1 Groupes quotients

Définition 1

Soient G un groupe et H un sous-groupe de G. On définit sur G la relation suivante :

$$xRy \Longleftrightarrow x^{-1}y\epsilon H.$$

La relation R est appelée relation d'équivalence à gauche modulo H.

Proposition 2

i) La relation R est une relation d'équivalence.

ii) Soit x un élément de G, sa classe d'équivalence pour la relation R est l'ensemble $xH = \{xh, h \in H\}$.

Proof.
i) Pour tout x de G, on a $x^{-1}x = 1_G \in H$, d'où xRx et la relation R est réflexive.

Pour tout x et tout y dans G, on a $(x^{-1}y)^{-1} = y^{-1}x$, d'où si xRy alors yRx et la relation R est symétrique. Si xRy et yRz , alors $x^{-1}y \in H$ et $y^{-1}z \in H$, d'où $x^{-1}yy^{-1}z = x^{-1}z \in H$ et xRz, la relation R est donc transitive.

ii) Si xRy il existe $h \in H$ tel que $x^{-1}y = h$, i.e, $y = xh$. ■

Remarque 3

1. On définit une relation d'équivalence à droite modulo H par:

$$(xRy) \Longleftrightarrow (xy^{-1} \in H)$$

   et la classe à droite de x modulo H est l'ensemble $Hx = \{hx, h \in H\}$.

Lorsque nous aurons à considérer les relations à gauche et à droite modulo H, nous noterons ces deux relations respectivement ${}_HR$ et R_H.

2. Quel que soit h dans H, on a $Hh = H = hH$ et H est la classe à droite et à gauche de l'élément neutre de G modulo H.

3. Si le groupe G est abélien, en notant sa loi additivement, les relations d'équivalences définies ci-dessus s'écrivent $(xRy) \Leftrightarrow ((x - y) \in H)$, et les relations d'équivalences (resp. les classes) à gauche et à droite modulo H coïncident.

Si le groupe G n'est pas abélien, ce n'est plus le cas, en général. On considère dans S_3 le sous-groupe $H = \langle \Gamma \rangle$ avec $\Gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. En remarquant que $S_3 = \{e, \Gamma, \sigma, \sigma^2, \Gamma \circ \sigma, \sigma \circ \Gamma\}$ avec

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, les classes à gauche et à droite modulo H sont respectivement :

$\sigma H = \{\sigma, \sigma \circ \Gamma\}$ $\qquad H\sigma = \{\sigma, \Gamma \circ \sigma\}$

$\sigma^2 H = \{\sigma^2, \sigma^2 \circ \Gamma = \Gamma \circ \sigma\}$ $\qquad H\sigma^2 = \{\sigma^2, \Gamma \circ \sigma^2 = \sigma \circ \Gamma\}$

qui sont deux à deux distinctes puisque $\Gamma \circ \sigma \neq \sigma \circ \Gamma$.

Notation 4

On note $(G/H)_g$ (resp. $(G/H)_d$) l 'ensemble des classes d'équivalence des éléments de G pour la relation à gauche (resp. à droite) modulo H. Ces ensembles sont aussi appelés ensembles quotients à gauche (resp. à droite) modulo H.

Proposition 5

Soient G un groupe et H un sous-groupe de G.

i) Toute classe à gauche xH (resp. à droite Hx) est équipotente à H.

ii) Les ensembles $(G/H)_g$ et $(G/H)_d$ sont équipotents.

Proof.

i) Pour tout élément x de G, l'application $\begin{array}{ccc} H & \longrightarrow & xH \\ h & \longmapsto & xh \end{array}$, est évidemment bijective.

ii) soit $\Phi : \begin{array}{ccc} (G/H)_g & \longrightarrow & (G/H)_d \\ xH & \longmapsto & \Phi(xH) = Hx^{-1} \end{array}$, montrons que Φ est une application. En effet, $xH = yH$ est équivalent à $x^{-1}y \in H$, d'où $x^{-1} \in Hy^{-1}$, et $Hx^{-1} = Hy^{-1}$, c'est-à-dire $\Phi(xH) = \Phi(yH)$.

D'autre part, $Hx^{-1} = Hy^{-1}$ est équivalent à $x^{-1}y \in H$, autrement dit, $xH = yH$. Ceci signifie que $\Phi(xH) = \Phi(yH)$ implique $xH = yH$ et donc que Φ est injective. De plus, pour tout Hx dans $(G/H)_d$, on a $Hx = \Phi(x^{-1}H)$, par conséquent Φ est surjective. Il existe donc une application bijective de $(G/H)_g$ sur $(G/H)_d$, ce qui prouve que ces deux ensembles sont équipotents.

■

Définition 6

Soient G un groupe et H un sous-groupe de G. On appelle indice de H dans G, qu'on note $[G : H]$, le cardinal de l'ensemble $(G/H)_g$ (ou $(G/H)_d$).

Définition 7

Un groupe G est dit fini s'il n'a qu'un nombre fini d'éléments. Dans ce cas, le cardinal de G s'appelle l'ordre du groupe G et est noté $|G|$.

Soient G un groupe et x un élément de G. On appelle ordre de x, qu'on note $O(x)$, le cardinal de $\langle x \rangle$. Si ce cardinal est infini, on dit que x est d'ordre infini.

Theorem 8 *(de Lagrange).*

Si G est un groupe fini, pour tout sous-groupe H de G on a:

$$|G| = |H|[G : H].$$

Proof.

Puisque les xH, $x \in G$, sont les classes d'équivalences pour la relation d'équivalence R, elles forment une partition de G. De plus, chacune de ces classes est équipotente à H. On en déduit que le cardinal de G est égal au cardinal de H, multiplié par le nombre de classes, qui est précisément le cardinal de l'ensemble quotient $(G/H)_g$, i.e,

$$G = \bigcup_{x \in \{x_1, \ldots, x_k\}} xH \text{ où } k = |(G/H)_g|$$

$$\begin{aligned} |G| &= |\bigcup_{i=1}^{k} x_i H| \\ &= \sum_{i=1}^{k} |x_i H| \\ &= \sum_{i=1}^{k} |H| \\ &= |H|[G : H] \end{aligned}$$

D'où la formule $|G| = |H|[G : H]$. ■

Remarque 9

Ce théorème est souvent énoncé de la façon suivante: dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe.

Corollary 10

Pour tout groupe fini, l'ordre de tout élément divise l'ordre du groupe.
Proof.
Pour tout x de G, l'ordre de x est l'ordre du sous-groupe $\langle x \rangle$ de G. On applique alors le théorème de Lagrange avec $H = \langle x \rangle$. ■

Définition 11

Soit E un ensemble muni d'une loi de composition interne (notée multiplicativement) sur lequel est définie une relation d'équivalence R.

i) R est compatible à droite (resp. à gauche) avec la loi si, quelsque soient x, y, a dans E, on a $(xRy) \Longrightarrow (xaRya)$ (resp.$(xRy) \Longrightarrow (axRay)$).

ii) R est compatible avec la loi si elle est compatible à droite et à gauche.

Proposition 12

R est compatible avec la loi de G si, et seulement si:

$$\forall x, \acute{x}, y, \acute{y} \in E, [(xR\acute{x}) \text{ et } (yR\acute{y})] \Longrightarrow [xyR\acute{x}\acute{y}].$$

Proof.
Supposons que R soit compatible avec la loi, alors si xRx' et yRy', on a $xyRx^{'}y$ et $x'yRx'y'$, d'où $xyRx'y'$ par transitivité.

Réciproquement, l'assertion de l'énoncé étant vraie pour tout $x, \acute{x}, y, \acute{y}$, c'est en particulier vraie pour $y = \acute{y}$, d'où si $xR\acute{x}$ alors $xyR\acute{x}y$ et la relation est compatible à droite avec la loi.

De même, en considérant $x = \acute{x}$, on montre qu'elle est compatible à gauche. ■

Proposition 13

Soient G un ensemble muni d'une loi de composition interne, R une relation d'équivalence définie sur G et G/R l'ensemble quotient de G par la relation d'équivalence R. Alors la loi interne de G induit une loi interne sur G/R, $(\overline{x}, \overline{y}) \to \overline{xy}$ (où pour $z \in G$, $\overline{z}$ désigne la classe d'équivalence de z) si, et seulement si, R est compatible avec la loi de G.
Proof.
La correspondance $(\overline{x}, \overline{y}) \to \overline{xy}$ définit une loi interne sur G/R si, et seulement si, elle définit une application $G/R \times G/R \to G/R$, autrement dit, si, et seulement si, $(\overline{x} = \overline{x_1}, \overline{y} = \overline{y_1}) \Rightarrow (\overline{xy} = \overline{x_1 y_1})$. ■

Remarque 14

Si la relation R est compatible avec la loi de G, la loi induite sur G/R par celle de G est définie par $\overline{x}\overline{y} = \overline{xy}$.

Il est clair que si la loi de G est associative (resp. commutative, resp. admet un élément neutree, resp. tout élément x admet un élément symétrique x^{-1}), il en est de même pour la loi induite sur G/R, $\overline{e}$ est l'élément neutre, l'élément symétrique de $\overline{x}$ est $\overline{x^{-1}}$.

Proposition 15

Soient G un groupe et R une relation d'équivalence définie sur G, compatible avec la loi de G. Alors l'ensemble quotient G/R, muni de la loi induite par la loi de G (définie par $(\overline{x}, \overline{y}) \to \overline{xy}$), est un groupe.

Proposition 16

Pour tout sous groupe H d'un groupe G, la relation R_H (resp.$_HR$) est compatible à droite (resp. à gauche) avec la loi de composition de G .

Réciproquement, si une relation R définie sur un groupe G est compatible à droite (resp. à gauche) avec la loi de composition du groupe G, alors il existe un unique sous-groupe H de G tel que $R = R_H$ (resp. $R =_H R$).

Proof.

Soient x, y, a des éléments de G tels que xR_Hy, i.e, $xy^{-1} \in H$. Alors, $(xa)(ya)^{-1} = xaa^{-1}y^{-1}$ appartient à H, i.e, xaR_Hya.

Une démonstration analogue donne le résultat pour $_HR$.

Soit R une relation d'équivalence définie sur G, compatible à droite avec la loi de G. On note H la classe d'équivalence de l'élément neutre 1_G de G. Montrons que H est un sous groupe de G. Puisque $1_G \in H$, H est non vide. Pour tous x et y dans$H$, on a $xR1_G$ et $yR1_G$.

La compatibilité de R avec la loi de G implique que $xy^{-1}Ry^{-1}$, de plus, puisque $yR1_G$, on a $yy^{-1}Ry^{-1}$, d'où 1_GRy^{-1} et $y^{-1}R1_G$.

On en déduit que $xy^{-1}R1_G$, i.e, $xy^{-1} \in H$, ce qui prouve que H est un sous-groupe de G. Vérifions que $R = R_H$. Si xRy alors, d'après la compatibilité , $xy^{-1}R1_G$, d'où $xy^{-1} \in H$ et xR_Hy. Si xR_Hy, $xy^{-1} \in H$, donc $xy^{-1}R1_G$ et, d'après la compatibilité, xRy. L'unicité de H découle du fait que si $R = R_H$, alors H est la classe d'équivalence de 1_G.

La relation d'équivalence R est donc compatible avec la loi de G si, et seulement si il existe un sous-groupe H de G tel que $R =_H R = R_H$. ■

Définition 17

Un sous-groupe H d'un groupe G est dit normal (ou distingué) dans G si ${}_H R = R_H$. On note alors $H \lhd G$.

Remarque 18

On peut énoncer plusieurs conditions équivalentes pour que H soit un sous-groupe distingué de G

1. $\forall x \in G, xH \subset Hx$.
2. $\forall x \in G, xH = Hx$.
3. $\forall x \in G, xHx^{-1} \subset H$.
4. $\forall x \in G, xHx^{-1} = H$.
5. $\forall h \in H, \forall x \in G, xhx^{-1} \in H$.

Corollary 19

1. Dans un groupe quelconque G, les sous groupes triviaux $\{e\}$ et G sont distingués.
2. Dans un groupe abélien, tout sous groupe est distingué.
3. Le noyau d'un homomorphisme de groupes est un sous groupe distingué : si $f : G \to G'$est un homomorphisme de groupes, alors $ker(f) \lhd G$.

Définition 20

soient G un groupe et H un sous-groupe normal de G. La relation binaire sur G définie par xRy si et seulement si $xy^{-1} \in H$ est une relation d'équivalence sur G compatible avec la loi du groupe est appelée relation de congruence modulo H.

Theorem 21

L'ensemble quotient, noté G/H, mmuni de la loi $\overline{x}, \overline{y} \in G/H, \overline{x} \bullet \overline{y} = \overline{xy}$, est un groupe appelé groupe quotient de G par H et la surjection canonique $\pi : G \longrightarrow G/H, x \longmapsto \overline{x}$ est un homomorphisme de groupe (on écrit dans ce cas, $x \equiv y (\text{mod } H)$ pour désigner que xRy).

Proof.

1) La loi $\bullet$ est bien définie car l'application $\bullet : \begin{array}{ccccc} (G\backslash H) & \times & (G\backslash H) & \longrightarrow & (G\backslash H) \\ (\overline{x} & , & \overline{y}) & \longmapsto & \overline{x} \bullet \overline{y} = \overline{xy} \end{array}$

Constitue ainsi une loi de composition interne sur $G\backslash H$.

2) La loi $\bullet$ est associative car :

$\forall x, y, z \in G : \overline{x} \bullet (\overline{y} \bullet \overline{z}) = \overline{x} \bullet \overline{(yz)} = \overline{x(yz)} = \overline{(xy)z} = \overline{(xy)} \bullet \overline{z} = (\overline{x} \bullet \overline{y}) \bullet \overline{z}$.

3) La loi admet élément neutre $\overline{e}$:

$\forall x \in G : \overline{e} \bullet \overline{x} = \overline{ex} = \overline{xe} = \overline{x} \bullet \overline{e} = \overline{x}$.

4) La loi $\bullet$ admet élément inverse $(\overline{x})^{-1} = \overline{x^{-1}}$:

$$\forall x \in G : \overline{x} \bullet \overline{x^{-1}} = \overline{xx^{-1}} = \overline{e} \text{ et } \overline{x^{-1}} \bullet \overline{x} = \overline{x^{-1}x} = \overline{e}.$$

Enfin, la surjection canonique $\pi : G \longrightarrow G/H, x \longmapsto \overline{x}$ est un morphisme de groupes.

i) $\forall x, y \in G : \pi(x * y) = \overline{xy} = \overline{x} \bullet \overline{y} = \pi(x) \bullet \pi(y)$.

ii) $\pi(e) = \overline{e}$. ■