Relations d'équivalence

Rappel :

Soit $|E| = n < \infty$. Considérons $U := P(E)$.

Soient A_1 et A_2 deux éléments de $U = P(E)$.

$A_1 \sim A_2$ ssi $|A_1| = |A_2|$.

Une classe d'équivalence

$$\binom{E}{i} := \{A \subseteq E \mid |A| = i\} \subseteq P(E),$$

La collection des classes :

$$U/\sim = \left\{\binom{E}{0}, \binom{E}{1}, \binom{E}{2}, \ldots, \binom{E}{n}\right\} \subseteq P(U) = P(P(E))$$

Chaque élément de $U = P(E)$ est dans une unique classe d'équivalence. Et donc

$$P(E) = \bigcup_{i=0}^{n} \binom{E}{i}$$

est une partition de $P(E)$:
c.-à-d. chaque $\binom{E}{i}$ non-vide, et $\binom{E}{i}$ et $\binom{E}{j}$ disjoints si $i \neq j$.
En conséquence :

$$\boxed{|P(E)| = \sum_{i=0}^{n} |\binom{E}{i}|}$$

$2^3 = 8 = 1 + 3 + 3 + 1$ ✓

Pour $E = \{a, b, c\}$, $U = P(E)$: $\binom{E}{0} = \{\emptyset\}$; $\binom{E}{1} = \{\{a\}, \{b\}, \{c\}\}$;

$$\binom{E}{2} = \{\{b, c\}, \{a, c\}, \{a, b\}\}; \quad \binom{E}{3} = \{E\};$$

$$U = \binom{E}{0} \cup \binom{E}{1} \cup \binom{E}{2} \cup \binom{E}{3};$$

$$U/\sim \;=\; \left\{\binom{E}{0}, \binom{E}{1}, \binom{E}{2}, \binom{E}{3}\right\}.$$

$|U/\sim| = 4$

On a : $a \in \{a, b\}$, $\{a, b\} \in \binom{E}{2}$, $\binom{E}{2} \in (U/\sim)$.

Mais : $\{a, b\} \subseteq E$, $\binom{E}{2} \subseteq U$. $= P(E)$

$A \subset B \wedge B \subset C \Rightarrow A \subset C$

$\cancel{A \in B \wedge B \in C \Rightarrow A \in C}$

Soit U un ensemble.
$F(u_1, u_2)$ une fonction propositionnelle avec univers du discours sur $U \times U$.
Définissons un sous-ensemble $R = R_F \subseteq U \times U$ ainsi :

$$R := \{(u_1, u_2) \in U \times U | \; F(u_1, u_2) \text{ est vraie}\}.$$

Dans le sens inverse. Soit $R \subseteq U \times U$.
Définissons une fonction propositionnelle $F^R(u_1, u_2)$ avec univers du discours sur $U \times U$ par

$$F^R(u_1, u_2) := \text{"}(u_1, u_2) \in R\text{"}.$$

Si $G(u_1, u_2)$ une autre fonction propositionnelle avec univers du discours sur $U \times U$.

Alors $R_F = R_G$ si et seulement si F et G sont logiquement équivalentes. C.-à-d., pour chaque (u_1, u_2) on a $F(u_1, u_2)$ est vraie (c.-à-d. $(u_1, u_2) \in R_F$)) si et seulement si $G(u_1, u_2)$ est vraie (c.-à-d. $(u_1, u_2) \in R_G$)).

La fonction F et la fonction associée à R_F sont logiquement équivalentes.

Exemple :
E un ensemble fini. $U = P(E)$. Une fonction propositionnelle sur $U \times U$:

$$F(A_1, A_2) := "|A_1| = |A_2|"$$

Exemple :
$U = \mathbb{Z}$. Une fonction propositionnelle sur $U \times U$:
$F(n, m)$:="La différence $n - m$ est un nombre entier pair".

Si nous avons fixé une telle fonction F (ou un tel sous-ensemble R), nous allons écrire

$u_1 \sim u_2$ si $(u_1, u_2) \in R$ (ou $F(u_1, u_2)$ est vraie)
et $u_1 \not\sim u_2$ si $(u_1, u_2) \notin R$ (ou $F(u_1, u_2)$ est fausse) .
($\sim$ est appelé la relation associée.)

Definition

Nous allons dire que $\sim$ (ou F ou R) est *une relation d'équivalence* sur U si pour chaque u, v, w élements de U on a
(i) $u \sim u$ (réflexive) ;
(ii) si $u \sim v$ alors $v \sim u$ (symétrique) ;
(iii) si $u \sim v$ et $v \sim w$ alors $u \sim w$ (transitive).
Dans ce cas nous allons dire que u *est équivalent à* v si $u \sim v$.

À la place du symbole $\sim$ aussi autres symboles sont souvent utilisés pour des relations d'équivalence, comme $\equiv$.

Mais le petit règlement restera en force :
(i) $u \equiv u$ (réflexive) ;
(ii) si $u \equiv v$ alors $v \equiv u$ (symétrique) ;
(iii) si $u \equiv v$ et $v \equiv w$ alors $u \equiv w$ (transitive).

Dans la suite nous fixons une relation d'équivalence $\sim$ sur U.

Posons pour $u \in U$ le sous-ensemble
$\mathrm{C}\ell(u) := \{\underline{v \in U} | \underline{u \sim v}\} \subseteq U$,
on dit que c'est la classe d'équivalence de u. C'est la collection de tous les éléments de U équivalents à u.

Chaque élément est contenu dans sa propre classe d'équivalence et si deux classes d'équivalence sont différentes, elles sont mêmes disjoints.

∅ Cℓ

Lemme

Soient $u, v \in U$.
(i) $u \in \mathrm{C}\ell(u)$ *;*
(ii) $\mathrm{C}\ell(u) \cap \mathrm{C}\ell(v) \neq \emptyset$ *si et seulement si* $\mathrm{C}\ell(u) = \mathrm{C}\ell(v)$.

Démonstration.

(i) $u \in \mathrm{C}\ell(u)$ parce que $u \sim u$ (par réflexivité).
(ii) Soit $w \in \mathrm{C}\ell(u) \cap \mathrm{C}\ell(v)$, c.-à-d., $u \sim w$ et $v \sim w$.
Par symétrie aussi $w \sim u$ et $w \sim v$ et
Donc par transitivité on a aussi $u \sim v$, $v \sim u$.
Si $x \in \mathrm{C}\ell(u)$ alors par définition $u \sim x$ et donc $x \sim u$.
Avec $u \sim v$ et transitivité il suit $x \sim v$ et $v \sim x$, alors $x \in \mathrm{C}\ell(v)$.
Donc $\mathrm{C}\ell(u) \subseteq \mathrm{C}\ell(u) \cap \mathrm{C}\ell(v) \subseteq \mathrm{C}\ell(u)$.
Il suit $\mathrm{C}\ell(u) = \mathrm{C}\ell(u) \cap \mathrm{C}\ell(v)$ et $\mathrm{C}\ell(u) = \mathrm{C}\ell(v)$. □

$(u \sim w) \wedge (w \sim v)$
$\rightarrow u \sim v$ ✓

Considérons la collection des classes d'équivalence différentes

$$U/\sim := \{C\ell(u) \mid u \in U\} \subseteq P(U).$$

$\neq$

$C\ell(u) \in P(U)$

Cet ensemble vient avec une fonction surjective

$$\boxed{C\ell : U \to U/\sim}$$

qui associe à u sa classe $C\ell(u)$, c'est la fonction "classification".

La partie gauche est la collection d'éléments qu'on veut classifier, la partie droite est la collection des classes.

La fonction $C\ell$ met chaque élément u dans la classe appropriée $C\ell(u)$.

Si $|U| < \infty$ alors

$$|U| = \sum_{C \in U/\sim} |C|$$

parce que chaque élément est dans une unique classe (on ne compte pas double).

Vous comprenez ?

Les fractions.

Soit $U := \{(n, d) \in \mathbb{Z} \times \mathbb{Z} | \ d \neq 0\}$.
Posons

$$(n, d) \sim (n', d') \text{ si et seulement si } nd' = n'd.$$

C'est une relation d'équivalence sur U.

Démonstration.

Soient (n_1, d_1), (n_2, d_2) et (n_3, d_3) trois éléments de U, c.-à-d., n_1, n_2, n_3 trois entiers, et d_1, d_2, d_3 trois non-zéro entiers.
Il faut vérifier trois choses.
(i) $(n_1, d_1) \sim (n_1, d_1)$; c'est le cas car $d_1 n_1 = d_1 n_1$.

(ii) si $(n_1, d_1) \sim (n_2, d_2)$ alors $(n_2, d_2) \sim (n_1, d_1)$; c'est le cas car $n_1 d_2 = n_2 d_1$ implique que $n_2 d_1 = n_1 d_2$. □

(Suite).

(iii) si $(n_1, d_1) \sim (n_2, d_2)$ et $(n_2, d_2) \sim (n_3, d_3)$ alors à montrer $(n_1, d_1) \sim (n_3, d_3)$.
Pour montrer ça, supposons que l'hypothèse est vraie, alors $n_1 d_2 = n_2 d_1$ et $n_2 d_3 = n_3 d_2$. Alors aussi $n_1 d_2 d_3 = n_2 d_1 d_3$ et $n_2 d_3 d_1 = n_3 d_2 d_1$ et $n_1 d_2 d_3 = n_3 d_2 d_1$. Donc $d_2(n_1 d_3 - n_3 d_1) = 0$.
Nous savons : si $rs = 0$ et $r \neq 0$ alors nécessairement $s = 0$ (r, s entiers).
Par hypothèse $d_2 \neq 0$ et $d_2(n_1 d_3 - n_3 d_1) = 0$. Donc nécessairement $(n_1 d_3 - n_3 d_1) = 0$, ou $n_1 d_3 = n_3 d_1$, ou $(n_1, d_1) \sim (n_3, d_3)$. ✓
Alors en effet, $\sim$ est une relation d'équivalence sur U. □

?

lemme acceptons

Nous connaissons déjà les classes d'équivalences !

Definition

Avec cette relation d'équivalence $\sim$ sur U.
(i) Pour $(n, d) \in U$ (donc n, d sont deux entiers, dont $d \neq 0$) nous définissons *la fraction*

$$\frac{n}{d} := \mathrm{C}\ell(n, d);$$

la classe d'équivalence de $(n, d) \in U$.
(ii) Nous définissons

$$\mathbb{Q} = U/\sim;$$

l'ensemble des classes d'équivalence.

En particulier $\frac{n_1}{d_1} = \frac{n_2}{d_2}$ si et seulement si (par définition) $n_1 d_2 = n_2 d_1$. Par exemple $\frac{2}{5} = \frac{6}{15}$, car $2 \cdot 15 = 6 \cdot 5 = 30$.
Et $\frac{2}{0}$ n'est pas définie !
Nous définissons l'addition et la multiplication :

$$\frac{n_1}{d_1} + \frac{n_2}{d_2} := \frac{n_1 d_2 + n_2 d_1}{d_1 d_2}; \quad \frac{n_1}{d_1} \cdot \frac{n_2}{d_2} := \frac{n_1 n_2}{d_1 d_2}.$$

Il y a une fonction injective $\iota : \mathbb{Z} \to \mathbb{Q}$ avec $\iota(n) := \frac{n}{1}$.
Puis on identifie $n = \frac{n}{1}$ (malgré que n est un entier et pas une fraction).

Et cetera.

$\frac{2}{5} = \frac{6}{15}$ [illegible] $2 \cdot 15 = 6 \cdot 5$

$cl(2,5) = cl(6,15)$

$\frac{2}{5} = \frac{6}{15} = 6.4$

Les classes d'entiers modulo m.

Soient d, n deux entiers. On dit que d divise n, et on écrit $d|n$ s'il existe un $q \in \mathbb{Z}$ tel que $n = qd$.

Chaque nombre naturel m donne une relation d'équivalence, $\equiv_m$, appelé la relation modulo m :

$$n_1 \equiv_m n_2 \text{ si } m \text{ divise } n_1 - n_2. \qquad m \mid (n_1 - n_2)$$

Autre notation $n_1 \equiv n_2 \mod m$.

Si $n_1 \equiv_m n_2$ on dit "n_1 est congru à n_2 modulo m".

La classe de n est notée $C\ell_m(n)$ ou $C\ell(n)$ si m est fixé dans la discussion.

L'ensemble des classes $\mathbb{Z}/\equiv_m$ est noté $\boxed{\mathbb{Z}/m\mathbb{Z}}$. $= \{ c\ell(0), c\ell(1), \ldots, c\ell(m-1) \}$ si $m > 0$

La fonction classification : $C\ell_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

$n \mapsto c\ell_m(n)$

Donc on peut considérer $\mathrm{C}\ell_m(n)$ comme un élément de $\mathbb{Z}/m\mathbb{Z}$ ou comme un certain sous-ensemble de $\mathbb{Z}$. Mais on ne peut pas le considérer comme un nombre entier.

On définit l'addition et la multiplication sur $\mathbb{Z}/m\mathbb{Z}$

$$\mathrm{C}\ell_m(n_1) + \mathrm{C}\ell_m(n_2) := \mathrm{C}\ell_m(n_1 + n_2)$$

et

$$\mathrm{C}\ell_m(n_1) \cdot \mathrm{C}\ell_m(n_2) := \mathrm{C}\ell_m(n_1 \cdot n_2).$$

$\frac{1}{2} = \frac{2}{4}$

Exemple à revenir avec les détails ! !

$f : \mathbb{Q} \longrightarrow \mathbb{Z}$ $\quad f\left(\frac{n}{m}\right) = n + m$

$f\left(\frac{1}{2}\right) = 1+2 = 3$

$f\left(\frac{2}{4}\right) = 2+4 = 6$

Autre exemple :
Chaque fonction avec domaine U induit une relation d'équivalence sur U.

Soit $f : U \to V$ une fonction. Définissons $F(u_1, u_2) :=$ "$f(u_1) = f(u_2)$" avec univers du discours $U \times U$. Alors F définit une relation d'équivalence sur U.

Classe d'équivalence de u est $\mathrm{C}\ell(u) = \{u' \in U |\ f(u') = f(u)\}$.
Donc les classes d'équivalence sont exactement les pré-images non-vides $f^{-1}(v)$ où $v \in \mathrm{Im}(f)$.

Il y a une fonction $\overline{f} : (U/\sim) \to V$ définie par $\overline{f}(\mathrm{C}\ell(u)) := f(u)$. Donc $f = \overline{f} \circ \mathrm{C}\ell$.

Démonstration.

(a) Une relation d'équivalence : Pour (i) : car $f(u) = f(u)$;
pour (ii) : car $f(u_1) = f(u_2)$ implique $f(u_2) = f(u_1)$;
pour (iii) : Si $u_1 \sim u_2$ et $su_2 \sim u_3$ alors $f(u_1) = f(u_2)$ et $f(u_2) = f(u_3)$.
Donc $f(u_1) = f(u_2) = f(u_3)$. D'où : $u_1 \sim u_3$.

(b) Est ce que $\overline{f}$ est en fait une fonction ?
Chaque élément de $(U/\sim)$ est de la forme $C\ell(u)$, mais u n'est pas unique.
On a $C\ell(u) = C\ell(u')$ si par définition $f(u) = f(u')$. Donc
$\overline{f}(C\ell(u)) = f(u) = f(u') = \overline{f}(C\ell(u'))$ et la définition ne dépend pas du choix de u dans sa classe d'équivalence.

$\square$

Par exemple, chaque relation d'équivalence $\sim$ donne une fonction avec domaine U :
$C\ell : U \to U/\sim$.
Mais la relation d'équivalence associée à cette fonction $C\ell$ coincide avec $\sim$. Il n'y a rien de nouveau.

Exemple :

Chaque partition de U donne une relation d'équivalence sur U.

Soit $U = \cup_{i \in I} A_i$ une partition de l'ensemble U.

C.-à-d. il existe un autre ensemble I et une fonction injective
$F : I \to P(A)$, disons $A_i := F(i)$, telle que
- $A_i \neq \emptyset$ pour chaque $i \in I$;
- A_i et A_j sont disjoints si $i \neq j$ et
- pour chaque $u \in U$ il existe un (unique) $i \in I$ tel que $u \in A_i$.

Définissons

$$F(u, v) := \text{"}\exists i \in I \, [u \in A_i] \wedge [v \in A_i]\text{"}$$

avec $U \times U$ l'univers du discours. Alors F induit une relation d'équivalence $\sim$ sur U.

Dans cette situation encore :

Définissons la fonction

$$f : U \to I$$

telle que $f(u) = i \in I$ si et seulement si $f(u) \in A_i$. C'est une fonction.

La relation d'équivalence associée à f est la même que la relation d'équivalence associée à la partition et celui associé à F.

Les A_i sont les classes d'équivalences. Soit $a_i \in A_i$ (existe, car non-vide). Alors $C\ell(a_i) = A_i$.

Chaque $i \in I$ détermine une unique classe d'équivalence : on obtient une fonction bijective

$$\overline{f} : I \to U/\sim .$$

Soit U un ensemble. Alors les partitions de U et les relations d'équivalence sur U sont presque "la même chose" : l'une donne l'autre et vice versa.

Chaque fonction avec domain U donne une relation d'équivalence. Chaque relation d'équivalence donne au moins la fonction $\mathrm{C}\ell : U \to U/\sim$.

Conclusion : Il y a beaucoup de relations d'équivalences sur U.

Si $|U| = n$. On a combien de partitions de U (où combien de relations d'équivalence sur U) ? On peut les compter ? On verra plus tard.

fin 13/10

Rappel :

Definition

Soient n, m deux entiers. On écrit $n \leq m$ (ou $m \geq n$) s'il existe un $r \in \mathbb{N}$ tel que $n + r = m$.

Definition

Soient d, m deux entiers. On écrit $d|m$ (ou $d \geq n$) s'il existe un $q \in \mathbb{Z}$ tel que $qd = m$.

Si $n \leq m$ on dit "n est plus petit que ou égal à m", ou "m est plus grand que ou égal à n".
Si $d|m$ on dit que "d divise m", ou "m est divisible par d".

Théorème

Soient a, b, c trois nombres entiers.
(i) Si $a \leq b$ et $b \leq c$ alors $a \leq c$.
(ii) Si $a \leq b$ alors $a + c \leq b + c$.
(iii) Si $a \leq b$ et $c \in \mathbb{N}$ alors $ac \leq bc$
(iv) Si $a \leq b$ alors $-b \leq -a$.

Théorème

Soient a, b, c trois nombres entiers.
(i) Si $a|b$ et $b|c$ alors $a|c$.
(ii) Si $a|b$ alors $ac|bc$ et $a|bc$.
(iii) Si $a|b$ et $a|c$ alors $a|(b + c)$.

Démonstration.

(i) Si $a \leq b$ et $b \leq c$ il existe $r, s \in \mathbb{N}$ tels que $a + r = b$ et $b + s = c$. Donc $a + (r + s) = b + s = c$ et $r + s \in \mathbb{N}$ donc $a \leq c$.

Si $a|b$ et $b|c$ il existe $r, s \in \mathbb{Z}$ tels que $ar = b$ et $bs = c$. Donc $a(rs)) = bs = c$ et $rs \in \mathbb{Z}$ donc $a|c$.

(ii) Si $a \leq b$ alors il existe $r \in \mathbb{N}$ tel que $a + r = b$. Donc $(a + c) + r = b + c$ et $a + c \leq b + c$.

Si $a|b$ alors il existe $r \in \mathbb{Z}$ tel que $ar = b$. Donc $(ac)r = bc$ et $ac|bc$. Aussi $a|ac$ donc par (i) : $a|bc$. $\square$

suite.

(iii) Si $a \leq b$ il existe $r \in \mathbb{N}$ tel que $a + r = b$. Si aussi $c \in \mathbb{N}$ alors $rc \in \mathbb{N}$ et $ac + rc = (a + r)c = bc$, donc $ac \leq bc$.
Si $a|b$ et $a|c$ alors il existe $r, s \in \mathbb{Z}$ tels que $ar = b$ et $as = c$. Donc $a(r + s) = ar + as = b + c$ et $a|(b + c)$.

(iv) Si $a \leq b$, il existe $r \in \mathbb{N}$ tel que $a + r = b$. Donc $-b + r = -a$ et $-b \leq -a$.

$\square$

Rappel : pour des entiers a, b, m :

$$a \equiv_m b \ \text{ si } \ m | (a - b).$$

Théorème

Soient a, b, c, d, m des nombres entiers.

Si $a \equiv_m b$ et $c \equiv_m d$, alors $(a + c) \equiv_m (b + d)$ et $(ac) \equiv_m (bd)$.

Ou si $\mathrm{C}\ell_m(a) = \mathrm{C}\ell_m(b)$ et $\mathrm{C}\ell_m(c) = \mathrm{C}\ell_m(d)$, alors $\mathrm{C}\ell_m(a + c) = \mathrm{C}\ell_m(b + d)$ et $\mathrm{C}\ell_m(ac) = \mathrm{C}\ell_m(bd)$.

Démonstration.

Si $a \equiv_m b$ et $c \equiv_m d$ alors il existe r, s entiers tels que $mr = (a - b)$ et $ms = (c - d)$.

Donc $m(r + s) = (a - b) + (c - d) = (a + c) - (b + d)$ et $(a + c) \equiv_m (b + d)$.

Et aussi $a = b + mr$ et $c = d + ms$. Donc

$$ac - bd = (b + mr)(d + ms) - bd = m(rd + bs + mrs),$$

ce qui implique que $(ac) \equiv_m (bd)$.

$\square$