Algèbre et Arithmétique Effectives — 03/11/26 cours 8

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, $a \star b = b \star a$, $\forall\, a,b \in G$.

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

Lemme : Soit $(G, \star)$ un groupe. Alors :

1) L'élément neutre est unique.

2) $\forall\, a \in G$, il existe un unique inverse de a, noté a^{-1}.

3) $\forall\, a,b \in G$, $(a^{-1})^{-1} = a$ et $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

Dém

1) Soient $e_1, e_2 \in G$ deux éléments tels que

$e_i * a = a * e_i = a$, pour $i = 1,2$.

Alors $e_1 * e_2 = e_2$ et $e_1 * e_2 = e_1$

(e_1 élément neutre) (e_2 élément neutre)

Donc $e_1 = e_2$.

2) Soient $b_1, b_2 \in G$ tels que :

$$a * b_i = b_i * a = 1_G \quad , \quad i = 1,2$$

où 1_G est l'élément neutre.

Alors on a :

$$b_1 = b_1 * 1_G = b_1 * (a * b_2) = (b_1 * a) * b_2 = 1_G * b_2 = b_2$$

Donc $b_1 = b_2$

3) $a * a^{-1} = 1_G \Rightarrow a = (a^{-1})^{-1}$

$$(a*b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * 1_G * a^{-1} =$$

$$= a * a^{-1} = 1_G$$

$$\Downarrow$$

$$(a*b)^{-1} = b^{-1} * a^{-1}.$$

Exemples

1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$ sont des groupes abéliens.

2) (Non-exemple) $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$, $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \cdot\right)$ ne sont pas des groupes, car 0 n'a pas d'inverse.

3) $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{R}\setminus\{0\}, \cdot)$, $(\mathbb{C}\setminus\{0\}, \cdot)$ sont des groupes abéliens

4) (Non-exemple) $(\mathbb{Z}\setminus\{0\}, \cdot)$ n'est pas un groupe car 2 n'a pas d'inverse

5) Soit $(\mathbb{Z})^\times$ l'ensemble des entiers inversibles dans $\mathbb{Z}$. On a

$$(\mathbb{Z})^\times = \{-1, 1\}$$

Alors $(\{-1,1\}, \cdot)$ est un groupe abélien, dont la table de multiplication est :

$\cdot$	-1	1
-1	1	-1
1	-1	1

6) Similairement on a que $\left(\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times, \cdot\right)$ est un groupe abélien.

En effet, si $a, b \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$, alors $\exists\, a^{-1}, b^{-1} \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ t.q. $aa^{-1} = 1$ et $bb^{-1} = 1$.

Donc $(ab)(b^{-1}a^{-1}) = 1 \Rightarrow ab \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$.

La multiplication est associative et commutative, car elle est associative et commutative dans $\mathbb{Z}/n\mathbb{Z}$ et $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times \subseteq \frac{\mathbb{Z}}{n\mathbb{Z}}$.

L'élément neutre est $1 \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$

Et $\forall\, a \in \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ il existe un inverse (aussi inversible) par définition

7) Soit K un corps et $\mathcal{M}_n(K)$ l'ensemble des matrices $n \times n$ à coefficients dans K. Alors $(\mathcal{M}_n(K), +)$ est un groupe abélien.

8) Soit $GL_n(K) = \{A \in \mathcal{M}_n(K) : A \text{ est inversible}\}$.

Alors $(GL_n(K), \cdot)$ est un groupe (non-commutatif pour $n > 1$)

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

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

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

L'élément neutre est $id_{\mathbb{R}} : x \longmapsto x$.

Il est non abélien, car par exemple pour $f(x) = 2x+1$ et $g(x) = 2x$ on a :

$$f \circ g(x) = 4x+1 \quad \text{et} \quad g \circ f(x) = 4x+2$$

et $f \circ g(x) \neq g \circ f(x) \quad \forall x \in \mathbb{R}$.

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

Règles de calculs (facilement démontrables)

- $g^m g^n = g^{m+n}$, $\forall m, n \in \mathbb{Z}$
- $(g^m)^n = g^{mn}$, $\forall m, n \in \mathbb{Z}$
- $(g^n)^{-1} = g^{-n}$, $\forall n \in \mathbb{Z}$

Attention : En général (si G n'est pas abélien) $(gh)^n \neq g^n h^n$

On a : $(gh)^n = \underbrace{gh \cdot gh \cdots gh}_{n \text{ fois}}$

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

$$\varphi_g : \begin{array}{ccc} G & \longrightarrow & G \\ h & \longmapsto & gh \end{array}$$

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 :

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

Donc φ_g est bijective. En particulier φ_g est surjective, donc $G = \varphi_g(G)$

$\{h : "h \in G"\}$ $\{gh : h \in G\}$

Donc on a :

$$\prod_{h\in G} h = \prod_{h\in G} gh \Rightarrow \underbrace{\prod_{h\in G} h}_{"a\in G"} = g^{|G|} \underbrace{\prod_{h\in G} h}_{a\in G}$$

(G abélien)

en multipliant par l'inverse de a

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

Remarque : Le théorème de Lagrange est vrai aussi pour un groupe fini non-abélien, mais on ne le démontrera pas.

On a deux corollaires du théorème de Lagrange que nous avons déjà rencontré en TD et en TP.

Corollaire 1 (Petit théorème de Fermat)

Soit p un nombre premier et soit $a \in \mathbb{Z}$ t.q. $p \nmid a$. Alors

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

Dém

$\left(\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times, \cdot\right)$ est un groupe abélien fini avec $\varphi(p) = p-1$ éléments. Alors, d'après le théorème de Lagrange,

$$a^{p-1} = 1, \quad \forall\, a \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times$$

Cela équivaut à

$$a^{p-1} \equiv 1 \pmod{p}, \quad \forall\, a \in \mathbb{Z},\ \operatorname{pgcd}(a,p) = 1$$

$\Updownarrow$

$p \nmid a$.

Corollaire 2 (Théorème d'Euler)

Soit $n \geq 1$ et $a \in \mathbb{Z}$ t.q. $\operatorname{pgcd}(a,n) = 1$. Alors

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Dém

Totalement analogue à la précédente, en considérant le groupe $\left(\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times, \cdot\right)$.

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 $H \leq G$.

Remarque : Si $H \leq G$, alors l'élément neutre de H est nécessairement 1_G.
De même, l'inverse d'un élément de H dans H est son inverse dans G.

Exemples :

1) Soit $(G,\cdot)$ un groupe.
Alors $\{1_G\}$ et G sont toujours deux sousgroupes 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 loi 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
$-a = n(-k) \in n\mathbb{Z}$.