1. (Eal01) On dit qu'un anneau commutatif est *intègre* lorsque tout élément non nul est *simplifiable* c'est à dire que si $a \neq 0_A$, $ab = 0_A$ entraine $b = 0_A$. Montrer qu'un anneau intègre fini est un corps.

2. (Eal02) Soit $C > 0$. Sur $I =]-C, C[$, on définit une opération $\tilde{+}$ en posant
$$\forall (a,b) \in I^2,\ a \tilde{+} b = \frac{a+b}{1+ab}$$
Vérifier que $\tilde{+}$ est interne, montrer que $(I, \tilde{+})$ est un groupe commutatif. Que peut-on dire de
$$\begin{cases} \mathbb{R} \to I \\ v \mapsto C \operatorname{th} v \end{cases} ?$$

3. (Eal03) Soit $(G, *)$ un groupe tel que $x^2 = e$ pour tous les x de G. En considérant les éléments de la forme $(x * y)^2$, montrer que G est commutatif.

4. (Eal04) Soit A et B deux sous-groupes d'un groupe $(G, .)$. On note AB l'ensemble des produits d'un élément de A par un élément de B. Montrer que AB est un sous-groupe si et seulement si $AB = BA$.

5. (Eal05) Théorème de Lagrange dans le cas commutatif.
Soit G un groupe commutatif fini de cardinal m et de neutre e.
   a. Soit $g \in G$. Montrer que l'application de G dans G qui a tout x de G associe gx est bijective.
   b. On note
   $$P = \prod_{x \in G} x$$
   En utilisant P, montrer que
   $$\forall g \in G, \qquad g^m = e$$

6. (Eal06) Soit A un ensemble muni d'une opération interne, associative . et admettant un élément neutre noté 1_A.
On dit que $a \in A$ est *inversible à droite* si et seulement si il existe $x \in A$ tel que $ax = 1_A$. On dit que a est simplifiable à droite si et seulement si $ax = ay$ entraine $x = y$ pour tous x et y de A. On note g_a l'application de A dans A telle que $g_a(x) = ax$ pour tout x de A.
   a. Montrer que a est simplifiable à droite si et seulement si g_a est injective.
   b. Montrer que a est inversible à droite si et seulement si g_a est surjective.
   c. Montrer que a est inversible si et seulement si g_a est bijective.
   d. Soit a et b deux éléments de A. Montrer que si ab est inversible à droite et ba simplifiable à droite alors a et b sont inversibles.

7. (Eal07) Théorème de Lagrange
Soit G un groupe (notation multiplicative) fini de cardinal m. On veut montrer que pour tout $g \in G$:
$$g^m = e$$
Soit H un sous-groupe de G. On définit une relation R_H dans G en posant
$$\forall (g, g') \in G^2 : gR_H g' \Leftrightarrow g{g'}^{-1} \in H$$
   a. Montrer que $Hg = Hg'$ si et seulement si $gR_H g'$.
   b. Montrer que R_H est une relation d'équivalence.
   c. En déduire que $\operatorname{Card} H$ divise $\operatorname{Card} G$.
   d. Soit $g \in G$, montrer qu'il existe un entier $m_g > 0$ tel que
   $$\{k \in \mathbb{Z} \operatorname{tq} g^k = e\} = \mathbb{Z} m_g$$
   e. En considérant le sous-groupe engendré par g, montrer le théorème de Lagrange.

8. (Eal08) Soit A un anneau et $z \in A$ est un élément *nilpotent* c'est à dire tel qu'il existe un entier non nul n, tel que $z^n = 0_A$.
   a. Montrer que
   $$1_A + z + z^2 + \cdots + z^{n-1}$$
   est inversible d'inverse $1_A - z$.
   b. Montrer que
   $$1_A + 2z + \cdots + nz^{n-1}$$
   est inversible d'inverse $(1_A - z)^2$.
   c. Soit $p \in \mathbb{N}$, montrer que
   $$\sum_{k \in \{0, \cdots n-1\}} \binom{k+p}{p} z^k$$
   est inversible et préciser son inverse.

9. (Eal09) Soit G un groupe et A une partie finie de G non vide et stable pour l'opération de G. Montrer que A est un sous-groupe.

10. (Eal10) Automorphismes intérieurs.
Soit G un groupe. Pour tout $a \in G$, on définit une applications c_a de G dans G par :
$$\forall x \in G : c_a(x) = axa^{-1}$$
   a. Montrer que c_a est un automorphisme de groupe
   b. Montrer que l'application $a \to c_a$ est un morphisme de groupe.

11. (Eal11) Sous-groupe distingué.
Soit G (notation multiplicative de l'opération) un groupe et H un sous-groupe. On dira que H est *distingué* lorsque :
$$\forall a \in G, \forall h \in H : a^{-1}ha \in H$$
Montrer que si H est distingué alors
$$\forall (g, g') \in G^2 : gH\, g'H = gg'H.$$

12. (Eal12) Sous-groupe des commutateurs.
Soit G un groupe, un *commutateur* est un élément de G de la forme
$$aba^{-1}b^{-1}\ (a,b) \in G^2$$
Soit H le sous-groupe engendré par l'ensemble de tous les commutateurs.
   a. Montrer que H est distingué.

b. Montrer que :
$$\forall (g,g') \in G^2 : gH\,g'H = g'H\,gH$$

13. (Eal13) Soit A et B deux sous-groupe d'un groupe $(G,*)$. Montrer que $A \cup B$ est un sous-groupe de $(G,*)$ si et seulement si $A \subset B$ ou $B \subset A$.

14. (Eal14) Soit A un anneau non commutatif et $a \in A$. On définit une application φ_a de A dans A par :
$$\forall b \in A : \varphi_a(b) = ab - ba$$
Soit n un entier. Trouver une jolie formule pour
$$\varphi_a^n(b) = \varphi_a \circ \cdots \varphi_a(b)$$
Que peut-on en déduire si a est nilpotent (ie il existe n tel que $a^n = 0_A$) ?

15. (Eal15) Soit G un groupe et A une partie de G. On désigne par A' l'ensemble des inverses des éléments de A.
    a. Soit z un élément de G. On désigne par zA' l'ensemble des zb pour $b \in A'$. On suppose A fini. Montrer que zA' est fini et contient le même nombre d'éléments que A.
    b. On suppose que G est fini et que $\sharp A > \frac{1}{2}\sharp G$. Montrer que tout élément de G est le produit de deux éléments de A.

16. (Eal16) Dérivations dans un anneau.
Soit A un anneau (pas forcément commutatif). On dira qu'une application D de A dans A est une *dérivation* lorsqu'elle vérifie :
$$\forall (a,b) \in A^2 : \begin{cases} D(a+b) = D(a) + D(b) \\ D(ab) = D(a)b + aD(b) \end{cases}$$
    a. Montrer que $D(1_A) = 0_A$ et $D(0_A) = 0_A$.
    b. Soit D_1 et D_2 deux dérivations, montrer que
    $$D_1 \circ D_2 - D_2 \circ D_1$$
    est une dérivation.
    c. On suppose A commutatif. Montrer que pour tout $a \in A$ et $n \in \mathbb{N}^*$
    $$D(a^n) = nD(a)a^{n-1}$$
    Si a est inversible, montrer que la formule est valable pour $n \in \mathbb{Z}$.

17. (Eal17) Action de groupe.
Soit G un groupe et Ω un ensemble. Les deux sont supposés finis. On désigne par $S(\Omega)$ le groupe des bijections (permutations) de Ω muni de la composition.
Une *action* de G sur Ω est un morphisme de groupe (noté A) de G dans $S(\Omega)$. On notera A_g au lieu de $A(g)$, il s'agit d'une permutation des éléments de Ω.
Pour tout $\omega \in \Omega$, on note :
$$G_\omega = \{g \in G \text{ tq } A_g(\omega) = \omega\}$$
$$O_\omega = \{A_g(\omega)\ ,\ \forall g \in G\}$$
On dit que G_ω est le *stabilisateur* de ω et que O_ω est l'*orbite* de ω.
    a. Montrer que G_ω est un sous-groupe de G.
    b. Soit $\omega_1 \in O_\omega$ et $g_0 \in A$ tel que $A_{g_0}(\omega) = \omega_1$. Soit U l'ensemble des $g \in G$ tels que $A_g(\omega) = \omega_1$. Montrer que U et G_ω ont le même nombre d'éléments. En déduire le nombre d'éléments de l'orbite de ω.
    c. Montrer que les orbites constituent une partition de Ω.

18. (Eal18) On définit une opération $*$ dans $\mathbb{R}$ en posant,
$$\forall (x,y) \in \mathbb{R}^2,\ x * y = x\sqrt{1+y^2} + y\sqrt{1+x^2}$$
    a. Pour tous t et u réels, trouver une expression simple de
    $$\mathrm{sh}(t) * \mathrm{sh}(u)$$
    b. L'opération $*$ définit-elle une structure de groupe sur $\mathbb{R}$?

19. (Eal19) Soit A un ensemble *fini* muni d'une opération (interne) *associative* notée ".", soit a un élément de A. Montrer que la suite $(a^n)_{n\in\mathbb{N}^*}$ est périodique à partir d'un certain rang.

20. (Eal20) Soit E un ensemble muni d'une opération interne $*$ associative et admettant un élément neutre e. Pour tout élément a de E, on note δ_a l'application (dite multiplication à droite par a)
$$E \to E$$
$$x \to x * a$$
    a. Soit a et b dans E. Que vaut $\delta_a \circ \delta_b$?
    b. Montrer que a inversible entraine δ_a bijective. Que vaut alors la bijection réciproque ?
    c. Montrer que δ_a bijective entraine a inversible.
    d. On suppose E fini. Montrer que a inversible à droite entraine a inversible.

21. (Eal21) Soit G un groupe. On suppose qu'il existe $k \in \mathbb{Z}$ tel que
$$\forall (a,b) \in G^2, \forall i \in \{k-1, k, k+1\} : (ab)^i = a^i b^i$$
Montrer que G est commutatif.

22. (Eal22) Soit G un ensemble non vide muni d'une loi associative $*$ admettant un neutre à droite e :
$$\forall g \in G,\ g * e = g$$
et telle que tout élément admette un inverse à droite :
$$\forall g \in G,\ \exists g' \in G \text{ tq } g * g' = e$$
Montrer que $*$ définit une structure de groupe.

23. (Eal23) Soit Ω un ensemble muni d'une opération interne $*$ associative pour laquelle il existe un élément neutre e. Soit f une application bijective de Ω dans Ω vérifiant
$$\forall (a,b) \in \Omega^2,\ f(a*b) = f(a) * f(b)$$
Montrer que, pour tout $a \in \Omega$,
$$f(a) = e \Leftrightarrow a = e$$
Soit I l'ensemble des éléments inversibles de Ω. Montrer que, pour tout $x \in \Omega$,
$$f(x) \in I \Leftrightarrow x \in I$$

24. (Eal24) Soit E un ensemble muni de deux opérations notées $+$ et $*$. Ces opérations vérifient seulement les deux propriétés suivantes :

$$\exists e \in E \text{ tq } \forall a \in E,\ a+e=e+a=a=e*a=a*e$$
$$\forall (a,b,a',b') \in E^4,\ (a+b)*(a'+b') = (a*a')+(b*b')$$

Montrer que $+ = *$ et que cette opération est commutative et associative.

25. (Cal25) On définit une opération $*$ interne dans $\mathbb{Z}^3$:

$$\begin{aligned}&\forall (u,v,w) \in \mathbb{Z}^3, \forall (x,y,z) \in \mathbb{Z}^3,\\ &\qquad (u,v,w)*(x,y,z)\\ &\qquad = (u+(-1)^v x, v+(-1)^w y, w+(-1)^u z).\end{aligned}$$

Cette opération est-elle associative ? admet-elle un élément neutre ?

26. (Eal25) Une présentation de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
Soit $(G,*)$ un groupe commutatif. On note $\mathcal{M}$ l'ensemble des morphismes de $(G,*)$. Un *morphisme* de $(G,*)$ est une application p de G dans G telle que

$$\forall (g,g') \in G^2,\ p(g*g') = p(g)*p(g').$$

a. Exemple. Soit $m \in \mathbb{Z}$, on définit p_m de G dans G par :
$$\forall g \in G,\ p_m(g) = g^m.$$
Montrer que $p_m \in \mathcal{M}$.

b. Opérations.
Pour tout $(p,p') \in \mathcal{M}^2$, on définit $p+p'$ par :
$$\forall g \in G,\ (p+p')(g) = p(g)*p'(g).$$
Montrer que $p+p' \in \mathcal{M}$. Montrer que $(\mathcal{M},+,\circ)$ est un anneau. Préciser les deux éléments neutres.

c. Cas particulier.
Ici, n est un entier naturel non nul, $(G,*)$ est le groupe multiplicatif des racines n-ièmes de l'unité $(\mathbb{U}_n,.)$ avec la multiplication complexe.
Montrer que, pour tout $p \in \mathcal{M}$, il existe un unique $r \in [\![0,n-1]\!]$ tel que $p = p_r$.
Que dire de $p_r + p_{r'}$ et $p_r \circ p_{r'}$ pour r et r' dans $[\![0,n-1]\!]$?

1. (Cal01) Soit A un anneau intègre fini de cardinal n et a un élément non nul de A. On veut montrer que a est inversible. Considérons l'application de $\mathbb{N}^*$ dans A qui à un entier k associe a^k. Comme A est fini et $\mathbb{N}^*$ infini, cette application n'est pas injective. Il existe donc des entiers $i < j$ dans $\mathbb{N}^*$ tels que $a^i = a^j$.
Remarquons que $a^i \neq 0_A$ car s'il l'était, en simplifiant par a on obtiendrait a^{i-1} nul et ainsi de suite jusqu'à une contradiction. On peut donc simplifier par a^i et obtenir
$$a^{j-i} = 1_A$$
avec $j-i > 0$. On en déduit que a est inversible d'inverse a^{j-i-1}.
2. pas de correction pour Eal02.tex
3. (Cal03) On veut montrer que
$$\forall (x,y) \in G^2,\ x * y = y * x.$$
Or :
$$\begin{aligned}
&(x*y)^2 = e = x*y*x*y \\
&\quad \Rightarrow x = y*x*y \text{ (avec } x* \text{ à gauche et } x^2 = e) \\
&\quad\quad \Rightarrow y*x = x*y \text{ (avec } y* \text{ à gauche et } y^2 = e).
\end{aligned}$$
4. pas de correction pour Eal04.tex
5. (Cal05)
   a. L'application $x \to gx$ est injective car on peut multiplier à gauche par g^{-1}. On en déduit qu'elle est bijective car c'est une application d'un ensemble *fini* dans lui même.
   b. D'après la première question P est aussi le produit des gx donc
$$P = \prod_{x \in G} (gx) = g^m P \Rightarrow g^m = e$$
en multipliant par P^{-1}.
6. (Cal06)
   a. Avec la définition de g_a, il s'agit d'une simple reformulation des propriétés.
   b. Supposons a inversible à gauche. Il existe alors b tel que $ab = 1_A$. On en déduit la surjectivité de g_a car, pour tout $y \in A$,
$$aby = y \Rightarrow g_a(by) = y$$
Supposons g_a surjectif. Il existe alors b tel que $g_a(b) = 1_A$ c'est à dire $ab = 1_A$.
   c. Supposons a inversible (des deux côtés). L'inversibilité à gauche entraine que g_a est surjective. Si x et y dans A sont tels que $g_a(x) = g_a(y)$ alors $ax = ay$ et en multipliant à gauche par l'inverse a^{-1} on obtient $x = y$ c'est à dire l'injectivité de g_a.
Supposons g_a bijectif. De la surjectivité, on tire l'existence d'un b tel que $ab = 1_A$. On multiplie à droite par a et on utilise l'injectivité
$$aba = a \Rightarrow g_a(ba) = g_a(1_A) \Rightarrow ba = 1_A$$
   d. Il est immédiat que $g_x \circ g_y = g_{xy}$. On peut reformuler les hypothèses de manière ensembliste.
$$\left.\begin{aligned}
g_a \circ g_b \text{ surjectif} \Rightarrow g_a \text{ surjectif} \\
g_b \circ g_a \text{ injectif} \Rightarrow g_a \text{ injectif}
\end{aligned}\right\} \Rightarrow g_a \text{ bijectif} \Rightarrow a \text{ inversible}$$
puis pour l'inversibilité de b :
$$\left.\begin{aligned}
g_a \circ g_b \text{ surjectif} \\
g_a \text{ bijectif}
\end{aligned}\right\} \Rightarrow g_b \text{ surjectif}$$
$$\left.\begin{aligned}
g_b \circ g_a \text{ injectif} \\
g_a \text{ bijectif}
\end{aligned}\right\} \Rightarrow g_b \text{ injectif}$$
7. (Cal07) Théorème de Lagrange.
   a. Si $Hg = Hg'$ alors $g = eg \in Hg = Hg'$ donc il existe $h \in H$ tel que
$$g = hg' \Rightarrow gg'^{-1} \in H$$
Réciproquement, supposons $gg'^{-1} \in H$.
$$\forall x \in Hg,\ \exists h \in H \text{ tq } x = hg = \underbrace{h(gg'^{-1})}_{\in H} g' \in Hg'$$
On en déduit $Hg \subset Hg'$.
On obtient l'autre inclusion en échangeant les rôles de g et g'. On peut le faire car
$$g'g^{-1} = (gg'^{-1})^{-1} \in H$$
   b. Réflexivité : un sous-groupe contient le neutre
$$gg^{-1} = e \in H \Rightarrow g\mathcal{R}_H g$$
Symétrie : par stabilité de H pour l'inversion :
$$\begin{aligned}
g\mathcal{R}_H g' \Rightarrow gg'^{-1} \in H \Rightarrow (gg'^{-1})^{-1} \in H \\
\Rightarrow g'g^{-1} \in H \Rightarrow g'\mathcal{R}_H g
\end{aligned}$$
Transitivité : stabilité de H pour l'opération.
$$\left.\begin{aligned}
g\mathcal{R}_H g' \\
g'\mathcal{R}_H g''
\end{aligned}\right\} \Rightarrow \left.\begin{aligned}
gg'^{-1} \in H \\
g'g''^{-1} \in H
\end{aligned}\right\} \Rightarrow gg''^{-1} = gg'^{-1}g'g''^{-1} \in H \Rightarrow g\mathcal{R}_H g''$$
   c. Comme $\mathcal{R}_H$ est une relation d'équivalence, ses classes forment une partition de G. D'après la question a., chacune de ses classes est de la forme Hg et contient donc $\operatorname{Card} H$ éléments. Toutes les classes ont le même nombre d'éléments $\operatorname{Card} H$.
$$\operatorname{Card} G = \text{Nb classes} \times \text{Nb elts dans une classe}$$
Si on note p le nombre de classes, on obtient
$$\operatorname{Card} G = p \times \operatorname{Card} H$$
qui traduit que $\operatorname{Card} H$ divise $\operatorname{Card} G$.

d. L'ensemble
$$N = \{k \in \mathbb{Z} \text{ tq } g^k = e\}$$
est un sous groupe de $(\mathbb{Z}, +)$. Il existe donc (cours) un unique $m_g \in \mathbb{N}$ tel que
$$N = m_g \mathbb{Z}$$

e. On vérifie que le sous-groupe de G engendré par g est
$$\{e, g, \cdots, g^{m_g - 1}\}$$
Il est donc de cardinal m_g. D'après la question c., il existe un entier p tel que
$$\operatorname{Card} G = p\, m_g \Rightarrow g^{\operatorname{Card} G} = (g^{m_g})^p = e^p = e$$

8. pas de correction pour Eal08.tex
9. (Cal09) Il s'agit en fait de montrer que la partie A est stable par inversion. C'est à dire que pour tout $a \in A$ l'inverse de A est encore dans A.
Si $a = e$ c'est évident. Supposons $a \neq e$. Comme A est stable, on peut définir une application $n \mapsto a^n$ de $\mathbb{N}^*$ dans A. Comme A est finie, cette application n'est pas injective. Il existe donc $p < q$ dans $\mathbb{N}^*$ tels que
$$a^p = a^q \Rightarrow a^{q-p-1} * a = e \Rightarrow a^{q-p-1} = a^{-1}.$$
Par définition $q - p - 1 \geq 0$ et l'inégalité est stricte sinon on aurait $a^{-1} = e = a$. Donc a^{-1} s'exprime comme une puissance de a avec un exposant naturel non nul. Par stabilité de A, ceci entraîne $a^{-1} \in A$.
10. pas de correction pour Eal10.tex
11. (Cal11) On suppose H distingué et on prouve les deux inclusions.
Pour tout $z \in gHg'H'$, il existe h et h' dans H tels que
$$z = ghg'h' = gg'\underbrace{(g'^{-1}hg')}_{\in H}h' \in gg'\,H.$$
Pour tout $z \in gg'\,H$, il existe $h \in H$ tel que
$$z = gg'h = g\underbrace{(g'hg'^{-1})}_{\in H}g'\underbrace{e}_{\in H} \in gH\,g'H.$$
12. pas de correction pour Eal12.tex
13. pas de correction pour Eal13.tex
14. pas de correction pour Eal14.tex
15. (Cal15)

a. L'inversion définit une bijection de A dans A'. La multiplication à droite par un z fixé est injective car on peut multiplier à gauche par z^{-1}. On en déduit que zA' a le même nombre d'éléments que A.

b. Pour tout z,
$$\sharp A + \sharp zA' = 2\sharp A > \sharp G$$
On en déduit que ces deux parties ne sont pas disjointes. Il existe a et b dans A tel que $a = zb^{-1}$ donc $z = ab$. Tout élément de G est produit de deux éléments de A.

16. pas de correction pour Eal16.tex
17. (Cal17) Le fait que A soit un morphisme se traduit par $A_{gh} = A_g \circ A_h$ et entraine aussi que $(A_g)^{-1} = A_{g^{-1}}$.

a. On vérifie les stabilités, si g et h sont dans G_ω,
$$A_{gh}(\omega) = A_g \circ A_h(\omega) = A_g(A_h(\omega)) = A_g(\omega) = \omega$$
Donc $gh \in G_\omega$. Comme A_g est une bijection, si $A_g(\omega) = \omega$, l'élément ω est son propre antécédent par A_g. On en déduit
$$\omega = A_{g^{-1}}(\omega) = A_{g^{-1}}(\omega)$$
donc $g^{-1} \in G_\omega$.

b. Soit $g_0 \in U$ c'est à dire $A_{g_0}(\omega) = \omega_1$. Pour tout $g \in G_\omega$, on a alors
$$A_{g_0 g}(\omega) = A_{g_0}(A_g(\omega)) = A_{g_0}(\omega) = \omega_1$$
On peut donc définir une application
$$\varphi : \begin{cases} G_\omega \to U \\ \quad g \to g_0 g \end{cases}$$
Cette application est injective car on peut multiplier à gauche par g_0^{-1}. Elle est surjective car, pour tout $h \in U$, l'élément $g_0^{-1}h$ est dans $G\omega$ et c'est un antécédent de h pour φ. C'est donc une bijection ce qui assure
$$\sharp G_\omega = \sharp U$$
Classons les éléments de G suivant la valeur de $A_g(\omega)$. On forme ainsi autant de classes qu'il y a d'éléments dans l'orbite. Soit ω_1 un élément de l'orbite, la classe associée est formée par les g tels que $A_g(\omega) = \omega_1$. Il s'agit donc de l'ensemble U du début de la question, il contient $\sharp G_\omega$ éléments qui est indépendant du ω_1 de l'orbite. Toutes les classes ont donc le même nombre d'éléments qui doit donc diviser le cardinal de G. On en déduit que le nombre d'éléments d'une orbite est
$$\frac{\sharp\, G}{\sharp\, G_\omega}$$

c. Tout élément de Ω est au moins dans une orbite : la sienne ! Supposons que deux orbites se coupent. Il existe alors ω_1, ω_2 dans Ω et g_1, g_2 dans G tels que $A_{g_1}(\omega_1) = A_{g_2}(\omega_2)$. On en déduit
$$\omega_1 = A_{g_1}^{-1} \circ A_{g_2}(\omega_2) = A_{g_1^{-1}g_2}(\omega_2)$$
Donc ω_1 est dans l'orbite de ω_2, on en déduit que l'orbite de ω_1 est dans celle de ω_2. On peut intervertir les rôles, les deux orbites sont donc égales lorsqu'elles se coupent.

18. (Cal18)

a. D'après les définitions de sh et ch,
$$\begin{aligned} \operatorname{sh}(t) * \operatorname{sh}(u) &= \operatorname{sh}(t)\operatorname{ch}(u) + \operatorname{sh}(u)\operatorname{ch}(t) \\ &= \frac{1}{4}\left(e^{t+u} + e^{-t+u} - e^{-t+u} - e^{-t-u}\right) \\ &= \operatorname{sh}(t+u) \end{aligned}$$

b. L'application sh est une bijection de $\mathbb{R}$ dans $\mathbb{R}$ qui transporte l'opération "$+$" sur l'opération "$*$". Celle ci définit donc une structure de groupe sur $\mathbb{R}$. Pour cette opération, sh est un isomorphisme de groupe de $(\mathbb{R},+)$ sur $(\mathbb{R},*)$.

19. pas de correction pour Eal19.tex

20. (Cal20)

a. Si a est inversible on vérifie facilement que $\delta_{a^{-1}}$ est la bijection réciproque de δ_a.

b. $\delta_a \circ \delta_b = \delta_{b*a}$.

c. Supposons δ_a bijective et notons b l'antécédent de e. On a donc $b*a=e$. Mais a-t-on $a*b=e$?
En fait
$$\delta_a \circ \delta_b = \delta_{b*a} = \delta_e = \operatorname*{Id}_E$$
Comme δ_a est bijective, on peut composer à gauche par la bijection réciproque et obtenir :
$$\delta_b = (\delta_a)^{-1}$$
De plus $a = e*a = \delta_a(e)$ donc
$$a*b = \delta_b(a) = \delta_b \circ \delta_a(e) = e$$

21. (Cal21) La propriété est évidente si $k \in [\![-2,3]\!]$. En effet dans ce cas la propriété est valable pour $i=-1$ ou pour $i=2$. Pour $i=-1$:
$$(ab)^{-1} = a^{-1}b^{-1} \Rightarrow b^{-1}a^{-1} = a^{-1}b^{-1}$$
Autrement dit, tous les inverses commutent. Mais comme tous les éléments du groupe sont des inverses, le groupe est commutatif.
Pour $i=2$:
$$(ab)^2 = a^2b^2 \Rightarrow abab = aabb \Rightarrow ba = ab$$
En multipliant à gauche par a^{-1} et à droite par b^{-1}.
Pour $k\in\mathbb{Z}$, on va d'abord montrer que le b quelconque commute avec certaines puissances.
$$\begin{aligned} ab = (ab)^k(ab)^{-(k-1)} &= (ab)^k((ab)^{k-1})^{-1} \\ = a^kb^k(a^{k-1}b^{k-1})^{-1} &= a^kb^kb^{-(k-1)}a^{-(k-1)} \\ &= a^kba^{-(k-1)} \Rightarrow ba^{k-1} = a^{k-1}b \end{aligned}$$
$$\begin{aligned} ab = (ab)^{k+1}(ab)^{-k} &= (ab)^{k+1}((ab)^k)^{-1} \\ = a^{k+1}b^{k+1}(a^kb^k)^{-1} &= a^{k+1}b^{k+1}b^{-k}a^{-k} \\ &= a^{k+1}ba^{-k} \Rightarrow ba^k = a^kb \end{aligned}$$
Si b commute avec les puissances $k-1$ de *tous* les éléments de G, il commute aussi avec toutes les puissances $-(k-1)$ car il suffit de considérer l'inverse. On peut donc écrire
$$ba = ba^ka^{-(k-1)} = a^kba^{-(k-1)} = a^ka^{-(k-1)}b = ab$$

22. (Cal22) Pour g quelconque, il existe g' tel que $g*g'=e$. Montrons que $g'*g=e$.
Il existe $g''\in G$ tel que $g*g''=e$. En multipliant à gauche par g' puis à droite par g'' :
$$\begin{aligned} g*g'=e \Rightarrow g'*g*g' = g' \Rightarrow g'*g*g'*g'' = g'*g'' \\ \Rightarrow g'*g = e \end{aligned}$$
On en déduit que e est un véritable élément neutre c'est à dire qu'il est neutre à gauche.
$$\forall g\in G,\ e*g = (g*g')*g = g$$

23. (Cal23)
– Montrons que $f(e)=e$. Par surjectivité, pour tout $x\in\Omega$, il existe $y\in\Omega$ tel que $f(y)=x$. Alors :
$$\begin{aligned} x*f(e) = f(y*e) = f(y) = x \\ f(e)*x = f(e*y) = f(y) = x \end{aligned}$$
– Réciproquement, par injectivité de f
$$f(a)=e \Rightarrow f(a)=f(e) \Rightarrow a=e$$
– Si $x\in I$ alors $f(x)\in I$. En effet :
$$\begin{aligned} x*x^{-1}=e \Rightarrow f(x)*f(x^{-1}) = f(e) = e \\ x^{-1}*x = e \Rightarrow f(x^{-1})*f(x) = f(e) = e \end{aligned}$$
ce qui entraine $f(x)$ inversible d'inverse $f(x^{-1})$.
– Supposons $f(x)$ inversible. Il admet un inverse et, comme f est surjective, il existe y tel que
$$\begin{aligned} f(x)^{-1} = f(y) \Rightarrow f(x*y) = f(x)*f(y) = e \\ \Rightarrow x*y = e \end{aligned}$$
De même de l'autre côté, x est donc inversible d'inverse y.

24. (Cal24) Montrer que les opérations sont égales, c'est montrer que
$$\forall (a,b)\in E^2,\ a+b = a*b$$
Considérons la deuxième propriété dans le cas particulier
$$(a+e)*(b+e) = (a*b)+(e*e)$$
puis utilisons la première (e est neutre pour les deux opérations)
$$a+b = a*b+e = a*b$$
On considère ensuite
$$(e+b)*(a+e) = (e*a)+(b*e) \Rightarrow b*a = a+b = a*b$$
et enfin, pour tout $c\in E$,
$$(a+b)*(e+c) = a+(b*c) \Rightarrow (a+b)*c = a+(b*c)$$
comme $* = +$, on obtient bien l'associativité.

25. pas de correction pour Eal26.tex

26. pas de correction pour Eal25.tex