Algèbre et Arithmétique Effectives — 04/11/25 Cours 7

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

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

(notation additive : $a-b \in H$)

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

Dém

1) $\sim_H$ est réflexive :

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

(H est un sous-groupe de G)

2) $\sim_H$ est symétrique :

$\forall a,b \in G$, si $a \sim_H b \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H$

$\Rightarrow ba^{-1} \in H \Rightarrow b \sim_H a$.

3) $\sim_H$ est transitive :

$\forall a,b,c \in G$, si $a \sim_H b$ et $b \sim_H c \Rightarrow$

$\Rightarrow ab^{-1} \in H$ et $bc^{-1} \in H \Rightarrow ab^{-1}bc^{-1} \in H$

$\Rightarrow ac^{-1} \in H \Rightarrow a \sim_H c$.

□

Soit $a \in G$. On considère la classe d'équivalence de a :

$$[a]_H = \{b \in G : a \sim_H b\} = \{b \in G : ab^{-1} \in H\} =$$

$$= \{ b \in G : \exists\, h \in H \text{ t.q. } ab^{-1} = h \} =$$
$$= \{ b \in G : \exists\, h \in H \text{ t.q. } b = \underbrace{h^{-1}}_{\in H} a = \}$$
$$= \{ b \in G : \exists\, h \in H \text{ t.q. } b = ha \} =$$
$$= \{ ah : h \in H \}$$

($\uparrow$ G abélien)

On appelle les classes d'équivalence

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

les <u>classes latérales</u> de H dans G et on note G/H l'ensemble des classes latérales de H dans G :

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

<u>Question</u> : Peut-on voir la relation de congruence modulo n :

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

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

Soit $G = \mathbb{Z}$ (avec $+$) et $H = n\mathbb{Z} = \{ nk : k \in \mathbb{Z} \}$.

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

$$a \equiv b \mod n \iff a \sim_H b$$

$a \equiv b \mod n \iff \exists\, k \in \mathbb{Z}$ t.q. $a - b = nk$

$\iff a - b \in H = n\mathbb{Z} \iff a \sim_H b.$

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

Sur G/H on définit l'opération suivante :

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

multiplication dans G

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

Est-ce $\cdot$ bien définie ? Pour cela il faut montrer que si $a' \sim_H a$ et $b' \sim_H b$, alors $a'b' \sim_H ab$. (laissé 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 $\frac{|G|}{|H|}$.

Dém

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

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

2) $\exists$ 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 que G est fini. Donc H aussi est fini.

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

Soit $a \in G$ et $[a]_H = \{ah : h \in H\}$.

Il est simple de voir que les éléments ah par $h \in H$

sont tous distincts : si $ah_1 = ah_2 \Rightarrow a^{-1}ah_1 = a^{-1}ah_2$
$\Rightarrow h_1 = h_2$.

Donc $\forall\, a \in G$, $|[a]_H| = |H|$.

De plus les classes d'équivalence forment une partition de G, donc :

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

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 :

On démontre le théorème dans le cas abélien, mais il est vrai aussi dans le cas non commutatif.

On a vu que $\frac{G}{H}$ est un groupe abélien d'ordre $\frac{|G|}{|H|}$. Donc $\frac{|G|}{|H|} \in \mathbb{N} \Rightarrow |H| \mid |G|$.

Exemple

$$G = \left(\frac{\mathbb{Z}}{15\mathbb{Z}}\right)^\times = \{1,2,4,7,8,11,13,14\}$$

Rappel : $\left|\frac{\mathbb{Z}}{15\mathbb{Z}}\right| = \varphi(15) = \varphi(3\cdot 5) = \varphi(3)\varphi(5) = 2\cdot 4 = 8$

1) G est cyclique ?

$\langle 1\rangle = \{1\}$
$\langle 2\rangle = \{2,4,8,1\}$
$\langle 4\rangle = \{4,1\}$
$\langle 7\rangle = \{7,4,13,1\}$
$\langle 8\rangle = \{8,4,2,1\}$
$\langle 11\rangle = \{11,1\}$
$\langle 13\rangle = \{13,4,7,1\}$
$\langle 14\rangle = \{14,1\}$

Donc G n'est pas cyclique.

2) Déterminer tous les sous-groupes de G.

Si H est un sous-groupe de $G \Longrightarrow |H| \,|\, |G|$ (théorème de Lagrange)

$\Rightarrow |H| \,|\, 8$

Donc j'ai 4 possibilités pour $|H|$: $1, 2, 4, 8$.

- $|H| = 1 \iff H = \{1\}$ (trivial)
- $|H| = 2 \iff H = \langle 4 \rangle$ ou $H = \langle 11 \rangle$ ou $H = \langle 14 \rangle$
- $|H| = 4 \iff H = \langle 2 \rangle$, $H = \langle 7 \rangle$, $H = \langle 8 \rangle$, $H = \langle 13 \rangle$

  $H = \langle 4, 11 \rangle = \{1, 4, 11, 14\} = \langle 4, 14 \rangle = \langle 11, 14 \rangle$
- $|H| = 8 \iff H = G$ (trivial)

3) Soit $H = \langle 11 \rangle = \{1, 11\}$

Décrire le groupe quotient G/H.

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

$[1]_H = \{1, 11\}$
$[2]_H = \{2, 7\}$
$[4]_H = \{4, 14\}$
$[7]_H = [2]_H$

$[8]_H = \{8, 13\}$
$[11]_H = [1]_H$
$[13]_H = [8]_H$
$[14]_H = [4]_H$

$\Rightarrow G/H = \{ [1]_H, [2]_H, [4]_H, [8]_H \}$

Soit $K = \langle 4, 11 \rangle = \{1, 4, 11, 14\}$

Donc $G/K = \{ [1]_H, [2]_H \}$

$\{1, 4, 11, 14\}$ $\{2, 7, 8, 13\}$

Homomorphismes (ou morphismes) de groupes

Considérons les groupes suivants :

- $\mathbb{Z}/15\mathbb{Z}$ avec l'addition classique
- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ avec l'opération suivante :

$$+ : \left(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\right) \times \left(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}\right) \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$\left((a_1,b_1),(a_2,b_2)\right) \longmapsto (a_1,b_1)+(a_2,b_2) := (a_1+a_2, b_1+b_2)$$

exemple : $(2,4)+(1,3) = (0,2)$

Par le théorème des restes chinois on a déjà vu qu'il existe une bijection

$$\theta : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$[a]_{15} \longmapsto ([a]_3, [a]_5)$$

exemple : $\theta(7) = (1,2)$
$\theta(10) = (1,0)$

θ a une autre propriété : θ est "compatible" avec les opérations définies sur $\mathbb{Z}/15\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, c'est-à-dire on a que :

$$\theta([a]_{15} + [b]_{15}) = \theta([a]_{15}) + \theta([b]_{15})$$

$$\theta([a+b]_{15}) \qquad ([a]_3,[a]_5)+([b]_3,[b]_5)$$
$$([a+b]_3, [a+b]_5) = ([a]_3+[b]_3, [a]_5+[b]_5)$$

Donc on a montré que $\forall a, b \in \mathbb{Z}/15\mathbb{Z}$ on a

$$\theta(a+b) = \theta(a) + \theta(b)$$

↑ + dans $\mathbb{Z}/15\mathbb{Z}$; ↑ + dans $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

θ est en effet un exemple d'homomorphisme de groupes, qu'on va définir dans le prochain cours.