Arithmétique modulo *n*

L'arithmétique modulo *n* permet de définir des groupes, des anneaux et des corps qui comptent un nombre fini d'éléments.

Voyons d'abord un exemple, celui de l'arithmétique modulo 5. Lorsqu'on divise un entier quelconque par 5, le reste peut être : 0, 1, 2, 3. 4. L'ensemble de ces restes est l'ensemble {0; 1; 2; 3; 4}, noté $\mathbb{Z}_5$. On peut définir des opérations sur cet ensemble en s'inspirant d'une horloge comme dans la remarque ci-contre.

Ensemble des entiers modulo *n*

Soit *n* un nombre entier positif. L'ensemble {0; 1; 2; 3; ...; (*n*–1)}, noté $\mathbb{Z}_n$, est appelé **ensemble des entiers modulo *n***.

L'ensemble des entiers modulo *n* non nuls est noté $\mathbb{Z}_n^*$.

Addition des entiers modulo *n*

L'addition de deux nombres de $\mathbb{Z}_n$ donne le reste de la division par *n* de la somme de ces deux nombres dans $\mathbb{Z}$.

En plus de l'addition, on peut définir une multiplication dans $\mathbb{Z}_5$. Considérons par exemple, les nombres 2 et 4. En multipliant ces nombres dans $\mathbb{Z}$, on obtient 8. En divisant ce résultat par 5, on obtient 1 comme quotient et 3 comme reste. Par conséquent, dans $\mathbb{Z}_5$, on a $2 \times 4 = 3$. En procédant ainsi, on peut déterminer la table de multiplication dans $\mathbb{Z}_5$.

Multiplication des entiers modulo *n*

La multiplication de deux nombres de $\mathbb{Z}_n^*$ donne le reste de la division par *n* du produit usuel de ces deux nombres dans $\mathbb{Z}$.

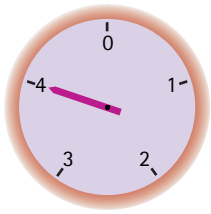
Lorsque *n* n'est pas un nombre premier, certains éléments de $\mathbb{Z}_n^*$ ne sont pas inversibles pour la multiplication. Considérons, par exemple $\mathbb{Z}_6^*$ dont la table de multiplication est donnée ci-contre. On constate que certains éléments de $\mathbb{Z}_6^*$ ne sont pas inversibles. Par exemple, 4 n'est pas inversible puisqu'il n'existe pas d'élément qui, multiplié par 4, donne l'élément neutre de la multiplication.

De plus, il existe des éléments non nuls dont le produit est 0. On dit que ces nombres sont des **diviseurs** de 0. Ainsi, 2 est un diviseur de 0 puisqu'il existe un élément non nul, soit 3, tel que $2 \times 3 = 0$.

On peut facilement montrer que si *p* est un nombre premier, l'ensemble des entiers modulo *p* muni de l'addition et de la multiplication, $\langle \mathbb{Z}_p, +, \times \rangle$, a une structure de corps commutatif.

REMARQUE

On peut définir une addition dans l'ensemble $\mathbb{Z}_5$ en s'inspirant du fonctionnement d'une horloge.



+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Le tableau sous l'horloge est appelé « table de l'addition dans $\mathbb{Z}_5$ ».

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

REMARQUE

Normalement, on tient compte seulement des éléments non nuls dans la table de multiplication, ce qui donne :

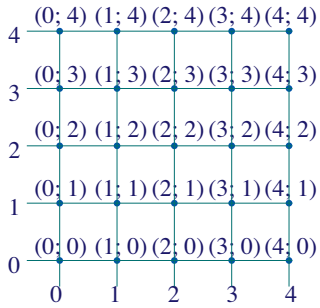
×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

×	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

REMARQUE

Si *n* n'est pas un nombre premier, l'ensemble $\mathbb{Z}_n$ muni de l'addition et de la multiplication, noté $\langle \mathbb{Z}_n, +, \times \rangle$, est un anneau commutatif unitaire car les éléments n'ont pas tous un inverse multiplicatif. Ainsi, dans la table de multiplication de $\mathbb{Z}_6$, l'élément neutre, 1, n'apparaît pas sur toutes les lignes et dans toutes les colonnes. Il y a donc des éléments qui n'ont pas d'inverse multiplicatif.

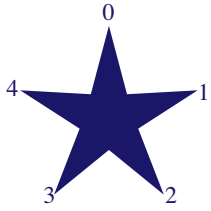
Considérons les couples formés des éléments de $\mathbb{Z}_5$ représentés ci-contre. Cet ensemble, notons-le $\mathbb{Z}_5^2$, a une structure de groupe abélien. De plus, on peut définir sur $\mathbb{Z}_5^2$ une multiplication par un scalaire en prenant les éléments de $\mathbb{Z}_5$ comme scalaires. On peut montrer que $\mathbb{Z}_5^2$ est un espace vectoriel sur le corps $\mathbb{Z}_5$.



On a donc un corps comportant un nombre fini d'éléments. De plus, on peut engendrer tous les éléments de $\mathbb{Z}_5^2$ par combinaison linéaire des vecteurs (0; 1) et (1; 0). Par conséquent, le sous-ensemble {(0; 1), (1; 0)} est une base de $\mathbb{Z}_5^2$. Puisque cette base ne contient que deux vecteurs, la dimension de $\mathbb{Z}_5^2$ est 2.

Et à quoi ça sert?

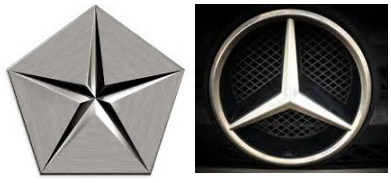
Considérons le pentagone étoilé ci-contre. En faisant effectuer une rotation de 72° à ce pentagone, il se retrouve dans la même position, mais la numérotation des sommets a changé. En fait, il y a cinq rotations possibles qui laissent l'image inchangée sauf pour la numérotation des sommets. La rotation de 0° laisse la numérotation inchangée. L'effet de la rotation de 72° peut être décrite en additionnant 1 en chacun des sommets. La rotation de 144° est équivalente à l'addition de 2 en chacun des sommets. Ainsi de suite, c'est donc dire que l'effet de ces rotations est décrit par la table d'addition de $\mathbb{Z}_5$.



+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

REMARQUE

Les symétries sont souvent utilisées dans les sigles car elles permettent de facilement identifier le produit.



En physique, la symétrie de rotation, ou invariance par rotation, est la propriété d'une théorie, ou d'un système physique de ne pas être modifié soit par une rotation spatiale quelconque, ou alors par seulement certaines d'entre elles. Lorsque le système est invariant pour n'importe quelle rotation d'espace, on parle d'isotropie. Dans ce cas, toutes les directions de l'espace sont équivalentes. L'isotropie de l'espace est à l'origine de la conservation du moment cinétique, en application du théorème de Noether.

REMARQUE

Le théorème de Noether (Emmy, 1882-1935), qualifié par Albert Einstein de « monument de la pensée mathématique », exprime l'équivalence qui existe entre les lois de conservation et l'invariance des lois physiques en ce qui concerne certaines transformations (typiquement appelées symétries)

Dans d'autres cas, l'invariance par rotation n'est valable que pour un sous-ensemble des rotations d'espace : par exemple seulement autour d'un certain axe (symétrie axiale) et/ou d'un certain angle (demi-tour, quart de tour...). Certaines directions de l'espace sont alors privilégiées, et l'espace n'est plus isotrope: cette situation se rencontre par exemple dans les cristaux ou encore en présence d'un champ extérieur appliqué.

En mathématiques l'invariance par rotation s'applique à un objet géométrique mais également à d'autres objets comme un opérateur (par exemple le laplacien de l'espace $\mathbb{R}^3$ est invariant par rotation).