

Eléments de théorie des groupes

Correction des exercices

Enoncés de Josette Calais.
Résolutions de Oestromemes abonnez vous

Table des matières

1	Structure de groupe	2
2	Classes modulo un sous-groupe	16

STRUCTURE DE GROUPE

1) Soit \mathbb{Z} l'ensemble des entiers rationnels, muni de la loi de composition interne notée $*$, définie par :

$$\begin{aligned} * : \mathbb{Z} \times \mathbb{Z} &\rightarrow \mathbb{Z}, \\ (a, b) &\mapsto a - b. \end{aligned}$$

- a) La loi $*$ est-elle associative? commutative?
 b) Vérifier qu'il existe dans $(\mathbb{Z}, *)$ un élément neutre à droite, c'est-à-dire un élément e tel que

$$\forall a \in \mathbb{Z}, a * e = a.$$

e est-il neutre dans $(\mathbb{Z}, *)$?

- c) Existe-t-il, pour tout $a \in \mathbb{Z}$, un symétrique à droite relativement à e , c'est-à-dire un élément a' tel que $a * a' = e$

-
- a) $\forall a, b, c \in \mathbb{Z}, (a * b) * c = a - b - c$, et $a * (b * c) = a - b + c$, la loi n'est pas associative (Comme tu le fais très juste après, il faut donner un contre exemple explicite *i.e.* donner un exemple d'entiers a, b et c tels que $a - b - c \neq a - b + c$. Ce n'est pas trivial car si l'on remplace \mathbb{Z} par $\mathbb{Z}/2\mathbb{Z}$, de telles valeurs n'existent pas.). Et $2 * 1 = 1 \neq -1 = 1 * 2$ montre qu'elle n'est pas non plus commutative.
 b) On vérifie que 0 est un neutre à droite pour $*$: $\forall a \in \mathbb{Z}, a * 0 = a - 0 = a$. Il n'est cependant pas un neutre pour $*$, car $0 * a = -a \neq a$ (Même remarque que précédemment.).
 c) $\forall a \in \mathbb{Z}, a * a' = e \Rightarrow a = a'$. Pour tout élément $a \in \mathbb{Z}$, a est son propre inverse à droite.

2) Soit \mathbb{Q} l'ensemble des nombres rationnels muni de la loi de composition interne notée $*$ définie par :

$$\begin{aligned} * : \mathbb{Q} \times \mathbb{Q} &\rightarrow \mathbb{Q}, \\ (a, b) &\mapsto a + b + ab. \end{aligned}$$

$(\mathbb{Q}, *)$ est-il un groupe?

La loi $*$ admet 0 comme élément neutre, en effet, $a * 0 = 0 * a = a$. Cependant, -1 n'est pas symétrisable par cette loi, car on a $a * -1 = a - 1 - a = -1$ ($\neq 0$, pour tout $a \in \mathbb{Q}$, mais je pinaille), donc $(\mathbb{Q}, *)$ n'est pas un groupe.

3) Soit G un ensemble non vide muni d'une loi de composition interne *associative* notée \cdot : on suppose que dans (G, \cdot) les deux conditions suivantes sont vérifiées :

- 1° il existe un élément *neutre à droite* e (voir exercice 1);
 2° tout élément $x \in G$ admet un *symétrique à droite*, x' (voir exercice 1).

Démontrer que (G, \cdot) est un groupe; vérifier, par un contre exemple, que, sans l'associativité de la loi \cdot , ce résultat n'est plus vrai.

Montrons que le symétrique à droite de tout élément a de G est aussi son symétrique à gauche.

$$\begin{aligned} aa' = e &\Rightarrow a'(aa') = a', \\ &\Rightarrow (a'a)a' = a'. \end{aligned}$$

En multipliant des deux cotés par le symétrique à droite de a' , on obtient :

$$a'a = e.$$

Ainsi, le symétrique à droite de a est aussi son symétrique à gauche.

Montrons que le neutre à droite de G est aussi un neutre à gauche, et donc un neutre tout court.

$$\begin{aligned} \forall a \in G, \quad ea &= (aa')a, \\ &= a(a'a), \\ &= a. \end{aligned}$$

Ainsi, le neutre à droite de G est aussi un neutre à gauche.

(G, \cdot) est donc un groupe.

On vérifie (Mieux que ça! on l'a vérifié à l'exo 1 (tu as fait le travail pénible une fois, autant le mettre en avant le plus possible)) que pour $(\mathbb{Z}, -)$, la loi n'est pas associative, mais que 0 est un neutre à droite (et non à gauche) et que tout élément est symétrisable.

4) Soit G un ensemble *fini*, non vide, muni d'une loi de composition interne notée \cdot ; on suppose que la loi \cdot est associative et que dans (G, \cdot) tout élément est simplifiable à droite et à gauche.

Démontrer que (G, \cdot) est un groupe.

Tout les éléments étant simplifiables à droite implique que les applications (Même si je comprends ce que tu voulais dire, cette phrase n'a pas vraiment de sens. Pour la rendre correcte, tu peux dire "« Tous les éléments sont simplifiables » implique que les applications... ", ou mieux, "Comme tous les éléments de G sont simplifiables, les applications...") :

$$\begin{aligned} \tau_g^y : G &\rightarrow G, & \tau_d^y : G &\rightarrow G \\ x &\mapsto yx, & x &\mapsto xy, \end{aligned}$$

Sont injectives. Le cardinal de G étant fini, ces translations sont bijectives.

Ainsi, pour a et b fixé, les équations $a = xb$ et $a = bx$ ont chacune une unique solution.

En particulier, pour chaque élément a de G , il existe des uniques e_d^a et e_g^a tel que $a = e_d^a a$ et $a = ae_g^a$.

Vérifions qu'ils sont égaux :

$$\begin{aligned} \forall a \in G, \quad aa &= aa, \\ a(e_g^a a) &= (ae_d^a)a, \\ ae_g^a a &= ae_d^a a, \\ ae_g^a &= ae_d^a \text{ (Simplification à droite),} \\ e_g^a &= e_d^a \text{ (Simplification à gauche).} \end{aligned}$$

Vérifions maintenant que tout les éléments ont le même neutre :

$$\begin{aligned} \forall a, b \in G, \quad ab &= ab, \\ (ae^a)b &= a(e^b b), \\ ae^a b &= ae^b b, \\ ae^a &= ae^b \text{ (Simplification à droite),} \\ e^a &= e^b \text{ (Simplification à gauche).} \end{aligned}$$

Ainsi, dans G , il existe un unique élément neutre e .

Reste à montrer que chaque élément a admet un unique inverse a^{-1} .

On sait que les équations $e = ax$ et $e = xa$ ont une unique solution chacune, notées respectivement a_g^* et a_d^* . Vérifions qu'il est le même des deux cotés, et est donc l'inverse de a .

$$\begin{aligned}\forall a \in G, \quad a &= a, \\ a(a_g^*a) &= (aa_d^*)a, \\ aa_g^*a &= aa_d^*a, \\ a_g^* &= a_d^* \text{ en simplifiant à droite et à gauche.}\end{aligned}$$

Chaque élément possède un unique inverse, et G possède un élément neutre pour la loi associative \cdot . Ainsi, (G, \cdot) est un groupe.

5) Soit G un groupe d'élément unité e vérifiant la condition (C) :

$$\forall x \in G, \quad x^2 = e.$$

- a) Donner au moins un exemple de groupe, non réduit à l'élément unité, vérifiant la condition (C).
- b) Démontrer que tout groupe vérifiant la condition (C) est abélien.

- a) Le groupe $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}, +\right)$ vérifie de façon évidente la condition.
- b) la condition (C) implique que chaque élément est son propre inverse, ainsi :

$$\begin{aligned}\forall a, b \in G, \quad (ab)^2 &= e, \\ abab &= e, \\ bab &= a, \\ ab &= ba.\end{aligned}$$

Tout groupe vérifiant la propriété est donc abélien.

6) G étant un groupe, prouver que l'application $f : \begin{matrix} G & \rightarrow & G, \\ x & \mapsto & x^{-1}. \end{matrix}$ est une permutation de G et que f est un automorphisme si et seulement si G est abélien.

Chaque élément d'un groupe possède un unique inverse, l'application est donc trivialement bijective. Supposons que G soit abélien :

$$\begin{aligned}\forall a, b \in G, \quad f(ab) &= (ab)^{-1}, \\ &= b^{-1}a^{-1}, \\ &= a^{-1}b^{-1}, \\ &= f(a)f(b).\end{aligned}$$

Donc abélien \Rightarrow (f est un) automorphisme.
Supposons que f soit un automorphisme :

$$\begin{aligned}\forall a, b \in G, \quad f(ab) &= f(a)f(b), \\ b^{-1}a^{-1} &= a^{-1}b^{-1}, \\ (\Rightarrow) ab &= ba \text{ (en appliquant } f \text{ des deux côtés).}\end{aligned}$$

ainsi, f est un automorphisme si et seulement si G est abélien.

7) Montrer que si G est un groupe fini d'ordre pair, il existe au moins un élément $x \neq e$, dans G , tel que $x^2 = e$.

Soit G d'ordre $2n$, définissons la relation d'équivalence :

$$x\mathcal{R}y \Leftrightarrow x = y \text{ ou } x = y^{-1}.$$

Soit $\{x_i\}_{i \in I}$ une famille de représentants des classes modulo \mathcal{R} . On a $1 \leq \overline{x_1} \leq 2$ (Dis comme ça, ce n'est pas évident mais ce que tu dis après le justifie bien). Aussi, $\overline{x_i}$ est un ensemble, pas un nombre, mais j'imagine bien que tu parlais de son cardinal. Enfin, pour lister les classes modulo \mathcal{R} , tu peux écrire « Pour tout $X \in G/\mathcal{R}$, on a $1 \leq |X| \leq 2$. »). le groupe se partitionne en k classes d'un élément (correspondant aux éléments qui sont leur propre inverse) et l classes de deux éléments (de la forme $\{x, x^{-1}\}$), et on a donc :

$$2n = k + 2l$$

Pour respecter la parité, il faut donc que k soit pair, et sachant que $k > 1$, qu'il existe au moins un élément différent du neutre tel que $x^2 = e$.

8) Dans l'ensemble des entiers \mathbb{Z} , on pose $U = \{-1, 1\}$.

- a) Vérifier que U est un groupe relativement à la multiplication des entiers, donc un sous-groupe de (\mathbb{Q}^*, \times) .
- b) Montrer que le groupe U est isomorphe au groupe $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}, +\right)$.

- a) On a $U \subset \mathbb{Z}$. On vérifie aussi que, $\forall x, y \in U$, $xy \in U$ et $x^{-1} \in U$, c'est donc un sous-groupe de (\mathbb{Q}^*, \times) .
- b) On pose l'application :

$$\begin{aligned} \varphi : \frac{\mathbb{Z}}{2\mathbb{Z}} &\rightarrow U, \\ x &\mapsto \begin{cases} 1 & \text{si } x = \overline{0} \\ -1 & \text{si } x = \overline{1} \end{cases} . \end{aligned}$$

On vérifie de façon exhaustive que c'est un morphisme :

$$\begin{aligned} \varphi(\overline{0+0}) &= 1 = 1 \times 1 = \varphi(\overline{0})\varphi(\overline{0}) \\ \varphi(\overline{0+1}) &= -1 = 1 \times -1 = \varphi(\overline{0})\varphi(\overline{1}) \\ \varphi(\overline{1+0}) &= -1 = -1 \times 1 = \varphi(\overline{1})\varphi(\overline{0}) \\ \varphi(\overline{1+1}) &= 1 = -1 \times -1 = \varphi(\overline{1})\varphi(\overline{1}) \end{aligned}$$

Elle est aussi bijective par définition, ainsi, U est isomorphe à $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}, +\right)$ (Une méthode peut-être overkill mais qui permet de ne pas vérifier à la main que φ est un morphisme c'est de considérer le morphisme exponentiel $\mathbb{Z} \rightarrow U$ envoyant n sur $e^{in\pi}$ qui est surjectif et de noyau $2\mathbb{Z}$)

9) Soit \mathbf{D} le sous ensemble de \mathbb{Q} formé par les nombres décimaux :

$$\mathbf{D} = \left\{ \frac{a}{10^n}; a \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

Prouvez que \mathbf{D} est un sous-groupe de $(\mathbb{Q}, +)$.

De façon évidente, $\mathbf{D} \subset \mathbb{Q}$. Soit $\frac{a}{10^n}, \frac{b}{10^m} (\in D)$,

$$\frac{a}{10^n} - \frac{b}{10^m} = \frac{10^m a - 10^n b}{10^{n+m}}.$$

On a $10^m a - 10^n b \in \mathbb{Z}$ (car $a, b \in \mathbb{Z}$), et $n + m \in \mathbb{N}$, donc $\frac{a}{10^n} - \frac{b}{10^m} \in \mathbf{D}$, ainsi $(\mathbb{D}, +)$ est un sous groupe de $(\mathbb{Q}, +)$

10) Soit, dans \mathbb{N} , un nombre premier p . On pose :

$$\mathbb{Q}_p = \left\{ \frac{a}{p^n}; a \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

a) Vérifier que \mathbb{Q}_p est un sous-groupe de $(\mathbb{Q}, +)$ et que $\mathbb{Q}_p = \bigcup_{n \in \mathbb{N}} \langle \frac{1}{p^n} \rangle$.

b) Montrer que l'application $\varphi : \begin{matrix} \mathbb{Q}_p & \rightarrow & \mathbb{Q}_p, \\ x & \mapsto & px. \end{matrix}$ est une permutation de \mathbb{Q}_p . L'application φ est-elle un automorphisme de $(\mathbb{Q}_p, +)$?

a) $\mathbb{Q}_p \in \mathbb{Q}$, et soit $\frac{a}{p^n}, \frac{b}{p^m} \in \mathbb{Q}_p$:

$$\frac{a}{p^n} - \frac{b}{p^m} = \frac{p^m a - p^n b}{p^{n+m}}.$$

On a $p^m a - p^n b \in \mathbb{Z}$, et $n + m \in \mathbb{N}$, donc $\frac{a}{p^n} - \frac{b}{p^m} \in \mathbb{Q}_p$, ainsi $(\mathbb{Q}_p, +)$ est un sous groupe de $(\mathbb{Q}, +)$. De plus :

$$\bigcup_{n \in \mathbb{N}} \langle \frac{1}{p^n} \rangle = \left\{ \frac{a}{p^n}; a \in \mathbb{Z}, n \in \mathbb{N} \right\} = \mathbb{Q}_p.$$

(Ce n'est pas assez détaillé. Tu peux écrire quelque chose du genre « Le groupe engendré par $1/p^n$ est $\mathbb{Z} \cdot \frac{1}{p^n}$ car \mathbb{Q}_p est une groupe abélien »)

b) φ est clairement injective (l'injectivité est aussi (non)-évidente que la surjectivité : φ admet comme bijection réciproque $x \mapsto p^{-1}x$). De plus, comme $\frac{a}{p^n} = p \frac{a}{p^{n+1}}$, on en déduit que φ est surjective, donc que c'est une permutation.

$$\begin{aligned} \forall x, y \in \mathbb{Q}_p, \varphi(x + y) &= p(x + y), \\ &= px + py, \\ &= \varphi(x) + \varphi(y). \end{aligned}$$

ce qui prouve que φ est un morphisme, et donc un automorphisme.

11) Soit p un nombre premier dans \mathbb{N} . Vérifier les propriétés suivantes :

$$\{a + b\sqrt{p}; (a, b) \in \mathbb{Z} \times \mathbb{Z}\} < (\mathbb{R}, +)$$

$$\{a + b\sqrt{p}; a \text{ et } b \text{ dans } \mathbb{Q} \text{ et non simultanément nuls}\} < (\mathbb{R}^*, \times)$$

$$\{a + ib\sqrt{p}; (a, b) \in \mathbb{Z} \times \mathbb{Z}\} < (\mathbb{C}, +)$$

$$\{a + ib\sqrt{p}; a \text{ et } b \text{ dans } \mathbb{Q} \text{ et non simultanément nuls}\} < (\mathbb{C}^*, \times)$$

On note que si p n'est pas un carré parfait, \sqrt{p} est irrationnel, chaque élément du groupe s'écrit de façon unique et tout se passe nickel.

Posons $G = \{a + b\sqrt{p}; (a, b) \in \mathbb{Z} \times \mathbb{Z}\}$

De façon évidente, $G \subset \mathbb{R}$. Soit $a + b\sqrt{p}, a' + b'\sqrt{p} \in G$:

$$a + b\sqrt{p} - (a' + b'\sqrt{p}) = (a - a') + (b - b')\sqrt{p} \in G$$

Et idem pour les 3 autres flemmes. (le calcul pour le deuxième groupe est quand même assez différent mais je comprends la flemmes ...)

12) On pose :

$$\Gamma_\infty = \{z \in \mathbb{C}; \exists n \in \mathbb{N}, z^n = 1\}.$$

Vérifier que Γ_∞ est un sous-groupe de (\mathbb{C}^*, \times) .

$\Gamma_\infty \subset \mathbb{C}$, soit $z_1, z_2 \in \Gamma_\infty$, il existe $n_1, n_2 \in \mathbb{N}$ tel que $z_1^{n_1} = z_2^{n_2} = 1$.

On constate que $(z_1 z_2^{-1})^{n_1 n_2} = (z_1^{n_1})^{n_2} (z_2^{n_2})^{-n_1} = 1$, et donc $z_1 (z_2)^{-1} \in \Gamma_\infty$, donc Γ_∞ est un sous-groupe de (\mathbb{C}^*, \times) . (Pour une méthode overkill : Γ_∞ est l'image de $(\mathbb{Q}, +)$ du morphisme exponentiel envoyant x sur $e^{2i\pi x}$ mais ça rajoute inutilement le fait de démontrer que l'ensemble des racines n -ièmes de l'unité sont les $e^{2i\pi k/n}$)

13) A tout nombre réel a on associe l'application

$$\begin{aligned} \tau_a : \mathbb{R} &\rightarrow \mathbb{R}, \\ x &\mapsto a + x. \end{aligned}$$

Justifier la propriété :

$T = \{\tau_a; a \in \mathbb{R}\}$ est un sous-groupe du groupe symétrique $S_{\mathbb{R}}$ et le groupe T est isomorphe au groupe $(\mathbb{R}, +)$.

Lemme (1.77)

14) On considère les groupes multiplicatifs \mathbb{R}^* , \mathbb{R}_+^* et \mathbb{C}^* (voir exemple (1.29)) et les applications :

$$\begin{aligned} f : \mathbb{R}^* &\rightarrow \mathbb{R}_+^*, \quad \text{où } |x| \text{ est la valeur absolue de } x. \\ x &\mapsto |x|. \end{aligned}$$

et $g : \mathbb{C}^* \rightarrow \mathbb{R}_+^*$, où $|z|$ est le module de z .

$$z \mapsto |z|.$$

Vérifier que f et g sont des épimorphismes de groupes.

Déterminer les noyaux de f et g .

Soit x un élément de \mathbb{R}_+^* , on a $f(x) = x$, donc f est surjective, vérifions que c'est un morphisme :

$$\begin{aligned} \forall x, y \in \mathbb{R}, \quad f(xy) &= |xy|, \\ &= |x||y|, \\ &= f(x)f(y). \end{aligned}$$

C'est donc un épimorphisme de groupe, déterminons son noyau :

$$\begin{aligned} \text{Ker } f &= \{x \in \mathbb{R}^*, f(x) = 1\}, \\ &= \{x \in \mathbb{R}^*, |x| = 1\}, \\ &= \{-1, 1\}. \end{aligned}$$

Soit x un élément de \mathbb{R}_+^* , on a $g(x) = x$, donc g est surjective, vérifions que c'est un morphisme :

$$\begin{aligned}\forall x, y \in \mathbb{R}, \quad g(xy) &= |xy|, \\ &= |x||y|, \\ &= g(x)g(y).\end{aligned}$$

C'est donc un épimorphisme de groupe, déterminons son noyau :

$$\begin{aligned}\text{Ker } g &= \{x \in \mathbb{C}^*, f(x) = 1\}, \\ &= \{x \in \mathbb{C}^*, |x| = 1\}, \\ &= \mathbb{U}.\end{aligned}$$

(Le fait que g soit un morphisme surjectif implique que f l'est aussi car f est la restriction de g à $\mathbb{R}^* \supset \mathbb{R}_+^*$)

15) Démontrer que l'application $\lambda: \begin{array}{ccc} \mathbb{R} & \rightarrow & \mathbb{R}_+^* \\ x & \mapsto & 10^x. \end{array}$ est un isomorphisme du groupe $(\mathbb{R}, +)$ sur le groupe (\mathbb{R}_+^*, \times) .

Vérifions que c'est une morphisme :

$$\begin{aligned}\forall a, b \in \mathbb{R}, \lambda(a+b) &= 10^{a+b}, \\ &= 10^a 10^b, \\ &= \lambda(a)\lambda(b).\end{aligned}$$

L'injectivité :

$$x \in \text{Ker } \lambda \Rightarrow 10^x = 1 \Rightarrow x = 0.$$

La surjectivité :

$$\forall y \in \mathbb{R}_+^*, \lambda(\log_{10} y) = y.$$

(On peut tout simplement dire que \log_{10} est une bijection réciproque.)

Donc λ est une isomorphisme de groupe.

16)

a) Le centre d'un groupe G étant désigné par $Z(G)$, démontrer la propriété :

$$H \leq G \Rightarrow Z(G) \cap H \leq Z(H)$$

b) G et G' étant deux groupes, si f est un épimorphisme de G sur G' , prouver que l'on a : $f(Z(G)) \leq Z(G')$

a) Un élément de H qui commute avec tout les éléments de G commute aussi avec tout les élément de H , d'où $Z(G) \cap H \subset Z(H)$. De plus, l'intersection de sous-groupes est un sous-groupe, donc $Z(G) \cap H \leq Z(H)$.

b) Soit $y \in f(Z(G))$, il existe $x \in Z(G)$ tel que $y = f(x)$. f étant surjective, pour tout $z \in G'$, il existe $w \in G$ tel que $z = f(w)$. On a donc :

$$yz = f(x)f(w) = f(xw) = f(wx) = f(w)f(x) = zy.$$

D'où $y \in Z(G')$, et comme $f(Z(G))$ est un sous-groupe de G' inclus dans $Z(G')$, on a bien $f(Z(G)) \leq Z(G')$.

17) Soit S une partie non vide d'un groupe G ; on pose :

$$C_G(S) = \{g \in G; gx = xg, \forall x \in S\}.$$

a) Vérifier que $C_G(S)$ est un sous-groupe de G .

$C_G(S)$ est appelé le *centralisateur* de S dans G . Si $S = \{x\}$, on le note $C_G(x)$ et on l'appelle le *centralisateur* de x dans G .

b) $Z(G)$ étant le centre de G , démontrer la relation : $\bigcap_{x \in G} C_G(x) = Z(G)$

c) Pour $x \in G$, posons $H = C_G(x)$; Vérifier que $x \in Z(H)$.

a) Soit $h, g \in C_G(S)$, pour tout $x \in S$, on a :

$$(hg^{-1})x = hxg^{-1} = xhg^{-1}.$$

Donc $\forall h, g \in C_G(S)$, $hg^{-1} \in C_G(S)$, c'est donc bien un sous-groupe de G .

b)

$$g \in Z(G) \Leftrightarrow \forall x \in G, gx = xg \Leftrightarrow \forall x \in G, g \in C_G(x) \Leftrightarrow g \in \bigcap_{x \in G} C_G(x)$$

c)

$$H = C_G(x) \Leftrightarrow \forall h \in H, hx = xh \Leftrightarrow x \in Z(H).$$

18) Soit A, B, C trois parties non vides d'un groupe G .

Soit $H = \langle A, B \rangle$ le sous-groupe de G engendré par $A \cup B$.

Si $K = \langle A, B, C \rangle$ est le sous-groupe de G engendré par $A \cup B \cup C$, démontrer que $K = \langle H, C \rangle$.

Soit \mathcal{H}_S l'ensemble des sous groupe de G contenant S . Par définition,

$$H = \bigcap_{L \in \mathcal{H}_{A \cup B}} L, \quad K = \bigcap_{L \in \mathcal{H}_{A \cup B \cup C}} L.$$

Montrons que $\mathcal{H}_{A \cup B \cup C} = \mathcal{H}_{H \cup C}$

Soit $L \in \mathcal{H}_{A \cup B \cup C}$, comme $A \cup B \subset L$, on a $L \in \mathcal{H}_{A \cup B}$ (donc L contient H), et, (comme L contient C , L contient $H \cup C$) donc $L \in \mathcal{H}_{H \cup C}$.

De façon réciproque, soit $L \in \mathcal{H}_{H \cup C}$, on a $A \cup B \subset H \subset L$, (et $C \subset L$), donc $L \in \mathcal{H}_{A \cup B \cup C}$.

Ainsi, on a $\mathcal{H}_{A \cup B \cup C} = \mathcal{H}_{H \cup C}$, et donc que $K = \langle H, C \rangle$.

(Je pense que seule la première des parenthèse que j'ai rajouté est vraiment nécessaire, le reste se comprend bien sans tout le détail.)

19) Démontrer que le groupe des quaternions (exemple (1.16)) est engendré par les matrices :

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

(j'ai repris la demo d'un mec, qui est pas complete je crois, la mienne a environ 200 indices avec des sommes donc chiant a taper)

Soit le groupe des quaternions :

$$\left\{ \begin{array}{l} q_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, q_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, q_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, q_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ q_5 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, q_6 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, q_7 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, q_8 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \end{array} \right\}$$

On calcule bêtement $\langle A, B \rangle$ et cqfd.

(Je pense que la correction concise serait d'exprimer tous les q_i en fonction de A et B sans expliciter les calculs :

- $q_1 = A^0$
- $q_2 = A^2 (= B^2)$
- $q_3 = A$
- $q_4 = q_2 A = A^3$
- $q_5 = B$
- $q_6 = q_2 B = A^2 B (= B^3)$
- $q_7 = BA$
- $q_8 = q_2 q_7 = A^2 BA (= B^3 A)$

20) Dans l'ensemble $M_2(\mathbb{R})$ des matrices carrées d'ordre 2 sur \mathbb{R} , on considère le sous-ensemble Γ tel que :

$$\Gamma = \left\{ \begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} : x \in \mathbb{R}^* \right\}.$$

Démontrer que Γ est un groupe par rapport à la multiplication des matrices, mais que ce groupe n'est pas un sous-groupe de $GL_2(\mathbb{R})$.

Vérifier que le groupe Γ est isomorphe au groupe (\mathbb{R}^*, \times) .

Soit $\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} y & y \\ 0 & 0 \end{pmatrix} \in \Gamma :$

$$\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} y & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} xy & xy \\ 0 & 0 \end{pmatrix} \in \Gamma.$$

De plus, pour tout $\begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix} \in \Gamma$, son inverse $\begin{pmatrix} 1/x & 1/x \\ 0 & 0 \end{pmatrix} \in \Gamma$, et $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ est le neutre pour la multiplication des matrices dans cet ensemble.

On sait la loi associative, ainsi, Γ est un groupe pour la multiplication des matrices.

Ce n'est cependant pas un sous-groupe de $GL_2(\mathbb{R})$, car elles ne sont pas inversibles, ayant toutes un déterminant nul.

On vérifie directement que $\varphi : \mathbb{R}^* \rightarrow \Gamma$, est un isomorphisme de groupe.

$$x \mapsto \begin{pmatrix} x & x \\ 0 & 0 \end{pmatrix}.$$

21) Soit $n > 1$ dans \mathbb{N} et $\left(\frac{\mathbb{Z}}{(n)}, +\right)$ le groupe des classes de congruence modulo n . On considère la correspondance μ définie par :

$$\begin{aligned} \mu : \frac{\mathbb{Z}}{(n)} \times \frac{\mathbb{Z}}{(n)} &\rightarrow \frac{\mathbb{Z}}{(n)}, \\ (\bar{x}, \bar{y}) &\mapsto \overline{xy}. \end{aligned}$$

a) Prouver que la correspondance μ est une application [c'est-à-dire que : $(\bar{x}' = \bar{x} \text{ et } \bar{y}' = \bar{y}) \Rightarrow \overline{x'y'} = \overline{xy}$].

En déduire que l'on peut définir dans $\frac{\mathbb{Z}}{(n)}$ une multiplication telle que $\bar{x} \cdot \bar{y} = \overline{xy}$.

Montrer alors que $\frac{\mathbb{Z}}{(n)}$ est un anneau unitaire. et commutatif.

b) Soit, dans \mathbb{N} , un nombre premier p . On désigne par G_p l'ensemble des éléments non nuls de $\frac{\mathbb{Z}}{(p)}$.

Prouver, en utilisant le résultat de l'exercice 4, que G_p est un groupe par rapport à la multiplication définie dans $\frac{\mathbb{Z}}{(p)}$.

En conclure que $\frac{\mathbb{Z}}{(p)}$ est un corps.

c) Vérifier que si n n'est pas premier $\frac{\mathbb{Z}}{(p)}$ n'est pas un corps.

a) Soit $x, y, x', y' \in \mathbb{Z}$ tel que $\bar{x} = \overline{x'}$ et $\bar{y} = \overline{y'}$. On rappelle que :

$$\begin{aligned}\bar{x} = \overline{x'} &\Leftrightarrow \exists k \in \mathbb{Z}, x = x' + kn, \\ \bar{y} = \overline{y'} &\Leftrightarrow \exists k' \in \mathbb{Z}, y = y' + k'n.\end{aligned}$$

Ainsi :

$$\begin{aligned}\overline{xy} &= \overline{(x' + kn)(y' + k'n)}, \\ &= \overline{x'y' + x'k'n + y'kn + kk'n^2}, \\ &= \overline{x'y' + n(x'k' + y'k + kk'n)}, \\ &= \overline{x'y'}.\end{aligned}$$

la multiplication ainsi définie est associative, commutative, de neutre $\bar{1}$, et est distributive par rapport à l'addition. $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est donc un anneau unitaire commutatif.

b) L'ensemble G_p est fini, est dans le a) on a montré que la loi de multiplication associée est associative. Montrons que chaque élément est simplifiable à droite et à gauche. Soit $\bar{a}, \bar{x}, \bar{y} \in G_p$ tel que $\bar{ax} = \bar{ay}$. On a $\bar{ax} = \bar{ay}$, autrement dit, que $ax - ay = a(x - y)$ est un multiple de p . \bar{a} étant non nul, $x - y$ est un multiple de p , et donc que $\bar{x} = \bar{y}$ (bien mettre en évidence l'argument : comme p est un nombre premier divisant $a(x - y)$ et ne divisant pas a par hypothèse, il divise $x - y$ d'après le lemme d'Euclide. Cela permet de bien identifier à quel moment on utilise le fait que p est premier.). Par commutativité, tout les éléments sont simplifiable à droite et à gauche. D'après l'exo 4, G_p est un groupe. De plus, tout élément non nul de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est inversible, donc c'est un corps.

c) Chapitre 3.

22) Vérifier que

$$\Gamma = \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \gamma_1 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \gamma_2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \gamma_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \gamma_4 = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \gamma_5 = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \right\}$$

est un sous-groupe de $GL(2, \mathbb{R})$ isomorphe au groupe $GL\left(2, \frac{\mathbb{Z}}{(2)}\right)$.

Ecrire la table de multiplication du groupe Γ ; en déduire que Γ est isomorphe au groupe symétrique S_3 .

Toutes les matrices de cet ensemble ont pour déterminant 1, la multiplication des matrices est associative, et $I \in \Gamma$. Posons dès maintenant la table de multiplication de Γ :

\times	I	γ_1	γ_2	γ_3	γ_4	γ_5
I	I	γ_1	γ_2	γ_3	γ_4	γ_5
γ_1	γ_1	γ_2	I	γ_5	γ_3	γ_4
γ_2	γ_2	I	γ_1	γ_4	γ_5	γ_3
γ_3	γ_3	γ_4	γ_5	I	γ_1	γ_2
γ_4	γ_4	γ_5	γ_3	γ_2	I	γ_1
γ_5	γ_5	γ_3	γ_4	γ_1	γ_2	I

On remarque que chaque élément possède un unique inverse. Γ est donc bien un sous-groupe de $GL(2, \mathbb{R})$.

On constate que ce groupe se décompose en deux sous groupes, $H = \{I, \gamma_1, \gamma_2\}$ et $K = \{I, \gamma_4\}$, tel que $\Gamma = HK$. D'où l'isomorphisme évident (aka, flemme de rédiger) avec $GL(2, \frac{\mathbb{Z}}{2\mathbb{Z}})$ et S_3 .

(Pour l'isomorphisme avec $GL(2, \mathbb{Z}/2\mathbb{Z})$, il n'y a pas grand chose à écrire : le morphisme canonique d'anneaux $\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ induit un morphisme de groupes $GL(2, \mathbb{Z}) \rightarrow GL(2, \mathbb{Z}/2\mathbb{Z})$ admettant comme section le morphisme envoyant une matrice de $GL(2, \mathbb{Z}/2\mathbb{Z})$ vers son représentant dans Γ . Pour S_3 , on peut en effet décomposer en

produit semi-direct (ce n'est pas grave si tu ne sais pas ce que c'est, mais c'est souvent ce qui se cache derrière les groupes qui se décomposent en produit $G = HK$ sans que ce soit un produit direct), c'est une bonne méthode en général. Mais, tu peux aussi simplement écrire la table de multiplication de S_3 et mettre en évidence que c'est la même que celle de Γ .)

(En fait, l'isomorphisme $G := GL(2, \mathbb{Z}/2\mathbb{Z}) \simeq S_3$ peut aussi s'obtenir en faisant agir G sur l'ensemble des droites vectoriels de $(\mathbb{Z}/2\mathbb{Z})^2$. Cet ensemble revête une nature géométrique et il porte le nom de « droite projective » (que l'on note $\mathbb{P}^1(\mathbb{F}_2)$ en général). L'étude de l'action des groupes de matrices sur les espaces projectifs (et plus généralement, les Grassmanniennes) sont la source de bon nombre d'isomorphismes exceptionnels comme celui-ci. Mon exercice préféré de théorie des groupes est de montrer qu'on a l'isomorphisme exceptionnel

$$GL(2, \mathbb{F}_3) \simeq (Q_8 \rtimes \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$$

où \mathbb{F}_3 est le corps $\mathbb{Z}/3\mathbb{Z}$, Q_8 est le groupe des quaternions et \rtimes est le symbole « produit semi-direct ».)

23)

a) Démontrer les résultats suivants :

$$\Gamma_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

est un sous-groupe de $GL(2, \mathbb{R})$.

$$\Gamma_2 = \{1, i, -1, -i\} \text{ où } i^2 = -1,$$

est un sous-groupe de (\mathbb{C}^*, \times) .

$$\Gamma_3 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

sous-ensemble de $\frac{\mathbb{Z}}{(5)}$ est un groupe par rapport à la multiplication définie dans $\frac{\mathbb{Z}}{(5)}$.

b) Prouver que $\Gamma_1, \Gamma_2, \Gamma_3$ sont trois groupes isomorphes. Sont-ils cycliques?

24)

a) Montrer que :

$$K_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

est un sous-groupe de $GL(2, \mathbb{R})$ et que $K_2 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, sous-ensemble de $\frac{\mathbb{Z}}{(8)}$, est un groupe par rapport à la multiplication définie dans $\frac{\mathbb{Z}}{(8)}$.

b) Vérifier qu ces deux groupes sont isomorphes. Ces groupes sont-ils isomorphes au groupe de Klein?

25)

a) Montrer que le groupe symétrique S_3 , les groupes Γ_2 et Γ_3 de l'exercice 23 et le groupe K_2 de l'exercice 24 admettent chacun une représentation matricielle fidèle de degré 2 sur \mathbb{R} .

b) En associant à tout nombre complexe non nul $a+ib$ la matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, vérifier que le groupe multiplicatif \mathbb{C}^* admet aussi une représentation fidèle de degré 2 sur \mathbb{R} .

26) Soit P le plan affine euclidien. Si f est une isométrie du plan P , on dit qu'un point A est fixe pour f si $f(A) = A$.

On désigne par $\mathcal{I}(2)$ l'ensemble des isométries du plan P .

Si Δ est une droite de P , on note s_Δ la symétrie du plan par rapport à Δ ; $s_\Delta : \begin{matrix} P & \rightarrow & P, \\ A & \mapsto & A'. \end{matrix}$, A' est tel

que Δ est la médiatrice de AA' .

a) Vérifier les propriétés suivantes :

- L'identité de P , notée id_P , appartient à $\mathcal{I}(2)$.
- quelle que soit la droite Δ , s_Δ appartient à $\mathcal{I}(2)$ et $s_\Delta \circ s_\Delta = id_P$.
- Si f_1 et f_2 sont dans $\mathcal{I}(2)$, alors $f_2 \circ f_1 \in \mathcal{I}(2)$; $f_2 \circ f_1$ sera appelé le produit de f_1 et f_2 dans $\mathcal{I}(2)$.

b) Soit $f \in \mathcal{I}(2)$; montrer que :

- si f à deux points fixes distincts A et B , alors tout point de la droite AB est fixe pour f ;
- Si f à trois points fixes, A, B, C non alignés, alors $f = id_P$.

c) Démontrer que toute isométrie $f \in \mathcal{I}(2)$ est le produit de 0, 1, 2, ou 3 symétries.

d) Prouver que $\mathcal{I}(2)$ est un sous-groupe du groupe symétrique S_P et que $\mathcal{I}(2)$ est non-abélien.

e) A tout vecteur v de l'espace vectoriel \mathbb{R}^2 on associe la translation de vecteur v du plan affine P , notée t_v . Montrer à l'aide de (c) que $t_v \in \mathcal{I}(2)$ et que $\mathcal{T}(P) = \{t_v; v \in \mathbb{R}^2\}$ est un sous-groupe abélien de $\mathcal{I}(2)$, isomorphisme à $(\mathbb{R}^2, +)$.

f) Soit O un point du plan P , pour $\alpha \in \mathbb{R}$; on note $r_{O,\alpha}$ la rotation du plan P de centre O et d'angle α .

Montrer à l'aide de (c) que $r_{O,\alpha} \in \mathcal{I}(2)$. $\mathcal{R}(P, O)$ désignant l'ensemble de toutes les rotations $R_{O,\alpha}$ pour $\alpha \in \mathbb{R}$, vérifier que $\mathcal{R}(P, O) = \{r_{O,\alpha}; 0 \leq \alpha < 2\pi\}$ et que $\mathcal{R}(P, O)$ est un sous-groupe abélien de $\mathcal{I}(2)$.

27) Notons \mathbb{C} le plan complexe, c'est-à-dire le plan affine euclidien \mathbb{R}^2 rapporté à un système d'axes ortho-normés Oxy et dont tout point $M(x, y)$ est considéré comme l'image du nombre complexe $z = x + iy$.

A toute famille de 4 nombres complexes (a, b, c, d) telle que $ad - bc \neq 0$, on associe l'application :

$$f : \mathbb{C} \rightarrow \mathbb{C}, \\ z \mapsto \frac{az + b}{cz + d}, \text{ où } z \in \mathbb{C}..$$

On remarque que si $c \neq 0$, le point $-\frac{d}{c}$ n'a aucune image par f ; d'autre part le point $\frac{a}{c}$ n'est l'image d'aucun point de \mathbb{C} . Pour remédier à ces difficultés, on rajoute au plan complexe un point dit à l'infini et noté ∞ .

On pose $\tilde{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, pour $c \neq 0$, $f\left(-\frac{d}{c}\right) = \infty$ et $f(\infty) = \frac{a}{c}$.

Une application telle que f est appelée une homographie du plan complexe.

a) Montrer que toute homographie f est une permutation de $\tilde{\mathbb{C}}$.

b) Démontrer que l'ensemble \mathcal{H} des homographies du plan complexe est un sous-groupe du groupe symétrique $S_{\tilde{\mathbb{C}}}$.

c) En considérant le cas où $c = 0$, prouver que \mathcal{H} contient comme sous-groupes le groupe des similitudes et translations du plan complexe.

d) Vérifier que l'homographie $z \mapsto \frac{1}{\bar{z}}$ est le produit (commutatif) de l'inversion de centre O et de puissance 1. et de la symétrie par rapport à l'axe Ox .

e) Démontrer que toute homographie f du plan complexe conserve les angles et leurs orientation, ce que l'on exprime en disant que f est une transformation conforme du plan.

f) Prouver que les homographies :

$$f_1 : z \mapsto z; \quad f_2 : z \mapsto -z; \quad f_3 : z \mapsto \frac{1}{z}; \quad f_4 : z \mapsto -\frac{1}{z}$$

forment un sous-groupe de \mathcal{H} isomorphe au groupe de Klein.

g) Prouver que les homographies :

$$g_1 : z \mapsto z; \quad g_2 : z \mapsto \frac{1}{1-z}; \quad g_3 : z \mapsto \frac{z-1}{z},$$

$$g_4 : z \mapsto \frac{1}{z}; \quad g_5 : z \mapsto 1-z; \quad g_6 : z \mapsto \frac{z}{z-1}$$

forment un sous-groupe de \mathcal{H} isomorphe au groupe symétrique S_3 .

28)

- a) Démontrer le corrolaire (1.49)
b) Démontrer la proposition (1.53)
-

29) Soit E un ensemble non vide et G un groupe d'élément unité e . On désigne par G^E l'ensemble des applications f de E dans G . On considère la loi de composition définie dans G^E par :

$$G^E \times G^E \rightarrow G^E$$

$$(f, g) \mapsto fg,$$

Où fg est telle que pour tout $x \in E$, $(fg)(x) = f(x)g(x)$.

Prouver que (G^E) est ainsi muni d'une structure de groupe.

Vérifier que G^E est un groupe abélien si et seulement si G est abélien.

30) \mathbb{R} désignant le groupe additif des réels, on pose :

$$J = \{x \in \mathbb{R}; 0 \leq x \leq 1\}.$$

L'addition de \mathbb{R} induit dans l'ensemble \mathbb{R}^J une structure de groupe additif abélien.

a) Vérifier les propriétés suivantes :

- l'ensemble des fonctions $f \in \mathbb{R}^J$, continues sur J , est un sous-groupe de $(\mathbb{R}^J, +)$, que l'on notera $\mathcal{C}(J)$;
- si, pour tout $a \in \mathbb{R}$, on note c_a la fonction constante de J dans \mathbb{R} telle que $c_a(x) = a$ pour tout $x \in J$, alors $\Gamma = \{c_a; a \in \mathbb{R}\}$ est un sous-groupe de $(\mathcal{C}(J), +)$.

b) On considère les applications F_i de $\mathcal{C}(J)$ dans \mathbb{R} telles que :

$$F_1 : f \mapsto f(1), \quad F_2 : f \mapsto |f(0)|, \quad F_3 : f \mapsto \int_0^1 f(x)dx$$

$$F_4 : f \mapsto \frac{\pi}{3} \int_0^1 f(x) \cos \frac{\pi x}{6} dx, \quad F_5 : f \mapsto \int_0^1 \cos \frac{\pi f(x)}{6} dx.$$

Déterminer les F_i qui sont des homomorphismes de groupes de $(\mathcal{C}(J), +)$ dans $(\mathbb{R}, +)$. Pour chacun des morphismes de groupes F_i , prouver que, quel que soit $a \in \mathbb{R}$, $F_i(c_a) = a$ et montrer qu'il existe un unique $m_i \in \mathbb{R}$ tel que $F_i(id_J - c_{m_i}) = 0$. En déduire que les $\text{Ker } F_i$ sont deux à deux distincts.

c) Démontrer que pour tout $F \in \text{Hom}(\mathcal{C}(J), \mathbb{R})$, tel que $F(c_a) = a$, quel que soit $a \in \mathbb{R}$, on a

$$\mathcal{C}(J) = \text{Ker } F \oplus \Gamma.$$

En conclure qu'il existe de nombreux sous-groupes de $\mathcal{C}(J)$ tels que $\mathcal{C}(J) = H \oplus \Gamma$.

31) Soit deux groupes G_1 et G_2 .

- a) Prouver que les groupes $G_1 \times G_2$ et $G_2 \times G_1$ sont isomorphes.
- b) Γ_1 et Γ_2 étant aussi deux groupes, démontrer la propriété : $(\Gamma_1 \simeq G_1 \text{ et } \Gamma_2 \simeq G_2) \Rightarrow \Gamma_1 \times \Gamma_2 \simeq G_1 \times G_2$.
- c) Si H_1 et H_2 sont respectivement des sous-groupes de G_1 et G_2 , montrer que $H_1 \times H_2$ est un sous-groupe de $G_1 \times G_2$.

Déterminer tous les sous-groupes de $\frac{\mathbb{Z}}{(2)} \times \frac{\mathbb{Z}}{(2)}$; en déduire compte tenu des notations précédentes, qu'un sous-groupe de $G_1 \times G_2$ n'est pas nécessairement de la forme $H_1 \times H_2$.

32) Pour deux groupes G_1 et G_2 , démontrer les propriétés :

- a) $G_1 \simeq G_2 \Rightarrow \text{Aut}(G_1) \simeq \text{Aut}(G_2)$
 - b) $G_1 \simeq G_2 \Rightarrow \text{Int}(G_1) \simeq \text{Int}(G_2)$.
-

33) Soit $\{G_i\}_{i \in I}$ une famille de groupes ; montrer que, pour tout groupe G , l'ensemble $\text{Hom}\left(G, \prod_{i \in I} G_i\right)$ est équipotent à l'ensemble $\prod_{i \in I} \text{Hom}(G, G_i)$.

CLASSES MODULO UN SOUS-GROUPE

1) TEST

TESTSOL

Remarques générales syntaxiques :

- On évite de mélanger les symboles de logique avec les phrases en français.
- L'utilisation des mots « évident » et « trivial » sont à éviter le plus possible (même quand c'est vraiment évident). La majorité des erreurs en maths se nichent dans les choses que l'on pense évidentes. Quand un truc est évident pour toi, tu peux faire le choix parmi trois possibilités en fonction du niveau d'évidence :
 - énoncer et faire la preuve détailler : Le groupe $(\mathbb{Z}/2\mathbb{Z}, +)$ vérifie la condition (C) de l'exo 5 car $0+0 = 0$ et $1+1 = 0$ modulo 2.
 - énoncer et donner une raison pour laquelle c'est vrai : L'application $\varphi : x \mapsto px$ de l'exo 10 est injective car \mathbb{Q}_p est simplifiable à gauche pour la multiplication.
 - énoncer et laisser la démo à la lectrice : Le groupe $(\mathbb{Z}/2\mathbb{Z}, +)$ vérifie bien la condition (C).
- On évite d'écrire « Soit $x \in X$, blablabla » mais plutôt « Soit $x \in X$. Blablabla »

Remarques générales mathématiques :

- Quand on démontre qu'une application est bijective, on essaie autant que possible d'identifier la bijection réciproque. Si ce n'est pas possible, alors, en général, c'est qu'on a l'injectivité et que la surjectivité est donnée gratuitement par un argument de finitude (ensembles finis, espaces vectoriels de dimension fini).
- De manière générale, quand on démontre qu'un sous-ensemble d'un groupe est un sous-groupe, il faut dire à un moment que ce sous-ensemble est non vide si l'on veut être rigoureux : on a bien

$$\forall a, b \in \emptyset, ab^{-1} = e$$

mais \emptyset n'est jamais un sous-groupe. C'est tellement évident la plupart du temps qu'on ne l'écrit pas mais ça vaut le coup de le préciser la première fois pour y faire penser (et montrer qu'on sait être rigoureux).