الجمهورية الجازئرية الديمقطارية الشعبية
République Algérienne Démocratique et Populaire
قرازو التعليمـ العالي اوليحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Réf :……

Centre Universitaire
Abd elhafid boussouf Mila

Institut des sciences et de la technologie **Département de Mathématiques et Informatique**

Mémoire préparé En vue de l'obtention du diplôme de Licence
En: - Filière Mathématiques

Sous-groupes distingués et groupes quotients

Préparé par :SID SAMIA
KHARBACHE MERIEM
LAKHDARI TAREK

Encadrer par : Kecies Mohamed

Année universitaire :2014/2015

Remerciement

Nous avons abouti un travail, qui a été le résultat d'un cheminement de tout un parcours pédagogique, qui a duré tout le long de notre parcours éducatif dans l'enseignement supérieur.

Un remerciement particulier à notre encadreur ***M Kecies*** *pour sa présence, son aide et surtout pour ses précieux conseils qui nous ont assistés pour l'accomplissement de notre projet.*

Nous tenons à exprimer nos sincères remerciements à tout le personnel de l'institut des sciences et de la technologie surtout les enseignants qui nous ont formé durant toutes nos années d'étude.

Un remerciement particulier à nos très chers parents, frères, sœurs, collègues et amies respectives qui nous ont encouragés, soutenu durant tout notre parcours.

MERCI À TOUS

Kharbeche Meriem

Sid Samia

Lakhdari Tarek

Table des matières

Introduction Générale

Nous savons que, pour tout n de $\mathbb{N}$, $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ et la loi interne de $\mathbb{Z}$, c'est-à-dire l'addition, induit une loi interne sur $\mathbb{Z}/n\mathbb{Z}$ qui munit cet ensemble d'une structure de groupe. De plus, la projection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes. L'objectif de ce mémoire est de formaliser cette situation pour un groupe quelconque. Autrement dit, étant donné un groupe G et un sous-groupe H, à quelles conditions peut-on définir un ensemble quotient G/H et une application canonique $\pi : G \to G/H$, de telle sorte que la loi de G induise sur G/H une loi interne le munissant d'une structure de groupe et que π soit un morphisme de groupes ? On va montrer qu'à tout sous-groupe H d'un groupe G est associée une relation d'équivalence $\mathcal{R}$ définie sur G. Si cette relation d'équivalence satisfait certaines conditions de compatibilité, la loi interne de G induit une loi interne sur l'ensemble des classes d'équivalence $G/\mathcal{R}$ qui munit cet ensemble d'une structure de groupe et la projection canonique $\pi : G \to G/\mathcal{R}$ est un morphisme de groupes. On montrera qu'inversement, à toute relation d'équivalence $\mathcal{R}$ définie sur un groupe G et satisfaisant les conditions de compatibilité, est associé un sous-groupe H de G tel que la relation $\mathcal{R}$ soit la relation associée au sous-groupe H. Ceci conduit à la notion de sous-groupes normaux qui sont importants dans l'étude des groupes quotients à cause du résultat suivant : on peut construire un groupe quotient G/H de loi compatible avec celle de G si et seulement si H est un sous-groupe distingué de G. Plus précisément, dans l'étude des groupes, le quotient d'un groupe est une opération classique permettant la construction de nouveaux groupes à partir d'anciens. À partir d'un groupe G, et d'un sous-groupe H, on peut définir une loi de groupe sur l'ensemble G/H des classes de G suivant H, à condition que les classes latérales droites soient égales aux classes latérales gauches ($xH = Hx$).

Ce mémoire est réparti sur l'introduction générale et deux chapitres. Dans le premier chapitre, on va donner les différentes notions de bases qui s'avèrent indispensable pour le reste de ce travail, en particulier les notions de groupes, sous groupes et morphismes de groupes avec leurs propriétés élémentaires.

Dans le deuxième chapitre nous étudierons les relations d'équivalence compatibles à droite et à gauche, puis les sous groupes distingués et leurs propriétés. Nous construirons aussi les groupes quotients par une relation d'équivalence associée à un sous groupe distingué. A la …n de ce chapitre, nous donnerons les di¤érents théorèmes d'isomorphismes (premier, deuxième et troisième théorème).

Chapitre 1

Généralités sur les groupes

Dans ce chapitre nous rappelons quelques généralités sur les groupes, sous groupes et morphismes de groupes qu'on aura besoin par la suite.

1.1 Groupes et morphismes de groupes

1.1.1 Dé...nitions et Propriétés

Dé...nition 1.1.1

1) Soit G un ensemble non vide muni d'une loi de composition interne : une application $g : G \quad G \;!\; G$, pour laquelle on note $8x; y \;2\; G; g(x; y) = x:y$ ou $xTy; x \;?\; y; :::$ ou simplement xy.

2) On dit que $(G; :)$, ou simplement G, est un groupe si et seulement si :

(i) La loi : est associative, i.e., $8x; y; z \;2\; G : x:(y:z) = (x:y):z$

(ii) La loi : possède un élément neutre, i.e., $9e \;2\; G : 8x \;2\; G; x:e = e:x = x$

(iii) Tout élément x de G possède un symétrique x^{0}, i.e., $8x \;2\; G; 9x^{0} \;2\; G : x:x^{0} = x^{0}:x = e$. On désigne ce symétrique par $x^{\ 1}$ et on l'appelle inverse de x.

3) Si de plus la loi : est commutative, i.e., $8x; y \;2\; G : x:y = y:x$, on dit que le groupe G est commutatif ou abélien.

4) On note souvent dans ce cas la loi +, le neutre 0, le symétrique (x) et on l'appelle opposé de x.

Exemple 1.1.2

1) $(R; +); (Q; +); (Z; +); (C; +)$ sont des groupes abéliens.

2) $(R \;; :); (Q \;; :)$, ainsi que $(R_{+}; :)$, $(Q_{+}; :)$ sont des groupes abéliens.

3) L'ensemble S(E) des bijections d'un ensemble E non vide muni de la composition des applications est un groupe d'élément neutre Id_E où Id_E appelée identité de E.

4) $(M_{n;p}(R); +)$ est un groupe abélien.
5) Soit n un entier naturel, $n \in \{0; 1\}$. Alors, l'ensemble $(GL_n(R); :)$ des matrices carrées inversibles d'ordre n à coefficients dans R, muni du produit des matrices, est un groupe non abélien appelé groupe linéaire.
6) $(Z=nZ; +); n \in N$ est un groupe commutatif.

Proposition 1.1.3 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) $\forall a \in G; \forall m; n \in Z : a^m : a^n = a^{m+n}$.
(iv) Si G et G' sont deux groupes, $G \times G'$ est muni d'une structure de groupe en posant :

$$\forall (a; b); (c; d) \in G \times G' : (a; b)(c; d) = (ac; bd)$$

$G \times G'$ 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 $x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''$: ■

1.1.2 Sous-groupes

Définition 1.1.4 Soit $(G; :)$ un groupe et H une partie de G. On dit que H est un sous-groupe de G si et seulement 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 1.1.5 (Caractérisation des sous groupes)
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) $H \neq \emptyset$, $\forall x; y \in H : x:y \in H$ et $\forall x \in H; x^{-1} \in H$
(iii) $H \neq \emptyset$ 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 $x \in H (H \neq \emptyset)$; 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. ■

Remarque 1.1.6 (Notation) Si H est un sous-groupe de G, on notera $H < G$.

Exemple 1.1.7
1) Si G est un groupe, alors $\{e\}$ et G sont des sous-groupes de G appelés sous-groupes triviaux de G.
2) 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.
3) Les sous-groupes de Z sont tous de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.
4) $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$ est un sous-groupe de $GL_n(\mathbb{R})$.
5) L'ensemble $\mathcal{R}(P)$ des rotations du plan P muni de la composition des applications est un sous groupe de $\mathcal{S}(P)$. 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 $r_\theta \circ r_{-\theta}^{-1} = r_\theta \circ r_{-\theta} \in \mathcal{R}(P)$.
6) 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, $H = 2\mathbb{Z}$ et $K = 3\mathbb{Z}$. Il est évident que H et K sont deux sous-groupes du groupe additif Z. Cependant, $H \cup K$ n'est pas un sous-groupe de Z car on a par exemple $2 + 3 = 5 \notin H \cup K$:

Définition 1.1.8 On appelle sous-groupe propre d'un groupe G tout sous groupe distinct de G et de l'élément neutre.

1.1.3 Morphismes de groupes

Définition 1.1.9 Soient G et G' deux groupes et $f : G \to G'$ une application de G vers G'.
1) On dit que f est un 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. On dit alors que G et G' sont isomorphes et on note $G \simeq G'$ (Cette notion est extrêmement importante, car deux groupes isomorphes ont exactement les mêmes propriétés algébriques).
2) 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 1.1.10
1) Soient G, G' deux groupes et e' l'élément neutre de G'. L'application $f : G \to G'; x \mapsto e'$ est un morphisme de groupes.
2) Soit G un groupe, $a \in G$. Alors l'application $f_a : G \to G; x \mapsto axa^{-1}$ est un automorphisme de G appelé automorphisme intérieur. On a $f_e = Id_G$ et si G est commutatif, alors $f_a = Id_G; \forall a \in G$:
3) Soit G un groupe noté multiplicativement. L'application $f : \mathbb{Z} \to G; n \mapsto a^n$ est un

morphisme de groupes.
4) Soit $f : R \to R(P)$; $\to r \circ f$ est bien un morphisme de groupes puisque $r \circ r_0 = r_{+0}$.

Dé...nition 1.1.11 Soient $G; G'$ deux groupes d'éléments neutres respectifs e et e' et $f : G \to G'$ un morphisme de groupes. Alors
1) On appelle noyau de f; et on note $\ker(f)$ l'ensemble dé...ni par

$$\ker(f) = \{x \in G : f(x) = e'\} = f^{-1}(\{e'\})$$

2) On appelle image de f; et on note $\mathrm{Im}(f)$ l'ensemble dé...ni par

$$\mathrm{Im}(f) = \{f(x) \in G'; x \in G\} = f(G)$$

Proposition 1.1.12 Soient $G; G'$ deux groupes d'éléments neutres respectifs e et e' et $f : G \to G'$ un morphisme 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 $f(H) = \{f(x) : x \in H\}$ est un sous-groupe de G'. En particulier, $\mathrm{Im}(f) = f(G)$ 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, $\ker(f) = f^{-1}(\{e'\})$ est un sous-groupe de G.
(iv) f est injective si et seulement si, $\ker(f) = \{e\}$.
(v) Soient $G; G'; G''$ trois groupes, $f : G \to G'; g : G' \to G''$ deux morphismes de groupes. Alors $g \circ f : G \to G''$ est un morphisme 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);) est un groupe.

1.2 Groupes monogènes, Groupes cycliques

Dé...nition 1.2.1 (Proposition)
1) Soit X une partie d'un groupe G. On appelle sous-groupe engendré par X et on note $< X >$ l'intersection de tous les sous-groupes de G contenant X.
2) $< X >$ est le plus petit sous-groupe de G contenant X (pour la relation d'inclusion).
3) Si H est un sous-groupe de G et si $H =< X >$, on dit que H est engendré par X et la partie X est appelée partie génératrice de H.

Remarque 1.2.2 Si H est un sous-groupe de G, on a toujours $H =< H >$, mais les parties génératrices intéressantes sont celles qui ont le moins d'éléments possibles.

Théorème 1.2.3 Soit X une partie non vide d'un groupe G noté multiplicativement. Alors $< X >= \{x = a_1 : a_2 ::: a_n : n \in \mathbb{N}$ et $a_i \in X$ ou $a_i^{-1} \in X$ pour $i \in \{1; 2; :::; n\}\}$. Autrement dit $< X >$ est l'ensemble des composés multiples d'éléments de X et de symétriques d'élément de X. C'est-à dire, si on note $X^{-1} = \{y \in G : y^{-1} \in X\} = \{x^{-1} : x \in X\}$ et $B = A \cup A^{-1}$, alors

$$< X >= \{x \in G; \exists n \in \mathbb{N}; \exists a_1; a_2; :::; a_n \in B : x = a_1 : a_2 ::: a_n\}$$

Preuve. Nous allons montrer que $H =< X >$ est le plus petit sous-groupe de G contenant X et H est un sous groupe de G.
1) i) Pour $a_1 \in X = \ldots$, on a $e = a_1 : a_1^{-1}$, alors l'élément neutre $e \in H$.
ii) Soient $x; y \in H$. Il existe $n; p \in \mathbb{N}; b_1; :::; b_n; c_1; :::; c_p \in B$ tels que $x = b_1 : b_2 ::: b_n \in H$ et $y = c_1 : c_2 ::: c_n$, alors

$$x : y = b_1 : b_2 ::: b_n : c_1 : c_2 ::: c_n = d_1 : d_2 ::: d_n : d_{n+1} ::: d_{n+p} \in H$$

Où

$$d_k = \begin{cases} b_k; \text{ si } 1 \leq k \leq n \\ c_{k-n}; \text{ si } n+1 \leq k \leq n+p \end{cases}$$

iii) Soit $x \in H$. Il existe $n \in \mathbb{N}; b_1; :::; b_n \in B$ tels que $x = b_1 : b_2 ::: b_n$, alors
$b_1^{-1}; b_2^{-1}; :::; b_n^{-1} \in B$ et $x^{-1} = (b_1 : b_2 ::: b_n)^{-1} = b_n^{-1} : b_{n-1}^{-1} ::: b_1^{-1} \in H$

2) On a H est un sous groupe de G et il contient X (car $X \subset H$) ; alors $< X > \subset H$. Inversement, tous les éléments de la forme $a_1 : a_2 ::: a_n$ appartiennent à tout sous groupe contenant X; alors ils appartiennent à $< X >$; d'où l'inclusion $H \subset < X >$ et par suite l'égalité $H =< X >$. ■

Remarque 1.2.4
1) Si la loi de G est notée additivement, on a

$$< X >= \{x = x_1 + ::: + x_n; n \in \mathbb{N}; \quad x_i \in X; \forall i \in \{1; 2; :::; n\}\}$$

2) Si $X = \ldots$, alors $H =< X >= \{e\}$.
3) Cas particulier important : Si $X = \{x\}$ pour $x \in G$, on note alors $< x >$ le sous-groupe engendré par x et il est clair que .

$$H =< x >= \{x^n; n \in \mathbb{Z}\}$$

Dé...nition 1.2.5

1) Un groupe engendré par un seul élément x (C.à.d $X = fxg$) est appelé groupe monogène.

2) Un groupe monogène ...ni, est appelé groupe cyclique.

Exemple 1.2.6

1) Tout sous-groupe de $(Z; +)$ est monogène : $f0g =< 0 >; Z =< 1 >=< \ 1 >$. En e¤et

$$8n \ 2 \ Z : \begin{cases} n = \underbrace{1 + 1 + ::: + 1}_{n \text{ termes}}, \text{ si } n > 0 \\ 0 = 1 + (\ 1) \\ n = \underbrace{(\ 1) + (\ 1) + ::: + (\ 1)}_{n \text{ termes}}, \text{ si } n < 0 \end{cases}$$

2) Si H est un sous-groupe non trivial de Z, n le plus petit entier positif non nul appartenant à H, on a $H =< n >= nZ$.

3) $(Z=nZ = \ 0; 1; :::; n\overset{.}{\square}1 \ ; +)$ où $n \ 2 \ N$ est un groupe cyclique d'ordre n engendré par 1.

$$0 = 0:1; 1 = 1:1; 2 = 1 + 1 = 2:1; :::; n\overset{.}{\square}1 = (n \ \ 1):1$$

Dé...nition 1.2.7

1) Un groupe G est dit ...ni s'il n'a qu'un nombre ...ni d'éléments. Dans ce cas, le cardinal de G s'appelle l'ordre du groupe G et est noté $jGj = ord(G) = o(G)$.

2) Soient G un groupe et x un élément de G. On appelle ordre de x, qu'on note o(x), le cardinal de sous-groupe $< x >$ de G engendré par x. Si ce cardinal est in...ni, on dit que x est d'ordre in...ni.

Remarque 1.2.8

(i) Soient G un groupe ...ni et x un élément de G, alors $o(x) \ \ o(G)$.

(ii) Dans tout groupe G, l'élément neutre est le seul élément d'ordre 1. En e¤et, si $x = e$, alors $< e >= feg$ et si $x = e$, alors $x^0 = e = x^1$ et $< x >$ a au moins deux éléments.

(ii) Pour tout $x \ 2 \ G$; on a $o(x) = o(x^{\ 1})$ puisque

$$< x^{\ 1} >= \ (x^{\ 1})^n : n \ 2 \ Z \ = \ x^{\ n} : n \ 2 \ Z \ =< x >$$

(iii) Tous les éléments d'un groupe ...ni sont d'ordres ...nis. En particulier dans $(Z=nZ; +)$, tout élément est d'ordre ...ni, on a par exemple : $o(1) = o(Z=nZ) = n$:

iiii) Si deux groupes sont isomorphes, ils ont même ordre (La réciproque est fausse)

Exemple 1.2.9 Dans $(\mathbb{Z}; +)$, tous les éléments non nuls sont d'ordre infini. En particulier $o(1) = o(-1) = +\infty$. Par contre $o(0) = 1$.

Proposition 1.2.10 Soit x un élément d'un groupe G. Alors :
(i) x est d'ordre fini dans G si et s'il existe $n \in \mathbb{N}^*$ tel que $x^n = e$. On a alors $o(x) = \min\{n \in \mathbb{N}^* : x^n = e\}$ (C-a-d : o(x) est le plus petit entier positif n tel que $x^n = e$). On écrit

$$< x >= \{e; x; x^2; :::; x^{n-1}\}$$

(ii) Si x est d'ordre fini $s \geq 1$, alors pour $k \in \mathbb{Z}$ on a $x^k = e$ si et si k est multiple de s.

Preuve.
(i) Supposons que x est d'ordre fini. Alors l'application

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & < x > \\ m & \longmapsto & x^m \end{array}$$

n'est pas injective (car l'ensemble $< x >$ est fini. Autrement dit si pour tout i et j dans $\mathbb{Z}$, $i = j$, on a $x^i = x^j$, alors l'ordre de x est infini, ce qui est contraire à l'hypothèse). Donc il existe deux entiers p et q tels que $p < q$ et $x^p = x^q$. On obtient $x^{q-p} = e$ avec $q - p > 0$.
Réciproquement supposons qu' il existe $n \in \mathbb{N}^*$ tel que $x^n = e$. Soit

$$A = \{n \in \mathbb{N}^* : x^n = e\}$$

A étant non vide, on peut considérer

$$s = \min(A) \in \mathbb{N}^*$$

Si y est un élément de $< x >$, alors il s'écrit x^m pour un $m \in \mathbb{Z}$ (d'après la remarque (1:2:4)). Par division euclidienne de m par s il existe $(q; r) \in \mathbb{Z} \times \mathbb{N}$ tel que $m = sq + r$ et $0 \leq r < s$. Comme $x^s = e$ on obtient $y = x^m = x^r$ donc

$$< x > \subset \{e; x; x^2; :::; x^{s-1}\}$$

L'inclusion inverse étant vraie on a donc

$$< x >= \{e; x; x^2; :::; x^{s-1}\}$$

et ainsi l'élément x est d'ordre fini.

En...n si i et j appartiennent à $\{0; 1; :::; s-1\}$ avec $i < j$ on a $x^i = x^j$ (sinon $x^{j-i} = e$ et $0 < j-i < s$ ce qui contredit la dé...nition de s), par conséquent l'ensemble $\{e; x; x^2; :::; x^{s-1}\} = < x >$ est de cardinal s soit $s = o(x)$:
(ii) Si x est d'ordre s, on a alors $x^s = e$ et pour $k = qs + r \in \mathbb{Z}$ avec $q \in \mathbb{Z}$ et $0 \leq r < s$ (division euclidienne), on a $x^k = x^r = e$ si et seulement si $r = 0$: ■

Remarque 1.2.11 Cas particulier important : Dans le cas où le groupe G est additif, l'ordre de $x \in G$ est dé...ni comme le plus petit entier $n \geq 1$, tel que $nx = 0$ quand cet ordre est ...ni. L'égalité $mx = 0$ équivaut alors à dire que m est multiple de n. Le groupe engendré par x est alors

$$< x >= \{kx; k \in \mathbb{Z}\} = \{rx; 0 \leq r \leq n-1\} = \{0; x; 2x; :::; (n-1)x\}$$

Théorème 1.2.12 Si $f : G \to G'$ est un isomorphisme de groupes, on a alors $o(f(x)) = o(x)$ pour tout $x \in G$.

Preuve. Pour $x \in G$; on a

$$< f(x) >= \{(f(x))^n : n \in \mathbb{Z}\} = \{f(x^n) : n \in \mathbb{Z}\} = f(< x >)$$

avec f est bijective, donc $card(< f(x) >) = card(< x >)$. ■

1.2.1 Produit de sous-groupes

Dé...nition 1.2.13 (Produit de sous-groupes) Soient $(G; :)$ un groupe, H et K deux sous-groupes de G. On considère les parties de G, $HK = \{hk : h \in H; k \in K\}$ et $KH = \{kh; k \in K; h \in H\}$, où le produit est la loi de G.

Remarque 1.2.14 En général, ces deux parties de G ne sont pas égales et ne sont pas des sous-groupes de G:

Proposition 1.2.15 Soient G un groupe, H et K deux sous-groupes de G. Alors HK est un sous-groupe de G si et seulement si $HK = KH$.

Preuve. Remarquons d'abord que HK et KH ne sont pas vides puisqu'ils contiennent l'élément neutre. Si HK est un sous-groupe de G, pour $h \in H$ et $k \in K$, on a $kh = (h^{-1}k^{-1})^{-1} \in HK$, donc KH est contenu dans HK. Soit $z \in HK$, alors $z^{-1} = hk$, et $z = k^{-1}h^{-1} \in KH$, d'où HK est contenu dans KH, et $HK = KH$.

Réciproquement, si $HK = KH$, soient h et h' dans H, k et k' dans K, alors $(hk)(h'k')^{-1} = hkk'^{-1}h'^{-1}$. Or, $kk'^{-1}h'^{-1} \in KH = HK$, donc il existe $h'' \in H$ et $k'' \in K$

tels que $kk^{o\,1}h^{o\,1} = h^{00}k^{00}$, d'où $(hk)(h^{0}k^{0})^{\ 1} = hh^{00}k^{00}$ 2 HK, et HK est un sous-groupe, ainsi que KH. ■

Remarque 1.2.16 Si G est abélien, pour tous sous-groupes H et K, HK est un sous-groupe de G.

Proposition 1.2.17 Soient G un groupe et $fH_i g_{1\ i\ n}$ une famille ...nie de sous groupes de G. Si, quels que soient i et j, 1 i < j n, $H_i H_j$ est un sous-groupe de G, alors $H_1 H_2 :::H_n = fx_1 :::x_n ; x_i$ 2 $H_i ; 1$ i ng est un sous groupe de G.

Preuve. On montre par raisonnement par récurrence, que cette proposition est un corollaire immédiat de la proposition (1:2:15) précédente. ■

Chapitre 2

Sous groupes distingués et groupes quotients

2.1 Classes modulo un sous groupe

La notion de relation d'équivalence utilisée au niveau des groupes va nous fournir un moyen de construire des groupes. Ces groupes s'appellent les groupes quotients et leur importance est capitale en mathématique.

Soit G un groupe que nous supposerons multiplicatif pour simpli...er les notations ; nous noterons e son élément neutre et x^{-1} le symétrique de $x \in G$. Soit H un sous-groupe de G. On dé...nit sur G la relation binaire $<$ par

$$\forall x, y \in G : x < y \Leftrightarrow x^{-1}y \in H \tag{2.1}$$

Proposition 2.1.1

(i) La relation $<$ est une relation d'équivalence sur G.

(ii) Soit x un élément de G, sa classe d'équivalence pour la relation $<$ est l'ensemble

$$xH = \{xh; h \in H\} = \{y \in G : x^{-1}y \in H\}$$

Preuve.

(i) j) Pour tout x de G, on a $x^{-1}x = e_G \in H$, d'où $x < x$ et la relation $<$ est ré‡exive.

jj) Pour tout x et tout y dans G; on a si $x < y$, alors

$$x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H$$

d'où $y < x$ et la relation $<$ est symétrique.

jjj) Pour tout x, tout y et tout z dans G; on a si x<x et y<z, alors $x^{-1}y \in H$ et $y^{-1}z \in H$, d'où $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$ et x<z, la relation < est donc transitive.
(ii) Soit $x \in G$, alors

$$\underline{x} = \{y \in G : y<x\} = \{y \in G : x^{-1}y \in H\} = \{y \in G; \exists h \in H : x^{-1}y = h\}$$

On obtient

$$\underline{x} = \{y = xh; h \in H\} = xH$$

■

Définition 2.1.2
1) La reltion < est appelée relation d'équivalence à gauche modulo H, et xH la classe à gauche de x modulo H.
2) On définit une relation d'équivalence à droite modulo H par

$$\forall x, y \in G : x<y \Leftrightarrow xy^{-1} \in H$$

et la classe à droite de x modulo H est l'ensemble

$$Hx = \{hx; h \in H\} = \{y \in G : yx^{-1} \in H\}$$

Lorsque nous aurons à considérer les relations à gauche et à droite modulo H, nous noterons ces deux relations respectivement $<_H$ et $_H<$.

Remarque 2.1.3
a) 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.

$$\underline{e} = eH = He = H$$

b) Pour tout x de G, on a $\underline{x} = H$ si et seulement si $x \in H$.
c) Si le groupe G est commutatif, alors les relations d'équivalences (resp. les classes) à gauche et à droite modulo H coïncident ($_H< = <_H$). Si le groupe G n' est pas abélien, ce n'ést plus le cas, en général.

Notation 2.1.4 (Cas particulier important)
i) Si G est un groupe additif, alors les relations d'équivalences définies ci-dessus s'écrivent

$$\forall x, y \in G : x<y \Leftrightarrow (x - y) \in H$$

Exemple 2.1.5

1) On considère un élément n de N et on pose H = nZ, sous groupe de Z, la relation d'équivalence (resp. les classes d'équivalence) modulo H coïncide(nt) avec la relation(resp. les classes) de congruence modulo n:

2) G = Z, H = 3Z. Les classes à gauche modulo H sont

i) classe à gauche de 0 : 0 + 3Z = 3Z.

ii) classe à gauche de 1 : 1 + 3Z.

iii) classe à gauche de 2 : 2 + 3Z.

3) Pour $H = \{I; (1\ 2)\}$ S_3, ($(S_3;)$ est le groupe des permutations d'ordre 3 ou groupe symétrique d'indice 3) on a les trois classes à gauches sont

$$IH = (1\ 2)H = H = \{I; (1\ 2)\}$$
$$(1\ 3)H = (1\ 2\ 3)H = \{(1\ 3); (1\ 2\ 3)\}$$
$$(2\ 3)H = (1\ 3\ 2)H = \{(2\ 3); (1\ 3\ 2)\}$$

Les classes à droites sont

$$HI = H(1\ 2) = H = \{I; (1\ 2)\}$$
$$H(1\ 3) = H(1\ 3\ 2) = \{(1\ 3); (1\ 3\ 2)\}$$
$$H(2\ 3) = H(1\ 2\ 3) = \{(2\ 3); (1\ 2\ 3)\}$$

Les classes à gauche et à droite ne coïncident pas.

Notation 2.1.6 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. On écrit

$$(G=H)_g = \{\underline{x} : x \in G\} = \{xH : x \in G\}$$

$$(G=H)_d = \{\underline{x} : x \in G\} = \{Hx : x \in G\}$$

Remarque 2.1.7 (Notation additive) En notation additive la relation (2:1) s'écrit

$$\forall x, y \in G : x \mathcal{R} y \Leftrightarrow (x - y) \in H$$

et on a les classes à gauche (resp. droite) sont dé...nies par $x + H$ (resp. $H + x$) pour tout $x \in G$ et $(G=H)_g = \{x + H; x \in G\}$ (resp. $(G=H)_d = \{H + x; x \in G\}$.

Proposition 2.1.8 Soient G un groupe et H un sous groupe de G. Les classes modulo H à gauche (resp. modulo H à droite) forment une partition de G. C'est-à-dire :
1) $8x \in G : xH = \ldots$ (resp. $Hx = \ldots$).
2) $8x, y \in G : xH = yH$ (resp. $Hx = Hy$) si et seulement si $xH \cap yH = \ldots$ (resp. $Hx \cap Hy = \ldots$).
3) $G = \bigcup_{x \in G} xH$ (resp. $G = \bigcup_{x \in G} Hx$).

Proposition 2.1.9 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: Autrement dit H et xH (resp. Hx) ont même nombre d'éléments.
(ii) Les ensembles $(G/H)_g$ et $(G/H)_d$ sont équipotents.

Preuve.
On rappelle qu'un ensemble E est équipotent à un ensemble F si et seulement s'il existe une bijection de E sur F. Alors
(i) Pour tout élément x de G, l'application $f : H \to xH$ qui à h associe xh, est évidemment bijective. En effet :
j) Soient $h_1, h_2 \in H$, alors

$$\begin{aligned} f(h_1) = f(h_2) &\Rightarrow xh_1 = xh_2 \\ &\Rightarrow (x^{-1}x)h_1 = (x^{-1})h_2 \\ &\Rightarrow h_1 = h_2 \end{aligned}$$

ceci montre l'injectivité de f.
jj) Soit $y \in xH$ telle que $f(h) = y$, alors

$$\begin{aligned} f(h) = y &\Rightarrow xh = y \\ &\Rightarrow h = x^{-1}y \in H \end{aligned}$$

ceci montre la surjectivité de f.
(ii) En remarquant que l'application $g : G \to G,\ x \to g(x) = x^{-1}$ réalise un isomorphisme de G.
Il faut d'abord définir une application de $(G/H)_g$ dans $(G/H)_d$. Soit donc xH une classe à gauche, associons-lui la classe à droite Hx^{-1}. On vérifie que cette correspondance est une application bien définie. On pose

$$\begin{aligned} \varphi : (G/H)_g &\to (G/H)_d \\ xH &\to \varphi(xH) = Hx^{-1} \end{aligned}$$

Soient $xH; yH \in (G/H)_g$, on a alors

$$xH = yH \Leftrightarrow x^{-1}y \in H$$

$$\Rightarrow x^{-1} \in Hy^{-1}$$

$$\Rightarrow Hx^{-1} = Hy^{-1}$$

$$\Rightarrow \varphi(xH) = \varphi(yH)$$

Montrons que φ est injective. Soient $xH; yH \in (G/H)_g$, alors

$$\varphi(xH) = \varphi(yH) \Rightarrow Hx^{-1} = Hy^{-1}$$

$$\Rightarrow x^{-1}y \in H$$

$$\Rightarrow xH = yH$$

Montrons que φ est surjective. Soit $Hx \in (G/H)_d$, alors

$$Hx = \varphi(x^{-1}H)$$

Par conséquent φ est surjective. Il existe donc une application bijective de $(G/H)_g$ sur $(G/H)_d$, ce qui preuve que ces deux ensembles sont équipotents. ■

Définition 2.1.10 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 $(G/H)_d$): On a donc

$$[G : H] = |(G/H)_g| = |(G/H)_d|$$

Le théorème qui vient maintenant et qui résulte des propositions précédentes est fondamental en algèbre.

Théorème 2.1.11 (de Lagrange)
Soit G un groupe fini. Si H est un sous groupe de G, alors

$$|G| = |H| : [G : H] \Leftrightarrow [G : H] = \frac{|G|}{|H|}$$

Autrement dit l'indice de H dans G est le quotient du cardinal de G par le cardinal de H.

Remarque 2.1.12
1) Ce théorème est souvent énoncé de la façon suivante : dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe. (C-à-d : l'ordre d'un groupe fini est multiple de

l'ordre de ses sous-groupes).
2) Dans un groupe, l'intersection d'un nombre ...ni de sous-groupes d'indice ...ni est un sous-groupe d'indice ...ni. En général, cette propriété n'est pas vraie pour un nombre in...ni de sous groupes d'indice ...ni (considérer les sous groupes de Z).

Preuve. On rappelle que l'ensemble des classes d'équivalence forme une partition d'un ensemble. Soit donc H un sous groupe de G. On considère la relation d'équivalence $<$ associée à H. Elle nous permet de dé...nir une partition de G par des sous ensembles des classes de la forme $xH;\ x \in G$. On peut donc trouver, G étant ...ni, un nombre $n \in \mathbb{N}$ et $x_1; x_2; :::; x_n \in G$ tels que $\{x_1H; x_2H; :::; x_nH\}$ forme une partition de G où n est le nombre de classes. Alors on peut écrire

$$G = \bigcup_{i=1}^{n} x_iH$$

G est clairement la réunion disjointes des x_iH. Alors

$$|G| = \sum_{i=1} |x_iH|$$

Mais les sous ensembles x_iH ont tous, d'après la proposition (2:1:9) précédente, le même nombre d'éléments. De plus, ce nombre est égal à $|H|$. (C-à-d : $|x_iH| = |H|$). Donc le cardinal de G s'écrit

$$|G| = \sum_{i=1} |x_iH| = \sum_{i=1} |H| = n|H|; n = |(G/H)_g|$$

$$\Rightarrow |G| = |(G \cap H)_g| : |H| = [G : H] : |H|$$

Ceci prouve notre théorème. ■

Exemple 2.1.13
1) Si l'on considère G comme sous-groupe de lui-même, on obtient le quotient $(G \cap G)_g = \{x:G; x \in G\}$. Comme $x:G = G$ pour tout $x \in G$, on a $(G \cap G)_g = \{G\}$, et donc $[G : G] = 1$.
2) Si l'on considère $H = \{e\}$ comme sous-groupe de G. Dans ce cas la relation $<$ est donnée par $x<y \Leftrightarrow x^{-1}:y \in \{e\}$ c'est-à-dire $x = y$. $<$ est donc la relation identité et ses classes sont $xH = x:\{e\} = \{x\}$. Le quotient est donc $(G \cap H)_g = \{\{x\}; x \in G\}$, il est ...ni si et seulement si G l'est et $[G : \{e\}] = |G|$ dans ce cas.
3) Pour $G = \mathbb{Z}$ et $H = 3\mathbb{Z}$. Alors les classes à gauches modulo H sont $3\mathbb{Z}; 1 + 3\mathbb{Z}; 2 + 3\mathbb{Z}$. On a bien

$$(G \cap H)_g = \{3\mathbb{Z}; 1 + 3\mathbb{Z}; 2 + 3\mathbb{Z}\}$$

4) Pour $H = \{I; (1\ 2)\}$ S_3, on a $[S_3 : H] = \frac{|S_3|}{|H|} = \frac{6}{2} = 3$. Les trois classes à gauches sont

$$\begin{aligned} IH &= (1\ 2)H = H = \{I; (1\ 2)\} \\ (1\ 3)H &= (1\ 2\ 3)H = \{(1\ 3); (1\ 2\ 3)\} \\ (2\ 3)H &= (1\ 3\ 2)H = \{(2\ 3); (1\ 3\ 2)\} \end{aligned}$$

Les classes à droites sont

$$\begin{aligned} HI &= H(1\ 2) = H = \{I; (1\ 2)\} \\ H(1\ 3) &= H(1\ 3\ 2) = \{(1\ 3); (1\ 3\ 2)\} \\ H(2\ 3) &= H(1\ 2\ 3) = \{(2\ 3); (1\ 2\ 3)\} \end{aligned}$$

Les classes à gauche et à droite ne coïncident pas.

On donne maintenant un corollaire du théorème de Lagrange qui est absolument fondamental dans la théorie des groupes …nis.

Corollaire 2.1.14 Soit G un groupe …ni. Soit x un élément de G d'ordre …ni. Alors l'ordre de x divise l'ordre de G et $x^{o(G)} = e$.

Preuve. Soit $x \in G$, on a $o(x) = o(H =< x >)$. D'après le théorème de Lagrange, cet entier $(o(H =< x >))$ divise $o(G)$. Il existe $m \in \mathbb{N}$ tel que

$$o(G) = m : o(< x >) = m : o(x)$$

Alors

$$x^{o(G)} = x^{m:o(x)} = \left(x^{o(x)}\right)^m = e^m = e$$

■

Théorème 2.1.15 (Formule des indices))
Soient H un sous-groupe de G et K un sous-groupe de H ($K \subset H \subset G$). Si l'indice de K dans G est …ni, alors l'indice de H dans G et celui de K dans H sont aussi …nis et on a

$$[G : K] = [G : H][H : K]$$

Preuve. On note respectivement $(g_iH)_{i\in I}$ et $(h_jK)_{j\in J}$ les classes à gauches modulo H dans G et modulo K dans H deux à deux distinctes. Alors $(g_iH)_{i\in I}$ (resp. $(h_jK)_{j\in J}$) forment une partition de G (resp. H) et card (I) = [G : H] (resp. card (J) = [H : K]). Nous allons alors montrer que la famille des classes à gauches modulo K dans G deux à deux distinctes est $(g_ih_jH)_{(i;j)\in I\ J}$. Dans le cas où [G : K] est …ni, il n'y a qu'un nombre …ni de telles classes, ce qui impose que I et J sont …nis et on a

$$[G : K] = \text{card}(I \quad J) = \text{card}(I):\text{card}(J) = [G : H][H : K]$$

Montrons le résultat annoncé.

Si $g \in G$, alors il existe un unique indice $i \in I$ tel que $gH = g_iH$ et il existe $h \in H$ tel que $g = g_ih$. De même il existe un unique indice $j \in J$ tel que $hK = h_jK$ et h s'écrit $h = h_jk$ avec $k \in K$, ce qui donne $g = g_ih_jk \in g_ih_jK$. On obtient

$$\begin{cases} g <_K (g_ih_j) \\ gK = g_ih_jK \end{cases}$$

Alors les classes à gauche dans G modulo K sont donc les g_ih_jK pour $(i; j) \in I \quad J$. Il reste à montrer que ces classes sont deux à deux distinctes.

Si $(i; j); (i^0; j^0) \in I \quad J$ sont tels que

$$g_ih_jK = g_{i^0}h_{j^0}K$$

$$\Rightarrow \exists k \in K : g_ih_j = g_{i^0}h_{j^0}k$$

$$\Rightarrow g_i = g_{i^0} \quad h_{j^0}kh \quad ;h_j \quad kh_j \quad {}_1 \in H$$
$$j^{\ 1} \qquad {}_0 \qquad {}_1$$

$$\Rightarrow g_i <_H (g_{i^0})$$

$$\Rightarrow \begin{cases} g_iH = g_{i^0}H \\ i = i^0 \end{cases}$$

Il en résulte que

$$h_j = h_{j^0}k; k \in K$$

$$\Rightarrow h_jK = h_{j^0}K$$

$$\Rightarrow j = j^0$$

■

Remarque 2.1.16 La démonstration ci-dessus montre que la formule de l'indice est vraie de façon plus générale dés que deux quelconques des trois termes qui apparaissent dans la

formule sont …nis le troisième étant alors nécessairement …ni.

Corollaire 2.1.17 Soient H et K deux sous groupes …nis d'un groupe G, alors

$$jHKj = jKHj = \frac{\frac{jHj:j}{Kj}}{jH \setminus Kj}$$

Preuve. Notons $I = H \setminus K$, c'est un sous-groupe de K. Alors

$$(K \quad I)_g = fIk_1; :::; I_{k_n}g$$

sont les classes à gauche de K modulo I. Montrons que HK est la réunion disjointe des H_{k_i}. En e¤et : d'une part, $hk \in HK$ et k peut s'écrire $k = zk_j; z \in I \quad H$ (puisque K est la réunion des Ik_j), d'où $hk = (hz)k_j \in Hk_j$.

D'autre part,

$$Hk_i \setminus Hk_j = \Rightarrow 9h; h' \in H : hk_i = h'k_j$$

$$\Rightarrow h'^{-1}h = k_j h_i^{-1} \in I = H \setminus K$$

$$\Rightarrow k_j \in Ik_i$$

Or deux classes ont une intersection vide.

En …n, comme ci-dessus

$$jHk_ij = jHj = jHk_jj$$

Donc

$$jjHKj = njHj = \frac{jK}{jIj} jHj = \frac{jKj}{jH \setminus Kj} jHj$$

■

2.2 Compatibilité avec la structure

Dé…nition 2.2.1 Soit E un ensemble muni d'une loi de composition interne (notée multiplicativement) sur lequel est dé…nie une relation d'équivalence <:
1) < est compatible à droite (resp. à gauche) avec la loi : si

$$\forall x; y; a \in E : x<y \Rightarrow xa<ya \text{ (resp. } x<y \Rightarrow ax<ay)$$

2) $<$ est compatible avec la loi : si elle est compatible à droit et à gauche.

$$8x; y; a \in E : x<y \Rightarrow \begin{cases} xa<ya \\ \text{et} \\ ax<ay \end{cases}$$

Proposition 2.2.2 La relation $<$ est compatible avec la loi de l'ensemble E si et seulement si

$$8x; x^0; y; y^0 \in E; [(x<x^0) \text{ et } (y<y^0)] \Rightarrow xy<x^0y^0$$

Preuve. Supposons que $<$ soit compatible avec la loi de E. Soient $x; x^0; y; y^0 \in E; (x<x^0)$ et $(y<y^0)$, alors

$$\begin{cases} xy<x^0y \\ \text{et} \\ x^0y<x^0y^0 \end{cases} \Rightarrow xy<x^0y^0$$

Par transitivité.

Réciproquement, l'assertion de l'énoncé étant vraie pour tout $x; x^0; y; y^0$; c'est en particulier vrai pour $y = y^0$; d'ou' si $x<x^0$ alors $xy<x^0y$ et la relation est compatible à droite avec la loi. De même, en considérant $x = x^0$; on montre qu'elle est compatible à gauche.

Remarque 2.2.3 Soit G un ensemble muni d'une loi de composition interne (notée multiplicativement). Si x est un élément de l'ensemble G, nous noterons x la classe d'équivalence de x dans G=<. Alors x sera un représentant de la classe d'équivalence x. Nous allons dé...nir une loi interne sur G=< par : Si x et y sont des éléments de G alors

$$x \quad y = \overline{x:y}$$

Quand aucune confusion n'est à craindre, nous noterons la loi interne de G=< de la même façon que celle de G. Cette loi est celle induite de G sur G=<.

■

Proposition 2.2.4 Soient G un ensemble muni d'une loi de composition interne, $<$ une relation d'équivalence dé...nie sur G et G=< l'ensemble quotient de G par la relation d'équivalence $<$. Alors la loi interne de G induit une loi interne sur G=<,

$$\begin{array}{ccc} G=< \quad G=< & \to & G=< \\ (x; y) & \to & \overline{x:y} = x:y \end{array}$$

si et seulement si $<$ est compatible avec la loi de G.

Preuve. On vérifie que cette loi est bien définie sur $G/\mathcal{R}$. Ceci revient à montrer que la correspondance $(x;y) \longmapsto \overline{x:y}$ est une application bien définie sur $G/\mathcal{R} \times G/\mathcal{R}$ dans $G/\mathcal{R}$.

Soient $(x_1;y_1);(x_2;y_2) \in G/\mathcal{R}$, alors

$$(x_1;y_1) = (x_2;y_2) \Longrightarrow \begin{cases} x_1 = x_2 \\ \text{et} \\ y_1 = y_2 \end{cases}$$

$$\Longrightarrow \begin{cases} x_1 \mathcal{R} x_2 \\ \text{et} \\ y_1 \mathcal{R} y_2 \end{cases}$$

Or $\mathcal{R}$ est une relation compatible avec la loi de G, alors $x_1y_1 \mathcal{R} x_2y$:Par cobséquent $\overline{x_1:y_1} = \overline{x_2:y_2}$. Ce qui montre que la loi est interne dans $G/\mathcal{R}$.

Réciproquement, supposons que la loi interne de G induit une loi interne sur $G/\mathcal{R}$. Soient $x_1;y_1;x_2;y_2 \in G$, alors

$$\begin{cases} x_1 \mathcal{R} y_1 \\ \text{et} \\ x_2 \mathcal{R} y_2 \end{cases} \Longrightarrow \begin{cases} x_1 = y_1 \\ \text{et} \\ x_2 = y_2 \end{cases}$$

D'autre part, on a

$$\overline{x_1:x_2} = x_1:x_2 = y_1:y_2 = \overline{y_1:y_2}$$

$$\Longrightarrow x_1y_1 \mathcal{R} x_2y_2$$

Alors $\mathcal{R}$ est compatible avec la loi de G. ■

Exemple 2.2.5 Pour tout entier n, la relation d'équivalence définie par la congruence modulo n dans $\mathbb{Z}$ est compatible avec l'addition et la multiplication des entiers. Ces deux lois induisent donc des lois de composition internes sur l'ensemble des entiers modulo n.

2.3 Groupes quotients

En général, les relations $x^{-1}y \in H$ et $xy^{-1} \in H$ sont distinctes ; pour qu'elles coïncident, il faut que les partitions qu'elles définissent sur G soient identiques, c'est-à-dire que pour tout $x \in G$, les classes xH et Hx soient égales. Cela peut encore se traduire par l'égalité $H = x^{-1}Hx$. Un tel sous-groupe H est appelé sous groupe distingué de G ou encore sous groupe invariant de G. On va maintenant étudier la situation où G est un groupe.

Proposition 2.3.1 Soient G un groupe et $<$ une relation d'équivalence dé...nie sur G compatible avec la loi de G: Alors l'ensemble quotient $G=<$, muni de la loi induite par la loi de G dé...nie par $(\overline{x};\overline{y}) \mapsto \overline{x:y}$ est un groupe. Si G est abélien il en est de même de $G=<$ équipé de la loi induite.

Preuve. C'est une conséquence directe de la proposition (2:2:4) précédente, qui assure que la loi sur le quotient est bien dé...nie. D'autre part, on a

1) Si G est abélien, alors

$$\forall \overline{x};\overline{y} \in G=< : \overline{x}:\overline{y} = \overline{x:y} = \overline{y:x} = \overline{y}:\overline{x}$$

Donc $G=<$ est abélien.

2) La loi de $G=<$ est associative, car

$$\forall \overline{x};\overline{y};\overline{z} \in G=< : \quad \overline{x}:\overline{y} \ :\overline{z} = \overline{(x:y):z} = \overline{(x:y)} \ :\overline{z} = \underline{x:(y:z)} = \underline{x}:\underline{(y:z)} = \underline{x}:\underline{(y:z)}$$

3) Si e est l'élément neutre de G, alors $\overline{e}$ est l'élément neutre de $G=<$, car

$$\forall \overline{x} \in G=< : \begin{cases} \overline{x}:\overline{e} = \overline{x:e} = \overline{x} \\ \overline{e}:\overline{x} = \overline{e:x} = \overline{x} \end{cases}$$

4) Soit $\overline{x} \in G=<$, alors $\overline{x}^{\,-1} = \overline{x^{-1}}$, car

$$\begin{cases} \overline{x}:\overline{x^{-1}} = \overline{x:x^{-1}} = \overline{e} \\ \overline{x^{-1}}:\overline{x} = \overline{x^{-1}:x} = \overline{e} \end{cases}$$

■

Proposition 2.3.2 Pour tout sous groupe H d'un groupe G, la relation $<_H$ (resp. ${}_H<$) est compatible à droite (resp. à gauche) avec la loi de composition de G. Réciproquement, si une relation $<$ dé...nie 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 $< = <_H$ (resp. $< = {}_H<$).

Preuve.

1) Soient $x; y; a$ des éléments de G tels que $x <_H y$. Alors

$$xy^{-1} \in H \Rightarrow (xa):(ya)^{-1} = xaa^{-1}y^{-1} = xy^{-1} \in H$$

Donc

$$xa <_H ya$$

D'autre part, on a

$$x_H < y \Rightarrow x^{-1}y \in H$$

$$\Rightarrow (ax)^{-1}:(ay) = x^{-1}a^{-1}ay = x^{-1}y \in H$$

$$\Rightarrow ax_H < ay$$

2) Soit $<$ une relation d'équivalence dé...nie sur G, compatible à droite avec la loi de G. On note H la classe d'équivalence de l'élément neutre e de G. Montrons que H est un sous groupe de G.

i) Puisque $e \in H$, alors H est non vide.

ii) Pour tout x et y dans H, on a

$$x<e \text{ et } y<e$$

La compatibilité de $<$ avec la loi de G donne

$$xy^{-1}<ey^{-1}; y^{-1} \in G$$

$$\Rightarrow xy^{-1}<y^{-1}$$

de plus

$$yy^{-1}<ey^{-1}$$

$$\Rightarrow e<y^{-1}$$

$$\Rightarrow y^{-1}<e$$

On obtient

$$\begin{cases} xy^{-1}<y^{-1} \\ \text{et} \\ y^{-1}<e \end{cases} \Rightarrow xy^{-1}<e$$

$$\Rightarrow xy^{-1} \in H$$

Ce qui prouve que H est un sous-groupe de G.

Montrons que

$$< = <_H \Leftrightarrow \forall x; y \in G : x<y \Leftrightarrow x<_H y$$

j) Soient $x; y \in G$, si $x<y$ alors, d'après la compatibilité de $<$, on a

$$xy^{-1}<e$$

Alors

$$xy^{-1} \in H$$

$$\Rightarrow x <_H y$$

jj) Si $x <_H y$, alors

$$xy^{-1} \in H$$

$$\Rightarrow xy^{-1} < e$$

D'après la compatibilité, on a $x < y$.
Une démonstration analogue donne le résultat pour $<=_H <$.
L'unicité de H découle du fait que si $< = <_H$, alors H est la classe d'équivalence de e. ■

Corollaire 2.3.3 La relation d'équivalence $<$ est donc compatible avec la loi de G si et seulement si il existe un sous-groupe H de G tel que $<=_H < = <_H$.

Dé...nition 2.3.4 Un sous-groupe H d'un groupe G est dit normal (ou distingué) dans G si $_H < = <_H$: On note $H \triangleleft G$ pour signi...er que H est un sous-groupe distingué de G.

La relation d'équivalence modulo un sous-groupe distingué est la seule qui permette de munir le quotient d'une structure de groupe telle que l'application canonique soit un morphisme. C'est ce que montre le théorème suivant.

Théorème 2.3.5 Si H est un sous-groupe normal d'un groupe G, la loi de composition interne induite sur l'ensemble G=H par celle de G munit G=H d'une structure de groupe. La surjection canonique (l'application de passage au quotient) $\pi : G \twoheadrightarrow G/H$ qui, à un élément de G associe sa classe modulo H, est un morphisme de groupes.

Preuve. On dé...nit une loi de composition sur G=H en posant

$$\forall x, y \in G : (xH) \cdot (yH) = (x \cdot y)H \Leftrightarrow \forall x, y \in G : \overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Montrons que ceci est bien dé...ni. On montre que si $x', y' \in G$ avec $x'H = xH$ et $y'H = yH$, alors $(x'y')H = (xy)H$. Or, l'hypothèse implique que

$$\begin{cases} x_H <x' \\ y_H <y' \end{cases} \Rightarrow \begin{cases} x^{-1}x' \in H \\ y^{-1}y' \in H \end{cases}$$

$$\Rightarrow \begin{cases} x' = xh; h \in H \\ y' = yk; k \in H \end{cases}$$

Alors

$$(x^0y^0)H = (xhyk)H \Rightarrow (x^0y^0)H = xy\ y^{-1}hy\ k\ H$$

Puisque H est un sous-groupe normal (C-à-d : $_H <= <_H$, $(xH = Hx)$), alors

$$y^{-1}hy \in H; kH \in H \Rightarrow y^{-1}hy\ k \in H$$

Donc

$$(x^0y^0)H = (xy)H$$

L'élément neutre est $eH = H$ et l'inverse de xH est $x^{-1}H$. On a bien

$$x^{-1}H : (xH) = xx^{-1}H = eH = H$$

En...n, l'associativité est immédiate. Donc $G=H$ est un groupe.
En...n, montrons que

$$\begin{aligned} : G &\to G=H \\ x &\to \overline{x} = xH \end{aligned}$$

est un morphisme de groupes. Soient $x; y \in G$, alors

$$(x:y) = \overline{x:y} = (x:y)H = (xH) : (yH) = \overline{x}:\overline{y} = (x): (y)$$

Il est claire que est surjective, car pour tout $t \in G=H$, on peut trouver $x \in G$ tel que $\overline{x} = t$. ■

Dé...nition 2.3.6 Soit G un groupe et H un sous-groupe distingué de G. On note $G=H$ l'ensemble quotient de G par la relation d'équivalence associée à H, et on l'appelle le groupe quotient de G par H. On a donc

$$G=H = f\overline{x}; x \in Gg$$

avec $\overline{x} = xH = Hx$.

Remarque 2.3.7
1) Si H est un sous-groupe distingué de G, l'ensemble quotient $G=H$ est l'ensemble des classes d'équivalence modulo H, sans préciser à droite ou à gauche puisque ce sont les mêmes et il peut être muni d'une structure de groupe en dé...nissant le composé de la classe de x et de la classe de y comme la classe de xy. Autrement dit $_H <= <_H$, pour tout x élément de G, $\overline{x}_g = xH = \overline{x}_d = Hx = \overline{x}$ et $G=H = (G=H)_g = (G=H)_d$.
2) Notons $_g : G \to (G=H)_g ; x \to xH$ et $_d : G \to (G=H)_d ; x \to Hx$ les surjections canoniques, alors $_g = _d$ lorsque $H \subset G$. Tout élément de $_d^{-1}(Hx)$ (resp. $_g^{-1}(Hx)$)

représente la classe Hx (en particulier x représente Hx), mais, bien entendu, il y a plusieurs représentants d'une même classe (en général). Ainsi $x; x'$ représentent la même classe à gauche ssi $x^{-1}x' \in H$.

3) Si $G=H$ est le groupe quotient de G par le sous-groupe distingué H, alors les deux propriétés suivantes sont équivalentes :

i) Le groupe $G=H$ est commutatif.

ii) Pour tous $x; y$ de G, l'élément $y^{-1}x^{-1}yx$ est dans H. En effet, soient $x; y$ deux éléments de G. On a les équivalences suivantes

$$\overline{x}:\overline{y} = \overline{y}:\overline{x} \Leftrightarrow \overline{x}:\overline{y} = \overline{y}:\overline{x} \Leftrightarrow (xy)<(yx) \Leftrightarrow (xy)^{-1}:(yx) \in H \Leftrightarrow y^{-1}x^{-1}yx \in H$$

Proposition 2.3.8 Un sous-groupe H d'un groupe G est normal dans G si et seulement s'il vérifie les conditions équivalentes suivantes :

(i) $\forall x \in G : xH \subset Hx$ (i')
) $\forall x \in G : xH = Hx$
(ii) $\forall x \in G : xHx^{-1} \subset H$
(ii') $\forall x \in G : xHx^{-1} = H$
(iii) $\forall h \in H; \forall x \in G : xhx^{-1} \in H$
(iv) Il existe un groupe G' et un morphisme de groupes $f : G \to G'$ tel que $H = \ker(f)$

Preuve. Le sous-groupe H est normal dans G si et seulement si les relations $_H<$ et $<_H$ sont égales, donc si et seulement si les classes à gauche et les classes à droite sont égales. Les assertions (i) et (i') sont équivalentes. En effet, l'implication (i') $\Rightarrow$ (i) est évidente. Pour l'implication (i) $\Rightarrow$ (i'), on a

$$\forall x \in G : xH \subset Hx \Rightarrow x^{-1}Hx \subset Hx^{-1}$$

On multiplie par x à gauche et à droite. On en déduit

$$x\,x^{-1}Hx \subset x\,Hx^{-1}x$$

$$\Rightarrow Hx \subset xH$$

C'est- à-dire $xH = Hx$.

Les assertions (ii) et (ii') sont clairement équivalentes. En effet, on a (ii') $\Rightarrow$ (ii) évident. Pour (ii) $\Rightarrow$ (ii'). Supposons que $xHx^{-1} \subset H$ et montrons que $H \subset xHx^{-1}$. Alors

$$\forall x \in G : xHx^{-1} \subset H \Rightarrow \forall x \in G : x^{-1}Hx^{-1^{-1}} \subset H$$

Soit $h \in H$, alors

$$h' = x^{-1}hx \in H$$

car $x^{-1}H(x^{-1})^{-1} \quad H$.
Alors

$$h = x\ x^{-1}hx\ x^{-1} = xh'x \in xHx^{-1}$$

Donc $H \quad xHx^{-1}$. D'autre part, (i) implique (ii), qui est équivalente à (iii):

Si $xhx^{-1} \in H, (x \in G;\ h \in H)$; alors il existe $h' \in H$ tel que $xh = h'x$; donc $xH \quad Hx$ et (iii) implique (i).

Supposons que H soit le noyau d'un morphisme de groupes f de G dans G'. En posant $H = \ker(f)$.

Montrons que

$$\forall h \in H; \forall x \in G : xhx^{-1} \in H$$

Soient $x \in G; h \in H$ alors

$$f\ xhx^{-1} = f(x)f(h)f(x^{-1}) = f(x)f(x^{-1}); f(h) = e'$$

$$\Rightarrow f\ xhx^{-1} = f(xx^{-1}) = f(e) = e'$$

Donc l'élément xhx^{-1} appartient à $H = \ker f$. Donc H est normal dans G.

Réciproquement, si H est distingué dans G alors G=H est un groupe pour la loi quotient et H est le noyau du morphisme de groupes de G dans G=H qui à x associe sa classe modulo H (est la surjection canonique de G sur G=H). (voir la proposition (2.3.14) ci-dessous). ■

Exemple 2.3.9

1) feg et G sont toujours des sous-groupes distingués, dits triviaux. En e¤et, on a

$$\forall x \in G : \begin{cases} xfeg = fegx = fxg \\ xG = Gx = G \end{cases}$$

Puisque les applications $g \mapsto xg$ et $g \mapsto gx$ sont des bijections de G dans lui-même.

2) Dans un groupe abélien G, tout sous-groupe H de G est un sous groupe distingué de G. En e¤et, soit H un sous-groupe de G. Si G est un groupe commutatif, alors tous les éléments de G commutent entre eux y compris ceux qui sont dans H (H est donc commutatif). Par conséquent,

$$\forall x \in G; \forall h \in H; xh = hx \Leftrightarrow xhx^{-1} = h$$

$$\Longrightarrow \forall x \in G, \forall h \in H : xhx^{-1} \in H$$

On conclut que tout sous-groupe H de G est distingué dans G.

3) L'ensemble $H = \{z \in G; \forall x \in G : zx = xzg$, noté $Z(G)$, est un sous-groupe distingué de G appelé centre de G. En effet, il est claire que $Z(G)$ est un sous groupe de G. Il reste à montrer que le sous-groupe $Z(G)$ de G est distingué. Or

$$\forall c \in H, \forall x \in G : cx = xc \text{ (car c commute avec tous les x de G)}$$

Alors pour tout x de G, on a donc $xH = Hx$.

4) Tout sous-groupe H d'indice 2 dans un groupe G est distingué. En effet, si l'indice est 2, cela signifie qu'il n'y a que 2 classes (à gauche ou à droite), autrement dit pour tout $x \notin H$, alors

$$\begin{cases} (G/H)_g = \{H; xH\} \\ (G/H)_d = \{H; Hx\} \end{cases}$$

et ainsi $xH = G \setminus H = Hx$.

5) L'ensemble des automorphismes intérieurs de G ($Int(G)$) est distingué dans le groupe des automorphisme ($Aut(G)$) de $(G; :)$. Où pour tout $g \in G$, $Int(G)$ est l'ensemble des automorphismes de G de la forme

$$\begin{aligned} \tau_g : G &\longrightarrow G \\ x &\longmapsto \tau_g(x) = gxg^{-1} \end{aligned}$$

En effet, soient $f \in Aut(G); \tau_g \in Int(G); x \in G$, alors

$$\begin{aligned} (f \circ \tau_g \circ f^{-1})(x) &= f \circ (\tau_g \circ f^{-1})(x) = f \circ \tau_g \circ f^{-1}(x) = f(g:f^{-1}(x):g^{-1}) \\ &= f(g):x:f(g^{-1}) = f(g):x(f(g))^{-1} = \tau_{f(g)}(x) \end{aligned}$$

Donc $f \circ \tau_g \circ f^{-1} \in Int(G)$.

Proposition 2.3.10 L'intersection de deux sous groupes distingués $H; K$ de G est un sous groupe distingué de G.

Preuve. Puisque H et K sont des sous groupes de G, alors $H \cap K$ est un sous groupe de G. Supposons que $H; K$ sont distingués dans G. Soient $g \in G; h \in H \cap K$, alors

$$\begin{cases} g \in G \\ h \in H \\ h \in K \end{cases} \Longrightarrow \begin{cases} ghg^{-1} \in H \\ ghg^{-1} \in K \end{cases}$$

$$\Longrightarrow ghg^{-1} \in H \cap K$$

■

Proposition 2.3.11 Soient G un groupe, H un sous-groupe de G et N un sous-groupe normal de G. Alors

1) $H \cap N$ est un sous-groupe normal de H.

2) NH est un sous-groupe de G.

3) N est un sous-groupe normal de NH.

4) Si H un sous-groupe normal de G, alors NH est normal de G.

Preuve.

1) Puisque H et N sont des sous groupes de G, alors $H \cap N$ est un sous groupe de G. Comme $H \cap N$ est inclus dans H, c'en est un sous-groupe. Soient n appartenant à $H \cap N$ et h appartenant à H. Alors, hnh^{-1} appartient à H car H est un sous-groupe et hnh^{-1} appartient à N car N est un sous-groupe normal de G. D'où $H \cap N$ est un sous-groupe normal de H.

2) On sait que $NH = \{nh : n \in N; h \in H\}$. Alors NH est un sous groupe de G si et seulement si $NH = HN$. On a

$$x \in NH \Rightarrow \exists n \in N; \exists h \in H : x = nh$$

Or $H \subset G$ et $N \subset G$, alors

$$hN = Nh$$

Il existe $n' \in N$ tel que

$$x = hn' = nh$$

Alors $x \in HN$, d'où $NH \subset HN$: L'inclusion réciproque se montre de la même façon, et ainsi HK est un sous groupe de G.

3) On peut écrire $N = N \cup \{e\}$ est clairement un sous-groupe de NH puisque N est un sous-groupe de G. Soient n appartenant à N et $n'h \in NH$ $(h \in H; n' \in N)$. Alors

$$(n'h).n.(n'h)^{-1} = (n'h).n.(h^{-1}n'^{-1}) = n'(hnh^{-1})n'^{-1}; hnh^{-1} \in N \text{ car } N \subset G$$

$$\Rightarrow (n'h).n.(n'h)^{-1} = n'n''n'^{-1} \in N$$

Alors N est un sous-groupe normal de NH.

4) Pour tout $g \in G$, on a

$$g(NH) = (Ng)H = NHg$$

donc $NH \subset G$. ■

2.3.1 Sous-groupes normaux et morphismes

Proposition 2.3.12 Soient G et G' deux groupes et $f : G \to G'$ un morphisme de groupes. Alors $\ker f$ est un sous-groupe normal de G.

Preuve. Soient $x \in G; h \in \ker f$, alors

$$f(xhx^{-1}) = f(x)f(h)f(x^{-1}) = f(x)f(x^{-1}); f(h) = e$$

$$\Rightarrow f(xhx^{-1}) = f(x)f(x)^{-1} = e'$$

$$\Rightarrow xhx^{-1} \in \ker f$$

Le sous-groupe $\ker f$ de G est donc distingué. ■

Exemple 2.3.13 Si K est un corps commutatif, alors l'ensemble

$$SL_n(K) = \{A \in M_n(K) : \det(A) = 1\}$$

est un sous-groupe distingué (appelé le groupe spécial linéaire) de $GL_n(K)$ comme noyau du morphisme de groupes :

$$\det : A \in GL_n(K) \to \det(A) \in K :$$

C'-à-d

$$SL_n(K) \subset GL_n(K) \text{ car } \ker(\det) = SL_n(K)$$

Proposition 2.3.14
Un sous-groupe normal est le noyau d'un morphisme de groupes.

Preuve. Soit G un groupe et $H \subset G$. Alors l'application

$$\begin{aligned} G &\to G/H \\ x &\to \overline{x} = xH \end{aligned}$$

est un morphisme de groupes. Montrons que $H = \ker$.
Si $x \in \ker$, alors

$$(x) = e_{G/H} = e = H$$

Donc $xH = H$ donc $x \in H$.
Si $x \in H$ alors

$$(x) = \overline{x} = H = e_{G/H}$$

Donc $x \in \ker$. ■

Exemple 2.3.15 Le centre $Z(G)$ est sous-groupe normal car il est le noyau d'un morphisme φ de groupe G dans le groupe des automorphismes (appelé automorphismes intérieurs) φ dé...ni par

$$\begin{array}{rccc} \varphi : & (G;:) & \longrightarrow & (Aut(G);\ \circ) \\ & g & \longrightarrow & \varphi_g \end{array}$$

Où

$$\begin{array}{rccc} \varphi_g : & G & \longrightarrow & G \\ & x & \longrightarrow & \varphi_g(x) = gxg^{-1} \end{array}$$

On a

$$\begin{aligned} \ker(\varphi) &= \{g \in G : \varphi_g = Id_G\} \\ &= \{g \in G; \forall x \in G : \varphi_g(x) = x\} \\ &= Z(G) \end{aligned}$$

Proposition 2.3.16 Soient $G; G'$ deux groupes et f un morphisme de groupes de G dans G'.
1) Si H est un sous-groupe distingué de G et f est surjectif, alors $f(H)$ est un sous groupe distingué de G'.
2) Si H' est un sous-groupe distingué de G', alors $f^{-1}(H')$ est un sous groupe distingué de G.

Preuve. On sait déjà que $f(H)$ est un sous-groupe de G' (que f soit surjectif ou non) et que $f^{-1}(H')$ est un sous-groupe de G.
1) Si f est surjectif, alors tout $g' \in G'$ s'écrit $g' = f(g)$ avec $g \in G$ et pour tout $h' = f(h) \in f(H)$ (avec $h \in H$), on a

$$g'h'g'^{-1} = f(g).f(h).(f(g))^{-1} = f(g).f(h).f(g^{-1}) = f(ghg^{-1}) \in f(H)$$

ce qui signi...e que $f(H)$ est distingué dans G'.
2) Pour $g \in G$ et $h \in f^{-1}(H')$, on a

$$f(ghg^{-1}) = f(g).f(h).f(g^{-1}) = f(g).f(h).(f(g))^{-1} \in f(g)H'(f(g))^{-1} = H'$$

et $ghg^{-1} \in f^{-1}(H')$. Donc $f^{-1}(H')$ est distingué dans G. ■

2.3.2 Caractérisation des sous-groupes normaux

Il est clair qu'un sous-groupe H d'un groupe G n'est pas nécessairement normal dans G. Nous allons introduire un sous-groupe intermédiaire entre H et G, appelé le

normalisateur de H dans G, dans lequel H sera un sous-groupe normal et qui permettra de déterminer si H est normal dans G.

Définition 2.3.17 Soient G un groupe et P(G) l'ensemble de ses parties. On dit que deux éléments S et S' de P(G), $(S = ?)$, sont conjugués s'il existe un élément x de G tel que

$$S' = xSx^{-1} = \{xsx^{-1}; s \in S\}$$

Remarque 2.3.18
1) En convenant que la partie vide est conjuguée d'elle-même, la relation de conjugaison est une relation d'équivalence sur P(G). Pour une partie $S = \{\}$ de G, sa classe d'équivalence pour cette relation est l'ensemble $\{xSx^{-1}; x \in G\}$; qu'on appelle classe de conjugaison de S.
2) Si $S = \{g\}$, où g est un élément de G, les éléments de sa classe de conjugaison sont appelés les conjugués de g dans G.
3) Une partie S' est conjuguée d'une partie S si elle est l'image de S par un automorphisme intérieur de G. Par conséquent, deux parties conjuguées sont équipotentes.

Définition 2.3.19 On dit que deux sous groupes H et K de G sont conjugués si il existe un élément g de G tel que $gHg^{-1} = K$.

Proposition 2.3.20 Si deux sous groupes H et K de G sont conjugués alors ils sont en bijection. Dans le cas où leur cardinal est fini, ils ont même cardinal.

Preuve. Soient H et K deux sous groupes conjugués de G. Soit donc g dans G tel que $gHg^{-1} = K$. Définissons l'application f par

$$\begin{aligned} f : H &\to K \\ h &\to f(h) = ghg^{-1} \end{aligned}$$

L'égalité $gHg^{-1} = K$ nous permet d'être convaincu de la surjectivité de f.

Pour l'injectivité : si $gh_1g^{-1} = gh_2g^{-1}$ alors en multipliant cette égalité à gauche par g^{-1} et à droite par g, on obtient $h_1 = h_2$.

Supposons que H est fini, alors $card(H) = card(K)$ car f est bijective. ■

Définition 2.3.21 Soient S et S' deux parties d'un groupe G et H un sous-groupe de G: Alors S et S' sont conjuguées sous H s'il existe un élément x de H tel que $S' = xSx^{-1}$.

Proposition 2.3.22 Soient S une partie d'un groupe G et H un sous-groupe de G:
1) L'ensemble $N_H(S) = \{x \in H : xSx^{-1} = S\}$ est un sous-groupe de H (donc de G) appelé le normalisateur de S dans H:

2) L'ensemble $Z_H(S) = \{x \in H; \forall s \in S : xsx^{-1} = s\}$ est un sous-groupe de H (donc de G) appelé le centralisateur de G dans H:
3) $Z_H(S) \subset N_H(S)$:

Preuve.
1) i) Il est clair que $e_H \in N_H(S)$.
ii) Soient $x, y \in N_H(S)$, alors

$$xSx^{-1} = S \text{ et } ySy^{-1} = S$$

On a

$$(xy)S(xy)^{-1} = xySy^{-1}x^{-1} = x(ySy^{-1})x^{-1} = xSx^{-1} = S$$

$$\Rightarrow xy \in N_H(S)$$

iii) Soit $x \in N_H(S)$, alors

$$xSx^{-1} = S$$

$$\Rightarrow S = x^{-1}Sx$$

$$\Rightarrow S = x^{-1}S(x^{-1})^{-1}$$

$$\Rightarrow x^{-1} \in S$$

2) Se démontre de la même façon.
3) Soient $x \in Z_H(S)$ et $a \in N_H(S)$, alors pour tout $s \in S$,

$$(axa^{-1})s(axa^{-1})^{-1} = (axa^{-1})s(ax^{-1}a^{-1}) = axs'x^{-1}a^{-1}; s' = a^{-1}sa$$

Puisque $x \in Z_H(S)$, alors

$$xs'x^{-1} = s'$$

d'ou'

$$(axa^{-1})s(axa^{-1})^{-1} = as'a^{-1} = aa^{-1}saa^{-1} = s$$

$$\Rightarrow axa^{-1} \in Z_H(S)$$

■

Proposition 2.3.23 Soient G un groupe et H un sous-groupe de G. Alors H est un sous-groupe normal de $N_G(H)$, et H est un sous-groupe normal de G si et seulement si $N_G(H) = G$.

Preuve. Découle de la dé...nition de $N_G(H)$. ■

2.4 Théorèmes d'isomorphismes

Théorème 2.4.1 (Premier théorème d'isomorphisme ou théorème de décomposition canonique)
Si $G; G^0$ sont deux groupes et $f : G \to G^0$ un morphisme de groupes, il existe alors un unique isomorphisme de groupes $\tilde{f} : G/\ker f \to \mathrm{Im}\, f = f(G)$ (i.e, $G/\ker f \simeq \mathrm{Im}\, f$) tel que $f = i \circ \tilde{f} \circ p$ où $p : G \to G/\ker f$ est un morphisme surjectif (la surjection canonique) et $i : \mathrm{Im}\, f \to G^0$ est un morphisme injectif (l'injection canonique).

Remarque 2.4.2 Le théorème précédent s'exprime aussi en disant qu'on a le diagramme commutatif

$$\begin{array}{ccc} G & \xrightarrow{f} & G^0 \\ p \downarrow & & \uparrow i \\ G/\ker f & \xrightarrow[\tilde{f}]{} & \mathrm{Im}\, f \end{array}$$

Alors

$$f = i \circ \tilde{f} \circ p$$

Preuve. Rappelons que $H = \ker f$ est un sous groupe distingué de G (d'après la proposition (2:3:12)) et donc on peut considérer l'ensemble quotient de G par $\ker f$ qui a une structure de groupe pour la loi induite de celle de G. $\ker f$, sous-groupe distingué associé à la relation d'équivalence $<$ dé...nie par

$$\forall x, y \in G : x < y \Leftrightarrow x^{-1} y \in H = \ker f$$

Rappelons aussi que l'on a un morphisme surjectif qui a tout élément de G associe sa classe d'équivalence dans $G/\ker f$. On dé...nit alors la projection p (surjection canonique)

$$\begin{array}{rccl} p : & G & \to & G/\ker f \\ & x & \mapsto & p(x) = \overline{x} = xH = x \ker f \end{array}$$

Par dé...nition $G/\ker f = \mathrm{Im}\, p$.
On dé...nit l'injection canonique i par

$$\begin{array}{rccl} i : & \mathrm{Im}\, f & \to & G^0 \\ & y & \mapsto & i(y) = y \end{array}$$

Rappelons que l'injection canonique de $A \subset B$ dans B est la restriction de l'identité sur B à A, $i = Id_B|_A$, elle "ne fait rien" à part changer l'ensemble d'arrivée. Il est claire que i est un morphisme de groupe injective.

Soit l'application $\bar{f}$ dé…nie par

$$\begin{array}{rccl} \bar{f}: & G=\ker f & \longmapsto & \operatorname{Im} f = f(G) \\ & \bar{x} & \longmapsto & \bar{f}(\bar{x}) = f(x) \end{array}$$

Montrons que l'application $\bar{f}$ est un morphisme bijectif. On montre d'abord que l'on peut dé…nir $\bar{f}$ par $\bar{f}(\bar{x}) = f(x)$ pour tout $\bar{x} \in G=\ker f$. Pour justi…er cette dé…nition, on doit véri…er qu'elle ne dépend pas du choix d'un représentant de $\bar{x}$.

Soient $x_1; x_2 \in G$, alors

$$\begin{aligned} \bar{x}_1 = \bar{x}_2 &\Longrightarrow x_1 < x_2 \\ &\Longrightarrow x_1^{-1} x_2 \in \ker f \\ &\Longrightarrow f(x_1^{-1} x_2) = e' \\ &\Longrightarrow f(x_1^{-1}) \cdot f(x_2) = f(x_1)^{-1} \cdot f(x_2) = e' \\ &\Longrightarrow f(x_1) = f(x_2) \end{aligned}$$

Alors

$$\bar{f}(\bar{x}_1) = \bar{f}(\bar{x}_2)$$

L'application $\bar{f}$ est donc bien dé…nie et par construction, on a

$$f = i \circ \bar{f} \circ p$$

$\bar{f}$ est un morphisme de groupes. Car $\forall \bar{x}_1; \bar{x}_2 \in G=\ker f$, on a

$$\bar{f}(\bar{x}_1 \cdot \bar{x}_2) = \bar{f}(\overline{x_1 \cdot x_2}) = f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2) = \bar{f}(\bar{x}_1) \cdot \bar{f}(\bar{x}_2)$$

D'autre part, $\bar{f}$ est injectif, car $\forall \bar{x} \in G=\ker f$, on a

$$\bar{f}(\bar{x}) = e' \Longrightarrow f(x) = e'$$

$$\Longleftrightarrow x \in \ker f$$

D'après la remarque (2:1:3), on a

$$x \in \ker f = H \Longleftrightarrow \bar{x} = \ker f = \bar{e}$$

Alors

$$\ker \bar{f} = \{\bar{e}\}$$

Ce morphisme est surjectif et à valeurs dans $\mathrm{Im}\, f = f(G)$. En effet, si $y \in f(G)$, alors $\exists x \in G$ tel que $f(x) = y$. Posons

$$z = xH = x \ker f = \bar{x}$$

Alors

$$f'(z) = f'(\bar{x}) = f(x) = y$$

En…n, si un tel isomorphisme f' existe, on a alors, pour tout $x \in G$

$$f(x) = i \circ f' \circ p\,(x) = i \circ f'\,(p(x)) = i \circ f'\,(\bar{x}) = i(f'(\bar{x})) = f'(\bar{x})$$

ce qui prouve l'unicité de f'. ■

Corollaire 2.4.3 Si $f : G \to G'$ est un morphisme de groupes surjective, il existe alors un isomorphisme de groupes $f' : G/\ker f \to G'$ (i.e, $G/\ker f \simeq G'$)

Preuve. Clair, car, ici $\mathrm{Im}(f) = G'$: ■

Corollaire 2.4.4 Soient G, G' deux groupes et $f : G \to G'$ un morphisme de groupes. Si G est …ni, on a alors

$$\mathrm{card}(G) = \mathrm{card}(\ker f) : \mathrm{card}(\mathrm{Im}\, f)$$

Preuve. Comme $G/\ker f$ et $\mathrm{Im}\, f$ sont isomorphes, dans le cas où G est …ni, on a d'après le théorème du Lagrange

$$\mathrm{card}(\mathrm{Im}\, f) = \mathrm{card}(G/\ker f) = \frac{\mathrm{card}(G)}{\mathrm{card}(\ker f)}$$

Alors

$$\mathrm{card}(G) = \mathrm{card}(\ker f) : \mathrm{card}(\mathrm{Im}\, f)$$

■

Exemple 2.4.5

1) Le morphisme $\mathrm{Id}_G : G \to G$ à le noyau $\{e\}$ et l'image G. On obtient donc $G/\{e\} \simeq G$.

2) Le morphisme $f : G \to G$ dé…nit par $f(x) = e$ pour tout $x \in G$ a pour noyau G et pour image $\{e\}$. On a donc $G/G \simeq \{e\}$.

3) L'application $f : \mathbb{R}^* \to \mathbb{R}^* ; x \to |x|$ est un morphisme des groupes. Alors, puisque $\ker f = \{-1, 1\}$, $\mathrm{Im}\, f = \mathbb{R}_+^*$ et $\mathbb{R}^*/\{-1, 1\} \simeq \mathbb{R}_+^*$.

4) Pour un autre exemple, revenons sur la dé…nition du centre $Z(G)$ comme noyau du

morphisme $f : G \to Aut(G)$. L'image de ce morphisme est le groupe $Int(G)$ des automorphismes intérieurs de G. Le centre $Z(G)$ est donc un sous-groupe distingué de G et $G/Z(G) \simeq Int(G)$.
Si G est abélien, $Z(G) = G$ et donc $Int(G) = \{Id_G\} \simeq G/G = \{G\}$. Dans le cas opposé où $Z(G) = \{e\}$, on a $Int(G) \simeq G/\{e\} \simeq G$.

Le théorème suivant généralise le premier théorème d'isomorphisme :

Proposition 2.4.6 (de passage au quotient)
Soient G et G' deux groupes, H (resp. H') un sous-groupe normal de G (resp. G'), $p : G \to G/H$ (resp. $p' : G' \to G'/H'$) la projection (surjection) canonique. Pour tout $f : G \to G'$ un morphisme de groupe tel que $f(H) \subset H'$, il existe un unique $\tilde{f} : G/H \to G/H'$ morphisme de groupe tel que

$$\tilde{f} \circ p = p' \circ f.$$

Preuve. Considérons le diagramme suivant

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ p \downarrow & & \downarrow p' \\ G/H & \xrightarrow{\tilde{f}} & G'/H' \end{array}$$

Si le morphisme $\tilde{f}$ existe et fait commuter le diagramme, il doit vérifier

$$\tilde{f}(p(x)) = p'(f(x))$$

et, tout élément de G/H s'écrivant p(x) pour $x \in G$, cette égalité impose l'unicité de $\tilde{f}$.

Montrons que l'égalité ci-dessus définit bien une application $\tilde{f}$, i.e. que $\tilde{f}(p(x))$ est indépendant du représentant x choisi dans G pour décrire sa classe dans G/H.

Si p(x) = p(y), alors

$$\overline{x} = \overline{y} \Rightarrow xy^{-1} \in H$$

$$\Rightarrow f(xy^{-1}) = f(x)f(y^{-1}) = f(x).f(y)^{-1} \in f(H) \subset H'$$

$$\Rightarrow p'(f(x)) = p'(f(y))$$

$$\Rightarrow \tilde{f}(p(x)) = \tilde{f}(p(y))$$

Montrons que $\tilde{f}$ est un morphisme de groupes. On a

$$\tilde{f}(p(x).p(y)) = \tilde{f}(p(x.y)) = p'(f(x.y)) = p'(f(x).f(y)) = p'(f(x)).p'(f(y)) = \tilde{f}(p(x)).\tilde{f}(p(y))$$

■

Théorème 2.4.7 (Deuxième théorème d'isomorphisme)
Soient G un groupe, N et H deux sous-groupes de G avec N distingué dans G. Alors, les groupes quotients $H=H\cap N$ et $HN=N$ existent et on a $H=H\cap N$ et $HN=N$ sont isomorphes, $H=H\cap N\simeq HN=N$.

Preuve. Rappelons que d'après la proposition (2:3:11) précédente, on a NH est un groupe, puisque N est normal dans G. Remarquons que N est aussi un sous-groupe normal de NH et on aussi $N\cap H$ est un sous groupe normal de H. Par conséquent $H=H\cap N$ et $NH=N$ sont des groupes existent.

Or $H\cap N$ (resp. N) est normal dans H (resp. NH), alors on peut dé...nir les morphismes canoniques (surjections canoniques) suivantes

$$\begin{cases} p : H \to H=H\cap N \\ p' : NH \to NH=N \end{cases}$$

Dé...nissons le morphisme (de l'inclusion) suivant

$$i : H \to NH$$

On a donc

$$H \xrightarrow{i} NH \xrightarrow{p'} NH=N$$

On obtient

$$p' \circ i : H \to NH=N$$

Montrons que $p' \circ i$ est surjectif. Soit $x \in NH=N$. Comme p' est surjectif, alors

$$\exists n \in N; \exists h \in H : p'(nh) = x$$

Mais,

$$p'(n.h) = p'(n).p'(h) = \bar{e}.p'(h) = p'(h) \text{ (car } n \in N \subset NH)$$

On a donc

$$(p' \circ i)(h) = p'(i(h)) = p'(h) = p'(n.h) = x$$

Donc, on a bien que $p' \circ i$ est surjectif. Par le premier théorème d'isomorphisme, on a

$$H=\ker(p' \circ i) \simeq NH=N$$

Il reste juste à montrer que

$$\ker(p' \circ i) = H \cap N$$

On sait que

$$e_{NH/N} = \bar{e} = N$$

Alors

$$\ker(p' \circ i) = \{h \in H : (p' \circ i)(h) = e_{NH/N} = \bar{e} = N\}$$

$$\Rightarrow \ker(p' \circ i) = \{h \in H : (p'(i(h)) = N\}$$

$$\Rightarrow \ker(p' \circ i) = \{h \in H : p'(h) = N\}$$

$$\Rightarrow \ker(p' \circ i) = \{h \in H : h \in N\}$$

Alors

$$\ker(p' \circ i) = H \cap N$$

On a donc

$$H/H \cap N \simeq HN/N$$

■

Exemple 2.4.8 Soient $a, b \in Z$ et $d = PGCD(a, b); m = PPCM(a, b)$. Comme

$$aZ \cap bZ = mZ$$
$$aZ + bZ = dz$$

Le second théorème d'isomorphisme donne

$$aZ/mZ = aZ/(aZ \cap bZ) \simeq (aZ + bZ)/bZ = dZ/bZ$$

Remarque 2.4.9 Soient G un groupe, K un sous-groupe normal de G et H un sous-groupe normal de G inclus dans K. Alors K/H est un sous-groupe normal de G/H.

$$K/H \triangleleft G/H$$

Autrement dit les sous groupes distingués de G/H sont de la forme K/H:

Théorème 2.4.10 (Troisième théorème d'isomorphisme)
Soient G un groupe, H et K des sous groupes de G. On suppose que $H \triangleleft G$ et que $K \triangleleft G$. On suppose de plus que $H \subset K$. Alors

$$(G/H)/(K/H) \simeq G/K$$

Preuve. On a H et K sont des sous-groupes normaux de G alors les groupes quotients G=H et G=K existent. D'après la remarque précédente, le groupe quotient (G=H)=(K=H) existe. Dé…nissons les surjections canoniques suivantes

$$p_1 : \begin{array}{ccc} G & \to & G/H \\ x & \to & p_1(x) = x = xH \end{array} ; \quad p_2 : \begin{array}{ccc} G & \to & G/K \\ x & \to & p_2(x) = x = xK = \end{array}$$

Soit g un élément de G. Notons $\bar{x}$ sa classe d'équivalence dans G=H et $\bar{\bar{x}}$ sa classe d'équivalence dans G=K. Soit f la correspondance de G=H dans G=K dé…nie par

$$\forall g \in G : f(gH) = gK \Leftrightarrow \forall g \in G : f(\bar{g}) = \bar{\bar{g}}$$

1) Montrons que f est une application : soient g et g' deux éléments de G véri…ant que

$$gH = g'H$$

On a alors $g^{-1}g' \in H$. Mais H est inclus dans K donc $g^{-1}g' \in K$. D'où

$$gK = g'K$$

et donc

$$f(gH) = f(g'H)$$

f est une application.

2) Montrons que f est un morphisme : soient g et g' appartenant à G. Alors

$$f((gH).(g'H)) = f(gg'H) = gg'K = gK.g'K = f(gH).f(g'H)$$

donc f est un morphisme de groupes.

Il est clair f est surjective.

Donc, on a bien que f est surjectif. Par le premier théorème d'isomorphisme, on a

$$(G=H) = (\ker f) \times \mathrm{Im}(f) = G=K$$

Cherchons le noyau de f. On a

$$\begin{aligned}\ker f &= \{gH : f(gH) = \bar{e} = K; g \in G\} \\ &= \{gH : gK = K; g \in G\} \\ &= \{gH : g \in K\} \\ &= \{kH : k \in K\} \\ &= K/H\end{aligned}$$

D'où, d'après le Premier Théorème d'isomorphisme, $(G/H)/(K/H)$ est isomorphe à G/K. ■

Bibliographie

[1] Azzouz Cherrabi, Elmostafa Jabbouri, Algèbre 4 structures algébriques. Université Mohamed V- Agdal Faculté des Sciences Département de Mathématiques Avenue Ibn Batouta, B.P. 1014, Rabat Maroc. 2007-2008.

[2] Cheikh Thiécoumba Gueye, Groupes et Corps ...nis, Cours d'Algèbre de Licence Mathématiques. Laboratoire d'Algèbre de Cryptographie de Géométrie Algébrique et Applications (LACGAA) Dept Maths et Info- FST-UCAD. 2013.

[3] Daniel Guin ,Thomas Hausberger, Algèbre, groupes, corps et théorie de Galois, tome1. Collection enseignement Sup mathématiques. EDP Sciences, Les Ulis Cedex A, France.

[4] D. Schaub, Eléments de la théorie des groupes. Licence de mathématiques Université d'Angers. 1997/98.

[5] Jean Marie Monier, Algèbre I cours et 600 exercices corrigés, 1ere année MPSI, PCSI, PTSI. 2eme édition DUNOD, Paris, 2000.

[6] Laurent SMOCH, Algèbre - Semestre 2. Licence 1 Sciences & Technologies, Université du Littoral - Côte d'Opale, La Citadelle, Janvier 2009.