Groupes, monoïdes (reliquat)

Marc SAGE

28 février 2018

Table des matières

1 Cours : groupes, monoïdes

EG de groupes d'inversibles :
$\mathfrak{P}(E)^\times = \begin{cases} \{\emptyset\} \text{ pour } \cup \\ \{E\} \text{ pour } \cap \\ \mathfrak{P}(E) \text{ pour } \Delta \end{cases}$ pour chaque ensemble E ;
et $\mathbf{N}^\times = \{0\}$ pour max.

EXO *Soient A et E deux ensembles, soit $f \in A^A$. Déterminer parmi les magmas suivants lesquels sont des monoïdes et préciser le cas échéant le neutre :*

a. $\mathbb{N}, \mathbb{N}^*, 18\mathbb{N}, \{42^n\}_{n\in\mathbb{N}}, \{18^n\}_{n\in\mathbb{N}^*}, \overline{\mathbb{N}}, \mathbb{Z}, \overline{\mathbb{Z}}, \mathbb{Q}, \mathbb{Q}^*, \mathbb{R}, \overline{\mathbb{R}}, \overline{\mathbb{R}_+^*}, [0,1]$, *resp. pour chacune des six lois* $+, \times, -, \div, \min, \max$ *;*
b. *l'espace* $\mathbb{R}^3$ *muni du produit vectoriel ;*
c. A^A, $\{f^{\circ n}\}_{n\in\mathbb{N}}$ *et* $\{f^{\circ n}\}_{n\in\mathbb{N}^*}$ *pour la composition ;*
d. $\mathfrak{P}(E)$ *resp. pour la réunion, l'intersection, la privation, la différence symétrique*[1] *;*
e. *l'ensemble* $A^* := \coprod_{n\in\mathbb{N}} A^n$ *des mots sur A muni resp. de la concaténation* $((a,b,c,...,z),(\alpha,\beta,\gamma,...,\omega)) \mapsto (a,b,c,...,z,\alpha,\beta,\gamma,...,\omega)$*, du mélange* ***faro***

$$((a_1,a_2,a_3,...,a_p),(b_1,b_2,b_3,...,b_q)) \mapsto \begin{cases} (a_1,b_1,a_2,b_2,a_3,b_3,...,a_p,b_p,b_{p+1},b_{p+2},...,b_q) & si\ p \le q \\ (a_1,b_1,a_2,b_2,a_3,b_3,...,a_q,b_q,a_{q+1},a_{q+2},...,a_p) & si\ p > q \end{cases}.$$

---

a. Observer que tous les ensembles donnés sont des parties de $\overline{\mathbb{R}}$ où est fixée la signification des six "lois" proposées.

Ces dernières ne font toutefois pas toujours sens, des composés pouvant être ou bien sans sens (tels $-\infty+\infty$ ou $0\times\infty$) ou bien sortir de l'ensemble donné (tel $1+1$ pour $[0,1]$). Nous conviendrons de signaler par une lettre barrée $\not{\text{l}}$ que la "**l**oi" n'en est pas une et commençons à remplir le tableau récapitulatif ci-dessous.

Ensuite, là où elles font sens, les lois $+$ et $\times$ sont associatives et ont pour neutres respectifs 0 et 1 : en l'absence de $\not{\text{l}}$, le caractère "être un monoïde pour $+$" se réduit donc à "contenir 0" (*idem* pour $\times$ et 1). L'absence de **n**eutre sera signalée par une lettre barrée $\not{\text{N}}$.

Concernant la soustraction, fixant un élément a dans un monoïde pour $-$, ce dernier doit contenir $a-a=0$, donc doit contenir $0-a=-a$. Par ailleurs, même si notre candidat contient 0 et est stable par opposition, il n'est jamais associatif vu les différences $\begin{cases} a-(a-a)=a \\ (a-a)-a=-a \end{cases}$ distinctes dès que a est non nul (tous les ensembles de l'énoncé contiennent un tel a). Nous signalerons la non-**a**ssociativité par $\not{\text{A}}$. Le même raisonnement permet d'éliminer les candidats pour $\div$ qui ne contiennent pas 1 ou qui ne sont pas stables par inversion (et tous les autres avec $\not{\text{A}}$ puisqu'ils contiennent tous un a tels que $a \neq \frac{1}{a}$).

Enfin, les lois min et max sont toujours associatives et stabilisent chaque ensemble. Un neutre n pour min doit vérifier $a = \min\{a,n\} \le n$ pour chaque élément a, donc doit être le *maximum* de l'ensemble considéré. De même, un neutre pour max doit être le *minimum*. Finalement, "être un monoïde pour min" (resp. max) se réduit à "admettre un *maximum*" (resp. *minimum*).

	$\mathbb{N}$	$\mathbb{N}^*$	$18\mathbb{N}$	$\{42^n\}_{n\in\mathbb{N}}$	$\{18^n\}_{n\in\mathbb{N}^*}$	$\overline{\mathbb{N}}$	$\mathbb{Z}$
$+$	oui 0	$\not{\text{N}}$	oui 0	$\not{\text{N}}$	$\not{\text{N}}$	oui 0	oui 0
$\times$	oui 1	oui 1	$\not{\text{N}}$	oui 1	$\not{\text{N}}$	$\not{\text{l}}$	oui 1
$-$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{A}}$
$\div$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$
min	$\not{\text{N}}$	$\not{\text{N}}$	$\not{\text{N}}$	$\not{\text{N}}$	$\not{\text{N}}$	oui ∞	$\not{\text{N}}$
max	oui 0	oui 1	oui 0	oui 1	oui 18	oui 0	$\not{\text{N}}$

	$\overline{\mathbb{Z}}$	$\mathbb{Q}$	$\mathbb{Q}^*$	$\mathbb{R}$	$\overline{\mathbb{R}}$	$\overline{\mathbb{R}_+}^*$	$[0,1]$
$+$	$\not{\text{l}}$	oui 0	$\not{\text{N}}$	oui 0	$\not{\text{l}}$	$\not{\text{N}}$	$\not{\text{l}}$
$\times$	$\not{\text{l}}$	oui 1	oui 1	oui 1	$\not{\text{l}}$	oui 1	oui 1
$-$	$\not{\text{l}}$	$\not{\text{A}}$	$\not{\text{l}}$	$\not{\text{A}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$
$\div$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{A}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$	$\not{\text{l}}$
min	oui ∞	$\not{\text{N}}$	$\not{\text{N}}$	$\not{\text{N}}$	oui ∞	oui ∞	oui 1
max	oui $-\infty$	$\not{\text{N}}$	$\not{\text{N}}$	$\not{\text{N}}$	oui $-\infty$	$\not{\text{N}}$	oui 0

[1] La ***différence symétrique*** de deux ensembles A et B est l'ensemble $A\Delta B := A\backslash B \amalg A\backslash B = (A\cup B)\backslash(A\cap B)$.

b. Le produit vectoriel $\wedge$ fait sens sur tout $\mathbb{R}^3$. Soit par l'absurde n un neutre pour $\wedge$: on a alors pour chaque a non nul (par exemple $(1,0,0)$) l'orthogonalité $a = a \wedge n \perp a$, d'où $a \perp a$ et l'absurde nullité de a.

On aurait également pu nier l'associativité en invoquant un trièdre direct (u,v,w) et en constatant la différence des composés $\begin{cases} (u \wedge u) \wedge v = 0 \wedge v = 0 \\ u \wedge (u \wedge v) = u \wedge w = -v \end{cases}$.

c. Le monoïde A^A est le premier exemple du cours. L'ensemble $\{f^{\circ n}\}_{n\in\mathbb{N}}$ contient le neutre $f^{\circ 0} = \mathrm{Id}$ et est stable par $\circ$ puisque $\mathbb{N}$ l'est par $+$. De même, la partie $\{f^{\circ n}\}_{n\in\mathbb{N}^*}$ est stable par $\circ$ mais est un monoïde ssi l'un des itérés de f vaut l'identité.

d. Les lois $\cup$ et $\cap$ sont associatives et admettent pour neutres respectifs $\emptyset$ et E (*cf.* cours de première année). De même, Δ est associative et commutative (exercice de première année) et admet pour neutre le vide vu pour chaque partie $P \subset E$ les égalités

$$P\Delta\emptyset = (P \cup \emptyset)\setminus(P \cap \emptyset) = P \setminus \emptyset = P.$$

En revanche, vu les égalités $\begin{cases} E\setminus(E\setminus E) = E\setminus\emptyset = E \\ (E\setminus E)\setminus E = \emptyset\setminus E = \emptyset \end{cases}$, la privation n'est jamais associative (sauf si E est vide, auquel cas $\mathfrak{P}(E)$ est un monoïde trivial).

e. On se convaincra aisément que la concaténation est associative et admet pour neutre le mot vide (unique élément de A^0), lequel est également un neutre pour le faro. Si A est un singleton, le faro $*$ est clairement associatif (et, quand A est vide, $A^* = A^0$ est un monoïde trivial). En revanche, si l'on peut invoquer dans A deux éléments $a \neq b$, on constatera la différence des mélanges $\begin{cases} [ab] * ([a] * [b]) = [ab] * [ab] = [aabb] \\ ([ab] * [a]) * [b] = [aab] * [b] = [abab] \end{cases}$.
Finalement, A^* est un monoïde pour le faro ssi $\mathrm{Card}\, A \leq 1$.

RQ **(réalisation matricielle des quaternions)** – Tout comme l'on peut construire l'algèbre $\mathbb{C}$ comme l'ensemble des matrices de similitude $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ où a et b décrivent $\mathbb{R}$ (lorsque $b = 0$ on retrouve une "copie" du réel a en la matrice scalaire $\mathrm{Diag}\,(a,a)$) avec la définition $i := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, on peut construire l'algèbre $\mathbb{H}$ comme l'ensemble des matrices de la forme $\begin{pmatrix} \alpha & -\beta \\ \beta & \overline{\alpha} \end{pmatrix}$ où α et β décrivent $\mathbb{C}$ (lorsque $\beta = 0$ on retrouve une "copie" du complexe α en la matrice $\mathrm{Diag}\,(\alpha,\overline{\alpha})$) avec les définitions $j := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $k := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Exercice (itérés du neutre). *Décrire dans un monoïde la suite des itérés du neutre.*
La composition par le neutre ne changeant rien, la suite de ses itérés est constante[2]. Son premier terme étant le neutre, elle vaut constamment le neutre :

$$\forall n \in \mathbf{N},\ 1^n = 1 \qquad (\text{en additif } n0 = 0).$$

Exercice (itérés commutant). *Soient a et b deux éléments qui commutent[3] dans un monoïde. Montrer alors que chaque itéré de a commute avec chaque itéré de b puis que la suite des itérés de leur composé vaut le composé de leurs suites des itérés : pour tous naturels p, q, n, on a les égalités*

$$\begin{cases} a^p b^q = b^q a^p \\ (ab)^n = a^n b^n \end{cases} \qquad \left(\textit{en additif :} \begin{cases} pa + qb = qb + pa \\ n(a+b) = na + nb \end{cases}\right).$$

En particulier, les itérés d'un même élément commutent entre eux.

DEM[4]

[2] *Rappel* : une suite a sera constante si $\forall n \in \mathbf{N},\ a_{n+1} = a_n$.
[3] Ne pas oublier l'hypothèse de *commutativité*, laquelle est nécessaire dans les groupes comme nous le verrons
[4] exemple de rigueur extrême sans profondeur, à savoir très vite reconstituer soi-même sans besoin qu'on le présente comme ici sur un plateau

1. Montrons déjà que a commute avec chaque itéré de b. C'est clair pour le premier par hypothèse (et pour le zéroième valant le neutre). Pour tout naturel n, notons alors A_n l'égalité $ab^n = b^n a$ (qui fait sens) et montrons $\forall n \in \mathbf{N}^*,\ A_n$ par récurrence (l'égalité A_0 est claire).

   Nous avons déjà A_1.

   Soit $n \in \mathbf{N}^*$ tel que A_n. On a alors les égalités

$$\begin{array}{lll} ab^{n+1} & \overset{\text{définition de la suite } (b^k)}{\underset{\text{par composition à droite}}{=}} & a\left(b^n b\right) \overset{\text{associativité}}{=} \left(ab^n\right) b \overset{A_n}{=} \left(b^n a\right) b \\ & \overset{\text{associativité}}{=} & b^n\left(ab\right) \overset{A_1}{=} b^n\left(ba\right) \overset{\text{associativité}}{=} \left(b^n b\right) a \\ & \overset{\text{définition de la suite } (b^k)}{\underset{\text{par composition à droite}}{=}} & b^{n+1}a, \text{ d'où } A_{n+1}, \text{ CQFD.} \end{array}$$

2. Soit $q \in \mathbf{N}$. Pour tout naturel p, notons E_p l'égalité $a^p b^q = b^q a^p$ (qui fait sens). Montrons $\forall p \in \mathbf{N},\ E_p$ par récurrence.

   L'égalité E_0 est $a^0 b^q = b^q a^0$, ied $1b^q = b^q 1$, ou encore $b^q = b^q$, ce qu'on a.

   Soit maintenant $p \in \mathbf{N}$ tel que E_p. On a alors (comme ci-dessus) les égalités[5]

$$\begin{array}{lll} a^{p+1}b^q & \overset{\text{définition de la suite } (a^n)}{\underset{\text{par composition à droite}}{=}} & \left(a^p a\right) b^q \overset{\text{associativité}}{=} a^p\left(ab^q\right) \overset{A_q}{=} a^p\left(b^q a\right) \\ & \overset{\text{associativité}}{=} & \left(a^p b^q\right) a \overset{E_p}{=} \left(b^q a^p\right) a \overset{\text{associativité}}{=} b^q\left(a^p a\right) \\ & \overset{\text{définition de la suite } (a^n)}{\underset{\text{par composition à droite}}{=}} & b^q a^{p+1}, \text{ d'où } E_{p+1}, \text{ CQFD.} \end{array}$$

   (apprécier ici que nous n'avons pas besoin de quantifier sur q dans l'énoncé E_p montré par récurrence)

3. Pour tout naturel n, on abrège P_n l'égalité $(ab)^n = a^n b^n$, laquelle fait sens et nous allons établir par récurrence.

   L'égalité P_0 est $(ab)^0 = a^0 b^0$, ied $1 = 1 \cdot 1$, ce qu'on a.

   Soit ensuite $n \in \mathbf{N}$ tel que P_n : on a alors les égalités[6]

$$\begin{array}{lll} (ab)^{n+1} & \overset{\text{définition de la suite } \left((ab)^k\right)}{\underset{\text{par composition à droite}}{=}} & (ab)^n\,(ab) \overset{P_n}{=} \left(a^n b^n\right) ab \overset{\text{associativité}}{=} a^n\left(b^n a\right) b \\ & \overset{\text{premier}}{\underset{\text{point } A_n}{=}} & a^b\left(ab^n\right) b \overset{\text{associativité}}{=} \left(a^n a\right)\left(b^n b\right) \\ & \overset{\text{définition des itérés}}{\underset{\text{par composition à droite}}{=}} & a^{n+1}b^{n+1}, \text{ d'où } P_{n+1}, \text{ CQFD.} \end{array}$$

Le lecteur établira de façon analogue les propriétés suivantes.

PROP (composés & itérés d'itérés). *Soit a dans un monoïde. On a alors pour tous naturels p, q les égalités*

$$\begin{array}{rcll} a^p a^q & = & a^{p+q} & \textit{(en additif : } pa + qa = (p+q)\,a\textit{),} \\ \left(a^p\right)^q & = & a^{pq} & \textit{(en additif : } p\,(qa) = (pq)\,a\textit{).} \end{array}$$

DEF-PROP (itérés "bilatères" d'un inversible). *Soit a un inversible dans un monoïde. Pour tout naturel n, on définit*

$$a^{-n} := \left(a^{-1}\right)^n \qquad \textit{(bien observer la cohérence lorsque } n = 0 \textit{ ou } n = 1\textit{).}$$

[5] C'est *de ce calcul* (troisième égalité) qu'émerge naturellement la propriété A_n établie précédemment ; comme souvent l'ordre génétique d'une preuve est inverse à celui de sa présentation

[6] encore un fois apparaît dans ce calcul (quatrième égalité) la propriété A_n, motivant d'autant plus le premier point

1. *On a pour tous relatifs p, q les égalités*

$$\begin{array}{rcll} a^p a^q & = & a^{p+q} & \textit{(en additif : } pa + qa = (p+q)\,a\textit{),} \\ (a^p)^q & = & a^{pq} & \textit{(en additif : } p\,(qa) = (pq)\,a\textit{).} \end{array}$$

   En conséquence, les itérés "bilatères" de a commutent.

2. *La suite "bilatère" $(a^z)_{z\in\mathbf{Z}}$ des itérés de a est déterminée par chacune des deux conjonctions*

$$\left\{\begin{array}{c} a^0 = 1 \\ \forall z \in \mathbf{Z},\ a^{z+1} = aa^z \end{array}\right. \qquad \textit{ou} \qquad \left\{\begin{array}{c} a^0 = 1 \\ \forall z \in \mathbf{Z},\ a^{z+1} = a^z a \end{array}\right. ,$$

   ied est l'unique suite obtenue à partir du neutre par itération de la composition par a (d'un côté comme de l'autre) :

$$\begin{array}{rl} & \cdots \longmapsto a^{-3} \longmapsto a^{-2} \longmapsto a^{-1} \longmapsto 1 \longmapsto a \longmapsto a^2 \longmapsto a^3 \longmapsto \cdots \\ \textit{(en additif :} & \cdots \longmapsto -3a \longmapsto -2a \longmapsto -a \longmapsto 0 \longmapsto a \longmapsto 2a \longmapsto 3a \longmapsto \cdots \textit{)}. \end{array}$$

3. *Soient enfin α et β deux inversibles qui commutent*[7]*. Alors chaque itéré de α commute avec chaque itéré de β et on a pour chaque relatif z les égalités*

$$(\alpha\beta)^z = \alpha^z \beta^z \qquad \textit{(en additif : } z\,(\alpha+\beta) = z\alpha + z\beta\textit{).}$$

Ces propriétés ne font qu'étendre celles déjà connues pour les itérés "unilatères". De fait, leurs démonstrations prolongent celles "unilatères", le complément à apporter étant relégué en exercices.

★ *Montrer que les deux suites définissant "la" suite des itérés coïncident.*

Soit a dans un monoïde. Notons g (resp. d) la suite définie par le terme initial a en itérant la composition à **g**auche (resp. **d**roite) par a. Pour tout naturel n, notons C_n la conjonction $\left\{\begin{array}{c} g_n = d_n \\ g_n a = a g_n \end{array}\right.$ (qui fait sens). Montrons $\forall n \in \mathbf{N},\ C_n$ par récurrence, d'où il découlera par le premier conjoint l'égalité désirée $g = d$.

La conjonction C_0 est $\left\{\begin{array}{c} g_0 = d_0 \\ g_0 a = a g_0 \end{array}\right.$, ied $\left\{\begin{array}{c} 1 = 1 \\ 1a = a1 \end{array}\right.$, ce qu'on a.

Soit $n \in \mathbf{N}$ tel que C_n. On a alors d'une part $g_{n+1}a = (ag_n)\,a = a\,(g_n a) \overset{C_n}{=} a\,(ag_n) = ag_{n+1}$, d'autre part $g_{n+1} = ag_n \overset{C_n}{=} g_n a \overset{C_n}{=} d_n a = d_{n+1}$, CQFD[8].

★ *Montrer que le théorème d'existence des suites d'itérés (dans les monoïdes) est équivalent au théorème fondamental de définition de suites par itération.*

L'implication $\Longleftarrow$ faisant l'objet du cours, montrons celle $\Longrightarrow$.

Soit A un ensemble. Soient $\blacklozenge \in A$ et $f \in A^A$. Dans ce dernier monoïde, on dispose par hypothèse d'une suite des itérés $(f^{\circ n})$. Définissons alors $(a_n) := (f^{\circ n}(\blacklozenge))$. Puisque chaque $f^{\circ n}$ reste dans A^A, chaque a_n tombe dans A ; la suite (a_n) est donc à valeurs dans A. Vérifions qu'elle répond à nos deux critères. On a d'une part les égalités

$$a_0 = f^{\circ 0}(\blacklozenge) = \underset{A}{\mathrm{Id}}\,(\blacklozenge) = \blacklozenge,$$

d'autre part à $n \in \mathbf{N}$ fixé les égalités

$$a_{n+1} = f^{\circ(n+1)}(\blacklozenge) = [f \circ f^{\circ n}](\blacklozenge) = f\,(f^{\circ n}(\blacklozenge)) = f\,(a_n)\,.$$

★*Montrer un théorème de définition de suites indexée par $\mathbf{Z}$ définies par itération en remplaçant dans le théorème fondamental les monoïdes A^A et $\mathbf{N}$ par les groupes $\mathfrak{S}_A$ et $\mathbf{Z}$ respectivement.*

[7] La commutativité est indispensable : si $\alpha\beta^2 = (\alpha\beta)^2$, simplifier par α à gauche et par β à droite donne alors $\alpha\beta = \beta a$.

[8] La dernière chaîne d'égalité fait apparaître clairement pourquoi nous avons "renforcé" l'énoncé à montrer par récurrence.

DEM Comme pour le cas du th fondamental, il suffit d'utiliser les itérés de l'application itérante. On recopie alors mot pour mot la démonstration ? ? ? en remplaçant les monoïdes A^A et $\mathbf{N}$ par les groupes $\mathfrak{S}_A$ et $\mathbf{Z}$ respectivement.

★ *Démontrer proprement les deux propriétés des itérés dans un monoïde laissées sans démonstration dans le cours.*

DEM

1. Pour tous naturels p et q, notons ${}^pE^q$ l'égalité $a^p a^q = a^{p+q}$ et ${}^p\mathcal{E}$ l'énoncé $\forall n \in \mathbf{N},\ {}^pE^n$ (qui font tous deux sens). Observer que les égalités ${}^pE^1$ (resp. ${}^1E^q$) découlent de la définition de la suite (a^n) par composition à droite (resp. gauche). Montrons $\forall p \in \mathbf{N},\ {}^p\mathcal{E}$ par récurrence, ce qui conclura.

   Soit $q \in \mathbf{N}$. L'égalité ${}^0E^q$ est $a^0 a^q = a^{0+q}$, ied $1a^q = a^q$, ce qu'on a, d'où ${}^0\mathcal{E}$.

   Soit $p \in \mathbf{N}$ tel que ${}^p\mathcal{E}$. Soit $q \in \mathbf{N}$. On a alors les égalités

$$a^{p+1}a^q \overset{{}^pE^1}{=} (a^p a)\, a^q \overset{\text{associativité}}{=} a^p\,(aa^q) \overset{{}^1E^q}{=} a^p a^{q+1}\,;$$

   or l'égalité ${}^pE^{q+1}$ découlant[9] de l'hypothèse ${}^p\mathcal{E}$ montre que le dernier composé vaut $a^{p+(q+1)} = a^{(p+1)+q}$, d'où l'égalité ${}^{p+1}E^q$; il en résulte ${}^{p+1}\mathcal{E}$, CQFD.

2. Soit $q \in \mathbf{N}$. Pour tout naturel n, on abrège A_n l'égalité $(a^n)^q = a^{nq}$. Montrons $\forall p \in \mathbf{N},\ A_p$ par récurrence.

   L'égalité A_0 est $\left(a^0\right)^q = a^{0q}$, ied $1^q = a^0$, ied $1 = 1$, ce qu'on a.

   Soit $p \in \mathbf{N}$ tel que A_p. On a alors les égalités[10]

$$\begin{aligned}\left(a^{p+1}\right)^q &\overset{{}^pE^1}{=} (a^p a)^q \overset{\text{exo sur les itérés qui commutent}}{=} (a^p)^q\, a^q \overset{A_p}{=} a^{pq}a^q \\ &\overset{{}^{pq}E^q}{=} a^{pq+q} = a^{(p+1)q}, \text{ d'où } A_{p+1}, \text{ CQFD.}\end{aligned}$$

★ *Établir les propriétés des itérés bilatères laissées sans démo dans le cours.*

Soit a un inversible. On reprend les mêmes notations que pour les itérés unilatères (*cf.* exercice précédent).

1. Reprenons les énoncés ${}^pE^q$ et ${}^p\mathcal{E}$. Les preuves de ${}^0\mathcal{E}$, ${}^1\mathcal{E}$ et $\mathcal{E}^1$ (dont on devenira le sens) sont identiques. Pour compléter la preuve par induction, il suffit de montrer que la récurrence se propage vers les négatifs. Reprendre la preuve "unilatère" en remplaçant $+1$ par -1 montre qu'il suffit d'établir ${}^{-1}\mathcal{E}$ et $\mathcal{E}^{-1}$, ce que nous ferons en parallèle.

   Soit $p \in \mathbf{Z}$. L'énoncé $\begin{matrix}{}^1\mathcal{E}\\ \mathcal{E}^1\end{matrix}$ spécialisé en $\begin{matrix}-1+p\\ p-1\end{matrix}$ donne $\begin{matrix}a^1a^{-1+p} = a^{1+(-1+p)}\\ a^{p-1}a^1 = a^{(p-1)+1}\end{matrix} = a^p$, composer à $\begin{matrix}\text{gauche}\\ \text{droite}\end{matrix}$ par a^{-1} donne $\begin{matrix}{}^{-1}E^p\\ {}^pE^{-1}\end{matrix}$, ce qui établit $\begin{matrix}{}^{-1}\mathcal{E}\\ \mathcal{E}^1\end{matrix}$.

2. Reprenons les énoncés A_n (à $q \in \mathbf{Z}$ fixé). Comme ci-dessus, remplacer $+1$ par -1 dans la preuve de l'hérédité montre qu'il suffit d'établir A_{-1} pour conclure.

   Puisque a et a^{-1} commutent, on peut écrire $a^q\left(a^{-1}\right)^q = \left(aa^{-1}\right)^q = 1^q = 1$. On conclut alors en composant à gauche par a^{-q} puis en utilisant l'égalité ${}^{-q}E^q$.

   (Autre preuve : disjonction des cas. Si $q \geq 0$, l'égalité A_{-1} est une définition. Sinon, en notant $b := a^{-1}$, on a alors $\left(a^{-1}\right)^q = b^q = \left(b^{-1}\right)^{-q} = a^{-q}$.)

3. Soit $(u_z)_{z\in\mathbf{Z}}$ une suite bilatère. On a alors les équivalences

$$\forall z \in \mathbf{Z},\ u_{z+1} = au_z \iff \left\{\begin{array}{c}\forall z \in \mathbf{N},\ u_{z+1} = au_z\\ \forall z \in -\mathbf{N}^*,\ u_z = a^{-1}u_{z+1}\end{array}\right. \iff \left\{\begin{array}{c}\forall n \in \mathbf{N},\ u_{n+1} = au_n\\ \forall n \in \mathbf{N},\ u_{-(n+1)} = a^{-1}u_{-n}\end{array}\right. .$$

   Ainsi la relation ci-dessus déterminera-t-elle entièrement, avec une condition initiale (fixer u_0), les deux suites (u_n) et (u_{-n}), ied la suite (u_z), d'où la caractérisation de la suite des itérés bilatères par itération de la composition par a à gauche (démonstration identique à droite).

[9] observer ici pourquoi nous avons rentré la quantification sur q dans l'énoncé ${}^p\mathcal{E}$ montré par récurrence

[10] apprécier ici que nous n'avons pas besoin de quantifier sur q dans l'énoncé montré par récurrence

4. Soit b un inversible qui commute avec a. Reprenons la preuve du cours ainsi que les notations A_n et E_p et P_n qui y figurent. Regardons ce dont il suffit pour enclencher la récurrence vers le bas en remplaçant dans les preuves les $+1$ par des -1.

   Pour les A_n, il suffit de montrer que a commute avec b^{-1}, ce qui s'écrit $ab^{-1} = b^{-1}a$, ou encore (composer à droite et à gauche par b) $ba = ab$, ce qu'on a.

   Pour les E_p, il suffit de montrer que a^{-1} commute avec b – preuve analogue.

   Pour les P_n, il suffit de montrer d'une part que a^{-1} commute avec les itérés de b (preuve analogue en distinguant selon le signe de l'exposant au-dessus de b) d'autre part P_{-1} (ce qui s'écrit $(ab)^{-1} = a^{-1}b^{-1}$, ied $b^{-1}a^{-1} = a^{-1}b^{-1}$, ce qui est un cas particulier de la première part).

1.1 Création de structures

À l'exception des corps, le produit cartésien de chaque famille de trucs, muni de la loi produit, reste un truc, appelé ***truc produit****.*

Attention : cela n'est pas vrai pour les corps !

★ *Soit M un magma.*

a. *Calculer les composés "parties" du vide. En déduire que $\mathfrak{P}(M)$ n'est jamais un groupe (sauf cas trivial à préciser).*

b. *Montrer que M est abélien (resp. associatif, unifère) ssi $\mathfrak{P}(M)$ l'est pour la loi "parties". Quelle hypothèse manque-t-il ?*

c. *Lorsque M est un monoïde, montrer que $\mathfrak{P}(M)$ est un monoïde pour la loi "parties" dont on précisera le neutre et les inversibles.*

d. *En déduire que $\mathfrak{P}(M)\setminus\{\emptyset\}$ n'est jamais un groupe (sauf cas trivial à préciser).*

---

a. Soit $A \subset M$, on veut calculer $A\emptyset$ et $\emptyset A$. Rappelons que le produit cartésien $A \times \emptyset$ est vide. Le cours de première année nous dit par ailleurs que l'image directe (par chaque application) de la partie vide est vide. En particulier, l'image directe de $A \times \emptyset$ par la loi de M est vide ; or cette image $\{ao\ ;\ (a,o) \in A \times \emptyset\}$ est précisément le composé $A\emptyset$ (même raisonnement pour $\emptyset A$). On obtient finalement les égalités

$$A\emptyset = \emptyset = \emptyset A \qquad \text{(on dit que } \emptyset \text{ est } \textbf{\textit{absorbant}} \text{ pour la loi "parties").}$$

Lorsque M est vide, le magma $\mathfrak{P}(M) = \{\emptyset\}$ est trivial et est donc un groupe (abélien). Supposons réciproquement que $\mathfrak{P}(M)$ est un groupe : simplifier l'égalité $\emptyset\emptyset = \emptyset$ montre alors que $\emptyset$ est un neutre "parties", d'où l'égalité $M \underset{\text{neutre}}{\overset{\emptyset \text{ est}}{=}} M\emptyset \underset{\text{absorbant}}{\overset{\emptyset \text{ est}}{=}} \emptyset$. (On retiendra plus généralement qu'*un groupe non trivial ne contient jamais d'absorbant.*)

Finalement, $\mathfrak{P}(M)$ est un groupe (alors trivial) ssi M est vide.

b. Soient $A, B, C \subset M$ et $m, \mu, \mathfrak{m} \in M$.

- Lorsque M est abélien, on a immédiatement

$$AB = \{ab\}_{b\in B}^{a\in A} \underset{\text{abélien}}{\overset{M \text{ est}}{=}} \{ba\}_{b\in B}^{a\in A} = BA.$$

  Supposer réciproquement $\mathfrak{P}(M)$ abélien donne les égalités

$$\{m\mu\} = \{m\}\{\mu\} \underset{\text{abélien}}{\overset{\mathfrak{P}(M) \text{ est}}{=}} \{\mu\}\{m\} = \{\mu m\}\text{, d'où } m\mu = \mu m.$$

- Vu les égalités $\begin{cases} (AB)C = \{xc\}_{c\in C}^{x\in AB} = \{(ab)c\}_{\substack{b\in B \\ c\in C}}^{a\in A} \\ A(BC) = \{ay\}_{y\in BC}^{a\in A} = \{a(bc)\}_{\substack{b\in B \\ c\in C}}^{a\in A} \end{cases}$, l'associativité de M implique celle de $\mathfrak{P}(M)$.

  Vu les égalités $\begin{cases} \{m\}\ (\ \{\mu\}\{\mathfrak{m}\}\ ) = \{m\}\{\mu\mathfrak{m}\} = \{m(\mu\mathfrak{m})\} \\ (\ \{m\}\{\mu\}\ )\ \{\mathfrak{m}\} = \{m\mu\}\{\mathfrak{m}\} = \{(m\mu)\mathfrak{m}\} \end{cases}$, supposer $\mathfrak{P}(M)$ associatif permet d'égaliser ces deux derniers singletons, d'où $m(\mu\mathfrak{m}) = (m\mu)\mathfrak{m}$.

- Supposons enfin M unifère et notons u son neutre. Alors la partie $\{u\}$ est un neutre pour $\mathfrak{P}(M)$ vu les égalités

$$Au = \{au\}_{a\in A} \underset{\text{neutre}}{\overset{u \text{ est}}{=}} \{a\}_{a\in A} = A \text{ (\textit{idem} de l'autre côté).}$$

Supposons réciproquement $\mathfrak{P}(M)$ unifère et notons U son neutre. On a alors les égalités

$$\{m\} \underset{\text{neutre}}{\overset{U \text{ est}}{=}} U\{m\} = \{um\}_{u\in U}\text{, d'où } \forall u \in U,\ um = m \text{ (\textit{idem} de l'autre côté),}$$

ce qui monte que chaque élément de U est un neutre pour M, d'où le caractère unifère de M *pourvu que U soit non vide*. Or la vacuité de U impliquerait celle de tous ses composés "parties", en particulier celle de $U\{m\} = \{m\}$, rendant illicite l'invocation de m et forçant ainsi la vacuité de M.

L'hypothèse manquante est donc « $M \neq \emptyset$ » : sinon $\mathfrak{P}(M) = \{\emptyset\}$ est un groupe trivial !

c. Par le point précédent, les caractères associatif et unifère "passent" de M à $\mathfrak{P}(M)$ dont le neutre est $\{1_M\}$.

Déterminons ses inversibles. Soient $A, B \subset M$ tels que $AB = \{1\} = BA$, égalités se réécrivant $\forall (a,b) \in A \times B,\ ab = 1 = ba$ et impliquant l'inversibilité de chaque élément de $A \cup B$ – *a fortiori* leur régularité. Montrons que A et B sont des singletons. Soient $a \in A$ et $b, b' \in B$: les éléments ab et ab' appartiennent au même singleton $AB = \{1\}$, donc sont égaux, d'où (par régularité de a) l'égalité $b = b'$ (même raisonnement pour A). Enfin, les parties A et B sont non vides car leur composé $\{1\}$ est non vide.

Finalement, les inversibles de $\mathfrak{P}(M)$ sont les singletons associés aux inversibles de M :

$$\mathfrak{P}(M)^\times = \left\{\{i\}\ ;\ i \in M^\times\right\}.$$

d. Supposons que $\mathfrak{P}(M)\setminus\{\emptyset\}$ est un groupe. Son neutre est alors une partie non vide de M ne contenant (suivant le point 1.1) que des neutres de M, donc est de la forme $\{1_M\}$. Le point 1.1 montre alors que les inversibles de $\mathfrak{P}(M)\setminus\{\emptyset\}$ sont des singletons ; or, $\mathfrak{P}(M)\setminus\{\emptyset\}$ étant un groupe, tous ses éléments sont inversibles, en particulier l'élément M (qui est bien non vide car unifère). Le monoïde M est donc trivial.

Réciproquement, si M est trivial, le magma $\mathfrak{P}(M)\setminus\{\emptyset\} = \{M, \emptyset\}\setminus\{\emptyset\} = \{M\}$ est un groupe trivial.

★ *Soit G un groupe dont chaque élément est involutif.*

a. *Donner une infinité d'exemples de tels groupes G.*

1. *Montrer que G est abélien. Sa loi sera désormais notée*[11] $+$.

b. *Montrer que G admet une unique structure de $\mathbb{F}_2$-espace vectoriel*[12].

c. *On suppose G fini. Montrer qu'il y a un naturel d et une bijection $\varphi : G \longrightarrow \left(\mathbb{Z}/2\right)^d$ préservant l'addition.*

---

a. Le groupe additif $\mathbb{F}_2$ en est un, *a fortiori* toutes ses puissances entières $\mathbb{F}_2^n$ et, plus généralement, la "puissance" $\mathbb{F}_2^{(I)}$ pour chaque ensemble I.

Remarque – Les $\mathbb{F}_2^n$ sont deux à deux non isomorphes (*cf.* section **??**) car leurs cardinaux sont (deux à deux) distincts. L'exercice montre que ces exemples épuisent les cas où G est fini.

b. On a pour tous $a, b \in G$ les égalités

$$ab = a1b = a(ab)^2 b = a(abab)b = a^2(ba)b^2 = ba.$$

c. Soit $g \in G$: le calcul vectoriel impose $\overline{0}g = 0$ et l'axiome neutre impose $\overline{1}g = g$, d'où l'unicité. Définissons donc l'action scalaire de $\mathbb{F}_2$ comme imposé par l'unicité et vérifions les quatre axiomes d'un espace vectoriel. Soient $a, b \in \mathbb{Z}$ et $g, h \in G$.

On a déjà $\lambda 0 = 0$ pour chaque scalaire λ (remplacer g par 0 dans la définition ci-dessus). Il en résulte les égalités[13]

$$\left\{\begin{array}{l}\overline{0}\,\boxed{\overline{b}g} = 0\\ \boxed{\overline{0}\overline{b}}g = 0\end{array}\right.,\ \left\{\begin{array}{l}\overline{0}\,\boxed{g+h} = 0\\ \boxed{\overline{0}g} + \boxed{\overline{0}h} = 0+0\end{array}\right. \text{ et } \left\{\begin{array}{l}\boxed{\overline{a}+\overline{0}}g = \boxed{\overline{a}}g\\ \overline{a}g + \boxed{\overline{0}g} = \overline{a}g + \boxed{0}\end{array}\right..$$

[11] À l'exception de l'addition ordinale, une loi notée $+$ sera toujours commutative.

[12] On admettra que $\mathbb{F}_2 := \mathbb{Z}/2$ est un corps pour les lois usuelles.

[13] La commutativité des additions permet d'éviter la vérifiation de $\left(\overline{0}+\overline{b}\right)g = \overline{0}g + \overline{b}g$.

On a par construction $\overline{1}g = g$, d'où les égalités

$$\left\{\begin{array}{l}\overline{1}\boxed{\overline{b}g} = \boxed{\overline{b}g} \\ \boxed{\overline{1}\overline{b}}g = \boxed{\overline{b}}g\end{array}\right. , \left\{\begin{array}{l}\overline{1}\boxed{g+h} = \boxed{g+h} \\ \boxed{\overline{1}g} + \boxed{\overline{1}h} = \boxed{g} + \boxed{h}\end{array}\right. \text{ et } \left\{\begin{array}{l}\boxed{\overline{1}+\overline{1}}g = \boxed{\overline{2}}g = \overline{0}g = 0 \\ \boxed{\overline{1}g} + \boxed{\overline{1}g} = \boxed{g} + \boxed{g} \underset{\text{involutif}}{\overset{g \text{ est}}{=}} 0\end{array}\right. .$$

c. Étant fini, le $\mathbb{F}_2$-espace vectoriel G est de dimension finie, donc isomorphe en tant qu'espace vectoriel à $\mathbb{F}_2^{\dim G}$. Or un isomorphisme d'espaces vectoriels préserve l'addition, ce qui conclut en posans $d := \dim_{\mathbb{F}_2} G$.

REMARQUE – Invoquer une $\mathbb{F}_2$-base vectorielle de G (notons I son ensemble indexant) donne toujours un isomorphisme d'espaces vectoriels $G \simeq \mathbb{F}_2^{(I)}$. Lorsque G est fini, on peut choisir I fini et l'on a alors $\mathbb{F}_2^{(I)} = \mathbb{F}_2^I$. Lorsque G est infini, une telle invocation requiert l'axiome du choix.

1.2 Morphismes

Exercice (sous-trucs). Soient M un truc et S une partie de M. *Montrer qu'il y a au plus une structure de truc sur S telle que l'inclusion canonique de S dans M soit un morphismes de trucs.*

SOL (pour les groupes, monoïdes & magmas) Soit $*$ une telle loi. En notant i l'inclusion canonique, on a alors à $s, \sigma \in S$ fixés

$$s * \sigma = i(s * \sigma) = i(s)\, i(\sigma) = s\sigma, \text{ ce qui détermine } *.$$

Par ailleurs (cas monoïdal), l'unité de S étant envoyée sur celle de M par l'inclusion canonique, ces unités sont égales. Enfin (cas des groupes), un symétrique étant uniquement défini par la loi et le neutre, l'inversion de S coïncide avec celle de M. Lorsqu'il existe une telle structure, on retrouve alors que S est un sous-truc de M.

1.2.1 Isomorphie, homomorphismes

Exercice (signature d'une permutation). Montrer que l'application $\sigma \overset{\varepsilon}{\mapsto} \prod_{1\leq i<j\leq n} \frac{\sigma(i)-\sigma(j)}{i-j}$ est un morphisme de $\mathfrak{S}_n$ sur $\mathbf{U}_2$.

Soient $\rho, \sigma \in \mathfrak{S}_n$. On a alors les égalités

$$\begin{aligned}\frac{\varepsilon(\rho\sigma)}{\varepsilon(\sigma)} &= \prod_{1\leq i<j\leq n} \frac{\rho\sigma(i)-\rho\sigma(j)}{i-j}\frac{i-j}{\sigma(i)-\sigma(j)} = \prod_{1\leq i<j\leq n} \frac{\rho\sigma(i)-\rho\sigma(j)}{\sigma(i)-\sigma(j)} \\ &= ???\text{ à finir }??? = \prod_{1\leq I<J\leq n} \frac{\rho(I)-\rho(J)}{I-J} = \sigma(\sigma)\end{aligned}$$

Attention : les objets dont parlent les axiomes de la théorie des groupes ne sont pas des groupes ! Ce sont des permutations, des symétries. Aussi devrait-on plutôt parler de *théorie des symétries*, tout comme on parle de théorie des ensembles, théorie des vecteurs ou de théorie des nombres. C'est seulement quand on jongle entre les différents modèles et que l'on étudie les morphismes les reliant que l'on devrait parler de *théorie des groupes*, théories des univers, théories des espaces vectoriels, théories des modèles des entiers...

1.2.2 Noyaux, quotients

lemme des noyaux (HP) *Chaque morphisme de groupes "passe au quotient"* modulo *son noyau ; plus précisément, chaque morphisme $\varphi : G \longrightarrow H$ de groupes induit un isomorphisme de groupes* $\left\{\begin{array}{ccc} {}^{G}\!/_{\operatorname{Ker}\varphi} & \xrightarrow{\sim} & \operatorname{Im}\varphi \\ \overline{g} & \longmapsto & \varphi(g)\end{array}\right.$.

DEM

Comme chaque application, φ induit une bijection[14] $\Phi := \left\{ \begin{array}{ccc} {}^{G}\!/_{\sim} & \longrightarrow & \operatorname{Im}\varphi \\ \overline{g} & \longmapsto & \varphi(g) \end{array} \right.$ où $\sim$ dénote la relation d'équivalence "avoir même image par φ". Montrons alors d'une part que cette dernière relation coïncide avec l'égalité *modulo* $K := \operatorname{Ker}\varphi$, d'autre part que le quotient ${}^{G}\!/_{K}$ est un groupe (pour la loi partie), ce qui permettra de conclure que Φ est un morphisme de groupes au vu des égalités à $g, \gamma \in G$ fixés

$$\Phi(\overline{g\gamma}) \underset{\text{quotient}}{\overset{\text{loi}}{=}} \Phi(\overline{g}\overline{\gamma}) \underset{\text{de } \Phi}{\overset{\text{prop.}}{=}} \varphi(g\gamma) \underset{\text{morphisme}}{\overset{\varphi \text{ est un}}{=}} \varphi(g)\varphi(\gamma) \underset{\text{de } \Phi}{\overset{\text{prop.}}{=}} \Phi(g)\Phi(\gamma).$$

L'égalité de relations annoncée découle des équivalences (à $g, \gamma \in G$ fixés)

$$g \sim \gamma \Longleftrightarrow \varphi(g) = \varphi(\gamma) \underset{\text{point (2)}}{\overset{\text{comme au}}{\Longleftrightarrow}} \gamma^{-1}g \in K \Longleftrightarrow g \in \gamma K.$$

Quant à l'aspect "groupe", il s'agit de montrer que K est un sous-groupe *distingué*[15] de G. Le point (**??**) nous dit déjà que ce noyau est un sous-groupe de G. Pour prouver son caractère distingué, soit $g \in G$ et calculons l'image directe[16]

$$\varphi\left(g^{-1}Kg\right) = \varphi\left(g^{-1}\right)\varphi(K)\varphi(g) = \varphi(g)^{-1}1\varphi(g) = \{1\}, \text{ d'où } g^{-1}Kg \subset K.$$

Composer à gauche par g permet alors de conclure.

Le point (1.2.2) va au contraire avoir de nombreuses répercussions et, bien que HP, nous l'utiliserons abondamment.

Applications (isomorphismes quotient). Rappelons que l'exponentielle est un morphisme de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \times)$.

1. Le morphisme $\left\{ \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{C}^* \\ t & \longmapsto & e^{it} \end{array} \right.$ est continu et non trivial (*cf.* chapitre ? ? ?), donc son noyau ne peut être dense, il est par conséquent discret (*cf.* section **??**), donc de la forme $2\pi\mathbb{Z}$ pour un certain réel[17] $\pi > 0$. L'image de ce morphisme valant par ailleurs tout le cercle unité $\mathbb{U}$, on en déduit un isomorphisme $\left\{ \begin{array}{ccc} {}^{\mathbb{R}}\!/_{2\pi} & \widetilde{\longrightarrow} & \mathbb{U} \\ \overline{a} & \longmapsto & e^{ia} \end{array} \right.$.
2. Soit $n \in \mathbb{N}^*$. Le morphisme $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{U} \\ z & \longmapsto & e^{2\pi i\frac{z}{n}} \end{array} \right.$ a pour noyau $n\mathbb{Z}$ et pour image $\mathbb{U}_n$, d'où un isomorphisme $\left\{ \begin{array}{ccc} {}^{\mathbb{Z}}\!/_{n} & \widetilde{\longrightarrow} & \mathbb{U}_n \\ \overline{z} & \longmapsto & e^{2\pi i\frac{z}{n}} \end{array} \right.$, lequel permet de traiter additivement les questions dans le groupe $\mathbb{U}_n$ sans se traîner les $e^{2\pi i\frac{\cdot}{n}}$ qui n'apportent rien.
3. Le morphisme $\left\{ \begin{array}{ccc} \mathbb{Q} & \longrightarrow & \mathbb{U} \\ \overline{q} & \longmapsto & e^{2\pi iq} \end{array} \right.$ a pour noyau $\mathbb{Z}$ et (**exercice !**) pour image $\bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n$, d'où un isomorphisme $\left\{ \begin{array}{ccc} {}^{\mathbb{Q}}\!/_{\mathbb{Z}} & \widetilde{\longrightarrow} & \bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n \\ \overline{q} & \longmapsto & e^{2\pi iq} \end{array} \right.$. Même remarque : il est bien plus pratique de travailler en additif pour étudier le groupe $\bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n$, les $e^{2\pi i\cdot}$ brouillant l'étude.
4. Soient a et b deux naturels non nuls. Le morphisme $\left\{ \begin{array}{ccc} \mathbb{U}_{ab} & \longrightarrow & \mathbb{U}_b \\ u & \longmapsto & u^a \end{array} \right.$ a pour noyau $\mathbb{U}_a$, d'où un morphisme injectif $\left\{ \begin{array}{ccc} {}^{\mathbb{U}_{ab}}\!/_{\mathbb{U}_a} & \longrightarrow & \mathbb{U}_b \\ \overline{u} & \longmapsto & u^a \end{array} \right.$; or l'égalité des cardinaux $\left|{}^{\mathbb{U}_{ab}}\!/_{\mathbb{U}_a}\right| = \frac{|\mathbb{U}_{ab}|}{|\mathbb{U}_a|} = \frac{ab}{a} = b = |\mathbb{U}_b|$ montre que cette injection est surjective, donc est un isomorphisme ${}^{\mathbb{U}_{ab}}\!/_{\mathbb{U}_a} \widetilde{\longrightarrow} \mathbb{U}_b$ (**exercice** : établir la (bien moins sympathique) version additive ${}^{\left({}^{\mathbb{Z}}/_{ab}\right)}\!/_{\left(b\,{}^{\mathbb{Z}}/_{ab}\right)} \widetilde{\longrightarrow} {}^{\mathbb{Z}}\!/_{b}$).
5. Soient K un corps et $n \geq 1$ un naturel. Le morphisme $\det : GL_n(K) \longrightarrow K^*$ est surjectif et de noyau $SL_n(K)$, d'où un isomorphisme $\left\{ \begin{array}{ccc} {}^{GL_n(K)}\!/_{SL_n(K)} & \widetilde{\longrightarrow} & K^* \\ \overline{M} & \longmapsto & \det M \end{array} \right.$. Cela est cohérent avec le fait que chaque matrice inversible M est produit de transvections (chacune élément de $SL_n(K)$) par une dilatation de rapport $\det M$.

[14] L'image directe par φ d'une classe $\overline{g}$ étant le singleton $\{\varphi(g)\}$, dont l'union vaut $\varphi(g)$, on définira Φ explicitement en envoyant une classe sur l'union de son image directe, ied par $C \mapsto \cup\varphi(C)$, puis on en *déduira* la propriété $\Phi(\overline{g}) = \varphi(g)$.

[15] *Cf.* exercices : une partie A d'un magma M est ***distinguée*** si $\forall m \in M,\ Am \subset mA$.

[16] Apprécier ici l'utilisation du langage des lois "parties"

[17] Voici la définition algébrique du demi-périmètre du cercle unité.

6. Soit $n \geq 2$ un naturel. La signature sur $\mathfrak{S}_n$ est un morphisme de noyau le groupe alterné $\mathfrak{A}_n$ et d'image $\mathbb{U}_2$, d'où un isomorphisme $\left\{ \begin{array}{ccc} {}^{\mathfrak{S}_n}\!/_{\mathfrak{A}_n} & \xrightarrow{\sim} & \mathbb{U}_2 \\ \overline{\sigma} & \longmapsto & \varepsilon(\sigma) \end{array} \right.$. On retrouve ainsi l'égalité[18] cardinale $|\mathfrak{A}_n| = \frac{|\mathfrak{S}_n|}{2} = \frac{n!}{2}$.

7. Soient a et b deux naturels premiers entre eux. L'application $\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & {}^{\mathbb{Z}}\!/_{a} \times {}^{\mathbf{Z}}\!/_{b} \\ z & \longmapsto & (\widetilde{z}, \widehat{z}) \end{array} \right.$ (inspirée du produit des projections canoniques *modulo* a et b resp.) est un morphisme de noyau $ab\mathbb{Z}$ vu à $z \in \mathbb{Z}$ fixé les équivalences

$$\begin{pmatrix} \widetilde{z} \\ \widehat{z} \end{pmatrix} = \begin{pmatrix} \widetilde{0} \\ \widehat{0} \end{pmatrix} \Longleftrightarrow \left\{ \begin{array}{l} a \mid z \\ b \mid z \end{array} \right. \overset{\text{GAUSS}}{\Longleftrightarrow} ab \mid z,$$

donc induit un isomorphisme $\left\{ \begin{array}{ccc} {}^{\mathbb{Z}}\!/_{ab} & \xrightarrow{\sim} & {}^{\mathbb{Z}}\!/_{a} \times {}^{\mathbb{Z}}\!/_{b} \\ \overline{z} & \longmapsto & (\widetilde{z}, \widehat{z}) \end{array} \right.$.

EXO *En déduire que l'ensemble* $\operatorname{Int} M$ *des automorphismes intérieurs de* M *est un groupe isomorphe au quotient de* $M^\times$ *par le centre de* M.

On en déduit que c induit un isomorphisme $\left\{ \begin{array}{ccc} {}^{M^\times}\!/_{Z} & \xrightarrow{\sim} & \operatorname{Int} M \\ \overline{i} & \longmapsto & m \mapsto imi^{-1} \end{array} \right.$, ce qui conclut.

Exercice (quotients et produits). Soient G et H deux groupes. *En identifiant* H *à son image par l'injection canonique dans* $G \times H$*, montrer l'isomorphie* ${}^{G \times H}\!/_{H} \cong G$.

SOL Notons $H' := \{1\} \times H$ l'image identifiée à H. La projection canonique $G \times H \twoheadrightarrow G$ est alors un morphisme de noyau H', donc induit un isomorphisme $\left\{ \begin{array}{ccc} {}^{G \times H}\!/_{H'} & \xrightarrow{\sim} & G \\ \overline{(g,h)} & \longmapsto & g \end{array} \right.$

1.2.3 Plongements (HP)

Rappelons qu'une inclusion ensembliste $A \subset B$ induit une injection $A \hookrightarrow B$ où la source A s'identifie (car est égale) à son image directe, partie du but B, et que réciproquement une injection $A \hookrightarrow B$ entre ensembles peut et doit être pensée comme une *inclusion* $A' \subset B$ où l'on a identifié A à son image directe A' par l'injection (on dit parfois qu'on a *plongé* A dans B). Les exemples abondent :

1. On plonge $\mathbb{C}^{18}$ dans $\mathbb{C}[X]$ *via* $c \mapsto \sum_{n=0}^{17} c_{n+1} X^n$.
2. On plonge $\mathbb{R}^{42}$ dans $M_{42}(\mathbb{R})$ *via* $r \mapsto \operatorname{Diag} r$.
3. On plonge $\mathbb{Q}$ dans $\mathbb{Q}[X]$ *via* $q \mapsto (q, 0, 0, 0...)$ lorsque l'on définit les polynômes par des suites stationnant à 0.
4. On plonge $\mathbb{R}$ dans $\mathbb{C}$ suivant $r \mapsto (r, 0)$ quand on définit $\mathbb{C}$ comme $\mathbb{R}^2$. On peut aussi l'y plonger à travers $r \mapsto \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ si l'on définit $\mathbb{C}$ par des matrices de similitudes.
5. On plonge $\mathbb{C}$ dans $\mathbb{H}$ *via* $c \mapsto \begin{pmatrix} c & 0 \\ 0 & \overline{c} \end{pmatrix}$ lorsque l'on définit $\mathbb{H}$ comme l'algèbre (réelle) des $\begin{pmatrix} \alpha & -\beta \\ \beta & \overline{\alpha} \end{pmatrix}$ où α et β parcourent $\mathbb{C}$.
6. On plonge $\mathbb{N}$ dans $\mathbb{Z}$ *via* $n \mapsto \overline{(n, 0)}$ si l'on définit $\mathbb{Z}$ comme quotient de $\mathbb{N}^2$ par la relation "avoir même différence". On peut également l'y plonger suivant $n \mapsto \widetilde{n}$ si l'on définit $\mathbb{Z}$ comme quotient de $\mathbb{N}[X_1, X_2, X_3, ...]$ par les relations $X_n + 1 = 0$.
7. On plonge $\mathbb{Z}$ dans $\mathbb{Q}$ à travers $z \mapsto \overline{(z, 1)}$ quand on définit $\mathbb{Q}$ comme quotient de $\mathbb{Z} \times \mathbb{N}^*$ par la relation d'égalité des produits en croix. Si on le définit plutôt comme quotient de $\mathbb{Z}[Y_1, Y_2, ...]$ par les relations $nY_n = 1$, on peut encore y plonger $\mathbb{Z}$ *via* $z \mapsto \widetilde{z}$.
8. On plonge $\mathbb{Q}$ dans $\mathbb{R}$ suivant $q \mapsto \overline{(n \mapsto q)}$ lorsque $\mathbb{R}$ est défini comme quotient de l'ensemble des suites de Cauchy rationnelles par la relation "la différence tend vers 0".

[18] Le cardinal de A_n peut se retrouver sans quotients en observant que la translation par une transposition donnée induit une bijection du groupe alterné sur son complémentaire ? ? ? en exo ? ? ?

Lorsqu'une injection préserve de plus la structure, le truc source pourra et devra être identifié à un *sous-truc* du truc but (son image directe). C'est le cas des exemples précédents où toutes les injections sont des *morphismes* : $\mathbb{N}$ est un sous-monoïde de $\mathbb{Z}$, lequel est un sous-anneau de $\mathbb{Q}$, qui est un sous-corps de $\mathbb{R}$, lui-même sous-corps de[19] $\mathbf{C}$, l'ev $\mathbb{Q}^{42}$ peut être vu comme sev de $\mathbb{Q}[X]$ ou de $M_{42}(\mathbb{Q})$, l'algèbre $\mathbb{Q}$ comme sous-algèbre de $\mathbb{Q}[X]$...

Revenons aux groupes. Nous avons vu que l'injection canonique d'un sous-groupe dans le groupe plein était un morphisme. Réciproquement, l'image d'un morphisme de groupes injectif étant isomorphe au groupe source (**pourquoi ?**),

★ *chaque morphisme injectif* doit *être vu* ★ *(on parle alors*
★★ *comme l'*inclusion *d'un sous-groupe* ★★ *de* ***plongement****).*

Par exemple, le théorème de Cayley peut se reformuler « *tout groupe se plonge dans un groupe symétrique* ».??? laisser en exo ??? Autre exemple, dans un produit de groupes, on *doit* penser les facteurs comme autant de sous-groupes grâce aux isomorphismes induits par les injections canoniques (à l'instar de $\left\{\begin{array}{ccc} A & \xrightarrow{\sim} & A\times\{1\} \\ a & \longmapsto & (a,1) \end{array}\right.$), on doit penser chaque facteur *plongé dans* le produit.

Exercice (plongements ${}^{\mathbb{Z}}\!/_{n} \hookrightarrow \mathbb{U}$). *Montrer que chaque groupe ${}^{\mathbb{Z}}\!/_{n}$ se plonge dans $\mathbb{U}$.*

SOL Il suffit pour chaque $n\in\mathbb{N}^*$ d'écrire ${}^{\mathbb{Z}}\!/_{n} \cong \mathbb{U}_n \subset \mathbb{U}$. Reste le cas $n=0$. L'irrationalité de $\sqrt{2}$ par exemple permet de justifier l'injectivité du morphisme $\left\{\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & {}^{\mathbb{R}}\!/_{\mathbb{Z}} \\ a & \longmapsto & \overline{a\sqrt{2}} \end{array}\right.$, d'où un plongement $\mathbb{Z}\hookrightarrow {}^{\mathbb{R}}\!/_{\mathbb{Z}} \cong \mathbb{U}$ (explicitement : $z\mapsto e^{2\pi i\sqrt{2}z}$).

Exercice (indécomposabilité de $\mathbb{Z}$). *Montrer que $\mathbb{Z}$ est indécomposable,* i. e. *n'est pas (isomorphe à un) produit fini de groupes non triviaux.*

SOL Soient A et B deux groupes non triviaux tels que $\mathbb{Z}\simeq A\times B$. Chacun des facteurs est alors (isomorphe à) un sous-groupe de $\mathbb{Z}$, donc est de la forme $n\mathbb{Z}$ pour un naturel n non nul (les facteurs étant non triviaux), donc est isomorphe à $\mathbb{Z}$. On obtient ainsi un isomorphie $\mathbb{Z}\simeq\mathbb{Z}\times\mathbb{Z}$, ce qui est impossible, le groupe de gauche droite n'étant pas monogène contrairement à celui de gauche. Pour les détails, étant donné un plongement $\mathbb{Z}^2 \overset{i}{\hookrightarrow} \mathbb{Z}$, en notant a et b les images respectives (non nulles) des générateurs $\binom{1}{0}$ et $\binom{0}{1}$, l'injectivité est mise en défaut en écrivant $i\binom{0}{0} = 0 = ba-ab = bi\binom{1}{0} - ai\binom{0}{1} = i\binom{b}{a}$.

***Exercice (indécomposabilité des sous-groupes de Prüfer).** Soit p un premier. *Montrer que le groupe ${}^{\mathbb{Z}\left[\frac{1}{p}\right]}\!/_{\mathbb{Z}}$ est indécomposable.*

SOL Commençons par étudier les sous-groupes de G. Il y a (modulo $\mathbb{Z}$) chacun des $G_n := \left\langle \frac{1}{p^n} \right\rangle$ pour n décrivant $\mathbb{N}$, ainsi que $G = \left\langle \frac{1}{p^n} \right\rangle_{n\in\mathbb{N}^*}$ lui-même (notons-le G_∞ pour homogénéiser les notations). On montre dans les exercices que ce sont les seuls.

Soient $a,b\in\overline{\mathbb{N}}$ tels que $G\simeq G_a\times G_b$. L'infinitude de G montre que a ou b est infini, mettons $G\simeq G_a\times G$. Supposons G_a non trivial, *i. e.* $a\geq 1$. Comptons les éléments tués en au plus p itérations. À gauche, il y en a p exactement (à savoir $\frac{1}{p}, \frac{2}{p}, ..., \frac{p}{p}$). À droite, il y a au moins les p^2 éléments de la partie $G_1\times G_1$, d'où la contradiction vu que $p\geq 2$.

1.3 Groupes monogènes

1.4 Quotients (HP)

Le seul point exigible de cette section est, dans le résumé qui suit, l'implication $3\Longrightarrow 2$ dans le cas du premier exemple (groupes ${}^{\mathbb{Z}}\!/_{n}$) ainsi que la description des générateurs des ${}^{\mathbb{Z}}\!/_{n}$. Le théorème de Lagrange, dont nous aurons besoin section **??**, n'utilise que l'implication $3\Longrightarrow 1$.

Les résultats du résumé seront utilisés sans restriction dans ce cours, les quotients permettant d'alléger la présentation de nombreuses notions.

Discussion (HP).

[19] et $\mathbb{U}$ est une sous-$\mathbb{R}$-algèbre de $\mathbb{H}$

Soient $(G,+)$ un groupe *abélien*[20] et A une partie *non vide* de G. Imaginons que, pour quelque raison, nous souhaitions "tuer" A, *i. e.* faire comme si tous ses éléments (et seulement eux) étaient nuls, tout en continuant à calculer "comme d'habitude" dans le groupe G (en profitant des avantages de sa structure). Formellement, cela revient à chercher une "égalité" sur G

1. telle que chaque élément est "nul" ssi il appartient à A (condition « tuer A précisément ») ;
2. qui soit "compatible" avec le calcul de G en un sens à préciser (condition « continuer à calculer » : on veut au moins pouvoir ajouter et soustraire à deux élément "égaux" un même élément et conserver une "égalité", ainsi que disposer d'un "zéro").

Une telle "égalité" (notons-la $\overset{A}{=}$) doit donc vérifier pour tous $g,\gamma\in G$ les équivalences

$$g\overset{A}{=}\gamma \underset{\text{"usuel"}}{\overset{\text{calcul}}{\iff}} g-\gamma\overset{A}{=}0 \underset{\text{exactement}}{\overset{A\text{ est tué}}{\iff}} g-\gamma\in A.$$

L'analyse ne laisse nous laisse aucun choix : définissons une relation $\overset{A}{=}$ (appelée ***égalité***[21] **modulo**[22] A) par l'équivalence précédente

$$g\overset{A}{=}\gamma \overset{\text{déf.}}{\iff} g\in\gamma+A.$$

Elle réalise en particulier notre premier souhait ainsi qu'une partie du second[23] (quasiment par définition[24]) :

$$\begin{aligned}\forall g\in G,\qquad & g\overset{A}{=}0\iff g\in A,\\ \forall g,g',\gamma\in G,\qquad & g\overset{A}{=}g'\implies g+\gamma\overset{A}{=}g'+\gamma.\end{aligned}$$

Il va falloir travailler un peu plus pour réaliser entièrement notre second souhait. On montre déjà que *la relation $\overset{A}{=}$ est :*

1. *réflexive ssi A contient 0 ;*
2. *symétrique ssi A est stable par opposition ;*
3. *transitive* $\begin{array}{l}\textit{ssi elle est compatible}^{25}\textit{ avec }+\\ \textit{ssi } A \textit{ est stable par somme}\end{array}$.

Par conséquent :

l'égalité modulo A *est une relation d'équivalence sur G*
ssi A est un sous-groupe de G.
Dans ces conditions, $\overset{A}{=}$ est de plus compatible avec $+$.

Démonstration

1. Supposons $\overset{A}{=}$ réflexive. On a alors $0\overset{A}{=}0$, *i. e.* $0\in 0+A=A$.

   Supposons $0\in A$. On a alors pour chaque $g\in G$ l'appartenance $g=g+0\in g+A$, *i. e.* $g\overset{A}{=}g$.

2. Supposons $\overset{A}{=}$ symétrique. Soit $a\in A$. Cela se réécrit $a-0\in A$, *i. e.* $a\overset{A}{=}0$, *i. e.* (par symétrie) $0\overset{A}{=}a$, *i. e.* $0-a\in A$, ou encore $-a\in A$.

   Supposons $-A\subset A$. Soient $g,\gamma\in G$ tels que $g\overset{A}{=}\gamma$. Cela se réécrit $g-\gamma\in A$, d'où (en opposant) $-(g-\gamma)\in A$, *i. e.* $\gamma-g\in A$, ou encore $\gamma\overset{A}{=}g$.

[20] la généralisation au cas non abélien est proposée en exercice

[21] Karl Gauss a introduit ce vocabulaire dans ses *Disquisitiones arithmeticae* de 1801. Il y remplaçait l'égalité $=$ par le symbole de ***congruence*** $\equiv$ mais ce n'est pas indispensable : l'essentiel est de signaler quelque part que l'on calcule *modulo* quelque chose et de préciser ce quelque chose, le ***module***, la mesure à l'aune de laquelle on calcule.

[22] *modulo* = « à la mesure de »

[23] ajouter γ à l'appartenance $g\in g'+A$ donne $g+\gamma\in(g'+A)+\gamma=g'+\gamma+A$ vu l'associativité et la commutativité de la loi partie

[24] pour le second, bien noter l'utilisation de la *commutativité* pour déduire de $g\in g'+A$ l'appartenance $g+\gamma\in g'+A+\gamma=g\prime+\gamma+A$

[25] Une relation $\overset{\circ}{=}$ sur un magma M est dit ***compatible*** avec la loi de ce dernier si

$$\forall m,m',\mu,\mu'\in M,\ \left\{\begin{array}{c} m\overset{\circ}{=}m'\\ \mu\overset{\circ}{=}\mu'\end{array}\right.\implies m\mu\overset{\circ}{=}m'\mu'.$$

L'archétype de la relation compatible est l'égalité $=$, d'où la notation semblable $\overset{\circ}{=}$ que nous avons utilisée et celle similaire $\equiv$ souvent rencontrée pour les relations *d'équivalence* compatibles (appelées ***congruences***).

3. Supposons $\overset{A}{=}$ compatible avec la loi de G et montrons que A est stable. Soient $a, \alpha \in A$. Cela se réécrit $\begin{cases} a \in 0+A \\ \alpha \in 0+A \end{cases}$, *i. e.* $\begin{cases} a \overset{A}{=} 0 \\ \alpha \overset{A}{=} 0 \end{cases}$, d'où (par compatibilité) $a+\alpha \overset{A}{=} 0+0=0$, *i. e.* $a+\alpha \in 0+A=A$.

Supposons A stable et montrons que $\overset{A}{=}$ est transitive. Soient $g, \gamma, \mathfrak{g} \in G$ tels que $\begin{cases} g \overset{A}{=} \gamma \\ \gamma \overset{A}{=} \mathfrak{g} \end{cases}$. Cela se réécrit $\begin{cases} g \in \gamma + A \\ \{\gamma\} \subset \mathfrak{g} + A \end{cases}$, d'où les inclusions et appartenance

$$g \in \{\gamma\} + A \subset (\mathfrak{g} + A) + A = \mathfrak{g} + (A + A) \subset \mathfrak{g} + A, \text{ d'où } g \overset{A}{=} \mathfrak{g}.$$

Supposons $\overset{A}{=}$ transitive et montrons qu'elle est compatible avec $+$. Soient $g, g', \gamma, \gamma' \in G$ tels que $\begin{cases} g \overset{A}{=} g' \\ \gamma \overset{A}{=} \gamma' \end{cases}$.

Notre second souhait partiellement réalisé permet alors d'ajouter $\begin{cases} \gamma \text{ à droite} \\ g' \text{ à gauche} \end{cases}$, ce qui donne $\begin{cases} g+\gamma \overset{A}{=} g'+\gamma \\ g'+\gamma \overset{A}{=} g'+\gamma' \end{cases}$, d'où (par transitivité) $g+\gamma \overset{A}{=} g'+\gamma'$.

Dans le cas général, pour chaque $g \in G$ notons $\overline{g} := g + A$ le translaté de A par g, aussi appelé ***classe***[26] ***de*** g **modulo** A. L'ensemble de ces classes est appelé ***quotient*** de G par A et est noté

$$G/A := \{\overline{g}\}_{g \in G} = \{g + A \ ; \ g \in G\}.$$

Une remarque uniquement pour éclairer la prochaine équivalence (ainsi qu'un exercice) : le groupe G étant invariant par translation, *translater* A *ne change pas le quotient* vu à $u \in G$ fixé les égalités

$$G/A+u = \{g + (A+u)\}_{g \in G} \overset{G=G-u}{=} \{g+u+A\}_{g \in G-u} \overset{\text{reparamétrage}}{\underset{\gamma := g+u}{=}} \{\gamma + A\}_{\gamma \in G} = G/A.$$

Partons maintenant du fait suivant (trivial) :

les g pour g décrivant G forment un groupe.

Calquant cela *modulo* A, on va obtenir l'équivalence suivante :

les $\overline{g}$ pour g décrivant G forment un groupe (pour la loi partie)
ssi (un certain translaté de) A est un sous-groupe de G.

Si l'on rajoute à gauche notre second souhait affaibli (que le calcul avec les $\overline{g}$ se passe "comme avec les g"), on retrouvera à droite la condition sus-établie de congruence de $\overset{A}{=}$:

les $\overline{g}$ pour g décrivant G forment un groupe où $\overline{0}+\overline{0}=\overline{0}$
ssi A est un sous-groupe de G.
Dans ces conditions, on a pour tous $g, \gamma \in G$ les égalités $\begin{cases} \overline{g}+\overline{0}=\overline{g}=\overline{0}+\overline{g} \\ \overline{g}+\overline{\gamma}=\overline{g+\gamma} \\ -\overline{g}=\overline{-g} \end{cases}$.

Démonstration
Supposons que G/A est un groupe pour la loi partie. La somme $A+A=\overline{0}+\overline{0}$ reste dans G/A, donc est un certain $\overline{-u}$ (penser u comme un vecteur de translation). Montrons que le translaté $S := \overline{u}$ est un sous-groupe ("S" comme "**s**ous-"). La stabilité par $+$ découle des égalités

$$S+S=(u+A)+(u+A)=2u+(A+A)=2u+\overline{-u}=2u+(-u+A)=u+A=S.$$

Opposer l'égalité $S+S=S$ donne alors $-S=-(S+S)=-S-S$; ainsi S et $-S$ sont-ils des idempotents du groupe G/A, donc sont égaux (au neutre), d'où $-S=S$. Soit enfin $s \in S$ (on peut en invoquer car A est non vide) : S contient alors $S+S=S-S \ni s-s=0$.

[26] on pourrait également la noter $\widehat{g}$, $\widetilde{g}$, $\dot{g}$ ou encore $[g]$; l'important est de voir tout de suite que *c'est bien l'élément g qu'on manipule*, à quelque chose près signalé de manière plus discrète

Supposons de plus l'égalité $\overline{0}+\overline{0}=\overline{0}$. Elle se réécrit $\overline{-u}=A$, *i. e.* $-u+A=A$, *i. e.* $A=A+u$, ce qui montre que $A=S$ est un sous-groupe.

Supposons réciproquement que A est le translaté $S-u$ d'un sous-groupe S. Ce dernier étant un groupe, on peut utiliser l'égalité $S+S=S$ (*cf.* calcul 1 section **??**). On sait déjà que la loi partie est associative. Soient $g,\gamma\in G$. Les égalités

$$\overline{g}+\overline{\gamma}=(g+(S-u))+(\gamma+(S-u))=(g+\gamma-u)+\overbrace{\underbrace{S+S}_{=S}-u}^{=A}=\overline{g+\gamma-u}$$

montrent d'une part que $\overline{u}$ est neutre, d'autre part pour chaque $\mathfrak{g}\in G$ que $\overline{\mathfrak{g}}$ et $\overline{2u-\mathfrak{g}}$ sont opposés l'un de l'autre. Lorsque A est un sous-groupe, on peut supposer $u=0$ et ce qui précède donne les trois propriétés annoncées.

Résumé (quotient d'un groupe abélien par un sous-groupe). Soient G un groupe abélien et A une partie non vide[27] de G. *Les conditions suivantes sont alors équivalentes :*

1. *l'égalité* modulo A *est une relation d'équivalence sur* G *compatible avec la loi de* G *;*
2. *les* $\overline{g}$ *pour* g *décrivant* G *forment un groupe où*[28] $\left\{\begin{array}{c}\overline{g}+\overline{0}=\overline{g}=\overline{0}+\overline{g}\\ \overline{g}+\overline{\gamma}=\overline{g+\gamma}\\ -\overline{g}=\overline{-g}\end{array}\right.$ *pour chaques* $g,\gamma\in G$ *;*
3. A *est un sous-groupe de* G.

Dans ces conditions, le quotient par la relation d'équivalence $\overset{A}{=}$ et celui ${}^{G}\!/_{A}$ des translatés de A coïncident et forment un même groupe appelé ***groupe quotient***[29] de G par[30] A. Le premier point doit guider l'intuition : on calculera "comme d'habitude" avec des vraies égalités dans G en précisant quelque part[31] « *modulo* A ». Le deuxième point légitime ce guide : on peut écrire de vraies égalités dans ${}^{G}\!/_{A}$ en mettant des barres partout et en calculant "comme dans G".

Dans l'optique de notre souhait initial (tuer A), on pourra visualiser la barre de quotient ${}/_{A}$ comme la trace d'un coup de sabre assassin[32]. « Quotienter par » doit en effet être compris par « tuer », « annuler », « assassiner » :

quotienter par quelque chose,
c'est tuer tous ses éléments.

Exemples 1 (quotients ${}^{\mathbb{Z}}\!/_{n}$). Lorque l'on s'intéresse aux questions resp. de parité, de jours de la semaine, de demi-tons dans une octave, d'heures dans la journée ou de minutes dans une heure, on considère des nombres entiers (ce qui dénombre) tout en "tuant" le naturel resp. $2,7,12,24,60$. Cela revient à se placer dans le groupe quotient[33] ${}^{\mathbb{Z}}\!/_{n}:={}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ pour le naturel n correspondant. On pourra visualiser que l'on "tord", "boucle", "enroule" la droite $\mathbb{Z}$ pour forcer $n=0$ et l'on retrouve en fait le groupe $\mathbb{U}_n$ (à un *isomorphisme* près, *cf.* section 1.2), à l'exception de ${}^{\mathbb{Z}}\!/_{0}$ qui s'identifie à $\mathbb{Z}$ ("tuer" 0 ne change pas grand chose !).

FIG

Vu le cours sur les sous-groupes de $\mathbb{Z}$, on vient de décrire chacun de ses quotients.

Exemples 2 (quotients réels ou rationnels). Lorsque l'on s'intéresse aux questions resp. de mesures d'angles, d'intervalles harmoniquement parfaits[34] ou de parties fractionnaires (ce qui chez un réel vient après

[27] lorsque A est vide, le quotient ${}^{G}\!/_{\emptyset}=\{g+\emptyset\}_{g\in G}=\{\emptyset\}_{g\in G}=\{\emptyset\}$ est un groupe trivial, ce qui met en défaut l'équivalence entre points (2) et (3)

[28] Ce deuxième point pourrait s'énoncer : « la projection canonique *modulo* A est un morphisme de groupes ».

[29] Pour une histoire de la notion de groupe quotient (de Galois à Hölder en passant par Jordan), on consultera l'article *The development and understanding of the concept of quotient group* de Julia Nicholson (disponible en ligne).

[30] Lorsque la partie dont on considère les translatés est un sous-groupe, l'ensemble de ces translatés est un quotient par une relation d'équivalence (l'égalité *modulo* cette partie), d'où la terminologie "quotient" en général.

[31] Un tel calcul est qualifié de ***modulaire*** (adjectif relatif à *modulo*).

[32] Une relation d'équivalence correspondant à une partition, "*quotienter* G par un sous-groupe A" (au sens du quotient ${}^{G}\!/_{\overset{A}{=}}$) signifie également "*diviser* le bloc G en parties chacune un translaté de A" , "le *partitionner* suivant les classes *modulo* A".

[33] Observer que tuer n revient à tuer chacun de ses multiples.

[34] L'octave correspond à un doublement de fréquence, soit à la deuxième harmonique. La quinte apparaît à la *troisième* harmonique : il s'agit en fait d'une quinte plus une octave, on divise donc la fréquence par 2 pour obtenir une vraie quinte, ce qui correspond en fin de compte à multiplier la fréquence par $\frac{3}{2}$. Or le monde additif des intervalles (ayant l'octave pour unité) s'obtient à partir de celui multiplicatif des fréquences en appliquant un logarithme de base 2, ce qui fait apparaître de pas très rationnels $\lg_2\frac{3}{2}$ en harmonie "parfaite".

la virgule), on considère des nombres réels (ce qui mesure) tout en "tuant" resp. l'angle 2π (tour complet), l'intervalle de longueur 1 (l'octave) ou les entiers (qui n'ont rien après la virgule). Cela revient à se placer dans le groupe quotient resp. $\mathbb{R}/_{2\pi} := \mathbb{R}/_{2\pi\mathbb{Z}}$ ou $\mathbb{R}/_1 := \mathbb{R}/_{\mathbb{Z}}$. Comme pour $\mathbb{Z}$, on pourra visualiser que l'on "enroule" la droite réelle autour d'un cercle (de rayon resp. 1 ou $\frac{1}{2\pi}$) et l'on retrouve le groupe $\mathbb{U}$ – toujours à isomorphisme près.

FIG

On aurait également pu regarder le quotient $\mathbb{Q}/_{\mathbf{Z}}$, qui sera isomorphe à $\bigcup_{n\in\mathbb{N}^*}\mathbb{U}_n$.

Il semble plus difficile de se représenter les *autres* quotients de $\mathbb{R}$ ou $\mathbb{Q}$, *i. e.* ceux par des sous-groupes *denses*, à l'instar de $\mathbb{R}/_{\mathbb{Q}}$.

Exemples 3 (quotients par un sous-espace vectoriel). Soit E un espace vectoriel, soit V un sous-espace vectoriel de E. En particulier, V est un sous-groupe additif de E, donc le groupe quotient $E/_V$ fait sens. En utilisant une généralisation naturelle des lois partie, l'action du corps de base induit alors[35] une action sur $\mathfrak{P}(E)$ telle que $\lambda\overline{e} = \overline{\lambda e}$ pour chaque scalaire λ et chaque vecteur $e \in E$ (clair si $\lambda = 0$, sinon l'égalité $\lambda V = V$ donne $\lambda\overline{e} = \lambda(e+V) = \lambda e + \lambda V = \lambda e + V = \overline{\lambda e}$), ce qui munit $E/_V$ d'une structure d'espace vectoriel[36], appelé ***espace vectoriel quotient*** de E par V.

On peut voir le quotient $E/_V$ comme une sorte de "supplémentaire de V générique", au sens où *l'espace vectoriel $E/_V$ est isomorphe à chaque supplémentaire*[37] *de V*. Cela découle du **théorème du rang** formulé en ces termes (et appliqué aux projecteurs sur V) : *chaque application linéaire f de source E induit un isomorphisme $E/_{\operatorname{Ker} f} \xrightarrow{\sim} \operatorname{Im} f$* (**exercice**[38] **!**). Pour retrouver la **formule du rang** (en termes de dimensions), on peut montrer (**exercice !**) qu'en dimension finie *la dimension du quotient est le complémentaire de la dimension* : $\dim E/_V = \dim E - \dim V$. C'est pourquoi la dimension du quotient est en général appelée la ***codimension*** du sous-espace vectoriel par lequel on quotiente : $\operatorname{codim} V := \dim E/_V$.

Toutes les démonstrations de sup invoquant un supplémentaire peuvent souvent se réécrire bien plus élégamment à l'aide des espaces vectoriels quotient.

Exemples 4 (fonctions périodiques).

Une fonction d'argument réel et 2π-périodique peut être vue comme une fonction définie sur le cercle unité $\mathbb{R}/_{2\pi}$.

FIG : graphe d'une fonction réelle sur le cercle

De même, l'exponentielle complexe (qui est $2\pi i$-périodique) peut être définie sur le "cylindre horizontal" $\mathbb{C}/_{2\pi i}$ ("enrouler" le plan complexe en "cousant" les droites $\mathbb{R}$ et $\mathbb{R}+2\pi i$).

FIG : enroulement du plan

Enfin, chaque fonction d'argument complexe qui possède deux périodes α et β formant une base de $\mathbb{C}$ peut être vue comme définie sur le "tore" $\mathbb{C}/_{\mathbb{Z}\alpha+\mathbb{Z}\beta}$, que l'on pourra visualiser dans chaque parallélogramme de côtés (α, β) en "recollant" les côtés opposés.

FIG : réseau et une cellule

Exercice (quotients, produits et théorème de Lagrange). Soit A un sous-groupe d'un groupe G. *Montrer que les ensembles G et $G/_A \times A$ sont équipotents. En déduire lorsque G est fini l'égalité $\left|G/_A\right| = \frac{|G|}{|A|}$ et conclure au* **théorème de Lagrange (HP)** *:*

dans un groupe fini, l'ordre de chaque sous-groupe divise celui du groupe plein.

SOL

Idée : les éléments du quotient $\mathcal{G} := G/_A$ forment une partition de G, chacun de ces éléments étant, en tant que translaté de A, équipotent à A, d'où les équipotences $G \simeq \coprod_{C\in\mathcal{G}} C \simeq \coprod_{C\in\mathcal{G}} A \simeq \mathcal{G}\times A$.

Précisons cette idée. Soit $g \in G$. La translation à gauche par g induit une bijection $A \xrightarrow{\sim} gA$, ce qui montre que les classes *modulo* A sont équipotentes. Par ailleurs, l'appartenance $g = g1 \in gA$ montre que ces classes recouvrent G et les implications (à $\gamma \in G$ et $a, \alpha \in A$ fixés) $ga = \gamma\alpha \Longrightarrow g = \gamma\alpha a^{-1} \in \gamma A$ que ce recouvrement

[35] L'action du corps K de base $\left\{\begin{array}{ccc} K\times E & \longrightarrow & E \\ (\lambda, e) & \longmapsto & \lambda\cdot e \end{array}\right.$ induit une action du même corps $\left\{\begin{array}{ccc} K\times \mathsf{P}(E) & \longrightarrow & \mathsf{P}(E) \\ (\lambda, A) & \longmapsto & \{\lambda\cdot a\}_{a\in A} \end{array}\right.$.

[36] chaque axiome se montre en "passant" tout "sous la barre" et en y utilisant l'axiome correspondant de E

[37] *Idée* : lorsque l'on "tue" V dans un cassage $E = V \oplus S$, il ne reste plus que le supplémentaire S

[38] *Idée "quotient" de démonstration* : "tuer" le noyau revient à "tuer" le défaut d'injectivité, donc à rendre injectif.

est une *partition* (remarquer que l'on a utilisé toute l'hypothèse $1 \in A \supset AA^{-1}$). On peut alors conclure quand G est fini[39] :

$$|G| = \left| \biguplus_{C \in {}^{G}\!/_{A}} C \right| = \sum_{C \in {}^{G}\!/_{A}} |C| = \sum_{C \in {}^{G}\!/_{A}} |A| = \left|{}^{G}\!/_{A}\right| |A| \,,$$

le théorème de Lagrange découlant de l'intégralité de $\left|{}^{G}\!/_{A}\right|$.

Remarque. Explicitement (même si G est infini), étant donnée une fonction de choix[40] $\gamma : \mathcal{G} \longrightarrow G$, on montrerait que les applications

$$\left\{ \begin{array}{ccc} \mathcal{G} \times A & \longrightarrow & G \\ (C, a) & \longmapsto & \gamma_C a^{-1} \end{array} \right. \text{ et } \left\{ \begin{array}{ccc} G & \longrightarrow & \mathcal{G} \times A \\ g & \longmapsto & \left(\overline{g}, g^{-1}\gamma_{\overline{g}}\right) \end{array} \right. \qquad \text{FIG}$$

sont bien définies et réciproques l'une de l'autre. (Bien observer où l'hypothèse « A sous-groupe » intervient.)

2 Exercices

2.1 Dans les monoïdes

2.1.1 variations axiomatiques

Montrer que :

1. *un neutre dans un magma est unique ;*
2. *un élément neutralise un magma associatif régulier ssi il en neutralise au moins un élément d'au moins un côté ;*
3. *un magma fini est unifère ssi il possède un élément régulier à gauche et un élément régulier à droite ;*
4. *un magma régulier fini est un groupe ssi il est un monoïde.*
5. *un magma associatif régulier fini est un groupe ;*
6. *un magma associatif régulier est un groupe ssi* $\exists a, b,\ \forall x, \left\{ \begin{array}{l} \exists d,\ xd = a \\ \exists g,\ gx = b \end{array} \right.$ *. Peut-on se passer de l'hypothèse de régularité ?*

SOL

1. Soient u et v deux neutres dans un magma. Le composé uv vaut alors d'une part u (car v est neutre) d'autre part v (car u est neutre), d'où l'égalité $u = v$.
2. $\boxed{\Longrightarrow}$ clair. $\boxed{\Longleftarrow}$ Soit ε un tel "neutre". Soit a neutralisé à gauche (par exemple) par ε. Pour chaque m dans notre magma, composer l'égalité $a\varepsilon = a$ à droite par m et simplifier par a donne $\varepsilon m = m$, puis composer à gauche par m et simplifier à droite par m donne $m\varepsilon = \varepsilon$, d'où la neutralité de ε.
3. $\boxed{\Longrightarrow}$ clair, un neutre étant régulier. $\boxed{\Longleftarrow}$ Soient γ et δ réguliers resp. à gauche et à droite. L'application $a \mapsto \gamma a \delta$ est alors injective (par régularité), donc (par finitude) surjective, donc atteint $\gamma\delta$, mettons en un certain ε. Pour chaque m dans notre magma, simplifier l'égalité $\gamma\delta = \gamma\varepsilon\delta$ par $\begin{array}{c} \delta \\ \gamma \end{array}$, composer à $\begin{array}{c} \text{droite} \\ \text{gauche} \end{array}$ par m, puis simplifier par $\begin{array}{c} \gamma \\ \delta \end{array}$ donne $\begin{array}{l} m = \varepsilon m \\ m = m\varepsilon \end{array}$, d'où la neutralité de ε.
4. $\boxed{\Longrightarrow}$ clair. $\boxed{\Longleftarrow}$ Soit m dans notre monoïde. Les translations $m\cdot$ et $\cdot m$ sont injectives (par régularité), donc surjectives (par finitude), donc atteignent 1, d'où des inverses pour m des deux côtés : un exercice du cours montre alors que m est inversible.
5. Soit m dans notre magma. La translation $m\cdot$ est injective (par régularité), donc surjective (par finitude), donc atteint m, mettons en un ε. La question 2 montre alors, avec l'égalité $m\varepsilon = m$, que ε est neutre, donc notre magma est un monoïde ; étant par ailleurs régulier fini, il est un groupe d'après la question 4.

[39] la notation $\uplus$ pour l'union disjointe rappelle l'aspect *additif* du langage vernaculaire (« Dans mon sac, j'ai une pomme plus un portefeuille plus un livre, plus...») et ainsi que le cardinal d'une union disjointe vaut la *somme* des cardinaux.

[40] ied telle que $\gamma_C \in C$ pour chaque classe C. Une fonction de choix "*choisit*" ainsi dans chaque classe un élément.

6. Soient d tel que $ad = a$: la question 2 montre alors que a est neutre. On obtiendrait de même la neutralité de b, d'où (par la question 1) l'égalité $a = b$. Chaque élément est alors inversible des deux côtés, donc (par un exercice du cours) inversible.

   La régularité est nécessaire : chaque magma associatif muni d'un absorbant (par exemple un monoïde multiplicatifs $\mathbf{Z}/n$ avec l'absorbant $\overline{0}$) vérifie la condition lorsque l'on impose a, b, d, g égaux à cet absorbant (mais aucun des $\mathbf{Z}/n$ n'est un groupe multiplicatif si $n \neq 1$).

2.1.2 autour de l'inversibilité

Soit M un monoïde, soit $m \in M$.

1. *Montrer que m est inversible ssi il admet un inverse à droite et un inverse à gauche.*
2. *Montrer que m est inversible ssi les deux compositions par m sont bijectives. Même question en remplaçant « bijectives » par « surjectives ».*
3. *On suppose M fini. Montrer que m est inversible ssi il est régulier.*

Solution proposée.

1. Le sens direct est trivial, un inverse étant bilatère. Soient réciproquement n et ν des inverses de m resp. à gauche et à droite : il suffit de montrer leur égalité, laquelle vient en écrivant

$$n = n1 = n(m\nu) = (nm)\nu = 1\nu = \nu.$$

2. Supposons m inversible. Les applications $m\,\mathrm{Id}$ et $m^{-1}\,\mathrm{Id}$ sont alors réciproques l'une de l'autre, donc bijectives, *a fortiori* surjectives (de même de l'autre sens).

   Supposons $m\,\mathrm{Id}$ et $\mathrm{Id}\,m$ surjectives. Des antécédents du neutre sont alors des inverses à droite et à gauche de m, donc (*cf.* 1) coïncident et m est inversible.

3. La régularité d'un m équivaut à l'injectivité des deux homothéties $m\,\mathrm{Id}$ et $\mathrm{Id}\,m$, *i. e.* (par finitude de M) à leur surjectivité, *i. e.* (d'après 2) à l'inversibilité de m.

2.1.3 Régularité dans A^A

Soit A un ensemble. *Montrer que, dans le monoïde A^A, la régularité et l'inversibilité coïncident. On pourra montrer plus précisément*[41] *les équivalences*

$$\begin{array}{rcl} f \text{ inversible à gauche} & \iff & f \text{ régulier à gauche} \iff f \text{ injectif,} \\ f \text{ inversible à droite} & \iff & f \text{ régulier à droite} \iff f \text{ surjectif.} \end{array}$$

SOL

Soient $f, g \in A^A$ tels que $g \circ f = \mathrm{Id}$. Alors f est simplifiable à gauche (en composant à gauche par g), donc injective (simplifications par des fonctions constantes). Par ailleurs, g est surjective (chaque $a \in A$ admet $f(a)$ comme antécédent par g), donc régulière à droite (si $\alpha f = \beta f$, alors α et β coïncident sur $\mathrm{Im}\, f = A$).

Soit f injective. On définit une application g sur $\mathrm{Im}\, f$ par $f(a) \mapsto a$ (bien défini par injectivité) et par n'importe quoi ailleurs. On a alors clairement $g \circ f = \mathrm{Id}$.

Soit g régulière à droite. Alors g est surjective (sinon deux fonctions α et β différant uniquement en un point non atteint par g vérifieront $\alpha g = \beta g$) et l'on peut définir[42] une application f qui envoie un a sur l'un de ses antécédents. Il est alors immédiat que $g \circ f = \mathrm{Id}$.

[41] de la surjectivité à l'inversibilité à droite il pourra servir d'utiliser l'axiome du choix

[42] à l'aide de l'axiome du choix

2.1.4 Déformation de la loi d'un monoïde

Soit M un monoïde, soit $i \in M$. Appelons ${}^iM$ le magma M muni de la loi $(m, \mu) \mapsto mi\mu$. *Montrer que* ${}^iM$ *est un monoïde ssi* i *est inversible ; préciser alors son neutre et exhiber un isomorphisme* ${}^iM \simeq M$.

SOL
L'associativité est toujours vérifiée et découle de celle de M, le composé (dans ${}^iM$) de plusieurs éléments $\alpha, \beta, \gamma, ..., \psi, \omega$ s'écrivant $\alpha i \beta i \gamma i \cdots i \psi i \omega$. La caractère unifère de ${}^iM$ se réécrit $\exists u \in M, \forall m \in M, uim = m = miu$, çàd[43] $\exists u \in M, ui = 1 = iu$, ied i inversible. Dans ce cas, le neutre de ${}^iM$ est i^{-1} et la composition à gauche par i réalise un isomorphisme ${}^iM \widetilde{\longrightarrow} M$ au vu (à $m, \mu \in M$ fixés) des égalités $i\,(m * \mu) = i\,(mi\mu) = (im)\,(i\mu)$.

2.1.5 Sous-monoïdes de N

Les sous-monoïdes de $\mathbf{N}$ *sont-ils monogènes ?*

SOL
Soit $n \geq 2$ un naturel et notons $M := \{0\} \cup [n, \infty[$. Il s'agit clairement d'un sous-monoïde. Supposons qu'il soit monogène, soit $g \in \mathbf{N}$ l'engendrant. Alors la plus petite différence entre deux éléments distincts de M vaut au moins g ; or M contient des entiers consécutifs, ce qui force $g \leq 1$, d'où l'une des absurdes égalités $M = \{0\}$ ou $M = \mathbf{N}$.

2.1.6 Groupes "unilatères"

1. *Dans les axiomes d'un groupe, on remplace les existences d'un neutre et d'un inverse par celles d'un neutre à gauche et d'un inverse à gauche. En d'autres termes, on considère un magma* M *associatif muni d'un élément* 1 *et d'une application* $m \mapsto m'$ *tels que*

$$\forall m \in M, \left\{ \begin{array}{l} 1m = m \\ m'm = 1 \end{array} \right. .$$

Montrer que M *est un groupe.*

2. *Que dire lorsque* M *a un neutre à gauche et que tous ses éléments ont un inverse à droite (pour ce neutre à gauche) ?*

Solution proposée.

1. Montrons déjà que tout inverse à gauche l'est aussi à droite. On en déduira, pour chaque $m \in M$ les égalités

$$m1 = m\,(m'm) = (mm')\,m = 1m = m,$$

de sorte que 1 sera un neutre à droite, donc un neutre bilatère, donc *le* neutre.

Soit $m \in M$. Il s'agit de montrer $m'' = m$, puisqu'alors $1 = m''m' = mm'$ et m' sera inverse à droite de m comme souhaité. Or les égalités

$$m''1 = m''\,(m'm) = (m''m')\,m = 1m = m$$

permettent de travailler

$$\begin{array}{rcl} m' & = & 1m' = (m'm)\,m' = m'\,(m)\,m' = m'\,(m''1)\,m' \\ & = & m'm''\,(1m') = m'\,(m''m') = m'1, \end{array}$$

ce qui montre que 1 est neutre à droite pour tous les éléments de la forme μ', en particulier m'', d'où $m'' = m''1 = m$, *CQFD.*

[43] Pour le sens $\Longrightarrow$, on impose $m = 1$, pour le sens $\Longleftarrow$, on multiplie par m.

2. M peut très bien ne pas être un groupe. Il suffit de mettre sur n'importe quel ensemble la loi $(a,b) \mapsto b$ pour laquelle n'importe quel élément est neutre à gauche et pour laquelle un inverse à droite pour un neutre a est a lui-même. Pour éviter les pathologies, on prend un ensemble ayant au moins deux éléments. En effet, si a était un neutre tout court, alors pour chaque b on aurait $b \overset{a \text{ neutre}}{=} ba \overset{\text{définition}}{=} a$ et notre ensemble serait un singleton.

Remarque (longue). Il n'est pas inintéressant de présenter les idées qui ont menée au contre-exemple ci-dessus.

Une idée pour imposer un neutre à gauche est de considérer une structure du type aG où a est un idempotent. Pour que tous les éléments soient inversibles à droite, cela pourrait servir de prendre pour G un groupe : pour conclure, il suffirait que les inverses des éléments de G restent dans aG.

Cherchons une algèbre muni d'un tel idempotent et d'un tel groupe. Il faut chercher du non-commutatif (sinon la première question s'applique), par exemple les algèbres de matrices. La plus simple (non commutative) est M_2. Ses idempotents ? Les projecteurs, tous semblables à 0, 1 ou $a := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$; le seul non trivial est a. Un sous-groupe de $M_2^\times$? Lui-même : GL_2. L'action de a à gauche conservant la première ligne et tuant la seconde, les éléments de aGL_2 sont les matrices de la forme $\begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix}$ avec $(\alpha,\beta) \neq (0,0)$ (la matrice de départ était inversible, donc de première ligne non nulle). On regarde si aGL_2 est stable par produit :

$$\begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix} \begin{pmatrix} u & v \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \alpha u & \alpha v \\ 0 & 0 \end{pmatrix}, \text{ problème si } \alpha = 0.$$

On remplace donc GL_2 par $G := GL_2 \cap T_2^+$ de sorte à ce que le α ci-dessus soit toujours non nul, ce qui permet de conclure.

Le magma obtenu est en fait isomorphe à $K^* \times K$ muni de la loi $\binom{\alpha}{\beta} * \binom{u}{v} := \alpha\binom{u}{v}$. En remplaçant le sous-magma $K^* \hookrightarrow K$ par n'importe quels autre sous-magma $M' \hookrightarrow M$, tout fonctionne. En particulier pour $M' = \{1\}$ lorsque M est unifère, mais alors la loi devient $\binom{1}{\beta} * \binom{1}{v} := (1,v)$, ce qui revient à poser $\beta * v := v$, définition valable pour n'importe quel ensemble (non vide).

2.2 Groupes

2.2.1 Produit semi-direct 1 (motivation)

1. Soient A et B deux parties d'un monoïde $(\mathcal{M},\cdot)$. On suppose que chaque élément de $\mathcal{M}$ s'écrit comme composé d'un élément de A par un élément de B, ce de manière unique. *On dit alors que $\mathcal{M}$ est **composé direct** de A et B et on note $\mathcal{M} = A \odot B$.* Supposons de plus $\mathcal{M}$ abélien et que A et B en sont des sous-monoïdes. *Montrer alors que $A \odot B$ est isomorphe au produit*[44] $A \times B$.

   Soit G un groupe.

2. *Montrer que la loi de G est un morphisme de groupes ssi G est abélien.*
3. On admet que $\left(\binom{a}{b}, \binom{\alpha}{\beta}\right) \mapsto \binom{ab\alpha b^{-1}}{b\beta}$ muni G^2 d'une structure de groupe. *Montrer alors que la loi de G est un morphisme de groupes lorsque G^2 est muni de la loi précédente.*
4. On reprend le cadre de la question (1) mais on ne suppose plus forcément $\mathcal{M}$ abélien. *Que serait-il raisonnable de supposer sur les sous-monoïdes A et B pour que $\mathcal{M}$ soit isomorphe à $A \times B$ muni de la loi de la question 3 ?*

SOL

1. L'application $\begin{cases} A \times B & \longrightarrow & A \odot B \\ (a,b) & \longmapsto & ab \end{cases}$ est un morphisme par abélianité, surjectif par définition de $A*B$, injectif par unicité de la décomposition.

[44] On retrouve la somme directe dans les evs, monoïdes abéliens pour l'addition vectorielle.

2. Lorsque G est abélien, sa loi $\mu := \left\{ \begin{array}{ccc} G^2 & \longrightarrow & G \\ (g,\gamma) & \longmapsto & g\gamma \end{array} \right.$ est clairement un morphisme de groupes. Réciproquement, supposant μ un morphisme et fixant g, γ dans G, on a

$$(g\gamma)^2 = \left(\mu\binom{g}{\gamma}\right)^2 = \mu\left(\binom{g}{\gamma}^2\right) = \mu\binom{g^2}{\gamma^2} = g^2\gamma^2\,;$$

appliquer $g^{-1}\,\mathrm{Id}\,\gamma^{-1}$ donne $\gamma g = g\gamma$, CQFD.

3. Soient $g, g', \gamma, \gamma' \in G$. Notons $*$ la loi de l'énoncé et toujours μ celle de G. On a alors

$$\mu\left(\binom{g}{\gamma} * \binom{g'}{\gamma'}\right) = \mu\binom{g\gamma g\gamma^{-1}}{\gamma\gamma'} = g\gamma g'\gamma^{-1}\gamma\gamma' = g\gamma g'\gamma' = \mu\binom{g}{\gamma}\mu\binom{g'}{\gamma'}.$$

4. La question 3 montre que la bijection de la question 1 est un morphisme si l'on munit $A\times B$ de la loi $*$. Il suffit donc que cette dernière fasse sens, çàd d'une part (pour que le b^{-1} dans chaque composé $\binom{a}{b} * \binom{\alpha}{\beta}$ fasse sens) que B soit stable par inversion (ied soit un sous-groupe de $\mathcal{M}^\times$), d'autre part (pour que chaque composé $\binom{1}{b} * \binom{\alpha}{1}$ reste dans $A \times B$) que A soit stable par conjugaison par chaque élément de B.

2.2.2 Produit semi-direct 2 (cas général, exemple)

Soient M et N deux monoïdes (on pourrait tout faire avec des groupes). Soit $\varphi : N \longrightarrow \mathrm{End}\, M$ un morphisme de monoïdes. Pour chaque $(m,n) \in M \times N$ on abrège ${}^n m := [\varphi(n)](m)$. On définit une loi $*$ sur $M \times N$ par

$$* : \left\{ \begin{array}{ccc} (M\times N)^2 & \longrightarrow & M \times N \\ \left(\binom{m}{n}, \binom{\mu}{\nu}\right) & \mapsto & \binom{m\ {}^n\mu}{n\ \nu} \end{array} \right. .$$

1. *Montrer que $*$ munit $M\times N$ d'une structure de monoïde, notée*[45] $M \overset{\varphi}{\rtimes} N$. *Quel est son neutre ? son groupe des inversibles ? En déduire, lorsque M et N sont des groupes, que $M \overset{\varphi}{\rtimes} N$ est un groupe (et que φ induit un morphisme de groupes $N \longrightarrow \mathrm{Aut}\, M$). Retrouver les résultats de l'exercice précédent.*
2. *Donner une CNS simple pour que le monoïde $M \overset{\varphi}{\rtimes} N$*
   (a) *coïncide avec celui produit $M \times N$;*
   (b) *soit abélien.*
3. Soit $n \geq 3$ un naturel. *Montrer que le groupe diédral d'ordre $2n$ est produit semi-direct de $\mathbf{Z}/_n$ par $\mathbf{Z}/_2$.*

SOL
Soient $\binom{m}{n}$ et $\binom{\mu}{\nu}$ dans $M \times N$. Les préservations du neutre et de la loi par φ s'écrivent[46]

$${}^1 m = m \qquad \text{et} \qquad {}^n({}^\nu m) = {}^{n\nu} m.$$

De même, les préservations par le morphisme $\varphi(t)$ du neutre et de la loi se réécrivent

$${}^n 1 = 1 \qquad \text{et} \qquad {}^n(m\mu) = {}^n m\ {}^n\mu.$$

1. Montrons que $\begin{pmatrix} 1_M \\ 1_N \end{pmatrix}$ est neutre : cela vient des égalités

$$\begin{array}{rcl} \binom{1}{1} * \binom{m}{n} & = & \binom{1\ {}^1 m}{1\ n} = \binom{1\ m}{n} = \binom{m}{n} \\ \text{et } \binom{m}{n} * \binom{1}{1} & = & \binom{m\ {}^n 1}{n\ 1} = \binom{m\ 1}{n} = \binom{m}{n}. \end{array}$$

[45] *Mnémo* : la barre verticale est du côté du monoïde *agissant*
[46] attention à ne pas écrire ${}^n m\ {}^\nu m = {}^{n\nu} m$: lorsque $n = 1 = \nu$, on obtiendrait alors $m^2 = m$, forçant l'idempotence de m

Montrons l'associativité : pour chaque $\binom{\mathfrak{m}}{\mathfrak{n}} \in M \times N$, on a

$$\begin{aligned}\binom{m}{n} * \left(\binom{\mu}{\nu} * \binom{\mathfrak{m}}{\mathfrak{n}}\right) &= \binom{m}{n} * \binom{\mu\ {}^{\nu}\mathfrak{m}}{\nu\mathfrak{n}} = \binom{m\ {}^{n}(\mu\ {}^{\nu}\mathfrak{m})}{n(\nu\mathfrak{n})} = \binom{m\ {}^{n}\mu\ {}^{n}({}^{\nu}\mathfrak{m})}{n\nu\mathfrak{n}} \\ \text{et } \left(\binom{m}{n} * \binom{\mu}{\nu}\right) * \binom{\mathfrak{m}}{\mathfrak{n}} &= \binom{m\ {}^{n}\mu}{n\nu} * \binom{\mathfrak{m}}{\mathfrak{n}} = \binom{m\ {}^{n}\mu\ {}^{n\nu}\mathfrak{m}}{(n\nu)\,\mathfrak{n}} = \binom{m\ {}^{n}\mu\ {}^{n\nu}\mathfrak{m}}{n\nu\mathfrak{n}} = \binom{\|}{\|}.\end{aligned}$$

Supposons enfin $\binom{m}{n}$ et $\binom{\mu}{\nu}$ inverses l'un de l'autre. Cela s'écrit $\binom{m\ {}^{n}\mu}{n\nu} = \binom{1}{1} = \binom{\mu\ {}^{\nu}m}{\nu n}$, donc ν et n sont inverses l'un de l'autre, d'où

$$\mu\ {}^{\nu}m = 1 = {}^{\nu}1 = {}^{\nu}(m\ {}^{n}\mu) = {}^{\nu}m\ {}^{\nu n}\mu = {}^{\nu}m\ {}^{1}\mu = {}^{\nu}m\ \mu,$$

ce que montre que μ et ${}^{\nu}m$ sont inverses l'un de l'autre. Finalement, m et n sont inversibles et l'on a $\binom{m}{n}^{-1} = \binom{{}^{n^{-1}}m^{-1}}{n^{-1}}$. Réciproquement, on vérifie quand $\binom{m}{n} \in M^{\times} \times N^{\times}$ que $\binom{{}^{n^{-1}}m^{-1}}{n^{-1}}$ en est un inverse :

$$\begin{aligned}\binom{m}{n} * \binom{{}^{n^{-1}}m^{-1}}{n^{-1}} &= \binom{m\ {}^{n}\left({}^{n^{-1}}m^{-1}\right)}{n\ n^{-1}} = \binom{m\ {}^{n\ {}^{n^{-1}}}m^{-1}}{1} = \binom{m\ {}^{1}m^{-1}}{1} = \binom{m\ m^{-1}}{1} = \binom{1}{1} \\ \text{et } \binom{{}^{n^{-1}}m^{-1}}{n^{-1}} * \binom{m}{n} &= \binom{{}^{n^{-1}}m^{-1}\ {}^{n^{-1}}m}{n^{-1}\ n} = \binom{{}^{n^{-1}}\left(m^{-1}\ m\right)}{1} = \binom{{}^{n^{-1}}1}{1} = \binom{1}{1}.\end{aligned}$$

On en déduit le groupe des inversibles : $(M \times N)^{\times} = M^{\times} \times N^{\times}$.

Lorsque M et N sont des groupes, l'égalité précédente devient $(M \times N)^{\times} = M \times N$, ce qui montre que ce dernier est un groupe. Le morphisme φ ayant alors pour source un groupe, son image est incluse dans le groupe $\operatorname{Aut} M$ des inversibles de son but $\operatorname{End} M$, donc induit (par corestriction) un morphisme de groupes $N \longrightarrow \operatorname{Aut} M$. Si l'on impose de plus φ envoyant chaque $\mathfrak{n} \in N$ sur la conjugaison par $\mathfrak{n}$, on retrouve alors la loi $*$ de la question 3 de l'exercice précédent. C'est également la conjugaison des éléments de A par des éléments de B qui permet de retrouver l'isomorphisme $A \rtimes B \cong A \odot B$ de la question 4 précédente.

2.

(a) Supposons identiques les lois de $M \overset{\varphi}{\rtimes} N$ et $M \times N$. On a alors les égalités

$$\binom{m}{n} * \binom{\mu}{\nu} = \binom{m}{n}\binom{\mu}{\nu}, \text{ ied } \binom{m\ {}^{n}\mu}{n\nu} = \binom{m\mu}{n\nu}, \text{ ied } \begin{cases} m\ {}^{n}\mu = m\mu \\ n\nu = n\nu \end{cases}, \text{ ied } {}^{n}\mu = \mu\,;$$

quantifier universellement sur μ donne $\varphi(n) = \mathrm{Id}$, puis quantifier universellement sur n donne "φ constant".

Réciproqement, la loi produit est clairement un cas particulier de loi $*$ quand le morphisme φ est trivial.

(b) Supposons $M \overset{\varphi}{\rtimes} N$ abélien. On a alors $\binom{m}{n}\binom{\mu}{\nu} = \binom{\mu}{\nu}\binom{m}{n}$, ied $\begin{cases} m\ {}^{n}\mu = \mu\ {}^{\nu}m \\ n\ \nu = \nu\ n \end{cases}$. Une quantification universelle sur les ordonnées montre que N est abélien. De même pour M en abscisse après avoir imposé $n = 1 = \nu$. Par ailleurs, imposer $m = 1$ donne ${}^{\nu}m = m$, d'où la trivialité du morphisme φ.

Réciproquement, lorsque φ est trivial, le monoïde $M \rtimes N$ vaut $M \times N$ (par le point (2a)) qui est abélien ssi chacun de ses facteurs l'est. Finalement, $M \overset{\varphi}{\rtimes} N$ est abélien ssi M et N le sont et si φ est trivial.

Sanity check : la loi d'un groupe G est toujours un morphisme lorsque G^2 est muni de la loi $*$ induite par la conjugaison dans G (*cf.* question 3 précédente). Lorque G est abélien, la conjugaison y devient triviale et la loi $*$ de G^2 est celle produit : on retrouve alors le fait que la loi de G est un morphisme (question 2 précédente).

3. Reprenons la bijection bonus $\Phi := \begin{cases} \mathbf{Z}/_{n} \times \mathbf{Z}/_{2} & \xrightarrow{\sim} & D \\ \left(\overline{a}, \widetilde{b}\right) & \longmapsto & r^{a}s^{b} \end{cases}$ de la section **??**. Pour chaque naturel A, l'égalité établie $sr^{A} = r^{-A}s$ induit par récurrence l'égalité $s^{B}r^{A} = r^{(-1)^{B}A}s$ pour chaque naturel B, d'où l'on tire pour tous naturels a, b, α, β les égalités

$$\Phi\binom{\overline{a}}{\widetilde{b}}\Phi\binom{\overline{\alpha}}{\widetilde{\beta}} = \left(r^{a}s^{b}\right)\left(r^{\alpha}s^{\beta}\right) = r^{a}\left(s^{b}r^{\alpha}\right)s^{\beta} = r^{a}\ r^{(-1)^{b}\alpha}\ s^{b}\ s^{\beta} = \Phi\binom{a + (-1)^{b}\alpha}{b + \beta}.$$

On reconnaît dans le dernier argument le composé des deux premiers dans le groupe $\mathbf{Z}/_n \overset{\varphi}{\rtimes} \mathbf{Z}/_2$ pour l'action $\varphi : \left\{ \begin{array}{ccc} \mathbf{Z}/_2 & \longrightarrow & \mathrm{Aut}\, \mathbf{Z}/_n \\ \widetilde{B} & \longmapsto & (-1)^B \mathrm{Id} \end{array} \right.$ (morphisme induit par l'itération de l'opposition dans $\mathbf{Z}/_n$), ce qui conclut à l'isomorphie $\mathbf{Z}/_n \overset{\varphi}{\rtimes} \mathbf{Z}/_2 \overset{\Phi}{\cong} D$.

2.2.3 Produit semi-direct 3 (lien avec les composés directs)

Soient M et N deux monoïdes.

1. Notons $G := N^\times$ et écrivons avec des primes les images des parties de M et N par leurs plongements dans le produit cartésien $M \times N$. *Montrer alors*
   (a) *l'égalité* $M \overset{\varphi}{\rtimes} N = M' \circledast N'$;
   (b) *que* M' *est stable par conjugaison par* G' ;
   (c) *que* $M \overset{\varphi}{\rtimes} G$ *est isomorphe à* $M' \overset{\text{conj.}}{\rtimes} G'$.

   Commenter.
2. *Soit réciproquement* $(\mathcal{M}, \cdot)$ *un monoïde de la forme* $M \odot G$ *où* G *est un sous-groupe de* $\mathcal{M}^\times$ *et où* M *est un sous-monoïde de* $\mathcal{M}$ *stable par conjugaison par* G. *Montrer que* $\mathcal{M}$ *est isomorphe à* $M \overset{\text{conj.}}{\rtimes} G$. *Commenter.*

SOL

1.
   (a) Vu pour chaque $\binom{m}{n} \in M \times N$ l'égalité $\binom{m}{1} * \binom{1}{n} = \binom{m\ {}^1 1}{1n} = \binom{m}{n}$, le composé "parties" $M' * N'$ vaut tout le produit $M \overset{\varphi}{\rtimes} N$. Les égalités précédentes montrant par ailleurs l'unicité de la décomposition, ce composé est direct[47].

   (b) Pour chaque $(m, g) \in M \times G$, le conjugué de m' par g' est

$$\begin{array}{rcl} \left(\binom{1}{g} * \binom{m}{1} \right) * \binom{1}{g}^{-1} & = & \binom{1\ {}^g m}{g\ 1} * \binom{{}^{g^{-1}}1^{-1}}{g^{-1}} = \binom{{}^g m}{g} * \binom{1}{g^{-1}} \\ & = & \binom{{}^g m\ {}^g 1}{g\ g^{-1}} = \binom{{}^g m}{1}, \text{ qui reste dans } M'. \end{array}$$

   Le calcul précis des abscisses était inutile pour établir la stabilité désirée mais révèle plus, à savoir les égalités ${}^{g'}m' = ({}^g m)'$ où la première action est celle par conjugaison, identités qui nous serviront.

   (c) La stabilité cherchée donne sens au produit semi-direct $M' \overset{\text{conj.}}{\rtimes} G'$ (dont on notera $*'$ la loi) où G' agit sur M' par conjugaison. Montrons alors que la bijection $\Phi := \left\{ \begin{array}{ccc} M \overset{\varphi}{\rtimes} G & \widetilde{\longrightarrow} & M' \overset{\text{conj.}}{\rtimes} G' \\ (m, g) & \longmapsto & (m', g') \end{array} \right.$ est un morphisme. Soient $m, \mu \in M^2$ et $g, \gamma \in G^2$. Il est utile de vérifier l'égalité[48] $(ab)' = a' * b'$ pour chaque $(a, b) \in M^2 \cup G^2$. On a alors

$$\begin{array}{rcl} \text{d'une part } \Phi\left(\binom{m}{g} * \binom{\mu}{\gamma} \right) & = & \Phi \binom{m\ {}^g\mu}{g\ \gamma} = \binom{(m\ {}^g\mu)'}{(g\ \gamma)'} = \binom{m'\ ({}^g\mu)'}{g'\ \gamma'} \\ \text{d'autre part } \Phi\binom{m}{g} *' \Phi\binom{\mu}{\gamma} & = & \binom{m'}{g'} *' \binom{\mu'}{\gamma'} = \binom{m'\ {}^{g'}\mu'}{g'\ \gamma'} ==== {}^{\text{''}}. \end{array}$$

Commentaire : le cas motivant de l'exercice précédent ("tordre" la loi d'un groupe à l'aide des conjugaisons afin de la transformer en un morphisme) est *générique* au sens où, aux primes près, on peut toujours supposer que le morphisme φ est donné par les *conjugaisons*.

[47] Lorsque φ est trivial, on retrouve l'égalité $M \times N = M' \odot N'$ (où le $\cdot$ dénote la loi produit).

[48] En d'autres termes, les deux bijections $\begin{array}{c} M \cong M' \\ G \cong G' \end{array}$ sont des isomorphismes de monoïdes pour la loi $*$ à l'arrivée.

2. L'application $\Psi := \left\{ \begin{array}{ccc} M \overset{\text{conj}}{\rtimes} G & \longrightarrow & \mathcal{M} \\ (m,g) & \longmapsto & mg \end{array} \right.$ est bijective puisque $\mathcal{M} = M \odot G$ et est un morphisme d'après un calcul déjà effectué à la question 3 de l'exercice précédent. Lorsque $\mathcal{M}$ est abélien, on retrouve les résultats du volet *motivations*.

Commentaire : la notion de produit semi-direct n'est pas plus compliquée que celle de composé direct (avec une bonne hypothèse de stabilité par conjugaison).

2.2.4 Produit semi-direct 4 (reverse mathematics)

Soient M et N deux magmas. Soit $\varphi : N \longrightarrow M^M$. On garde les même notations exponentielles pour l'action de N qu'à l'exercice précédent.

1. *Montrer que $M \rtimes N$ est associatif ssi N est associatif et si*
$$\begin{array}{c} \forall m, \mu, \mathfrak{m} \in M \\ \forall n, \nu \in N \end{array} \ , \ m\,{}^{n}(\mu\,{}^{\nu}\mathfrak{m}) = (m\,{}^{n}\mu)\ {}^{n\nu}\mathfrak{m}.$$
2. *Montrer que $M \rtimes N$ est unifère ssi N est unifère et si M contient un u tel que*
$$\forall m \in M,\ u\,{}^{1}m = m = m\,{}^{n}u.$$
3. On suppose ici que N et M sont des monoïdes resp. trivial et muni d'un élément i tel que $\forall m \in M,\ {}^{1}m = im$. *Montrer alors que $M \rtimes N$ est un monoïde ssi i est inversible mais qu'alors on n'a pas forcément $1_{M\rtimes N} = (1_M, 1_N)$.*
4. On suppose que la loi $*$ munit le produit $M \times N$ d'une structure de monoïde dont le neutre est de la forme $(1_M, ?)$. *Montrer que M et N sont des monoïdes et que φ est un morphisme $N \longrightarrow \operatorname{End} M$ de monoïdes*

Solution proposée.

1. Calcul.
2. Calcul, u étant l'abscisse du neutre de $M \rtimes N$.
3. On a toujours l'associativité, le composé de trois éléments s'écrivant
$$\binom{m}{1}\binom{\mu}{1}\binom{\mathfrak{m}}{1} = \binom{m\ i\ \mu\ i\ \mathfrak{m}}{1}.$$
Trivialiser N revient en fait à se placer dans le cadre de l'exercice *Déformations de la loi d'un monoïde* dont on reprendra la démonstration de l'équivalence souhaitée. Dans le cas où i est inversible, le neutre de $M \rtimes N$ est $\left(i^{-1}, 1\right)$ et, dès que $M^\times$ n'est pas trivial, on peut imposer $i \neq 1$ pour éviter l'égalité $1_{M\rtimes N} = (1_M, 1_N)$.
4. Soient $m, \mu, \mathfrak{m} \in M$ et $n, \nu, \mathfrak{n} \in N$. Le caractère unifère se réécrit ${}^{1}m = m = m\,{}^{n}1$, imposer $m = 1$ donne ${}^{n}1 = 1$. Dans l'égalité $m\,{}^{n}(\mu\,{}^{\nu}\mathfrak{m}) = (m\,{}^{n}\mu)\ {}^{n\nu}\mathfrak{m}$, imposer $n = 1 = \nu$ donne l'associativité de M, puis imposer $m = 1 = \mu$ donne ${}^{n}({}^{\nu}\mathfrak{m}) = {}^{n\nu}\mathfrak{m}$, puis imposer $\binom{m}{n} = \binom{1}{1}$ donne ${}^{n}(\mu\ \mathfrak{m}) = {}^{n}\mu\,{}^{n}\mathfrak{m}$. Le lecteur est invité à quantifier universellement là où il le faudrait.

2.3 Sous-groupes

2.3.1 Commutant

Soit G un groupe. Soit $A \subset G$. *Montrer l'inclusion*
$$A \subset \operatorname{Comm}(\operatorname{Comm}(A)) \ \textit{avec égalité ssi } A \textit{ est de la forme } \operatorname{Comm}(B).$$

SOL Abrégeons $C := \operatorname{Comm}$. Montrons $A \subset \operatorname{Comm} C(A)$. Soit $a \in A$. Soit $c \in C(A)$. Par définition de $C(A)$, on a $ac = ca$, ce qui montre que a commute avec tous les éléments de $C(A)$, donc appartient à $\operatorname{Comm} C(A)$, d'où l'inclusion annoncée.

S'il y a égalité, alors A est bien de la forme $C(B)$ voulue en posant $B := C(A)$.

Supposons réciproquement que A est de la forme $C(B)$ pour une certaine partie $B \subset G$. Le point précédent $\forall P \subset G,\ P \subset CC(P)$ montre, en remplaçant P par B puis par $C(B)$, les inclusions $B \subset CC(B)$ et $C(B) \subset CCC(B)$ or la décroissance de Comm appliquée à la première inclusion donne $CCC(B) \subset C(B)$, d'où l'égalité $A = C(B) = CCC(B) = CC(A)$.

2.3.2 Composé de sous-groupes

Soit G un groupe. Soient A et B deux sous-groupes de G.

1. *Montrer que AB est un sous-groupe ssi $AB = BA$.*
2. On suppose $G = GL_2\left(\mathbb{Z}/n\right)$ où n est un entier impair et que A et B sont engendrés respectivement par les matrices $a := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $b := \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. *Montrer $\forall p, q \in \mathbb{N},\ a^p b^q = b^q \left(a^p\right)^{2^q}$. En déduire $ab \neq ba$ et $AB = BA$.*
3. *La condition $AB = BA$ équivaut-elle à $\forall\, (a, b) \in A \times B,\ ab = ba$?*

Démonstration

1. Supposons $AB = BA$. On a alors $(AB)(AB) = A(BA)B = A(AB)B = (AA)(BB) = AB$, ce qui montre que AB est stable par produit. De même, on a $(AB)^{-1} = B^{-1}A^{-1} = BA = AB$, ce qui montre la stabilité par inversion. Enfin, la partie AB contient toujours $1 = 1 \cdot 1$.

   Supposons que AB est un sous-groupe. Soit $(a, b) \in A \times B$. Alors le produit $ba = (1b)(a1)$ reste dans AB, ce qui montre l'inclusion $BA \subset AB$. Réciproquement, l'inverse de ab reste dans AB, mettons $(ab)^{-1} = \alpha\beta$ pour un $(\alpha, \beta) \in A \times B$, d'où $ab = \beta^{-1}\alpha^{-1} \in BA$, ce qui montre l'inclusion $AB \subset BA$.
2. Observer que la matrice b est inversible puisque le coefficient diagonal 2, étant premier avec n, est inversible *modulo* n. On a plus précisément $b^{\varphi(n)} = 1$ (vu que $2^{\varphi(n)} = 1$) et par ailleurs l'égalité $a^n = 1$. Ainsi a et b sont-ils d'ordre fini, mettons $\binom{\alpha}{\beta} := \binom{\omega(a)}{\omega(b)}$, et l'on pourra décrire au besoin $BA = \left\{b^\ell a^k\right\}_{0 \leq k < \alpha}^{0 \leq \ell < \beta} = \left\{b^\ell a^k\ ;\ k, \ell \in \mathbb{N}\right\}$.

   Deux récurrences immédiates montreraient pour chaque naturel n les égalités $a^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ et $b^n = \begin{pmatrix} 1 & 0 \\ 0 & 2^n \end{pmatrix}$. On en déduit à $p, q \in \mathbb{N}$ fixés les égalités

$$\begin{aligned} a^p b^q &= \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2^q \end{pmatrix} = \begin{pmatrix} 1 & p2^q \\ 0 & 2^q \end{pmatrix} \text{ et} \\ b^q \left(a^p\right)^{2^q} &= \begin{pmatrix} 1 & 0 \\ 0 & 2^q \end{pmatrix}\begin{pmatrix} 1 & p2^q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & p2^q \\ 0 & 2^q \end{pmatrix}, \end{aligned}$$

   ce qui montre que BA est stable par produit (écrire $b^\Diamond a^p b^q a^\triangle = b^{\Diamond+q} a^{p2^q+\triangle}$) et que $ab = ba^2 \neq ba$. Montrons que BA est stable par inverse, ce qui conclura à $AB = BA$ d'après la question suivante (BA contient trivialement $1 = b^0 a^0$). Nous savons a et b d'ordres finis α et β, d'où l'on déduit pour tous p et q naturels

$$(b^q a^p)^{-1} = 1a^{-p}1b^{-q} = a^{p\alpha}a^{-p}b^{q\beta}b^{-q} = a^{p(\alpha-1)}b^{q(\beta-1)} = b^{q(\beta-1)}\left(a^{p(\alpha-1)}\right)^{2^{q(\beta-1)}} \in BA.$$

3. La question précédente[49] fournit un contre-exemple.

2.3.3 Sous-groupes de type fini

On dit qu'une structure est ***de type fini*** lorsqu'elle admet une partie génératrice finie. Par exemple, un espace vectoriel est de type fini ssi il est de dimension finie. Nous voulons montrer (contrairement au cas des espaces vectoriels) qu'un sous-groupe d'un groupe de type fini n'est pas forcément de type fini.

Notons d et t resp. la matrice diagonale $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et la transvection $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Définissons $G := \langle d, t\rangle$. *Montrer que les produits $d^p t^q d^{-p}$ pour p et q parcourant les relatitfs engendrent un sous-groupe de G isomorphe à $\mathbb{Z}\left[\frac{1}{2}\right]$. Conclure.*

SOL

[49] On aurait pu simplifier ce contre-exemple en se plaçant dans $\mathbb{Z}/3$, il aurait alors été facile d'expliciter les six éléments de AB et de BA. Nous souhaitions montrer le caractère générique des contre-exemples où A et B sont cycliques et dont des générateurs a et b respectifs vérifient $ab = ba^2$ (cette dernière égalité étant l'idée la plus simple à imaginer, avec $ab = b^2 a$, pour imposer $ab \in BA \setminus \{ba\}$).

Il est aisé d'expliciter pour chaque $(p,q) \in \mathbb{Z}^2$ le produit

$$\begin{aligned} d^p t^q d^{-p} &= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^p \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^q \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-p} = \begin{pmatrix} 2^p & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2^{-p} & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2^p & 2^p q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2^{-p} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2^p q \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Le sous-groupe S considéré est donc inclus dans les matrices de la forme $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ pour a rationnel, d'où un plongement $\varphi := \left\{ \begin{array}{ccc} (S,\times) & \hookrightarrow & (\mathbb{Q},+) \\ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} & \longmapsto & a \end{array} \right.$ identifiant S à son image directe

$$\varphi(S) = \varphi\left(\left\langle d^p t^q d^{-p} \right\rangle_{p,q\in\mathbb{Z}}\right) = \left\langle\ \varphi\left(d^p t^q d^{-p}\right)\ \right\rangle_{p,q\in\mathbb{Z}} = \left\langle\ 2^p q\ \right\rangle_{p,q\in\mathbb{Z}} = \mathbb{Z}\left[\frac{1}{2}\right].$$

Or ce dernier n'est pas de type fini (considérer la plus petite valuation 2-adique : elle vaut $-\infty$ pour $\mathbb{Z}\left[\frac{1}{2}\right]$ mais est finie pour chacun de ses sous-groupes de type fini), donc G (qui est de type fini car bigène) contient un sous-groupe qui n'est pas de type fini.

2.4 Morphismes

2.4.1 Variations du cours

On reprend les trois points définissant un morphisme de groupes (début section **??**). *Est-ce que les points (2) et (3) impliquent conjointement celui (1) ? Et si l'on rajoute la bijectivité de l'application concernée ?*

SOL
Plaçons nous dans le groupe $\mathbb{Z}$, dont nous connaissont les endomorphismes (les homothéties). La conjonction des points (2) et (3) équivalant à l'imparité de la fonction concernée, on voit mal comment forcer une fonction impaire à être linéaire, même si elle est bijective. N'importe quelle permutation de $\mathbb{N}^*$ autre que l'identité (par exemple l'involution $(1,2)\,(3,4)\,(5,6)\cdots$) engendre un contre-exemple (imposer 0 en 0 puis symétriser le graphe par rapport à l'origine).

2.4.2 Compatibilité du produit cartésien avec "être isomorphe à"

Soient $\alpha : A \xrightarrow{\sim} A'$ et $\beta : B \xrightarrow{\sim} B'$ deux isomorphismes de groupes. *Montrer que que les groupes produit $A\times B$ et $A'\times B'$ sont isomorphes.* **Bonus sagittal** *: montrer l'unicité de l'isomorphisme si l'on exige la commutativité du diagramme* $\begin{array}{ccccc} A & \hookrightarrow & A\times B & \hookleftarrow & B \\ \alpha\downarrow\simeq & & \downarrow? & & \beta\downarrow\simeq \\ A' & \hookrightarrow & A'\times B' & \hookleftarrow & B' \end{array}$.

2.4.3 Commutativité et associativité du produit de groupes

Soient trois groupes A, B, C.
Montrer que les produits $A\times B$ et $B\times A$ sont isomorphes. **Bonus sagittal** *: montrer l'unicité de l'isomorphisme si l'on exige la commutativité du diagramme* $\begin{array}{ccccc} & & \hookrightarrow & A\times B & \hookleftarrow & \\ A & & & \downarrow? & & B \\ & & \hookrightarrow & B\times A & \hookleftarrow & \end{array}$.

Montrer que les produits $A\times(B\times C)$ et $(A\times B)\times C$ sont isomorphes. **Bonus sagittal** *: montrer l'unicité de l'isomorphisme si l'on exige la commutativité du diagramme*

$$\begin{array}{ccccccc} & \hookrightarrow & A\times(B\times C) & \hookleftarrow & A & \hookrightarrow & \\ & \uparrow & & & & \downarrow & \\ B\times C & & \hookleftarrow & B & \hookrightarrow & A\times B & \\ & \uparrow & & & & \downarrow & \\ & \hookleftarrow & C & \hookrightarrow & (A\times B)\times C & \hookleftarrow & \end{array}$$

(où le morphisme $A\times(B\times C)\overset{?}{\longrightarrow}(A\times B)\times C$ n'a pas été précisé par commodité de lecture).

2.4.4 ce qui ne marche pas avec les monoïdes

Un morphisme de monoïdes est-il injectif ssi son noyau est neutre ?
Un morphisme de monoïdes induit-il un isomorphisme de monoïdes en quotientant par le noyau ?

SOL

La réponse à ces deux questions est *non*. Pour éviter les groupes (où le cours nous répond "oui"), cherchons des idempotents non trivaux, par exemple dans un ev un projecteur autre que l'identité.

Soit i un tel idempotent. Alors son itération $\left\{\begin{array}{ccc}\mathbf{N} & \twoheadrightarrow & \{1,i\}\\ n & \longmapsto & i^n\end{array}\right.$ est un morphisme de monoïdes non injectif (sa source est infinie et son but est fini) et de noyau neutre (vu les égalités $\forall n\in\mathbf{N}^*,\ i^n=i\neq 1$).

Quotienter par ce noyau redonne un monoïde isomorphe à $\mathbf{N}$, donc infini, qui ne saurait par conséquent être équipotent (*a fortiori* isomorphe) au monoïde fini $\{1,i\}$.

2.4.5 Une condition suffisante d'involutivité

Soit un endomorphisme d'un groupe fini qui inverse strictement plus de la moitié des éléments de ce dernier. *Montrer l'involutivité de ce morphisme.*

SOL

Appelons G et φ resp. le groupe et l'endomorphisme de l'énoncé. Notons $I:=\left\{i\in G\ ;\ \varphi(i)=i^{-1}\right\}$ la partie des éléments **i**nversés par φ et $D:=\left\{g\in G\ ;\ \varphi^2(g)\neq g\right\}$ celle qui mesure le **d**éfaut d'involutivité de φ. On veut montrer l'implication $|I|>\frac{|G|}{2}\Longrightarrow D=\emptyset$. Raisonnons par contraposée et supposons D non vide.

Il convient déjà de remarquer que $\varphi_{|I}$ est une involution : en effet, pour chaque $i\in I$, on a

$$\varphi^2(i)=\varphi(\varphi(i))=\varphi\left(i^{-1}\right)=\varphi(i)^{-1}=\left(i^{-1}\right)^{-1}=i.$$

Il s'ensuit que D ne saurait rencontrer I. Par ailleurs, D est stable par translation par les éléments de I vu les implications (à $d,i\in G$ fixés)

$$\left.\begin{array}{c}d\in D\\ i\in I\end{array}\right\}\implies\varphi^2(di)=\varphi^2(d)\,\varphi^2(i)=\varphi^2(d)\,i\neq di\implies di\in D.$$

On en déduit l'inclusion $DI\subset D$. La partie DI est donc disjointe de I, ce qui donne (en passant aux cardinaux) la comparaison $|DI|\leq|G|-|I|$.

Par ailleurs, D est non vide par hypothèse, donc contient au moins un élément, mettons d ; la partie DI contient alors dI qui est de cardinal $|I|$, d'où l'inégalité $|DI|\geq|I|$.

Combiner les deux comparaisons ci-dessus donne $|I|\leq|G|-|I|$, *i. e.* $|I|\leq\frac{|G|}{2}$, *CQFD.*

Remarque. On aura bien sûr pris garde à ne pas dire que la partie I est un sous-groupe de G. Elle contient bien le neutre et est stable par passage à l'inverse, mais n'a aucune raison d'être stable par produit si G n'est pas abélien.

2.4.6 Caractères 1 (prolongement et séparation)

Pour chaque magma M, on appelle ***caractère*** de M tout morphisme de M vers $\mathbb{C}^*$ et on note $\widehat{M}$ leur ensemble, appelé ***dual*** de M.

1. *Calculer le dual d'un groupe monogène.*
   Soit G un groupe abélien fini
2. **Montrer que chaque caractère défini sur un sous-groupe de G se prolonge en un caractère de G.*
3. *En déduire que les caractères de G séparent ses éléments, au sens où il existe pour tous $g \neq h$ dans G un caractère χ tel que $\chi(g) \neq \chi(h)$.*

SOL

1. (en substance déjà fait en exercice de cours section **??**) Soit n un naturel. Un morphisme de source ${}^{\mathbb{Z}}\!/_{n} = \langle \overline{1} \rangle$ est entièrement déterminé par l'image du générateur $\overline{1}$; or, ce dernier devenant le neutre après n itérations, son image également, donc cette image tombe dans $\mathbb{U}_n$. Réciproquement, l'itération $z \mapsto u^z$ de n'importe quel élément $u \in \mathbb{U}_n$ a un noyau contenant $\mathbb{Z}n$, donc induit au quotient par $\mathbb{Z}n$ un caractère de ${}^{\mathbb{Z}}\!/_{n}$. Cette correspondance étant bijective, on peut conclure $\widehat{{}^{\mathbb{Z}}\!/_{n}} = \mathbb{U}_n$. (Lorsque n est nul, on obtient $\widehat{\mathbb{Z}} = \mathbb{C}^*$.)
2. Soient S un sous-groupe et χ un caractère de S. Essayons de prolonger χ petit à petit, en rajoutant à S un élément a qui n'est pas dans S. Si l'on y parvient, il suffira de répéter l'opération tant que le groupe $\langle S, a \rangle$ ne vaudra pas G tout entier, procédé qui est assuré de terminer étant donnée la finitude de G.

   On veut prolonger χ à $\langle S, a \rangle$; on a envie de définir

   $$X := sa^z \mapsto \chi(s)\,\chi(a)^z$$

   mais $\chi(a)$ n'a aucun sens. Cependant, il y a une puissance de a qui tombe dans S : considérer l'ordre n de la classe de a dans ${}^{G}\!/_{S}$. Ainsi, $\chi(a^n)$ a un sens, et puisqu'on doit avoir $X(a^n) = X(a)^n$, le complexe $X(a)$ doit être défini comme une racine n-ième de $X(a^n) = \chi(a^n)$. Il faut donc définir

   $$X := sa^z \mapsto \chi(s)\,\alpha^z.$$

   où α est une telle racine. Sous cette forme, il est clair que X est un morphisme qui prolonge χ mais rien ne garantit encore que cette "définition" en soit une.

   Pour que X soit bien défini, il s'agit de montrer les implications (à $(s, z) \in S \times \mathbb{Z}$ fixé)

   $$sa^z = 1 \implies \chi(s)\,\alpha^z = 1.$$

   En effet, si l'on a deux écritures $sa^z = s'a^{z'}$ d'un même élément de $\langle S, a \rangle$, l'implication précédente donne successivement

   $$s's^{-1}a^{z'-z} = 1 \implies \chi\left(s's^{-1}\right)\alpha^{z'-z} = 1 \underset{\text{morphisme}}{\overset{\chi \text{ est un}}{\implies}} \chi(s')\,\alpha^{z'} = \chi(s)\,\alpha^z.$$

   Partant de $sa^z = 1$, la puissance $a^z = s^{-1}$ est dans S, donc z est un multiple de l'ordre de a dans ${}^{G}\!/_{S}$ (*i. e.* n), mettons $z = nd$, ce qui donne $1 = s\ (a^n)^d$. On peut alors appliquer χ vu que tout le monde est dans S :

   $$1 = \chi(s)\ \chi(a^n)^d = \chi(s)\ (\alpha^n)^d = \chi(s)\ \alpha^z,\ \textit{CQFD.}$$

   RQ – Si G n'est pas supposé fini, les résultats restent valable en appliquant le lemme de Zorn[50].
3. Soit $g \neq 1$ dans G dont note n l'ordre. Le sous-groupe $\langle g \rangle$ est isomorphe à $\mathbb{U}_n$, d'où un caractère de $\langle g \rangle$ séparant 1 et g (d'images respectives 1 et $e^{\frac{2\pi i}{n}}$ distinctes car $n > 1$). Alors chaque caractère prolongeant ce dernier sépare g et 1.

   Soient $g \neq h$ dans G. Soit χ un caractère de G séparant gh^{-1} et 1. Cela s'écrit $1 \neq \chi\left(gh^{-1}\right) = \chi(g)\,\chi(h)^{-1}$, *i. e.* $\chi(h) \neq \chi(g)$, ce qui conclut.

[50] Considérons l'ensemble X des caractères prolongeant χ qui sont définis sur un sous-groupe de G. On ordonne X par l'inclusion des ensembles de définition. Alors toute chaîne de X admet un majorant (prendre la réunions des sous-groupes de définition, c'est encore un sous-groupe car chacun est inclus dans ou contient l'autre), donc X admet un élément maximal χ défini sur un sous-groupe S. Si $S \neq G$, la solution ci-dessus ci-dessus montre que l'on peut prolonger strictement χ, contredisant son caractère maximal.

2.4.7 Caractères 2 (orthogonalité, bidual)

Soit G un groupe abélien fini.

1. *Montrer les égalités*[51]

$$\forall g \in G,\ \frac{1}{\left|\widehat{G}\right|}\sum_{\chi\in\widehat{G}}\chi(g)=\delta_g^1 \qquad \text{et} \qquad \forall \chi \in \widehat{G},\ \frac{1}{|G|}\sum_{g\in G}\chi(g)=\delta_\chi^1$$

En déduire que $\widehat{G}$ et G ont même ordre.

2. *Montrer que G est isomorphe à son bidual $\widehat{\widehat{G}}$.*
3. *Déterminer les caractères continus de $\mathbb{U}$,* i. e. *les morphismes de groupes continus 2π-périodiques de $\mathbb{R}$ vers $\mathbb{C}^*$.* (On pourra utiliser le théorème de Stone-Weierstrass.)

Démonstration

1. Soit $\chi \in \widehat{G}$. Observer à $h \in G$ l'invariance de la somme $\sum_{g\in G}\chi(g)$ après multiplication par $\chi(h)$:

$$\chi(h)\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(h)\chi(g)\overset{\chi \text{ est un}}{\underset{\text{caractère}}{=}}\sum_{g\in G}\chi(hg)\overset{\text{reparamétrage}}{\underset{\gamma:=hg}{=}}\sum_{\gamma\in hG}\chi(\gamma)\overset{G=hG}{=}\sum_{\gamma\in G}\chi(\gamma).$$

Cette somme sera donc nulle si l'on peut trouver un h tel que $\chi(h)\neq 1$, *i. e.* si $\chi\neq 1$. Dans le cas contraire, chaque $\chi(g)$ de la sommande vaut 1 et la somme étudiée vaut $\frac{1}{|G|}\sum_{g\in G}1=\frac{1}{|G|}|G|=1$. Dans les deux cas, on trouve δ_χ^1.

Soit $g \in G$. L'évaluation en g est un caractère de $\widehat{G}$: on peut donc appliquer l'égalité précédente en remplaçant (G,χ) par $\left(\widehat{G},\mathrm{eval}_g\right)$, ce qui donne

$$\frac{1}{\left|\widehat{G}\right|}\sum_{\chi\in\widehat{G}}\chi(g)=\frac{1}{\left|\widehat{G}\right|}\sum_{\chi\in\widehat{G}}\mathrm{eval}_g(\chi)=\delta_1^{\mathrm{eval}_g};$$

or eval_g vaut constamment 1 si $g=1$ et réciproquement (si $g\neq 1$, il y a un caractère séparant g et 1 par l'exercice précédent), ce qui s'écrit $\delta_1^{\mathrm{eval}_g}=\delta_1^g$.

La somme $\sum_{(g,\chi)\in G\times\widehat{G}}\chi(g)$ vaut alors

$$\begin{aligned}\text{d'une part}\ \sum_{g\in G}\sum_{\chi\in\widehat{G}}\chi(g) &= \sum_{g\in G}\left|\widehat{G}\right|\delta_1^g=\left|\widehat{G}\right|\sum_{g\in G}\delta_1^g=\left|\widehat{G}\right|,\\ \text{d'autre part}\ \sum_{\chi\in\widehat{G}}\sum_{g\in G}\chi(g) &= \sum_{\chi\in\widehat{G}}|G|\,\delta_1^\chi=|G|\sum_{\chi\in\widehat{G}}\delta_1^\chi=|G|,\ \text{ce qui conclut}\end{aligned}$$

2. L'évaluation $g\mapsto \mathrm{eval}_g$ est un morphisme de G vers son bidual, injectif par séparation (*cf.* les égalités $\delta_1^{\mathrm{eval}_g}=\delta_1^g$), donc bijectif par égalité des cardinaux.
3. Est un caractère (continu) la fonction $t\mapsto e^{it}$, *a fortiori* chacun de ses itérés pour la multiplication complexe, à savoir chaque $e_z := t\mapsto e^{zit}$ lorsque z décrit $\mathbb{Z}$. Montrons la réciproque.

Soit χ un caractère continu. Essayons de montrer que χ est un e_z, *i. e.* qu'un caractère $\frac{\chi}{e_z}$ vaut 1. Le point (1) incite à regarder la "somme" $\sum_{t\in\ \mathbb{R}/\mathbb{Z}}\frac{\chi}{e_z}(t)$ (insensée) dont l'analogue faisant sens est l'intégrale $\int\frac{\chi}{e_z}$ sur n'importe segment de longueur 2π. Il était pertinent dans le cas fini de multiplier cette somme par une valeur fixée : calquons. Pour chaque $(z,r)\in\mathbb{Z}\times\mathbb{R}$, l'intégrale $\int_{-\pi}^{\pi}\frac{\chi}{e_z}$ est inchangée après multiplication par $\frac{\chi}{e_z}(r)$ (reparamétrer en translatant de r), ce qui montre ou bien que chacune de ces intégrales est nulle, ou bien qu'il y a un relatif z pour lequel le facteur $\frac{\chi}{e_z}(r)$ vaut constamment 1 (ce qui conclurait). Dans le premier cas[52], intégrer χ contre n'importe quel polynôme en $e_{\pm 1}$ donne zéro ; or le théorème de Stone-Weierstrass affirme que χ est la limite uniforme d'une suite (P_n) de tels polynômes. La nullité de $\int\chi\overline{P_n}$ se propage alors à la limite et donne celle de $\int\chi\overline{\chi}=\int|\chi|^2$, *i. e.* celle absurde de χ qui ne peut plus atteindre 1.

[51] *Rappel* : le ***symbole de Kronecker*** δ_a^b vaut (le nombre) 1 quand a et b sont égaux et est nul sinon.

[52] En termes hermitiens, on dirait que χ est orthogonal aux e_z, donc à l'adhérence de leur Vect, laquelle contient χ d'après Stone-Weierstrass, d'où la nullité de χ qui se retrouve orthogonal à lui-même.

Remarque. En munissant $\mathbb{C}^G$ et $\mathbb{C}^{\widehat{G}}$ de produits hermitiens de la forme $(a,b) \mapsto \frac{1}{|G|}\sum_s \overline{a_s} b_s$ (où s parcourt la source G ou $\widehat{G}$), le point (1) se reformule en termes hermitiens : *les caractères resp. de G et de $\widehat{G}$ forment une base orthonormée resp. de $\mathbb{C}^G$ et $\mathbb{C}^{\widehat{G}}$.*

2.4.8 Caractères 3 (théorie de Fourier discrète)

Pour chaque monoïde abélien fini M, on définit sur $\mathbb{C}^M$ un ***produit de convolution*** $*$ par

$$(a,b) \overset{*}{\mapsto} \left(\sum_{xy=m} a_x b_y\right)_{m\in M} : m \mapsto \sum_{\mu\in M} a_\mu b_{\frac{m}{\mu}}.$$

Soit G un groupe abélien fini. *Montrer qu'est un isomorphisme d'algèbres abéliennes la correspondance*

$$\begin{cases} \mathbb{C}^G \text{ (pour } * \text{)} & \cong & \mathbb{C}^{\widehat{G}} \text{ (pour } \times_{\mathbb{C}} \text{)} \\ a & \longmapsto & \left(\sum_{g\in G} \overline{a_g}\chi_g\right)_{\chi\in\widehat{G}} \\ \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \overline{\alpha_\chi}\chi & \longleftarrow & \alpha \end{cases}.$$

SOL

Montrons déjà que l'ev $\mathbb{C}^G$ est une algèbre abélienne pour $*$ (c'est clair pour $\mathbb{C}^{\widehat{G}}$ munie de la multiplication $\times_{\mathbb{C}}$ produit) La bilinéarité de $*$ est claire et va permettre de montrer ses abélianité et associativité en ne regardant que les Dirac δ_g pour g décrivant G. Soient $g,h,i,\gamma \in G$. On a alors[53]

$$[\delta_g * \delta_h](\gamma) = \sum_{x\in G} \delta_g^x \delta_x^{\frac{\gamma}{h}} = \delta_h^{\frac{\gamma}{g}} = \delta_{gh}^{\gamma}, \text{ d'où } \delta_g * \delta_h = \delta_{gh},$$

ce qui montre d'une part la neutralité du Dirac en le neutre de G, d'autre part l'abélianité de $*$ vu celle de G, d'où découle l'associativité :

$$(\delta_g * \delta_h) * \delta_i = \delta_{gh} * \delta_i = \delta_{(gh)i} = \delta_{i(gh)} \overset{\text{même}}{\underset{\text{calcul}}{=}} \delta_i * (\delta_g * \delta_h) \overset{* \text{ abélien}}{=} (\delta_g * \delta_h) * \delta_i.$$

On retiendra l'écriture plus "symétrique" du composé d'une famille :

$$a * b * c * \cdots * z = \left(\sum_{\mathfrak{a}\mathfrak{b}\mathfrak{c}\cdots\mathfrak{z}=\gamma} a_{\mathfrak{a}} b_{\mathfrak{b}} c_{\mathfrak{c}} \cdots z_{\mathfrak{z}}\right)_{\gamma\in G}.$$

Montrons à présent que la correspondance de l'énoncé (qui fait sens) est bijective. Notons resp. $\mathcal{F}$ (comme "**F**ourier") et $\mathcal{G}$ les applications $\longrightarrow$ et $\longleftarrow$. Ces dernières étant linéaires, il suffira d'évaluer $\mathcal{G}\circ\mathcal{F}$ et $\mathcal{F}\circ\mathcal{G}$ sur des vecteurs de bases de $\mathbb{C}^G$ et $\mathbb{C}^{\widehat{G}}$ resp., par exemples les Dirac. On utilisera les deux identités établies à l'exercice précédent concernant les moyennes des $\chi(g)$. On observera également, pour chaque $(g,\chi) \in G\times\widehat{G}$, que $\chi(g)$ est *unitaire* (car devenant 1 après $|G|$ itérations), ce qui permet de réécrire son conjugué $\overline{\chi(g)} = \chi(g)^{-1} = \chi\left(g^{-1}\right)$. On a alors pour chaque $g \in G$ les égalités

$$\delta_g \overset{\mathcal{F}}{\mapsto} \left(\sum_{\gamma\in G} \overline{\delta_g^\gamma}\chi_\gamma\right)_{\chi\in\widehat{G}} = \left(\chi_g\right)_\chi \overset{\mathcal{G}}{\mapsto} \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \overline{\chi_g}\chi = \left(\frac{1}{|G|}\sum_{\chi\in\widehat{G}} \chi\left(\frac{\gamma}{g}\right)\right)_{\gamma\in G}$$

$$\text{(noter au passage l'identité } \mathcal{F}(\delta_g) = \text{eval}_g \text{)} \quad = \quad \left(\delta^1_{\frac{\gamma}{g}}\right)_{\gamma\in G} = \left(\delta_g^\gamma\right)_{\gamma\in G} = \delta_g$$

et pour chaque $\chi \in \widehat{G}$ les égalités

$$\delta_\chi \overset{\mathcal{G}}{\mapsto} \frac{1}{|G|}\sum_{\psi\in\widehat{G}} \delta_\chi^\psi \psi = \frac{\chi}{|G|} \overset{\mathcal{F}}{\mapsto} \left(\sum_{g\in G} \frac{\overline{\chi(g)}}{|G|}\psi_g\right)_{\psi\in\widehat{G}} = \left(\frac{1}{|G|}\sum_{g\in G} \frac{\psi}{\chi}(g)\right)_{\psi\in\widehat{G}}$$

$$= \left(\delta^1_{\frac{\psi}{\chi}}\right)_{\psi\in\widehat{G}} = \left(\delta_\chi^\psi\right)_{\psi\in\widehat{G}} = \delta_\chi.$$

[53] En d'autres termes, l'injection "Dirac" $g \mapsto \delta_g$ *plonge* le groupe G dans le monoïde $\left(\mathbb{C}^G, *\right)$. On pourra donc écrire des *combinaisons linéaires* d'éléments de G en identifiant ces derniers à leurs Dirac respectifs, ce qui permet d'évaluer des *polynômes* en de tels éléments, d'où la notation $\mathbb{C}[G]$ parfois rencontrée pour l'ev $\mathbb{C}^G$.

Il reste à montrer que notre isomorphisme $\mathcal{F}$ d'evs préserve l'unité et le produit $*$. Vu l'égalité $\mathcal{F}(\delta_1) = \mathrm{eval}_1$, l'unitarité découle de celle des caractères ; que ces derniers préservent le produit permet par ailleurs d'égaliser à $g, h \in G$ fixés $\mathcal{F}(\delta_g * \delta_h) = \mathcal{F}(\delta_{gh}) = \mathrm{eval}_{gh}$ et $\mathrm{eval}_g \mathrm{eval}_h = \mathcal{F}(\delta_g)\mathcal{F}(\delta_h)$, ce qui conclut.

Remarque (produit scalaire). En munissant $\mathbb{C}^G$ et $\mathbb{C}^{\widehat{G}}$ des produits hermitiens de l'exercice précédent, on montrerait aisément que $\mathcal{F}$ est une isométrie d'algèbres hermitiennes qui fixe le groupe G, au sens où un $g \in G$ (identifié à son Dirac δ_g) est envoyé sur lui-même (identifié à son image eval_g dans le bidual). Cette "fixation" de G équivaut à la commutativité du diagramme suivant, qui "raffine" l'isomorphie du groupe G avec son bidual établie plus haut :

$$\begin{array}{ccc} G & \hookrightarrow & \mathbb{C}[G] \text{ pour} * \\ \text{groupes} & & \text{algèbres hermtiennes} \\ \downarrow\cong & & \downarrow\cong \\ \widehat{\widehat{G}} & \subset & \mathbb{C}\left[\widehat{G}\right] \text{ pour } \times_{\mathbb{C}} \end{array}.$$

2.5 Quotients

On reprend les notations du cours : A est une partie non vide d'un groupe G et on abrège pour chaques $g, \gamma \in G$

$$g \overset{A}{=} \gamma \overset{\text{déf.}}{\iff} g \in \gamma + A.$$

On ne suppose plus G abélien.

2.5.1 Commutateurs, groupe dérivé

On appelle ***commutateur*** de deux éléments g et γ le produit $[g, \gamma] := g\gamma g^{-1}\gamma^{-1}$. Le groupe engendré par ces commutateurs s'appelle le ***groupe dérivé*** de G et est noté $D(G)$.

1. *Expliquer en quoi un commutateur mesure le défaut de commutativité entre deux éléments.*
2. **Soient $n \geq 3$? ? ?un naturel et K un corps (implicite). Montrer que chaque transvection de GL_n (resp. chaque 3-cycle de $\mathfrak{S}_n$) est un commutateur. En déduire le groupe dérivé de GL_n (resp. $\mathfrak{S}_n$).*
3. *Montrer que chaque morphisme de source G à valeurs dans un groupe <u>abélien</u> induit un morphisme de source ${}^{G}\!/_{D(G)}$. Commenter.*
4. *Montrer que $D(G)$ est le plus petit sous-groupe distingué de G tel que ${}^{G}\!/_{D(G)}$ est abélien.*

SOL

1. Deux éléments g et γ commutent ssi $g\gamma = \gamma g$, ied ssi $g\gamma(\gamma g)^{-1} = 1$, ou encore ssi leur commutateur vaut 1. On a plus précisément $g\gamma = [g, \gamma]\gamma g$.
2. Soit T une transvection. Le résultat tombe dès que l'on se souvient que les transvections sont toutes semblables : T^2 étant une transvection (? ? ?traiter à part car2 ? ? ?), elle est semblable à T, d'où un automorphisme α tel que $T^2 = \alpha T \alpha^{-1}$, ce qui se réécrit $T = [\alpha, T]$. Il s'ensuit que le groupe engendré par les transvections est inclus dans celui engendré par les commutateurs, ce qui s'écrit $SL_n \subset D(GL_n)$. Le déterminant étant par ailleurs trivial sur les commutateurs, il l'est sur le sous-groupe qu'il engendre, d'où l'inclusion réciproque.

   Même chose dans $\mathfrak{S}_n$: tous les 3-cycles sont conjugués, donc chaque 3-cycle est conjugué à son carré et est (*cf.* paragraphe précédent) un commutateur. Il en résulte que le groupe engendré par les 3-cycles (qui vaut $\mathfrak{A}_n$) est inclus dans celui engendré par les commutateurs. La signature étant par ailleurs triviale sur les commutateurs, on a l'inclusion réciproque $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$.
3. Soient A un groupe abélien et $\varphi : G \longrightarrow A$ un morphisme. Vu que l'image d'un commutateur vaut le commutateur des images, l'abélianité du groupe but montre que $\mathrm{Ker}\,\varphi$ contient chaque commutateur, donc contient le sous-groupe $D(G)$ qu'il engendre, d'où un morphisme induit $\begin{cases} {}^{G}\!/_{D(G)} & \longrightarrow & A \\ \overline{g} & \longmapsto & \varphi(g) \end{cases}$ comme souhaité. Commentaire : *un morphisme à but abélien ne voit pas les commutateurs* (en particulier ne voit ni les transvections ni les 3-cycles).

4. Soient $d \in D(G)$ et $g \in G$. Le conjugué gdg^{-1} se réécrit $[g,d]\,d$, qui reste dans le sous-groupe $D(G)$, ce qui montre que ce dernier est distingué. Le caractère abélien du quotient est immédiat en écrivant (à $g, \gamma \in G$ fixés)
$$\overline{g}\ \overline{\gamma} = \overline{g\gamma} = \overline{[g,\gamma]\,\gamma g} = \overline{[g,\gamma]}\overline{\gamma g} = \overline{1}\ \overline{\gamma}\ \overline{g}.$$
Soit par ailleurs S un sous-groupe distingué de S tel que ${}^{G}\!/_{S}$ soit abélien. *Modulo* S, on a alors (toujours à $g, \gamma \in G$ fixés) $\overline{[g,\gamma]} = [\overline{g},\overline{\gamma}] = \overline{1}$, d'où $[g,\gamma] \in S$, ce qui montre que S contient chaque commutateur, *a fortiori* le sous-groupe $D(G)$ qu'ils engendrent.

2.5.2 Quotients non abéliens, parties distinguées

1. *Montrer que la relation $\overset{A}{=}$ est d'équivalence et compatible avec la loi de G ssi A est un sous-groupe de G* ***distingué****, ied tel que $\forall g \in G,\ Ag \subset gA$.*
2. Supposons que A est une partie distinguée de G. *Montrer que le quotient ${}^{G}\!/_{A}$ est un groupe ssi A est (le translaté d')un sous-groupe de G.*
3. *Dans les isométries planes, montrer que les réflexions forment une partie distinguée mais qu'aucune d'elle n'engendre un sous-groupe distingué.*

DEM

1. Reprenons telles quelles nos trois caractérisations de l'égalité *modulo* A (réflexivité, symétrie, transitivité) : seule achoppe dans notre démonstration le passage de la transitivité à la compatibilité. Avec les même notations (sauf pour la loi), on partait de deux égalités *modulo* A, ied $\begin{cases} g \in g'A \\ \gamma \in \gamma' A \end{cases}$, on composait par $\begin{cases} \gamma \text{ à droite} \\ g' \text{ à gauche} \end{cases}$, ce qui donne en prenant cette fois garde à l'ordre $\begin{cases} g\gamma \in g'A\gamma \\ g'\gamma \in g'\gamma' A \end{cases}$. On aimerait en haut plutôt $g\gamma \in g'\gamma A$ (pour pouvoir comme avant conclure $g\gamma \overset{A}{=} g'\gamma \overset{A}{=} g'\gamma'$), ce qui découlerait de l'inclusion $A\gamma \subset \gamma A$, laquelle tient quand A est distingué.

   Montrons par ailleurs que le caractère distingué de A découle de la réflexivité et de la compatibilité conjointes de $\overset{A}{=}$ (nous laissons ensuite le lecteur s'assurer que tout boucle bien correctement pour établir l'équivalence souhaitée). Soit $g \in G$ et montrons $Ag \subset gA$. Soit $a \in A$: on a alors (avec la réflexivité) $\begin{cases} a \overset{A}{=} 1 \\ g \overset{A}{=} g \end{cases}$, d'où (par transitivité) $ag \overset{A}{=} 1g$, ied $ag \in gA$, ce qui conclut.
2. Il suffit de reprendre la démonstration du cours telle quelle. L'hypothèse intervient dans la série d'égalités
$$SS = uAuA \underset{\text{distingué}}{\overset{A \text{ est}}{\subset}} uuAA = u^2\overline{u^{-1}} = u^2u^{-1}A = uA = S,$$
l'inclusion étant en fait une égalité puisque $uA = u\left(Au^{-1}\right)u \subset u\left(u^{-1}A\right)u = Au$.
3. Tout repose sur le principe de conjugaison vu section **??**. Lorsque le conjuguant est une rotation non triviale, il devient alors clair qu'aucun sous-groupe engendré par une réflexion n'est distingué.

2.5.3 Quotients et produits

On impose que A soit un sous-groupe distingué de G. Les groupes équipotents G et ${}^{G}\!/_{A} \times A$ sont-ils isomorphes ?

La réponse est négative en général. Soit $n \geq 2$ un naturel. Lorsque $\binom{G}{A} = \binom{\mathbf{U}_{2n}}{\mathbf{U}_n}$, le quotient est d'ordre $\frac{2n}{n} = 2$, donc est isomorphe à $\mathbf{U}_2$, donc le groupe produit ${}^{G}\!/_{A} \times A$ est isomorphe à $\mathbf{U}_2 \times \mathbf{U}_n$ où chaque chaque élément est d'ordre au plus n, tandis que G en contient un d'ordre n^2. (Peut se rédiger sans parler d'ordre en imposant $n = 2$ et en comptant alors les involutifs.)

2.5.4 Quotients et partitions

Montrer que les classes modulo A *partitionnent* G *ssi (un certain translaté de)* A *est un sous-groupe de* G.

DEM

$\boxed{\Longleftarrow}$ Lorsque A est un sous-groupe, la relation $\overset{A}{=}$ est d'équivalence et les classes $\overline{g}$ partitionnent G. Or on a vu que l'ensemble des classes était inchangé par translation.

$\boxed{\Longrightarrow}$ La partie A est déjà non vide (sinon les classes seraient vides et leur réunion G aussi), ce qui permet d'invoquer un $a \in A$. Montrons alors que $B := a^{-1}A$ est un sous-groupe. Il contient déjà $a^{-1}a = 1$ (ce pour quoi nous avons translaté par a^{-1}. Observons ensuite que, si deux classes *modulo* A se rencontrent, alors elles sont égales : en particulier, pour chaque $g \in G$, si gB et B se rencontrent, alors $gB \subset B$. Appliquons cette observation à deux reprises. Soit $b \in B$. Alors d'une part bB et B contiennent tous deux $b1 = b$, d'où l'inclusion $bB \subset B$ et la stabilité de B, d'autre part $b^{-1}B$ et B contiennent tous deux $b^{-1}b = 1$, d'où l'inclusion $b^{-1} \in b^{-1}B \subset B$ et la stabilité de B par inversion.

2.5.5 La relation $\overset{A}{=}$ dans un monoïde

On impose désormais que A soit une partie d'un monoïde M.

1. *Montrer que la relation* $\overset{A}{=}$ *est symétrique ssi* A *est incluse dans* $M^\times$ *et stable par inversion.*
2. *Montrer que la relation* $\overset{A}{=}$ *est réflexive, transitive et compatible avec la loi de* M *ssi* A *est un sous-monoïde distingué de* M. *Dans ces conditions, montrer que le quotient* ${}^{M}\!/_{A}$ *est un monoïde de neutre* $\overline{1}$ *où l'on a* $\overline{m}\ \overline{\mu} = \overline{m\mu}$ *pour tous* $m, \mu \in M$.
3. *Montrer que la relation* $\overset{A}{=}$ *est d'équivalence et compatible avec la loi de* M *ssi* A *est un sous-groupe distingué de* $M^\times$. *Commenter.*

DEM

1. Le sens $\boxed{\Longleftarrow}$ a été fait en cours. Supposons donc $\overset{A}{=}$ symétrique et soit $a \in A$. Cela se réécrit $a \overset{A}{=} 1$, ied (par symétrie) $1 \overset{A}{=} a$, ied $1 \in aA$, d'où un $b \in A$ tel que $1 = ab$. Appliquant ce qui précède en remplaçant a par b donne un $c \in A$ tel que $1 = bc$. L'élément b est donc inversible à droite et à gauche, donc (*cf.* un exercice du cours) inversible d'inverse $a = c$, ce qui montre que a est inversible, son inverse b ayant été invoqué dans A.
2. Il suffit de reprendre le cours et l'exercice *Quotients non abéliens* : tout fonctionne. Récapitulons au besoin les chaînes d'implications en jeu :

$$\left\{\begin{array}{l} \overset{A}{=} \text{ transitive} \\ A \text{ distingué} \end{array}\right. \Longrightarrow \overset{A}{=} \text{ compatible} \iff A \text{ stable} \Longrightarrow \overset{A}{=} \text{ transitive}$$

$$\overset{A}{=} \text{ réflexive et compatible} \iff A \text{ distingué}$$

3. Découle des deux points précédents. Ainsi n'y a-t-il pas grand intérêt, si l'on veut conserver une relation d'équivalence, à généraliser en remplaçant le groupe quotienté par un monoïde.

2.5.6 Centre et probabilités

1. Soit G un groupe dont le quotient par son centre est cyclique. *Montrer que* G *est abélien.*
2. On note p la probabilité que deux éléments dans un groupe fini donné commutent (les éléments sont tirés au hasard selon la loi uniforme). **Montrer l'implication* $p > \frac{5}{8} \implies p = 1$.
3. *Peut-on remplacer* $\frac{5}{8}$ *par une valeur inférieure ?*

SOL

1. Notons Z le centre de G. Soit a un élément de G dont la classe $\overline{a}$ *modulo* Z engendre ${}^{G}\!/_{Z}$. Prenons deux éléments g et g' dans G dont on veut montrer qu'ils commutent. Leurs classes modulo Z sont des puissances de $\overline{a}$, mettons $\overline{g} = \overline{a}^n = \overline{a^n}$ pour un certain relatif n. Il y a donc un $z \in Z$ tel que $g = za^n$. De même, on peut écrire $g' = z'a^{n'}$ pour un certain $z' \in Z$. Il est alors clair que g et g' commutent :

$$gg' = zz'a^{n+n'} = g'g.$$

2. Notons G notre groupe fini : notre probabilité p s'exprime alors par

$$p = \frac{1}{|G|^2} \sum_{a \in G} \#\left\{b \in G \ ; \ ab = ba\right\}.$$

La cardinal dans la somme est aisé à évaluer lorsque a dans le centre Z de G : il vaut alors $|G|$. Dans le cas contraire, le commutant $\#\left\{b \in G \ ; \ ab = ba\right\}$ est un sous-groupe strict, donc est d'ordre $\leq \frac{|G|}{2}$. En séparant la sommation sur Z de la sommation ailleurs, on obtient l'inégalité

$$|G|^2 p \leq |Z|\,|G| + (|G| - |Z|)\,\frac{|G|}{2}, \text{ } i.\ e.\ p \leq \frac{|Z|}{2\,|G|} + \frac{1}{2}.$$

Si (par contraposée) on a $p < 1$, alors notre groupe G n'est pas commutatif, donc (*cf.* point précédent) le quotient par son centre n'est pas cyclique, donc le quotient ${}^{G}\!/_{Z}$ n'est pas d'ordre premier, donc est d'ordre ≥ 4, ce qui s'écrit $\frac{|Z|}{|G|} \leq \frac{1}{4}$; en réinjectant dans l'inégalité ci-dessus, on obtient $p \leq \frac{5}{8}$, *CQFD.*

3. Cherchons à réaliser l'égalité $p = \frac{5}{8}$, ce qui montrera que la valeur $\frac{5}{8}$ est minimale. Il s'agit de réaliser les égalités dans toutes les comparaisons précédentes, *i. e.* de trouver un groupe dont le centre soit d'indice[54] 4 et dont chaque commutant soit d'indice 1 ou 2. Essayons un groupe d'ordre 8 (pour avoir le dénominateur de p) non abélien. À part des produits (semi-)directs de groupes $\mathbb{U}_n$, il y a le groupe $\mathbb{H}_8$. On vérifiera que son centre, qui vaut $\{\pm 1\}$, est bien d'indice 4 et que le commutant de $\pm i$, qui vaut $\{\pm 1, \pm i\}$, est bien d'indice 2 (de même pour $\pm j$ et $\pm k$).

2.5.7 *Sous-groupes de Prüfer

Soit p un premier. *Déterminer les sous-groupes de* ${}^{\mathbb{Z}\left[\frac{1}{p}\right]}\!/_{\mathbb{Z}}$.

SOL Pour chaque naturel n, notons $G_n := \left\langle \frac{1}{p^n} \right\rangle$? ? ?préciser le cadre ? ? ? Abrégeons $G_\infty := \left\langle \frac{1}{p^n} \right\rangle_{n \in \mathbb{N}}$ pour homogénéiser. Il est clair que les G_n pour n parcourant $\overline{\mathbb{N}}$ forment une suite strictement croissante de sous-groupes. Montrons la réciproque.

Soit S un sous-groupe. Notons $M := \sup_{\overline{\mathbb{N}}} \left\{ n \in \mathbb{N} \ ; \ \frac{1}{p^n} \in S \right\}$ et montrons $S = G_M$ (intuité par notre attente).

Si M est infini, alors il y a (par propriété d'un *supremum*) une suite strictement croissante de naturels $(n_k)_{k \in \mathbf{N}}$ telle que $\frac{1}{p^{n_k}} \in S$. Pour chaque $k \in \mathbb{N}^*$, la comparaison $n_k \geq k$ permet de récupérer $\frac{1}{p^k}$ dans S comme un itéré de $\frac{1}{p^{n_k}}$; notre sous-groupe S contient donc chaque $\frac{1}{p^k}$, donc le sous-groupe G_∞ qu'il engendre.

Supposons à présent M fini : ce *supremum* est donc un *maximum.* Puisque $\frac{1}{p^M} \in S$, on a l'inclusion $G_M = \left\langle \frac{1}{p^M} \right\rangle \subset \langle S \rangle = S$. Soit maintenant $s \in S$. Ce s s'écrit $\frac{a}{p^n}$ pour certains naturel a et n : il s'agit pour conclure $s \in G_M$ de montrer $n \leq M$, comparaison qui découlera par définition d'un *maximum* des appartenances $\forall k \in [\![0, n]\!], \ \frac{1}{p^k} \in S$. Montrons ces dernières par récurrence. L'initialisation est triviale (on raisonne *modulo* $\mathbb{Z}$). Soit $k \in [\![1, n]\!]$ tel que $\frac{1}{p^{k-1}} \in S$. Quitte à considérer la forme irréductible de s, on peut imposer que a et p soient premiers entre eux, ce qui permet d'invoquer par Bézout deux relatifs λ et μ tels que $\lambda a + \mu p = 1$. Le $p^{n-k}\lambda$-ième itéré de s vaut alors $\frac{\lambda a}{p^k} = \frac{1}{p^k} - \frac{\mu}{p^{k-1}}$ et doit rester dans le sous-groupe S, tout comme le $(-\mu)$-ième itéré de $\frac{1}{p^{k-1}}$, donc leur somme $\frac{1}{p^k}$ tombe dans S, CQFD

[54] l'***indice*** d'une partie d'un groupe est le cardinal du quotient par cette partie

2.6 Groupes monogènes

2.6.1 Produits de groupes cycliques, théorème chinois *bis*

1. *Soient dans un groupe g et h deux éléments commutant et d'ordres premiers entre eux. Montrer que la loi du groupe induit par restriction un isomorphisme $\langle g\rangle \times \langle h\rangle \cong \langle gh\rangle$.*
2. *Retrouver le théorème chinois lorsque $ab > 0$ et comparer l'isomorphisme obtenu à celui du cours.*
3. *Adapter la démarche précédente pour obtenir le même isomorphisme.*

Démonstration

1. Notons α et β les ordres respectifs de g et h. Un exercice du cours montre alors que l'ordre π de gh vaut $\alpha\beta$. Puisque g et h commutent, leurs itérés également, donc la loi restreinte à $\langle g\rangle \times \langle h\rangle$ est un morphisme. Regardons les couples (g^n, h^n) pour n naturel décrivant $[0, \pi[$. L'image d'un tel couple vaut $g^n h^n = (gh)^n$ toujours par l'hypothèse $gh = hg$, donc ces images coïncident avec les π itérés de gh. Elles sont en particulier distinctes, donc les couples précédents également ; or il y en a $\pi = \alpha\beta = \#\langle g\rangle \,\#\langle h\rangle$, *i. e.* autant que d'éléments dans $\langle g\rangle \times \langle h\rangle$. Le morphisme ci-dessus induit donc une bijection $\langle g\rangle \times \langle h\rangle \cong \langle gh\rangle$, ce qui conclut.
2. La multiplication dans le groupe $\mathbb{C}$ et les éléments $g := e^{\frac{2\pi i}{a}}$ et $h := e^{\frac{2\pi i}{b}}$ (qui font sens vu l'hypothèse $ab > 0$) induisent un isomorphisme de source $\langle g\rangle \times \langle h\rangle = \mathbb{U}_a \times \mathbb{U}_b$ dont l'image est un sous-groupe fini de $\mathbb{C}$ de cardinal $|\mathbb{U}_a \times \mathbb{U}_b| = ab$, à savoir $\mathbb{U}_{ab}$ (d'après un exercice du cours). On obtient ainsi un isomorphisme (explicite)
$$\left\{\begin{array}{ccccccc} {}^{\mathbb{Z}}\!/_{a} \times {}^{\mathbb{Z}}\!/_{b} & \xrightarrow{\sim} & \mathbb{U}_a \times \mathbb{U}_b & \xrightarrow{\sim} & \mathbb{U}_{ab} & \xrightarrow{\sim} & {}^{\mathbb{Z}}\!/_{ab} \\ \left(\widetilde{k}, \widehat{\ell}\right) & \longmapsto & \left(e^{2\pi i \frac{k}{a}}, e^{2\pi i \frac{\ell}{b}}\right) & \longmapsto & e^{2\pi i \frac{kb+\ell a}{ab}} & \longmapsto & \overline{bk + a\ell} \end{array}\right. .$$
Or celui du cours envoit l'image ci-dessus $\overline{bk + a\ell}$ sur $\left(\widetilde{bk + a\ell}, \widehat{bk + a\ell}\right) = \left(\widetilde{bk}, \widehat{a\ell}\right)$, ce qui *semble* différent de l'antécédent $\left(\widetilde{k}, \widehat{\ell}\right)$ ci-dessus. Précisons ce semblant.

Supposons l'égalité $\begin{pmatrix}\widetilde{k}\\ \widehat{\ell}\end{pmatrix} = \begin{pmatrix}\widetilde{bk}\\ \widehat{a\ell}\end{pmatrix}$ pour chaque $\begin{pmatrix}\widetilde{k}\\ \widehat{\ell}\end{pmatrix}$ source. On a en particulier $\begin{pmatrix}\widetilde{1}\\ \widehat{1}\end{pmatrix} = \begin{pmatrix}\widetilde{b}\\ \widehat{a}\end{pmatrix}$, d'où deux entiers λ et μ tels que $\left\{\begin{array}{c} b = 1 + \lambda a \\ a = 1 + \mu b \end{array}\right.$ (observer la *positivité* de λ et μ vu l'hypothèse $ab > 0$). Remplacer a dans la première ligne donne $(1 - \lambda\mu)\, b = 1 + \lambda > 0$, d'où $1 - \lambda\mu > 0$ (car $b > 0$), *i. e.* $\lambda\mu < 1$, ou encore $\lambda\mu = 0$, d'où l'une des égalités $\left\{\begin{array}{c} b = 1 \\ \text{ou} \\ a = 1 \end{array}\right.$ et la trivialité de l'un des groupes ${}^{\mathbb{Z}}\!/_{a}$ ou ${}^{\mathbb{Z}}\!/_{b}$. Réciproquement, par exemple quand $a = 1$, l'isomorphisme ci-dessus devient $\left\{\begin{array}{ccc} {}^{\mathbb{Z}}\!/_{1} \times {}^{\mathbb{Z}}\!/_{b} & \xrightarrow{\sim} & {}^{\mathbb{Z}}\!/_{1b} \\ \left(\widetilde{0}, \widehat{\ell}\right) & \longmapsto & \overline{b0 + 1\ell} = \overline{\ell} \end{array}\right.$, ce qui est précisément celui du cours.
3. Bézout nous donne deux relatifs λ et μ tels que $\lambda a + \mu b = 1$. Afin qu'un $\left(\widetilde{k}, \widehat{\ell}\right)$ source soit envoyé sur la classe $\overline{(b\lambda)\, k + (a\mu)\, \ell}$ du cours, il suffit de remplacer la multiplication complexe $\left\{\begin{array}{ccc} \mathbb{U}_a \times \mathbb{U}_b & \xrightarrow{\sim} & \mathbb{U}_{ab} \\ (x, y) & \longmapsto & xy \end{array}\right.$ par l'application $(x, y) \mapsto x^\mu y^\lambda$, ce qui peut se faire en composant *à droite* la multiplication complexe par le produit des applications $\begin{array}{c} \text{"élever dans } \mathbb{U}_a \text{ à la puissance } \mu\text{"} \\ \text{"élever dans } \mathbb{U}_b \text{ à la puissance } \lambda\text{"} \end{array}$ – mais pourquoi ce produit (de morphismes) serait-il un *iso*morphisme ? Simplement : l'identité de Bézout montre que $x \mapsto x^\mu$ et $x \mapsto x^b$ sont réciproques l'une de l'autre, de même pour $y \mapsto y^\lambda$ et $y \mapsto y^a$, d'où le caractère bijectif cherché (qui passe au produit).