ECOLE NORMALE SUPERIEURE
UNIVERSITÉ HASSAN II DE CASABLANCA

Cours :

Structures, polynômes et fractions rationnelles

Licence : Mathématiques,

Semestre I

Prof. Hicham Yamoul

Chapitre 2

Groupes

2.1 Groupes, premières notions

2.1.1 Définitions et Propriétés

Définition 2.1.1 *Soit G un ensemble non vide muni d'une loi de composition interne : une application $g : G \times G \to G$, pour laquelle on note $\forall x, y \in G, g(x, y) = x.y$ ou $x * y, x \top y$,... ou simplement xy. On dit que $(G, .)$, ou simplement G, est un* ***groupe*** *si :*

(i) la loi . est associative, i.e., $\forall x, y, z \in G, x.(y.z) = (x.y).z$,

(ii) la loi . possède un élément neutre, i.e., $\exists e \in G : \forall x \in G,\ x.e = e.x = x$,

(iii) tout élément x de G possède un symétrique x', i.e., $\forall x \in G, \exists x' \in G : x.x' = x'.x = e$. On désigne ce symétrique par x^{-1} et on l'appelle inverse de x.

Si de plus la loi . est commutative, i.e., $\forall x, y \in G x.y = y.x$, on dit que le groupe G est ***commutatif*** *ou* ***abélien****. On note souvent dans ce cas la loi $+$, le neutre 0, le symétrique $-x$ et on l'appelle opposé de x.*

Exemple 2.1.1 *1) $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ sont des groupes abéliens.*

2) $(\mathbb{R}^*, .)$, $(\mathbb{Q}^*, .)$, ainsi que $(\mathbb{R}_+^*, .)$, $(\mathbb{Q}_+^*, .)$ sont des groupes abéliens.

3) L'ensemble $\mathcal{B}(E)$ des bijections d'un ensemble E non vide muni de la composition des applications : $f \circ g : E \to E, x \mapsto f \circ g(x) = f(g(x))$ est un groupe d'élément neutre $Id_E : E \to E, x \mapsto x$ appelée identité de E. Ce groupe n'est pas commutatif dès que $Card(E) \geq 3$. En effet, soient x, y, z trois éléments de E deux à deux différents et soient f et g les deux applications définies par : $f(x) = y$, $f(y) = z$, $f(z) = x$, $f(t) = t$ si $t = x$, $t = y$, $t = z$ et $g(x) = x$, $g(y) = z$, $g(z) = y$ et $g(t) = t$ si $t = x$, $t = y$, $t = z$. Alors, f et g sont des bijections et $f \circ g(x) = f(g(x)) = f(x) = y$ et $g \circ f(x) = g(f(x)) = g(y) = z$. Ainsi $f \circ g = g \circ f$.

Proposition 2.1.1 *Soit G un groupe noté multiplicativement. Alors,*

(i) L'élément neutre de G est unique, aussi le symétrique de tout élément a de G est unique.

(ii) $\forall a \in G, \forall m, n \in Z : a^m a^n = a^{m+n}$.

(iii) tout élément a de G est régulier, plus précisément : $\forall a, b \in G$, *l'équation* $ax = b$ *(resp.* $xa = b$*) possède une unique solution qui est* $x = a^{-1}b$ *(resp.* $x = ba^{-1}$*).*

(iv) Si $(G, *)$ *et* $(G', \top)$ *sont deux groupes,* $G \times G'$ *est muni d'une structure de groupe en posant :* $\forall (a, b), (c, d) \in G \times G' : (a, b) \bullet (c, d) = (a * c, b \top d)$. $G \times G'$ *muni de cette loi est appelé groupe produit (des groupes G et G').*

Preuve : Montrons par exemple la propriété (i) : Si e et e' sont neutres, $e' = ee' = e$. De même, si x' et x'' sont des symétriques de x, alors $x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''$ ■

2.1.2 Sous-groupes

Définition 2.1.2 *Soit* $(G, .)$ *un groupe et H une partie de G. On dit que H est un sous-groupe de G si :*

(i) H est stable, i.e., $\forall x, y \in H,\ x.y \in H$, *autrement dit la restriction de la loi . à H est une loi de composition interne.*

(ii) $(H, .)$ *est un groupe.*

Proposition 2.1.2 *Soit G un groupe et H une partie de G. Alors, on a l'équivalence des trois propositions suivantes :*

(i) H est un sous-groupe de G.

(ii) $H \neq \varnothing, \forall x, y \in H,\ x.y \in H$ *et* $\forall x \in H,\ x^{-1} \in H$.

(iii) $H \neq \varnothing$, *et* $\forall x, y \in H,\ x.y^{-1} \in H$

Preuve :

Par définition (i) entraine (ii) et (ii) implique aussi (iii) car $\forall x, y \in H$, on a $y^{-1} \in H$ et $xy^{-1} \in H$.

Montrons que (iii) entraine (i) : considérons $x \in H$ $(H = \varnothing)$, alors $e = xx^{-1} \in H$. De même, $\forall x \in H : x^{-1} = ex^{-1} \in H$ et on a $\forall x, y \in H : xy = x((y)^{-1})^{-1} \in H$. L'associativité de . dans H découle de l'associativité de . dans G ■

Exemple 2.1.2 *1)* $(\mathbb{Z}, +)$ *est un sous-groupe de* $(\mathbb{Q}, +)$ *et* $(\mathbb{Q}, +)$ *est un sous-groupe de* $(\mathbb{R}, +)$.

2) $(\{-1, 1\}, .)$ *est un sous-groupe de* $(\mathbb{Q}^*, .)$ *qui lui même est un sous-groupe de* $(\mathbb{R}^*, .)$.

3) Si G est un groupe, alors $\{e\}$ *et G sont des sous-groupes de G appelés sous-groupes triviaux de G.*

4) Si H et K sont des sous groupes de G, alors $H \cap K$ est un sous-groupe de G. En général si I est un ensemble d'indices et $(H_i)_{i \in I}$ *une famille de sous-groupes de G, alors* $\bigcap_{i \in I} H_i$ *est un sous-groupe de G.*

5) Les sous-groupes de $\mathbb{Z}$ sont tous de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

6) L'ensemble $R(P)$ des rotations du plan P muni de la composition des applications est un sous-groupe de $S(P)$. En effet, si r_θ (resp. $r_{\theta'}$) est une rotation d'angle θ (resp. θ'), alors $r_\theta \circ r_{\theta'} = r_{\theta+\theta'}$ et ainsi $r_\theta \circ r_\theta^{-1} = r_{\theta-\theta'} \in R(P)$...

Remarque 2.1.1 *Si H et K sont deux sous-groupes de G, alors, en général, $H \cup K$ n'est pas un sous-groupe de G. Soient, par exemple, $H = \{(x, y) \in \mathbb{R}^2;\ x = 0\}$ et $K = \{(x, y) \in \mathbb{R}^2;\ y = 0\}$. Il est évident que H et K sont deux sous-groupes du groupe additif $\mathbb{R}^2$. Cependant, $H \cup K$ n'est pas un sous-groupe de $\mathbb{R}^2$ car on a par exemple $(0, 1) + (1, 0) = (1, 1) \notin H \cup K$.*

Exercice 2.1.1 *Soient H et K deux sous-groupes d'un groupe G. Montrer que $H \cup K$ est un sous-groupe de G si, et seulement si, $H \subseteq K$ ou $K \subseteq H$.*

Exercice 2.1.2 *Soient G un groupe noté multiplicativement, H et K deux sous-groupes de G. Montrer que $HK = \{x \in G;\ \exists h \in H,\ \exists k \in K;\ x = hk\}$ est un sous-groupe de G si, et seulement si, $HK = KH$.*

2.1.3 Homomorphismes de groupes

Soient G et G' deux groupes et $f : G \to G$une application de G vers G'.

Définition 2.1.3 *On dit que f est un homomorphisme de groupes, ou morphisme de groupes, si pour tous $x,\ y$ éléments de G : $f(xy) = f(x)f(y)$. Si de plus f est bijective, f est appelé un isomorphisme de groupes. Si $G = G'$, on dit que f est un endomorphisme de G et si en outre f est une bijection, on dit alors que f est un automorphisme de G.*

Exemple 2.1.3 *1) Soient $G,\ G'$ deux groupes et e' l'élément neutre de G'. L'application $f : G \to G',\ x \mapsto e'$ est un homomorphisme de groupes.*

2) Soit G un groupe, $a \in G$. Alors l'application $\tau_a : G \to G,\ x \mapsto axa^{-1}$ est un ***automorphisme*** *de G appelé* ***automorphisme intérieur.*** *On a $\tau_e = Id_G$ et si G est commutatif, $\tau_a = Id_G,\ \forall a \in G$.*

3) Soit G un groupe noté multiplicativement. L'application $\varphi : \mathbb{Z} \to G,\ n \to a^n$ est un homomorphisme de groupes.

4) Soit $f : \mathbb{R} \to R(P),\ \theta \mapsto r_\theta$. f est bien un homomorphisme de groupes puisque $r_\theta \circ r_{\theta'} = r_{\theta+\theta'}$.

Proposition 2.1.3 *Soient $G,\ G'$ deux groupes d'éléments neutres respectifs e et e' et $f : G \to G'$ un homomorphisme de groupes. Alors,*

i) $f(e) = e'$ et $\forall x \in G,\ f(x^{-1}) = (f(x))^{-1}$.

ii) Pour tout sous-groupe H de G, l'ensemble $f(H) = \{f(x) \mid x \in H\}$ est un sous-groupe de G'. En particulier, $Imf = f(G)$ est un sous-groupe de G'.

*iii) Pour tout sous-groupe H de G, $f^{-1}(H') = \{x \in G / f(x) \in H'\}$ est un sous-groupe de G. En particulier, $f^{-1}(\{e'\}) = \{x \in G \mid f(x) = e'\}$ est un sous-groupe de G noté $\ker f$ est appelé **noyau** de f.*

iv) f est injective si ,et seulement si, $\ker f = \{e\}$.

v) Soient G, G', G'' trois groupes, $f : G \to G'$ et $g : G' \to G''$ deux homomorphismes de groupes. Alors $g \circ f$ est un homomorphisme de groupes.

vi) Si f est un isomorphisme alors f^{-1} est aussi un isomorphisme de groupes. De sorte que si on note $Aut(G)$ l'ensemble de tous les automorphismes de G, alors $(Aut(G), \circ)$ est un groupe.

Preuve. En exercice.