Chapitre 9 : « Les groupes »

I. Structure de groupe

1) Définition : loi de composition interne

On appelle **loi de composition interne** d'un ensemble E toute application * :

$E\times E \to E$, $(x,y) \to *(x,y)$

On privilégie la notation : x*y

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

-associative : $\forall(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}) \in \boldsymbol{E}^3, \boldsymbol{a} * (\boldsymbol{b} * \boldsymbol{c}) = (\boldsymbol{a} * \boldsymbol{b}) * \boldsymbol{c}$

-commutative: $\forall(\boldsymbol{a},\boldsymbol{b}) \in \boldsymbol{E}^2$, **a*b = b*a**

Remarque: le couple (E,*) avec * loi de composition interne s'appelle **un magma**.

2) Eléments remarquables :

Un élément e de (E,*) est dit neutre si $\forall a \in E$, a*e = e*a=a

Si (E,*) possède un élément neutre et si * est associative, on appelle symétrique d'un élément x de E pour *, l'élément x' de E tel que x*x' = x'*x = e

Remarques :

Si e est élément neutre de (E,*) alors il est unique

S'il existe, le symétrique d'un élément de (E,*) est unique aussi.

Itération : Pour (E,*) avec * loi de composition interne associative, alors on peut définir $x_1*x_2*\ldots*x_n$ sans parenthèses, et en particulier $x^{*n} = x*x*\ldots*x$ (n fois)

3) Quelques notations :

Pour une loi « quelconque », on privilégie a*b, le neutre : e, le symétrique de x est x', $x*x\ldots*x = x^{*n}$

Pour une loi notée « + » (souvent pour des lois commutatives), on note a+b, le neutre : 0, le symétrique de x est -x, et x+x…+x = nx

Pour une loi notée « × », on note a×b, le neutre 1, le symétrique de x est $x^{-1,}$

4) Groupe

Définition : Soit G un ensemble muni d'une loi ce composition interne *

On dit que (G,*) est **un groupe** si :

-la loi* est associative

-la loi * possède un élément neutre, on dit que * est unifère

-tout élément de G possède un symétrique pour *

Exemple : $(\mathbb{Z},+)$ est un groupe, $(\mathbb{R}^*,\times)$ est un groupe

5) Groupe abélien

Si de plus, la loi * est commutative, c'est-à-dire $\forall(a,b) \in G, a * b = b * a$, alors G est **dit commutatif ou abélien**.

6) Etude de deux exemples :

a) Démontrer que $(\mathbb{C},+)$ est un groupe abélien

b) Est-ce que $(\mathbb{N},+)$ est un groupe ?

La loi + sur $\mathbb{C}$ est clairement une loi associative, avec un élément neutre : 0, pour tout z de $\mathbb{C}$, -z est dans $\mathbb{C}$ et z+(-z) = 0

2 est un entier naturel dont le symétrique -2 n'est pas un entier naturel !

II. Sous-groupe

1) Définition :

Une partie H d'un groupe (G,*) est **un sous-groupe** de G lorsqu'elle vérifie les propriétés suivantes :
-H n'est pas vide
-H est stable par *, c'est-à-dire : $\forall(x,y) \in H^2, x * y \in H$
-Le symétrique de tout élément de H est un élément de H.

2) Proposition

H est un sous-groupe de (G,*) si et seulement si H contient l'élément neutre e ET $\forall(x,y) \in H^2, x * y^{-1} \in H$

Remarque : On se contente de fusionner les deux derniers points de l'axiomatique…

3) Proposition

Toute intersection de sous-groupes de (G,*) est un sous-groupe.

Démonstration :
Soit H et K deux sous-groupes de (G,)*
D'abord, $e_G \in H \cap K$ donc $H \cap K \neq \emptyset$
Soit (h,k)$\in H \cap K^2$, hk$\in$H car H sous-groupe, et hk$\in$K car K sous-groupe, donc hk$\in H \cap K$
Soit h$\in H \cap K$, comme h$\in$H, $h^{-1} \in$H, de même $h^{-1} \in$K, donc $h^{-1} \in H \cap K$
Finalement ($H \cap K$,) est un sous-groupe de (G,*)*

4) Etude d'un exemple :

Soit G = $\mathbb{R}^* \times \mathbb{R}$, et * la loi de G définie par : (x,y)*(x',y') = (xx',xy'+y)

Montrer que (G,*) est un groupe.

En évaluant (2,1)*(1,3) et (1,3)*(2,1), que peut-on conclure ?

On montre que * est une lci, unifère (de neutre (1,0)), symétrisable, associative

(2,1)*(1,3) = (2,7) et (1,3)*(2,1) = (2,4) donc non commutatif.

III. Morphismes de groupe : noyaux, images

1) Définition :

Soient (G,*) et (G', Δ) deux groupes. On appelle morphisme de groupes de (G,*) dans (G', Δ) une application f de G dans G' vérifiant : $\forall(\boldsymbol{a},\boldsymbol{b}) \in \boldsymbol{G}^2, \boldsymbol{f}(\boldsymbol{a} * \boldsymbol{b}) = \boldsymbol{f}(\boldsymbol{a})\Delta\boldsymbol{f}(\boldsymbol{b})$

Exemple : Soit (G,*) un groupe et a$\in$G
Soit $\varphi: \mathbb{Z} \to G, k \to a^k$ est un morphisme du groupe ($\mathbb{Z}$,+) dans (G,*)

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

Exemple :
La fonction logarithme népérien est un isomorphisme de $(\mathbb{R}^{+*},\times)$ dans $(\mathbb{R},+)$

2) Exercice permettant d'obtenir une propriété importante :
Soit f un morphisme de $(G,*)$ dans (G', Δ),
Montrer que $f(e) = e'$ (e est l'élément neutre de G et e' celui de G')
Montrer que pour tout x de G : $f(x^{-1}) = f(x)^{-1}$

On a $f(e*e) = f(e)$, de plus $f(e*e) = f(e)\,\Delta\, f(e)$, soit $f(e) = f(e)\,\Delta\, f(e)$, or $f(e)\in G'$, donc est symétrisable pour la loi Δ, on compose alors par $f(e)^{-1}$ de chaque côté, et on obtient : $f(e)^{-1}\,\Delta f(e) = f(e)^{-1}\, f(e)\,\Delta\, f(e)$, et $e' = f(e)$

De plus, $\forall x \in G$, $f(xx^{-1}) = f(e) = e'$ et $f(xx^{-1}) = f(x)\Delta f(x^{-1})$ donc $f(x)\Delta f(x^{-1}) = e'$
Soit : $f(x^{-1}) = f(x)^{-1}$

3) Proposition
Soit f un morphisme de $(G,*)$ dans (G', Δ)
   a) Si H est un sous-groupe de G alors f(H) est un sous-groupe de G'
   b) Si H' est un sous-groupe de G', alors $f^{-1}(H') = \{x\in G, f(x) \in H'\}$ est un sous-groupe de G

On a vu que $f(e)\in H$

Soit $h\in H$, $f(h)\in f(H)$, et $f(h)^{-1} = f(h^{-1})\in f(H)$ car $h^{-1}\in H$ (car H est un sous-groupe de G)

Soit $(h,k)\in H^2$, Est-ce $f(h)f(k)\in f(H)$? $f(h)f(k) = f(hk)\in f(H)$

$f^{-1}(H') = \{x\in G, f(x)\in H'\}$, donc $e\in f^{-1}(H')$, car $f(e) = e'$

Soit $h\in f^{-1}(H')$, est ce que $h^{-1}\in f^{-1}(H')$? on a $f(h)\in H''$ donc $f(h)^{-1}\in H''$, $f(h^{-1})\in H''$

Soit $(h,k)\in f^{-1}(H')^2$, est ce que $hk\in f^{-1}(H')$? on $f(h)\in H'$ et $f(k)\in H'$, donc $f(h)f(k)\in H'$, $f(hk)\in H'$

4) Définitions :
Soit f un morphisme de $(G,*)$ dans (G', Δ), on appelle :
-noyau de f, et on note $\ker(f) = \{x\in G, f(x) = e'\} = f^{-1}(\{e'\})$
-image de f, et on note $\mathrm{Im}(f) = \{y\in G';\ \exists x \in G, y = f(x)\} = f(G)$

Exemple :
Justifier que $\exp: \mathbb{C}\to\mathbb{C}^*$ est un morphisme du groupe $(\mathbb{C},+)$ vers $(\mathbb{C}^*,\times)$.
En déterminer image et noyau.

Clairement $\exp(z+z') = \exp(z)\exp(z')$
$\mathrm{Ker}(f) = \{x\in \mathbb{C}, f(x) = 1\} = \{x\in \mathbb{C}, \exp(z) = 1\}=\{2ik\pi, k \in \mathbb{Z}\}$ et $\mathrm{Im}(f) = \mathbb{C}^*$

5) Propositions : Si f un morphisme de $(G,*)$ dans (G', Δ) alors Ker(f) est un sous-groupe de G et Im(f) est un sous-groupe de G'

Montrons que Ker(f) est un sous-groupe de G
Ker(f) = {x∈ G, $f(x) = e_{G'}$}
On a: e∈Ker(f) car f(e) = $e_{G'}$
Soit (h,k) ∈ $(Kerf)^2$, f(h) = $e_{G'}$ et f(k) = $e_{G'}$, f(h)f(k) = $e_{G'}$ d'où f(hk) = $e_{G'}$ et hk∈ (Kerf)
Soit h∈ (Kerf), $f(h^{-1}) = f(h)^{-1} = e_{G'}{}^{-1} = e_{G'}$

Exercice : Montrer que : Im(f) est un sous-groupe de G'

6) Propriété :
On a f surjectif si et seulement si Im f = G'
On a f injectif si et seulement si Ker f = {e}

Démonstration : Montrons que f injectif si et seulement si Ker f = {e}
Si f est injectif, si f(x) = $e_{G'}$ comme $f(e_G) = e_{G'}$ on a $f(e_G)$ = f(x) et x = e_G
Si Ker f = {e}, supposons que f(x) = f(x') alors $f(x)f(x')^{-1} = e_{G'}$, et $f(xx'^{-1}) = e_{G'}$
D'où $xx'^{-1} = e_{G'}$ et x=x'

7) Définition
Deux groupes de (G,*) et (G', Δ) sont dits **isomorphes** s'il existe un isomorphisme de groupes de (G,*) dans (G', Δ).

8) Proposition :
Si f est un isomorphisme de groupes de (G,*) dans (G', Δ), alors sa bijection réciproque f^{-1} est un isomorphisme de (G', Δ) dans (G,*).

Démonstration : Clairement f^{-1} est bijective
Est-ce que : $f^{-1}(h'\Delta k') = f^{-1}(h') * f^{-1}(k')$?
On a $f(f^{-1}(h'\Delta k')) = h'\Delta k'$ et $f(f^{-1}(h') * f^{-1}(k')) = f(f^{-1}(h'))\, \Delta f(f^{-1}(k')) = h'\Delta k'$
D'où : $f^{-1}(h'\Delta k') = f^{-1}(h') * f^{-1}(k')$

9) Exercice « classique »

Soit G un groupe noté multiplicativement. Pour a ∈G, on note τ_a l'application de G vers G définie par $\tau_a(x)=axa^{-1}$
a) Montrer que τ_a est un morphisme du groupe G vers lui-même.
b) Vérifier $\tau a \circ \tau b=\tau_{ab}$ pour tous a et b dans G.
c) Montrer que τa est bijective et exprimer son application réciproque.

a) On a pour (x,x')∈G^2, $\tau_a(xx')=axx'a^{-1} = (axa^{-1})\,(ax'a^{-1})$ ∈G
b) $\tau a \circ \tau b(x) = a(bxb^{-1})a^{-1} = abxb^{-1}a^{-1} = abx(ab)^{-1} = \tau_{ab}(x)$
c) Soit y∈G, on cherche x dans G, tel que $y = axa^{-1}$, d'où $a^{-1}ya = x$, τ_a est surjective
Si $\tau_a(x)= \tau_a(x')$ alors $axa^{-1} = ax'a^{-1}$ et x = x' (en composant par a^{-1} à gauche et a à droite), et τ_a est surjective
Ainsi : τ_a est bijective
De $y = axa^{-1}$, on tire : $x = a^{-1}ya$, soit : $(\tau_a)^{-1} = \tau_{a^{-1}}$