois, l'ensemble vide.
4. Non car il n'y a pas le même neutre pour la deuxième loi : E n'est pas un élément de $\mathscr{P}(F)$ (sauf si $E = F$ mais alors là il n'y a plus de question).
5. Si E est fini, oui car alors $\mathscr{P}(E) = \mathscr{P}_f(E)$, mais ce n'est plus le cas si E est infini car il n'y a pas de neutre pour l'intersection (puisque E n'appartient pas à l'ensemble).

Les quatre exercices suivants utilisent le fait (cf. cours) que si A est un anneau et I un ensemble non vide, alors A^I est muni d'une structure d'anneau quand on le munit de la somme et du produit de fonctions.

Exercice 55 : ✪ Si K est un corps, l'ensemble K^I est-il muni d'une structure de corps pour ces mêmes lois ? d'une structure d'anneau intègre ?

Correction : Si I est un singleton, alors K^I et K sont isomorphes (exo) donc K^I est un corps. Supposons K^I n'est pas muni d'une structure de corps car si f est une fonction qui s'annule mais qui n'est pas la fonction nulle, il n'y a aucune fonction g telle que $f \times g$ soit la fonction constante égale à 1. Il n'est pas non plus muni d'une structure d'anneau intègre puisque si f s'annule mais n'est pas la fonction nulle, en prenant g qui s'annule là où f ne s'annule pas, et réciproquement, on a $f \times g = 0$ mais f et g non nulles : on n'a pas un anneau intègre.

Exercice 56 : ✪ Soit A un anneau et soit I un ensemble non vide. Montrer que $U\left(A^I\right) = U(A)^I$.

Correction : En d'autres termes, montrons qu'une fonction est inversible (pour le produit) si et seulement si elle ne prend que des valeurs inversibles (de A). Soit $f \in U(A^I)$. Alors il existe $g \in A^I$ telle que $f \times g = 1$ i.e. la fonction constante égale à 1 (le neutre du produit de A i.e. 1_A). En d'autres termes, pour tout $x \in A$, $f(x)g(x) = 1$ donc $f(x) \in U_A$: $f \in U(A)^I$. Réciproquement, soit $f \in U(A)^I$ i.e. pour tout x, $f(x) \in U(A)$. Soit g définie sur I par : $\forall x, g(x) = f(x)^{-1}$. Alors, pour tout x, $f(x) \times g(x) = 1$ donc $f \in U(A^I)$.

Exercice 57 : ✪ Soit E un ensemble non vide. Donner les diviseurs de zéro et les inversibles de $\mathbb{Z}^E$.

Correction : Supposons que E ne soit pas un singleton sinon l'exercice n'a pas beaucoup d'intérêt. Montrons que les diviseurs de 0 sont les fonctions qui s'annulent (sauf la fonction nulle), et les inversibles les fonctions qui ne prennent que les valeurs ± 1. Soit f une fonction qui s'annule mais différente de la fonction nulle. On note g la fonction qui est nulle là où f ne s'annule pas et qui vaut 1 là où f s'annule, si bien que $f \times g = 0$: f est un diviseur de 0. Réciproquement, si f ne s'annule pas, la seule façon d'avoir $f \times g = 0$ est que g soit la fonction nulle.

Soit f une fonction ne prenant que les valeurs ± 1. Alors $f \times f$ est la fonction constante égale à 1 donc f est inversible et est sa propre inverse. Si f s'annule, alors f est un diviseur de 0 (ou la fonction nulle) donc n'est pas inversible. Sinon, supposons qu'il existe n tel que $|f(n)| \geq 2$: alors il n'existe pas de fonction g telle que $f(n)g(n) = 1$: f n'est pas inversible.

Exercice 58 : ✪✪✪ On note S_t l'ensemble des suites stationnaires à valeurs dans $\mathbb{Z}$.

1. Vérifier que S_t est un sous-anneau de $\mathbb{Z}^{\mathbb{N}}$.
2. On souhaite déterminer tous les morphismes d'anneaux de S_t dans $\mathbb{Z}$.
   (a) Si $i \in \mathbb{N}$, on note v_i l'application évaluation en i c'est-à-dire que pour toute suite $u \in S_t$, on a $v_i(u) = u_i$. Montrer que v_i est un morphisme d'anneaux de S_t dans $\mathbb{Z}$.
   (b) Notons v_∞ l'application limite c'est-à-dire la fonction qui à toute suite $u \in S_t$ associe sa limite. Prouver que v_∞ est bien définie puis que c'est un morphisme d'anneaux.

   On souhaite montrer que ce sont les seuls morphismes d'anneaux de S_t dans $\mathbb{Z}$. On se donne dans la suite φ un morphisme d'anneaux de S_t dans $\mathbb{Z}$. De plus, si $i \in \mathbb{N}$, on note e_i la suite dont tous les termes valent 0 sauf celui d'indice i qui vaut 1 et, enfin, on note $\tilde{1}$ la suite constante égale à 1

   (c) Montrer qu'il existe au plus un $i \in \mathbb{N}$ tel que $\varphi(e_i) \neq 0$.
   (d) Supposons qu'il existe $i_0 \in \mathbb{N}$ tel que $\varphi(e_{i_0}) \neq 0$. Montrer que $(\varphi - v_{i_0})(e_i) = 0$ pour tout $i \in \mathbb{N}$ et que $(\varphi - v_{i_0})\left(\tilde{1}\right) = 0$. En déduire que $\varphi = v_{i_0}$.
   (e) Montrer de même que si $\varphi(e_i) = 0$ pour tout $i \in \mathbb{N}$, alors $\varphi = v_\infty$.

Correction :

1. La suite nulle est stationnaire donc S_t est non vide. Soient (u_n) et (v_n) deux suites stationnaires, respectivement à partir d'un rang n_0 et à partir d'un rang n_1. Alors $(u_n) + (v_n)$ est stationnaire à partir du rang $\max(n_0, n_1)$, donc $(u_n) + (v_n) \in S_t$, S_t est stable par somme, et $-(u_n)$ est aussi stationnaire à partir du rang n_0 donc $-(u_n) \in S_t$, S_t est stable par opposé donc S_t est un sous-groupe de $\mathbb{Z}^{\mathbb{N}}$. La suite constante égale à 1 est stationnaire donc appartient à S_t. Enfin, $(u_n) \times (v_n)$ est stationnaire à partir du rang $\max(n_0, n_1)$, S_t est stable par produit : c'est un sous-anneau de $\mathbb{Z}^{\mathbb{N}}$.
2. (a) Immédiat : pour toutes suites u et v, $v_i(u+v) = (u+v)_i = u_i + v_i = v_i(u) + v_i(v)$, idem pour le produit, et si u est la suite constante égale à 1, alors $v_i(u) = 1$.
   (b) v_∞ est bien définie puisqu'une suite stationnaire converge. Puisque la limite d'une somme est la somme des limites (toutes les suites considérées convergent), que la limite d'un produit est le produit des limites, et que la limite de la suite constante égale à 1 vaut 1, alors v_∞ est un morphisme d'anneaux.
   (c) Supposons qu'il existe $i \neq j$ tels que $\varphi(e_i)$ et $\varphi(e_j)$ soient non nuls. Alors $\varphi(e_i \times e_j) = \varphi(e_i) \times \varphi(e_j) \neq 0$ mais $e_i \times e_j$ est la suite nulle donc $\varphi(e_i \times e_j) = 0$ ce qui est absurde.
   (d) si $i \neq i_0$, alors $v_{i_0}(e_i) = 0$ et, d'après ce qui précède, $\varphi(e_i) = 0$ puisque $\varphi(e_{i_0}) \neq 0$ et que φ est non nulle en au plus une suite e_i. De plus, $\varphi(\tilde{1}) = v_{i_0}(\tilde{1}) = 1$, d'où la deuxième égalité voulue. Soit u une suite stationnaire égale à L à partir du rang n_0. Alors

   $$u = L \times \tilde{1} + (u_0 - L)e_0 + (u_1 - L)e_1 + \cdots + (u_{n_0-1} - L)e_{n_0-1}$$

   φ et les v_i étant des morphismes d'anneaux, on a :

$$(\varphi - e_i)(u) = L \times (\varphi - e_i)(\tilde{1}) + (u_0 - L)(\varphi - e_i)(e_0) + (u_1 - L)(\varphi - e_i)(e_1) + \cdots + (u_{n_0-1} - L)(\varphi - e_i)(e_{n_0-1})$$

En effet, si $k \in \mathbb{Z}$ et v est une suite, $(\varphi - e_i)(kv) = k(\varphi - e_i)(v)$: on fait comme d'habitude, les entiers positifs puis les entiers négatifs. Finalement, $(\varphi - e_i)(u) = 0$ donc $\varphi = e_i$ puisque c'est vrai pour toute suite stationnaire u.

(e) De même, $(\varphi - v_i\infty)(e_i) = 0$ pour tout i et $(\varphi - v_\infty)(\tilde{1}) = 0$ et on conclut de la même façon.

Exercice 59 - Anneaux de Boole : ✪✪ Un anneau de Boole est un anneau dans lequel tout élément vérifie $x^2 = x$.

1. Donner un exemple d'anneau de Boole non réduit à un élément.
2. Montrer que, dans un anneau de Boole, tout élément x vérifie $x = -x$.
3. Montrer qu'un anneau de Boole est commutatif.
4. Déterminer (à isomorphisme près) le seul anneau de Boole intègre.
5. On définit une relation binaire $\preccurlyeq$ sur A par : $x \preccurlyeq y \iff yx = x$. Montrer que $\preccurlyeq$ est une relation d'ordre.

Correction :

1. $\mathbb{Z}/2\mathbb{Z}$ est un anneau de Boole non réduit à un élément.
2. On se place dans un anneau de Boole noté A. Soit $x \in A$. Alors $(x+1)^2 = x^2+2x+1 = x+2x+1$ (x et 1 commutent) mais $(x+1)^2 = x+1$ donc $2x = 0$ si bien que $x + x = 0$ donc $x = -x$.
3. Soient x et y deux éléments de A, un anneau de Boole. Alors $(x+y)^2 = x+y$ mais on a aussi $(x+y)^2 = x^2+xy+yx+y^2 = x + xy + yx + y$ donc $xy + yx = 0$: on trouve que $xy = -yx$ donc, d'après la question précédente, $xy = yx$, l'anneau est commutatif.
4. On se place dans A un anneau intègre. Soit $x \neq 0$. Alors $x^2 = x$ donc $x(x-1) = 0$ et comme l'anneau est intègre, $x = 1$: A n'a donc que deux éléments, et donc A est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
5. - Soit $x \in A$. $x^2 = x$ donc $x \preccurlyeq x$: $\preccurlyeq$ est réflexive.
   - Soient x et y deux éléments de A tels que $x \preccurlyeq y$ et $y \preccurlyeq x$ donc $yx = x$ et $xy = y$. Dès lors, l'anneau étant commutatif d'après la question 3, $xy = yx$ donc $x = y$: $\preccurlyeq$ est antisymétrique.
   - Soient x, y, z trois éléments de A tels que $x \preccurlyeq y$ et $y \preccurlyeq z$: on en déduit que $yx = x$ et $zy = y$ si bien que $zx = z(yx) = (zy)x = yx = x$: $x \preccurlyeq z$, $\preccurlyeq$ est transitive, c'est une relation d'ordre.

Exercice 60 - Anneau produit : ✪ Soient $(A_1, +_1, \times_1)$ et $(A_2, +_2, \times_2)$ deux anneaux. S'inspirer du cours pour munir $A_1 \times A_2$ d'une structure d'anneau. Donner les inversibles de $A_1 \times A_2$ en fonction de ceux de A_1 et de ceux de A_2.

Correction : On sait déjà (cf. cours) que $A_1 \times A_2$ est muni d'une structure de groupe abélien avec la loi produit : $(a_1, a_2) + (b_1, b_2) = (a_1 +_1 b_1, a_2 +_2 b_2)$. On définit de même une loi $\times$ produit : $(a_1, a_2) \times (b_1, b_2) = (a_1 \times_1 b_1, a_2 \times_2 b_2)$. Alors $(A, +, \times)$ est bien un anneau commutatif de neutre pour la loi $\times$: $(1_{A_1}, 1_{A_2})$ (exo). Prouvons que les inversibles de A sont exactement les couples de la forme (u_1, u_2) avec u_1 inversible de A_1 et u_2 inversible de A_2. Un élément de cette forme est bien inversible, d'inverse $({u_1}^{-1}, {u_2}^{-1})$, et si un élément (x, y) de A a une coordonnée non inversible, disons x, on ne peut pas le multiplier par un autre couple (z, t) tel que $(x, y) \times (z, t) = (1, 1)$ puisqu'il n'existe aucun z tel que $xz = 1$.

Exercice 61 - L'anneau $\mathbb{Z}^2$: ✪✪✪ On munit $\mathbb{Z}^2$ de sa structure d'anneau produit comme dans l'exercice 61.

1. Quels sont les diviseurs de 0, les éléments inversibles de $\mathbb{Z}^2$?
2. Trouver tous les morphismes d'anneaux de $\mathbb{Z}^2$ dans $\mathbb{Z}$. On pourra s'intéresser aux images de $e_1 = (1, 0)$ et $e_2 = (0, 1)$ par un tel morphisme.
3. Déterminer les sous-anneaux de $\mathbb{Z}^2$.

Correction :

1. D'après l'exercice précédent (mais on peut le reprouver à la main), les inversibles de $\mathbb{Z}^2$ sont exactement les quatre éléments $(\pm 1, \pm 1)$. Les diviseurs de zéro sont exactement les couples avec exactement une coordonnée nulle. En effet, si $a \neq 0$, $(a, 0) \times (0, 1) = (0, 0)$ et idem pour $(0, a)$: les éléments avec une seule coordonnée nulle sont des diviseurs de 0, et si (a, b) n'a aucune coordonnée nulle, si $(a, b) \times (x, y) = (ax, by) = (0, 0)$ donc $x = y = 0$: (a, b) n'est pas un diviseur de zéro.
2. Analyse : soit φ un tel morphisme. Alors $f(1, 1) = 1$. Suivons l'indication de l'énoncé et étudions $f(e_1)$ et $f(e_2)$. Puisque $f(e_1 + e_2) = 1$, alors $f(e_1) + f(e_2) = 1$ donc $f(e_2) = 1 - f(e_1)$. Notons $n = f(e_1)$ si bien que $f(e_2) = 1 - n$. De même que d'habitude, pour tout $k \in \mathbb{Z}$, $f(ke_1) = kf(e_1) = kn$ et $f(ke_2) = kf(e_2) = k - kn$. Finalement, pour tout $(x, y) \in \mathbb{Z}^2$:

$$\begin{aligned} f(x,y) &= f(xe_1+ye_2) \\ &= xn+y(1-n) \\ &= n(x-y)+y \end{aligned}$$

Enfin, $f(e_1\times e_2)=f(0,0)$ (on fait le produit coordonnée par coordonnée) donc $f(e_1)\times f(e_2)=n(1-n)=0$: on en déduit que $n=0$ ou $n=1$, c'est-à-dire que $f(x,y)=y$ (cas où $n=0$) ou $f(x,y)=x$ (cas où $n=1$). Réciproquement, on montre facilement que ces deux fonctions sont bien des morphismes d'anneaux, ce sont donc les seuls : les seuls morphismes de $\mathbb{Z}^2$ dans $\mathbb{Z}$ sont les morphismes coordonnées.

3. Soit A un sous-anneau de $\mathbb{Z}^2$. Alors $(1,1)\in A$ donc, pour tout $n\in\mathbb{Z}$, $(n,n)\in A$. S'il n'y a aucun élément $(x,y)\in A$ tel que $x\neq y$, alors $A=\{(n,n)\,|\,n\in\mathbb{Z}\}$, et réciproquement, cet ensemble est bien un sous-anneau de $\mathbb{Z}^2$. Supposons à présent qu'il existe $(x,y)\in A$ avec $x\neq y$. Alors $(-x,-y)\in A$ puisque A est un sous-groupe de $\mathbb{Z}^2$: il existe dans tous les cas un élément (a,b) avec $a>b$, et en faisant la différence avec (b,b), il vient $(a-b,0)\in A$. Notons $n=\min\{a>0\,|\,(a,0)\in A\}$. Montrons que A est l'ensemble des couples $(n+ak,n)$ avec n et k dans $\mathbb{Z}$. Soit $(x,y)\in A$. Si $x=y$ alors (x,y) est de la bonne forme avec $n=x=y$ et $k=0$. Sinon, $(x,y)-(y,y)=(x-y,0)\in A$. Effectuons la division euclidienne de $x-y$ par a : il existe $k\in\mathbb{Z}$ et $r\in[\![\,0\,;\,a-1\,]\!]$ tels que $x-y=ak+r$ donc

$$(x-y,0)-k(a,0)=(r,0)\in A$$

donc $r=0$ par choix de a si bien que a divise $x=y+ka$ donc $(x,y)=(y+ka,y)$. Réciproquement, pour tout $a\in\mathbb{N}^*$, $A=\{(n+ak,n)\,|\,(n,k)\in\mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{Z}^2$ (exo).

Exercice 62 - Idéaux : ✪✪✪ Si A est un anneau et si I est une partie de A, on dit que I est un idéal de A si I est un sous-groupe de $(A,+)$ absorbant pour la loi $\times$, i.e. :

$$\forall(a,i)\in A\times I,\qquad a\times i\in I\qquad\text{et}\qquad i\times a\in I$$

1. Donner les idéaux de $\mathbb{Z}$.
2. Soit $f:A_1\to A_2$ un morphisme d'anneaux. Montrer que $\ker(f)$ est un idéal de A_1.
3. Soit I un idéal d'un anneau A. Montrer que I contient un élément inversible de A si et seulement si $I=A$.
4. Soit K un corps. Montrer que $\{0\}$ et K sont les seuls idéaux de K. En déduire qu'un morphisme de corps est forcément injectif.
5. Réciproquement, supposons que A soit un anneau commutatif dont les seuls idéaux sont $\{0\}$ et A. Montrer que A est un corps. On pourra s'intéresser, pour $x\in A$ non nul, à l'ensemble $xA=\{xa\,|\,a\in A\}$.
6. Supposons que A soit commutatif et que les tous les idéaux I de A vérifient :

$$\forall(x,y)\in A^2, xy\in I\Rightarrow x\in I\text{ ou }y\in I$$

Montrer que A est intègre puis que $x\in x^2A$ pour tout $x\in A$. En déduire que A est un corps.

7. Soit I un idéal d'un anneau commutatif A. On appelle radical de I l'ensemble noté $\sqrt{I}$ défini par :

$$\sqrt{I}=\{x\in A\,|\,\exists n\in\mathbb{N},x^n\in I\}$$

Montrer que $\sqrt{I}$ est un idéal de A. Expliciter $\sqrt{12\mathbb{Z}}$.

Correction :

1. Un idéal de $\mathbb{Z}$ étant en particulier un sous-groupe de $\mathbb{Z}$, les seuls idéaux éventuels de $\mathbb{Z}$ sont les $n\mathbb{Z}$, et il est immédiat que ces ensembles sont absorbants : si $n\in\mathbb{Z}$:

$$\forall a\in\mathbb{Z},\forall i\in n\mathbb{Z}, a\times i\in n\mathbb{Z}\qquad\text{et}\qquad i\times a\in n\mathbb{Z}$$

2. On sait que $\ker(f)$ est un sous-groupe de A. Montrons qu'il est absorbant. Soit $(a,i)\in A\times\ker(f)$. f étant un morphisme d'anneaux, $f(a\times i)=f(a)\times f(i)$ et puisque $i\in\ker(f)$, $f(i)=0$ et on sait que 0 est absorbant donc $f(a\times i)=f(a)\times 0=0$ donc $a\times i\in\ker(f)$, et idem pour $i\times a$: $\ker(f)$ est un idéal de A.
3. Si $I=A$ alors I contient un élément inversible (le neutre pour le produit, 1). Réciproquement, supposons que I contienne un élément inversible i. Soit $a\in A$. Alors

$$a=(a\times i^{-1})\times i\in I$$

car I est absorbant : on en déduit que $A\subset I$, et puisque $I\subset A$ par définition, on a l'égalité $A=I$ voulue.

4. Rappelons que, dans un corps, tout élément non nul est inversible. Ainsi, d'après la question précédente, si un idéal contient un élément non nul, il contient un élément inversible donc est égal à K tout entier. Les seuls idéaux sont donc $\{0\}$ et K. Or, si f est un morphisme de corps, $\ker(f)$ est un idéal distinct de K (puisque $f(1) = 1$, $1 \notin \ker(f)$) donc $\ker(f) = \{0\}$: f est injectif.
5. Soit $x \in A$ non nul. Montrons que x est inversible. Montrons que xA est un idéal de A. $0 = x0$ donc $0 \in xA$: xA est non vide. Soient u et v deux éléments de xA : il existe a et b dans A tels que $u = xa$ et $v = xb$ donc $u + v = x(a + b) \in xA$ et $-u = x(-a) \in xA$: xA est un sous-groupe de A. De plus, pour tout $i \in xA$, il existe $a \in A$ tel que $i = xa$ et pour tout $b \in A$, $bi = x(ab) \in xA$ (l'anneau est commutatif) et $ib = x(ab) \in xA$: xA est absorbant, c'est un idéal. Or, il contient x puisque $x = x \times 1$ donc il contient un élément non nul donc $xA = A$: en particulier, il existe $a \in A$ tel que $xa = 1$: x est inversible, tout élément non nul est inversible, A est un corps.
6. $I = \{0\}$ est un idéal de A donc vérifie la condition de l'énoncé, à savoir : $xy = 0 \Rightarrow x = 0$ ou $y = 0$, l'anneau est intègre. Soit $x \in A$. De même que ci-dessus, x^2A est un idéal de A. Alors $x^3 = x^2 \times x \in x^2A$. Par hypothèse, $x^2 \in x^2A$ ou $x \in x^2A$. Si $x \in x^2A$, c'est bon, sinon $x^2 = x \times x \in x^2A$ donc $x \in x^2A$ ou $x \in x^2A$: dans tous les cas, on a le résultat voulu : il existe $a \in A$ tel que $x = x^2a$ si bien que $x - x^2a = 0$ donc $x(1 - xa) = 0$: si x est non nul, $xa = 1$: x est inversible, A est un corps.
7. I est un idéal donc un sous-groupe de A donc contient 0. En particulier, $0^1 \in I$ donc $0 \in \sqrt{I}$, $\sqrt{I}$ est non vide. Soient x et y deux éléments de $\sqrt{I}$: il existe n et k tels que x^n et $y^k \in I$. Alors (on peut appliquer le binôme de Newton puisque l'anneau est commutatif) :

$$(x+y)^{n+k} = \sum_{i=0}^{n+k} \binom{n+k}{i} x^i y^{n+k-i}$$

Si $i \geq k$, $y^{n+k-i}x^i = y^{n+k-i}x^{i-k}x^k \in I$ puisque $x^k \in I$ et I est absorbant. De même, si $i \leq k$, $y^{n+k-i}x^i = x^i y^{k-i}y^n \in I$ pour les mêmes raisons : tous les termes de la somme appartiennent à I donc la somme aussi puisque I est un sous-groupe. On en déduit que $(x + y)^{n+k} \in I$ donc $x + y \in \sqrt{I}$: $\sqrt{I}$ est stable par somme. Enfin $(-x)^k = (-1)^k x^k$ (car l'anneau est commutatif) donc $(-x)^k \in I$ car I absorbant donc $-x \in \sqrt{I}$: $\sqrt{I}$ est un sous-groupe de A. Enfin, il est absorbant : en effet, si $a \in A$, alors (l'anneau est commutatif)

$$(ax)^k = a^k x^k \in I$$

puisque I est absorbant : $ax \in \sqrt{I}$, et l'anneau est commutatif donc $xa \in \sqrt{I}$: $\sqrt{I}$ est absorbant, c'est un idéal. Pour $\sqrt{12\mathbb{Z}}$, on cherche les entiers n dont il existe une puissance divisible par 12. Montrons que $\sqrt{12\mathbb{Z}} = 6\mathbb{Z}$: si $x \in 6\mathbb{Z}$ alors x^2 est divisible par 36 donc par 12 donc $x^2 \in 12\mathbb{Z}$ si bien que $x \in \sqrt{12\mathbb{Z}}$. Réciproquement, si $x \in \sqrt{12\mathbb{Z}}$, alors il existe n tel que x^n soit divisible par 12 donc en particulier x^n est pair et divisible par 3 donc x également : $v_2(x^n) = nv_2(x) > 0$ donc $v_2(x) > 0$ et idem pour $v_3(x)$ donc (2 et 3 sont premiers entre eux) x est divisible par 6, $x \in 6\mathbb{Z}$, ce qui permet de conclure.

Exercice 63 : ✪✪ Soit A un anneau. On suppose que pour tout $(x, y) \in A^2$, $xy = yx$ ou $-yx$.

1. On pose $Z(A) = \{x \in A \,|\, \forall y \in A, xy = yx\}$ (Z est donc le centre de A) et $Y(A) = \{x \in A \,|\, \forall y \in A, xy = -yx\}$. Montrer que $Z(A)$ et $Y(A)$ sont des sous-groupes de A.
2. Montrer par l'absurde que $A = Z(A) \cup Y(A)$.
3. En déduire que A est commutatif.

Correction :

1. Pour $Z(A)$: cf. exercice 45. Pour $Y(A)$: idem.
2. Supposons que $A \neq Z(A) \cup Y(A)$: il existe $a \in A$ tel que $a \notin Z(A) \cup Y(A)$: $a \notin Z(A)$ donc il existe y tel que $ay \neq ya$, et $a \notin Y(A)$ donc il existe $z \in A$ tel que $az \neq -za$. Dès lors, par hypothèse sur A, on a forcément $ay = -ya$ et $az = za$ donc $ay + ay = za - ya$ donc $a(y + z) = (z - y)a$. Or, toujours par hypothèse sur A, $a(y + z) = (y + z)a$ ou $a(y + z) = -(y + z)a$. Dans le premier cas, $(z - y)a = (y + z)a$ donc $za - ya = ya + za$ si bien que $ya = -ya = ay$ ce qui est exclu. Dans le second cas, $(z - y)a = -(y + z)a$ donc $za - ya = -ya - za$ donc $za = -za = -az$ ce qui est aussi exclu. On en déduit que $A = Z(A) \cup Y(A)$.
3. On a une union de sous-groupes de A qui est un sous-groupe de A (A lui-même) : d'après le cours, l'un est inclus dans l'autre donc soit $A = Z(A)$, et alors A est commutatif, soit $A = Y(A)$. Mais alors, tout élément de A est dans $Y(A)$ c'est-à-dire que pour tous x et y, $xy = -yx$ donc, en particulier, pour tout $a \in A$, $a \times 1 = -1 \times a$ donc $a = -a$ donc tout élément est égal à son opposé. En particulier, pour tous x et y, puisque $xy = -yx$, alors $xy = yx$ (tout élément est égal à son opposé) : l'anneau est tout de même commutatif.

Exercice 64 - Un théorème de Kaplansky : ✪✪✪ On se donne dans cet exercice un anneau A commutatif et intègre, et on suppose que pour tout $a \in A$, il existe $b \in A$ tel que $a + b - ba = 0$.

1. Montrer que la loi $*$ définit par $a*b=a+b-ba$ est une loi de composition interne sur $A\backslash\{1\}$ qui en fait un groupe.
2. En déduire que A est un corps.

Correction :

1. Montrons tout d'abord que cette loi est bien interne. Soient x et y deux éléments de $A\backslash\{1\}$ et supposons que $x*y=1$. Alors $x+y-xy=1$ d'où : $x(1-y)=1-y$ ou encore $(x-1)(1-y)=0$. L'anneau étant intègre, $x=1$ ou $y=1$ ce qui est exclu : la loi est bien intègre. Prouvons qu'elle est associative. Soient a,b,c trois éléments de A. D'une part (on ne confondra pas la nouvelle loi $*$ avec le produit qui fait de A un anneau) :
$$\begin{aligned} a*(b*c) &= a*(b+c-cb) \\ &= a+b+c-cb-a(b+c-cb) \\ &= a+b+c-cb-ab-ac+abc \end{aligned}$$
et on trouve la même chose pour $(a*b)*c$: la loi est associative. Il est immédiat que 0 (qui appartient bien à $A\backslash\{1\}$) est un élément neutre (puisqu'il est absorbant, i.e. qu'on a $a0=0a=0$) et, par hypothèse, tout élément $a\in A\backslash\{1\}$ admet un symétrique pour la loi $*$: prouvons que ce symétrique est bien dans $A\backslash\{1\}$. S'il est égal à 1, alors $a+1-a=0$ donc $0=1$ ce qui est absurde : le symétrique est bien dans $A\backslash\{1\}$, c'est bien un groupe.
2. On se dit qu'il faut utiliser la question précédente : on a prouvé que $A\backslash\{1\}$ est un groupe (muni d'une certaine loi) et on veut prouver que A^* est un groupe (muni du produit). Il suffit de prouver que ces ensembles sont isomorphes (en faisant un léger abus de langage puisque A^* n'est pas encore un groupe mais ce n'est pas grave). On cherche une bijection de $A\backslash\{1\}$ dans A^* qui envoie le neutre 0 sur le « futur neutre » 1 mais on veut aussi que la valeur interdite 1 corresponde à la valeur interdite d'arrivée, 0 : on aimerait envoyer 0 sur 1 et « éviter d'envoyer 1 sur 0 » : tout ça pour dire qu'on s'intéresse à
$$f:\begin{cases} A\backslash\{1\} & \to & A^* \\ a & \mapsto & 1-a \end{cases}$$
Alors f est évidemment bijective. Prouvons qu'elle est compatible avec les lois $*$ et $\times$: soient a et b dans $A\backslash\{1\}$. Alors
$$\begin{aligned} f(a*b) &= 1-a*b \\ &= 1-a-b+ba \\ &= (1-a)(1-b) \\ &= f(a)f(b) \end{aligned}$$
D'après l'exercice 22, A^*, muni de la loi $\times$, est un groupe : A est un corps.

Exercice 65 : ✪✪✪ Soit $\mathbb{K}$ un corps. Le but de cet exercice est de prouver que les groupes $(\mathbb{K},+)$ et $(\mathbb{K}^*,\times)$ ne sont pas isomorphes.

1. Démontrer ce résultat lorsque $\mathbb{K}$ est fini. On suppose dans la suite que $\mathbb{K}$ est infini.
2. Soit $\varphi:\mathbb{Z}\to K$ définie par $\varphi(n)=\underbrace{1_\mathbb{K}+\cdots+1_\mathbb{K}}_{n \text{ fois}}$ si $n\geq 0$, et $\varphi(n)=\underbrace{-1_\mathbb{K}-\cdots-1_\mathbb{K}}_{-n \text{ fois}}$ sinon. On rappelle (cf cours) que φ est un morphisme d'anneaux.
   (a) Justifier qu'il existe $p\in\mathbb{N}$ tel que $\ker(\varphi)=p\mathbb{Z}$: p est appelé la caractéristique de $\mathbb{K}$.
   (b) Montrer que p est nulle ou est un nombre premier.
3. Prouver que $(\mathbb{K},+)$ et $(\mathbb{K}^*,\times)$ ne sont pas isomorphes. On s'intéressera à l'équation $x^2=1_\mathbb{K}$.

Correction :

1. Si $\mathbb{K}$ est fini, alors $\mathbb{K}$ et $\mathbb{K}^*$ n'ont pas le même cardinal (fini) donc il n'existe aucune bijection entre ces deux ensembles, et en particulier aucun isomorphisme.
2. (a) Le noyau de φ est un sous-groupe de $\mathbb{Z}$ donc est de la forme $p\mathbb{Z}$ avec $p\in\mathbb{N}$.

(b) Tout d'abord, $p \neq 1$ car on ne peut pas avoir $\ker(\varphi) = \mathbb{Z}$ puisque $\varphi(1) = 1$: on en déduit que $p = 0$ ou $p \geq 2$. Supposons que p ne soit pas nulle et ne soit pas un nombre premier : alors il existe $1 < a, b < p$ tels que $p = ab$. Alors $f(ab) = f(p) = 0$ puisque $\ker(\varphi) = p\mathbb{Z}$, donc $f(a)f(b) = 0$. Or, a et b n'appartiennent pas à $\ker(\varphi) = p\mathbb{Z}$ donc $f(a)$ et $f(b)$ sont non nuls mais $f(a)f(b) = 0$ ce qui est absurde puisque $\mathbb{K}$ est un corps donc un anneau intègre.

3. Raisonnons par l'absurde et supposons que ces deux groupes soient isomorphes, avec $\varphi : \mathbb{K}^* \to \mathbb{K}$ un isomorphisme. Soit $x \in \mathbb{K}$. Puisque φ est un isomorphisme (i.e un morphisme bijectif),

$$\begin{aligned} x^2 = 1 &\iff \varphi(x^2) = \varphi(1) \\ &\iff \varphi(x \times x) = 0 \\ &\iff \varphi(x) + \varphi(x) = 0 \\ &\iff 2\varphi(x) = 0 \end{aligned}$$

Or, $2 = 1_{\mathbb{K}} + 1_{\mathbb{K}} = \varphi(2)$ avec φ la fonction de la question précédente. Supposons que $p \neq 2$ dans la question précédente. Alors $\varphi(2) \neq 0$ donc : $x^2 = 1 \iff \varphi(x) = 0 \iff x = 1$ puisque 1 est l'unique antécédent de 0 par φ, ce qui est absurde puisque $-1 \neq 1$ (puisque $1 + 1 \neq 0$ car $p \neq 2$) est aussi solution de l'équation $x^2 = 1$. Supposons à présent $p = 2$ si bien que $1 + 1 = 0$ et plus généralement $x + x = 0$ pour tout x. Alors tout élément de $\mathbb{K}$ vérifie $x + x = 0$ et, en particulier, vérifie $2\varphi(x) = 0$ c'est-à-dire (par équivalences) que tout élément de $\mathbb{K}$ est solution de $x^2 = 1$: cette équation admet une infinité de solutions, ce qui est absurde car cette équation est équivalente à $(x - 1)(x + 1) = 0$ et $\mathbb{K}$ étant un anneau interne, elle n'admet que ± 1 comme solutions (en fait, une solution puisque $1 = -1$). On en déduit que ces deux groupes ne sont pas isomorphes.

4 Deuxième année : Lagrange, ordre et $\mathbb{Z}/n\mathbb{Z}$

Exercice 66 : ✪ Soit $n \geq 2$. Donner les diviseurs de zéro éventuels de $\mathbb{Z}/n\mathbb{Z}$.

Correction : Montrons que les diviseurs de zéro sont exactement les $\overline{d}$ avec d non multiple de n non premier avec n. En particulier, si n est premier, il n'y a aucun diviseur de zéro non nul (i.e. distinct de $\overline{0}$) ce qui est cohérent avec le fait que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Soit d premier avec n. Alors (cf. cours) $\overline{d}$ est inversible donc n'est pas un diviseur de zéro. Si d est un multiple de n alors $\overline{d} = \overline{0}$ donc n'est pas un diviseur de zéro (un diviseur de zéro est non nul par définition). Soit enfin un entier d non multiple de n et non premier avec n. Puisque n ne divise pas d, alors $\overline{n} \neq \overline{0}$. Soit $m = d \wedge n$ et soit $k = n/m$. Alors $m > 1$ donc $n/d < n$ si bien que $\overline{n/d} \neq \overline{0}$ et $\overline{d} \times \overline{k} = \overline{d/m} \times \overline{n} = \overline{0}$ puisque d/m est entier donc $(d/m) \times n$ est un multiple de n, c'est-à-dire que $\overline{d}$ est un diviseur de zéro.

Exercice 67 : ✪ Soit $n \geq 2$. Donner une CNS sur n pour que $\mathbb{Z}/n\mathbb{Z}$ admette des éléments nilpotents non nuls.

Correction : Un élément $\overline{d}$ est nilpotent s'il existe $k \geq 1$ tel que $\overline{d}^k = \overline{0}$ donc s'il existe k tel que n divise d^k. Supposons que d soit nilpotent. Alors il existe k tel que n divise d^k donc, pour tout p premier, $v_p(n) \leq v_p(d^k) = kv_p(d)$. En particulier, pour tout p facteur premier de n, $1 \leq kv_p(d)$ donc $v_p(d) \neq 0$: tous les facteurs premiers de n sont aussi facteurs premiers de d. Dès lors, les diviseurs de zéro éventuels sont parmi les nombres ayant les mêmes facteurs premiers que n mais qui ne sont pas divisibles par n (on cherche les éléments nilpotents non nuls). Supposons que les facteurs premiers de n soient tous de multiplicité 1 (i.e. n est de la forme $p_1 \times \cdots \times p_k$ avec les p_i premiers distincts). Alors tout nombre d ayant les mêmes facteurs premiers que n est divisible par n donc $\overline{d} = \overline{0}$: il n'y a aucun élément nilpotent non nul. Réciproquement, supposons que les facteurs premiers de n ne soient pas tous de multiplicité 1, i.e. n est de la forme ${p_1}^{\alpha_1} \times \cdots \times {p_k}^{\alpha_k}$ avec les p_i premiers distincts et au moins un $\alpha_i > 1$. Posons $d = p_1 \times \cdots \times p_k$. Alors d n'est pas divisible par n donc $\overline{d}$ est non nul dans $\mathbb{Z}/n\mathbb{Z}$ et $\overline{d}$ est nilpotent. En conclusion, $\mathbb{Z}/n\mathbb{Z}$ admet des éléments nilpotents non nuls si et seulement si les valuations p-adiques de n ne sont pas toutes égales à 1 i.e. n admet au moins un facteur premier dont la puissance est au moins égale à 2.

Exercice 68 : ✪ Expliciter tous les automorphismes de groupes de $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$.

Correction : Commençons par $\mathbb{Z}/2\mathbb{Z}$. Un morphisme de groupes envoie forcément le neutre sur le neutre donc un automorphisme de groupes vérifie forcément $\varphi(\overline{0}) = \overline{0}$, et puisqu'on cherche un morphisme bijectif, il doit forcément vérifie $\varphi(\overline{1}) = \overline{1}$. On en déduit que le seul automorphisme de $\mathbb{Z}/2\mathbb{Z}$ est l'identité.

Passons à présent à $\mathbb{Z}/3\mathbb{Z}$. Raisonnons par analyse-synthèse (c'est un peu ce que nous avons fait ci-dessus) et supposons que φ soit un automorphisme de $\mathbb{Z}/3\mathbb{Z}$. Pour la même raison que ci-dessus, $\varphi(\overline{0}) = \overline{0}$. Par bijectivité de φ, on a soit $\varphi(\overline{1}) = \overline{1}$ et $\varphi(\overline{2}) = \overline{2}$, et alors φ est l'identité (de $\mathbb{Z}/3\mathbb{Z}$), soit $\varphi(\overline{1}) = \overline{2}$ et $\varphi(\overline{2}) = \overline{1}$. Puisque l'identité est évidemment un automorphisme, vérifions que, dans le deuxième cas, on a bien un automorphisme de groupes. Soient x et y deux éléments de $\mathbb{Z}/3\mathbb{Z}$. Si l'un des

deux est égal à $\overline{0}$, disons x, alors $x+y=y$ et $\varphi(x)+\varphi(y)=\varphi(y)$ (puisque $\varphi(\overline{0})=\overline{0}$) donc on a bien $\varphi(x+y)=\varphi(x)+\varphi(y)$. Si $x=y=1$, alors

$$\begin{aligned}\varphi(x+y) &= \varphi(\overline{2})\\ &= \overline{1}\end{aligned}$$

et

$$\begin{aligned}\varphi(x)+\varphi(y) &= \varphi(\overline{1})+\varphi(\overline{1})\\ &= \overline{2}+\overline{2}\\ &= \overline{1}\end{aligned}$$

puisqu'on travaille modulo 3, si bien qu'on a encore $\varphi(x+y)=\varphi(x)+\varphi(y)$, et idem dans tous les autres cas. Finalement, $\mathbb{Z}/3\mathbb{Z}$ admet exactement deux automorphismes : l'identité, et la fonction φ définie par : $\varphi(\overline{0})=\overline{0}, \varphi(\overline{1})=\overline{2}$ et $\varphi(\overline{2})=\overline{1}$.

Plaçons-nous enfin sur $\mathbb{Z}/4\mathbb{Z}$ et raisonnons par analyse synthèse. Soit φ un automorphisme de groupes. On a alors $\varphi(\overline{0})=\overline{0}$. De plus, toujours car c'est un morphisme :

$$\begin{aligned}\varphi(\overline{2})+\varphi(\overline{2}) &= \varphi(\overline{2}+\overline{2})\\ &= \varphi(\overline{0})\\ &= \overline{0}\end{aligned}$$

c'est-à-dire que $2\varphi(\overline{2})=\overline{0}$. Or, les seules solutions de cette équation sur $\mathbb{Z}/4\mathbb{Z}$ sont $\overline{0}$ et $\overline{2}$. De plus, $\varphi(\overline{0})=\overline{0}$ et φ est injective donc $\varphi(\overline{2})=\overline{2}$. Par bijectivité de φ, on a soit $\varphi(\overline{1})=\overline{1}$ et $\varphi(\overline{3})=\overline{3}$, et alors φ est l'identité (de $\mathbb{Z}/4\mathbb{Z}$), soit $\varphi(\overline{1})=\overline{3}$ et $\varphi(\overline{3})=\overline{1}$. On prouve alors réciproquement que la fonction φ définie par : $\varphi(\overline{0})=\overline{0}, \varphi(\overline{1})=\overline{3}$, $\varphi(\overline{2})=\overline{2}$ et $\varphi(\overline{3})=\overline{1}$ est un automorphisme, ce qui fait deux automorphismes avec l'identité.

Exercice 69 : ✪✪ Montrer qu'un sous-groupe d'un groupe cyclique est cyclique.

Correction : Soit G un groupe cyclique. Plus précisément, on suppose que G est cyclique engendré par x d'ordre n i.e. $G=\{e;x;x^2;\dots:x^{n-1}\}$. Soit H un sous-groupe de G. Si $H=\{e\}$ alors H est cyclique. Sinon, posons $k=\min\{i\in[\![1\,;n-1]\!]\,|\,x^i\in H\}$. Montrons que $H=\mathrm{gr}(x^k)$ ce qui permettra de conclure. Soit $y\in H$. Il existe m tel que $y=x^m$. Faisons la division euclidienne de m par k : il existe $q\in\mathbb{Z}$ et $0\leq r<i$ tel que $m=qk+r$ donc $y=x^{qk+r}$ si bien que

$$x^r=x^y\times(x^{qk})^{-1}\in H$$

Par définition de k, cela implique que $r=0$ donc que k divise H. On en déduit que $H\subset\mathrm{gr}(x^k)$ et l'inclusion réciproque est immédiate par définition d'un groupe engendré.

Exercice 70 : ✪✪ Soit $n\geq 2$. Montrer que tous les diviseurs de zéro de $\mathbb{Z}/n\mathbb{Z}$ sont nilpotents si et seulement s'il existe p premier et $\alpha\geq 1$ tel que $n=p^\alpha$.

Correction : Rappelons (cf. exercices 66 et 67) que les diviseurs de zéro sont les $\overline{d}$ avec d non multiple de n et non premiers avec n ou, si on raisonne modulo n, les $\overline{d}$ avec $1<d<n-1$ non premier avec n, et que les éléments nilpotents sont exactement les nombres ayant les mêmes facteurs premiers que n. Si n a au moins deux facteurs premiers, alors il existe des diviseurs de 0 qui ne sont pas nilpotents (prendre un seul facteur premier) tandis que si n a un seul facteur premier i.e. n est de la forme p^α, alors un élément est un diviseur de 0 si et seulement s'il n'est pas premier avec n si et seulement s'il est divisible par p si et seulement s'il est nilpotent.

Exercice 71 : ✪✪ Soit G un groupe. Montrer que G n'admet aucun sous-groupe différent de $\{e\}$ et de lui-même si et seulement si G est fini et $\mathrm{card}(G)$ est un nombre premier. Que dire alors de G ?

Correction : Soit $x\neq e$. Alors $\mathrm{gr}(x)=G$ tout entier car c'est un sous-groupe de G distinct de $\{e\}$. Si G est infini, ce groupe est monogène infini donc isomorphe à $\mathbb{Z}$ ce qui est absurde car $\mathbb{Z}$ admet des sous-groupes distincts de $\{0\}$ et de lui-même : on en déduit que G est fini et cyclique puisque $G=\mathrm{gr}(x)$ monogène fini. Notons p l'ordre de x. Si p n'est pas premier, soit d un diviseur de p distinct de 1 et p. Alors $\mathrm{gr}(x^d)$ est un sous-groupe distinct de $\{e\}$ et de G ce qui est absurde : l'ordre de x est premier, et donc G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Exercice 72 : ✪✪✪ Soit G un groupe fini non abélien. On pose $A=\{(a,b)\in G^2\,|\,ab=ba\}$. Montrer que :

$$\mathrm{card}(A)\leq\frac{5}{8}\times\mathrm{card}(G)^2$$

Remarque : Il en découle que, dans un groupe fini non abélien, la probabilité que deux éléments commutent est inférieure ou égale à 5/8.

Correction : Rappelons (cela découle du théorème de Lagrange, cf. cours) que si H est un sous-groupe strict d'un groupe fini G, alors $\text{card}(H) \leq \text{card}(G)/2$ puisque $\text{card}(H)$ divise $\text{card}(G)$ et que $H \neq G$. L'idée est de s'intéresser au centre : on a $\text{card}(Z(G)) \leq \text{card}(G)/2$ mais en fait on peut faire mieux en définissant un groupe intermédiaire. Soit $x \notin Z(G)$ (possible car le groupe n'est pas abélien) et posons Z_x l'ensemble des éléments qui commutent avec x. Alors (cf. cours) Z_x est un sous-groupe de G et $Z(G)$ est un sous-groupe de G. De plus, $Z(G) \neq Z_x$ car $x \in Z_x$ (x commute avec lui-même) mais $x \notin Z(G)$ (par hypothèse, x n'est pas dans le centre) et $Z_x \neq G$ car x ne commute pas avec tout le monde par hypothèse donc l'ensemble des éléments qui commutent avec x n'est pas le groupe tout entier. On en déduit que $\text{card}(Z(G)) \leq \text{card}(Z_x)/2$ et que $\text{card}(Z_x) \leq \text{card}(G)/2$ donc $\text{card}(Z(G)) \leq \text{card}(G)/4$. Intéressons-nous à présent au cardinal de A. Tout dépend si la première coordonnée x est dans le centre ou non. Si oui, la seconde coordonnée est quelconque, sinon la seconde coordonnée est dans Z_x. Plus précisément :

$$A = \{(x,y) \,|\, x \in Z(G), y \in G\} \cup \{(x,y) \,|\, x \in G \backslash Z(G), y \in Z_x\}$$

On peut même écrire chacun des deux ensembles ci-dessus comme une union disjointe :

$$A = \bigcup_{x \in Z(G)} \{(x,y) \,|\, y \in G\} \bigcup_{x \notin Z(G)} \{(x,y) \,|\, y \in Z_x\}$$

Les unions étant disjointes :

$$\text{card}(A) = \sum_{x \in Z(G)} \text{card}\left(\{(x,y) \,|\, y \in G\}\right) + \sum_{x \in G \backslash Z(G)} \text{card}\left(\{(x,y) \,|\, y \in Z_x\}\right)$$

Or, chaque élément de la première somme est égal à $\text{card}(G)$ et chaque élément de la deuxième somme à $\text{card}(Z_x)$. Dans la première somme, le terme sommé ne dépend pas de l'indice de sommation si bien que :

$$\text{card}(A) = \text{card}(Z(G)) \times \text{card}(G) + \sum_{x \in G \backslash Z(G)} \text{card}(Z_x)$$

Notons $n = \text{card}(G)$ si bien que $\text{card}(Z_x) \leq n/2$:

$$\begin{aligned} \text{card}(A) &\leq \text{card}(Z(G)) \times n + \sum_{x \in G \backslash Z(G)} \frac{n}{2} \\ &\leq \text{card}(Z(G)) \times n + (n - \text{card}(Z(G)))\frac{n}{2} \\ &\leq \text{card}(Z(G)) \times \frac{n}{2} + \frac{n^2}{2} \end{aligned}$$

Il suffit d'utiliser le fait que $\text{card}(Z(G)) \leq n/4$ pour conclure. Il y a égalité lorsque le centre a un cardinal égal à $n/4$ et si pour tout élément x hors du centre, $\text{card}(Z_x) = n/2$: c'est le cas par exemple pour le groupe des quaternions $\mathbb{H}_8$.

Exercice 73 : ✪✪✪

1. Soit $n \geq 1$. Donner les sous-groupes de $\mathbb{U}_n$. On rappelle (cf. chapitre 7) que $\mathbb{U}_d \subset \mathbb{U}_n$ si et seulement si d divise n.
2. Montrer que les seuls sous-groupes finis de $\mathbb{C}^*$ sont de la forme $\mathbb{U}_n$.

Correction :

1. Soit d un diviseur (positif évidemment de n). Alors $\mathbb{U}_d$ est inclus dans $\mathbb{U}_n$ et est un groupe donc est un sous groupe de $\mathbb{U}_n$ (tout ça pour la multiplication). Réciproquement, montrons que tout sous-groupe de $\mathbb{U}_n$ est de cette forme. Raisonnons comme pour les sous-groupes de $\mathbb{Z}$: soit H un sous-groupe de $\mathbb{U}_n$. Si $H = \{1\}$ alors $H = \mathbb{U}_1$. Sinon, il existe $z = e^{2ik\pi/n} \in H$ avec $k \in [\![1\,;n-1]\!]$. Notons $A = \{k \in [\![0\,;n-1]\!] \,|\, e^{2ik\pi/n} \in H\}$. A est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément b. Notons $\omega = e^{2ib\pi/n}$. Soit $z \in H$ qu'on écrit sous la forme $z = e^{2ik\pi/n}$ avec $k \in [\![0\,;n-1]\!]$ et faisons la division euclidienne de k par b : il existe q et r avec $0 \leq r < b$ tel que $k = bq + r$. Or,

$$e^{2ir\pi/n} = e^{2ik\pi/n} \times \frac{1}{\left(e^{2ib\pi/n}\right)^q}$$

Or, $e^{2ib\pi/n} \in H$ et H est stable par produit et par inverse, si bien que $e^{2ir\pi/n} \in H$: par définition de b, cela implique que $r = 0$ donc b divise q : si on note $\omega = e^{2ib\pi/n}$, on vient de prouver que H est inclus dans $\text{gr}(\omega) = \{\omega^k \,|\, k \in \mathbb{N}\}$. L'inclusion réciproque étant immédiate, $H = \text{gr}(\omega)$. Or, $\omega^n = 1$ donc ω est d'ordre un diviseur de n, qu'on note d, si bien que ω est une racine d-ième de l'unité, et donc $\text{gr}(\omega) \subset \mathbb{U}_d$. Or, ω est d'ordre d donc $\text{gr}(\omega)$ est de cardinal d donc on a égalité. Finalement, $H = \mathbb{U}_d$: les sous-groupes de $\mathbb{U}_n$ sont exactement les $\mathbb{U}_d$ avec $d|n$.

2. Les $\mathbb{U}_n$ sont évidemment des sous-groupes finis de $\mathbb{C}^*$ (muni de la multiplication). Réciproquement, soit H un sous-groupe fini de $\mathbb{C}^*$. H étant fini, tout élément de H est d'ordre fini. Soit n le PPCM des ordres du groupe. Soit $x \in H$. Alors l'ordre de x divise n donc $x^n = 1$ si bien que $x \in \mathbb{U}_n$: $H \subset \mathbb{U}_n$, H est donc un sous-groupe de $\mathbb{U}_n$ donc est de la forme $\mathbb{U}_d$ avec $d|n$, ce qui est le résultat voulu.