Lois de composition
(version chantier)

Marc SAGE

<2017

Table des matières

Algèbre provient du mot arabe al jabr que l'on retrouve dans le titre du livre de Al Khwarizmi, *Kitab al jabr wa muqabala*. Il signfie remise en place. Dans cet ouvrage, cela consistait à changer de côté d'une équation les termes de signe négatif pour les rendre positifs. En Espagne, on pouvait lire autrefois sur les enseignes de certains guérisseurs algebrista y sangredor. Ceux-ci remettaient les os en place et pratiquaient les saignées.

À la Renaissance, l'algèbre désigne une extension des méthodes de calculs généralisées à des nombres éventuellement négatifs avec utilisation d'inconnues et de paramètres. Curieusement, François Viete propose en 1590 de remplacer ce mot par le mot analyse, sans succès. Au début du XIXème siècle, l'algèbre est encore considérée comme une arithmétique avec des symboles. On s'intéresse alors de plus en plus aux opérations en elles-mêmes. On se rend compte que sur différents ensembles de nombres, elles vérifient des propriétés telles l'associativité,l'existence de l'élément neutre. Ceci conduit à l'étude des strctures abstraites comme les groupes, les anneaux, les espaces vectoriels de manière générale : c'est l'algèbre abstraite. La construction des nombres complexes au début du XIXème siècle et celle des quaternions d'Hamilton en 1843 amènent à imaginer des hypernombres. Ces nouvelles structures deviennent trop éloignées de la conception que l'on a du nombre. On définit alors une nouvelle structure appelée algèbre. Dans le langage courant, l'affirmation « Pour moi, c'est de l'algèbre ! » est synonyme de « C'est incompréhensible ». Le sens est tout à fait différent de « C'est mathématique » qui fait référence à une affirmation confirmée, selon le locuteur, par la logique. L'adjectif algébrique, relatif à l'algèbre remplace au XVIIIème siècle algébraïque apparu deux siècles plus tôt. Il se rencontre dans les expressions clôture algébrique, ensemble algébrique, extension algébrique, géométrie algébrique, nombres algébriques, surfaces algébriques. Elles sont toutes de création récente.

Les termes *commutatif* et *distributif* ont été introduits par Servois en 1814 et repris par Boole dont l'influence a sans doute contribué à répandre leur usage en Grande-Bretagne.

1 LCI et magmas

$a \cdot b$ s'appelle le *composé* de a et de b pour la loi $\cdot$.
Un ensemble muni d'une lci est un *magma* (=pas de structure)
EG : magma triviaux $\{0\}$ muni de la lci $0 \times 0 = 0$.
EG . magma avec loi constante
la lois $(a, b) \mapsto b \cdot a$ est la *loi inverse* de $\cdot$.
Pourquoi la loi $\times$ est sous-entendue ? Parce que trois patates, 3 patates, $3p$

EXo : combien de composés peut-on former ?
Mauvaise question : ce n'est pas la valeurs des composées, mais le parenthésage. SI C_n désigne le nombre de composée à n éléemtns, on a $C_1, C_2, C_3, C_4 = 1, 1, 2, 5$, et plus gnérlament $C_n = \sum_{p+q=n}^{p,q>0} C_p C_q$. Série géné donnc $C^2 = C - X$, d'où $C = \frac{1-\sqrt{1-4X}}{2}$ et $C_n = Cat_{n-1}$.

loi *commutative*
Le $+$ est pour les lois commutative exclusivment[1].
On peut préciser au besoin les magma *additif* ou *muliplicatif*, ce qui évite les notations lourdes $(M, +)$ ou $(M, \times)$ ou $(M, \cdot)$
EG : N, Z, Q, R, C sont des magmas additif mais aussi multiplicatif, et les propriétés sont très différentes.
Si pas commutatif, on peut se placer dans le *centre* de M, défini par $Z(M) := \{m \in M,\ \forall x, mx = xm\}$. Il mesure le "degré" de commutativité de M.

un *neutre* est un élément e tel que $\forall x, ex = xe = x$. S'il existe, il est unique, et le magma est dit *unitaire* ou *unifière*. On note (très) souvent 1 un neutre multiplicatif et 0 un neutre additif.
un *absorbant* est un élément ω tel que $\forall x, \omega x = x\omega = \omega$. S'il existe, il est unique.
distinguer à droite/gauche, parler de *bilatère* juste pour insister
PROP : *un neutre à droite et un neutre à gauche coincident, d'où un neutre bilatère (unique)*
Idem pour les absorbant
RQ : neutre et abs vont ensemble : dans $ab = a$, quantif $\begin{matrix}\forall a \\ \forall b\end{matrix}$ donne $\begin{matrix}\text{neutre droite} \\ \text{absorbant gauche}\end{matrix}$

EG :

[1] même si l'addition des ordinaux n'est pas commutative

dans $(Z, \times)$, 1 est neutre et 0 est absorbant
dans $N \cup \{\infty\}$ additif, 0 est neutre et ∞ est absorbant

Si 0 est un neutre d'un magma M, et si f est une fonction à valeurs dans M, on peut toujours prolonger f en posant 0 (d'où $M^X \hookrightarrow M^Y$ lorsque $X \hookrightarrow Y$)

EG tordus
Z muni de $-$ est un magma non commutatif, unifère à droite 0, sans neutre bilatère ni absorbant, dont tous les éléments vérifient $a - a = 0$.
Z muni de $(a, b) \mapsto \left\lfloor \frac{ab}{18} \right\rfloor$ a neutre, pas d'absorbant, mais que 3 a plusieurs symétriques (donc non assoc), sans
R^3 muni du produit vectoriel est un magma non unifère ($a \wedge x$ est toujours $\perp a$, donc $\neq a$ sauf si a est nul), avec absorbant 0, dont tous les éléments vérifent $a \wedge a = 0$.
N^* muni de $(a, b) \mapsto a^b$ est un magma non commutatif, unifère à droite et absorbant à gauche 1, mais sans neutre ni absorbant biltatères.
N muni de $(a, b) \mapsto \left\lfloor \frac{a}{b+1} \right\rfloor$ est un magma non comm, avec neutre à droite et absorbant à gauche 0, mais sans neutre ni absorbant bilatère.
N muni de $(a, b) \mapsto b + \min\{a, b\}$ est magma non com, non assoc, avec neutre à gauche et absorbant à droite 0,

Aucun des magmas ci-dessus ne permet de calculer aisménet des itérés, au sens suivant.

1.1 Associativité

on a envie de définir un loi multiple qui prolonge $\cdot$: quel sens donner à abc ? problème ordre : $a(bc) = (ab)c$ pas automatique -> soustraction et division :-) on peut si assoc.

EG : dans C, on pose $a * b := \overline{ab}$. Sens de $a * b * c$?
EG : dans $\mathfrak{P}(E)$, on pose $A \cdot B = \begin{matrix} \emptyset \text{ si } A \cap B = \emptyset \\ E \text{ sinon} \end{matrix}$: sens à $A \cdot B \cdot C \cdot D$?
Même si la première loi est apprament bp + simpl que la seconde, elle n'est pas assoc au contraire de l'autre.
$(a * (b * c) = \overline{a}bc \neq ab\overline{c} = (a * b) * c)$

1.1.1 calcul d'un produit

Loi *associative* : on peut associer les élément comme on veut. Plus précisément, on peut découper un mot $a_1 \cdot a_2 \cdot ... \cdot a_n$ en paquets $(m_1) \cdot (m_2) \cdot ... \cdot (m_k)$, composer chaque paquet, puis composer les résultats des paquets, et le résultat final ne dépend pas du découpage en paquets. Formalisons.

Un *mot* de M est un l-uplet d'éléments de M où l est un entier ≥ 1 appelé *longueur* du mot. L'ensemble des mots sur M sera noté M^*. Si $\alpha = (a_1, ..., a_p)$ et $\beta = (b_1, ..., b_q)$ sont des mots, on définit le mot *concaténé* $\alpha * \beta$ par $(a_1, ..., a_p, b_1, ..., b_q)$, et de la même manière la concaténation de plusieurs mots qui rend évident son associativité.
Nous souhaitons montrer qu'il y a une unique application $\pi : \left\{ \begin{matrix} M^* & \longrightarrow & M \\ (a_1, ..., a_p) & \longmapsto & a_1 \cdot ... \cdot a_p \end{matrix} \right.$ telle que $\pi(a) = a$, $\pi(a, b) = ab$ et vérifiant

$$\forall k \geq 1,\ \forall (m_i) \in M^*,\ \pi(m_1 * ... * m_k) = \pi(m_1) \cdot ... \cdot \pi(m_k)$$

(autrement dit π est un morphisme du monoïde $(M^*, *)$ dans $(M, \cdot)$)
Algorithmquement : remplacer tous les $(ab)c$ par $a(bc)$, ce qui fnit par s'arêter (pourquoi ?) : un mot $a_1...a_n$ sera alors mis sous forme canonique $a_1(a_2(a_2...(a_{n-2}(a_{n-1}a_n))...))$.
Pour l'unicité, on sait que le résultat ne doit pas dépendre de l'ordre choisi, donc on prend n'importe quoi, par exemple $a_1 \cdot ... \cdot a_n = a_1 \cdot (a_2 \cdot (...a_{n-2} \cdot (a_{n-1} \cdot a_n)...))$ (déf propre par itération ?). Vérifions que ce π fonctionne. Les deux premières propriétés sont tautologiques et montrent la cohérence de la notation $a_1 \cdot ... \cdot a_p$.
Pour la troisième, on fait une récurrence sur $k \geq 2$ (rien à faire pour $k = 1$).

Pour $k=2$, montrons $\pi(\alpha * \beta) = \pi(\alpha) \cdot \pi(\beta)$ par récurrence sur le nombre n de termes du mot $\alpha * \beta$. Pour $n = 2$, rien à faire, une seule maière de composer. Soit $n \geq 3$; montrons que toutes les manières $(a_1 ... a_{i-1})(a_i ... a_n)$ de composer pour $1 < i < n$ coincident : à i fixé, on récurre à l'intéreiru, puis on applique $n = 3$:

$$\begin{aligned}
(a_1 \cdot ... \cdot a_{i-1}) \cdot (a_i \cdot ... \cdot a_n) &= (a_1 \cdot ... \cdot a_{i-1}) \cdot (a_i \cdot (a_{i+1} \cdot ... \cdot a_n)) \text{ def de } \pi \\
&= ((a_1 \cdot ... \cdot a_{i-1}) \cdot a_i) \cdot (a_{i+1} \cdot ... \cdot a_n) \text{ def de assoc} \\
&= (a_1 \cdot (a_2 \cdot ... \cdot a_i)) \cdot (a_{i+1} \cdot ... \cdot a_n) \text{ HR} \\
&= (a_1 \cdot a_2 \cdot ... \cdot a_i) \cdot (a_{i+1} \cdot ... \cdot a_n) \text{ def de } \pi
\end{aligned}$$

Pour $k \geq 2$, on utilise la définiton de π pour se ramenr au cas précédent :

$$\begin{aligned}
\pi(m_0) \cdot ... \cdot \pi(m_k) &= \pi(m_0) \cdot (\pi(m_1) \cdot ... \cdot \pi(m_k)) \\
&= \pi(m_0) \cdot \pi(m_1 * ... * m_k) \\
&= \pi(m_0 * (m_1 * ... * m_k)) \\
&= \pi(m_0 * m_1 * ... * m_k), \text{ CQFD.}
\end{aligned}$$

Rq : si loi comm, pour montrer assos, n'utiliser qu'un côté !

EXO rigolo : on écrit au tableau les inverses des nombres de 1 à 1981 (naissance de mon grand frère).
On efface deux nombres a et b et on les remplace par $a + b + ab$.
Quel est le dernier nombre écrit ?
loi $*$ comm et asso, on trouve $1 * \frac{1}{2} * \frac{1}{3} * ....$ Or $n * \frac{1}{n+1} = n + 1$, d'où le résultat 1981.
(en fait, on triche, c'est l'addition usuel congujuée par l'incrémentation)

1.1.2 Itérés d'un élément (idempotent, involutif, nilpotent)

itéré d'un élément : on défini a^n par la récurrence $a^1 = a$ et $a^{n+1} = aa^n$. On montre aisément $a^p a^q = a^{p+q}$ et $(a^p)^q = a^{pq}$ pour $p, q \geq 1$

En additif, l'itéré est noté na, et vérifie $1a = a$, $(p+q)a = pa + qa$ et $p(qa) = (pq)a$. On dit que l'on a une action de $\mathbb{N}$ sur A *associative* et distributive à droite (attention, on n'a la distributivité à gauche seulement pour les monoïdes commutatifs : $a + b + a + b = 2(a + b) \stackrel{?}{=} 2a + 2b = a + a + b + b$? ? ?).

On dit que a est *idempotent* lorsque toutes ses puissances ≥ 1 sont égales, ie lorsque $a^2 = a$. Exemple : $\cap$ et $\cup$, produit sur $\{0,1\}^A$.

On dit que a est *involutif* lorsque ses seules puissances sont a et 1, ie lorsque $a^2 = 1$. Exemple : tout entier relatif pour $-$, tout réel non nul pour le quotient.

Lorsque M a un absorbant ω, on dit que a est *nilpotent* si $\exists n \geq 1,\ a^n = \omega$. Le plus petit tel n est appelé l'*indice de nilpotence* de ω. On dit aussi que a est n-nilpotent. Exemple : le tapis roulant est n-nilpotent

PROP : *un produit de nilpotent qui commutent est nilpotent*
CEG : *deux tapis roulant en sens contraire*

EXO : *dans magma assoc fini, il y a un idempotent.*
Idée : si vrai, doit être vrai dans magman monogène. Alors on a plus généralement que tout morphisme (en particulier le carré) a un point fixe. On itère un point : $af(a) f^2(a) \cdots f^n(a)$ avec $f^{n+1}(a) = a$, d'où le produit fixe par f car tout commute.

RQ : lorsque les entiers font partie du magma, il pourrai y avoir confusion : dans Q/Z, $n\widetilde{\frac{a}{b}} \neq \widetilde{n}\widetilde{\frac{a}{b}}$!

1.2 Distributivité

Loi **distrib** : $a(x+y)$on distribue le a aux élémnet de la parethèse. En déduire $a(x_1+...+x_n)=...$ On **développe** = on a deux paquet $()()$ que l'on ouvre, et on met toutes les choses qu'ils contiennt devant nous (on a ax, puis ay, puis... le $+$ joue le role du "puis")

Exemples.
$\times$ sur $+$ sur N, Z, Q, R, C
$\div$ sur $-$ pas assoc
$\cap, \cup, \Delta$ sur $P(A)$ (associativité de Δ sur $\cap$= bon prétexte au transport de structures)
$\sqcup$ et $\times$ (si fait sens)
$\circ$ sur A^A et $\mathfrak{S}(A)$: premère lci assoc, neutre, pas com $\left(\left(X^X, \circ\right)\right.$ abélien $\implies S(X)$ abélien $\implies |X| \leq 2)$: pour l'inverse, dire retirer ses chaussurres puis ses chaussttes
pgcd ppcm sur $\times$ dans N ou Z (assoc, commu, neutre)
min et max sur $\times$ sur N, Q^+, R^+ (neutre et absorbant sur $[0,1]$)
$\wedge$ sur $+$ dans R^3 (pas assoc)

EXO (généralise $\cap$ et $\cup$ autodistributif)
Soit M mni de deux lois $\cdot$ et $*$ ayant chacune un neutre et dstribuitve l'une par rapport à l'autre. Montrer que tout élément est idempotent – pour chacune des lois
Soient $1^{\cdot}$ et 1^* les neutre. L'élément $1^* \cdot (1^{\cdot} * 1^*)$ se calcule d'une part en utilisant les propriéts des neutres

$$= 1^* \cdot 1^{\cdot} = 1^*$$

d'autre part en développant

$$= (1^* \cdot 1^{\cdot}) * (1^* \cdot 1^*) = (1^*) * (1^*)^{\cdot 2} = (1^*)^{\cdot 2}.$$

Ainsi, 1^* est idempotent. On en déduit pour tout $m \in M$:

$$m = m * 1^* = m * (1^* \cdot 1^*) = (m * 1^*)^{\cdot 2} = m^{\cdot 2}.$$

Le role des lois est symétriques, donc terminé.

Règle de calul.
Soit A muni d'une loi $+$ abélienne et d'une loi $\times$ unifère distributive sur $+$.
Soient $a_1, ..., a_n, b_1, ..., b_n \in A^n$ des éléments qui commutent. Notre but est de développer le produit $(a_1+b_1)(a_2+b_2)...(a_n+$
Que se passe-t-il si l'on développe naïvement ? On pioche dans chaque facteur a_i+b_i un terme a_i ou b_i, on fait le produit des n termes ainsi trouvés, ce qui donne un terme de la forme $\prod_{i\in I} a_i \prod_{j\in J} b_j$ avec $I \sqcup J = \{1, ..., n\}$: en effet, I correspond aux places des facteurs dans lesquels on a pioché un a_i, et J aux places des facteurs où l'on a pioché un b_j, ils forment donc une réunion disjointe de $\{1, ..., n\}$; noter que I ou J pourrait très bien être vide (cas où l'on ne pioche que des a_i ou que des b_j), puis on somme sur toutes les manières de piocher des a_i et des b_j, çàd sur toutes les façons d'écrire $\{1, ..., n\}$ comme réunion disjointe de deux partie $I \sqcup J$. On devrait donc trouver

$$\prod_{i=1}^{n} (a_i + b_i) = \sum_{\substack{I,J\subset\{1,..,n\} \\ I\sqcup J=\{1,..,n\}}} \prod_{i\in I} a_i \prod_{j\in J} b_j.$$

Proposition.
Soit $\overrightarrow{a}$ et $\overrightarrow{b}$ des n-uplets d'éléments de A qui commutent deux à deux. La formule ci-dessus est valide.

Démonstration.
Montrons cela par récurrence sur $n \geq 0$ (c'est naturel vue la forme du terme de gauche).
Pour $n = 0$, le produit de gauche est vide, donc vaut 1, et la somme de droite ne comporte qu'un seul terme correspondant à $I = \emptyset = J$ dont la réunion disjointe vaut $\{1, ..., 0\} = \emptyset$, ce terme étant un produit de deux produits vides, donc égal à 1.

Supposons le résultat vrai pour un $n \geq 0$. Soient a_0 et b_0 d'autres éléments de A qui commutent avec tout le monde. On écrit

$$\begin{aligned}\prod_{i=0}^{n}(a_i+b_i) &= (a_0+b_0)\prod_{i=1}^{n}(a_i+b_i) = (a_0+b_0)\sum_{\substack{I,J\subset\{1,\dots,n\}\\ I\sqcup J=\{1,\dots,n\}}}\prod_{i\in I}a_i\prod_{j\in J}b_j \\ &= \sum_{\substack{I,J\subset\{1,\dots,n\}\\ I\sqcup J=\{1,\dots,n\}}}\left(a_0\prod_{i\in I}a_i\right)\prod_{j\in J}b_j + \sum_{\substack{I,J\subset\{1,\dots,n\}\\ I\sqcup J=\{1,\dots,n\}}}\prod_{i\in I}a_i\left(b_0\prod_{j\in J}b_j\right).\end{aligned}$$

Faisons le changement de variables $A := I \cup \{0\}$ dans la première somme et $B := J \cup \{0\}$ dans la seconde. On obtient

$$= \sum_{\substack{A,B\subset\{0,\dots,n\}\\ 0\in A,\ 0\notin B\\ A\sqcup B=\{0,\dots,n\}}}\prod_{i\in A}a_i\prod_{j\in B}b_j + \sum_{\substack{A,B\subset\{0,\dots,n\}\\ 0\notin A,\ 0\in B\\ A\sqcup B=\{0,\dots,n\}}}\prod_{i\in A}a_i\prod_{j\in B}b_j.$$

Pour voir que l'on somme en fait sur tous les $A \sqcup B \subset \{0, ., n\}$, il suffit de partir de la somme souhaitée

$$\sum_{\substack{A,B\subset\{0,\dots,n\}\\ A\sqcup B=\{0,.,n\}}}\prod_{i\in A}a_i\prod_{j\in B}b_j$$

et de diviser la somme en deux parties, selon que $0 \in A$ ou $0 \in B$ (ces cas s'excluant mutuellement puisque $A \cap B = \emptyset$), ce qui nous fait retomber sur la grosse somme ci-dessus, *CQFD.*

Il serait aisé de montrer la généralisation suivante : si a_i^j sont np éléments qui commutent, où i décrit $\{1, ..., n\}$ et j décrit $\{1, ..., p\}$, alors

$$\prod_{i=1}^{n}\left(a_i^1 + a_i^2 + ... + a_i^p\right) = \sum_{\substack{I_1,\dots,I_p\subset\{1,\dots,n\}\\ I_1\sqcup\cdots\sqcup I_p=\{1,\dots,n\}}}\prod_{i\in I_1}a_i^1\prod_{i\in I_2}a_i^2 ... \prod_{i\in I_p}a_i^p.$$

Ceci résoud le problème du développement dans un anneau, à savoir comment transformer un produit de sommes en une sommes de produits.

1.3 création d'autres lois (induite ->sousmagama, partie, produit)

sous magma : partie tq loi induites lui donnet une sturcuter de magma.
EG : $\{e\}$ sous magama ssi e idempotent
EG : $2\mathbb{N}$ sous magama de $\mathbb{N}$ (la somem de deux enteirs et paires)
loi induites : quelle propriété passent ? assoc, commu, distrib, neutre absorbant et sym **s'ils sont déjà dedans** (écrire dans M et restreindre)

loi parties : $A \cdot B$: assoc, comm, neutre, absorbant
génerlament, pas d'ambuiguité, mais attetion à $\mathcal{A} \cup \mathcal{B}$ pour $\mathcal{A}$,$\mathcal{B} \subset \mathfrak{P}(E)$
plus génerleent, toute "loi" $A \times B \longrightarrow C$ induit une "loi partie" $\mathfrak{P}(A) \times \mathfrak{P}(B) \longrightarrow \mathfrak{P}(C)$.

loi produit : écrire en colonne $\begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} aa' \\ bb' \end{pmatrix}$, puis généraliser à $A_1 \times ... \times A_n$, puis à $\prod A_i$.
Tout passe coordonnée par coordonnée : assoc, commut, distrib, neutre, absorbant, symétrique. DE même pour les centres : $Z(\prod M_i) = \prod Z(M_i)$.

Si lci sur A, alors lci sur A^X : cas particulier de loi produit ($A_i = A\ \forall i$), donc toutes propriétés passent (assoc, commut, distrib, neutre, absorbant, symétrique).
Noter le morphisme de magma $A \hookrightarrow A^X$.

De même, produit de convolution sur l'anneau $\mathbb{R}^A$ ou $\mathbb{C}^A$, assoc car

$$[f_1 * ... * f_n](a) = \sum_{a_1...a_n=a} f(a_1)...f_n(a_n).$$

eg : produit de Dirichlet

$$f * g(n) = \sum_{dd'=n} f(d)\, g(d')$$

conjugaison par bijecion : si $f \in \mathfrak{S}_M$, alors $(a,b) \overset{*}{\mapsto} f^{-1}(f(a) f(b))$ est une loi qui hérite des prop de $\cdot$ (car f alors morphisme de $\cdot$ dans $*$)
EG : $a * b := ab + a + b = (a+1)(b+1) - 1$ dans R (ou R^{++})
EG : $a * b := ab - a - b + 2 = (a-1)(b-1) + 1$ dans R
EG : $a * b := \frac{a+b}{1+ab} = \operatorname{th}(\operatorname{ath} a + \operatorname{ath} b)$
EG : $a * b := \sqrt[3]{a^3 + b^3} = c^{-1}(c(a) + c(b))$ où $c = \sqrt[3]{\square}$
EG $A \Delta B = \chi^{-1}(\chi_A + \chi_B)$, d'où toutes les propriétés de Δ

partie/famille *génératrice*, système/famille de *générateur*, partie *monogène*, *sousmagma engendré*
EG : 1 est un générateur de $(N^*, +)$
EG : $\{2, 3\}$ est une partie génratrice de $(Z, +)$, $(3, 2)$ est une famille de génrateur

1.3.1 extrait cours TSI 1

Définitions (lois produit). Soient $(A, \sharp)$ et $(B, \dagger)$ deux magmas.
*On appelle **magma produit** de A par B le produit cartésien $A \times B$ muni de la l. c. i.*

$$\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} \alpha \\ \beta \end{pmatrix}\right) \mapsto \begin{pmatrix} a \sharp \alpha \\ b \dagger \beta \end{pmatrix} \qquad \textit{(appelée \textbf{loi produit} de } \sharp \textit{ par } \dagger\textit{).}$$

*Soit X un ensemble. On appelle **magma produit** A puissance X l'ensemble A^X muni de la l. c. i.*

$$(f, g) \mapsto \left\{ \begin{array}{ccc} X & \longrightarrow & A \\ x & \longmapsto & f(x) \sharp g(x) \end{array} \right. \qquad \textit{(appelée \textbf{loi produit} } \sharp \textit{ puissance } X\textit{).}$$

À RETENIR : *tout se passe indépendamment coordonnée par coordonnée.*

Exemples.
Le magma additif des complexes peut être vu comme le magma produit de $(\mathbf{R}, +)$ par lui-même.
Le magma additif $\mathbf{R}^I$ (où I est un intervalle de $\mathbf{R}$) est le magma produit $(\mathbf{R}, +)$ puissance I.

Notations. Soient A et B deux parties de M et soit $(\alpha, \beta) \in A \times B$. On note respectivement

$$A \sharp B := \{a \sharp b \ ; \ a \in A \text{ et } b \in B\}, \qquad \alpha \sharp B := \{\alpha \sharp b \ ; \ b \in B\} \qquad \text{et} \qquad A \sharp \beta := \{a \sharp \beta \ ; \ a \in A\}$$

l'image par $\sharp$ des produits cartésiens $A \times B$, $\{\alpha\} \times B$ et $A \times \{\beta\}$.

Exemples.

1. La notation $2\mathbf{N} + 1$ désigne l'ensemble des entiers naturels impairs ;
2. l'ensemble $2\pi\mathbf{Z}$ est formé des multiples entiers de 2π ;
3. on a l'égalité $\mathbf{R} + i\mathbf{R} = \mathbf{C}$;
4. on a l'égalité $\mathbf{R}\binom{1}{1} + \mathbf{R}\binom{1}{-1} = \mathbf{R}^2$;
5. on a l'inclusion $\mathbf{R}_- + \mathbf{R}_- \subset \mathbf{R}_-$.

1.4 Commutativité

commutant, centre, élméent ou partie *centrale*
commuter *avec / à*
$\mathrm{Comm}\,\langle A\rangle = \langle \mathrm{Comm}\,A\rangle$, donc pour appartenir au commutant d'une partie, il suffit de comuuter avec une partie génératrice.
Comm stable par inverse (si $xa = ax$, alors $x^{-1}xax^{-1} = x^{-1}axx^{-1}$, ie $ax^{-1} = x^{-1}a$)
comm unino = inter comm
comm décroissant
$A \subset \mathrm{Comm}\,\mathrm{Comm}\,A$ (égalité stricte en général) (pb du *bicommutant*)
$\mathrm{Comm}^3 A = \mathrm{Comm}\,A$ (en effet, $A \subset \mathrm{Comm}^2 A$, d'où par croissance $\mathrm{Comm}^3 A \subset \mathrm{Comm}\,A$)
si a_i finis comutetn 2 à 2, alors $\prod a_i$ indépendant de l'ordre choisi (dem par réc : clair pour aucun ou pour un élément, ensuite, $\prod_0^n a_{\sigma(i)} = ()\,a_0\,()\,() = a_0\,()\,() = a_0 \prod_1^n a_i = \prod_0^n a_i$)
Cor : assosciatiité du gros produit (choisi un ordre adapté à la partition)

EG : carré enteir uniion de singleton, partition en dorite verticales, horizontale ,diagonale

1.5 morphismes

homomorphisme= même forme =conserve la strucute

vision catégorielle /sagitale : morphissme ssi commute avec loi.
image $\mathrm{Im}\,f$
antimorphisme

EG : transliation γ_a δ_b (anti)morphisme
γ_a et δ_a commutaeten : le produit vaut $a \cdot a$
CEG : le produit n'est pas un morphisme (en général), mais oui si M commutatif

transport de structures : assos, commut, distrib, neutre, absorbant ?, symétrique. Eg : $\Delta\cap$ et $+\times$, exp pour $+\times$
la loi sur les parties induit un morphisme de $P\,(E)$.
exemple important du quotient, projection canonique.

soit f et g deux morphsime : Est-ce fg morphisme ? le calcul montre qu'il suffit que $\mathrm{Im}\,f$ et $\mathrm{Im}\,g$ commutent.

$\mathrm{End}\,M$ est un magma assos pour la composition, qui a un neutre (->monoide).

2 Monoïdes

la présence d'un neutre et de l'assoc est très agréable.
Abélien si commutatif
Rq : un produit de mono est nul ssi chq mono est nul (car chaque mono s'injecte dans le produit). —> cf. morsphismes ?
(vrai pour les magma, mais il semble nécessaire d'invoquerAC)

PEut plonger un magma M dans le monoïde M^M ?
EXO : *un magma M est assos ssi l'une de* $\begin{matrix} M \\ a \end{matrix}$ $\begin{matrix} M^M \\ a\,\mathrm{Id} \end{matrix}$ *ou* $\begin{matrix} M \\ a \end{matrix}$ $\begin{matrix} M^M \\ \square a \end{matrix}$ *est un morphisme.*
EXO *: l'application* $\begin{matrix} M \\ a \end{matrix}$ $\begin{matrix} M^M \\ a\,\mathrm{Id} \end{matrix}$ *est inj ssi un $m \in M$ est déterminé par son action multiplicative.*
Si pas inj, alors pas de simplifiable, donc pas de neutre. COR : *si neutre, alors injective* (CEG : les triplets descalaires de produit nuls)

Notatations factorielles : origine 1798 par C. Kramp (alors *faculté*) puis 1808 en mémoire de L. F. A. Arbogast

$a^{\downarrow n}$ puis $\binom{a}{n}$

$n!$ peut se prolonger à R^{++} par $\Gamma(x) := \lim_{n\infty} (n-1)! \frac{n^x}{x^{\uparrow n}}$ (Euler à Goldbach, 1729). Depuis Legendre, Γ s'appelle aussi *fonction eulérienne de seconde espèce*.

2.1 composé d'une famille

calcul dans un monoïde : on se donne un ensemble fini d'éléments que l'on veut composer.

cas simple : *itéré* d'un élément : on prolonge la définition de a^n par $a^0 = 1$, les lois usuelles sont prolongées.

En additif, l'itéré est noté na : on dit que l'on a une action de $\mathbb{N}$ sur A avec *neutre*, *associative* et distributive à gauche (attention, on n'a la distributiivté à droite seulement pour les monoïdes commutatifs).

On dit que a est *involutif* lorsque ses seules puissances sont 1 et lui-même, ie quand $a^2 = 1$. Exemple : Δ, produit sur $\{-1,1\}^A$, une symétrie axiale

Rq : itérer un élément est le premier moyen de créer de nouveaux objets dans un monoïde, y penser !

EXO : dans un monoïde **fini**, il y a toutjours un idempotent (déjà vu plus haut ? ? ?)

Cas général ! déjà, problème de l'ordre si pas commutatif -> mieux d'avoir un n-uplet $(a_1, ..., a_n)$, et le produit $a_1...a_n$ est noté $\prod_{i=1}^n a_i$. (défintino par itération : on prend $I := [1,n]$ comme partie de N, et on pose $f_k(x_1, ..., x_{k-1}) = x_1...x_{k-1}a_k$ pour $k = 1, ..., n$, d'où une suite $(u_i)_{i\in I}$ dont on prend le n-ième terme)

Si tout commute, on numérote les éléments de la famille puis on montre que le produit ne depend pas de la numéroation choisie –> $\prod_{i\in I} a_i$. Attention : indexation de la famille est comme toujours muette....

EG : si tous les a_i égaux, on retrouve $\prod_{i=1}^n a = a^n$ (en effet, la suite $u_i = a^i$ vérifie les condition souhaitées). Ainsi, on doit avoir $\prod_\emptyset = a^0 = 1$.

Par ailleurs, on a $\prod a^{n_i} = a^{\sum n_i}$ et $(\prod a_i)^n = \prod a_i^n$ si tous les a_i commutent.

On prolonge à famille ASF : $\prod_{i\in I} a_i := \prod_{i\in \mathrm{Supp}\, a_i} a_i$.

Pour composer les éléments d'un **enesemble** fini (au lieu d'une famille), on compose les éléments de la famille canoniqmeu asoic $\prod_{a\in A} a$.

Remarque : on aimerait prolonger la relation $\underset{A\sqcup B}{*} x_i = \left(\underset{A}{*} x_i\right) * \left(\underset{B}{*} x_i\right)$, $\emptyset$ est le neutre pour $\cup$, donc $\underset{\emptyset}{*}$ est le neutre pour $*$.

Exemples :
$\sum_\emptyset = 0$
$\prod_\emptyset = 1$
$\bigcup_\emptyset = \emptyset$
$\bigcap_\emptyset = E$
$\Delta_\emptyset = \emptyset$
$\max \emptyset = \min$, $\min \emptyset = \max$
$\underset{\emptyset}{*} = \{1\}$ (loi partie)

Explicter un $\sum$ ou un $\prod$, c'est écire tout les termes sans signe.

ATTENTION aux ... : toujours écrire suffisamment de termes pour que le motif soit clair (commencer par deux termes au moins). Et attenion à la composition –> démo foiruse par récurrence :

$$\frac{n(n+1)}{2} = 1 + 2 + ... + n = 1 + 2 + ... + (n-1) + 1 = \frac{n(n-1)}{2} + 1, \text{ d'où } n = 1\,!$$

thchangement d'indice : c'est jsute décrire autrement le domaine de compisiton, on le paramètre d'une autre façon (le paremètre est muet, il n'a aucun **aucune existence** endehors de sa fonction descriptive). Ex :
$\sum_{i=0}^4 = \sum_{j=1}^5 = \sum_{i=1}^5$ (quand on est grand, on fait $i \longleftarrow i+1$)
$\prod_{i=1}^5 \frac{i+1}{i} = \prod_{i=2}^6 \frac{i}{i-1}$
$\sum_{i=0}^n a_i b_{n-j} = \sum_{i+j=n} a_i b_j$
$\sum_{A_0\subset X} f(X) = \sum_Y f(A_0 \sqcup Y)$
soyez très large pour les notations, tant que c'est clair.

Théorème d'associativité (regroupement par paquets)
On partitionne le domaine de composition en paquets pertinents : appliation à $\cup$, $\cap$, $+$, $\times$.
partitino en droites de pentes $0, \infty, 1, -1$, en équerres ! ($\sum \min\{i,j\}$ et max, ou encore $(a_n + b_n)\prod_{i<n}(a_i + b_n)\prod_{i<n}(a_n + b_$
appl : produit de polynôme, exponentiels de nilpotents, inversion Pascal, liberté de $\{(X-a)^p (X-b)^q\}_{p+q=n}$.

Application : numérotation en base b :

$$\forall b \geq 2,\ \forall N \in \mathbb{N},\ \exists!\,(a_n) \in [0,b[^{(\mathbb{N})},\ N = \sum a_n b^n$$

2.2 régulier – inversibles – groupes

def de *réguliers* d/g (monoide *régulier* d/g) et *inversibles/symétrisable* d/g, *inverse/symétrique* d/g
RQ : a régulaier ssi γ_a / δ_a inj
EXO : *soit e régulier. Alors e neutre (bilatère) ssi e neutralise au moins un élt d'au moins un côté*
dem soit a tq $ae = a$. Appliquer $\cdot x$ et simplifier $a\cdot$ donne $ex = x$, puis appliquer $y\cdot$ et simplifir $\cdot x$ donne $ye = e$, d'où e neutre.

inversible d/g => régulierd/g.
involutif => inversible (EG : une petit équa fontionnelle ?)
Si assoc, inverse unique (marche pas biliaère : prendre des application)

on le note x^{-1} ou $\frac{1}{x}$.
attnteion à la notation $\frac{a}{b}$: elle peut signier à la fois $a\frac{1}{b}$ ou $\frac{1}{b}a$ et sera donc exclusivement réservée au cas où a et b commutent (on sait alors que a et $\frac{1}{b}$ commutent)
évidememnt, en addifi, on note $-x$ et on l'appelle l'*opposé.*

Théo : inv = inv gauche et inv droite (point subtil : un inv droite et un inv gauche coincident)
contre exemple : tapis roulant !

Argument classique et important :
pour un monoide **fini**, inversible équivaut à inversbile à droite/gauche, ou encore (plus faible) à régulier à droite/gauche

EG *Soit M magma fini. On supose qu'il y a un élément γ régulier à gauche et δ régulier à droite. Montrer que M est unifère.*
$a \mapsto \gamma a \delta$ est injective, donc surj, donc $\exists e \in A,\ \gamma\delta = \gamma e \delta$, d'où $e\delta = \delta$ et $\gamma e = \gamma$, donc $\gamma a = \gamma e a \implies a = ea$ et $a\delta = ae\delta \implies a = ae$, ie e unité.

PROP des inverses
$1^{-1} = 1$
$(ab)^{-1} = b^{-1}a^{-1}$ (enlever chaussettes / chaussures, tout ca)
$\left(a^{-1}\right)^{-1} = a$
(l'inversion est un *anti-morphisme* involutif)
si tous le monde commute, on a $\left(\prod a_i\right)^{-1} = \prod a_i^{-1}$.
puissance négative : si $a \in M^\times$, on note $a^{-n} = \left(a^{-1}\right)^n$. L'action de N se prolonge en une action de Z, toujours avec neutre, assoc, distrib à gauche

rq : si un absorbant est inversible, le monoide est trivial (ω vaut le neutre car il absorbe son inverse, donc tout x vaut $x1 = x\omega = \omega$)

exemples :
$(N,+) \longrightarrow \{0\}$
$(N,\times) \longrightarrow \{1\}$
$Z,Q,R,C,+ \longrightarrow Z,Q,R,C$
$Z,\times \longrightarrow \{\pm 1\}$

$Q, R, C, \times \longrightarrow Q^*, R^*, C^*$
$P(A), \cup \longrightarrow \{\emptyset\}$
$P(A), \cap \longrightarrow \{A\}$
$P(A), \Delta \longrightarrow P(A)$
N, max $\longrightarrow 0$
l'inverse de $\frac{a\Box+b}{c\Box+d}$ est $\frac{d\Box-b}{-c\Box+a}$
$A^A, \circ \longrightarrow \mathfrak{S}_A$ (en fait, inv à droite = régulier à droite = surj (pour $gf = hf \implies g = f$, utiliser $g = \chi_{\operatorname{Im} f}$ et $h = 1$), et idem pour gauche et injective)
$(\prod M_i)^\times = \prod M_i^\times$
loi parties –> $\{1\}$ (par unicité de l'inverse)
$\mathbb{C}^A, *$ ⟶difficile en général.

Un *groupe* est un monoïde où tout élément est inverisble, ie $G^\times = G$.
EG : parmi ci-dessus, Z, Q, R, C sont des groupes additif
CEG : sur R, $(a, b) \mapsto |a| b$ est assoc, unifère, inverse à droite, mais pas à gauche (les négatifs)
CEG : sur $\{1, a, b, c...\}$, on définit un table de multiplication commutative par

$$\begin{array}{c|ccccc} & 1 & a & b & c & \cdots \\ 1 & 1 & a & b & c & \cdots \\ a & a & 1 & 1 & 1 & \cdots \\ b & b & 1 & 1 & 1 & \cdots \\ c & c & 1 & 1 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

par construction, 1 est neutre, tout élément est involutif donc inversible. En revanche, on a

$$a(ab) = a1 = a \neq b = 1b = (aa)b,$$

donc pas d'assoc. D'ailleurs, on a une infinité d'inverses !!

EXO *magm fini régulier : monoide <=> groupe*
dem : soit a : les translations $a\cdot$ et $\cdot a$ sont inj, donc surj, donc atteingent 1, d'où des inverses des deux côtés qui coïncident par asso.
EXO *: un magma associatif régulier* ***fini*** *est un groupe (ne pas oublier l'unité...)*
dem : soit $a \in M$. l'app $a\cdot$ est inj, donc surj, donc atteitn a, disson $ae = a$. Lemme mq e neutre, atteinidre donc M monoïde régulier fini, donc groupe.
EXO *: un magma associatif où* $\exists a, b,\ \forall x, \exists x_d, x_g, xx_d = a, x_g x = b$ *est un groupe*
FAUX *:* a, b, x_d, x_g =absorbant !

EXO : *un magma assoc avec neutre à gauche et tout élément inversibles à gauche est un groupe/*
Idem si gauche <- droit, mais pas idem si g/d répartis (cf feuille groupe)

EG tordus
si G est un groupe, la loi $(a, b) \mapsto ab^{-1}$ le transforme en un magma non associatif (sauf si tous les élément sont involutifs, auquel cas on retrouve la loi de G), unifère à droite, dont tous les éléments sont involutifs (donc inversibles)
pour la loi $(a, b) \mapsto \left\lfloor \frac{a}{b+1} \right\rfloor$ sur R^+ de neutre à droite 0, fixons un $\alpha \in R$; tout réel de $[0, \alpha]$ est "inverse à droite" et tout réel de $[\alpha, \infty[$ est "inverse à gauche"
On consièdre le monoïde N^N usuel. Fixant un injection non surjective f (par exemple $a \mapsto 2a$) on construit des application f_n valant f^{-1} sur $\operatorname{Im} f$ et contante n ailleurs. Alors $f \circ f_n = \mathrm{Id}$, d'où une infinité d'inverse à droite. Mais aucun inverse à gauche car pas surjectve ! (en inversant les roles inj/surj, on inverse les roles de droite/gauche)

a et b sont *pseudo inverses* si $aba = a$ et $b = bab$. EG :
dans $\mathfrak{P}(E)$, à A fixé, les applications $\cup A$ et $\setminus A$.
dans les ensemble, $\mathfrak{P}$ et $\cup$
dans $\mathbb{N}$, les opérations $\Box + 1$ et $\max\{0, \Box - 1\}$
dans $\mathbb{C}$, $i\,\mathrm{Re}$ et Im (voir dans $\mathbb{R}^2$: tapis roulant $(a, b) \mapsto (0, a)\text{ou}(b, 0)$)

2.3 sous-monoide

sous-ensemble : toujours possible, mais est-ce que les lois induites donnent une structure identique ? –> *sous-monoide*. Exmple :
$\{1\}$ et $M \hookrightarrow M$
si $A \subset E$ alors $P(A) \hookrightarrow P(E)$ pour $\cap \cup \Delta$
$2\mathbb{N} \hookrightarrow \mathbb{N}$
$M^\times \hookrightarrow M$
$\mathrm{Comm}\, A \hookrightarrow M$
d'où $Z(M) \hookrightarrow M$
(exo : $Z\left(A^A\right) = \{\mathrm{Id}_A\}$, $Z(\mathfrak{S}(A)) = \{\mathrm{Id}_A\}$ pour $|A| \neq 2$)
les régulier forment un sousmonon (les inversibles aussi...)

N sous mono = N stable par composition finie = le composé de toute famille à support fini reste dans N, çàd

$$\forall (n_i) \in N^{(N)},\ \prod n_i \in N$$

subtil : le produit de la famille vide est le neutre !

Question : *est-ce partie stable ayant un neutre est un sous-mono ? (les neutres coincident-ils ?).* NON
Soit p un idempotent : alors $\{1, p\}$ est un monoïde et $\{p\}$ est une sous-partie stable.
Aussi,
Tu pars de n'importe quel monoïde A, tu lui ajoutes un nouvel élément e que tu forces à être le neutre (ça impose complètement sa multiplication, et l'associativité est triviale) : alors $M := A \sqcup \{e\}$est un monoïde qui a A comme sous-partie stable mais avec un neutre différent.
Autre réponse : N muni de max, $[0, 1]$ muni de max ou min (ou n'importe quel compact de R)

Parler un peu de morphisme de groupes
préserve la loi et l'inverse. Mais ce dernier est automatique.
vocabulaire : endo, auto, iso, mono, epi.
comment rendre le produit un morphsime ? avec un produit semi direct (en parler un peu)

2.4 morphismes

morphisme de mono : conserve la structure du mono = une loi et un neutre
notation : $\mathrm{Hom}(M, N)$, $\mathrm{End}(M)$. Eg : $\mathrm{Id}_M \in \mathrm{End}\, M$
prop : la composée de deux morphisme (lorsqu'elle existe) est un morphismes
cor : $\mathrm{End}\, M$ est un mono pour la composition

notion de sous mono passent bien aux images directes et réciproques

exos :
iso entre $N, +$ et $N^*, \times$? non, l'un est monogène et l'autre libre de base les premiers
$P(A)$ ok pour $\cup$ et $\cap$ via complémentaire
$P(A)$ pas ok pour $\cup$ ou $\cap$ (les duex sont iso, de toute façon) contre Δ : idempotent contre involutif !

3 action opération lce

3.1 defin exemple

Une *lce* sur A à *opérateurs* Ω est une applciation de Ω dans A^A : on notera $\omega \cdot a$ l'image d'un a par ω. On dira aussi qu'on a une *opération* ou *action* de Ω sur A, ou encore que Ω *opère* ou *agit* sur A. Une lce ets donc la donnée d'un Ω opérant/agissant sur A via $(\omega, a) \mapsto \omega \cdot a$.
action identité $\omega \cdot a = a$

actions constantes $\omega \cdot a = a_0$
Si A est muni d'une lci, A agit sur lui-même par multiplication (gauche ou droite).
Si A est un monoïde, N agit en itérant un élément donné.
actoin fonctionneell A^A agit sur A par $f \cdot a = f(a)$ (c'est la défiition pour $\mathrm{Id} : \Omega \hookrightarrow A^A$)
action par conjugaison : une partie A d'un groupe agit dessus par $a \cdot g = aga^{-1}$

3.2 associativité

L'action d'un **magma** Ω est dite associative si

$$\forall \omega, \omega' \in \Omega,\ \forall a \in A,\ \omega \cdot (\omega' \cdot a) = (\omega\omega') \cdot a.$$

C'est dire que l'action revient à un

$$\textit{morphisme de } \textbf{magmas } \Omega \longrightarrow A^A$$

Alors $[\omega \cdot (\omega' \cdot \omega'')] \cdot a = [(\omega \cdot \omega') \cdot \omega''] \cdot a$, donc du point de vue de l'action

OPS Ωassocitif

Exemple :
action identité
action constante
si A monoide, action par multiplication (à gauche !)
l'itération d'un élément par action de $(N, \times)$ est associative (jamais pour + sauf sur monoide trivial)
action fonctionnelle de A^A : $g \cdot (f \cdot a) = g(f(a)) = [g \circ f](a) = (gf) \cdot a$: c'est la définiton de la compositio
action d'une partie d'un groupe par conjugaison : $h\left(gag^{-1}\right) g^{-1} = (hg)\, a\, (hg)^{-1}$.

Footnote ; on aurait pu étudier l'assoc de l'action sur un monoïde,ie $\omega \cdot (ab) = (\omega \cdot a)\, b$, mais c'est beaucop moins intéressant (raison profonde : ne se formule pas en termes de morphises !) –> Exo :
action identité
action constante pas ok (sauf si $A = \{1\}$)
action par multiplication ok
action par itératoin : si A commutatif, pas ok (sauf si $A = \{0\}$) ;
action fonctionnelle pas ok du tout (sauf si $A^A = \{\text{homothéties}\}$)
conjugasion pas ok du tout (sauf si $A \subset Z(G)$)

3.3 neutre

Une lce a un *neutre*, généraemnt noté 1, si

$$\forall a \in A,\ 1 \cdot a = a.$$

Exmple :
tout opérateur est neutre pour l'action identité
l'action constante n'a pas de neutre (sauf si $|A| \leq 2$).
Si A agit sur lui-mêm via une lci, un neutre de l'action est un neure pour la lci.
L'action de N par itération admet 1 pour neutre.
Id unique neutre de l'action fonctionelle de A^A sur A.
être neutre pour la conjugaion, c'est commuter avec tous le monde ; ainis, les neutres pour l'action de conjugaision de A sur G sont $A \cap Z(G)$

MAGMA + NEUTRE = MONOIDE

Soit l'action d'un *magma* M. SOit u un neutre : alors $mu \cdot a = m \cdot a = um \cdot a$m, donc du pit de l'action

OPS M monoïde.

(rq : on peut aussi quotienter M par $\left(\operatorname{Ker} M \longrightarrow A^A\right)$)

De fait, si M monoide, alors demander "$\exists$ neutre" équivaen à ce que 1_M soit neutre, ie àce que

l'action $M \longrightarrow A^A$ *soit morphisme de* **monoïdse**

–> Prop : *Soit* $\cdot$ *l'action associative d'un monoïde* Ω. *S'il y un neutre (ou plus généralement si* $\cdot$ *est surjective), alors il y a au moins* 1_Ω. *Si action sur au moins un point est injective, alors il y a au plus un neutre.*

Cor : *si l'action sur au moins un point est bijective, alors* 1_Ω *est neutre et le seul.*

Ainsi, les exemples des neutre 1 de l'action du monoïde $(N, \times)$ et de Id de l'action de A^A se généralisent :

MAGMA + NEUTRE+ INVEB = GROUPE

Un action de monodîde se restrein aux inversible en une action $M^\times \longrightarrow \mathfrak{S}_A$.

Ainsi, une action *de groupe* sur A est la donnée d"un morphisme $G \longrightarrow \mathfrak{S}_A$ (acton d'un groupe G qui est associative et qui admet un neutre)

Exemple : la multplication à gauche ou la conjugaison dans un groupe, S_A sur A. Plus générament, sI G agit sur A, on dit que deux éléments de G sont *conjugués* s'ils dans une même orbite..

RQ ORBITES : disons b est un conjugé de a si $b \in M \cdot a$. Alors :
réf <=> $\forall a,\ \exists u_a,\ u_a a = a$ ok si neutre
sym <=> de $b = m \cdot a$ on aimeirait inverser $a = ?b$ ok si inversisble
transi : de $c = nb$ et $b = ma$ on a $c = n\,(ma) = ? \cdot a$, ok si assoc
CONCLUSION : la structure de groupe est bien pratique pour que les orbites partitionnent

3.4 distributivité

On suppose que Ω et A sont des monoïdes. L'action de Ω est dite *distributive* si

$$\begin{aligned} \omega \cdot (ab) &= (\omega \cdot a)\,(\omega \cdot b) \text{ (distributive à gauche / vers la droite)} \\ (\omega\omega') \cdot a &= (\omega \cdot a)\,(\omega' \cdot a) \text{ (distributive à droite / vers la gauche)} \end{aligned}$$

cela 'sécrit aussi en termes de diagrrammes commutatifs.

Disucsison droite/gauche : le côté désigne celui de *ce qui* est distribuable ω, ou bien celui *vers lequel* on distribue le ω ?

EXEMPLES
l'action de $\{\mathrm{Id}\}$ sur A est distributive à gauche, mais pas à droite en général (sauf si tous est idempotent)
l'action constante $= 1_A$ est distributive
l'action de $(N, \times)$ par itération est distributive à gauche, jamais à droite(sauf si $A = \{1\}$)
l'action de $(N, +)$ par itération est distributive à droite, jamais à gauche (sauf si $A = \{1\}$)
Dans un anneau, l'action par multiplication sur $(A, +)$ est distribtive
l'action de A^X sur A est distributive à droite, mais pas à gauche(sauf si tout est additif)
l'action d'un groupe sur lui-même par conjugaison est distributive à gauche **(important)** mais pas à droite (cela dit, on peut toujours définir une congujuasion $g \cdot a = a^{-1}ga$ qui soit une action à droite)

rq : distrib à gauche s'écirt multiplicaiton à gauche par ω qcq est un morphisme (de monoïdes), çàd action $\Omega \longrightarrow A^A$ arrive dans $\operatorname{End} A$
distrib à droite s'écirt multiplication à droite par a qcq est un morphisme (de monoïdes) : ? ? ?
★distrib s'écirt "la multiplication $\cdot$ est un morphisme" : ça devrait être automatique !

BILAN sur une strucure S
Action de magma : morphsime de magmas $M \longrightarrow \operatorname{End} S$
Action de monoide : morphsime de monoides $M \longrightarrow \operatorname{End} S$
Action de groupe : morphsime de grupe $M \longrightarrow \operatorname{Aut} S$ (<= suffit action magma !)

3.5 Morphismes ? ?

Appelons momentanément Ω-ensemble tout ensemble sur lequel agit Ω.

Soit A vers B deux Ω-ensembles. Un Ω-*morphisme* (ou morphisme d'Ω-ensembles) de E vers F est une application $f : A \longrightarrow B$ telle que

$$f(\omega \cdot a) = \omega \cdot f(a)$$

On parle également d'*application (Ω-)homogène*, et on dit encore que f préserve/respecte.conserve l'action de Ω.

Plus génréalement, si A est un Ω-ensemble, A' un Ω'-ensemble, et si $\rho : \Omega \longrightarrow \Omega'$est une applciation, on appelle ρ-morphisme tout $f : A \longrightarrow A'$ telle que

$$f(\omega \cdot a) = \omega' \cdot f(a).$$

EG :
action identité : tout $f \in B^A$ est homogène
actions constantes : un $f \in B^A$ est homogène ssi $f(a_0) = b_0$ où a_0, b_0 sont les constantes de l'action
Si A magma agit sur lui-même par multiplication (gauche ou droite), un $f \in A^A$ est homogène ssi homothéie
actoin de A^A sur A par $f \cdot a = f(a)$; un A^A-morphisme est une aplication commutant avec tout tle monde

4 lois et relations : compatibilité

Soit M un magama relié par R. Notons

$$\begin{array}{l} \overrightarrow{a} := \{m \in M \ ; \ aRm\} \\ \overleftarrow{a} := \{m \in M \ ; \ mRa\} \end{array} \text{ abrégé en } \overline{a} \text{ lorsque } = \text{ (çàd quand } R \text{ symétrique)}$$

PRop. *R est compatible avec la loi de M ssi $\overrightarrow{a} \cdot \overrightarrow{b} \subset \overrightarrow{ab}$ ou ssi $\overleftarrow{a} \cdot \overleftarrow{b} \subset \overleftarrow{ab}$.*

** Dans ce cas, si de plus $\begin{array}{c} M \text{ est un groupe} \\ R \text{ est réflexive} \end{array}$, on a alors l'inclusions réciproque (et donc les égalités $\overrightarrow{a} \cdot \overrightarrow{b} = \overrightarrow{ab}$ et $\overleftarrow{a} \cdot \overleftarrow{b} = \overleftarrow{ab}$)*

** si $\begin{array}{c} M \text{ monoïde,} \\ N \text{sm distingué} \end{array}$ et aRb ssi $aN \ni b$, alors $\overrightarrow{a}\,\overrightarrow{b} = \overrightarrow{ab}$*

DEM => On a les inclusions $\overrightarrow{a} \cdot \overrightarrow{b} = \{m \cdot n \ ; \ aRm \text{ et } bRn\} \subset \{o \ ; \ abRo\} = \overrightarrow{ab}$ idem de l'uatre côté

<= suppososn $\begin{array}{c} aR\alpha \\ bR\beta \end{array}$. Alors $\alpha\beta \in \overrightarrow{a}\,\overrightarrow{b} \subset \overrightarrow{ab}$, d'où $abR\alpha\beta$

Supposons M groupe et R ref. On a alors les inclusions $\overleftarrow{ab} \overset{M \text{ gpe}}{=} \left(\overleftarrow{ab}b^{-1}\right) b \overset{\text{compatib}}{\subset} \left(\overleftarrow{(ab)\,b^{-1}}\right) b = \overleftarrow{a}\,b \overset{\text{réf}}{\subset} \overleftarrow{a}\,\overleftarrow{b}$ (idem autre côté).

Supposons $\begin{array}{c} M \text{ monoïde,} \\ N \text{sm distingué} \end{array}$, aRb ssi $aN \ni b$. Alors $\overrightarrow{a} = aN = Na$). On obtient $\overrightarrow{a}\,\overrightarrow{b} = aNbN = abNN = abN = \overrightarrow{ab}$

Question : ces deux cas ont-ils un rapport ? ? ? ? ?

Soit $\sim$ une relation d'équivalence sur un monoïde M. Les classes modulo $\sim$ sont des parties de M, donc on peut regarder leur produit pour la loi de M :

$$\overline{a} \cdot \overline{b} = \{\alpha\beta\}_{\beta \sim b}^{\alpha \sim a}.$$

On aimerait bien pouvoir écrire $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$, ce qui revient à dire que la projection canonique $M \twoheadrightarrow {}^{M}\!/_{\sim}$ est un morphisme, mais cette relation n'a a priori rien d'évident. Pour éclairer la subtilité, écrivons plutôt cette identité sous la forme $A \cdot B = \overline{a \cdot b}$ où a est **un** représentant de la classe A et de même $b \in B$: qui nous dit que le résultat est indépendant des représentants a et b choisis ? Le problème revient donc à montrer que $\begin{cases} \forall a, a' \in A \\ \forall b, b' \in B \end{cases}$, $\overline{ab} = \overline{a'b'}$. Précisons cela.

Analyse.

Supposons la relation $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ valable pour tous $a, b \in M$. Si l'on prend d'autres représentants $a' \sim a$ et $b' \sim b$, on devra avoir

$$\overline{ab} = \overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'} = \overline{a' \cdot b'}, \text{ d'où } ab \sim a'b'.$$

Synthèse.

On part de la condition $\forall a, b \in M, \left\{ \begin{array}{c} a \sim a' \\ b \sim b' \end{array} \right. \implies ab \sim a'b'$. Montrons alors l'égalité des classes $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ pour a et b deux élements fixés dans M.

D'une part, un élément $m \in \overline{a} \cdot \overline{b}$ s'écrit $\alpha \cdot \beta$ où $\alpha \sim a$ et $\beta \sim b$, d'où l'équivalence $m = \alpha\beta \sim ab$, ce qui s'écrit aussi $m \in \overline{ab}$.

D'autre part, un élément $m \in \overline{ab}$ s'écrit $a\left(a^{-1}m\right)$ avec $a^{-1}m \sim a^{-1}(ab) = b$, donc est de la forme $\alpha\beta$ avec $\alpha := a \sim a$ et $\beta := a^{-1}m \sim b$, donc appartient à $\overline{a} \cdot \overline{b}$.

Conclusion : la projection canonique $M \twoheadrightarrow {}^{M}\!/_{\sim}$ est un morphisme ssi

$$\forall a, b \in M, \left\{ \begin{array}{c} a \sim a' \\ b \sim b' \end{array} \right. \implies ab \sim a'b'.$$

On dit alors que la relation d'équivalence $\sim$ et la loi $\cdot$ sont *compatibles*, et que $\sim$ est une *relation de congruence* pour la loi $\cdot$. Les relation de congruences sont usuelleement notées par le symbole $\equiv$. Par exemple, sur le monoïde $(\mathbb{N}, +)$, la relation de congruence modulo un entier $n \geq 1$:-)

5 Symétrisation d'un monoïde

5.1 Cas abélien ♮

Soit $(M, +)$ un monoïde abélien, à l'instar de $(\mathbb{N}, +)$. On veut en faire un groupe, que nous noterons $M^{\natural}$ et appellerons le *symétrisé* de M. Il s'agit donc rajouter les opposés des éléments qui n'en admettraient pas. On pensera au passage de $\mathbb{N}$ à $\mathbb{Z}$: comment construire ce dernier ?

Analyse heuristique.

$M^{\natural}$ doit contenir les différences $a - b$ pour a et b décrivant M, deux différences $a - b$ et $a' - b'$ donnant le même "objet" ssi $a - b = a' - b'$, *i.e.* ssi $a + b' = a' + b$. Ainsi, si l'on définit une relation d'équivalence sur M^2 par

$$(a, b) \equiv (a', b') \iff a + b' = a' + b,$$

alors la classe de (a, b) va représenter la différence $a - b$ (on peut imaginer un couple avoir-dette), tandis que les $a \in M$ seront représentés par les $\overline{(a, 0)}$ vu comme différences $a - 0$. On a donc un bon candidat, $M^{\natural} := {}^{M^2}\!/_{\equiv}$, dans lequel on trouvera une copie de M comme image du morphisme de monoïdes $a \mapsto \overline{(a, 0)}$.

Synthèse.

Vérifions que $\equiv$ est une relation d'équivalence. Elle est clairement réflexive et symétrique. Cependant, pour la transitivité, on a beson de simplifier, ce qui a priori n'est pas autorisé. Pour tenir compte des éléments non réguliers, on va modifier $\equiv$ en posant

$$(a, b) \equiv (a', b') \overset{\text{déf.}}{\iff} \exists m \in M,\ a + b' + m = a' + b + m.$$

Ainsi, la transitivité se passe bien :

$$\begin{array}{rcl} \left\{ \begin{array}{c} (a, b) \equiv (a', b') \\ (a', b') \equiv (a'', b'') \end{array} \right. & \implies & \exists m, n \in M, \left\{ \begin{array}{c} a + b' + m = a' + b + m \\ a' + b'' + n = a'' + b' + n \end{array} \right. \\ & \implies & (a + \underline{b' + m}) + (\underline{a'} + b'' + n) = (\underline{a'} + b + \underline{m}) + (a'' + \underline{b'} + n) \\ & \implies & a + b'' + x = b + a'' + x \text{ (avec } x := a' + b' + m) \\ & \implies & (a, b) \equiv (a'', b'')\,. \end{array}$$

Vérifions que $\equiv$ est bien compatible pour la loi de M^2, ce qui justifiera *a posteriori* sa notation comme une relation de congruence :

$$\begin{array}{lll}
\left\{\begin{array}{l}(a,b)\equiv(a',b')\\(c,d)\equiv(c',d')\end{array}\right. & \Longrightarrow & \exists m,n\in M,\ \left\{\begin{array}{l}a+b'+m=a'+b+m\\c+d'+n=c'+d+n\end{array}\right.\\
& \Longrightarrow & (a+b'+m)+(c+d'+n)=(a'+b+m)+(c'+d+n)\\
& \Longrightarrow & (a+c)+(b'+d')+m+n=(a'+c')+(b+d)+m+n\\
& \Longrightarrow & (a+c,b+d)\equiv(a'+c',b'+d')\\
& \Longrightarrow & (a,b)+(c,d)\equiv(a',c')+(b',d')\text{, } CQFD.
\end{array}$$

On pourra observer que toutes les classes $\overline{(a,a)}$ sont nulles (elles doivent correspondre aux différences $a-a$) :

$$(a,a)\overset{?}{\equiv}(0,0)\iff\exists m,\ a+0+m\overset{?}{=}a+0+m\impliedby a\overset{?}{=}a,\ ok.$$

La loi du monoïde M^2 passe donc au quotient $M^\natural$, de neutre $\overline{(0,0)}$, dans lequel M s'envoie par $\left\{\begin{array}{ccc}M&\longrightarrow&M^\natural\\a&\longmapsto&\overline{(a,0)}\end{array}\right.$.

Il est aisé de constater que tous les éléments de $M^\natural$ admettent un opposé donné par $-\overline{(a,b)}=(b,a)$:

$$\overline{(a,b)}+\overline{(b,a)}=\overline{(a+b,b+a)}=\overline{(a+b,a+b)}=\overline{(0,0)}.$$

$M^\natural$ est donc bien un groupe abélien. Par ailleurs, en identifiant (plus qu'abusivement) les éléments de M à leur image dans $M^\natural$, tout élément de $M^\natural$ s'écrit sous la forme

$$\overline{(a,b)}=\overline{(a,0)}+\overline{(0,b)}=\overline{(a,0)}-\overline{(b,0)}=a-b,$$

ce qui était précisément la description recherchée du symétrisé de M.

Attention, l'injectivité de ce morphisme est mise en défaut par les monoïdes non réguliers ! Par exemple, tous les idempotents disparaissent : ainsi, le monoïde $\{1,p\}$ où p est un idempotent se symétrise en $\{1\}$, puisque p devient $\frac{p}{1}=\frac{p^2}{p}=\frac{p}{p}=1$. Plus précisément, vues les équivalences

$$\overline{(a,0)}=\overline{(b,0)}\iff\exists m,\ a+m=b+m,$$

on peut affirmer que

$$M\hookrightarrow M^\natural\ \textit{ssi}\ M\ \textit{est régulier.}$$

Enfin, il serait bon de vérifier que $M^\natural=M$ lorsque M est déjà un groupe : dans ce cas, M s'identie à son image $\left\{\overline{(m,0)}\right\}_{m\in M}$ dans $M^\natural=\left\{\overline{(a,b)}\right\}_{a,b\in M}=\left\{\overline{(a-b,0)}\right\}_{a,b\in M}$. Réciproquement, étant un $a\in M$, si on peut dire que $\overline{(0,a)}$ est atteint par un élément de M, mettons $\overline{(m,0)}=\overline{(0,a)}=-\overline{(a,0)}$, alors $\overline{(a+m,0)}=\overline{(0,0)}$, d'où par injetivité a symétrisable. On en déduit l'équivalence

$$M\widetilde{\longrightarrow}M^\natural\ \textit{ssi}\ M\ \textit{est un groupe.}$$

Application.

On pose $\mathbb{Z}:=\mathbb{N}^\natural$ muni de sa structure d'anneau ordonné. En notant $m:=\min\{a,b\}$ et $\left\{\begin{array}{l}a'=a-m\\b'=b-m\end{array}\right.$, les entiers a' et b' sont dans $\mathbb{N}$, l'un des deux au moins est nul, de sorte que toute différence $a-b$ de $\mathbb{Z}$ s'écrit $a'-b'=a'$ ou $-b'$. Ainsi, tout entier relatif est un entier naturel ou l'opposé d'un entier naturel. La terminologie *symétrisé* prend ici tout son sens (et resterait valide sur tout monoïde totalement ordonné).

5.2 Cas non abélien ♯

qd M anabélien, l'ensembel ds différences $a-b$ n'eest plus stable par somme -> il faut les mettre bout à bout.

on passe en notation multiplicatives.

(cf exos lois pour détails où l'on inverse seulement une partie du monoïde)

Analyse ; si $M\hookrightarrow G$gpe, G contient les élemtnde M et leur inverses, donc les produit ab^{-1} pour $a,b\in M$, donc vaut le sg engendré par ces derniesr, dont les élément sont $a\alpha^{-1}b\beta^{-1}c\gamma^{-1}...z\omega^{-1}$. Il y a des simplifications

possible : au sein d'un même produit on peut simplifier $(a\lambda)\,\lambda^{-1} = a1^{-1}$ et $\mu\,(a\mu)^{-1} = 1a^{-1}$, et d'un produit au suivant $\left[ab^{-1}\right]\left[(bx)\,y^{-1}\right] = (ax)\,y^{-1}$.

Synthèse : on code ab^{-1} par un couple $\binom{a}{b}$ (penser à l'écriture $\left(\frac{a}{b}\right)$ d'un fraction). Alors le produit de tels élmetns est un mot fini (non vide) $\begin{pmatrix} a & b & c & \cdots & z \\ \alpha & \beta & \gamma & \cdots & \omega \end{pmatrix}$sur l'alphabet M^2. On impose les identification $\binom{\lambda}{\lambda} = \binom{1}{1}$ et $\binom{m\ sn}{s\ \ t} = \binom{mn}{t}$ (dont vont découler les autres)

Propprement, on dit que deux mots a et b sur M^2 sont équivalents (et on note $a \equiv b$) s'il y a une suite finie $a = w_1 \sim w_2 \sim \cdots \sim w_n = b$ de mots où $\sim$ désigne l'une des deux transformations ci-dessus (ref sym trans). Vérifions que la concat est compatible[2] avec $\equiv$. Déjà, si $a \sim a'$, alors $ab \equiv a'b$ (faire la même transfo), d'où en itérant $a \equiv a' \Rightarrow a \sim a_1 \sim a_2 \sim \cdots \sim a_p = a' \Rightarrow ab \equiv a_1 b \equiv a_2 b \equiv \cdots \equiv a_p b = a'b$. On ferait de même en concaténant à gauche, *CQFD*. On note alors $\frac{a}{b}$ la classe d'un couple $\binom{a}{b} \in M^2$, ce qui permet d'écrire tout élément de $M^\sharp$ sous la forme$\frac{a}{\alpha}\frac{b}{\beta}\frac{c}{\gamma}\cdots\frac{z}{\omega}$ (attention à l'ordre : pas possible de regrouper).

Lorsuqe M abélien, mq les deu symétrisés $M^\sharp$ et $M^\natural$sont isomorphes.

On essaie de poser $\begin{array}{ccc} \frac{a}{\alpha}\frac{b}{\beta}\frac{c}{\gamma}\cdots\frac{z}{\omega} & \longmapsto & \overline{\binom{abc\cdots z}{\alpha\beta\gamma\cdots\omega}} \\ \frac{a}{\alpha} & \longleftarrow & \overline{\binom{a}{\alpha}} \end{array}$. Pour mq $\longmapsto$ bien def, on montre que deux mot différant d'*une* simplifcation ont même image. Pour mq$\longleftarrow$ bien def, on vérife $\binom{a}{\alpha} \equiv \binom{b}{\beta} \implies \exists m, a\beta m = \alpha b m \implies \frac{a}{\alpha} = \frac{a\beta m}{\alpha\beta m} = \frac{\alpha b m}{\alpha\beta m} = \frac{b}{\beta}$

$M^\sharp$ est groupe : $\frac{1}{1}$ neutre ($\frac{a}{b}\frac{1}{1} = \frac{a}{b}\frac{b}{b} = \frac{a}{b}$ et $\frac{1}{1}\frac{a}{b} = \frac{a}{a}\frac{a}{b} = \frac{a}{b}$) et inverse ($\frac{a}{b}\frac{b}{a} = \frac{1}{1}$ (idem autre sens par symétrie))

La flèche $a \mapsto \frac{a}{1}$ est un morphisme (cf exos lois pour détail)

M régulier si $M \hookrightarrow M^\sharp$: soient a, b, m tq $am = bm$, alors $\frac{a}{1} = \frac{am}{m} = \frac{bm}{m} = \frac{b}{1}$ donc $a = b$ (<= semble délicate)

EG d'élémént indistingualbe ? Groupifier tue les idempotents : $i = i^2 \Rightarrow \frac{i}{1} = \frac{i^2}{i} = \frac{i}{i} = \frac{1}{1}$.

$M \widetilde{\longrightarrow} M^\sharp$ ssi M groupe : si M groupe, la fléèche est injective et tout élément de $M^\sharp$ est $\frac{a}{b} = \frac{a}{b}\frac{b^{-1}}{b^{-1}} = \frac{ab^{-1}}{1} \in$ Im. <= par surj, tout $\binom{1}{b}$ est un $\binom{1}{a}$, d'où $\frac{ab}{1} = \frac{a}{1}\frac{b}{1} = \frac{1}{b}\frac{b}{1} = \frac{1}{1}$ et (par inj) $ab = 1$ et $a = b^{-1}$.

Rq : $M^\natural = \{0\}$ *dès que M contient un absorbant* (car l'absorbant vu dans le groupe $M^\natural$ets inversible

EG : $L(E)$ pour $\circ$, $\mathfrak{P}(A)$ pour $\cup$

5.3 Cas des bioïdes

Si M était muni d'une autre loi, disons multiplicative et distributive par rapport à $+$, on aimerait bien prolonger cette dernière au quotient $M^\natural$ par la formule

$$(a-b)\,(\lambda-\mu) := a\lambda - a\mu - b\lambda + b\mu,$$

utilisant implicitement la structure souhaitée d'anneau sur $M^\natural$ et le fait que le morphisme $M \longrightarrow M^\natural$ soit multiplicatif.

Pour obtenir cela, il est nécessaire de pouvoir écrire (on note avec un prime l'image par la flèche $M \longrightarrow M^\natural$)

$$\overline{(a,b)}\times\overline{(\lambda,\mu)} = (a'-b')\left(\lambda'-\mu'\right) \overset{\text{distributivité}}{=} a'\lambda' - a'\mu' - b'\lambda' + b'\mu' \underset{\text{un morphisme}}{\overset{\text{la flèche est}}{=}} (a\lambda+b\mu)' - (a\mu+b\lambda)' = \overline{(a\lambda+b\mu, a\mu+b\lambda)}.$$

Ainsi, la loi sur M^2 définie par

$$\binom{a}{b} * \binom{\lambda}{\mu} := \binom{a\lambda+b\mu}{a\mu+b\lambda}$$

doit pouvoir passer au quotient et définir la multiplication sur $M^\natural$. Par ailleurs, un élément $\lambda\,(a+b)$ est envoyé sur $\lambda'\,(a'+b') = \lambda'a' + \lambda'b' = (\lambda a + \lambda b)'$, donc la multiplication de M est distributive sur $+$ "modulo régularité". Enfin, $\overline{\binom{ab}{0}} = \overline{\binom{a}{0}}\overline{\binom{b}{0}} = \overline{\binom{ab+0^2}{a0+0b}}$ implique $0^2 = 0a + 0b$ pour tout a, b moduo régularité, d'où 0 absorbant mod régularité.

[2] **Rq utile** : sur un ensemble de mot, si une reltaion remplace des lettres avec une fonction de *ces* lettres, alors cette relation est compatible avec la concat (ya rien à faire :tout se passe "localement")

Montrons que, sous ces deux dernières hypothèses, la loi $*$ ci-desssus est bien compatible avec $\equiv$ et induit une multiplication sur $M^\natural$ distributive sur sa somme qui fait de la flèche $M \longrightarrow M^\natural$ un morphisme de bioïdes.

Supposons $\times^\natural$ bien définie. Pour montrer sa distributivité, il suffit de vérifier celle de $*$ est distribtive sur $+$, puis de tout envoyer par transport de structure via la projection canonique. Or, il vient

$$\begin{aligned}
\alpha * (\beta + \gamma) &= (a,b) * (p+q, x+y) \\
&= (ap+aq+bx+by, bp+bq+ax+ay) \\
&= (ap+bx, ax+bp) + (aq+by, ay+bq) \\
&= (a,b)*(p,x) + (a,b)*(q,y) \\
&= \alpha*\beta + \alpha*\gamma
\end{aligned}$$

et pareillement de l'autre côté.

Fixons $\alpha, \beta, \alpha', \beta'$ dans $M^\natural$ et montrons les implications $\begin{array}{l} \alpha \equiv \alpha' \implies \alpha*\beta \equiv \alpha'*\beta \\ \beta \equiv \beta' \implies \alpha*\beta \equiv \alpha*\beta' \end{array}$. Ceci entraînera les implications $\left\{ \begin{array}{l} \alpha \equiv \alpha' \\ \beta \equiv \beta' \end{array} \right. \implies \alpha*\beta \equiv \alpha'*\beta \equiv \alpha'*\beta'$, *CQFD.* (Lorsque $\times$ commute, so does $*$ et il n'y a qu'une implication à vérifier). On a d'une part

$$\begin{array}{rl}
& \alpha \equiv \alpha' \iff (a,b) \equiv (a',b') \iff \exists m,\ a+b'+m = a'+b+m \\
\overset{\times\lambda \text{ et } \times\mu}{\implies} & \exists m,\ (a+b'+m)\,\lambda = (b+a'+m)\,\lambda \text{ et } (a+b'+m)\,\mu = (b+a'+m)\,\mu \\
\overset{\text{somme}}{\implies} & \exists m,\ (a+b'+m)\,\lambda + (b+a'+m)\,\mu = (a+b'+m)\,\mu + (b+a'+m)\,\lambda \\
\overset{\substack{\text{distributivité} \\ \text{mod. régularité}}}{\implies} & \exists m,x,y,\ [a\lambda+b\mu] + [a'\mu+b'\lambda] + \underline{mc+md+x+y} = [a\mu+b\lambda] + [a'\lambda+b'\mu] + \underline{mc+md+x+y} \\
\implies & (a\lambda+b\mu, a\mu+b\lambda) \equiv (a'\lambda+b'\mu, a'\mu+b'\lambda) \\
\iff & (a,b)*(\lambda,\mu) = (a',b')*(\lambda,\mu) \\
\iff & \alpha*\beta \equiv \alpha'*\beta,
\end{array}$$

d'autre part

$$\begin{array}{rll}
\beta & \equiv & \beta' \implies (c,d) \equiv (c',d') \implies \exists m,\ c+d' = c'+d \\
& \implies & \exists m,\ a\,(c+d'+m) = a\,(d+c'+m) \text{ et } b\,(c+d'+m) = b\,(d+c'+m) \\
& \implies & \exists m,\ a\,(c+d'+m) + b\,(d+c'+m) = b\,(c+d'+m) + a\,(d+c'+m) \\
& \implies & \exists m,\ [ac+bd] + [bc'+ad'] + \underline{am+bm} = [bc+ad] + [ac'+bd'] + \underline{am+bm} \\
& \implies & (ac+bd, bc+ad) \equiv (ac'+bd', bc'+ad') \\
& \implies & (a,b)*(c,d) = (a,b)*(c',d') \\
& \implies & \alpha*\beta \equiv \alpha*\beta'.
\end{array}$$

Enfin, on vérifie $\overline{\binom{a}{0}}\overline{\binom{b}{0}} = \overline{\binom{ab+0^2}{a0+0b}} \overset{?}{=} \overline{\binom{ab}{0}}$ ssi $\exists m,\ ab+0^2+0+m = ab+a0+0b+m$, ok par absorbance mod rég.

5.4 Prolongement de l'ordre

Enfin, si M était ordonné par $\leq$ compatible avec l'addition, au sens où

$$\forall m \in M,\ a \leq b \iff a+m \leq b+m,$$

toute relation d'ordre sur $M^\natural$ prolongeant $\leq$ devrait vérifier

$$a-b \leq a'-b' \iff a+b' \leq a'+b,$$

ce qui incite à poser la relation suivante sur M^2, destinée à passer au quotient :

$$(a,b) \leq (a',b') \iff a+b' \leq a'+b.$$

La réflexivité est claire et la transitivité se traite comme celle de $\equiv$ (bien noter que l'on a besoin de "simplifier" des éléments dans une inégalité, d'où l'hypothèse de compatibilité de $\leq$ et $+$). Pour l'anti-symétrie, il faut écrire :

$$\begin{aligned}
\left\{ \begin{array}{l} (a,b) \leq (a',b') \\ (a',b') \leq (a,b) \end{array} \right. &\iff \left\{ \begin{array}{l} a+b' \leq a'+b \\ a'+b \leq a+b' \end{array} \right. \iff \exists m \in M,\ \left\{ \begin{array}{l} a+b'+m \leq a'+b+m \\ a'+b+m \leq a+b'+m \end{array} \right. \\
&\iff \exists m,\ a+b'+m \leq a'+b+m \leq a+b'+m \\
&\iff \exists m,\ a+b'+m = a'+b+m \\
&\iff (a,b) \equiv (a',b')\,.
\end{aligned}$$

Cela ne fonctionne pas, notre relation n'est qu'un préordre sur M^2. On sait toutefois qu'elle définit un ordre sur le quotient par la relation $x \sim y \iff \left\{ \begin{array}{l} x \leq y \\ y \leq x \end{array} \right.$, et cette relation est précisément – d'après le calcul ci-dessus – la relation de congruence $\equiv$.