PROGRAMME DE COLLE S17

NB : seules les démonstrations des théorèmes, propositions étoilées ne sont pas exigées.

STRUCTURES ALGÉBRIQUES FONDAMENTALES

■■■ Lois de composition interne

Définition : *Une loi de composition interne $\star : E \times E \to E$ est dite :*

- ***associative*** *si* $\forall (x,y,z) \in E^3,\ x \star (y \star z) = (x \star y) \star z$.
- ***commutative*** *si* $\forall (x,y) \in E^2,\ x \star y = y \star x$.

Un élément de $(E,\star)$ est dit ***élément neutre*** *pour $\star$ si :* $\forall x \in E,\ x \star e = e \star x = x$

Vocabulaire : *Un ensemble E, muni d'une lci $\star$ est appelé un magma.*

Définition : *On suppose que $(E,\star)$ a un élément neutre e et que $\star$ est associative. Un élément $x \in E$ est dit symétrisable s'il existe $x' \in E$, tel que $x \star x' = x' \star x = e$. x' est alors appelé le* ***symétrique*** *de x.*

Savoir-faire : une l.c.i. est généralement notée $+$, $\times$, ou $\star$. Vous devez savoir adapter suivant les cas ($+$, $\times$, $\star$) les notions de symétrique, d'élément neutre, et d'itéré d'un élément.

Proposition.— Soit $(E,\star)$ un magma. Si E possède un élément neutre, il est unique.

Proposition.— Soit $(E,\star)$ un magma associatif. Le symétrique d'un élément x, s'il existe, est unique.

Définition : Itérés d'un élément —. *Soit $(E,\star)$ un magma associatif unitaire. Soit $x \in E$. On définit la suite des itérés de x par $x^{\star 0} = e$, et pour tout entier naturel $n \in \mathbf{N}$, $x^{\star(n+1)} = x \star x^{\star n}$.*

■■■ Groupes

Définition : *Soit G un ensemble muni d'une loi de composition interne $\times$.*

On dit que $(G,\times)$ est un ***groupe*** *si*

- (G_1) *la loi $\times$ est associative*
- (G_2) *la loi $\times$ possède un élément neutre*
- (G_3) *tout élément possède un symétrique.*

Si de plus la loi $\star$ est commutative, on dit que G est groupe ***abélien****, ou* ***commutatif****.*

Théorème*.— Règles de calcul dans un groupe —. Soit $(G,\times)$ un groupe, $(x,y) \in G^2$. Pour tout couple $(n,m) \in \mathbf{Z}^2$ d'entiers relatifs, on a :

- $\forall (x,y) \in G^2, (x \times y)^{-1} = y^{-1} \times x^{-1}$
- $\forall x \in G, \left(x^{-1}\right)^{-1} = x$.
- $x^n \times x^m = x^{n+m}$
- $\left(x^n\right)^m = x^{n \times m}$.

Proposition.— Équations dans un groupe —. Soit $(G,.)$ un groupe, $(a,b) \in G^2$.

- L'équation $a \times x = b$ possède une unique solution dans G : $x = a^{-1} \times b$.
- L'équation $x \times a = b$ possède une unique solution dans G : $x = b \times a^{-1}$.

■■■ Sous-groupes

Définition : *Soit $(G,\times)$ un groupe et $H \subset G$ une partie de G. H est un* ***sous-groupe de*** *G ($H < G$) si :*

- *H est stable par pour la loi de G :* $\forall (x,y) \in H \times H,\ x \times y \in H$.
- *$(H,\times)$ est un groupe.*

Théorème*.— Caractérisation des sous-groupes— Soit $(G,\times)$ un groupe et H un sous-ensemble de G. Alors

H est un sous groupe de G si et seulement si

- (SG_1) $H \neq \emptyset$
- (SG_2) $\forall (x,y) \in H \times H,\ x \times y^{-1} \in H$

Définition : *Soit $(G,\times)$ et $(G',\star)$ deux groupes. $f : G \to G'$ est appelée un* ***morphisme de groupe*** *si :*

$$\forall (x,y) \in G \times G, \quad f(x \times y) = f(x) \star f(y).$$

■■■ Étude du groupe symétrique

Proposition.— Soit $n \in \mathbf{N}^\star$, $(\mathfrak{S}_n, \circ)$ est un groupe pour la composition des applications, appelé **groupe symétrique**. L'élément neutre est l'application identité.

Définition : *Soit $(n,p) \in \mathbf{N}^2$ tel que $2 \leq p \leq n$. Soit $S = \{a_1, \ldots, a_p\}$ une partie de $[\![1,n]\!]$ à p éléments. On définit la permutation $c \in \mathfrak{S}_n$ par $c(a_1) = a_2, c(a_2) = a_3, \ldots, c(a_p) = a_1$, et pour tout $k \notin S$, $c(k) = k$. c est appelé un **cycle de longueur** p, et $S = \{a_1, \ldots, a_p\}$ est le **support** de c.*

Théorème*.— Décomposition d'une permutation en produit de cycles —. Soit $n \in \mathbf{N}^\star$. Toute permutation $\sigma \in \mathfrak{S}_n$ est décomposable en produit de cycles à supports deux à deux disjoints. Cette décomposition est unique à l'ordre des cycles près.

Théorème.— Décomposition d'une permutation en produit de transpositions — . Soit $n \in \mathbf{N}^\star$.

- $c = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_{p-1} & a_p \end{pmatrix}$
- toute permutation σ de $\mathfrak{S}_n$ est décomposable en un produit d'au plus $n-1$ transpositions.

Savoir-faire : décomposer une permutation de $\mathfrak{S}_n$ en produit de transpositions.

Définition : *Soit $\sigma \in \mathfrak{S}_n$ une permutation. On note $I(\sigma)$ le **nombre d'inversions** de σ, i.e. le nombre de couples $(i,j) \in [\![1,n]\!]^2$ tels que $i < j$ et $\sigma(i) > \sigma(j)$.*

Définition : *Soit $n \in \mathbf{N}^\star$, $\sigma \in \mathfrak{S}_n$. On appelle **signature** de σ le nombre réel $\varepsilon(\sigma) = (-1)^{I(\sigma)}$. σ est dite **paire** (resp. impaire) si $\varepsilon(\sigma) = 1$ (resp. $\varepsilon(\sigma) = -1$).*

Théorème*.— L'application $\varepsilon : \big(\mathfrak{S}_n, \circ\big) \to \big(\{\pm 1\}, \times\big)$ est un morphisme de groupes. Autrement dit,

$$\boxed{\forall (\sigma, \rho) \in \mathfrak{S}_n^2, \quad \varepsilon\big(\sigma \circ \rho\big) = \varepsilon\big(\sigma\big) \times \varepsilon\big(\rho\big)}$$

Proposition*.— Soit $n \in \mathbf{N}^\star$, et $c = \begin{pmatrix} a_1 & a_2 & \cdots & a_p \end{pmatrix}$ un p-cycle de $\mathfrak{S}_n$. Alors $\varepsilon(c) = (-1)^{p-1}$.
En particulier, les transpositions ont pour signature -1.

■■■ Anneaux et corps

Définition : *Soit A un ensemble muni de deux l.c.i., notées $+$ et $\times$. $(A, +, \times)$ **est un anneau** si :*

(A_1) *$(A,+)$ est un **groupe commutatif**. L'élément neutre de $+$ est noté 0_A.*

(A_2) *la loi $\times$ est **associative**.*

(A_3) *la loi $\times$ est **distributive par rapport à la loi** $+$,* $\begin{array}{l} \forall (x,y,z) \in A^3,\ x \times (y+z) = x \times y + x \times z \\ \forall (x,y,z) \in A^3,\ (x+y) \times z = x \times z + y \times z \end{array}$.

(A_4) *la loi $\times$ possède un **élément neutre**, noté 1_A*

*Si de plus la loi $\times$ est commutative, on dit que $(A, +, \times)$ est un **anneau commutatif**.*

Définition : *Soit $(A, +, \times)$ un anneau.On appelle sous-anneau de A toute partie B de A, stable par $+$ et $\times$, contenant 1_A et telle que $(B, +, \times)$ est un anneau.*

Théorème*.— Identité géométrique et formule du binôme —. Soit $(A, +, \times)$ un anneau, a et b deux éléments de A qui commutent, c'est-à-dire $a \times b = b \times a$, alors pour tout entier $n \in \mathbf{N}$:

- $a^{n+1} - b^{n+1} = (a-b) \times \displaystyle\sum_{k=0}^{n} a^{n-k} \times b^k$
- $(a+b)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Définition : *Soit $\mathbf{K}$ un ensemble muni de deux lois de composition interne $+$ et $\times$. $(\mathbf{K}, +, \times)$ est un **corps** si*

- *$(\mathbf{K}, +, \times)$ est un anneau commutatif non réduit à $\{0\}$,*
- *$\mathbf{K}^\times = \mathbf{K} \setminus \{0\}$, c'est-à-dire que tout élément non nul est inversible.*

Exemple : Munis de leurs opérations usuelles, $\mathbf{Q}, \mathbf{R}$ et $\mathbf{C}$ sont des corps