Résumé de Math Sup : structures

I. Lois de composition interne (ou opérations).

1) Définition. Soit E un ensemble non vide. Une **loi de composition interne** sur E (ou encore une opération dans E) est une application de $E \times E$ dans E.

2) Propriétés éventuelles des lois de composition interne. Soient E un ensemble non vide et $*$ une loi de composition interne sur E. $*$ peut avoir ou non une ou plusieurs des propriétés suivantes :

a) Commutativité. $*$ est commutative $\Leftrightarrow \forall (x,y) \in E^2,\ x * y = y * x$.

b) Associativité. $*$ est associative $\Leftrightarrow \forall (x,y,z) \in E^3,\ (x * y) * z = x * (y * z)$.
Si $*$ est associative, les expressions $(x * y) * z$ et $x * (y * z)$ peuvent se noter tout simplement $x * y * z$.

c) Distributivité d'une loi sur une autre. Soient E un ensemble non vide et $*$ et T deux lois de composition internes sur E.
T est distributive sur $* \Leftrightarrow \forall (x,y,z) \in E^3,\ x\ T\ (y * z) = (x\ T\ y) * (x\ T\ z)$ et $(y * z)\ T\ x = (y\ T\ x) * (z\ T\ x)$.
Si on sait que T est commutative, une et une seule des deux égalités ci-dessus suffit.

3) Eléments particuliers.
Soient E un ensemble non vide et $*$ une loi interne sur E.

a) Elément neutre. Soit $e \in E$. e est élément neutre pour $* \Leftrightarrow \forall x \in E,\ e * x = x * e = x$.
$*$ admet un élément neutre dans $E \Leftrightarrow \exists e \in E / \forall x \in E,\ x * e = e * x = x$.
Si on sait que la loi $*$ est commutative, une et une seule des deux égalités ci-dessus suffit.

Théorème. Si $*$ admet un élément neutre, celui-ci est unique.

b) Elément absorbant. Soit $a \in E$.a est élément absorbant pour $* \Leftrightarrow \forall x \in E,\ a * x = x * a = a$.

c) Elément symétrique d'un élément. Soit $x \in E$. x admet un symétrique pour $* \Leftrightarrow \exists x' \in E / x * x' = x' * x = e$.

Si on sait que la loi $*$ est commutative, une et une seule des deux égalités ci-dessus suffit.

Théorème. Soit x un élément de E. Si $*$ est associative (et admet un élément neutre) et si x admet un symétrique pour $*$, celui-ci est unique.

d) Elément simplifiable. Soit $x \in E$. x est simplifiable à gauche pour $* \Leftrightarrow \forall (y,z) \in E^2,\ x * y = x * z \Rightarrow y = z$.
De même, x est simplifiable à droite pour $* \Leftrightarrow \forall (y,z) \in E^2,\ y * x = z * x \Rightarrow y = z$. Enfin, x est simplifiable si et seulement si x est simplifiable à gauche et à droite.

Théorème. Si $*$ est associative, tout élément symétrisable est simplifiable.

II. Groupes.

1) Groupes.
Définition. Soit G un ensemble non vide muni d'une loi de composition interne (notée $*$). $(G, *)$ est un **groupe** si et seulement si

1) $*$ est **associative**,
2) $*$ possède un **élément neutre** dans G
3) tout élément de G possède un **symétrique** dans G.

De plus, $(G, *)$ est commutatif (ou abélien) si et seulement si $*$ est commutative.

Théorème. Dans un groupe, tout élément est simplifiable.

2) Groupes connus.
- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$.
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$.
- $(\mathbb{K}^D, +)$ (fonctions de D dans $\mathbb{K}$) et en particulier $(\mathbb{K}^{\mathbb{N}}, +)$.
- $(S(E), \circ)$ et en particulier $(S_n, \circ)$ (groupe symétrique).
- $(\mathbb{K}^n, +)$.
- $(L(E), +)$ et $(M_{n,p}(\mathbb{K}), +)$.
- $(GL(E), \circ)$, $(O(E), \circ)$, $(SL(E), \circ)$ et $(O^+(E), \circ)$.
- $(GL_n(\mathbb{K}), \times)$, $(O_n(\mathbb{R}), \times)$, $(SL_n(\mathbb{K}), \times)$ et $(O_n^+(\mathbb{R}), \times)$.
- $(\mathbb{K}[X], +)$ et $(\mathbb{K}(X), +)$.
- $(\mathbb{K}(X) \setminus \{0\}, \times)$.

3) Sous-groupes.

Soient $(G,*)$ un groupe et H une partie de G. H est un sous-groupe de $(G,*)$ si et seulement si H est **non vide**, **stable** pour $*$ (c'est à dire $\forall (x,y)\in H^2,\ x*y\in H$) et, muni de la loi induite (c'est à dire de la restriction à H^2 de la loi $*$), est un groupe.

$\{e\}$ et G sont des sous-groupes de $(G,*)$ appelés sous-groupes triviaux du groupe $(G,*)$. Les autres sous-groupes, s'il en existe, sont appelés sous-groupes propres de $(G,*)$.

Théorème (en général).

$$H \text{ est un sous-groupe de } (G,*) \Leftrightarrow \left\{\begin{array}{l}(1)\ H\subset G\\ 2)\ e\in H\\ 3)\ \forall (x,y)\in H^2,\ x*y\in H\\ 4)\ \forall x\in H,\ x'\in H\end{array}\right. \text{(I)} \Leftrightarrow \left\{\begin{array}{l}(1)\ H\subset G)\\ 2)\ H\neq\varnothing\\ 3)\ \forall (x,y)\in H^2,\ x*y'\in H\end{array}\right. \text{(II).}$$

Théorème (en notation additive).

$$H \text{ est un sous-groupe de } (G,+) \Leftrightarrow \left\{\begin{array}{l}(1)\ H\subset G\\ 2)\ 0\in H\\ 3)\ \forall (x,y)\in H^2,\ x+y\in H\\ 4)\ \forall x\in H,\ -x\in H\end{array}\right. \text{(I)} \Leftrightarrow \left\{\begin{array}{l}(1)\ H\subset G)\\ 2)\ 0\in H\\ 3)\ \forall (x,y)\in H^2,\ x-y\in H\end{array}\right. \text{(II).}$$

Théorème (en notation multiplicative).

$$H \text{ est un sous-groupe de } (G,\times) \Leftrightarrow \left\{\begin{array}{l}(1)\ H\subset G\\ 2)\ 1\in H\\ 3)\ \forall (x,y)\in H^2,\ x\times y\in H\\ 4)\ \forall x\in H,\ x^{-1}\in H\end{array}\right. \text{(I)} \Leftrightarrow \left\{\begin{array}{l}(1)\ H\subset G)\\ 2)\ 1\in H\\ 3)\ \forall (x,y)\in H^2,\ x\times y^{-1}\in H\end{array}\right. \text{(II).}\ .$$

Théorème (avec la loi $\circ$).

$$H \text{ est un sous-groupe de } (G,\circ) \Leftrightarrow \left\{\begin{array}{l}(1)\ H\subset G\\ 2)\ \mathrm{Id}\in H\\ 3)\ \forall (f,g)\in H^2,\ f\circ g\in H\\ 4)\ \forall f\in H,\ f^{-1}\in H\end{array}\right. \text{(I)} \Leftrightarrow \left\{\begin{array}{l}(1)\ H\subset G)\\ 2)\ \mathrm{Id}\in H\\ 3)\ \forall (f,g)\in H^2,\ f\circ g^{-1}\in H\end{array}\right. \text{(II).}\ .$$

Remarque. L'élément neutre d'un groupe appartient toujours à un sous-groupe. Mais si $(E,*)$ possède un élément neutre e et si $E'\subset E$ est stable pour $*$ et possède un élément neutre e', il est possible que $e'\neq e$. Par exemple, si E est un ensemble quelconque, E est élément neutre pour $\cap$ dans $P(E)$. Soit F une partie stricte de E. $P(F)$ est stable pour $\cap$ et $\cap$ possède un élément neutre dans $P(F)$ à savoir F. Cet élément neutre n'est pas l'élément neutre de $(P(E),\cap)$ qui est E.

Théorème. Si H et K sont des sous-groupes de $(G,*)$, $H\cap K$ est un sous-groupe de $(G,*)$ (une intersection de sous-groupes est un sous-groupe).

III. Anneaux et corps.

1) Anneaux

Soit A un ensemble non vide ayant au moins deux éléments muni de deux lois de composition interne (notées $+$ et $\times$).

$$(A,+,\times) \text{ est un anneau} \Leftrightarrow \left\{\begin{array}{l}1)\ (A,+) \text{ est un groupe commutatif}\\ 2)\ \text{a) } \times \text{ est associative}\\ \quad\ \text{b) } \times \text{ possède un élément neutre dans } A\\ 3)\ \times \text{ est distributive sur } +\end{array}\right.$$

. Si $\times$ est commutative, l'anneau est dit **commutatif**.

Deux exemples fondamentaux d'anneaux commutatifs sont $(\mathbb{Z},+,\times)$ et $(\mathbb{K}[X],+,\times)$. Deux exemples importants d'anneaux non commutatifs sont $(L(E),+,\circ)$ et $(M_n(\mathbb{K}),+,\times)$.

2) Corps

Soit $(\mathbb{K},+,\times)$ un anneau. $(\mathbb{K},+,\times)$ est un corps si et seulement si tout élément non nul de K admet un inverse (pour $\times$) dans K. Si $\times$ est commutative, le corps est dit commutatif.

$(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps commutatifs.