STRUCTURES ALGÉBRIQUES 2017/2018 UE: ENSMI6UX

Les structures algébriques étudiées ici sont les groupes, les anneaux et les corps. La première moitié du corps se passe dans le monde des groupes.

Définition 1. *Un* **groupe** $(G, *)$ *est un ensemble* G *muni d'une opération (ou loi)* $*$*, c'est à dire une application* $m : G \times G \to G$ *— on écrira* $a * b$ *pour l'image* $m(a, b)$ *le "produit"de* a *et* b *— tel que*

(i) l'opération est **associative** *:* $\forall a, b, c \in G$ *on a* $(a * b) * c = a * (b * c)$ *;*

(ii) Il existe un élément **identité** *ou* **neutre** $e \in G$ *avec la propriété :* $\forall g \in G$*, on a* $e * g = g = g * e$ *;*

(iii) $\forall g \in G\ \exists$ **inverse** *ou* **symétrique** $g^{-1} \in G$ *t.q.* $g^{-1} * g = e = g^{-1} * g$ *.*

Un groupe $(G, *)$ *est* **abelien** *ou* **commutatif** *si* $\forall g, h \in G$ *on a* $g * h = h * g$*.*

Un sous–ensemble $H \subset G$ *est un* **sousgroupe** *de* $(G, *)$ *si la restriction de l'opération* $*$ *à* H *donne un structure de groupe. On écrit souvent* $H < G$*.*

Vérifier que $H \subset G$ *est un sousgroupe ssi (a)* $e \in H$*, (b)* $\forall h \in H$ *on a* $h^{-1} \in H$*, et (c)* $\forall h_1, h_2 \in H$ *on a* $h_1 * h_2 \in H$*.*

Soient $(G, *)$ *et* $(K, \odot)$ *des groupes. Une application* $h : G \to K$ *est un* **homomorphisme** *ou* **morphisme** *si* $\forall g_1, g_2 \in G$ *on a* $h(g_1 * g_2) = h(g_1) \odot h(g_2)$*. "l'image du produit est le produit des images"*

Donc le diagramme commute:

$$\begin{array}{ccc} G \times G & \xrightarrow{h \times h} & K \times K \\ * \downarrow & & \downarrow \odot \\ G & \xrightarrow{h} & K \end{array} \qquad \text{c'est à dire} \qquad \begin{array}{ccc} (g_1, g_2) & \xrightarrow{h \times h} & (h(g_1), h(g_2)) \\ * \downarrow & & \downarrow \odot \\ g_1 * g_2 & \xrightarrow{h} & h(g_1 * g_2) = h(g_1) \odot h(g_2) \end{array}$$

L'application identité du groupe $id_G : G \to G$ *où* $id_G(g) = g$ *pour tout* $g \in G$ *est un homomorphisme.*

Si H *est un sous–groupe de* G *alors l'inclusion de* H *dans* G *est un homomorphisme.*

Si $(G, *)$ *et* $(K, \odot)$ *sont des groupes et* $e_G \in G$ *est l'identité de* G*, net* $e_K \in K$ *est l'identité de* K*, alors l'application* $h(g) = e_k$ $\forall g \in G$ *est un homomorphisme.*

Pour un groupe fini on peut écrire une table de multiplication, avec une ligne pour chaque $g_i \in G$, et une colonne pour chaque $g_j \in G$, et à l'intersection de cette ligne et cette colonne on place l'élément $g_i * g_j$. Il n'est pas dificil de voir que chaque élément apparaît exactement une fois dans chaque ligne et exactement une fois dans chaque colonne (si on a $g_i * g_j = g_i * g_k$ et si on multiplie par l'inverse de g_i alors ....)

Quelques Exemples Importants

I. Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ avec la loi d'addition sont des groupes abeliens.

Aussi, pour $n \in \mathbb{N}$, les groupes cycliques $\frac{\mathbb{Z}}{n\mathbb{Z}}$ (les entiers modulo n) avec addition.

Les ensembles $\mathbb{Q}^* = \mathbb{Q} - \{0\}, \mathbb{R}^* = \mathbb{R} - \{0\}$ et $\mathbb{C}^* = \mathbb{C} - \{0\}$ avec multiplication.

Aussi les inversibles dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$, en particulier les élements non-nuls de $\frac{\mathbb{Z}}{p\mathbb{Z}}$ (p premier), avec multiplication forment des groupes abéliens (on trouve les inverses utilisant Bezout).

II. Soient $(A, *), (B, \odot)$ des groupes: alors le produit cartesien $A \times B$ avec opération

$(a_1, b_1) \otimes (a_2, b_2) = (a_1 * a_2, b_1 \odot b_2)$: l'élément neutre est ???

III. Soit Ω un ensemble non–vide. La collection $S(\Omega)$ de toutes les permutations (ou symétries) de Ω, c'est à dire les applications bijectives $\Omega \to \Omega$ munie de la loi de composition d'applications, est un groupe (non–abélien si $Card(\Omega) > 2$).

Le groupe symétrique, $S_n = S(\{1, 2, \ldots, n)\})$ possède $n!$ éléments: on l'a utilisé pour la définition du déterminant d'une matrice.

IV. L'ensemble des matrices $M(2, \mathbb{Z}) = M_2(\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}\}$ avec addition.

V. Les ensembles $GL_2(\mathbb{R}) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, \det(A) \neq 0\}$ ou $GL_2(\mathbb{Z}) = GL(2, \mathbb{Z}) =$

$\{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, \det(A) = \pm 1\}$ munis de multiplication. L'élément neutre est ???

Date: January 19, 2018.

VI. L'ensemble fini $\{1,-1\}$ avec multiplication. On a une table de multiplication (*cfr.* le groupe d'addition modulo 2, $\mathbb{Z}/2\mathbb{Z}$)

$*$	1	-1
1	$1*1=1$	$1*-1=-1$
-1	$-1*1=-1$	$1*1=1$

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

Le groupe symétrique $S_3 = \{Id, \tau_1, \tau_2, \tau_3, \rho_1, \rho_2\}$, où $\tau_1 = (2\,3)$, $\tau_2 = (1\,3)$ $\tau_3 = (1\,2)$ $\rho_1 = (1\,2\,3)$ $\rho_2 = (1\,3\,2)$
Table de multiplication: $\tau_1 * \tau_2 = \rho_1$ ...

$*$	Id	τ_1	τ_2	τ_3	ρ_1	ρ_2
Id	Id	τ_1	τ_2	τ_3	ρ_1	ρ_2
τ_1	τ_1	Id	ρ_1	ρ_2	τ_2	τ_3
τ_2	τ_2	ρ_2	Id	ρ_2	τ_3	τ_1
τ_3	τ_3	ρ_1	ρ_2	Id	τ_1	τ_2
ρ_1	ρ_1	τ_3			ρ_2	Id
ρ_2	ρ_2	τ_2				

Quelques sous-groupes

I. $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$.
Les entiers pairs, $2\mathbb{Z} = \{2n \mid n \in Z\}$ est un sous–groupe de $(\mathbb{Z},+)$.
Avec multiplication, $\{1,-1\}$ est un sous–groupe de $(\mathbb{Q}^*,\times) < (\mathbb{R}^*,\times) < (\mathbb{C}^*,\times)$.

II. Soient e_A, e_B les éléments neutres de $(A,*)$ et $(B,\odot)$.
Alors $A \times \{e_B\}$ et $\{e_A\} \times B$ sont des sous–groupes de $(A \times B, \otimes)$
Plus généralement, si H, K sont des sous–groupes de $(A,*)$ et $(B,\odot)$ alors $H \times K$ est un sous–groupe de $(A \times B, \otimes)$

III. Dans le groupe symétrique S_n, on a le sous–groupe des permutations qui fixent un élément choisi. Ainsi on voit des copies de S_{n-1} dans S_n. Ainsi $\{Id, \tau_1\}$, $\{Id, \tau_2\}$ et $\{Id, \tau_3\}$ sont des sous–groupes de S_3.
De la même façon, pour $\Omega' \subset \Omega$ on voit $S(\Omega')$ comme sous–groupe de $S(\Omega)$.

IV. L'ensemble $\left\{ \begin{pmatrix} 2a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z} \right\} < (M_2(\mathbb{Z}),+)$; $\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} a,b,d \in \mathbb{Z} \right\}$ aussi.

V. $SL_2(\mathbb{Z}) = \left(\left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}, \det(A) = 1 \right\}, \times \right) < (GL_2(\mathbb{Z}),\times) < (Gl_2(\mathbb{R}),\times) < (Gl_2(\mathbb{C}),\times)$
$\left(\left\{ A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, b \in \mathbb{Q} \right\}, \times \right) < \left(\left\{ A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, a,b,d \in \mathbb{Q}, ad \neq 0 \right\}, \times \right) < Gl_2(\mathbb{Q},\times)$

VI. Pour $g \in G$, on dénote par g^n le produit de n facteurs g, quand $n > 0$, et le produit de $|n|$ facteurs g^{-1} quand $n < 0$ et on pose $g^0 = e$, l'élément neutre de G.
L'ensemble $\{g^n \mid n \in \mathbb{Z}\}$ est un sous–groupe de G, le *sous–groupe cyclique engendré par* g, dénoté $\langle g \rangle$.
L'ordre de g dans G est le nombre d'éléments dans $\langle g \rangle$: montrer $= \min\{k \mid k \in \mathbb{N}^*, g^k = e\}$) —on dit que l'ordre est infini quand l'ensemble $\{k \mid k \in \mathbb{N}^*, g^k = e\}$ est vide.

Quelques homomorphismes

I. L'application $f : (\mathbb{Z},+) \to (\mathbb{Z},+)$ t.q. $f(n) = 3n$ est un homomorphisme.
L'application $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ où l'image $\bar{m}$ est le reste de m après division eucildien de m par n. Si $m = kn+r$ et $m' = k'm+r'$, alors $m+m' = (k+k')m+r+r'$ et ..... donc on a un homomorphisme.
L'application $(\mathbb{C},+) \to (\mathbb{C},+) : z \to \mathfrak{Re}(z)$ la partie réelle, est un homomorphisme.
La valeur absolue $z \to |z|$ est un homomorphisme de $(\mathbb{C}^*,\times) \to (\mathbb{R}^{>0},\times)$.
L'argument $z = re^{i\theta} \to \theta (\mathrm{mod} 2\pi)$ est un homomorphisme de $(\mathbb{C}^*,\times) \to ([0,2\pi[,+(\mathrm{mod}2\pi))$.

II. Si $(A \times B, \otimes)$ est le produit cartesien de $(A,*)$ et $(B,\odot)$, alors sont des homomorphismes
$\pi_1 : (A \times B, \otimes) \to (A,*) : \pi_1(a,b) = a$ et $\pi_2 : (A \times B, \otimes) \to (B,\odot) : \pi_2(a,b) = b$

III. Soit $\mathbb{R}^{>0} = \{r \in \mathbb{R} \mid r > 0\}$, muni de l'opération de multiplication, et soit $\mathbb{R}$ le groupe des réels avec la loi d'addition. Alors l'application $\mathrm{Log} : (\mathbb{R}^{>0},\times) \to (\mathbb{R},+)$ est un homomorphisme.

IV. Signature: $sign : S_n \to (\{1,-1\},\times)$ (où $sign(\sigma)$ est la parité du nombre de transpositions requises pour écrire σ comme produit de transpositions) est un homomorphisme.

V. L'application $det : (Gl_n(\mathbb{R}),\times) \to (\mathbb{R}^*,\times)$ est un homomorphisme.