Lois de composition
(version chantier)

Marc SAGE

18 octobre 2007

Table des matières

1 Ordre et loi

Soit A magma ordonné tq $ab \leq a, b$ et $a, b \geq x \implies ab \geq x$.
EG ?
Mq loi est asso et comm (ou pourra mq $\leq$ et loi sont compatibles)

Solution proposée.
EG : $A = \mathfrak{P}(E)$ ordonné par $\subset$ et régi par $\cap$

$\boxed{ab} \leq a, b$, donc $\boxed{ab} \leq ba$, et de même dans l'uatr sens
Mq $\leq$ et loi sont compatibles. Soit $a \leq c$ et $b \leq d$. Alors $ab \leq \binom{a \leq c}{b \leq d}$, donc $ab \leq cd$.
Soit a, b, c. Puisque $ab \leq b$, on a $(ab)c \leq bc$;or, $(ab)c \leq ab \leq a$; les deux donnent $(ab)c \leq a(bc)$. L'inégalité dans l'ordre sens vient de la commutativité.

2 Un tableau et de la craie

On écrit au tableau les 2001 nombres $1, \frac{1}{2}, \frac{1}{3}, ..., \frac{1}{2001}$. On efface deux de ces nombres, x et y, et on écrit alors le nombre $x + y + xy$. On effectue 2000 fois cette opération ; il reste un nombre au tableau. Quels sont les nombres qui peuvent, ainsi, être obtenus ?

Solution proposée.
Des essais avec $1, \frac{1}{2}, \frac{1}{3}$ montrenr que un seul nombre reste. Pour montrer cela, il suffut mq $*$ associatif

$$a * (b * c) = a * (b + c + bc) = a + b + c + bc + ab + ac + abc = e_1 + e_2 + e_3.$$

On intuite ainsi que $a_1 * \cdots * a_n = e_1 + \cdots + e_n$.
Ensuite, on calcule $1 * \frac{1}{2} = 1 + \frac{1}{2} + \frac{1}{2} = 2$, $2 * \frac{1}{3} = 2 + \frac{1}{3} + \frac{2}{3} = 3$, et $n * \frac{1}{n+1} = n + \frac{1}{n+1} + \frac{n}{n+1} = n + 1$.
Rq : on a envie de rajouter un 1 : $(*a_i) + 1 = e_0 + e_1 + \cdots + e_n = \prod (a_i + 1)$, ce qui fait apparaitre morphisme. il s'agit de tordre la loi produit par une incrémentatin $i : x \mapsto x + 1$. En effet, $x * y = i^{-1}(i(x)\, i(y))$.! donc assoc se transporte tout naturellement.

3 Inverser dans un monoïde (prétexte pour introduire aux catégories)

Soit M un monoïde, soit P une partie de M. On cherche à "rajouter" à M des "inverses" de chaque élément de M (et rien d'autre). Cela revient à cherche un monoïde M_P dont M est un sous-monoïde tel que $\begin{cases} P \subset M_P^{\times} \\ M_P = \langle M, P^{-1} \rangle \end{cases}$. Par exemple pour $M = \binom{\mathbf{N}}{+}$ et $P = \{1\}$ on a un candidat $\mathbf{Z}$. De même pour $M = \binom{\mathbf{Z}}{\times}$ et $P = \mathbf{N}^*$ on a pour cacndiat $\mathbf{Q}$

Quitte à remplacer P par le sous-monoïde qu'il engendre, on supposera P sous-monoïde et on le renommera du coup S.

3.1 Approche formelle & quelques égalités utiles

Un élément de $M_S = \langle M, S^{-1} \rangle$ devant être de la forme $\prod m_i s_i^{-1}$, définissons pour commencer M_S comme l'ensemble $(M \times S)^*$ des mots sur $M \times S$, un mot $\binom{m_i}{s_i}$ codant l'élément $\prod m_i s_i^{-1}$. Selon ce codage, on attend évidemment des simplifications :

1. le minmum syndical est $\binom{s}{s} = \emptyset$ (mot vide) pur chaque $s \in S$ dans chaque mot de $(M \times S)^*$, relation d'équivalene sur $(M \times S)^*$ notée $\mathcal{N}$ (pour "neutre")
2. concernant le "pont" entre deux lettres, *à* $\left(\begin{smallmatrix} m & n \\ s & t \end{smallmatrix}\right) \in \frac{M^2}{S^2}$ fixés, on veut identifier

(a) $\begin{pmatrix} m & s \\ s & t \end{pmatrix}$ *avec* $\begin{pmatrix} m \\ t \end{pmatrix}$ (relation notée $\mathcal{P}$ pour "**p**ont"),

(b) $\begin{pmatrix} m & n \\ 1 & 1 \end{pmatrix}$ avec $\begin{pmatrix} mn \\ 1 \end{pmatrix}$ (relatino notée $\mathcal{M}$ pour dire qu'est un **m**orhpisme l'application $\begin{array}{ccc} M & \longrightarrow & M' \\ m & \longmapsto & \frac{m}{1} \end{array}$),

(c) et plus généralement $\begin{pmatrix} m & sn \\ s & t \end{pmatrix}$ avec $\begin{pmatrix} mn \\ t \end{pmatrix}$ (notée $\mathcal{P}^+$).

Notons M' le monoïde qutoeint ${}^{(M\times S)^*}\diagup_{\mathcal{N}}$ muni de la concaténation[1]. On notera $\frac{m}{s}$ la classe d'une "lettre" $\begin{pmatrix} m \\ s \end{pmatrix}$, de sorte que chaque élément de M' s'écrit $\prod \frac{m_i}{s_i}$.

On a alors dans M' les égalités $\forall s \in S,\ \frac{s}{s} = \frac{1}{1}$, schéma que l'on notera également abuseviemnt $\mathcal{N}$. Même notation pour $\mathcal{P}$ et $\mathcal{P}^+$ (égalités que l'on n'a pas *a priori*)

(un peu de finesse) *Montrer alors l'équivalence* $\mathcal{P}^+ \Longleftrightarrow \mathcal{P} \wedge \mathcal{M}$.

DEM $\Longrightarrow$clair ($n \leftarrow 1$ pour $\mathcal{P}$, $s, t \leftarrow 1$ pour $\mathcal{M}$).
$\Longleftarrow$utilisaons 3 lemmes :.Notons 1 les relation $\frac{ms}{s} = \frac{m}{1}$ 2 $\frac{t}{st} = \frac{1}{s}$ 3 $\frac{1}{s}\frac{sm}{t} = \frac{m}{t}$

M$\Longrightarrow$1 $\frac{ms}{s} \overset{\mathcal{P}}{=} \frac{ms}{1}\frac{1}{s} \overset{\mathcal{M}}{=} \left(\frac{m}{1}\frac{s}{1}\right)\frac{1}{s} = \frac{m}{1}\left(\frac{s}{1}\frac{1}{s}\right) \overset{\mathcal{P}}{=} \frac{m}{1}\frac{s}{s} \overset{\mathcal{N}}{=} \frac{m}{1}$
1$\Longrightarrow$2 $\frac{s}{1}\frac{t}{st} \overset{1}{=} \frac{st}{t}\frac{t}{st} \overset{\mathcal{P}}{=} \frac{st}{st} \overset{\mathcal{N}}{=} 1$ (idem autre côté) donc $\frac{t}{st}$ est linverse de $\frac{s}{1}$, çàd vaut $\frac{1}{s}$
M$\wedge$2 $\Longrightarrow$3 $\frac{1}{s}\frac{sm}{t} \overset{\mathcal{P}}{=} \frac{1}{s}\frac{sm}{1}\frac{1}{t} \overset{\mathcal{M}}{=} \frac{1}{s}\left(\frac{s}{1}\frac{m}{1}\right)\frac{1}{t} = \left(\frac{1}{s}\frac{s}{1}\right)\left(\frac{m}{1}\frac{1}{t}\right) \overset{\mathcal{P}}{=} \frac{1}{1}\frac{m}{t} = \frac{m}{t}$
M$\wedge$3 $\Longrightarrow \mathcal{P}^+$ $\frac{m}{s}\frac{sn}{t} \overset{\mathcal{P}}{=} \left(\frac{m}{1}\frac{1}{s}\right)\frac{sn}{t} = \frac{m}{1}\left(\frac{1}{s}\frac{sn}{t}\right) \overset{3}{=} \frac{m}{1}\frac{n}{t} \overset{\mathcal{P}}{=} \frac{m}{1}\left(\frac{n}{1}\frac{1}{t}\right) = \left(\frac{m}{1}\frac{n}{1}\right)\frac{1}{t} \overset{\mathcal{M}}{=} \frac{mn}{1}\frac{1}{t} \overset{\mathcal{P}}{=} \frac{mn}{t}$

On pourra utiliser les égalités $1, 2, 3$ à la secetion 3.3 QQ2.

3.2 Analyse-Synthèse

Puisque M_S est *a priori* à construire *ex nihilo*, il est plus raisonnable de chercher un plongement de monoïdes $\iota : M \hookrightarrow M_S$ tq $\begin{cases} \iota(S) \subset M_S^\times \\ M_S = \left\langle \iota(M), \iota(S)^{-1} \right\rangle \end{cases}$.

Chaque élément inversible étant régulier, l'existence d'un tel plongement implique la régularité de chaque élément de S : on peut se libérer de cette condition si l'on accepte de "fusionner" dans M_S certains éléments distincts de M (par exemple deux $m \neq n$ tels que $\exists s \in S,\ sm = sn$). Nous allons donc lever l'injectivité du morphisme ι et l'appeler plutôt σ

Donnons donc un $\sigma : M \longrightarrow M_S$ tq $\begin{cases} \sigma(S) \subset M_S^\times \\ M_S = \left\langle \sigma(M), \sigma(S)^{-1} \right\rangle \end{cases}$ (remplace old $\begin{array}{c} P \subset M_P^\times \\ M_P = \left\langle M, P^{-1} \right\rangle \end{array}$). On va traduire la 2e égalité "M_S" minimal *uniqement en terme de morhpismes (style "catégoriel")* (QQ1&2), trouver par analyse un candidat pour M_S (QQ3) et synthétisser à la QQ4.

1. *Soit* $f : M \longrightarrow N$ *morphisme. Mq il y a au plus un* $\widetilde{f} : \left\langle \sigma(M), \sigma(S)^{-1} \right\rangle \longrightarrow N$ tq $\widetilde{f} \circ \sigma = f$. *Interprétez quand* σ *est injective. Mq l'existence d'un tel* $\widetilde{f}$ *implique* $f(S) \subset N^\times$.
2. *Montrer que si chaque morphisme* f *de source* M *se prolonge sur* M_S *d'une unique manière alors* $M_S = \left\langle \sigma(M), \sigma(S)^{-1} \right\rangle$.
3. *Montrer que l'application* $\begin{array}{ccc} (M \times S)^* & \twoheadrightarrow & M_S \\ \begin{pmatrix} m_i \\ s_i \end{pmatrix} & \longmapsto & \prod \sigma(m_i)\, \sigma(s_i)^{-1} \end{array}$ *est un morphisme pour la concaténation qui passe au quotient pour* $\mathcal{N}$ *et* $\mathcal{P}^+$. *En déduire que* M_S *est un quotient de* $MS^{-1} := {}^{(M\times S)^*}\diagup_{\mathcal{N}\&\mathcal{P}^+}$
4. *Montrer que le morphisme* $\sigma := \begin{array}{ccc} M & \longrightarrow & MS^{-1} \\ m & \longmapsto & \frac{m}{1} \end{array}$ *vérifie les trois conditions*

   (a) $\sigma(S) \subset \left[MS^{-1}\right]^\times$

   (b) $MS^{-1} = \left\langle \sigma(M), \sigma(S)^{-1} \right\rangle$

[1] **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")

(c) *chaque morphisme* $f : M \longrightarrow N$ *tq* $f(S) \subset N^{\times}$ *induit un unique morphisme* $\widetilde{f} : MS^{-1} \longrightarrow N$ *tq* $\widetilde{f} \circ \sigma = f$
$$\begin{tikzcd} MS^{-1} \arrow[rr, "\exists!\widetilde{f}"] & & N \\ & M \arrow[ul, "\sigma"] \arrow[ur, "\forall f"'] \arrow[u, phantom, "\circlearrowleft"] & \end{tikzcd}$$
. COmmentez la condition "$f(S) \subset N^{\times}$*".*

Solution proposée.

1. $\prod \sigma(m_i)\,\sigma(s_i)^{-1} \mapsto \prod f(m_i)\,f(s_i)^{-1}$ (chq $f(s) = \widetilde{f}(\sigma(s))$ a pour inverse $\widetilde{f}\left(\sigma(s)^{-1}\right)$ d'où $f(S) \subset N^{\times}$). Quand σ injective, chaque morphsime de source M admet au plus un prolongement sur M_P. l
2. Def $N := \langle \sigma M, \sigma S^{-1} \rangle$, soit $\widetilde{\sigma} : M_S \longrightarrow N$ "prlongeant" $\sigma^{|N} : M \subset N$ et notons i l'inj canon $N \subset M_S$
$$\begin{tikzcd} M_S \arrow[r, "\widetilde{\sigma}"] & N \arrow[r, phantom, "\overset{i}{\subset}"] & M_S \\ & M \arrow[ul, "\sigma"] \arrow[u, "\sigma^{|N}"'] \arrow[ur, "\sigma"'] \arrow[ul, phantom, shift right=4, "\circlearrowleft"] & \end{tikzcd}$$
. Alors l'identiét de M_S est lunique morhpsiem "prolongeant" σ, d'où $i \circ \widetilde{\sigma} =$ Id, donc i surj, donc $i = \mathrm{Id}$ et $M_S = N$.
3. fait sens car $\sigma(S) \subset M_S^{\times}$, surj car $M_S = \langle \sigma M, \sigma S^{-1} \rangle$, clairement morpshime, pase quaotient par $\mathcal{N}$ (clair) et par $\mathcal{P}^{+}$ (car σ morphsime), d'où un "relèvement"
$$\begin{tikzcd} & MS^{-1} \arrow[d, "\text{surj}"] \\ M \arrow[ur] \arrow[r, "\sigma"] & M_S \end{tikzcd}$$
qui agit comme
$$\begin{tikzcd} & \frac{\sigma(m)}{1} \arrow[d] \\ m \arrow[ur] \arrow[r] & \sigma(m) \end{tikzcd}$$
. PLus on relève "haut" (çed plus on quotiente), plus on fusionne d'élément à la source M : à l'extrème on pourrait tout fusionner et avoir $MS^{-1} = 1$!! Alors on relève au plus bas, çed carrément "plat" en imposant $MS^{-1} = M_S$
4.
   (a) chaque $\frac{s}{1}$ est inversible d'inverse $\frac{1}{s}$ (grace à $\mathcal{N}$ et $\mathcal{P}$)

   (b) chaque élément de MS^{-1} s'écrit $\prod \frac{m_i}{s_i}$.

   (c) Soit un tel f (la condition "$f(S) \subset N^{\times}$ est nécessaire à la conclusion d'après QQ1). Alors le morphsime
$$\begin{array}{ccc} (M \times S)^{*} & \longrightarrow & N \\ \binom{m_i}{s_i} & \longmapsto & \prod f(m_i)\,f(s_i)^{-1} \end{array}$$
passe au quotient pour $\mathcal{N}$ et $\mathcal{P}^{+}$ donc induit un $\widetilde{f} : MS^{-1} \longrightarrow N$ qui fait bien commuter (et est unique d'après QQ1)

3.3 conclusion

1. *Monrer qu'il y a un unique (à unique iso près) mophsime* $\sigma : M \longrightarrow M_S$ *tel que*

   (a) $\sigma(S) \subset M_S^{\times}$

   (b) *chaque morphisme* $f : M \longrightarrow N$ *tq* $f(S) \subset N^{\times}$ *induit un unique morphisme* $\widetilde{f} : MS^{-1} \longrightarrow N$ *tq* $\widetilde{f} \circ \sigma = f$
$$\begin{tikzcd} MS^{-1} \arrow[rr, "\exists!\widetilde{f}"] & & N \\ & M \arrow[ul, "\sigma"] \arrow[ur, "\forall f"'] \arrow[u, phantom, "\circlearrowleft"] & \end{tikzcd}$$
2. **bonus** *Donner des relations dans* $\operatorname{Ker} \sigma$ *non encore mises à jour.*
3. **EG** *Décrire* σ *quand* $P \subset M^{\times}$*. Commenter.*
4. **EG** *Décrire* σ *quand* M *est un monoïde matriciel.*
5. **EG (plus dur)** *décrire le noayu de* σ *quand* S *monogène et* M *abélien. On pourra réaliser* M_S *à l'aide de polynômes.*
6. **Q OUVERTE** *retirer* M abélien, puis S monogène

DEM

1. La sectin précédente montre l'existence.

   Montrons l'unicité. Soit $\tau : M \longrightarrow N$ un autre. Comme en QQ2
$$\begin{tikzcd} M_S \arrow[r, "\widetilde{\tau}"] & N \arrow[r, "\widetilde{\sigma}"] & M_S \\ & M \arrow[ul, "\sigma"] \arrow[u, "\tau"'] \arrow[ur, "\sigma"'] \arrow[ul, phantom, shift right=4, "\circlearrowleft"] \arrow[ur, phantom, shift left=4, "\circlearrowleft"] & \end{tikzcd}$$
on "prolonge" τ à M_S (prop de σ) et on "prlonge" σ à N (prop de τ). On peut le faire grâce à 1a ! Alors

$\widetilde{\sigma}\widetilde{\tau}$ "polonge" σ à M_S mais Id_{M_S} convient déjà, d'où (par unicité du prolpongemeot) $\widetilde{\sigma}\widetilde{\tau} = \mathrm{Id}_{M_S}$. En échangeant les rôles, $\widetilde{\sigma}$ et $\widetilde{\tau}$ sont des isos réicproqes l'un de autre.

L'unicité de l'iso suite d'un arguemnt quasi similaire. Soit $\widehat{\sigma} : N \xrightarrow{\sim} M_S$ un 2e iso faisant commuter $\begin{array}{ccccc} M_S & \xrightarrow{\widetilde{\tau}} & N & \xrightarrow{\widehat{\sigma}} & M_S \\ \sigma \nwarrow & \circlearrowleft & \uparrow \tau & \circlearrowleft & \nearrow \sigma \\ & & M & & \end{array}$. Même argument donne $\widehat{\sigma}\widetilde{\tau} = \mathrm{Id}_{M_S}$ d'où $\widehat{\sigma} = \widetilde{\sigma}$.

2. Exempes déjà évoqué si il y a des irrég : $ms = ns$. Plus genréalement, si $\exists s, t \in S$ tq $smt = snt$, alors m et n sont fusionnés par σ. DEM : $\frac{m}{1} \overset{3}{=} \frac{1}{s}\frac{sm}{1} \overset{1}{=} \frac{1}{s}\frac{smt}{t}$ (intuit : $m = s^{-1}smtt^{-1}$)
3. Id_M fonctionne : il n'ya ucun inverse à rajouter puisuqu'ils sont déjà dans M.
4. Soit K un corps, soit $n \in \mathbf{N}$, imposons $M = M_n(K)$ et soit $s \in S$ non inversile (on vient de traiter le cas $S \subset M^\times$). Il y a alors (exo classique) un nilmpotent n (soit $\nu \in \mathbf{N}$ tq $n^\nu = 0$) et deux inversibles[2] i, j tq $s = inj$, donc (cf QQ 2) $\frac{s}{1} = \frac{n}{1} = \frac{n^{\nu+1}}{n^\nu} = \frac{0}{n^\nu} = \frac{0n^\nu}{n^\nu} \overset{1}{=} \frac{0}{1}$ est absorbant et inversible, donc M_S est trivial.
5. Soit $s \in S$ tq $S = \langle s \rangle$, on inverse s à la main avec les polynômes : $M \hookrightarrow K[M] \hookrightarrow K[M][X] \twoheadrightarrow {}^{K[M,X]}\!/_{sX=1}$. Déf (par corestric) $\sigma := M \longrightarrow \langle M, X \rangle \subset {}^{K[M,X]}\!/_{sX=1}$.

Soit $f : M \longrightarrow N$ tq $f(s) \in N^\times$. Induit $\begin{array}{ccc} K[M] & \longrightarrow & K[N] \\ m \in M & \longmapsto & f(m) \end{array}$ d'où $\begin{array}{ccc} K[M][X] & \longrightarrow & K[N] \\ X & \longmapsto & f(s)^{-1} \end{array}$ qui passe modulo $sX - 1$, d'où $\begin{array}{ccc} {}^{K[M,X]}\!/_{sX=1} & \longrightarrow & K[N] \\ X & \longmapsto & f(s)^{-1} \end{array}$. En restrienat à $\langle M, X \rangle$ l'image tombe dans N, d'où un "prolongement" de f qui convient (unicité automatique)

Soient $m, m' \in M$ tq $\sigma(m) = \sigma(m')$, def $\lambda := m - m' \in K[M]$, alors $\lambda = 0 \bmod sX - 1$, soit $P \in K[M][X]$ tq $\lambda = (1 - sX)P$. Intuit : $P = \frac{\lambda}{1-sX} = \sum \lambda s^n X^n$ a un degré (fini !). Propre : éval[3] en 0 donne $\lambda = P(0)$, def $P =: \lambda + XQ$, alors

$$\begin{array}{rcl} \lambda & = & (1 - sX)(\lambda + XQ) = \lambda + X(Q - s\lambda - sXQ) \text{ d'où} \\ s\lambda & = & (1 - sX)Q \text{ (on était parti de } \lambda = (1 - sX)P); \end{array}$$

de proche en proche, soit $(P_n) \in K[M][X]^{\mathbf{N}}$ tq $\forall n \in \mathbf{N}$, $\begin{array}{l} s^n\lambda = (1 - sX)P_n \\ P_n = s^n\lambda + XP_{n+1} \end{array}$ $(P_0 = P)$, alors

$$\begin{array}{rcl} P & = & \lambda + XP_1 = \lambda + X\left(s\lambda + \lambda^2 P_2\right) \\ & = & \lambda + Xs\lambda + X^2s^2\lambda + X^3P_3 = \cdots \\ & = & \sum_{i=0}^{N} \lambda s^i X^i + \underbrace{X^{N+1}P_{N+1}}_{\text{pas de terme en } X^N} \quad \text{où } N := 1 + \partial P \\ \text{d'où } (\mathrm{coef}_{X^n})\ 0 & = & \lambda s^N = (m - m')s^N \text{ et } ms^N = m's^N. \end{array}$$

Réciproque claire par QQ 2).

Conclusion : les éléments de M fusionnés par σ sont les a, b tq $\exists n \in \mathbf{N},\ as^n = bs^n$. Ainsi σ inj si s rég.

4 Produit semi-direct (& reverse mathematics)

Soient M et N deux monoïdes. On se donne un morphisme de monoïdes $\left\{ \begin{array}{ccc} N & \longrightarrow & \mathrm{End}\, M \\ n & \longmapsto & m \mapsto {}^n m \end{array} \right.$ et l'on note $M \rtimes N$ le produit cartésien $M \times N$ muni la loi $\begin{pmatrix} m \\ n \end{pmatrix}\begin{pmatrix} \mu \\ \nu \end{pmatrix} := \begin{pmatrix} m\ {}^n\mu \\ n\ \nu \end{pmatrix}$.

1. *Montrer que $M \rtimes N$ est un monoïde dont on précisera le neutre.*
2. *Montrer $(M \rtimes N)^\times = M^\times \rtimes N^\times$.*

[2] m est équivalente à un I_r avec $r < n$ car m pas inver, donc I_r équivalente à J_r nilpotente

[3] bien un morphisme même si M anabélien

3. *Donner une CNS pour ce que ce monoïde soit abélien.*

Solution proposée.

1. calcul, neutre $\begin{pmatrix} 1_M \\ 1_N \end{pmatrix}$
2. Soit $\begin{pmatrix} m \\ n \end{pmatrix}$ et $\begin{pmatrix} \mu \\ \nu \end{pmatrix}$ inverss l'un de l'autre. On a alors $\begin{cases} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} m \\ n \end{pmatrix}\begin{pmatrix} \mu \\ \nu \end{pmatrix} := \begin{pmatrix} m\ {}^n\mu \\ n\ \nu \end{pmatrix} \\ \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \mu \\ \nu \end{pmatrix}\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} \mu\ {}^\nu m \\ \nu\ n \end{pmatrix} \end{cases}$ donc n et ν sont inverse l'un de l'autre ON a par aileurs $1 = {}^\nu 1 = {}^\nu(m\ {}^n\mu) = {}^\nu m\ {}^{\nu n}\mu = {}^\nu m\ {}^1\mu = {}^\nu m\ \mu$, ce qui montre que ${}^\nu m$ et μ sont inverses l'un de l'autre, d'où $\mu = {}^\nu m^{-1} = {}^{n^{-1}}m^{-1}$. Réciproquement, si $\begin{pmatrix} m \\ n \end{pmatrix} \in M^\times \times N^\times$, on vérifie que $\begin{pmatrix} m \\ n \end{pmatrix}$ et $\begin{pmatrix} {}^{n^{-1}}m^{-1} \\ n^{-1} \end{pmatrix}$ sont invers l'un de l'autre.
3. Suppoons abélien. Alors N abélien et $m\ {}^n\mu = \mu\ {}^\nu m$. Prendre $n = 1 = \nu$ mq M abélien. Prendre $\mu = 1$ mq ${}^\nu m = m$. La réciproque est claire. Finalement, $M \rtimes N$ est abélien ssi M et N le sont et si l'action est triviale (on rertouve le produit direct $M \times N$).

On s'intéresse maintenant à la nécessité des hypothèses portant sur les applications $m \mapsto {}^n m$.
Spoiler : *le magma $M \rtimes N$ est un monoïde ssi :*

1. *M et N sont des monoïdes ;*
2. *le neutre de M est l'abscisse du neutre de $M \rtimes N$;*
3. *l'application $n \mapsto (m \mapsto {}^n m)$ est un morphisme de monoïdes $N \longrightarrow \operatorname{End} M$.*

(et on ne peut pas se passer de la deuxième ligne)

Soient M et N deux magmas et $\begin{cases} N & \longrightarrow & M^M \\ n & \longmapsto & m \mapsto {}^n m \end{cases}$ une application. On note $M \rtimes N$ le même magma que ci-dessus.

1. *Montrer que $M \rtimes N$ est associatif ssi N est associatif et si*
$$m\ {}^n(\mu\ {}^\nu\mathfrak{m}) = (m\ {}^n\mu)\ {}^{n\nu}\mathfrak{m}.$$
2. *Montrer que $M \rtimes N$ est unifère ssi N est unifère et si M contient un u tel que*
$$u\ {}^1m = m = m\ {}^n u.$$
3. On suppose ici $\begin{cases} M \text{ monoïde} \\ N \text{ monoïde } \{1\} \end{cases}$ et $\exists \upsilon \in M,\ {}^1m = \upsilon m$. *Montrer alors que $M \rtimes N$ est un monoïde ssi υ est inversible mais qu'alors on n'a pas forcément $1_{M \rtimes N} = (1_M, 1_N)$.*

Solution proposée.

1. calcul
2. calcul
3. $M \rtimes N$ est tjs asso : $\begin{pmatrix} m \\ 1 \end{pmatrix}\begin{pmatrix} \mu \\ 1 \end{pmatrix}\begin{pmatrix} \mathfrak{m} \\ 1 \end{pmatrix} = \begin{pmatrix} m\upsilon\mu\upsilon\mathfrak{m} \\ 1 \end{pmatrix}$.
   L'unifarité de $M \rtimes N$ se réécrit $\exists u, u\upsilon m = m$ et $m\upsilon u = m$, çàd $\exists u, \upsilon u$neutre, çàd υ invesible. Dès que $M^\times$ n'est psa trivial, on peut imposer $\upsilon \neq 1$.

On suppose que $M \rtimes N$ est un monoïde dont on note $\begin{pmatrix} u \\ v \end{pmatrix}$ le neutre.

1. *Montrer que N est un monoïde dont on précisera le neutre.*
2. *Montrer que M n'est pas forcément unifère ni associatif, même si ${}^1u = u$.*

3. *Montrer que u n'est pas forcément un neutre pour M, même si M est un monoïde.*
4. On suppose que u est un neutre pour M. *Montrer alors* ${}^1m = m$, ${}^n1 = 1$, *que M est un monoïde puis* ${}^n(m\mu) = {}^nm\ {}^n\mu$ *et* ${}^n({}^\nu m) = {}^{n\nu}m$.
5. On suppose M associatif et $u \in \{{}^1u, u^2\}$. *Même question.*
6. On suppose M fini et ${}^1u = u$. *Même question.*

Solution proposée.

1. neutre de N est l'ordéonnée du neutr de $M \rtimes N$
2. Prenons $\begin{array}{c} M = \{a,b\} \\ N = \{1\} \end{array}$ avec $\begin{pmatrix} {}^1a \\ {}^1b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}$ et M : $\begin{array}{ccc} \Rsh & a & b \\ a & b & a \\ b & b & b \end{array}$. Alors $M \rtimes N$ monoïde, ni a ni b n'est neutre et M pas asso car $\left\{ \begin{array}{l} a(ba) = ab = a \\ (ab)a = aa = b \end{array} \right.$.

   Pour imposer en plus ${}^1u = u$, la question 6 nous dit qu'il faut prendre M infini. La condition $u\ {}^1m = m$ implique $\begin{array}{c} \text{l'injectivité de } m \mapsto um \\ \text{la surjectivité de } m \mapsto {}^1m \end{array}$ (mais pas de bijectivité sinon u serait neutre et la question 4 concluerait), par exemple, deux tapis roulants (sauf u qui est fixé) : $\begin{array}{c} M = \{u, \alpha, \beta, \gamma, ...\} \\ N = \{1\} \end{array}$ avec

   $${}^1m = \downarrow \begin{array}{ccccc} u & \alpha & \beta & \gamma & \cdots \\ u & \beta & \gamma & \cdots & \end{array} \downarrow \text{ et } \begin{array}{ccccccc} \Rsh & u & \alpha & \beta & \gamma & \cdots & \\ u & u & & \alpha & \beta & \gamma & \cdots \\ \alpha & \alpha & & & & & \\ \beta & \beta & & & & & \\ \gamma & \gamma & & & & & \\ \vdots & \vdots & & & & & \end{array}$$

   . Alors $M \rtimes N$ monoïde et M pas unifère car $\forall \Diamond \neq u,\ u\Diamond \neq \Diamond$ (l'injectivité empeche $u\alpha = \alpha$) et M pas ass car $\left\{ \begin{array}{l} u(u\gamma) = u\beta = \alpha \\ (uu)\gamma = u\gamma = \beta \end{array} \right.$.
3. cf question 3
4. L'uniférité se réécrit ${}^1m = m = m\ {}^n1$, remplacer $m \leftarrow 1$ donne ${}^n1 = 1$. Dans $m\ {}^n(\mu\ {}^\nu\mathfrak{m}) = (m\ {}^n\mu)\ {}^{n\nu}\mathfrak{m}$ remplacer $n = \nu = 1$ donne l'associativité de M, puis rempalcer $m = 1 = \mu$ donne ${}^n({}^\nu\mathfrak{m}) = {}^{n\nu}\mathfrak{m}$, puis remplacer $m = 1 \text{et} \nu = 1$ donne ${}^n(\mu\ \mathfrak{m}) = {}^n\mu\ {}^n\mathfrak{m}$.
5. supp $u^2 = u$. Alors $\begin{array}{c} u(u\ {}^1m) = um \\ (uu)\ {}^1m = u\ {}^1m = m \end{array}$ donc u neutre gauche donc neutre bilatère (cf question 4)

   supp ${}^1u = u$. Alors dans $m = u\ {}^1m$ remplacer $m = u$ donne $u = u\ {}^1u = u^2$.
6. Suppo M fini. PUisque $u\cdot$ est surj, elle est inj : de $m\ {}^1u = m$ on déduit $(m \leftarrow u)$ alors $u\ {}^1ux = ux$, d'où ${}^1ux = x$ et ${}^1u$ neutre pour M. Puisque $u^1 = u$, cf question 4.

5 Comment construire des anneaux horribles

http ://www.math.ens.fr/~madore/algebre2/

Pour toute partie stricte $A \subsetneq \mathbb{N}$, on pose $\operatorname{mex} A := \min \mathbb{N} \backslash A$.
On définit alors sur $\mathbb{N}$ deux lois # (somme de Conway) et @ (produit de Conway) par les récurences

$$\begin{aligned} a\#b \ &: = \operatorname{mex}\left(\{a'\#b\}_{a'<a} \cup \{a\#b'\}_{b'<b}\right) \text{ et} \\ a@b \ &: = \operatorname{mex}\{(a'@b)\#(a'@b')\#(a@b')\}_{a'<a}^{b'<b} \end{aligned}$$

1. Montrer que # est commutative, admet pour neutre 0, $a\#b = 0$ ssi $a = b$, associative (supposer $e < a\#(b\#c)$ et prouver par exemple $e \neq (a\#b)\#c$).
2. Montrer que @ est commutative, 0 absorbant, 1 neutre, associatif, $a@b = 0$ ssi $a \text{ou} b = 0$, distributif sur #.
3. Décrire $a\#b$ en base 2. Calculer $2^{2^a}@2^{2^b}$ et montrer que $\left[0, 2^{2^a}\right[$ muni de la somme # et du produit @ est isomorphe à $\mathbb{F}_{2^{2^a}}$.
4. On remplace l'ordinal $\mathbb{N} = \omega$ par ω^ω. Montrer que l'on obtient une clôture algébrique de $\mathbb{F}_2$.