Algèbre et Arithmétique Effectives — 14/10/25 Cours 6

STRUCTURES ALGÉBRIQUES : Groupes

Déf. Un groupe est un couple $(G, \star)$ où G est un ensemble et $\star$ est une opération binaire interne :

$$\star : \begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & a \star b \end{array}$$

telle que :

① $\forall\, a,b,c \in G$, $(a \star b) \star c = a \star (b \star c)$ (associativité)

② $\exists\, e \in G$ tel que, $\forall\, a \in G$, $a \star e = e \star a = a$ (élément neutre)

③ $\forall\, a \in G$, $\exists\, b \in G$ tel que $a \star b = b \star a = e$ (inverse pour tout élément)

Un groupe est abélien ou commutatif si en plus, $\forall\, a,b \in G$, $a \star b = b \star a$.

On parle de groupe additif si $\star = +$ et de groupe multiplicatif si $\star = \cdot$.

Exemples

1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$

2) $(\mathbb{R}\setminus\{0\}, \cdot)$

3) $G = \{ f : \mathbb{R} \to \mathbb{R} \,:\, f \text{ est bijective} \}$

$$\circ : \begin{array}{ccc} G \times G & \longrightarrow & G \\ (f,g) & \longmapsto & f \circ g \end{array}$$

$(G, \circ)$ est un groupe (pas abélien)

2) $(\mathbb{Z}, \cdot)$ n'est pas un groupe car 0 n'est pas inversible.

Même chose pour $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$

3) $(\{1, -1\}, \cdot)$

$$\cdot : \{1,-1\} \times \{1,-1\} \longrightarrow \{1,-1\}$$
$$(1,1) \longmapsto 1$$
$$(1,-1) \longmapsto -1$$
$$(-1,1) \longmapsto -1$$
$$(-1,-1) \longmapsto 1$$

est un groupe abélien

4) $\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}, \cdot\right)$ est un groupe abélien

↑ les éléments inversibles mod n

À partir de maintenant on utilise la notation multiplicative :

1_G : élément neutre

g^n : $\underbrace{g \cdots g}_{n \text{ fois}}$, $\forall\ n \in \mathbb{Z}_{>0}$

g^0 : 1_G

g^{-n} : $\underbrace{(g^{-1}) \cdots (g^{-1})}_{n \text{ fois}}$, $\forall\ n \in \mathbb{Z}_{>0}$

Déf : L'ordre d'un groupe $(G,\cdot)$, noté $|G|$ est le nombre d'éléments de G. C'est soit un entier positif, soit ∞.

Un groupe d'ordre fini est appelé un groupe fini.

Théorème de Lagrange (version 1)

Soit $(G,\cdot)$ un groupe abélien fini d'ordre n.

Alors $\forall g \in G,\ g^n = 1_G$.

Dém

Soit $g \in G$ et on considère l'application

$$\begin{aligned} \varphi_g : G &\longrightarrow G \\ h &\longmapsto gh. \end{aligned}$$

On montre que cette application est bijective. Puisque G est fini, par cela il suffit de montrer que φ_g est injective :

Soient $h_1, h_2 \in G$ tels que :

$$\varphi_g(h_1) = \varphi_g(h_2) \Longrightarrow gh_1 = gh_2 \Longrightarrow g^{-1}gh_1 = g^{-1}gh_2$$
$$\Rightarrow h_1 = h_2.$$

Donc φ_g est bijective. Alors

$$\prod_{h\in G} h = \prod_{h\in G} gh \Longrightarrow \prod_{h\in G} h = g^{|G|} \prod_{h\in G} h$$

(G est abélien ; $\{gh : h\in G\} = \{\varphi_g(h) : h\in G\} = \varphi_g(G) = G$ ← φ_g est surjective ; $\prod_{h\in G} h = a \in G$; $a \in G$)

en multipliant par l'inverse de a

$$\Rightarrow 1_G = g^{|G|} = g^n.$$

Def : Soit $(G,\cdot)$ un groupe.
Un sous-ensemble $\emptyset \neq H \subseteq G$ est un sous-groupe de G si $(H,\cdot)$ est un groupe.

Si H est un sous-groupe de G on écrit $H \leq G$.

Exemples :

1) Soit $(G,\cdot)$ un groupe.
Alors $\{1_G\}$ et G sont toujours deux sougroupes de G (Sous-groupes triviaux)

2) $(\mathbb{Z},+)$
$\forall\, n \in \mathbb{Z}_{>0}$, le sous-ensemble
$$n\mathbb{Z} := \{nk, k \in \mathbb{Z}\}$$ (les multiples de n)
est un sous-groupe de $\mathbb{Z}$:

1) $+ : n\mathbb{Z} \times n\mathbb{Z} \to n\mathbb{Z}$, $(a,b) \mapsto a+b$ est une lois binaire interne
(ou $n\mathbb{Z}$ est fermé par rapport à $+$)
$a,b \in n\mathbb{Z} \Rightarrow \exists\, k_1, k_2 \in \mathbb{Z}$ t.q. $a = nk_1$, $b = nk_2$
$\Rightarrow a+b = nk_1 + nk_2 = n(k_1+k_2) \in n\mathbb{Z}$.

2) L'associativité est induite de l'associativité dans $\mathbb{Z}$.

3) $0 = 0 \cdot n \in n\mathbb{Z}$

4) Soit $a \in n\mathbb{Z} \Rightarrow a = nk$, $k \in \mathbb{Z}$. Alors
$-a = n(-k) \in n\mathbb{Z}$.

Proposition : Soit $(G,\cdot)$ un groupe.
Un sous-ensemble non vide $H \subseteq G$ est un sous-groupe de G si et seulement si $\forall\, a,b \in H$, $ab^{-1} \in H$

Dém : par exercice.

Déf : Soit $(G,\cdot)$ un groupe et $a \in G$. L'ensemble

$$\langle a \rangle := \{ a^n : n \in \mathbb{Z} \}$$

est un sous-groupe de G, appelé le sous-groupe engendré par a.

Dém : Montrons que $\langle a \rangle$ est un sous-groupe de G.

Clairement $\langle a \rangle$ est non vide, car $a \in \langle a \rangle$.

Soient $g_1, g_2 \in \langle a \rangle \Rightarrow \exists\, n_1, n_2 \in \mathbb{Z}$ t.q. $g_1 = a^{n_1}$ et $g_2 = a^{n_2}$.

Alors on a :

$$g_1 \cdot g_2^{-1} = a^{n_1} \cdot a^{-n_2} = a^{\underbrace{n_1 - n_2}_{\in \mathbb{Z}}} \in \langle a \rangle.$$

Donc $\langle a \rangle$ est un sous-groupe de G.

Déf : Un groupe $(G,\cdot)$ est dit cyclique s'il existe $g \in G$ tel que :

$$G = \langle g \rangle.$$

Dans ce cas l'élément g est dit un générateur de G.

Déf : Soit $(G,\cdot)$ un groupe et $a \in G$.

L'ordre de a, noté $\mathrm{ord}(a)$, est l'ordre du sous-groupe engendré par a.

En particulier, si l'ordre de a est fini, alors c'est le plus petit entier $k > 0$ tel que $a^k = 1_G$.

Exemples

1) $(\mathbb{Z}, +)$, est-il cyclique ?

Attention : en notation additive, si $a \in \mathbb{Z}$, alors :

$$\langle a \rangle = \{na : n \in \mathbb{Z}\} = a\mathbb{Z}$$

Oui, car $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ et 1 et -1 sont les seuls générateurs de $(\mathbb{Z}, +)$.

2) $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$, est-il cyclique ?

Oui, car $\frac{\mathbb{Z}}{n\mathbb{Z}} = \langle 1 \rangle$.

Exemple : $\frac{\mathbb{Z}}{10\mathbb{Z}}$: 2 n'est pas un générateur car $\langle 2 \rangle = \{0, 2, 4, 6, 8\} \neq \frac{\mathbb{Z}}{10\mathbb{Z}}$

$\frac{\mathbb{Z}}{10\mathbb{Z}} = \langle a \rangle$, $\forall$ a t.q. $\text{pgcd}(a, 10) = 1$.

3) Si $(G, \cdot)$ est un groupe, alors $\forall a \in G$ le sous-groupe engendré $\langle a \rangle$ est cyclique.

4) $\left(\left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^{\times}, \cdot\right)$: est-il cyclique ? Si oui, quel est un générateur ?

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

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

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^{\times} ?$$

$$\langle 1 \rangle = \{1\} \neq \left(\frac{\mathbb{Z}}{11\mathbb{Z}}\right)^{\times}$$

$\langle 2 \rangle = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\} =$

$= \{1, \_, 10\} = (\mathbb{Z}/11\mathbb{Z})^\times$

$\Rightarrow (\mathbb{Z}/11\mathbb{Z})^\times$ est cyclique et 2 est un générateur.

$\forall\, a \in (\mathbb{Z}/11\mathbb{Z})^\times$, déterminer l'ordre de a :

- $\text{ord}(1) = 1$
- $\text{ord}(2) = |\langle 2 \rangle| = 10$
- $\langle 3 \rangle = \{1, 3, 9, 5, 4\} \Rightarrow \text{ord}(3) = 5$

  $\Rightarrow$ 3 n'est pas un générateur.

  ⋮
- $\langle 10 \rangle = \{1, 10\} \Rightarrow \text{ord}(10) = 2.$

5) $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$

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

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

$\langle 5 \rangle = \{1, 5\}$

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

Donc $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est pas cyclique et tous les éléments, sauf 1, ont ordre 2.