

La dernière fois :

1) Définition de groupe

2) Théorème de Lagrange (version 1) :

Si G est un groupe abélien d'ordre n , alors $\forall g \in G, g^n = e_G$.

[Version additive : ---, alors $\forall g \in G, ng = 0_G$]

3) Sous-groupe d'un groupe.

4) Définition de groupe cyclique:

Un groupe (G, \cdot) est dit cyclique s'il existe $g \in G$ tel que $G = \langle g \rangle := \{g^n : n \in \mathbb{Z}\}$.

Dans ce cas g est dit un générateur de G .

Exemples

- $\mathbb{Z}/_{2\mathbb{Z}} = \langle 1 \rangle = \{0, 1\}$ est cyclique.

$\mathbb{Z}/_{n\mathbb{Z}} = \langle 1 \rangle = \{1, 2, 3, \dots, n-1, 0\}$ est cyclique

si n .

- \mathbb{Z}

$\langle 1 \rangle = \{n \cdot 1 : n \in \mathbb{Z}\} = \{n : n \in \mathbb{Z}\} = \mathbb{Z}$

Oui! \mathbb{Z} est cyclique

- Si (G, \cdot) est un groupe, alors $\forall a \in G$ le sous-groupe engendré $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$ est cyclique.

Exercice : $\left(\left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^\times, \cdot\right)$ est cyclique?

Si oui, quel est un générateur du groupe?

$$\left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^\times = \{1, \dots, 10\}$$

Question: $\exists a \in \{1, \dots, 10\}$ tel que :

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{1, \dots, 10\}?$$

$$\langle 1 \rangle = \{1\}$$

$$\begin{aligned} \langle 2 \rangle &= \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\} = \\ &= \left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^\times \end{aligned}$$

Donc $\frac{\mathbb{Z}}{11\mathbb{Z}}$ est cyclique et 2 est un générateur.

Déterminer un élément d'ordre 2 et un élément d'ordre 5.

$\langle 10 \rangle = \{10, 1\} \Rightarrow 10$ est un élément d'ordre 2
(dans $\frac{\mathbb{Z}}{11\mathbb{Z}}$, $10 = -1$)

$\langle 3 \rangle = \{3, 9, 5, 4, 1\} \Rightarrow 3$ est un élément d'ordre 5.

Donc 3 et 10 ne sont pas des générateurs de $\left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^\times$.

Déf. Soit (G, \cdot) un groupe et $a \in G$. L'ordre de a , noté $\text{ord}(a)$, est l'ordre du sous-groupe $\langle a \rangle$.

Remarque : Si G est fini, alors $\forall a \in G$ $\text{ord}(a)$ est fini.

(Parce que $\langle a \rangle \subseteq G$ et donc si G est fini, aussi $\langle a \rangle$ est fini).

Soit (G, \cdot) un groupe abélien et soit $H \leq G$ un sous-groupe de G . On définit la relation suivante sur G :

$$\forall a, b \in G, a \sim_H b \iff a \cdot b^{-1} \in H$$

Proposition : La relation \sim_H sur G est une relation d'équivalence, appelée relation de congruence modulo H .

Démo

• \sim_H est réflexive :

$$a \sim_H a, \text{ car } a \cdot a^{-1} = 1_G \in H$$

car H est un sous-groupe de G

• \sim_H est symétrique :

$$\begin{aligned} \text{Si } a \sim_H b &\Rightarrow a \cdot b^{-1} \in H \Rightarrow (a \cdot b^{-1})^{-1} \in H \Rightarrow \\ &\Rightarrow (b^{-1})^{-1} \cdot a^{-1} \in H \Rightarrow b \cdot a^{-1} \in H \Rightarrow b \sim_H a. \end{aligned}$$

• \sim_H est transitive :

$$\begin{aligned} \text{Si } a \sim_H b \text{ et } b \sim_H c &\Rightarrow a \cdot b^{-1} \in H \text{ et } b \cdot c^{-1} \in H \\ &\Rightarrow a \cdot b^{-1} \cdot b \cdot c^{-1} \in H \Rightarrow a \cdot c^{-1} \in H \Rightarrow a \sim_H c. \end{aligned}$$

□

Soit $a \in G$ et on considère la classe d'équivalence:

$$\begin{aligned}
 [a]_H &:= \{ b \in G : a \sim_H b \} = \\
 &= \{ b \in G : ab^{-1} \in H \} = \\
 &= \{ b \in G : \exists h \in H \text{ t.q. } ab^{-1} = h \} = \\
 &= \{ b \in G : \exists h \in H \text{ t.q. } b = ah^{-1} \} = \\
 &\supseteq \{ ah : h \in H \}
 \end{aligned}$$

\hookleftarrow $\in H$

G est abélien

On appelle les classes d'équivalence:

$$[a]_H := \{ ah : h \in H \}$$

les classes latérales de H dans G et on note
 G/H l'ensemble des classes latérales de H dans G .

$$G/H = \{ [a]_H, a \in G \}$$

Question: Peut-on voir la relation de congruence modulo n :

Soient $a, b \in \mathbb{Z}$, $a \sim_n b \iff n \mid a - b$

comme une relation de congruence sur \mathbb{Z} modulo n sous-groupe de \mathbb{Z} ?

Soit $G = \mathbb{Z}$ et $H = n\mathbb{Z} = \{ nk : k \in \mathbb{Z} \}$
 (on a vu dans le cours précédent que $n\mathbb{Z}$ est un sous-groupe de \mathbb{Z})

On montre que $\forall a, b \in \mathbb{Z}$

$$a \equiv b \text{ mod } n \iff a \sim_H b$$

$$\begin{aligned}
 a \equiv b \text{ mod } n &\iff n \mid a - b \Rightarrow \\
 &\iff \exists k \in \mathbb{Z} \text{ t.q. } a - b = nk \iff \\
 &\iff a - b \in n\mathbb{Z} \iff a \sim_H b
 \end{aligned}$$

Cela nous explique pourquoi on utilise la notation $\mathbb{Z}/n\mathbb{Z}$ pour les entiers modulo n .

Sur G/H on peut définir l'opération suivante :

$$\cdot : G/H \times G/H \longrightarrow G/H$$

$$([a]_H, [b]_H) \longmapsto [a]_H [b]_H := [ab]_H$$

Est-elle bien définie? Pour cela il faut montrer que si $a \sim_H a'$ et $b \sim_H b' \Rightarrow ab \sim_H a'b'$. (laissez par exercice)

Proposition : Si (G, \cdot) est un groupe abélien et $H \leq G$ est un sous-groupe de G alors $(G/H, \cdot)$ est un groupe abélien. De plus, si G est fini alors G/H est fini et son ordre est $|G|/|H|$.

Dém

On montre d'abord que G/H est un groupe abélien :

1) Le fait que \cdot est commutative et associative dans G/H décale du fait que \cdot est commutative et associative dans G .

2) Il y a un élément neutre : $[1]_H$

3) $\forall [a]_H \in G/H$, l'inverse est $[a^{-1}]_H$.

Donc G/H est un groupe abélien.

On suppose G fini. Donc H aussi est fini.

On montre d'abord que chaque classe d'équivalence contient exactement $|H|$ éléments :

Soit $a \in G$ et $\{ah\}_H := \{ah : h \in H\}$. Il est simple de voir que pour $h \in H$, les éléments ah sont tous distincts (si $ah = ah'$ $\Rightarrow a^{-1}ah = a^{-1}ah' \Rightarrow h = h'$)

Donc $|\{ah\}_H| = |H|$ et donc G/H a $|G|/|H|$ éléments.

Théorème de Lagrange (version 2)

Soit (G, \cdot) un groupe fini et soit H un sous-groupe de G . Alors l'ordre de H divise l'ordre de G .

Dém : cas abélien. G/H est un groupe avec $|G|/|H|$ éléments. Donc puisque $|G|/|H|$ est un entier, alors $|H| \mid |G|$.

Le résultat est vrai aussi par G non abélien, mais on ne le montre pas ici.

TD 5 - Exercice 1

$$G = (\mathbb{Z}/20\mathbb{Z})^\times$$

$$(a) G = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

$$(b) \langle 1 \rangle = \{1\}$$

$$\langle 3 \rangle = \{1, 3, 9, 7\}$$

$$\langle 7 \rangle = \{1, 7, 9, 3\}$$

$$\langle 9 \rangle = \{1, 9\}$$

$$\langle 11 \rangle = \{1, 11\}$$

$$\langle 13 \rangle = \{1, 13, 9, 17\}$$

$$\langle 17 \rangle = \{1, 17, 9, 13\}$$

$$\langle 19 \rangle = \{1, 19\}$$

(c) G n'est pas cyclique

$$(d) \quad \langle 11, 13 \rangle = \left\{ 11^n \cdot 13^m : n=0,1, m=0,1,2,3 \right\} = \\ = \{ 1, 13, 9, 17, 11, 3, 19, 7 \} = G$$

Donc G est engendré par l'ensemble $\{11, 13\}$

(e) Par le théorème de Lagrange, si H est un sous-groupe de $G = \left(\frac{N}{2NR}\right)^{\times}$,

alors $\{H\} \mid 8 \Rightarrow$ On a 4 possibilités pour $\{H\}$:

$$*) \quad |H| = \ell \iff H_1 = \{id\}$$

$$2) \quad |H| = 2 \Rightarrow H_2 = \langle 9 \rangle, \quad H_3 = \langle 11 \rangle, \quad H_4 = \langle 19 \rangle$$

$$3) \quad |H|=4 \quad \Rightarrow \quad H_5 = \langle 3 \rangle, \quad H_6 = \langle 13 \rangle,$$

$$H_7 = \langle 9, 11 \rangle = \{1, 9, 11, 19\}$$

$$* \quad 4) \quad |H|=8 \quad \Rightarrow \quad t_{\text{g}} = 6$$

*: sous-groupes triviaux

$$(f) \quad H = \langle 3 \rangle = \{1, 3, 7, 9\}$$

$$G/H = \{ [2]_H, [3]_H, [7]_H, [9]_H, [11]_H, [13]_H, [17]_H, [19]_H \}$$

$$[1]_H = \{ f \cdot h : h \in H \} = \{ 1, 3, 7, 9 \} = [3]_H = [7]_H = [9]_H$$

$$[11]_H = \{11, 13, 17, 19\} = [13]_H = [17]_H = [19]_H$$

$$\Rightarrow \mathbb{G}_{\mathbb{H}} = \{ [2]_{\mathbb{H}}, [4]_{\mathbb{H}} \} = \{ \{1, 3, 7, 9\}, \{11, 13, 17, 19\} \}$$

$$\left| \frac{G}{H} \right| = \frac{|G|}{|H|} = \frac{8}{4} = 2.$$

Anneaux

Def: Un anneau $(A, +, \cdot)$ est un ensemble A muni de deux opérations binaires, internes à A :

addition: $+ : A \times A \rightarrow A$

multiplication $\cdot : A \times A \rightarrow A$

tel que:

- 1) $(A, +)$ est un groupe abélien.
- 2) l'opération \cdot est associative et il existe un élément neutre par rapport à \cdot .
- 3) \cdot est distributive sur $+$:

$$a \cdot (b+c) = ab + ac$$

$$(a+b) \cdot c = ac + b \cdot c$$

Si \cdot est aussi commutative, alors $(A, +, \cdot)$ est dit un anneau commutatif.

Def: Un corps est un anneau commutatif $(K, +, \cdot)$ où tout élément non nul possède un inverse par rapport à \cdot .

Remarque: Un anneau commutatif $(A, +, \cdot)$ est un corps $\Leftrightarrow (A \setminus \{0\}, \cdot)$ est un groupe abélien.

Exemples

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ sont des anneaux
- $(\mathbb{Z}, +, \cdot)$ n'est pas un corps car $\forall a \neq 1, -1$, a n'est pas inversible.
- $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps $\Leftrightarrow n$ est un nombre premier.

- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sont des exemples de corps.
- $(n\mathbb{Z}, +, \cdot)$ est un anneau $\Leftrightarrow n = 1, -1$, car sinon $-1 \notin n\mathbb{Z}$.
- $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas un anneau:
 $1, \underbrace{n-1}_{\substack{\equiv \\ -1}} \in (\mathbb{Z}/n\mathbb{Z})^\times$, mais $1+n-1 = n=0$
n'est pas inversible.

Déf: Soit $(A, +, \cdot)$ un anneau. Un élément non nul $a \in A$ est un diviseur de zéro si l existe $b \in A \setminus \{0\}$ tel que $ab = 0$.
Un anneau sans diviseur de zéro est appelé un anneau intègre.

Exemple : Si n n'est pas premier, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Si n n'est pas premier, alors il existe $1 < a, b < n$ tel que $n = ab \rightarrow a$ et b sont deux diviseurs de zéro.

Remarque : Un corps est un anneau intègre :

$$\begin{aligned} &\text{Si } ab = 0 \text{ et } a \neq 0 \Rightarrow a^{-1}ab = a^{-1}0 \\ &\Rightarrow b = 0. \quad \begin{matrix} \uparrow \\ \text{si } a \neq 0, \exists a^{-1} \end{matrix} \end{aligned}$$