27/03/2007

3 Morphismes de lois

def Soit $(X, \perp_X)$ et $(Y, \perp_Y)$ deux ensembles munis de lois.

un morphisme de $(X, \perp_X)$ vers $(Y, \perp_Y)$ est $f : X \to Y$ t.q.

$$\forall x, y \in X \quad f(x \perp y) = f(x) \perp f(y)$$

Exemples a) $Id_X : X \to X$ $x \mapsto x$ est un morphisme de $(X, \perp_X)$ vers $(X, \perp_X)$

b) $\exp : \mathbb{R} \to \mathbb{R}$, $t \mapsto e^t$ est un morphisme de $(\mathbb{R}, +)$ vers $(\mathbb{R}, \times)$

c) Exercice $\mathbb{R} \to M_2(\mathbb{R})$ $t \mapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ est morphisme de $(\mathbb{R}, +)$ vers $(M_2(\mathbb{R}), \circ)$

$\mathbb{R} \to M_2(\mathbb{R})$ $x \mapsto \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ ——— $(\mathbb{R}, \times)$ ———

$\mathbb{R} \setminus \{0\} = \mathbb{R}^* \to M_2(\mathbb{R})$ $x \mapsto \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ ——— $(\mathbb{R}^*, \times)$ ———

d) Si $\perp$ est associative et $x \in X$

$$\mathbb{N} \setminus \{0\} \to X, \; n \mapsto x^n = \overbrace{x \perp \cdots \perp x}^{n \text{ fois}}$$ est un morphisme de $(\mathbb{N} \setminus \{0\}, +)$ vers $(X, \perp)$

Proposition 1 Soit $f : (X, \perp_X) \to (Y, \perp_Y)$ et $g : (Y, \perp_Y) \to (Z, \perp_Z)$ deux morphismes

alors $g \circ f : (X, \perp_X) \to (Y, \perp_Y)$ est un morphisme

pv $\forall x', x'' \in X$ $g \circ f(x' \perp_X x'') = g(f(x' \perp_X x'')) \underset{\uparrow}{=} g(f(x') \perp_Y f(x'')) \underset{\uparrow}{=} g(f(x')) \perp_Z g(f(x'')) = g \circ f(x') \perp_Z g \circ f(x'')$ $\square$

f morphisme   g morphisme

def un isomorphisme de $(X, \perp_X)$ sur $(Y, \perp_Y)$ est un morphisme $f : (X, \perp_X) \to (Y, \perp_Y)$

t.q il y a un morphisme $g : (Y, \perp_Y) \to (X, \perp_X)$ avec $g \circ f = Id_X$ et $f \circ g = Id_Y$

Proposition 2 un morphisme $f : (X, \perp_X) \to (Y, \perp_Y)$ est un isomorphisme ssi il est bijectif.

En ce cas $g = f^{-1}$ (la bijection réciproque) et est dit isomorphisme réciproque de f
l'inverse

pv $\Rightarrow$ $g\circ f = Id_X$ donc f injectif ; $f\circ g = Id_Y$ donc f surjectif ainsi f bijectif et $f^{-1} = f^{-1}\circ Id_Y = f^{-1}\circ(f\circ g)$
$= (f^{-1}\circ f)\circ g = Id_X\circ g = g$ □

$\Leftarrow$ Si f morphisme bijectif alors $\forall y', y'' \in Y$, $f^{-1}(y'), f^{-1}(y'') \in X$ et

$$f(f^{-1}(y')\perp_X f^{-1}(y'')) = f(f^{-1}(y'))\perp_Y f(f^{-1}(y'')) = y'\perp_Y y''$$

donc $f^{-1}(y'\perp_Y y'') = f^{-1}(f(f^{-1}(y')\perp_X f^{-1}(y''))) = f^{-1}(y')\perp_X f^{-1}(y'')$ ■

Exemples a) Id_X isomorphisme de $(X,\perp_X)$ sur $(X,\perp_X)$

b) $\exp : \mathbb{R} \to]0,+\infty[$ isomorphisme de $(\mathbb{R},+)$ sur $(]0,+\infty[,\times)$ et $\exp^{-1} = \lg :]0,+\infty[\to \mathbb{R}$

mais $\exp : \mathbb{C} \to \mathbb{C}^* =]0,+\infty[$ morphisme surjectif non injectif $[\exp(2\pi i) = 1 = \exp(0)]$

Déf Si il y a un isomorphisme $f : (X,\perp_X) \to (Y,\perp_Y)$ on dit que $(X,\perp_X)$ et $(Y,\perp_Y)$ sont isomorphes.

Les lois $\perp_X$ et $\perp_Y$ ont alors les m̃ propriétés ($\perp_X$ associative ssi $\perp_Y$ associative, ...)

Exemples

Exercices 1) $]-\frac{\pi}{2},\frac{\pi}{2}[\times]-\frac{\pi}{2},\frac{\pi}{2}[\to]-\frac{\pi}{2},\frac{\pi}{2}[$ $\quad \alpha\perp\beta = \operatorname{Arctg}\left(\dfrac{2\sin(\alpha+\beta)}{\cos(\alpha+\beta)+\cos(\alpha-\beta)}\right)$

a) prouver directement que $\perp$ est associative.

b) Vérifier $\lg :]-\frac{\pi}{2},\frac{\pi}{2}[\to \mathbb{R}$ est un isomorphisme de $(]-\frac{\pi}{2},\frac{\pi}{2}[,\perp)$ sur $(\mathbb{R},+)$.

2) a) Pour $n = 2,3,4,5$ calculer $\begin{pmatrix}3&4\\-1&-1\end{pmatrix}^n$ $\left(= \overbrace{\begin{pmatrix}3&4\\-1&-1\end{pmatrix}\cdots\begin{pmatrix}3&4\\-1&-1\end{pmatrix}}^{n \text{ fois}} \in M_2(\mathbb{R})\right)$

b) Vérifier $\begin{pmatrix}3&4\\-1&-1\end{pmatrix} = \begin{pmatrix}2&-1\\-1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\1&2\end{pmatrix}$ et $\begin{pmatrix}1&1\\1&2\end{pmatrix}$ inversible ds $M_2(\mathbb{R})$ $\begin{pmatrix}1&1\\1&2\end{pmatrix}^{-1} = \begin{pmatrix}2&-1\\-1&1\end{pmatrix}$

c) Prouver que si $\perp : X\times X \to X$ associative avec un élément neutre et $x\in X$ inversible

$c_x : X \to X$ $\quad c_x(y) = x^{-1}yx$ isomorphisme de $(X,\perp_X)$ sur $(X,\perp_X)$ d'inverse $c_{x^{-1}}$

d) En déduire $\forall n \in \mathbb{N}\setminus\{0\}$ $\quad \begin{pmatrix}3&4\\-1&-1\end{pmatrix}^n = \begin{pmatrix}2&-1\\-1&1\end{pmatrix}\begin{pmatrix}1&n\\0&1\end{pmatrix}\begin{pmatrix}1&1\\1&2\end{pmatrix} = \begin{pmatrix}2n+1&4n\\-n&1-2n\end{pmatrix}$

4 Lois quotients

Théorème Soit X un ensemble muni d'une loi $\perp$ et d'une relation d'équivalence R

Alors il y a sur l'ensemble quotient $X/_R$ une loi $\perp_R$ tq $\pi : X \to X/_R$ est morphisme de $(X,\perp)$ vers $(X/_R, \perp_R)$

ssi $\forall x, x', y, y' \in X$ (1) $x \equiv x' \bmod R \Rightarrow x \perp y \equiv x' \perp y \bmod R$
et (2) $y \equiv y' \bmod R \Rightarrow x \perp y \equiv x \perp y' \bmod R$

En ce cas la loi $\perp_R$ est uniquement déterminée et $\underset{\pi(x)\perp_R \pi(y)}{\underset{\shortparallel}{\overline{x} \perp_R \overline{y}}} = \underset{\pi(x\perp y)}{\underset{\shortparallel}{\overline{x \perp y}}}$

c'est la loi quotient de $\perp$ par R on dit que $\perp$ passe au quotient par R

et que R est compatible à $\perp$

pv $\Rightarrow$ $x \equiv x' \bmod R \Rightarrow \pi(x \perp y) \underset{\substack{\uparrow \\ \pi \text{ morphisme}}}{=} \pi(x) \perp \pi(y) \underset{\overline{x} = \overline{x}'}{=} \pi(x') \perp \pi(y) = \pi(x' \perp y)$ donc $x \perp y \equiv x' \perp y \bmod R$

et de m̃ $y \equiv y' \bmod R \Rightarrow \dots \Rightarrow x \perp y \equiv x \perp y' \bmod R$

$\Leftarrow$ si $x' \in \overline{x}$ et $y' \in \overline{y}$: $x \equiv x' \bmod R$ donc $x \perp y \equiv x' \perp y \bmod R$; $y \equiv y' \bmod R$ donc $x' \perp y \equiv x' \perp y' \bmod R$ $\Big| \underset{\text{transitivité de } R}{\Rightarrow}$ $x \perp y \equiv x' \perp y' \bmod R$

donc on peut définir $\overline{x} \perp \overline{y}$ par $\overline{x \perp y}$ (ça ne dépend pas des choix de $x \in \overline{x}$, $y \in \overline{y}$)

$$\pi(x \perp y) = \overline{x \perp y} = \overline{x} \perp \overline{y} = \pi(x) \perp \pi(y) \text{ donc } \pi \text{ morphisme.} \square$$

Remarque Si $\perp$ est commutative il suffit de vérifier (1) (ou (2))

Exemples a) Soit $N \in \mathbb{N}$ $+$ et $\times$ sont compatibles à mod N

b) sur $GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \;\middle|\; ad - bc \neq 0 \right\}$ $\left(= \{ M \in M_2(\mathbb{R}) \mid M \text{ inversible} \}\right)$

la relation $\mathcal{L}$ de colinéarité $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \bmod \mathcal{L}$ ssi $\exists \lambda \in \mathbb{R}^*$ $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} \lambda a' & \lambda b' \\ \lambda c' & \lambda d' \end{pmatrix} = \left(\lambda \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \circ \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$

est d'équivalence et compatible avec la composition

Remarque Si R est compatible avec $\perp : X \times X \to X$ et $\perp$ est associative (resp commutative, a un élément neutre e, $x \in X$ a un inverse x^{-1}) alors $\perp_R$ est associative (resp commutative, a un élément neutre $\bar{e}$, $\bar{x} \in X/_R$ a un inverse $\overline{x^{-1}}$)

mais 1 n'a pas d'inverse pour $+$ dans $\mathbb{N}$ et $\overline{N-1}$ est inverse de $\bar{1}$ pour $+_{modN}$ dans $\mathbb{N}/_{modN}$:

« on peut gagner des propriétés en passant au quotient »

Exemples construction de $\mathbb{Z}$ à partir de $\mathbb{N}$ et $\mathbb{Q}_+$ à partir de $\mathbb{N}\setminus\{0\}$

def Soit $(X, \perp_X)$ et $(Y, \perp_Y)$ deux ensembles munis de lois

la loi produit $(\perp = (\perp_X, \perp_Y))$ sur l'ensemble produit $X \times Y$ est

$$(x,y) \perp (x',y') = (x \perp_X x', y \perp_Y y')$$

(on opère composante par composantes, ainsi si $\perp_X$ et $\perp_Y$ sont associatives (resp commutatives; ont des élément neutre e_X, e_Y; $x \in X$ a un inverse $x^{-1} \in X$ et $y \in Y$ a un inverse $y^{-1} \in Y$) alors

$\perp = (\perp_X, \perp_Y)$ est associative [resp commutative; a un élément neutre (e_X, e_Y); $(x,y) \in X \times Y$ a un inverse $(x^{-1}, y^{-1}) \in X \times Y$]

def Soit $\perp$ une loi commutative sur X. Un élément $z \in X$ est régulier si $\perp z : X \to X$ $x \mapsto x \perp z$ est injective $[x \perp z = y \perp z \Rightarrow x = y]$

Théorème Soit sur un ensemble X une loi associative et commutative

1/ Alors la relation S sur $X \times X$ $(x,y) \equiv (x',y')$ mod S ssi $\exists z \in X$ tq $x \perp y' \perp z = x' \perp y \perp z$ est une relation d'équivalence compatible avec la loi produit $(\perp, \perp)$ et pour tout $x \in X$, $y \in Y$

(1) la loi quotient a $\overline{(x,x)}$ pour élément neutre

(2) $\overline{(x,y)}$ a pour un inverse $\overline{(x,y)} = \overline{(y,x)}$

(3) $X \to X \times X$ $x \mapsto (x \perp x, x)$ est un morphisme passant au quotient en ~~un~~ morphisme $X \to X\times X/S$ $x \mapsto \overline{(x\perp x, x)}$ qui est injectif si tout élément de X est régulier.

pv réflexivité $x \perp x \perp x = x \perp x \perp x$ donc $(x,x) \equiv (x,x) \bmod S$ $(z = x)$

symétrie $(x,y) \equiv (x',y') \bmod S \Rightarrow \exists z \in X$ $x \perp y' \perp z = x' \perp y \perp z$

$\Rightarrow \exists z \in X$ $x' \perp y \perp z = x \perp y' \perp z \Rightarrow (x',y') \equiv (x,y) \bmod S$

symétrie de $=$

transitivité $(x,y) \equiv (x',y') \bmod S$ $\exists z \in X$ $x \perp y' \perp z = x' \perp y \perp z$

$(x',y') \equiv (x'',y'') \bmod S \Rightarrow \exists z' \in X$ $x' \perp y'' \perp z' = x'' \perp y' \perp z'$

donc

$$(x \perp y'') \perp (y' \perp z \perp z') = (x \perp y' \perp z) \perp (y'' \perp z') = (x' \perp y \perp z) \perp (y'' \perp z')$$

associativité et commutativité de $\perp$ $\longrightarrow$ $\parallel$

$$(x'' \perp y) \perp (y' \perp z \perp z') = (x'' \perp y' \perp z') \perp (y \perp z) = (x' \perp y'' \perp z') \perp (y \perp z)$$

et avec $z'' = y \perp z \perp z'$ $x \perp y'' \perp z'' = x'' \perp y \perp z''$ c.a.d $(x,y) \equiv (x'',y'') \bmod S$

compatibilité de S avec $(\perp, \perp)$

$(x',y') \equiv (x'',y'') \bmod S$ donc $\exists z \in X$ $x' \perp y'' \perp z = x'' + y' \perp z$

$$(x \perp x') \perp (y \perp y'') \perp z = x \perp (x' \perp y'' \perp z) \perp y = x \perp (x'' \perp y' \perp z) \perp y$$

$$(x \perp x'') \perp (y \perp y') \perp z = (x \perp x'') \perp (y \perp (y' \perp z)) = (x \perp x'') \perp ((y' \perp z) \perp y)$$

donc $(x \perp x', y + y'') \equiv (x \perp x'', y + y') \bmod S$.

(1) $\forall (x', y') \in X \times X$

(1) $(x', y') \perp (x, x) = (x' \perp x, y' \perp x)$

et $x' \perp (y' \perp x) \perp x = x' \perp (x \perp y') \perp x = (x' \perp x) \perp y' \perp x$

donc $(x', y') \equiv (x', y') \perp (x, x) \bmod S$ (prendre $z = x$ de la def)

et $\overline{(x,x)}$ élément neutre de $(\perp, \perp)_S$ □

(2) $(x, y) \perp (y, x) = (x \perp y, y \perp x) \underset{\substack{\uparrow \\ \text{commutativité}}}{=} (x \perp y, x \perp y)$

donc $\overline{(x,y)} \perp \overline{(y,x)} = \overline{(x \perp y, x \perp y)}$ élément neutre de $(\perp, \perp)_S$ □

(3) $\forall x, y \in X$

$(x \perp x, x) \perp (y \perp y, y) = ((x \perp x) \perp (y \perp y), x \perp y) \underset{\substack{\uparrow \\ \text{commutativité de } \perp}}{=} ((x \perp y) \perp (x \perp y), x \perp y)$ □.

$\overline{(x \perp x, x)} = \overline{(y \perp y, y)} \iff \exists z \in X \quad (x \perp x) \perp y \perp z = (y \perp y) \perp x \perp z$

donc (associativité) $x \perp (x \perp y \perp z) = y \perp (y \perp x \perp z)$ et $x \perp (x \perp y \perp z) = y \perp (x \perp y \perp z)$ (commutativité)

et ($x \perp y \perp z$ est régulier) $x = y$ ■

<u>Exemples</u> a) $X = X_1 = \mathbb{N} \setminus \{0\}$ $\perp_1 = +$

b) $X = X_2 = \mathbb{N}$ $\perp_2 = +$

c) $X = X_3 = \mathbb{N} \setminus \{0\}$ $\perp_2 = \times$

dans les trois cas $\perp_i$ est associative commutative et tout $z \in X_i$ est régulier

<u>Exercice</u> a) $X_1 \hookrightarrow X_2$ induit un isomorphisme $X_1 \times X_1 /_{\bmod S_1} \to X_2 \times X_2 /_{\bmod S_2}$

On note $\mathbb{Z} = X_1 \times X_1 /_{\bmod S_1} \text{ "="} X_2 \times X_2 /_{\bmod S_2}$ et identifie $n \in \mathbb{N}$ à $\overline{(m+n, m)} \in \mathbb{Z}$

et note $-n = \overline{(n, n+n)}$ l'opposé de $\overline{(n+n, n)}$ dans $\mathbb{Z}$

On note $\mathbb{Q}_+^* = X_3 \times X_3 /_{\mathrm{mod}\, S_3}$ identifie $n \in \mathbb{N}\setminus\{0\}$ à $\overline{(n\times n, n)} \in \mathbb{Q}_+^*$

et note $\frac{1}{n} = \overline{(n, n\times n)}$ l'inverse dans $\mathbb{Q}_+^*$ de $\overline{(n\times n, n)}$ dans

Remarque a) comme $\forall m, n \in \mathbb{N}$ on a soit $m \leq$

soit $m \geq n$ et il y a $k \in \mathbb{N}$ tq $m = n + k$ donc $(m, n) \equiv (k+k, k)$ mod S

soit $m < n$ et il y a $l \in \mathbb{N}\setminus\{0\}$ tq $n = m + l$ donc $(m, n) \equiv (l, l+l)$ mod S

et $\mathbb{Z} = \mathbb{N} \cup \{-n \,;\, n \in \mathbb{N}\setminus\{0\}\}$

b) mais il y a $k \in \mathbb{N}\setminus\{0\}$ tq $m = n \times k$ ssi $n \mid m$

$l \in \mathbb{N}\setminus\{0\}$ tq $n = m \times l$ ssi $m \mid n$

On note $\frac{m}{n} = \overline{(m, n)} \in \mathbb{Q}$ ainsi $\frac{1}{n} = \overline{(1, n)} = \overline{(n, n\times n)}$ l'inverse de $n = (n, 1) = (n\times n, n)$ dans $\mathbb{Q}$

et comme on n'a pas toujours soit $n \mid m$ soit $m \mid n$ on a

$$(\mathbb{N}\setminus\{0\}) \cup \left\{\frac{1}{n} \,;\, n \in \mathbb{N}\setminus\{0\}\right\} \underset{\neq}{\subset} \mathbb{Q}_+^* = \left\{\frac{m}{n} \,;\, m, n \in \mathbb{N}\setminus\{0\}\right\}$$

Exercice $\mathbb{Q}_+^* = \left\{\frac{a}{b} \,;\, a, b \in \mathbb{N}\setminus\{0\}\ a \text{ et } b \text{ premiers entre eux}\right\}$

et $m, n \in \mathbb{N}\setminus\{0\}$ alors $\frac{m}{n} = \frac{a}{b}$ ssi $\exists\, k \in \mathbb{N}\setminus\{0\}$ $m = ka$ et $n = kb$

en particulier si m et n premiers entre eux et $\frac{m}{n} = \frac{a}{b}$ (a et b premiers entre eux)

$\frac{m}{n} = \frac{a}{b}$ alors $m = a$, $n = b$

$\left\{\frac{a}{b} \,;\, a, b \in \mathbb{N}\setminus\{0\}, a, b \text{ premiers entre eux}\right\}$ est un système

de représentant de mod S_3 dans $(\mathbb{N}\setminus\{0\}) \times (\mathbb{N}\setminus\{0\})$