13/02/2007

<u>Proposition et def</u> Soit $(E, <_E)$ et $(F, <_F)$ deux ensembles ordonnés.

Sur $E \times F$ la relation $(x,y) <_{E,F} (x',y')$ ssi $\underset{x \neq x'}{x <_E x'}$ ou $((x = x')$ et $(y \leq_F y'))$

est une relation d'ordre. L'ordre lexicographique de $<_E$ et $<_F$

De plus si $<_E$ et $<_F$ sont des bons ordres alors $<_{E,F}$ est un bon ordre

pr transitivité $(x,y) <_{E,F} (x',y') \leq_{E,F} (x'',y'')$

donc $x \leq_E x' \leq_E x''$ et si $x = x'$ $y \leq_F y'$, si $x' = x''$ $y \leq_F y''$

d'où ($<_E$) transitivité et $x \leq_E x''$. ①

② Si $x'' = x$ $(\leq_E x' \leq_E x'')$ on a $x = x'' \leq_E x'$ et $x' \leq_E x'' = x$

donc (antisymétrie de $<_E$) $x = x'' = x'$ et $y \leq_F y' \leq_F y''$

d'où (transitivité de $<_F$ $y \leq_F y''$

① et ② $\overset{def}{\Longleftrightarrow}$ $(x,y) \leq_{E,F} (x'',y'')$ $\square$

réflexivité et antisymétrie de $<_{E,E}$: Exercice

Soit $\emptyset \neq C \subset E \times F$ et $\emptyset \neq A = \mathrm{Pr}_1(C) = \{x \in E \mid \exists y \in F\ (x,y) \in C\} \subset E$

Soit $a = m_E(A)$ et $\emptyset \neq B = \{y \in F \mid (a,y) \in C\} \subset F$

et $b = m_F(B)$ alors $(a,b) \in C$ et $\forall (x,y) \in C$ $(a,b) \leq (x,y)$.

<u>Exemple</u> La preuve de $z_{\lambda_i, k_i} (= e^{\lambda_i t} t^{[k_i]})$ $1 \leq i \leq q$, $0 \leq k_i < m_i$

sont linéairement indépendant est une récurrence sur (i, k_i)

dans le bon ordre lexicographique de $\mathbb{N} \times \mathbb{N}$. $\square$

III Relations d'équivalence

1 définition et exemples

déf. une relation d'équivalence R sur un ensemble E est une relation binaire sur E qui est reflexive, symétrique et transitive.

Si $x, y \in E$ verifient $x R y$ on note $x \equiv y \mod R$ ou $x \underset{R}{\sim} y$ et dit x est $\left\{\begin{array}{l}\text{congru à}\\ \text{équivalent à}\end{array}\right\}$ y modulo R. [$x \sim y$ si la relation est claire par le contexte]

Exemples ① égalité ds E

② V espace vectoriel réel $E = V \setminus \{0\}$ (ens des vecteurs non nuls de E)

relation $\mathcal{L}$ "être liés" ou "être colinéaire"

③ $f : E \to F$ une application, $x, y \in E$ $x \equiv y \mod R_f$ ssi $f(x) = f(y)$

pr ① et plus généralement

③' Si S est une relation d'équivalence sur F, $f^*(S)$: $\forall x, y \in E$ $x \equiv y \mod f^*(S)$ ssi $f(x) \equiv f(y) \mod S$

pr S reflexive donc $\forall x \in E$ $f(x) \equiv f(x) \mod S \overset{def}{\Leftrightarrow} x \equiv x \mod f^*(S)$: $f^*(S)$ reflexive

S symétrique donc $\forall x, y \in E$ $(f(x) \equiv f(y) \mod S) \underset{\Rightarrow}{\Leftrightarrow} (f(y) \equiv f(x) \mod S)$

$$\Uparrow \Updownarrow def \qquad\qquad \Downarrow \Updownarrow def$$

$$x \equiv y \mod f^*(S) \qquad y \equiv x \mod S$$ donc $f^*(S)$ sym.

S transitive donc $\forall x, y, z \in E$

$$(f(x) \equiv f(y) \mod S) \text{ et } (f(y) \equiv f(z) \mod S) \Rightarrow (f(x) \equiv f(z) \mod S)$$

$$\Updownarrow def \ \Uparrow \qquad\qquad \Downarrow \Updownarrow def$$

$$(x \equiv y \mod f^*(S)) \text{ et } (y \equiv z \mod f^*(S)) \qquad x \equiv z \mod f^*(S)$$ donc $f^*(S)$ trans.

Remarque ça n'aurait pas marché avec une relation d'ordre

ex $f:\mathbb{R}\to\mathbb{R}$ $f(x)=x^2$ $f(-1)\leq f(1)$ donc $-1 \; f^*(\leq) \; 1$

$f(1)\leq f(-1)$ donc $1 \; f^*(\leq) \leq -1$

mais $-1\neq 1$ donc $f^*(\leq)$ n'est pas antisymétrique.

④ Soit $N\in\mathbb{N}$. Si $m,n\in\mathbb{N}$ m est congru à n modulo N noté $m\equiv n \bmod N$ ssi $\exists k,l\in\mathbb{N}$ t.q. $m+kN=n+lN$ est une relation d'équivalence

pv trans. $\forall m,n,p\in\mathbb{N}$ $(m\equiv n \bmod N)$ et $(n\equiv p \bmod N)$

$\overset{def}{\Leftrightarrow} \exists k,l,i,j\in\mathbb{N}$ tq $(m+kN=n+lN)$ et $(n+iN=m+jN)$

$\Rightarrow \exists f=k+i, g=j+l$ t.q. $m+fN=p+gN$ c.a.d $m\equiv p \bmod N$

pv $m+(k+i)N = m+(kN+iN) = (m+kN)+iN = (n+lN)+iN = n+(lN+iN)$

$$\|$$

$m+(j+l)N = m+(jN+lN) = (m+jN)+lN = (n+iN)+lN = n+(iN+lN)$

reflexivité et symétrie : Exercice

Remarques ① Souvent c'est la transitivité qui nécessite une preuve

"non tautologique"

② comme $\forall k,l\in\mathbb{N}$ $k+1=l+1\Rightarrow k=l$

et $\forall a\in\mathbb{N}$ $a>0\Rightarrow \exists a'\in\mathbb{N}$ $a=a'+1$ (donc $a'\lneq a$)

on prouve $a+N=b+N\Rightarrow a=b$

et donc si $\mathbb{N}\ni k,l>0$ $(a+kN=b+lN\Rightarrow a+k'N=b+l'N$

donc le plus petit $(k,l)\in\mathbb{N}\times\mathbb{N}$ (pour l'ordre lexicographique)

$k=0$ ou $l=0$

vérifie $k=0$ ou $l=0$.

C'est une propriété utile mais à ne surtout pas mettre dans la définition (par exemple il faudrait faire 4 démonstrations ($k=0$, $i=0$) ; ($k=0$, $j=0$) ; ($l=0$, $i=0$), ($l=0$, $j=0$) pour la pv de trans. !!)

③ Si $N=0$ $\quad m \equiv n \bmod N$ ssi $m = n$

④ On a supposé donné $\mathbb{N}$ et les propriétés de ses opérations.

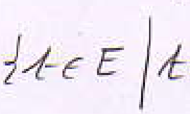
On dégagera les propriétés utilisées dans les preuves (comme celle de la transitivité de $\equiv \bmod R$ ou de la remarque de simplification ②) et s'il reste du temps à la fin du cours on donnera une construction ou une axiomatique de $\mathbb{N}$ justifiant ces manipulations.

2 Classes d'équivalence et ensemble quotient.

Soit E un ensemble muni d'une relation d'équivalence R

def La classe d'équivalence de x est $\overline{x}_R = \overline{x} = \{t \in E \mid t \equiv x \bmod R\}$

la partie de E formée des éléments équivalents à x modulo R

Exemple $E = V \setminus \{0\}$ $\quad R = \mathcal{L}$ $\quad v \in E$ $\quad \overline{v} = \{\lambda v \in E ;\ \lambda \in \mathbb{R}\ \lambda \neq 0\}$  $V = \mathbb{R}^2$

Théorème Pour tout $x \in E$ on a $x \in \overline{x}$ donc $\overline{x}$ est non vide de plus pour tout $y \in E$ sont équivalents (1) $x \equiv y \bmod R$ (2) $\overline{x} \subset \overline{y}$ (3) $\overline{x} \cap \overline{y} \neq \emptyset$ (4) $\overline{x} = \overline{y}$

pv comme R est réflexive $x \equiv x \bmod R$ donc $x \in \overline{x}$ $\square$

le reste suivant le schéma (1) (2) (3) (4)

$$(1) \Rightarrow (2) \quad \left.\begin{array}{l} \forall t \in \overline{x} \quad t \equiv x \bmod R \\ (1) \quad x \equiv y \bmod R \end{array}\right\} \underset{\text{trans.}}{\Rightarrow} t \equiv y \bmod R, \text{ cad } t \in \overline{y} \quad \square$$

$(2) \Rightarrow (3)$ $x \equiv x \bmod R$ donc $x \in \bar{x} \underset{(2)}{\subset} \bar{y} \Rightarrow x \in \bar{x} \cap \bar{y}$, c.a.d. $\bar{x} \cap \bar{y} \neq \emptyset$ □

$(3) \Rightarrow (4)$ $t \in \bar{x} \cap \bar{y}$ donc $(t \equiv x \bmod R)$ et $(t \equiv y \bmod R)$

$\Downarrow$ sym

$(x \equiv t \bmod R)$

$\Big\} \underset{\text{trans}}{\Rightarrow} x \equiv y \bmod R$ □

$\big((1)$ et $(1) \Rightarrow (2)\big) \Rightarrow (4)$ $x \equiv y \bmod R \underset{(1) \Rightarrow (2)}{\Rightarrow} \bar{x} \subset \bar{y}$

$\Downarrow$ sym

$y \equiv x \bmod R \Rightarrow \bar{y} \subset \bar{x}$

$\Big\} \Rightarrow \bar{x} = \bar{y}$ □

$(4) \Rightarrow (2)$ $\bar{x} = \bar{y} \underset{\subset \text{ est reflexive}}{\Rightarrow} \bar{x} \subset \bar{y}$ ■

def une partition d'un ensemble E est une famille $(E_i)_{i \in I}$ de parties non vides $\emptyset \neq E_i \subset E$ de E tq $E_i \cap E_j \neq \emptyset \Rightarrow i = j$ (les E_i deux à deux disjoints) et $\forall x \in E \ \exists i \in I$ tq $x \in E_i$ $\left(E = \bigcup_{i \in I} E_i\right)$ on note $E = \coprod_{i \in I} E_i$

(cette notation est aussi utilisée sans $E_i \neq \emptyset$)

Le théorème assure que les classes d'équivalence forment une partition de E.

def l'ensemble quotient de la relation d'équivalence R est l'ensemble de ses classes d'équivalence $E/_R = \{X \in \mathcal{P}(E) \mid \exists x \in E, X = \bar{x}\}$ (une partie de $\mathcal{P}(E)$)

L'application quotient est $\pi_R = \pi : E \to E/_R$, $x \mapsto \pi(x) = \bar{x}$

elle est surjective et, d'après le thm, $\forall x, y \in E$ $x \equiv y \bmod R \Leftrightarrow \pi_R(x) = \pi_R(y)$

[Ainsi l'exemple ③ est "le cas général", cependant il est utile de penser en terme de relation car, la plus part du temps (Ex la congruence mod N dans $\mathbb{N}$) c'est la relation d'équivalence qui permet de construire l'application $\pi : E \to E/_R$]

un ~~système de representant modulo~~ R est une partie $Y \subset E$ t.q.

(1) $\forall x \in E \ \exists y \in Y$ tq $x \equiv y \mod R$

(2) $\forall y, y' \in Y \quad y \equiv y' \mod R \Rightarrow y = y'$

ainsi la restriction de π à Y $\pi_1 : Y \to E/_R$ est bijective et la bijection inverse $s : E/_R \to Y$ est une section de π, c.a.d vérifie $\pi \circ s = Id_{E/_R}$

Dans le cas où E est muni d'un bon ordre (par exemple $E = \mathbb{N}$ et R congruence mod N)

on a le système des plus petits representants, image de la section

$$s_m : E/_R \to E \quad s(\bar{x}) = m(\bar{x}) \text{ le plus petit élement}$$

de la partie non vide $\emptyset \neq \bar{x} \subset E$

La remarque ② donne si $N > 0$

$$s_m\left(\mathbb{N}/_{\mathrm{mod}\,N}\right) \subset \{n \in \mathbb{N} \mid n \lneq N\} = \{0, 1, \dots, N-1\}$$

et si $0 \leqslant r, r' < N$ avec $r \equiv r' \mod N$ alors

(quitte à permutter r et r' il y a $k \in \mathbb{N}$ tq $r + kN = r' \lneq N$

comme si $k > 0$ on a $r + kN \geqslant r + N \geqslant N$ on a $k = 0$ donc $r = r'$. De plus $0 \equiv N \mod N$ donc

Corollaire 1 Si $N > 0$ $\{0, 1, \dots, N-1\}$ est le système des plus petits représentants modulo N et $\{1, \dots, N\}$ est le système des plus petit representants positifs modulo N.

<u>Corollaire 2 (Division euclidienne)</u> Soit N un entier positif ($N \in \mathbb{N}, N > 0$)

Alors pour tout $n \in \mathbb{N}$ il y a des uniques $(q, r) \in \mathbb{N} \times \mathbb{N}$ tq

$$n = r + qN \qquad 0 \leqslant r < N$$

r est le reste de la division de N par q et q le quotient de la division de q par N

pr existence r le plus petit reste modulo N de n et q fourni par Rmq②

unicité si $n = r + qN$ alors $\overline{n} = \overline{r}$ et, comme $0 \leqslant r < N$ r est le plus petit reste mod N,

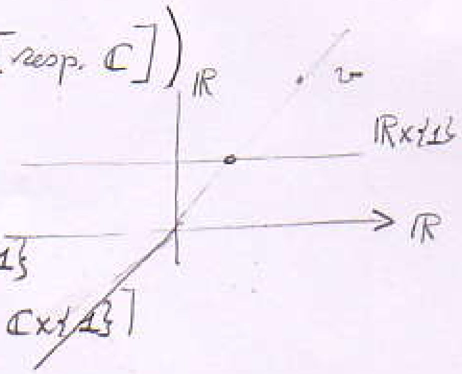
et si $r + qN = r + q'N$ alors Rmq② $qN = q'N$ et, comme $N \neq 0$, $q = q'$. □

<u>Autres exemples d'ens. quotients et de représentant les droites projectives</u>

$E = \mathbb{R} \times \mathbb{R} \setminus \{(0,0)\}$ $\quad$ [resp. $\mathbb{C} \times \mathbb{C} \setminus \{(0,0)\}$]

sur E la relation d'équivalence de colinéarité réelle [resp. complexe] $\mathcal{L}$

(être linéairement indépendant sur $\mathbb{R}$ [resp. $\mathbb{C}$])



Si $0 \neq v = (x, y) \notin \mathbb{R} \times \{0\}$ [resp. $\mathbb{C} \times \{0\}$] : $y \neq 0$

alors $y^{-1} \cdot v = (y^{-1} x, y^{-1} y) = \left(\frac{x}{y}, 1\right) \in \mathbb{R} \times \{1\}$
[resp. $\mathbb{C} \times \{1\}$]

et si $u = (x, 1)$, $u' = (x', 1) \in \mathbb{R} \times \{1\}$ [resp. $\mathbb{C} \times \{1\}$] et $u \equiv u' \bmod \mathcal{L}$

il y a $(\lambda, \lambda') \in \mathbb{R} \times \mathbb{R}$ [resp. $\mathbb{C} \times \mathbb{C}$] $(\lambda, \lambda') \neq 0$ tq $0 = \lambda u + \lambda' u' = (\lambda u + \lambda' u', \lambda + \lambda')$

d'où $\lambda' = -\lambda \neq 0$ et $u' = (\lambda')^{-1} \cdot \lambda' u' = (\lambda')^{-1} \cdot \lambda u = u$

Ainsi $\{(x, 1) \mid x \in \mathbb{R}$ [resp. $\mathbb{C}$]$\}$ est un système de représentants

modulo N sur $E \setminus \mathbb{R} \times \{0\}$ [resp $E \setminus \mathbb{C} \times \{0\}$]

d'autre par $\mathbb{R} \times \{0\}$ [resp $\mathbb{C} \times \{0\}$] $= \overline{(1, 0)}$

La droite projective réelle est $P_1(\mathbb{R}) = \mathbb{R}\times\mathbb{R}\setminus\{(0,0)\} / \mathcal{L}$ [resp. complexe $P_1(\mathbb{C}) = \mathbb{C}\times\mathbb{C}\setminus\{(0,0)\} / \mathcal{L}$]

on note $\overline{(x,y)} = [x:y]$ (coordonnées homogènes) et $\infty = [1:0]$

ainsi, avec la convention si $x \neq 0$ $\frac{x}{0} = \infty$ on identifie $[x:y]$ à $\frac{x}{y} \in \mathbb{R}\cup\{\infty\}$ [resp $\mathbb{C}\cup\{\infty\}$]

3 Passage au quotient

A

Proposition Soit R une relation d'équivalence sur un ens. X et $f : X \to Y$ une application

Alors il y a $\bar{f} : X/_R \to Y$ tq $f = \bar{f}\circ\pi_R$:
$$\begin{tikzcd} X \arrow[rr] \arrow[dr, "\pi"'] & & Y \\ & X/_R \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$
(f se factorise par $X/_R$)

si et seulement si pour tout $x, x' \in X$ $x \equiv x' \bmod R \Rightarrow f(x) = f(x')$

De plus un tel $\bar{f}$ est uniquement déterminé par f : si $\bar{x} \in X/_R$ on a $\bar{f}(\bar{x}) = f(x)$

pv $\Rightarrow$ Si $f = \bar{f}\circ\pi$ et $x \equiv x' \bmod R$ on a $\pi(x) = \pi(x')$ donc
$$f(x) = \bar{f}(\pi(x)) = \bar{f}(\pi(x')) = f(x')$$

$\Leftarrow$ Pour tout $t \in \bar{x}$ (c.à.d $t \equiv x \bmod R$) on a $f(t) = f(x)$

et on peut définir $\bar{f} : X/_R \to Y$ par $\bar{f}(\bar{x}) = x$ (ça ne dépend pas du choix de $x \in \bar{x}$)

Corollaire 1 Soient X et Y deux ens. munis de relations d'équivalence R et S

et $g : X \to Y$ alors g passe au quotient c.a.d. il y a $\bar{g} : X/_R \to Y/_S$ tq $\pi_S\circ g = \bar{g}\circ\pi_R$
$$\begin{tikzcd} X/_R \arrow[r, "\bar{g}"] & Y/_S \\ X \arrow[u, "\pi_R"] \arrow[r, "g"'] & Y \arrow[u, "\pi_S"'] \end{tikzcd}$$
(le diagramme commute)

ssi $\forall x, x'$ tq $x \equiv x' \bmod R$ on a $g(x) \equiv g(x') \bmod S$
(on dit g compatible à R et S [à R si $R = S$]
En ce cas un tel $\bar{g}$ est uniquement déterminé par g : $\bar{g}(\bar{x}_R) = \overline{g(x)}_S$

pv Soit $f = \pi_S\circ g$ on a $f(x) = f(x')$ ssi $g(x) \equiv g(x') \bmod S$ le cas est la prop. pour f. $\square$

<u>co-corollaire</u> Soit X, Y, Z trois ens. munis de relations d'équivalence R, S, T

et $f : X \to Y$, $g : Y \to Z$ deux applications passant au quotient

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d] & Y \arrow[d] \\ X/R \arrow[r, "\bar f"] & Y/S \end{tikzcd} \qquad \begin{tikzcd} Y \arrow[r, "g"] \arrow[d] & Z \arrow[d] \\ Y/S \arrow[r, "\bar g"] & Z/T \end{tikzcd}$$

alors la composée $\begin{tikzcd} X \arrow[r, "g\circ f"] \arrow[d] & Z \arrow[d] \\ X/R \arrow[r, "\overline{g\circ f}"] & Z/S \end{tikzcd}$

passe au quotient en $\overline{g\circ f} = \bar g \circ \bar f$

pv $\pi_T \circ (g\circ f) = (\pi_T \circ g)\circ f = (\bar g \circ \pi_S)\circ f = \bar g \circ (\pi_S \circ f) = \bar g \circ (\bar f \circ \pi_R) = (\bar g \circ \bar f)\circ \pi_R$

d'où le résultat $\bar g \circ \bar f = \overline{g\circ f}$ par l'unicité dans le corollaire. □

<u>Exemple</u> On note $K = \mathbb{R}$ ou $\mathbb{C}$ Soit $f = f_M : K^2 \to K^2$ linéaire injective

de matrice $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(K)$ $(a, b, c, d \in K)$ $\det M = ad - bc \neq 0$

alors f induit $f_1 : K^2 \setminus \{0\} \to K^2 \setminus \{0\}$ compatible avec la colinéarité

pv $x \in K^2 \setminus \{0\}$ donc $x \neq 0 \underset{f \text{ inj}}{\Longrightarrow} f(x) \neq f(0) \underset{\substack{\uparrow \\ f \text{ linéaire}}}{=} 0$ donc $f(x) \in K^2 \setminus \{0\}$

$(\lambda, \mu) \in K^2 \setminus \{(0,0)\}$ $u, v \in K^2 \setminus \{0\}$ $0 = \lambda u + \mu v \Rightarrow 0 = f(\lambda u + \mu v) \underset{f \text{ linéaire}}{=} \lambda f(u) + \mu f(v)$.

elle induit donc l'<u>homographie</u> $\bar f = \bar f_M : P_1(K) \to P_1(K)$

qui dans le système de représentant $K \cup \{\infty\}$ "=" $P_1(K)$ s'écrit

(avec la <u>convention</u> si $x \in K$ $x \neq 0$ $\frac{x}{0} = \infty$) $K \ni t \mapsto \dfrac{at+b}{ct+d}$ $\infty \mapsto \dfrac{a}{c}$

et si $N \in M_2(K)$ $\det N \neq 0$ on a $\bar f_{NM} = \bar f_N \circ \bar f_M$, $\bar f_I = Id_{P_1(K)}$

donc $\bar f_M$ est bijective et si $\tilde M = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ $\bar f_M^{-1} = \bar f_{\tilde M}$.

pv $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = (ad - bc)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ d'où $\bar f_M \circ \bar f_{\tilde M} = \bar f_{\lambda I} = \bar f_{\tilde M} \circ \bar f_M$

et si $\lambda \neq 0$ $\bar f_{\lambda I}(u) = \lambda u \equiv u \bmod \mathcal{L}$ donc $\bar f_{\lambda I} = Id_{P_1(K)}$ ▪

/!\ <u>Exercice</u> En distinguant les $\underbrace{16 = 4 \times 4}$ cas prouver $\overline{f_N} \circ \overline{f_M} = \overline{f_{NM}}$

$(t = \infty$ et $c \neq 0$; $t = \infty$ et $c = 0$; $t \in K$ et $ct + d \neq 0$; $t \in K$ et $ct + d = 0)$ $(f(t) = \infty$ et $\gamma \neq 0$; $f(t) = \infty$ et $\gamma \neq 0$; $f(t) \in K$ et $\gamma f(t) + \delta \neq 0$; $f(t) \in K$ et $\gamma f(t) + \delta = 0)$