



Groupe 3



LES ANNEAUX, CORPS \mathbb{Z} , $\mathbb{Z}/n\mathbb{Z}$

Présenté par: **Groupe 3**

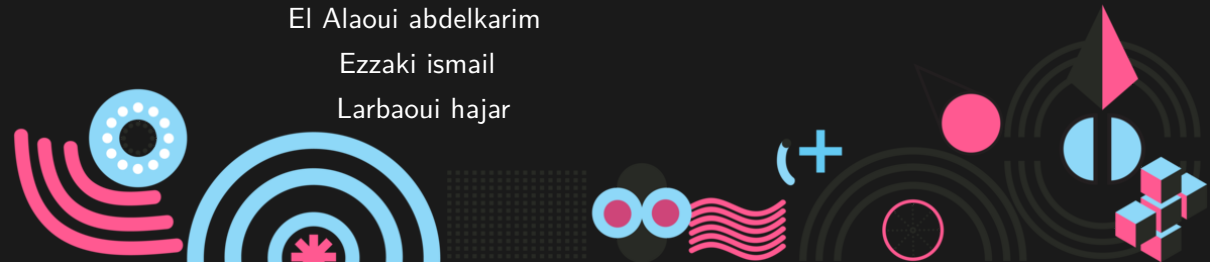
Encadré par : **Pr. Driss AMRANI**

Ahmidany fatiha

El Alaoui abdelkarim

Ezzaki ismail

Larbaoui hajar



Plan

1. Anneaux
2. Idéaux et Corps
3. Construction de l'ensemble \mathbb{Z} des entiers relatifs
4. L'anneau $\mathbb{Z}/n\mathbb{Z}$

anneaux

DEFINITION

Un anneau est un ensemble muni de deux LCI $(A, +, \cdot)$ tels que :

- ❖ $(A, +)$ est un groupe commutatif de neutre noté 0_A .
- ❖ La loi \cdot est une LCI sur A associative et distributive à gauche et à droite par rapport à $+$:

$$\forall x, y, z \in A, \quad x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{et} \quad (x + y) \cdot z = x \cdot z + y \cdot z$$

Si la loi \cdot est commutative, l'anneau est dit commutatif ou abélien.

EXERCICE

Si $x \in A$, montrer que $0_A \cdot x = 0_A$ (considérer $0_A \cdot x + 0_A \cdot x$).

EXEMPLES

- ❖ - $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$ sont des anneaux bien connus.
- ❖ - L'ensemble des suites réelles, muni de l'addition et du produit des suites, est un anneau. Même chose pour l'ensemble des fonctions de I dans \mathbb{R} . On déterminera précisément les neutres de ces anneaux.

Sous-anneaux

DEFINITION

Soit $(A, +, \cdot)$ un anneau. Une partie non vide A_1 de A est un sous-anneau de A lorsque :

- ❖ - $1_A \in A_1$;
- ❖ - les lois $+$ et \cdot induisent des LCI sur A_1 , et, muni de ces lois, $(A_1, +, \cdot)$ est un anneau.

PROPOSITION

Une partie A_1 non vide de A est un sous-anneau si et seulement si

- ❖ - $(A_1, +)$ est un sous-groupe de $(A, +)$;
- ❖ - $1_A \in A_1$
- ❖ - induit une LCI sur A_1 .

EXEMPLES

- ❖ - Bien entendu, \mathbb{Z} est un sous-anneau de \mathbb{Q} qui est un sous-anneau de...
- ❖ - L'ensemble des fonctions dérivables sur I constitue un sous-anneau des fonctions continues sur I , qui constitue lui-même un sous-anneau de l'ensemble des fonctions de I dans \mathbb{R} .
- ❖ - L'ensemble des suites réelles stationnaires est un sous-anneau de $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$, qui est un sous-anneau de $(\mathbb{C}^{\mathbb{N}}, +, \cdot)$

Morphismes d'anneaux

DEFINITION

Soient $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux (on note de la même façon les lois de A et $B \dots$). Un morphisme d'anneaux de A vers B est une application de A vers B telle que :

- ❖ - $f(1_A) = 1_B$
- ❖ - pour tout $x, y \in A$, $f(x + y) = f(x) + f(y)$ et $f(x \cdot y) = f(x) \cdot f(y)$.

EXEMPLES

- ❖ - $z \mapsto \bar{z}$ réalise un automorphisme d'anneaux de \mathbb{C} .
- ❖ - $f \mapsto f(\pi)$ réalise un morphisme d'anneaux de $\mathbb{R}^{\mathbb{R}}$ sur $\mathbb{R}\mathbb{R}$.

Divisibilité

DEFINITION

Soit $(A, +, \cdot)$ un anneau commutatif.

- ❖ - On dit que $x \in A$ est inversible s'il admet un symétrique pour la loi \cdot .
- ❖ - On dit que $a \neq 0$ divise b s'il existe $c \in A$ tel que $b = ca$. On note $a \mid b$.
- ❖ - On dit que $a \neq 0$ est un diviseur de 0 s'il existe $b \neq 0$ tel que $ab = 0$.
- ❖ - Un anneau est dit intègre s'il ne contient pas de diviseur de 0 autre que 0 lui-même.

PROPOSITION

Dans un anneau commutatif $(A, +, \cdot)$:

- ❖ - 0_A n'est jamais inversible.
- ❖ - Si $x_1, x_2, y \in A$ intègre, avec $y \neq 0$ et $x_1 y = x_2 y$, alors $x_1 = x_2$. On dit qu'"on peut simplifier" (ce qui ne veut pas dire diviser) par $y \neq 0$.

EXEMPLES

-

- ❖ \mathbb{Z} est intègre, et ses éléments inversibles sont 1 et -1 .
- ❖ - \mathbb{Q} , \mathbb{R} et \mathbb{C} sont des anneaux intègres dont tous les éléments non nuls sont inversibles.
- ❖ - L'ensemble des fonctions de \mathbb{R} dans \mathbb{R} n'est pas intègre : toute application f qui s'annule est diviseur de 0 (le montrer). Les éléments inversibles sont les fonctions qui ne s'annulent pas.

EXERCICE

Montrer que $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ est un sous-anneau intègre de \mathbb{C} , dont les inversibles sont 1, i , -1 et $-i$.

Idéaux

Définition

on appelle idéal à gauche de l'anneau A , un sous-groupe de $(A, +)$ tel que:

$$\forall a \in A \forall x \in I \quad ax \in I$$

on appelle idéal à droite de A un sous groupe de $(A, +)$ tel que:

$$\forall a \in A \forall x \in I \quad xa \in I$$

On appelle idéal bilatère de A un sous- groupe de $(A, +)$ qui vérifie les deux conditions précédentes.

Évidemment, si l'anneau A est commutatif, les trois notions sont identiques. On dit alors tout simplement, "un idéal" de A . Dans un anneau A , il existe au moins deux idéaux bilatères, à savoir $\{0\}$ et A .

Supposons A unifère. Pour que $I \neq \emptyset$ soit un idéal à gauche, il suffit que

$$\forall x \in I \quad \forall y \in I \quad x + y \in I \quad \text{et} \quad \forall a \in A \quad \forall x \in I \quad ax \in I.$$

car alors $0 = 0x \in I$ et $-x = (-1)x \in I$ pour tout $x \in I$. Ainsi I est un sous-groupe de $(A, +)$.

Supposons A unitaire. Si un idéal à gauche (resp. à droite) I de A contient l'unité 1 de A , alors $I = A$ car alors $a = a1 \in I$ pour tout $a \in A$. Plus généralement, si I contient un élément inversible u de A , alors $1 = u^{-1}u \in I$ et donc $I = A$.

Un idéal de A est un sous-anneau de A car (1) ou (2), montre que $xy \in I$ pour tout $x \in I$ et tout $y \in I$. La réciproque est fausse : par exemple \mathbb{Z} est un sous-anneau de \mathbb{R} mais n'est pas un idéal de \mathbb{R} .

Prposition

Soit $f : A \longrightarrow B$ un morphisme d'anneaux.

(i) Soit J un idéal à gauche (resp. à droite, bilatère) de B . Alors $f^{-1}(J)$ est un idéal à gauche (resp. à droite, bilatère) de A . En particulier, le noyau $\text{Ker}(f) = f^{-1}(\{0\})$ de f est un idéal bilatère de A .

(ii) Supposons f surjectif. L'image $f(I)$ de tout idéal à gauche (resp. à droite, bilatère) I de A , est un idéal à gauche (resp. à droite, bilatère) de B .

(iii) Supposons f surjectif. L'application $\alpha : J \mapsto f^{-1}(J)$ est une bijection, de l'ensemble \mathcal{J} des idéaux bilatères de B sur l'ensemble \mathcal{F} des idéaux bilatères de A contenant $\text{Ker}(f)$ et α respecte l'inclusion.

Proof.

(i) $f^{-1}(J)$ est un sous-groupe additif de A . Pour $x \in f^{-1}(J)$ et $a \in A$ on a $f(x) \in J$, d'où $f(ax) = f(a)f(x) \in J$ et donc $ax \in f^{-1}(J)$.

(ii) Nous laissons la vérification au lecteur.

(iii) D'après (i), si J est un idéal bilatère de B , alors $f^{-1}(J)$ est un idéal bilatère de A . Il contient $\text{Ker}(f) = f^{-1}(\{0\})$. Ainsi α est une application de \mathcal{J} dans \mathcal{F} . Si $J, J' \in \mathcal{J}$ sont tels que $J \subset J'$ on a $f^{-1}(J) \subset f^{-1}(J')$ donc α respecte l'ordre. Pour tout $J \in \mathcal{J}$ on a $f[f^{-1}(J)] = J$ car f est surjective donc α est injective. Elle est surjective car pour tout $I \in \mathcal{F}$, on a $\text{Ker}(f) \subset I$ et donc $f^{-1}(f(I)) = I + \text{Ker}(f) = I$. □

Intersection et somme d'idéaux

Proposition

|| Soit $(I_k)_{k \in K}$ une famille d'idéaux à gauche de l'anneau A . (i) $\bigcap_{k \in K} I_k$ est un idéal à gauche de A . (ii) L'ensemble $\sum_{k \in K} I_k$ des éléments $x \in A$ qui sont somme finie $x_{i_1} + \cdots + x_{i_k}$ d'éléments de $\bigcup_{k \in K} I_k$, est un idéal à gauche de A . C'est le plus petit idéal à gauche de A contenant I_k pour tout $k \in K$. En particulier, la somme $I + J = \{x + y; x \in I, y \in J\}$ de deux idéaux à gauche I et J de A , est un idéal à gauche de A .

Quotient d'un anneau par un idéal bilatère

Lemme

Soient A un anneau, I un sous-groupe du groupe additif $(A, +)$. La relation d'équivalence de congruence modulo le sous-groupe I ,

$$x \equiv y \Leftrightarrow y - x \in I,$$

est compatible avec le produit de A , si et seulement si I est un idéal bilatère de A .

Proof.

L'équivalence est compatible avec les multiplications à gauche, si pour $x, y \in A$, la condition $x \equiv y$ implique que $ax \equiv ay$ pour tout $a \in A$, soit si pour tout $z \in I$ et tout $a \in A$, on a $az \in I$, c'est-à-dire si I est idéal à gauche. De même, l'équivalence est compatible avec le produit du côté droit si et seulement si I est un idéal à droite de A , d'où le lemme. □

Proposition

Soient A un anneau et I un idéal bilatère de A . Le quotient A/I , muni des opérations

$$\bar{x} + \bar{y} = \overline{x + y} \quad , \quad \bar{x}\bar{y} = \overline{xy}$$

est un anneau. Si A a une unité, alors $\bar{1}$ est une unité pour A/I . L'application canonique $\varphi : x \mapsto \bar{x}$ est un homomorphisme d'anneaux surjectif de A sur A/I , de noyau I et le couple $(A/I, \varphi)$ a la propriété universelle suivante (factorisation des homomorphismes): (P) Si un homomorphisme fde A dans un anneau B est nul sur I , alors il existe un homomorphisme unique $\bar{f} : A/I \rightarrow B$ tel que $\bar{f} \circ \varphi = f$. De plus, on a $\text{Im}(\bar{f}) = \text{Im}(f)$ et $\text{Ker}(\bar{f}) = \text{Ker}(f)/I$.

Proof.

A/I est un groupe additif. D'après le lemme, le produit est bien défini sur A/I et les axiomes des anneaux sont vérifiés (voir 1-2). Soit $f \in \text{Hom}(A, B)$ nul sur I . on définit un homomorphisme de groupes additifs en posant $\bar{f}(\bar{x}) = \overline{f(x)}$ pour tout $\bar{x} \in A/I$. On a

$$\bar{f}(\overline{xy}) = \overline{f(xy)} = \overline{f(x)f(y)} = \bar{f}(\bar{x})\bar{f}(\bar{y}),$$

donc \bar{f} est un homomorphisme d'anneaux, d'où la propriété universelle (P). □

Idéaux maximaux

Définition

On appelle idéal à gauche maximal de l'anneau A , un idéal à gauche I de A , distinct de A , tel que les seuls idéaux à gauche de A contenant I soient I et A . On définit de même les notions d'idéal à droite maximal et d'idéal bilatère maximal.

Proposition

Soit A un anneau avec unité. Tout idéal à gauche de A , distinct de A , est inclus dans un idéal à gauche maximal. Tout idéal à droite de A , distinct de A , est inclus dans un idéal à droite maximal. Tout idéal bilatère de A , distinct de A , est inclus dans un idéal bilatère maximal.

Corps

Définition

Un corps est un anneau K , possédant une unité 1 (distincte du zéro) tel que tout élément non nul x possède un inverse x^{-1} . Si le produit est commutatif, on dit que K est un corps commutatif. On appelle sous-corps de K un sous-anneau K_0 de K contenant l'unité de K et tel que pour tout $x \in K_0$ non nul on ait $x^{-1} \in K_0$.

Un corps K est donc un anneau unitaire dont le groupe des unités est $K_* = K \setminus \{0\}$.
Un corps est intègre : si $xy = 0$ et si $x \neq 0$ alors x est inversible et $y = x^{-1}(xy) = 0$.
L'intersection d'une famille $(K_i)_{i \in I}$ de sous-corps d'un corps K est non seulement un sous-anneau de K contenant l'unité mais c'est un sous-corps de K . En effet, pour tout $x \in \bigcap_{i \in I} K_i$, avec $x \neq 0$, on a $x^{-1} \in K_i$ pour tout $i \in I$ et donc $x^{-1} \in \bigcap_{i \in I} K_i$. Soit X une partie non vide de K . L'intersection des sous-corps de K contenant X , est le plus petit sous-corps de K contenant X , appelé le sous-corps engendré par X . Les corps Q, R, C jouent un rôle essentiel en mathématique.

Proposition

Soit K un anneau avec unité. Pour que K soit un corps, il faut et il suffit que $\{0\}$ et K soient les seuls idéaux à gauche de K . Il en est de même pour les idéaux à droite.

Proof.


Soit I un idéal à gauche du corps K . Si $I \neq \{0\}$, il existe $x \in I$ non nul. On a $1 = x^{-1}x \in I$ et donc $I = K$. Réciproquement, soit K un anneau unitaire ayant pour seuls idéaux à gauche $\{0\}$ et K . Pour tout $x \neq 0$ l'idéal à gauche Kx de K contient x . Il est donc égal à K . En particulier, il existe $y \in K$ tel que $yx = 1$. Comme $y \neq 0$, il existe de même $z \in K$ tel que $zy = 1$. Alors y qui a un inverse à droite x et un inverse à gauche z , est inversible d'inverse $y^{-1} = x$. Tout élément non nul x de K est donc inversible et K est un corps. On montre de même l'assertion concernant les idéaux à droite. □

Quotient par un idéal maximal

Proposition

Soit A un anneau commutatif unitaire. Pour qu'un idéal I de A soit maximal, il faut et il suffit que A/I soit un corps.

Proof.

l'anneau commutatif unitaire A/I est un corps si et seulement si $\{0\}$ et A/I sont ses seuls idéaux. D'après , prop. (iii), cela signifie que I et A sont les seuls idéaux de A contenant 1, c'est-à-dire que I est maximal. 

Corollaire

|| L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si $p \in \mathbb{N}$ est premier.

Construction de l'ensemble \mathbb{Z} des entiers relatifs

Pourquoi on appelle les entiers relatifs \mathbb{Z}

- ❖ $\mathbb{N} \Rightarrow$ Nombre
- ❖ $\mathbb{R} \Rightarrow$ Reel
- ❖ $\mathbb{C} \Rightarrow$ Complexe
- ❖ $\mathbb{Z} \Rightarrow$

Pourquoi on appelle les entiers relatifs \mathbb{Z}

- ❖ $\mathbb{N} \Rightarrow$ Nombre
- ❖ $\mathbb{R} \Rightarrow$ Reel
- ❖ $\mathbb{C} \Rightarrow$ Complexe
- ❖ $\mathbb{Z} \Rightarrow$ Nombre en allemand **Zahlen**

Normalement, en utilisant les nombres naturels, on peut facilement définir les entiers relatifs comme suit : Les **entiers relatifs**, notés \mathbb{Z} , sont tous les nombres entiers positifs et négatifs : soit

$$\mathbb{Z} = \{\dots - 2, -1, 0, 1, 2, 3, \dots\}.$$

Cependant, on peut facilement voir que la définition ci-dessus est suspecte,

- ❖ Que signifie -3 ?
- ❖ Comment -3 interagit-il avec l'addition et la multiplication ?
- ❖ nous n'avons pas de règles qui équivalent à "vous pouvez faire une deuxième copie de votre premier ensemble mais avec des symboles spéciaux devant tous ces éléments"

classes d'équivalence I

Prenons un ensemble quelconque S avec une relation d'équivalence R . Pour tout élément $x \in S$, nous pouvons définir la **classe d'équivalence** correspondant à x comme l'ensemble

$$\{y \in S \mid yRx\}$$

Par exemple, dans l'arithmétique modulo 3 il existe trois classes d'équivalence possibles :

$$\{\dots - 6, -3, 0, 3, 6 \dots\}$$

$$\{\dots - 5, -2, 1, 4, 7 \dots\}$$

$$\{\dots - 4, -1, 2, 5, 8 \dots\}$$

Chaque élément correspond à l'une de ces trois classes.

Définir \mathbb{Z}

En utilisant ce concept, nous définissons les entiers relatifs comme suit :

Définir \mathbb{Z}

En utilisant ce concept, nous définissons les entiers relatifs comme suit :

définition

Construire $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$, le produit cartésien des nombres naturels par eux-mêmes.

Créer une relation d'équivalence \sim sur $\mathbb{N}\mathbb{N}$ de la manière suivante :

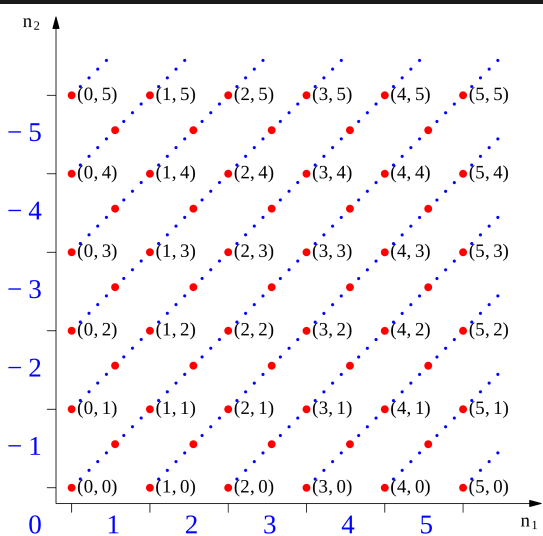
- ❖ écrivez $(a, b) \sim (c, d)$ si et seulement si $a - b = c - d$. ($(a, b) \sim (c, d)$ si et seulement si $a + d = b + c$; ceci est équivalent).
- ❖ Prenez la collection de toutes les classes d'équivalence de \mathbb{N}^2 sous cette relation. Nous appelons cet ensemble le **entiers relatifs**, et l'écrivons \mathbb{Z} .

Définir \mathbb{Z}

- (a, b) correspond à l'entier $a - b$, où notre relation d'équivalence est une façon de dire que (a, b) et $(a + k, b + k)$ représentent tous deux le même "entier relatif".

Définir \mathbb{Z}

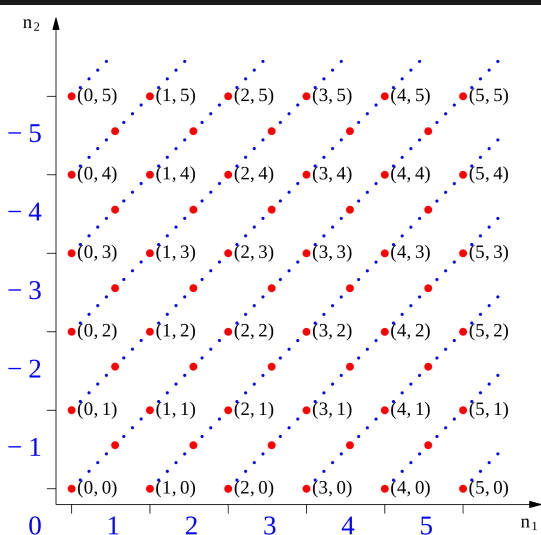
- (a, b) correspond à l'entier $a - b$, où notre relation d'équivalence est une façon de dire que (a, b) et $(a + k, b + k)$ représentent tous deux le même "entier relatif".



Définir \mathbb{Z}

- (a, b) correspond à l'entier $a - b$, où notre relation d'équivalence est une façon de dire que (a, b) et $(a + k, b + k)$ représentent tous deux le même "entier relatif".

- Cela peut sembler bizarre, mais cela a l'avantage d'être un ensemble que nous pouvons étudier (c'est une collection de sous-ensembles de \mathbb{N}^2).



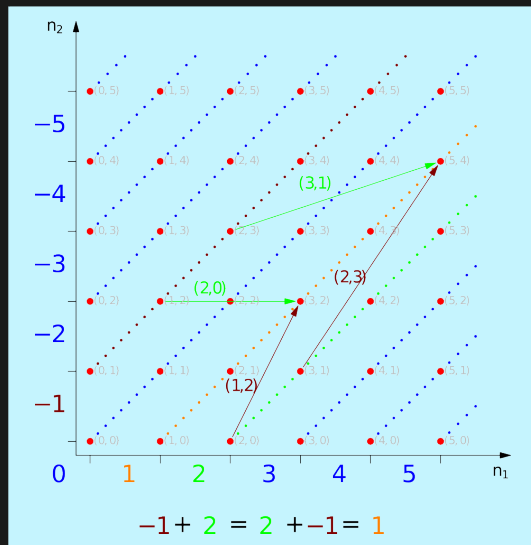
Définition de la structure de groupe

L'addition

- ❖ On définit la somme de deux couples d'entiers ainsi :
 $(n_1, n_2) + (n'_1, n'_2) = (n_1 + n'_1, n_2 + n'_2)$; cette opération est commutative, associative et d'élément neutre $(0, 0)$ sur les couples d'entiers, dont le neutre est la classe de $(0, 0)$, constituée des couples (n, n) .
- ❖ si (n_1, n_2) représente un entier relatif dans les couples d'entiers,
 $(n_1, n_2) + (n_2, n_1) = (n_1 + n_2, n_1 + n_2)$ donc équivalent à $(0, 0)$. \Rightarrow La classe d'équivalence de (n_2, n_1) est donc opposée à la classe d'équivalence de (n_1, n_2) .
- ❖ Il existe une classe d'équivalence Z contenant cette paire, car les classes d'équivalence partitionnent \mathbb{N}^2 !
- ❖ Remarquez que le représentant choisi n'a pas d'importance, car choisir n'importe quel autre représentant $(n_1 + c, n_2 + c), (n'_1 + d, n'_2 + d)$ donnerait $(n_1 + n_2 + c + d, n'_1 + n'_2 + c + d)$, ce qui est équivalent à $(n_1 + n'_1, n_2 + n'_2)$, il s'agit d'une opération bien définie !

Définition de la structure de groupe

L'addition



Définition de la structure de groupe

la multiplication

On peut alors définir la multiplication comme suit :

$(n_1, n_2) \times (m_1, m_2) = (n_1 m_1 + n_2 m_2, n_1 m_2 + m_1 n_2)$ Cette opération définie sur $\mathbb{N} \times \mathbb{N}$ est associative, commutative, possède un élément neutre $(1, 0)$ et est distributive pour l'addition précédemment définie. De plus, elle donne à \mathbb{Z} une structure d'anneau unitaire. Les égalités

$$\blacksquare (d, 0) \times (d', 0) = (dd', 0)$$

$$\blacksquare (d, 0) \times (0, d') = (0, dd')$$

$$\blacksquare (0, d) \times (0, d') = (dd', 0)$$

permettent les écritures

$$\blacksquare d \times d' = dd'$$

$$\blacksquare d \times (-d') = (-dd')$$

$$\blacksquare (-d) \times (-d') = dd'$$

qui permettent de démontrer que l'anneau est aussi intègre.

Définition de la structure de groupe

la relation d'ordre

Pour comparer deux classes d'équivalence quelconques X, Y :

- ❖ choisissez un représentant $(x_1, x_2) \in X, (y_1, y_2) \in Y$.
- ❖ On dit que $X < Y$ si et seulement si $x_1 - x_2 < y_1 - y_2$, ou de manière équivalente $x_1 + y_2 < y_1 + x_2$.
- ❖ Là encore, on peut vérifier que cette propriété ne dépend pas des représentants choisis dans les classes d'équivalence de X, Y , donc elle aussi est bien définie.

Écriture simplifiée des éléments de \mathbb{Z}

Notons $(n ; m)$ la classe d'un couple d'entiers naturels (n, m) . Elle est de l'un des trois types suivants :

- ❖ $(d ; 0)$ si $n > m$ avec $n = m + d$ et d non nul
- ❖ $(0 ; d)$ si $n < m$ avec $n + d = m$ et d non nul
- ❖ $(0 ; 0)$ si $n = m$

Or l'ensemble des classes $(d ; 0)$ est isomorphe à \mathbb{N} ; on note donc ces classes sous la forme simplifiée d . D'autre part, pour d non nul, les classes $(d ; 0)$ et $(0 ; d)$ sont opposées. En effet, $(d ; 0) + (0 ; d) = (d ; d) = (0 ; 0)$. On note donc les classes $(0 ; d)$ sous la forme simplifiée $(-d)$. L'ensemble \mathbb{Z} retrouve alors sa forme plus classique de $\mathbb{N} \cup \{(-d) \mid d \in \mathbb{N}^*\}$.

Propriétés de \mathbb{Z}

Les entiers satisfont toutes les propriétés énumérées précédemment pour \mathbb{N} , à l'exception du bon ordre :

- ❖ **stabilité(+)**: $\forall a, b \in \mathbb{Z}$, on a $a + b \in \mathbb{Z}$.
- ❖ **Identité(+)**: $\exists 0 \in \mathbb{Z}$ tel que $\forall a \in \mathbb{Z}$, $0 + a = a$.
- ❖ **Commutativité(+)**: $\forall a, b \in \mathbb{Z}$, $a + b = b + a$.
- ❖ **Associativité(+)**: $\forall a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.
- ❖ **stabilité(\cdot)**: $\forall a, b \in \mathbb{Z}$, on a $a \cdot b \in \mathbb{Z}$.
- ❖ **Identité(\cdot)**: $\exists 1 \in \mathbb{Z}$ tel que $\forall a \in \mathbb{Z}$, $1 \cdot a = a$.
- ❖ **Commutativité(\cdot)**: $\forall a, b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.
- ❖ **Associativité(\cdot)**: $\forall a, b, c \in \mathbb{Z}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- ❖ **Distributivité**: $(+, \cdot) : \forall a, b, c \in \mathbb{Z}$, $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

En outre, il satisfait aux deux propriétés supplémentaires suivantes :

- Inverses($+$) : $\forall a \in \mathbb{Z}$, \exists a unique $(-a) \in \mathbb{Z}$ tel que $a + (-a) = 0$.
- Ordre de multiplication($<, \cdot$) : $\forall a, b, c \in \mathbb{Z}$, si $a < b$, $0 < c$ alors $ac < bc$.

Proposition : L'anneau $(\mathbb{Z}, +, *)$

Le triplet $(\mathbb{Z}, +, *)$ est un anneau commutatif , intègre et unitaire

pour approfondir : la construction de $\mathbb{N}, \mathbb{R}, \mathbb{C}$

https :

//web.math.ucsb.edu/ padraic/ucsb_2014_15/ccs_proofs_f2014/ccs_proofs_f2014.html

L'anneau $\mathbb{Z}/n\mathbb{Z}$

Congruences dans \mathbb{Z}

Soit n un entier naturel.

Rappels Nous avons vu en première année la relation de congruence modulo n définie par :

$$x \equiv y \quad [n] \iff y - x \in n\mathbb{Z}.$$

Il s'agit d'une relation d'équivalence sur \mathbb{Z} qui est compatible avec les opérations de \mathbb{Z} , c'est-à-dire qui vérifie :

$$\forall (x, y, x', y') \in \mathbb{Z}^4 \left\{ \begin{array}{l} x \equiv x' \quad [n] \\ y \equiv y' \quad [n] \end{array} \right. \implies \left\{ \begin{array}{l} x + y \equiv x' + y' \quad [n] \\ x \times y \equiv x' \times y' \quad [n] \end{array} \right.$$

Notation On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation. La classe d'un élément k de \mathbb{Z} est notée \bar{k} .

Proposition

Pour $n \in \mathbb{N}^*$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ a n éléments, et l'on a :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

Remarque $\mathbb{Z}/n\mathbb{Z}$ est appelé ensemble quotient de \mathbb{Z} par $n\mathbb{Z}$, ce qui explique sa notation.

Proposition

1. Il existe sur $\mathbb{Z}/n\mathbb{Z}$ des lois, notées $+$ et \times (ou implicitement pour le produit) et appelées lois quotient, telles que : $\forall (x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \quad \bar{x} + \bar{y} = \overline{x+y}$ et $\bar{x} \times \bar{y} = \overline{xy}$.
2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif d'éléments neutres $\bar{0}$ et $\bar{1}$.
3. La projection canonique $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux surjectif de noyau $n\mathbb{Z}$.

Remarque

- On peut aussi prendre pour représentants des classes modulo $n \neq 0$, n'importe quel n -uplet d'entiers consécutifs.

Par exemple, pour étudier la multiplication sur $\mathbb{Z}/5\mathbb{Z}$, il pourra être intéressant d'écrire $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \pm\bar{1}, \pm\bar{2}\}$.

- Les éléments $0, 1, \dots, n-1$ sont privilégiés dans leurs classes respectives. Il arrivera donc que l'on note p à la place de \bar{p} lorsque $0 \leq p < n$, s'il n'y a pas de confusion possible.

Proposition

(Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$) 1. La classe de $k \in \mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, k est premier avec n .

2. Pour $n \in \mathbb{N}^*$, les assertions suivantes sont équivalentes : (i) $\mathbb{Z}/n\mathbb{Z}$ est un corps;

(ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre;

(iii) n est premier.

Théorème chinois

On note ici $[k]_n$ la classe de l'entier k modulo un entier naturel non nul n .

Proposition

Soit n et m des entiers premiers entre eux. Les anneaux $\mathbb{Z}/(nm)\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ sont isomorphes par le morphisme d'anneaux φ :

$$\begin{aligned}\mathbb{Z}/(nm)\mathbb{Z} &\longrightarrow (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \\ [k]_{nm} &\longrightarrow ([k]_n, [k]_m)\end{aligned}$$

Corollaire

(Théorème chinois) Si n et m sont des entiers premiers entre eux, pour tout $(a, b) \in \mathbb{Z}^2$, il existe un entier k vérifiant le système:

$$\begin{cases} k \equiv a & [n] \\ k \equiv b & [m] \end{cases}$$

et les solutions de ce système sont exactement les entiers congrus à k modulo nm .

Le théorème chinois permet de ramener l'étude d'une équation sur $\mathbb{Z}/n\mathbb{Z}$ lorsque n n'est pas premier, à celle d'équations sur des anneaux plus simples.

Point méthode (pour obtenir une solution de (S)) A partir d'une relation de Bézout $nu + nv = 1$, on trouve deux entiers $k_1 = mu$ et $k_2 = nv$ vérifiant respectivement les systèmes de congruences:

$$\begin{cases} k_1 \equiv 1 & [n] \\ k_1 \equiv 0 & [m] \end{cases}$$

et

$$\begin{cases} k_2 \equiv 1 & [n] \\ k_2 \equiv 0 & [m] \end{cases}$$

et une solution du système (S) est alors $k = k_1a + k_2b$ (vérification immédiate en prenant les congruences modulo n et m) **Remarque** L'obtention d'une telle solution est non triviale, mais sa vérification est immédiate. Il ne faut donc pas oublier de la faire pour repérer une erreur de calcul éventuelle.

The background of the slide consists of several concentric circles. The innermost circle is a dark blue. Surrounding it are three rings of a deep red color, followed by an outermost ring of a lighter orange-red color. The text is centered within the dark blue circle.

Merci pour votre Attention ?