Rappels . loi de composition : application : $E \times E \to E$ $:(x,y) \longmapsto x*y \in E$

. Groupe : $(G;*)$, G ensemble, $*$ loi de composition associative + él neutre, tout élément inversible.

. sous groupe : $(H;*)$ avec $H \subset G$ t.q $*$ de G définit un groupe sur H.

. Thm : H sous groupe de G $\iff$ $x,y \in H \Rightarrow x*y \in H$ et $x^{-1} \in H$

II. Les corps

Nous avons passé une semaine à étudier les lois de composition et la notion de groupe, un ensemble muni d'une loi de composition particulièrement chouette. Aujourd'hui, pour abstraire l'essence des nombres réels, rationnels ou complexes, nous allons ajouter une deuxième loi de composition, compatible avec la première. Nous serons ainsi amenés à considérer des objets appelés *anneaux* dont les plus aboutis sont les *corps*.

1 Les anneaux

Lorsque l'on a deux nombres réels dans la main, on peut les additionner ou les multiplier. Ces deux opérations, l'addition et la multiplication, sont des lois de composition.

Définition 1.1. Un *anneau* est un ensemble A muni de deux lois de compositions, notées $+$ et $\cdot$, telles que :

a) $(A,+)$ est un groupe abélien ; (↪ commutatif)

b) la multiplication est associative et possède un élément neutre, noté 1_A ou 1 ;

c) la multiplication est distributive par rapport à l'addition : (à gauche ou à droite)

$$x(y+z) = xy + xz \text{ et } (x+y)z = xz + yz,$$

pour tous $x, y, z \in A$.

a priori, on ne demande pas l'inversibilité pour $\cdot$, ni la commutativité.

On dit que l'anneau $(A,+,\cdot)$ est *commutatif* si la multiplication est commutative.

Voici quelques propriétés élémentaires, valides dans tous les anneaux, qui permettent aussi de simplifier les notations. Les preuves sont basées principalement sur la distributivité.

Lemme 1.2. *Soient $x, y \in A$. Alors :*

a) $0 \cdot x = 0 = x \cdot 0$; (où 0 est l'élément neutre de + : $0 = e_+$)

b) $(-1) \cdot x = -x = x \cdot (-1)$; (−x est donc "l'inverse" de x relativement à +, c'est-à-dire l'opposé de x)

c) $(-x)y = -xy = x(-y)$.

Démonstration.

a) On écrit $0 = 0 + 0$ et on multiplie à droite par $x \in A$. Il vient

$0x = (0+0)x = 0x + 0x$ (distributivité)

L'oppose de $0 \cdot x$ est $-(0x)$, qu'on ajoute de chaque côté de l'égalité :

$0 = -0x + 0x = -0x + 0x + 0x = 0x$ ✓

De même $0 = x \cdot 0$ en multipliant $0 = 0+0$ à gauche par x.

b) En utilisant a), on peut écrire

$0 = 0x = (1+(-1))x = 1 \cdot x + (-1)x = x + (-1)x$.

$\Rightarrow (-1)x$ est l'oppose de x, c'est-à-dire $(-1)x = -x$.

De même, $0 = x \cdot 0 = \dots = x(-1) + x$ d'où $x(-1) = -x$.

c) En utilisant b), on peut écrire

$$(-x)y \overset{\text{b)}}{=} ((-1)x) \cdot y \overset{\text{associativité}}{=} (-1)(x \cdot y) \overset{\text{b)}}{=} -xy$$

□

Exemple 1.3. Les nombres entiers $\mathbb{Z}$ forment un anneau avec l'addition et la multiplication usuelle. Nous savons que $(\mathbb{Z}, +)$ est un groupe abélien, que la multiplication est une loi de composition associative pour laquelle 1 est l'élément neutre. Enfin, la multiplication est définie de telle sorte que la distributivité soit vérifiée puisqu'on pose par récurrence $(n+1)k = nk + k$.
De même, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ forment des anneaux qui contiennent chaque fois le précédent.

Exemple 1.4. L'*anneau nul* n'a qu'un élément, à savoir 0. On définit $0 + 0 = 0$ et $0 \cdot 0 = 0$.

Exemple 1.5. L'ensemble des parties $\mathcal{P}(E)$ d'un ensemble E est un anneau. commutatif car $\cap$ l'est.

Addition : différence symétrique Δ et la multiplication : intersection

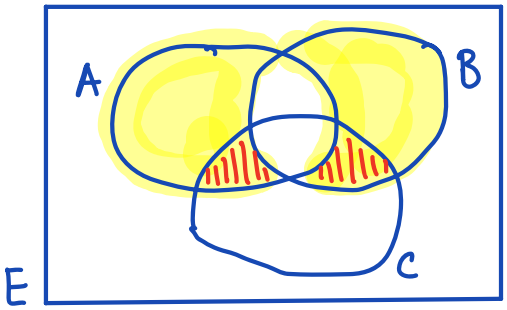
Vu dans la série 13 : $(\mathcal{P}(E) ; \Delta)$ est un groupe abélien.

Vu la semaine dernière : $\cap$ est une loi de composition associative avec pour élément neutre E.

Il nous reste à vérifier la distributivité, ce que nous ferons sur la base d'un diagramme de Venn :

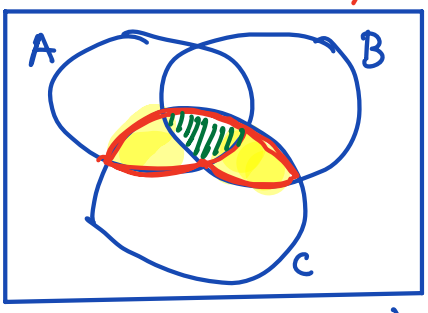
Soit $A, B, C \in \mathcal{P}(E)$. On veut $(A \Delta B) \cap C = (A \cap C) \Delta (B \cap C)$

Rappel : $A \Delta B = (A \cup B) \setminus (A \cap B)$



$(A \Delta B) \cap C$

$(A \cap C) \cup (B \cap C)$ $(A \cap C) \cap (B \cap C)$



$(A \cap C) \Delta (B \cap C)$

⚠ ça ne marche pas si on remplace $\cap$ par $\cup$.

On appelle cet anneau *booléen* car $A \cap A = A$ pour tout $A \subset E$.
En notation muliplicative, cette propriété s'écrit $x \cdot x = x$, c'est-à-dire, $x^2 = x$.

Algèbre de Bool dans $\{0;1\}^n$

Définition 1.6. Soit A un anneau. Un sous-ensemble $B \subset A$ est un *sous-anneau* de A si les lois de composition $+$ et $\cdot$ de A définissent des lois de composition sur B qui en font un anneau.

Exemple 1.7. Puisque l'addition et la multiplication des nombres réels coïncident avec ces opérations définies sur les nombres entiers, nous en déduisons que $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$.

Comme dans le cas des sous-groupes, il existe un critère pratique et écologique du point de vue du gain d'énergie qui permet de reconnaître les sous-anneaux.

Proposition 1.8. *Soit A un anneau.*
Un sous-ensemble $B \subset A$ est un sous-anneau de A si et seulement si
$\forall x, y \in B$, *les éléments* $x+y$, $x \cdot y$, $-x$, 1 *appartiennent à B.*

Démonstration. $\Rightarrow$: vrai puisque B est un sous-anneau donc un anneau.

$\Leftarrow$:

Pour que $(B,+)$ soit un groupe, on doit avoir $x+y \in B$ et $-x \in B$ (thm 2.6, groupe)

De plus, l'addition est commutative car elle l'est dans A.

Pour que $(B,+,\cdot)$ soit un anneau, la multiplication doit être une loi interne à B, ce qui est assuré par le fait que $x \cdot y \in B$.

Elle est distributive par rapport à l'addition car elle l'est dans A.

On doit demander que $1 \in B$ puisque les éléments de A (ou B) ne sont pas forcément inversible. □

Nous avons vu la semaine dernière que les conditions sur l'addition forcent l'élément 0 à faire partie de B. Pourquoi faut-il alors demander explicitement la présence de 1 dans B ?
C'est le manque d'inverse qui nous force à le faire. Par exemple, le sous-groupe des nombres pairs ne forme pas un sous-anneau de $\mathbb{Z}$, même si le produit de deux nombres pairs est bel et bien pair.

Exemple 1.9. Considérons l'ensemble $M_2(\mathbb{R})$ des matrices carrées 2×2 à coefficients réels.
L'addition est définie "terme à terme" et nous rappelons que la multiplication est définie "ligne par colonne" :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} a\cdot x + b z & a y + b w \\ c x + d z & c y + d w \end{pmatrix}$$

Élément neutre : addition $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ = "matrice nulle"

multiplication $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ = "matrice identité"

Il n'est pas difficile de vérifier que $M_2(\mathbb{R})$ forme un anneau.

Le sous-ensemble B des matrices de la forme $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ forme un sous-anneau de $M_2(\mathbb{R})$.

En effet, on voit que la somme et l'opposé de matrices de cette forme sont encore dans B et que la matrice unité est aussi dans B. Il reste donc à vérifier que le produit de deux matrices de B est dans B, ce que nous faisons sans attendre :

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} x & y \\ -y & x \end{pmatrix} = \begin{pmatrix} ax - by & ay + bx \\ -bx - ay & -by + ax \end{pmatrix}$$

Tiens, tiens, on retrouve les formules définies pour la multiplication complexe...

$$(a+bi)(x+yi) = ax - by + (ay + bx)\, i$$

2 Les corps

Voici enfin la définition d'un corps, traduit de l'allemand "Körper", mot qui explique aussi l'utilisation de la lettre K pour désigner un tel objet.

Définition 2.1. Un *corps* K est un anneau commutatif dans lequel $0 \neq 1$ et tout élément non-nul est inversible.

tout élément $x \neq e_+ = 0$ admet un inverse pour $\cdot$: x^{-1}.

Exemple 2.2.

- Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, mais
- $\mathbb{Z}$ n'est pas un corps car les éléments autres que ± 1 n'admettent pas d'inverse dans $\mathbb{Z}$.
- L'anneau nul n'est pas un corps car $0 = 1$ dans cet anneau dégénéré.
-

Proposition 2.3. *Soit K un corps et $x, y \in K$. Si $xy = 0$, alors soit $x = 0$, soit $y = 0$.*

Démonstration.

Supposons que $y \neq 0$.

Alors l'inverse y^{-1} existe et on peut écrire

$$0 = 0 \cdot y^{-1} = (xy) \cdot y^{-1} = x(y \cdot y^{-1}) = x \cdot 1 = x$$

($=$: associativité ; $=$: déf de l'inverse)

□

Remarque 2.4. En pratique, on utilise surtout la contraposée de cette proposition :

Si $\exists\, x, y \in K$ t.q. $x, y \neq 0$ et $x \cdot y = 0$, alors K n'est pas un corps.

Exemple : $M_2(\mathbb{R})$ n'est pas un corps car par exemple

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

ou encore

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Voyons maintenant le plus petit corps du monde.

Exemple 2.5. Le corps à deux éléments. L'ensemble $\{0,1\}$ muni de l'addition pour laquelle $1+1=0$ est un groupe abélien. Nous définissons la multiplication en posant

$0\cdot 0 = 0$, $1\cdot 0 = 0\cdot 1 = 0$ et $1\cdot 1 = 1$ (pas le choix !)

La multiplication a donc 1 pour élément neutre et est associative :

On doit vérifier que $(a\cdot b)\cdot c = a\cdot(b\cdot c)$

Si $c=0$, il vient $0=0$ ✓ et si $c=1$, il vient $a\cdot b = a\cdot b$ ✓

Pour la distributivité, on doit vérifier que $(a+b)c = ac+bc$

Si $c=0$, on a $0=0$ ✓ et si $c=1$, on a $a+b=a+b$ ✓

Tout élément non nul est inversible : 1 est son propre inverse et $0\neq 1$.

$\Rightarrow \{0;1\}$ est un corps.

On utilise souvent la notation $\mathbb{F}_2$ pour le corps à deux éléments.

3 Le corps à p éléments

Nous aimerions maintenant généraliser l'exemple du corps à deux éléments et construire des corps à trois, cinq, sept, ou onze éléments ! Il nous faut à tout prix trouver une méthode qui nous évitera de devoir démontrer à la main l'associativité et la distributivité...

Définition 3.1. Soit n un nombre entier naturel. $n>1$
Les entiers a et b sont *congruents* modulo n si leur différence $a-b$ est un multiple de n.
On note alors $a \equiv b (\mathrm{mod} n)$, ou $a \equiv b(n)$ ou même $a \equiv b$ si le contexte est clair.
La classe de congruence d'un nombre entier a est notée $[a]$.
L'ensemble des classes d'équivalence (de congruence modulo n) est noté $\mathbb{Z}/n\mathbb{Z}$.

Ainsi 7 et 11 sont congruents modulo 4. La classe de congruence de 7 modulo 4 (ou de manière équivalente celle de 11) est formée de tous les nombres entiers de la forme

$4k+3$, $k\in\mathbb{Z}$ (ici $n=4$)

Le fait que la classe d'équivalence est bien définie découle de la proposition suivante.

Proposition 3.2. *La relation de congruence est une relation d'équivalence.*

Démonstration.
Réflexivité : $a \equiv a \pmod n$ car $a - a = 0$ qui est multiple de n.
$\Rightarrow a \in [a]$

Symétrie : Supposons que $a \in [b] \iff$
$a \equiv b \pmod n \iff$
$a - b$ est un multiple de $n \iff b - a$ aussi $\iff$
$b \equiv a \pmod n \iff b \in [a]$.

Transitivité :
Supposons que $a \in [b]$ et $b \in [c]$
$\iff a \equiv b \pmod n$ et $b \equiv c \pmod n$
$\iff a - b$ est multiple de n et $b - c$ aussi.
$\Rightarrow a - c = (a - b) + (b - c)$ est multiple de n (somme de deux multiple de n)
$\Rightarrow a \equiv c \pmod n \iff a \in [c]$. □

Nous pouvons maintenant définir une addition et une multiplication sur les classes de congruence grâce aux opérations homonymes sur les entiers. Il y a n classes de congruence dans $\mathbb{Z}$ modulo n : $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ puisque tout entier k est congru à son reste de la division par n.

Définition 3.3. Soient $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$. Alors la *somme* est définie par $[a] + [b] = [a + b]$ et le *produit* est défini par $[a] \cdot [b] = [ab]$.

Nous devons vérifier que ces définitions ne dépendent pas du choix du représentant de la classe de congruence. Pour la somme par exemple, si $a \equiv a' \pmod n$ et $b \equiv b' \pmod n$,
alors $(a+b) - (a'+b') = (a-a') + (b-b')$ est un multiple de n
$\Rightarrow a + b = (a' + b') \pmod n$.
Les autres vérifications sont du même genre.

Théorème 3.4.
L'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo n forme un anneau commutatif.

Démonstration. Tous les axiomes sont vérifiés parce qu'ils le sont dans $\mathbb{Z}$.
Prenons par exemple l'associativité de la multiplication. Soient $[a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$. Alors

$$[a] \cdot ([b] \cdot [c]) = [a] \cdot [b \cdot c] = [a \cdot (b \cdot c)] = [(a \cdot b) \cdot c]$$
(dif de. ; dif de. ; $a, b, c \in \mathbb{Z}$)
$$= [a \cdot b] \cdot [c] = ([a] \cdot [b]) \cdot [c]$$

Les autres vérifications sont du même genre. □

Exemple 3.5. Il existe un anneau ayant 6 éléments $[0], [1], [2], [3], [4], [5]$. Dans cet anneau on calcule par exemple $[2] + [5] = [1]$ ou encore $[2]\,[3] = [0]$. En particulier, cet anneau n'est pas un corps car $[2]$ "divise" $[0]$, ou encore $[2][3] = [0]$ alors que ni $[2]$, ni $[3]$ n'est l'élément 0.

Théorème 3.6. *L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.*

Démonstration.

$\Rightarrow$ par contraposée : Si p n'est pas premier, on peut l'écrire comme produit rs avec $r, s > 1$. Alors, $[r]$ est un "diviseur" de $[0]$ puisque $[r][s] = [0] = 0$
$\overset{\text{prop 2.3.}}{\Rightarrow}$ $\mathbb{Z}/p\mathbb{Z}$ ne peut pas être un corps.

$\Leftarrow$ directement : Supposons que p est un nombre premier. Nous devons montrer que tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. Soit $1 \leq a \leq p-1$ et $[a]$ sa classe de congruence modulo p. Considérons l'ensemble $\{a, 2a, \ldots, (p-1)a\}$. Nous affirmons que ces éléments appartiennent à $p-1$ classes de congruence modulo p distinctes. En effet, pour k, ℓ tels que $1 \leq k < \ell \leq p-1$. La différence $\ell a - ka = (\ell - k)a$ n'est pas divisible par p car $\ell - k$ et a sont deux nombres naturels non nuls et inférieurs à p. Ainsi $[\ell a] \neq [ka]$.
$\Rightarrow$ on a exactement $(p-1)$ classes de congruences non nulles et distinctes dans $\{a; 2a; \ldots; (p-1)a\}$.
L'une est la classe $[1]$, disons $[ka] = [k][a] = 1$.
Ainsi, $[k]$ est l'inverse de $[a]$. □

Exemple 3.7. L'anneau $\mathbb{Z}/6\mathbb{Z}$, rencontré il y a un instant et qui n'est pas un corps, a la table de multiplication suivante où on note k au lieu de $[k]$ pour alléger la notation :

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

0 $\Rightarrow$ $\mathbb{Z}/6\mathbb{Z}$ n'est pas un corps !