SAVOIRS

Thème 1 - Structures algébriques usuelles

[S1.1] Magmas

- Un magma est un couple $(E,*)$, où E est un ensemble et $*$ une loi de composition interne sur E, c'est-à-dire une application de E^2 dans E.
  Si $(E,*)$ est un magma, une partie F de E est dite stable par la loi $*$ si :
  $$\forall\,(x,y) \in F^2,\ x * y \in F\,.$$
  La restriction de la loi $*$ à F^2 s'appelle alors la loi induite sur F.

- **Associativité**
  Soit $(E,*)$ un magma. La loi $*$ est dite associative si :
  $$\forall\,(x,y,z) \in E^3,\ (x * y) * z = x * (y * z)\,.$$
  Si tel est le cas, pour tout élément x de E, et tout entier n de $\mathbb{N}^*$, on pourra définir l'itéré n^{e} de x par : $x^{(n)} = \underbrace{x * x * \ldots * x}_{n \text{ fois}}$ (noté x^n si la loi est notée multiplicativement, ou nx si la loi est notée additivement).
  On a facilement, pour tous n et m de $\mathbb{N}^*$:
  $$x^{(n+m)} = x^{(n)} * x^{(m)} \quad \text{et} \quad \left(x^{(n)}\right)^{(m)} = x^{(nm)}.$$

- **Commutativité**
  Soit $(E,*)$ un magma. Deux éléments x et y de E sont dits permutables (ou qu'ils commutent) si $x * y = y * x$.
  Si x et y sont deux éléments permutables d'un magma associatif $(E,*)$, alors :
  - pour tous entiers n et m de $\mathbb{N}^*$, $x^{(n)}$ et $y^{(m)}$ sont permutables ;
  - pour tout entier $n \in \mathbb{N}^*$, $x^{(n)} * y^{(n)} = (x * y)^{(n)}$.

  La loi $*$ est dite commutative si tous les éléments commutent entre eux, soit :
  $$\forall\,(x,y) \in E^2,\ x * y = y * x\,.$$

- **Élément neutre**
  On appelle élément neutre d'un magma $(E,*)$ un élément $e \in E$ tel que :
  $$\forall\, x \in E,\ x * e = e * x = x\,.$$
  Si $(E,*)$ possède un élément neutre, celui-ci est unique. Un magma qui possède un élément neutre est dit unifère.

- **Symétrique**
  - Soit $(E,*)$ un magma unifère d'élément neutre e, et x un élément de E.
    On appelle symétrique à gauche (respectivement à droite) de x un élément x' (respectivement x'') de E, s'il existe, tel que :
    $$x' * x = e \quad (\text{respectivement } x * x'' = e)\,.$$
    Si x' (respectivement x'') existe, on dit que x est symétrisable à gauche (respectivement à droite).

▪ Soit $(E,*)$ un magma unifère d'élément neutre e, et x un élément de E.
On appelle symétrique de x un élément x' de E, s'il existe, tel que :

$$x' * x = x * x' = e\,.$$

Si x' existe, x est dit symétrisable.

Cela équivaut à dire que x est symétrisable à droite *et* à gauche *et* que ses symétriques à droite et à gauche sont égaux.

Exemple : dans l'ensemble $\mathcal{A}(E,E)$ des applications de E dans E, muni de la loi $\circ$, les éléments symétrisables à droite sont les applications surjectives et les éléments symétrisables à gauche sont les applications injectives. Les éléments symétrisables sont donc les applications bijectives de E sur E.

▪ Soit $(E,*)$ un magma *associatif et unifère* ($(E,*)$ s'appelle alors un *monoïde*).

– Si un élément x de E admet un symétrique à droite et un symétrique à gauche, ceux-ci sont égaux (et x est alors symétrisable).

– Si un élément x de E est symétrisable, son symétrique est unique.

– Si un élément x de E est symétrisable, de symétrique x', alors x' est symétrisable, de symétrique x.

– Si x et y sont symétrisables (de symétriques respectifs x' et y') , il en est de même de $x * y$ et : $(x * y)' = y' * x'$.

✓ Lorsque la loi est notée multiplicativement, on parle *d'inverse* au lieu de symétrique. Lorsqu'elle est notée additivement, on parle *d'opposé*.

▪ Soit $(E,*)$ un magma unifère, et x un élément de E. On note : $x^{(0)} = e$.

Si x est symétrisable, de symétrique x', pour tout $n \in \mathbb{N}^*$ on note $x^{(-n)}$ l'élément $x'^{(n)}$ (ainsi, $x' = x^{(-1)}$).

On peut ainsi, lorsque x est symétrisable, étendre la notation $x^{(n)}$ pour $n \in \mathbb{Z}$.

– Soit x un élément *symétrisable* de E. Alors, pour tous n et m de $\mathbb{Z}$, on a :

$$x^{(n+m)} = x^{(n)} * x^{(m)} \quad \text{et} \quad \left(x^{(n)}\right)^{(m)} = x^{(nm)}.$$

– Soient x et y deux éléments *permutables* et *symétrisables* de E. Alors :

– pour tous entiers n et m de $\mathbb{Z}$, $x^{(n)}$ et $y^{(m)}$ sont permutables ;

– pour tout entier $n \in \mathbb{Z}$, $x^{(n)} * y^{(n)} = (x * y)^{(n)}$.

• **Éléments réguliers**

Soit $(E,*)$ un magma. Un élément a de E est dit régulier (ou simplifiable) à gauche (respectivement à droite) si :

$\forall\,(x,y) \in E^2,\ a * x = a * y \ \Rightarrow\ x = y$ (respectivement $x * a = y * a \ \Rightarrow\ x = y$) .

Un élément a de E est dit régulier s'il est à la fois régulier à gauche *et* à droite.

Soit $(E,*)$ un magma associatif et unifère. Si un élément a de E est symétrisable, (à droite, à gauche), *alors* il est régulier (à droite, à gauche).

✓ La réciproque de cette proposition est fausse en général.
Par exemple, dans $(\mathbb{Z},\times)$, 2 est régulier mais non symétrisable.

[S1.2] Morphismes de magmas

- Soient $(E,*)$ et $(F,\square)$ deux magmas.

  On dit qu'une application $f\colon E \to F$ est un morphisme de $(E,*)$ dans $(F,\square)$ si :

  $$\forall\,(x,y) \in E^2,\ f(x*y) \ = \ f(x)\square f(y)\,.$$

  Un isomorphisme est un morphisme bijectif. Un endomorphisme est un morphisme de $(E,*)$ dans lui-même. Un automorphisme est un endomorphisme bijectif.

  Exemple : si $(E,*)$ est un magma associatif unifère et si x est un élément symétrisable de E, l'application $n \mapsto x^{(n)}$ est un morphisme de $(\mathbb{Z},+)$ dans $(E,*)$.

- Si f est un morphisme de $(E,*)$ dans $(F,\square)$ et si g un morphisme de $(F,\square)$ dans $(G,\triangle)$, la composée $g \circ f$ est un morphisme de $(E,*)$ dans $(G,\triangle)$.

- Si f est un isomorphisme de $(E,*)$ dans $(F,\square)$, alors son application réciproque f^{-1} est un isomorphisme de $(F,\square)$ dans $(E,*)$.

  Exemple : l'application $x \mapsto \mathrm{e}^x$ est un isomorphisme de $(\mathbb{R},+)$ sur $(\mathbb{R}_+^*,\times)$.

- **Transport de structure**

  Soit $f : (E,*) \to (F,\square)$ un morphisme de magmas.

  - L'image $f(E)$ de E par f est une partie stable de $(F,\square)$.
  - Si $*$ est commutative, alors $\square$ est commutative *dans le magma* $(f(E),\square)$.
  - Si $*$ est associative, alors $\square$ est associative *dans le magma* $(f(E),\square)$.
  - Si e est l'élément neutre de $(E,*)$, alors $f(e)$ est l'élément neutre de $(f(E),\square)$.
  - Si x est symétrisable dans $(E,*)$, de symétrique x', alors $f(x)$ est symétrisable dans $(f(E),\square)$, de symétrique $f(x')$, et on a alors, pour tout $n \in \mathbb{Z}$, $f\left(x^{(n)}\right) = \big(f(x)\big)^{(n)}$.

[S1.3] Groupes

- On appelle groupe un *magma* $(G,*)$ tel que :

  (i) $*$ est associative ;

  (ii) $*$ possède un élément neutre *(généralement noté e_G)* ;

  (iii) tout élément de G est symétrisable pour la loi $*$.

  Le groupe est dit abélien (ou commutatif) si, de plus, la loi $*$ est commutative.

  Exemple : soit E un ensemble non vide. Alors l'ensemble $\mathfrak{S}(E)$ des *permutations* de E (c'est-à-dire l'ensemble des bijections de E dans E) est un groupe pour la loi $\circ$; ce groupe n'est pas commutatif dès que $\mathrm{Card}(E) \geqslant 3$.

- **Produit de groupes**

  Soient $(G,*_{_G})$ et $(H,*_{_H})$ deux groupes. On peut alors munir l'ensemble produit $G \times H$ de la loi $\square$ définie par :

  $$\forall\,(x_1,y_1),(x_2,y_2) \in (G\times H)^2,\ (x_1,y_1)\square(x_2,y_2) \ = \ (x_1 *_{_G} x_2, y_1 *_{_H} y_2)\,.$$

  Alors $(G\times H,\square)$ est un groupe, appelé groupe produit de G et H ; son élément neutre est $(e_{_G},e_{_H})$.

On peut bien sûr étendre cette définition à un produit d'un nombre fini quelconque de groupes.

[S1.4] Sous-groupe

- Soit $(G,*)$ un groupe. On dit qu'une *partie* H de G est un sous-groupe de G si $(H,*)$ est encore un groupe.
  Si H est un sous-groupe de G, alors :
  - l'élément neutre de H est celui de G ;
  - si x est un élément de H, son symétrique dans H est le même que dans G.
- **Caractérisation d'un sous-groupe**
  Soit $(G,*)$ un groupe. Pour qu'une *partie* H de G soit un sous-groupe de G, il faut et il suffit que les trois conditions suivantes soient vérifiées :
  (i) $H \neq \emptyset$;
  (ii) H est stable par la loi $*$;
  (iii) pour tout élément x de H, son symétrique x^{-1} est dans H.
  Ces trois conditions sont aussi équivalentes aux deux conditions suivantes :
  (i) $H \neq \emptyset$;
  (ii) $\forall\,(x,y) \in H^2,\ x * y^{-1} \in H$.
  Lorsque la loi est notée additivement, cette dernière condition s'écrit : $\forall\,(x,y) \in H^2,\ x - y \in H$.
  Exemples
  - $(\{-1,1\},\times)$ est un sous-groupe de $(\mathbb{R}^*,\times)$.
  - L'ensemble $\mathbb{U}$ des nombres complexes de module égal à 1 est un sous-groupe de $(\mathbb{C}^*,\times)$ (il s'agit du *cercle unité*).
  - Si n est un entier non nul, l'ensemble $\mathbb{U}_n$ des racines n-ièmes de l'unité est un sous-groupe de $(\mathbb{U},\times)$.
- **Théorème de Lagrange**
  Si G est un groupe fini, le cardinal de tout sous-groupe de G est un diviseur de $\operatorname{Card} G$.
- **Intersection de sous-groupes**
  Soit $(G,*)$ un groupe. L'intersection d'une famille $(H_i)_{i\in I}$ de sous-groupes de G est encore un sous-groupe de G.

  ✓ La *réunion* de sous-groupes de G n'est pas en général un sous-groupe de G. Plus précisément, si H et H' sont deux sous-groupes de G, $H \cup H'$ est encore un sous-groupe de G si et seulement si $H \subset H'$ ou $H' \subset H$.
- **Sous-groupe engendré**
  - Soit $(G,*)$ un groupe, et X une partie de G. L'intersection de tous les sous-groupes de G contenant X est un sous-groupe de G ; c'est le plus petit sous-groupe de G contenant X (au sens de l'inclusion) ; on l'appelle sous-groupe engendré par X, et on le note $\operatorname{gr}(X)$.

. Si $X = \emptyset$, $\mathrm{gr}(\emptyset) = \{e_{_G}\}$. Sinon, $\mathrm{gr}(X)$ est exactement l'ensemble des éléments de la forme :

$$x_1 * x_2 * \cdots * x_n$$

où $n \in \mathbb{N}^*$ et où pour tout $i \in [\![1\,;n]\!]$, $x_i \in X$ ou $x_i^{-1} \in X$.

[S1.5] Morphismes de groupes

- Un morphisme de groupes est (tout simplement) un morphisme entre deux groupes $(G,*)$ et $(H,\square)$.
  On définit de la même façon qu'auparavant les notions d'iso-, d'endo- et d'automorphisme de groupes.
- **Propriétés**
  - Soit f un morphisme d'un groupe G vers un groupe H. Alors :
    - $f(e_{_G}) = e_{_H}$;
    - $\forall\, x \in G,\ \forall\, n \in \mathbb{Z},\ f\left(x^{(n)}\right) = (f(x))^{(n)}$.
  - La composée de deux morphismes de groupes est un morphisme de groupes.
  - Si f est un isomorphisme de groupes, il en est de même de f^{-1}.
  - Si G est un groupe, l'ensemble $\mathrm{Aut}(G)$ des automorphismes de G est un groupe pour la loi $\circ$; c'est un sous-groupe du groupe des permutations $\big(\mathfrak{S}(G),\circ\big)$.
- **Images directe et réciproque d'un sous-groupe**
  - Soit f un morphisme d'un groupe $(G,*)$ vers un groupe $(H,\square)$.
    Si G' est un sous-groupe de $(G,*)$, son image $f(G')$ est un sous-groupe de $(H,\square)$.
  - Si H' est un sous-groupe de $(H,\square)$, son image réciproque par f, $f^{-1}(H')$, est un sous-groupe de $(G,*)$.
- Si f est un morphisme d'un groupe $(G,*)$ vers un groupe $(H,\square)$, on appelle :
  - image de f, notée $\mathrm{Im}\, f$, l'image de G par f, soit : $\mathrm{Im}\, f = \{f(x)\ ,\ x \in G\}$;
  - noyau de f, noté $\mathrm{Ker}\, f$, l'image réciproque de $\{e_{_H}\}$ par f, soit :

$$\mathrm{Ker}\, f = \{x \in G \mid f(x) = e_{_H}\}\,.$$

  On alors les résultats suivants.
  - $\mathrm{Im}\, f$ est un sous-groupe de H, et : f surjective $\iff \mathrm{Im}\, f = H$.
  - $\mathrm{Ker}\, f$ est un sous-groupe de G, et : f injective $\iff \mathrm{Ker}\, f = \{e_{_G}\}$.
- **Exemples**
  - L'application « déterminant » est un morphisme du magma $(\mathcal{M}_n(\mathbb{K}),\times)$ dans le magma $(\mathbb{R},\times)$.
  - C'est aussi un morphisme du groupe $(\mathrm{GL}_n(\mathbb{K}),\times)$ dans le groupe $(\mathbb{R}^*,\times)$.
  - C'est aussi un morphisme du groupe orthogonal $(\mathcal{O}_n(\mathbb{R}),\times)$ dans $(\{-1,1\},\times)$, sous-groupe de $(\mathbb{R}^*,\times)$.
    Dans ce cas, son noyau est l'ensemble des matrices orthogonales de déterminant $+1$; c'est le groupe spécial orthogonal $\mathcal{O}_n^+(\mathbb{R})$.

[S1.6] Groupes monogènes et cycliques

- **Sous-groupes de** $(\mathbb{Z},+)$

  Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les ensembles $n\mathbb{Z}$ où $n \in \mathbb{N}$ (ensemble des multiples de n).

  $(n\mathbb{Z},+)$ est le sous-groupe de $(\mathbb{Z},+)$ engendré par n ou par $-n$.

- **Le groupe** $(\mathbb{Z}/n\mathbb{Z},+)$

  . **Congruences**

  Soit $n \in \mathbb{N}$. On dit que deux entiers x, $y \in \mathbb{Z}$ sont congrus modulo n, et l'on note $x \equiv y \pmod{n}$, s'il existe $k \in \mathbb{Z}$ tel que $y = x + kn$.

  Cela équivaut à dire que $x - y$ appartient à $n\mathbb{Z}$, ou que (lorsque $n \geqslant 1$), x et y ont le même reste dans la division euclidienne par n.

  Il s'agit d'une relation d'équivalence sur $\mathbb{Z}$, compatible avec l'addition et la multiplication, c'est-à-dire que pour tous entiers x, y, x', y' :

  $$x \equiv y \pmod{n} \text{ et } x' \equiv y' \pmod{n} \\ \Longrightarrow x + x' \equiv y + y' \pmod{n} \text{ et } xx' \equiv yy' \pmod{n}.$$

  En particulier, pour tout $(x,y) \in \mathbb{Z}^2$ et tout entier naturel $k \in \mathbb{N}$:

  $$x \equiv y \pmod{n} \Longrightarrow x^k \equiv y^k \pmod{n}.$$

  . La classe d'équivalence de x modulo n est l'ensemble des $y \in \mathbb{Z}$ congrus à x :

  $$\overline{x} = \{y \in \mathbb{Z} \mid x \equiv y \pmod{n}\} = \{x\} + n\mathbb{Z}.$$

  L'ensemble de toutes les classes d'équivalence modulo n se note $\mathbb{Z}/n\mathbb{Z}$.
  Si $n = 0$, $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$; si $n = 1$, $\mathbb{Z}/\mathbb{Z} = \{\overline{0}\}$; sinon, pour $n \geqslant 2$ (ce que l'on supposera pour la suite),

  $$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ \ldots, \overline{n-1}\}.$$

  . **Addition dans** $\mathbb{Z}/n\mathbb{Z}$

  Elle est définie par :

  $$\forall\, (\overline{x},\overline{y}) \in (\mathbb{Z}/n\mathbb{Z})^2,\ \overline{x} + \overline{y} = \overline{x+y}.$$

  Muni de cette loi, l'ensemble $(\mathbb{Z}/n\mathbb{Z},+)$ est un groupe abélien ; l'application $\pi : \begin{cases} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & \overline{x} \end{cases}$ est alors un morphisme de groupes surjectif, dont le noyau est $n\mathbb{Z}$. π s'appelle la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

- **Groupe monogène, cyclique**

  . Un groupe $(G,*)$ est dit monogène s'il est engendré par un unique élément $a \in G$. Dans ce cas, en notant la loi multiplicativement :

  $$G = \{a^k,\ k \in \mathbb{Z}\}.$$

  Un groupe est dit cyclique s'il est monogène et de cardinal fini.

- Tout groupe monogène de cardinal infini est isomorphe à $(\mathbb{Z},+)$.
- Si G est un groupe cyclique engendré par a et de cardinal $n \in \mathbb{N}^*$, G est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z},+)$. De plus, on a alors : $a^n = e_G$.

- **Générateurs d'un groupe cyclique**

  Soit $n \geqslant 2$. Les générateurs du groupe $(\mathbb{Z}/n\mathbb{Z},+)$ sont les éléments $\overline{k}$ où k est premier avec n.

  Le nombre de ces générateurs, c'est-à-dire le nombre d'entiers de $[\![0\,;n-1]\!]$ premiers avec n se note $\varphi(n)$; φ s'appelle l'indicateur d'Euler.

  Par isomorphisme, il en résulte que si $(G,*)$ est un groupe cyclique engendré par a et de cardinal n, les générateurs de G sont exactement les éléments a^k où $k \in \mathbb{Z}$ est un entier premier avec n.

  Exemple : l'ensemble $\mathbb{U}_n$ des racines n^{es} de l'unité est un sous-groupe cyclique de $(\mathbb{C}^*,\times)$.

  Ses générateurs sont les nombres complexes de la forme $\mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}}$ avec $k \in [\![0\,;n-1]\!]$ premier avec n. Ces nombres sont appelés les racines primitives n^{es} de l'unité.

[S1.7] Ordre d'un élément dans un groupe

- Un élément a d'un groupe $(G,*)$ est dit d'ordre fini si le groupe engendré par a,

$$\mathrm{gr}(a) = \left\{a^k,\, k \in \mathbb{Z}\right\},$$

  est de cardinal fini d. d s'appelle alors l'ordre de a.

  Si a est d'ordre fini, l'ordre de a est le plus petit entier $n \in \mathbb{N}^*$ tel que $a^n = e_G$; plus précisément, si d est l'ordre de a :

$$a^n = e_G \iff n \text{ multiple de } d\,.$$

- D'après le théorème de Lagrange, si $(G,*)$ est un groupe fini de cardinal n, tout élément $a \in G$ est d'ordre fini et son ordre d divise le cardinal de G $(d \,|\, n)$.

  En particulier, pour tout $a \in G$, on a $a^n = e_G$.

- En regroupant alors les éléments du groupe $(\mathbb{Z}/n\mathbb{Z},+)$ selon leur ordre, on obtient la propriété suivante de l'indicateur d'Euler φ :

$$n = \sum_{d \text{ divise } n} \varphi(d)\,.$$

[S1.8] Le groupe symétrique $\mathfrak{S}_n$

- Soit $n \in \mathbb{N}^*$. On appelle groupe symétrique d'ordre n, noté $\mathfrak{S}_n$, l'ensemble des permutations de l'ensemble $[\![1\,;n]\!]$.

  $\mathfrak{S}_n$ est un groupe pour la loi $\circ$ de composition des applications. C'est un groupe fini de cardinal $n!$, non commutatif dès que $n \geqslant 3$.