Aujourd'hui nous allons discuter :

- Rappel : relation d'équivalence
- Nouveaux "nombres" : $\mathbb{Q}$ et $\mathbb{Z}/m\mathbb{Z}$.
- Calculer avec $\mathbb{Q}$ et $\mathbb{Z}/m\mathbb{Z}$.

Relations d'équivalences

Rappel. Soit U un ensemble avec une relation $a \sim b$ entre deux élements de U.
Alors $\sim$ est une relation d'équivalence si pour chaque a, b, c dans U on aurait :

(i) $a \sim a$;

(ii) $(a \sim b) \to (b \sim a)$;

(iii) $((a \sim b) \wedge (b \sim c)) \to (a \sim c)$.

Soit $\sim$ une relation d'équivalence sur U. Et $a \in U$.

$$C\ell(a) := \{u \in U | \ c \sim u\}.$$

Considère $C\ell(a) \in P(U)$.
L'ensemble des classes d'équivalence différentes :

$$U/\sim := \{C\ell(a) | \ a \in U\} \subset P(U).$$

Et la fonction classification :

$$C\ell : U \to U/\sim .$$

Qui est surjective.
On a divisé U en classes.

On a $C\ell(a) = C\ell(b)$ si et seulement si $a \sim b$.

Les classes forment une partition de U :

les classes sont non-vides, l'union des classes est U, et l'intersection de deux classes diférentes est vide.

$\equiv_m$

Pour chaque entier $m > 0$, la relation $\equiv_m$ est une relation d'équivalence sur $\mathbb{Z}$.

La classe de n s'écrit comme $\mathrm{C}\ell_m(n)$. On a

$$\mathrm{C}\ell_m(n) = \mathrm{C}\ell_m(n + 3 \cdot m) = \mathrm{C}\ell(n - 1234 \cdot m)$$

Il y a exactement m classes d'équivalence différentes.

L'ensemble des classes d'équivalence s'écrit comme

$$\mathbb{Z}/m\mathbb{Z} := \mathbb{Z}/\equiv_m$$

$$= \{\mathrm{C}\ell_m(0), \mathrm{C}\ell_m(1), \mathrm{C}\ell_m(2), \ldots, \mathrm{C}\ell_m(m-1)\}$$

On définit :

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

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

Est-ce que ça fait du sens ?

Ils se comportent comme des "nombres".

Autre exemple : Les fractions.

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

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

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 parce que $d_1 n_1 = d_1 n_1$. □

(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) Supposons $(n_1, d_1) \sim (n_2, d_2)$ et $(n_2, d_2) \sim (n_3, d_3)$.
(Il faut montrer $(n_1, d_1) \sim (n_3, d_3)$.)

Par cette hypothèse : $n_1 d_2 = n_2 d_1$ 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. □

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 $(n_1, d_1) \sim (n_2, d_2)$
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 :

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

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

Est-ce que ça fait du sens ?

Il y a quelque chose à vérifier : est-ce que ça dépend du choix d'écrire la fraction ? Si

$$\frac{n_1}{d_1} = \frac{n_1'}{d_1'} \text{ et } \frac{n_2}{d_2} = \frac{n_2'}{d_2'}$$

est-ce que aussi

$$\frac{n_1 d_2 + n_2 d_1}{d_1 d_2} = \frac{n_1' d_2' + n_2' d_1'}{d_1' d_2'}$$

et

$$\frac{n_1' n_2'}{d_1' d_2'} = \frac{n_1' n_2'}{d_1' d_2'} ?$$

OUI. (Ce sera une exercice pour le TP de la semaine prochaine.)

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).

Autre exemple

Soit E un ensemble fini et $U = P(E)$. Une fonction propositionnelle avec univers de discours $U \times U$ est

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

Nous allons classifier les sous-ensembles selon leur taille.
$A_1 \sim A_2$ si $P(A_1, A_2)$ vraie, c-à-d., si $|A_1| = |A_2|$

On a trivialement

- $A_1 \sim A_1$,
- si $A_1 \sim A_2$ alors $A_2 \sim A_1$,
- si $A_1 \sim A_2$ et $A_2 \sim A_3$ alors $A_1 \sim A_3$.

Une classe d'équivalence est la réunion de tous les éléments de $P(E)$ d'un même taille. Notation :

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

l'ensemble de tous les sous-ensembles de E avec exactement i éléments.

La collection des classes (différentes) est notée :

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

Chaque élément de $U = P(E)$ (=chaque sous-ensemble de 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 $\binom{E}{i}$ est non-vide, et $\binom{E}{i}$ et $\binom{E}{j}$ sont disjoints si $i \neq j$.

En conséquence :

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

Si $E = \{a, b, c\}$.

$$\begin{aligned}
\binom{E}{0} &= \{\emptyset\} \\
\binom{E}{1} &= \{\{a\}, \{b\}, \{c\}\} \\
\binom{E}{2} &= \{\{b, c\}, \{a, c\}, \{a, b\}\} \\
\binom{E}{3} &= \{E\}
\end{aligned}$$

La collection des classes est un ensemble soi-même !

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

Il y a une fonction naturelle :

$$f : P(E) \to P(E)/\sim$$

où on définit $f(A) = \binom{E}{|A|}$.
C.-à-d., on envoie chaque élément vers la classe qui le contient.

Et la fonction $f : P(E) \to P(E)/\sim$ devient

$$f = \begin{pmatrix} \{\emptyset\} & \{a\} & \{b\} & \{c\} & \{b,c\} & \{a,c\} & \{a,b\} & E \\ \binom{E}{0} & \binom{E}{1} & \binom{E}{1} & \binom{E}{1} & \binom{E}{2} & \binom{E}{2} & \binom{E}{2} & \binom{E}{3} \end{pmatrix}$$

Par exemple $f(\{a,c\}) = \binom{E}{2}$.

Saisir les différences :

$$\begin{aligned} U &= P(E) = \binom{E}{0} \cup \binom{E}{1} \cup \binom{E}{2} \cup \binom{E}{3}; \\ U/\sim &= \{\binom{E}{0}, \binom{E}{1}, \binom{E}{2}, \binom{E}{3}\} \subset P(P(E)). \end{aligned}$$

On a :

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

Mais :

$$\{a, b\} \subset E,\ \binom{E}{2} \subset U.$$

Partition et relation d'équivalence

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

Soit

$$U = U_1 \cup U_2 \cup \ldots \cup U_n$$

une partition de U.
C.-à-d. Les U_i sont des sous-ensembles non-vides de U et

$$U_i \cap U_j = \emptyset$$

si $i \neq j$.
Ou, chaque $u \in U$ est dans un unique U_i.

Définissons

$$u \sim v := \text{"}\exists i\ [u \in U_i] \wedge [v \in U_i]\text{"}$$

une relation sur $U \times U$.
C'est une relation d'équivalence sur U. (Facile à vérifier, à vous le faire.)

Si $u \in U_i$, alors $u \sim v$ si et seulement si (aussi) $v \in U_i$, donc $C\ell(u) = U_i$.

Donc les tranches U_i sont aussi les classes d'équivalence si chaque U_i est non-vide.

Exemples :

$g : \mathbb{Q} \to \mathbb{Z}$ est une fonction si $g(\frac{n}{d}) = n + d$? Non.

$g : \mathbb{Q} \to \mathbb{R}$ est une fonction si $g(\frac{n}{d}) = (3n^2 + 2d^2)/d^2$? Oui.

$g : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ est une fonction si $g(\frac{n}{d}, \frac{n'}{d'}) = \frac{nd' + n'd}{dd'}$? Oui.

$g : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}$ est une fonction si $g(C\ell(n)) = n$? Non.

$g : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ est une fonction si
$g(C\ell(n), C\ell(n')) = C\ell(n + 3n')$? Oui.

La fonction mod *m*

Fixons $m > 0$. Soit $a = qm + r$, ou $q \in \mathbb{Z}$ et $0 \leq r < m$. Alors ce reste r est unique.
On obtient une fonction

$$\text{Reste-modulo-}m : \mathbb{Z} \to \{0, 1, 2, \ldots, m-1\}$$

définie par

$$\text{Reste-modulo-}m(a) = r.$$

On a $a \equiv_m b$ si et seulement si a et b ont le même reste modulo m, ou
Reste-modulo-$m(a)$ = Reste-modulo-$m(b)$

Modulo m et division.

C'est utile de voir les $C\ell_m(a)$ comme une sorte de nombre, avec addition, multiplication, soustraction.

Est-ce qu'on peut diviser ?

Nos algorithmes d'Euclide et de Bézout ont des conséquences "modulo m" aussi.

Une formulation

Théorème

Fixons trois nombres entiers a, b, m et supposons $m > 0$. Mettons $d = \text{pgcd}(a, m)$. Considérons l'équation

$$aX \equiv_m b.$$

(i) On peut trouver un entier x qui satisfait cette équation si et seulement si

$$d \mid b.$$

(ii) Si $x' \equiv_m x$, alors x est aussi une solution.

Reformulé :

Théorème

Fixons $m > 0$ et deux classes-modulo-m $\mathrm{C}\ell_m(a)$, $\mathrm{C}\ell_m(b) \in \mathbb{Z}/m\mathbb{Z}$. Mettons $d = \mathrm{pgcd}(a, m)$. Considérons l'équation

$$\mathrm{C}\ell_m(a) \cdot X = \mathrm{C}\ell_m(b).$$

On peut trouver une classe-modulo-m $X = \mathrm{C}\ell(x) \in \mathbb{Z}/m\mathbb{Z}$ qui satisfait cette équation
si et seulement si

$$d | b.$$

Démonstration.
(i) Supposons d'abord que pour $x \in \mathbb{Z}$ on a $ax \equiv_m b$. Alors $m|(ax - b)$ et il existe un entier c tel que $ax - b = cm$. On a que $d|a$ et $d|m$ et on conclut que $d|(ax - cm)$ et $d|b$.

Par contre, supposons $d|b$. Il existe un entier c tel que $b = cd$. Par le théorème de Bézout, il existe deux entiers s, t tels que $sa + tm = d$; et donc aussi $csa + ctm = cd = b$. Alors $csa - b$ est divisible par m et

$$csa \equiv_m b.$$

Alors $x = cs$ satisfait l'équation.
(ii) Si $x' \equiv_m x$, alors il existe $s \in \mathbb{Z} : x' = x + sm$, alors $ax' = a(x + sm) = ax + asm \equiv_m ax \equiv_m b$. □

Peut-on résoudre-modulo-1064 l'équation

$$1351x \equiv_{1064} 21?$$

Heureusement, nous avons déjà calculé que $\text{pgcd}(1351, 1074) = 7$, et 7 divise la partie droite 21 : une solution existe !

Par contre l'équation

$$1351x \equiv_{1064} 29$$

on ne peut pas résoudre, car 7 ne divise pas 29.

Pour trouver une solution, on commence par trouver s, t par la méthode de Bézout, tels que $s1351 + t1064 = 7$. Ce que nous avons aussi déjà fait !

$$(-63) \cdot 1351 + 80 \cdot 1064 = 7$$

donc en multipliant par 3 :

$$(-3 \cdot 63) \cdot 1351 + (3 \cdot 80) \cdot 1064 = 3 \cdot 7 = 21$$

et

$$(-3 \cdot 63) \cdot 1351 \equiv_{1064} 21$$

Donc $x = -3 \cdot 63 = -189$ est une solution.
Si on veut une solution positive on ajoute 1064, c.-à-d.,
$x = -189 + 1064 = 875$ est aussi une solution.

Simplification :

Si a, b, c sont trois entiers et

$$ac = bc.$$

On ne peut pas conclure que $a = b$, sauf si $c \neq 0$.

Et modulo m ?
Attention :
$1 \cdot 2 \equiv_4 3 \cdot 2$ mais $1 \not\equiv_4 3$.
Donc on ne peut pas toujours simplifier.

Mais on peut simplifier sous une condition.

Proposition

Soit m un entier positif, et a, b, c des entiers. Si $ac \equiv_m bc$ et $\text{pgcd}(c, m) = 1$, alors $a \equiv_m b$.

Démonstration.

Par Bézout, il existe entiers s et t tels que $sm + tc = 1$, donc $tc \equiv_m 1$. Donc si $ac \equiv_m bc$ on a aussi $atc \equiv_m btc$ et

$$a \equiv_m atc \equiv_m btc \equiv_m b.$$

Soit $m > 0$.
On dit que $\mathrm{C}\ell_m(b)$ est un inverse-modulo-m de $\mathrm{C}\ell_m(a)$ si

$$\mathrm{C}\ell_m(a)\,\mathrm{C}\ell_m(b) = \mathrm{C}\ell_m(1).$$

Proposition

(i) Une telle inverse existe si et seulement si $\mathrm{pgcd}(a, m) = 1$.
(ii) m est un nombre premier, si et seulement si un inverse-modulo-m existe pour chaque $\mathrm{C}\ell_m(a) \neq \mathrm{C}\ell_m(0)$.

Si un inverse existe, c'est unique. Pouvez-vous montrer ça ?

Démonstration.

(i) est un corollaire de la prop. avant. Si m est premier, et $\mathrm{C}\ell(a)\neg\,\mathrm{C}\ell(0)$ alors $\mathrm{pgcd}(a,m)=1$, alors $\mathrm{C}\ell(a)$ a un inverse. Si m est un nombre tel que un inverse-modulo-m existe pour chaque $\mathrm{C}\ell_m(a)\neq\mathrm{C}\ell_m(0)$. Si $m=rs$ est composé, alors $\mathrm{C}\ell(r)\,\mathrm{C}\ell(s)=\mathrm{C}\ell(m)=\mathrm{C}\ell(0)$. Soit $\mathrm{C}\ell(b)$ l'inverse de $\mathrm{C}\ell(r)$, alors

$$\mathrm{C}\ell(s)=\mathrm{C}\ell(b)\,\mathrm{C}\ell(r)\,\mathrm{C}\ell(s)=\mathrm{C}\ell(b)\,\mathrm{C}\ell(0)=\mathrm{C}\ell(0)$$

et $\mathrm{C}\ell(1)=\mathrm{C}\ell(s)\,\mathrm{C}\ell(r)=\mathrm{C}\ell(0)$. Contradiction. Donc m est premier. □

Si $C\ell_m(b)$ est un inverse-modulo-m de $C\ell_m(a)$, nous pouvons résoudre l'équation

$$C\ell_m(a)X = C\ell(c)$$

Car $C\ell_m(a) \cdot X = C\ell_m(c)$ si et seulement si

$$X = C\ell_M(b)\, C\ell_m(a)X = C\ell_m(b)\, C\ell_m(c) = C\ell_m(bc).$$

Alors $X = C\ell_m(bc)$ est une solution :

$$C\ell_m(a)\, C\ell_m(bc) = C\ell_m(a)\, C\ell_m(b)\, C\ell_m(c) = C\ell(c).$$

Si p est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. Par contre $\mathbb{Z}$ n'est pas un corps.

Conséquence : une très grande partie de MAT1600 reste valable si on remplace $\mathbb{R}$ par un corps, en particulier $\mathbb{Z}/p\mathbb{Z}$!

Résoudre un système d'équations linéaires, méthode de Gauss, forme échelonnée, matrices inversibles, déterminant, espace vectoriel.... On a beaucoup de théorèmes et méthodes sur les équations linéaires avec coefficients dans $\mathbb{Z}/p\mathbb{Z}$ sans frais additionnels, (presque] pour le même prix. Ex :

$$M = \begin{pmatrix} C\ell_5(2) & C\ell_5(3) \\ C\ell_5(1) & C\ell_5(2) \end{pmatrix}$$

est inversible car son déterminant est $C\ell_5(1)$ et donc non-zéro. $M^{-1} =$?.