HAX501X – Groupes et anneaux 1

CM2 08/09/2023

Clément Dupont

Rappel de l'épisode précédent

- Division euclidienne.
- Notion de congruence, notion d'inversibilité modulo un entier.
- Sous-groupes de $\mathbb{Z}$, classification.

Théorème
Soit H un sous-groupe de $\mathbb{Z}$. Il existe un unique $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.

Démonstration. Ingrédient : la division euclidienne. Revoyez ça ! □

- PGCD et PPCM : $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.
- Lemme de Gauss (et sa variante), lemme d'Euclide.
- Factorisation en produit de nombres premiers.

Théorème (Factorisation en produit de nombres premiers)
Tout entier $n \in \mathbb{N}^*$ peut s'écrire comme un produit de nombres premiers, de manière unique à l'ordre des facteurs près.

Démonstration. Ingrédient : le lemme d'Euclide. Revoyez ça ! □

Le théorème de Bézout

Théorème (Théorème de Bézout)

Soient $a, b \in \mathbb{Z}$, et soit $d \in \mathbb{N}$. On a équivalence entre les deux assertions suivantes :

(i) $d = a \wedge b$;

(ii) $d|a$, $d|b$, *et il existe* $u, v \in \mathbb{Z}$ *tels que* $au + bv = d$.

Théorème (Théorème de Bézout, cas particulier)

Soient $a, b \in \mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

- On trouve une relation de Bézout par divisions euclidiennes successives. C'est l'**algorithme d'Euclide étendu**.

Application à l'inversion modulo n

Proposition

Soit $a \in \mathbb{Z}$. Alors a est inversible modulo n si et seulement si $a \wedge n = 1$. Dans ce cas-là, si $au + nv = 1$ est une relation de Bézout pour a et n, on a que u est un inverse de a modulo n.

Le théorème chinois des restes

Théorème (Théorème chinois des restes)

Soient $m, n \in \mathbb{N}$ tels que $m \wedge n = 1$. Soient $a, b \in \mathbb{Z}$. Alors le système

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

a une solution $x_0 \in \mathbb{Z}$. De plus, l'ensemble des solutions est l'ensemble des entiers congrus à x_0 modulo mn.

Remarque

Si m et n ne sont pas premiers entre eux, il se peut que le système n'ait même pas de solution. Par exemple, le système suivant n'a aucune solution $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 1 \pmod{4} \end{cases}$$

En effet, si $x \equiv 2 \pmod{6}$ alors x est pair... et si $x \equiv 1 \pmod{4}$ alors x est impair !

Le petit théorème de Fermat

Théorème (Petit théorème de Fermat)

Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$ on a :

$$a^p \equiv a \pmod{p}.$$

Théorème (Petit théorème de Fermat, variante)

Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$, si a n'est pas un multiple de p alors :

$$a^{p-1} \equiv 1 \pmod{p}.$$

Comment montre-t-on le petit théorème de Fermat ?

Proposition

Soit p un nombre premier. Pour tout $k \in \{1, \ldots, p-1\}$, p divise le coefficient binomial $\binom{p}{k}$.

- Implique (grâce à la formule du binôme de Newton) la congruence, pour tous $x, y \in \mathbb{Z}$:
$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$
- Permet de montrer le petit théorème de Fermat par récurrence.

Exercices

- Les exercices du chapitre 1 du poly sont à préparer pour le premier TD (semaine prochaine).

2 – Étude de $\mathbb{Z}/n\mathbb{Z}$

Relation d'équivalence

- Une relation binaire sur un ensemble E est une partie $\mathcal{R} \subset E \times E$. On utilise la notation $x \mathcal{R} y$ à la place de $(x, y) \in \mathcal{R}$.

Définition

Soit E un ensemble. Une **relation d'équivalence** *sur E est une relation binaire $\sim$ sur E qui est réflexive, symétrique, et transitive, c'est-à-dire telles que les propriétés suivantes sont vérifiées.*

- *Réflexivité :* $\forall x \in E\,,\ x \sim x$;
- *Symétrie :* $\forall x, y \in E\,,\ x \sim y \implies y \sim x$;
- *Transitivité :* $\forall x, y, z \in E\,,\ (x \sim y \ \text{ et } \ y \sim z) \implies x \sim z.$

Exemple

Soit $n \in \mathbb{N}^*$. La relation $\sim$ sur l'ensemble $E = \mathbb{Z}$ définie par

$$a \sim b \quad \iff \quad a \equiv b \pmod{n}$$

est une relation d'équivalence.

Un exercice

Exercice 13

On définit une relation $\sim$ sur $\mathbb{R}^2$ par :

$$\vec{u} \sim \vec{v} \quad \Longleftrightarrow \quad \exists \lambda > 0 \ , \ \vec{u} = \lambda \vec{v}.$$

Montrer que c'est une relation d'équivalence.

Classes d'équivalence

Définition

La **classe d'équivalence** *d'un élément $x \in E$ est l'ensemble*

$$\overline{x} = \{y \in E \mid y \sim x\}.$$

Exemple

Pour la relation de congruence modulo 7 on a

$$\overline{0} = \{\ldots, -7, 0, 7, 14, 21, 28, 35, \ldots\},$$

$$\overline{3} = \{\ldots, -4, 3, 10, 17, 24, 31, \ldots\},$$

On remarque que :

$$\overline{24} = \overline{3}.$$

Une proposition importante

Proposition

Pour $x_1, x_2 \in E$ on a :

$$\overline{x_1} = \overline{x_2} \quad \Longleftrightarrow \quad x_1 \sim x_2.$$

Définition

Soit $C \subset E$ une classe d'équivalence. Un élément $x \in C$ est appelé un **représentant** *de la classe d'équivalence C.*

Exemple

Pour la relation de congruence modulo 7, 20 est un représentant de la classe d'équivalence $\overline{34}$.

Partition en classes d'équivalences

Proposition

Les classes d'équivalence forment une partition de E, c'est-à-dire que tout élément de E est dans une et une seule classe d'équivalence.

Exemple

Pour la relation de congruence modulo 2, la partition en classes d'équivalence est :

$$\mathbb{Z} = \overline{0} \sqcup \overline{1} = \{\text{entiers pairs}\} \sqcup \{\text{entiers impairs}\}.$$

Exercice 14

Dans le contexte de l'exercice précédent, quelle est la classe d'équivalence de $(1, 0)$? de $(1, 2)$? de $(0, 0)$? Décrire la partition de $\mathbb{R}^2$ en classes d'équivalence.

Quotient par une relation d'équivalence

Définition

L'ensemble des classes d'équivalence est appelé **quotient** *de* E *par la relation d'équivalence* $\sim$ *et noté* $E/\sim$.

- Un élément de l'ensemble quotient $E/\sim$ est une classe d'équivalence $\overline{x}$, pour un $x \in E$.
- On a égalité $\overline{x_1} = \overline{x_2}$ dans $E/\sim$ si et seulement $x_1 \sim x_2$ dans E.

Remarque

Le quotient est la manière mathématique d'*identifier* certains éléments de E entre eux. En effet, on décrète que des éléments qui sont équivalents (pour $\sim$) dans E sont maintenant *égaux* dans $E/\sim$.

L'application de quotient

Définition
L'application

$$\pi : E \longrightarrow E/\sim\ ,\ x \mapsto \overline{x}$$

est appelée **application de quotient**.

- Il est clair que π est surjective, par définition.

Définir une application sur un quotient

Définition

Soit une application

$$f : E \longrightarrow F.$$

- *On dit que f* **passe au quotient** *par $\sim$ si f prend la même valeur sur tous les éléments d'une même classe d'équivalence, c'est-à-dire si :*

$$\forall x, x' \in E\,,\ x \sim x' \implies f(x) = f(x').$$

- *Si f passe au quotient par $\sim$ alors on peut définir l'application*

$$g : E/\sim \longrightarrow F\ ,\ \overline{x} \mapsto f(x)$$

qui à une classe d'équivalence associe la valeur prise par f sur n'importe quel élément de cette classe d'équivalence.

- *On dit que g est l'application* **induite par** *f sur le quotient $E/\sim$.*

Un exercice

Exercice 15

Les applications suivantes passent-elles au quotient par la relation de congruence modulo 6 ?

$$f_1 : \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ n \mapsto (-1)^n\ ;$$

$$f_2 : \mathbb{Z} \longrightarrow \mathbb{Z}\ ,\ n \mapsto n^2 - 1\ .$$

Version à plusieurs variables

Remarque

On considérera aussi des applications définies non pas sur E mais sur le produit cartésien de E avec lui-même :

$$f : E \times E \longrightarrow F.$$

Dans ce cas-là on dit que f passe au quotient si elle passe au quotient "en chaque variable", c'est-à-dire si le résultat de $f(x_1, x_2)$ ne dépend que des classes d'équivalence $\overline{x_1}$ et $\overline{x_2}$, ou plus formellement si

$$\forall x_1, x_2, x_1', x_2' \in E\,,\ (x_1 \sim x_1' \ \text{ et } \ x_2 \sim x_2') \implies f(x_1, x_2) = f(x_1', x_2').$$

Dans ce cas-là on peut définir

$$g : (E/\sim) \times (E/\sim) \longrightarrow F\ ,\ (\overline{x_1}, \overline{x_2}) \mapsto f(x_1, x_2).$$

Définition

On fixe dans cette partie un entier $n \in \mathbb{N}^*$. On a vu que la relation de congruence modulo n,

$$a \sim b \quad \Longleftrightarrow \quad a \equiv b \,(\mathrm{mod}\, n)\,,$$

est une relation d'équivalence sur l'ensemble $\mathbb{Z}$.

Définition

On définit $\mathbb{Z}/n\mathbb{Z}$ comme le quotient de l'ensemble $\mathbb{Z}$ par la relation de congruence modulo n. Pour un entier $k \in \mathbb{Z}$, on note donc $\overline{k}$ sa classe d'équivalence dans $\mathbb{Z}/n\mathbb{Z}$.

- On a donc, pour $a, b \in \mathbb{Z}$:

$$\overline{a} = \overline{b} \quad \text{dans} \quad \mathbb{Z}/n\mathbb{Z} \qquad \Longleftrightarrow \qquad a \equiv b \pmod{n}.$$

- Notamment, pour $a \in \mathbb{Z}$:

$$\overline{a} = \overline{0} \quad \text{dans} \quad \mathbb{Z}/n\mathbb{Z} \qquad \Longleftrightarrow \qquad n|a.$$

Description de $\mathbb{Z}/n\mathbb{Z}$

Proposition

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ a n éléments : $\overline{0}$, $\overline{1}, \ldots, \overline{n-1}$.

Démonstration. Par division euclidienne, pour tout $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, il existe un unique $r \in \{0, \ldots, n-1\}$ tel que $\overline{a} = \overline{r}$ dans $\mathbb{Z}/n\mathbb{Z}$. C'est exactement ce que dit la proposition. □

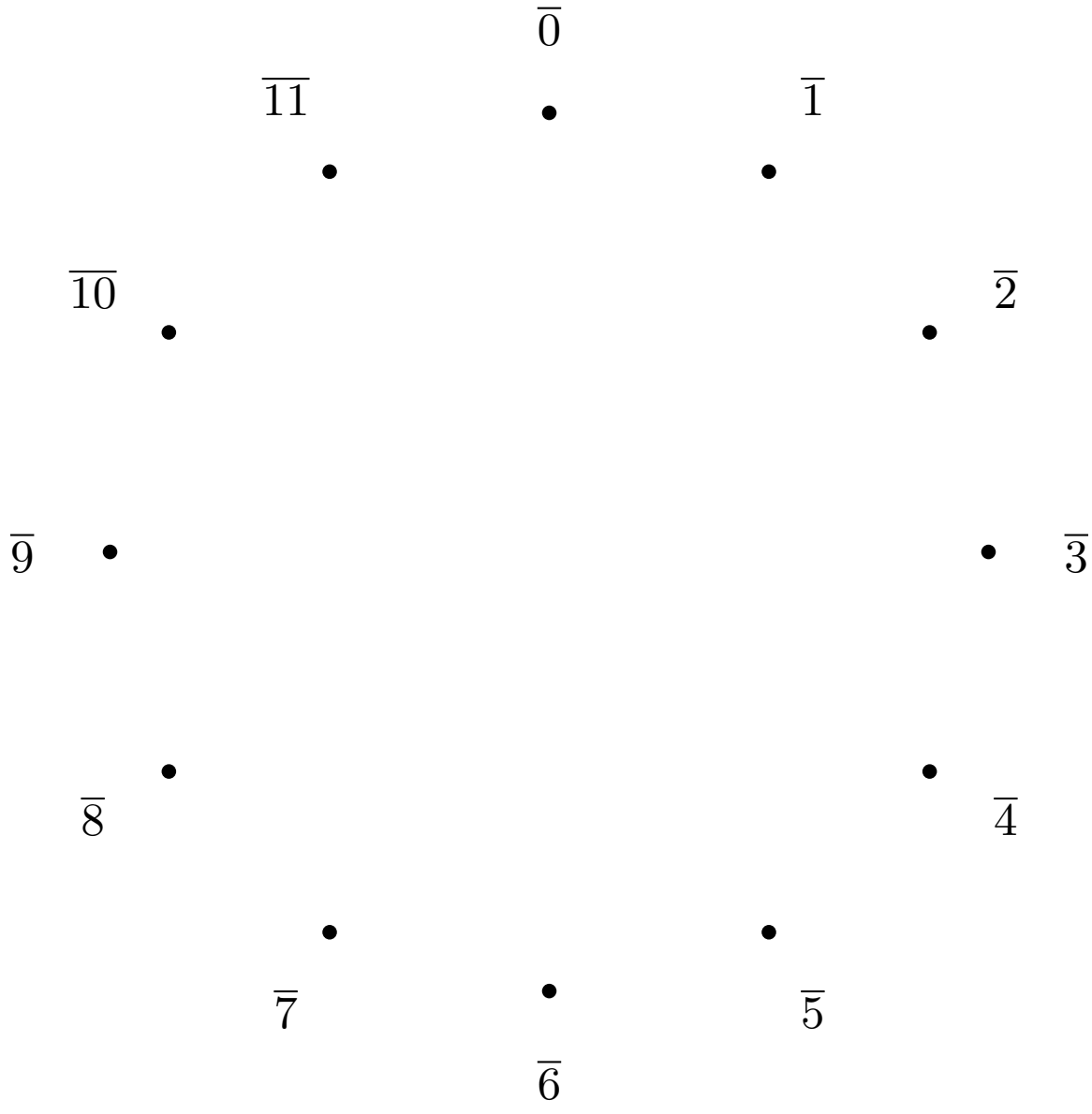
- Dit autrement, la partition de $\mathbb{Z}$ en classes d'équivalence pour la relation de congruence modulo n est :

$$\mathbb{Z} = \overline{0} \sqcup \overline{1} \sqcup \cdots \sqcup \overline{n-1}.$$

Exemple

Dans $\mathbb{Z}/7\mathbb{Z}$ on a $\overline{3} = \overline{10} = \overline{73} = \overline{-4}$, qui est l'ensemble des entiers $a \equiv 3 \pmod 7$, c'est-à-dire l'ensemble des $a \in \mathbb{Z}$ dont le reste dans la division euclidienne par 7 est 3, ou encore l'ensemble $\{7k + 3\,,\ k \in \mathbb{Z}\}$.

$\mathbb{Z}/12\mathbb{Z}$ est une horloge



Les lois $+$ et $\times$ dans $\mathbb{Z}/n\mathbb{Z}$

Proposition

L'addition dans $\mathbb{Z}$ passe au quotient et induit une loi $+$ dans $\mathbb{Z}/n\mathbb{Z}$ définie par

$$\overline{a} + \overline{b} = \overline{a+b}.$$

La multiplication dans $\mathbb{Z}$ passe au quotient et induit une loi $\times$ dans $\mathbb{Z}/n\mathbb{Z}$ définie par

$$\overline{a} \times \overline{b} = \overline{a \times b}.$$

Démonstration. C'est une traduction du fait que la relation de congruence modulo n est compatible à la somme et au produit.

- En effet, pour montrer que la somme $+$ dans $\mathbb{Z}/n\mathbb{Z}$ est bien définie, il faut montrer que le résultat $\overline{a+b}$ ne dépend pas du choix des représentants a et b.
- Dit autrement, on veut montrer que si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$ alors $\overline{a+b} = \overline{a'+b'}$ dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire que $a+b \equiv a'+b' \pmod{n}$.
- C'est exactement la compatibilité de la relation de congruence avec la somme.
- Il en va de même pour le produit.

□

Une remarque

Remarque

De manière plus formelle, on vient de "faire passer au quotient" l'application

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \ , \ (a, b) \mapsto \overline{a + b}$$

(et de même pour le produit).

Exemples (addition)

Exemple

Dans $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ on a

$$\overline{1} + \overline{1} = \overline{1+1} = \overline{2} = \overline{0}.$$

L'égalité "$\overline{1} + \overline{1} = \overline{0}$" veut dire : "la somme d'un nombre impair avec un nombre impair est un nombre pair".

Exemple

Dans $\mathbb{Z}/7\mathbb{Z}$ on a $\overline{3} + \overline{6} = \overline{3+6} = \overline{9} = \overline{2}$.

Exercice 16

Écrire la table d'addition de $\mathbb{Z}/7\mathbb{Z}$.

Illustration

- Voici une illustration de l'addition dans $\mathbb{Z}/12\mathbb{Z}$, vu comme une horloge.