CHAPITRE 1

# Introduction sur l'histoire de l'Algèbre

L'Algèbre c'est l'étude des régles de calcul avec des opérations définies sur des ensembles. Ces régles définissent, en particulier, des structures abstraites, telles que les groupes, les anneaux, les corps, les espaces vectoriels, les structures quotients et les formes quadratiques. Dans la suite je vais donner un survol historique sur l'origine de l'Algèbre, des Groupes et de l'Algèbre linéare.

1. Dans son livre " Hissab al gabre oua al moukabala", le Mathématicien Alkhawarizmi a introduit pour la première fois le mot " algèbre". Dans ce dernier livre, Alkhawarizmi avait donné des régles de calcul des racines de la majorité des équations du second degré. Il a en plus montré dans un deuxième livre, comment avec les chiffres $0$, $1$, $2$, $3$, $4$, $5$, $6$, $7$, $8$ et $9$ on peut faire tous les calculs.
Après Alkhawarizmi, plusieurs mathématiciens Arabes et des Mathématiciens d'Europe ont contribué au développement de l'Algèbre.

2. Dans une note écrite par Galois, le 29 Mai 1832, dans la nuit qui a précédé le jour du duel de sa mort, on trouve pour la première fois le mot "groupe". Cette note a été écrite sur la marge de son manuscript sur " la résolubilité des équations par radicaux". C'est le manuscript qu'il a présenté trois fois pour publication sans succès.
Le premier qui a donné une définition axiomatique des groupes était Kayley en 1854. Après ces travaux, on trouve dans un premier temps, ceux de Liouville, Cauchy, Abel, Burnside et ensuite beaucoups d'autres.

3. Les premières notions d'Algèbre linéaire ont vu le jour avec les travaux de Bolzano(1804), Mobius(1827) et surtout Hamilton(1833) lorsqu'il a representé l'ensemble des nombres complèxes comme étant un espace vectoriel de dimension $2$ sur l'ensemble des réels.
Les premières définitions axiomatiques des espaces vectoriels, ont été donné en 1844 par Grassmann et en 1853 par Cauchy. En suite, en 1857 Kayley avait introduit l'Algèbre des matrices qui a été une partie très utile pour la résolution des systèmes d'équations linéaires. En 1867, Laguerre avait écrit une lettre à

Hermite sur le calcul des systèmes linéaires. Ces systèmes linéaires était représenté par des tables des coefficients des systèmes linéaires; sur lesquelles Laguerre avait défini l'addition, la soustraction et la multiplication. Après ces travaux on trouve d'autres travaux comme ceux de Peano en 1888 et bien d'autres après. C'est ainsi que l'Algèbre linéaire a fait ses premiers pas, mais son grand dévelopement est réalisé au cours du vinghtième ciècle.

4. Actuellement, l'Algèbre est devenu un vaste domaine de recherches et d'applications. Plusieurs options algébriques ont vu le jour comme la théorie algébrique des nombres, l'Algèbre commutatif, l'Algèbre non associative, la K-théorie, l'Homologie, la Cohomologie et bien d'autres.
Plusieurs domaines scientifiques reposent sur L'Algèbre tel que l'Analyse, la Physique, la Chimie, la Biologie, l'Informatique, la Télécommunication, l'Economie et d'autres. D'où l'importance d'assimiler les notions de bases d'Algèbre qu'on va voir dans la suite de ce livre.

CHAPITRE 2

# Rappel sur les groupes

## 1. Raisonnement par récurence

Soient $\mathbb{N}$ l'ensemble des entiers naturels et $I$ une partie de $\mathbb{N}$, alors $I$ possède un plus petit élément. Parmi les méthodes de raisonnement utilisé en mathématique on trouve le raisonnement par récurence. Il existe deux formes de raisonnement par récurence: la récurence et la récurence complète.

**Récurence:**

Soient $m$ un entier fixe et $P(n)$ une propriété définie pour tout entier $n$ plus grand que $m$. Si $P(m)$ est vrai, $P(m+1)$ est vrai et si pour tout $i$ plus grand que $m$, $P(i)$ vrai entraîne que $P(i+1)$ est vrai, alors $P(n)$ est vrai pour tout entier $n$ plus grand que $m$.

**Récurence Complète:**

Soient $m$ un entier fixe et $P(n)$ une propriété définie pour tout entier $n$ plus grand que $m$. Si $P(m)$ est vrai, $P(m+1)$ est vrai et si pour tout $j$ plus grands que $m$ on a, si $P(i)$ vrai pour tout $i$ tels que $i < j$ entraîne que $P(j)$ est vrai, alors $P(n)$ est vrai pour tout entier $n$ plus grand que $m$.

Nous aurons l'occasion d'utiliser ce dernier principe de récurence dans les chapitres qui vont suivre.

## 2. Généralités sur les Groupes

Soient $G$ un ensemble munie d'une loi de composition interne notée $*$ et $H$ un sous-ensembles de $G$.

1) On dit que $(G,*)$ est un groupe si et seulement si les trois conditions suivantes sont vérifiées:

i) Pour tout $x$, tout $y$ et tout $z$ de $G$, on a $(x*y)*z = x*(y*z)$. Si cette condition est satisfaite on dit que $*$ est associative.

ii) Il existe un élément $e$ de $G$ tel que pour tout $x$ de $G$ on a $e*x = x*e = x$. Cet élément est appelé l'élément neutre de $G$.

iii) Pour tout $x$ de $G$, il existe $y$ dans $G$ tel que $x*y = y*x = e$. L'élément $y$ est appelé l'inverse de $x$ ou bien le symétrique de $x$.

Si de plus, pour tout $x$ de $G$ et tout $y$ de $G$ on a $x*y = y*x$; on dit que $(G,*)$

est un groupe abélien.
2) On dit que $H$ est un sous-groupe de $G$ si et seulement si:
- il contient l'élément neutre,
- pour tout $x$ et tout $y$ de $H$, $x * y$ et l'inverse de $x$ appartiennent à $H$.

**Exemples**
a) Soient $Z$ l'ensemble des entiers relatifs et $+$ l'addition dans $Z$; alors $(Z, +)$ est un groupe abélien. On vérifie facilement que tout sous-groupe de $Z$ est de la forme $nZ$ où $n$ est entier naturel.
b) Soient $G$ un groupe et $x$ un élément de $G$. Soient $x^n = x * x^{n-1}$ et $y = x^{-1}$ l'inverse de $x$. L'ensemble $H$ constitué des éléments de la forme $x^n$ ou bien de la forme $y^n$ avec $x^0 = e$ et $n$ un entier naturel; est un sous-groupe de $G$. On dit que $H$ est un sous-groupe cyclique engendré par $x$.
c) Soient $G$ un groupe et $x$ un élément de $G$. Si $G$ possède un nombre fini d'éléments on dit que $G$ est un groupe fini et que le nombre de ses éléments est l'ordre de $G$. Si $G$ est un groupe fini, alors il existe un entier $n$ tel que $x^n = e$; le plus petit des entiers $n$ vérifiant $x^n = e$ est appelé l'ordre de $x$.
Ainsi un groupe d'ordre $2$, $3$ ou $5$ est cyclique tandis qu'un groupe d'ordre $4$ est cyclique ou bien tout éléments de $G$ autre que l'élément neutre est d'ordre $2$. Un groupe d'ordre $4$ qui n'est pas cyclique est dit de Klein.
d) Soit $S_n$ l'ensemble des permutations des entiers naturels de $1$ à $n$. Muni de la composition des applications, $S_n$ est un groupe qui n'est pas abélien pour $2 < n$ et son ordre est gal à $n!$. Ainsi $S_3$ est un groupe d'ordre $6$ et il n'est pas abélien. Tout groupe dont l'ordre est inférieur ou égal à $5$ est abélien.
Dans toute la suite sauf mention du contraires, on notera multiplicativement les loi de composition des groupes utilisés.
e) Soient $G$ un groupe et $S = \{a_1, a_2, ..., a_n\}$ une partie de $G$. L'ensemble des éléments de $G$ qui sont produit d'éléments de $S$ et des inverses des éléments de $S$, est un sous-groupe; qu'on appelle sous-groupe engendré par $S$. Le groupe $S_n$ des pérmutaion est engendré par les transpositions.
f) Soient $G$ un groupe dont la loi est noté $*$ et $H$ un autre groupe muni d'une loi noté $\circ$. Soit $G \times H$ le produit cartésien des deux ensembles $G$ et $H$; qu'on muni de la loi $(*, \circ)$ définie par

$$(g, h)(*, \circ)(g', h') = (g * g', h \circ h').$$

Alors muni de cette loi $G \times H$ est un groupe.
g) Soient $G$ un groupe fini et $a$ et $b$ deux éléments de $G$ tels que $ab = ba$, alors l'ordre de $ab$ est égal à l'ordre de $a$ multiplié par l'ordre de $b$ divisé par le plus grand commun diviseur des deux ordres:

$$ord(ab) = \frac{ord(a) \times ord(b)}{p.g.c.d(ord(a), ord(b))}.$$

THÉORÈME 1. *Théorème de Lagrange.*
*Soient $G$ un groupe fini et $H$ un sous-groupe de $G$; alors l'ordre de $H$ divise l'ordre de*

*$G$. De plus si $R_d$ est la relation d'équivalence définie comme suit : $xR_dy \Leftrightarrow y \in Hx$, alors $\mid G/R_d \mid = \mid G \mid / \mid H \mid$ où $\mid B \mid$ désigne le cardinal de $B$.*

**Preuve.**
Soit $R_d$ la relation d'équivalence définie comme suit : $xR_dy \Leftrightarrow y \in Hx$. Alors $R_d$ est une relation d'équivalence et toute classe modulo $R_d$ est de la forme $Hx$. Par suite deux classes ont un même nombre d'éléments qui est égal à l'ordre de $H$. D'autre part, $G$ est une réunion disjointe de classes d'équivalence; donc le nombre des éléments de $G$ est égal à la somme des nombres d'éléments des classes d'équivalence. Or les classes d'équivalence ont un même nombre d'éléments qui est l'ordre de $H$, donc l'ordre de $H$ divise l'ordre de $G$.

## 3. Homomorphisme de Groupes et Sous-groupe Distingués

Soient $G$ un groupe, $H$ un sous-groupe de $G$ et $R_d$ et $R_g$ les deux relations d'équivalence définies comme suit : $xR_dy \Leftrightarrow y \in Hx$ et $xR_gy \Leftrightarrow y \in xH$.
Le sous-groupe $H$ est distingué dans $G$ si et seulement si $\forall x \in H,\ \forall z \in G,\ zxz^{-1} \in H$. Ceci est équivalent à $\forall z \in G,\ zHz^{-1} = H$ ou encore à $\forall z \in G,\ zH = Hz$. Donc si $H$ est distingué dans $G$, alors les deux relations $R_d$ et $R_g$ coîncident. Ainsi les deux ensembles des classes d'équivalences sont identiques et on note alors $G/R_d = G/R_g = G/H$.

DÉFINITION 1. Soient $G$ et $G^{'}$ deux groupes et $f$ une application de $G$ dans $G^{'}$. On dit que $f$ est un homomorphisme de $G$ dans $G^{'}$ si et seulement si pour tout $x$ et tout $y$ de $G$, on a $f(xy) = f(x)f(y)$. Si de plus $f$ est une bijection, on dit que $f$ est un isomorphisme de groupes. Si $G = G'$, un isomorphisme de $G$ est dit automorphisme de $G$.

**Exemples**
1. Soient $\mathbb{C}$ le corps des nombres complèxes et $f$ l'application de $(\mathbb{C}, +)$ vers $(\mathbb{C}^*, \times)$ qui à $x$ fait correspondre $e^x$. Alors $f$ est un homomrphisme de groupes.
2. Soient $G$ et $G^{'}$ deux groupes et $f$ un homomorphisme de $G$ dans $G^{'}$. Soient $e'$ l'élément neutre de $G'$ et $Ker(f)$ le noyau de $f$: l'ensemble des $x$ de $G$ tel que $f(x) = e'$; alors $Ker(f)$ est un sous-groupe distingué de $G$.
3. Soient $A_n$ l'ensemble des permutations paires de $S_n$ et $f$ l'application de $S_n$ dans $\{1, -1\}$ qui à $\sigma = \tau_1\tau_2...\tau_r$ fait correspondre $(-1)^r$ où $\sigma = \tau_1\tau_2...\tau_r$ est une décomposition de $\sigma$ en produit de transpositions. Alors $A_n = Ker(f)$ et $A_n$ est distingué dans $S_n$.
4. Soient $G$ un groupe, $a$ un élément de $G$ et $H$ un sous-groupe distingué de $G$; on définit une application $f_a$ de $H$ dans $H$ par: $f_a(x) = axa^{-1}$; alors $f_a$ est un automorphisme de $H$.
5. Soient $G$ un groupe et $H$ un sous-groupe de $G$ tel que $G/R_d$ est d'ordre $2$, alors $H$ est un sous-groupe distingé de $G$.

CHAPITRE 3

# LES GROUPES QUOTIENTS

## 1. Ensembles quotients

Soient $E$ et $F$ deux ensembles, $f$ une application de $E$ dans $F$ et $R$ une relation d'équivalence sur $E$. L'ensemble des classes d'équivalences modulo $R$ s'appelle l'ensemble quotient de $E$ par $R$ ; on le note par $E/R$. L'application $p$ de $E$ dans $E/R$ qui à tout $x$ de $E$ fait correspondre $\overline{x}$ est une surjection qu'on appelle la surjection canonique ou la projection canonique.

PROPOSITION 1. *On garde les notations précédentes ; alors il existe une application $\overline{f}$ de $E/R$ dans $F$ telle que $f = \overline{f} \circ p \Longleftrightarrow \forall (x,y) \in E^2,\ xRy \Longrightarrow f(x) = f(y)$.*

**Preuve.**
Si on a $f = \overline{f} \circ p$ alors $xRy \Longleftrightarrow \overline{x} = \overline{y} \Longrightarrow \overline{f}(\overline{x}) = \overline{f}(\overline{y})$
d'où

$$f(x) = f(y).$$

Inversement. Soit $\overline{y} \in E/R$, on pose $\overline{f}(\overline{y}) = f(y)$. La fonction $\overline{f}$ est bien une application car :
$\overline{x} = \overline{y} \Longleftrightarrow xRy \Longrightarrow f(x) = f(y)$ donc $\overline{f}(\overline{x}) = \overline{f}(\overline{y})$. ∎

DÉFINITION 2. On dit que la relation $R$ est compatible avec l'application $f$ si et seulement si:
$\forall (x,y) \in E^2,\ xRy \Longrightarrow f(x) = f(y)$.
A toute application $f$ on associe une relation $R_f$ définie par:
$xR_fy \Longleftrightarrow f(x) = f(y)$.
$R_f$ est dite relation d'équivalence associée à $f$.

**Corrolaire** Toujours avec les mêmes notations, soit $R_f$ la relation d'équivalence associée à $f$. Alors il existe une application $\overline{f}$ injective de $E/R_f$ dans $F$ telle que : $f = \overline{f} \circ p$.
**Preuve.**
L'application $\overline{f}$ existe d'après la proposition précédente. De plus on a:
$\overline{x} = \overline{y} \Longleftrightarrow xR_fy \Longleftrightarrow f(x) = f(y) \Longleftrightarrow \overline{f}(\overline{x}) = \overline{f}(\overline{y})$. D'où $\overline{f}$ est injective.
**Exemple.**

$\phi : (\mathbb{R}, +) \to (\mathbb{C}^*, .)$
$x \mapsto e^{ix}$
Alors on a $\mathbb{R}/ker\phi \simeq Im\phi \Leftrightarrow \mathbb{R}/2\pi\mathbb{Z} \simeq \{\mathsf{z} \in \mathbb{C} \,/\, |\mathsf{z}| = 1\}$.

## 2. Groupes quotients

Soient $G$ un groupe, $H$ un sous-groupe de $G$ et $R_d$ et $R_g$ les deux relations d'équivalence définies comme suit : $xR_dy \Leftrightarrow y \in Hx$ et $xR_gy \Leftrightarrow y \in xH$
On sait que :
$H$ est distinguée $\Leftrightarrow \forall x \in H,\ \forall z \in G,\ \ zxz^{-1} \in H \quad \Leftrightarrow \forall z \in G\ zHz^{-1} = H$
$\Leftrightarrow \forall z \in G\ zH = Hz \quad \Leftrightarrow$ Les deux relations $R_d$ et $R_g$ coincident.
Ainsi $G/R_d = G/R_g = G/H$.
Soient $xH$ et $yH$ deux éléments de G/H, on définit :

$$xH.yH = x.yH.$$

On a bien une loi de composition interne, en effet :
Si $x^{'}H = xH$ et $y^{'}H = yH$ on a $x = x^{'}h$ et $y = y^{'}h^{'}$, donc $xy = x^{'}h.y^{'}h^{'} = x^{'}y^{'}h^{''}h^{'}$ où $hy^{'} = y^{'}h^{''}$ car $Hy^{'} = y^{'}H$. Donc $x.yH = x^{'}y^{'}h^{''}h^{'}H = x^{'}y^{'}H$.
On vérifie facilement la proposition suivante.

PROPOSITION 2. *Soient $G$ un groupe et $H$ un sous-groupe distingué de $G$. Alors $G/H$ est munie d'une structure de groupe. On dit alors que $G/H$ est le groupe quotient de $G$ par $H$.*

DÉFINITION 3. Soit $R$ une relation d'équivalence définie sur $G$ ; on dit que $R$ est compatible avec la loi du groupe $G$ si et seulement si :
$\forall (x, y, z) \in G^3\ xRy \Rightarrow\ x.zRy.z$ et $z.xRz.y$. Ceci est encore équivalent à $\forall (x, y) \in G^2,\ \forall (x^{'}, y^{'}) \in G^2,\ xRy$ et $x^{'}Ry^{'} \Rightarrow x.x^{'}Ry.y^{'}$.

PROPOSITION 3. *Soient $G$ un groupe et $R$ une relation d'équivalence définie sur $G$. Alors $R$ est compatible avec la loi de $G \Leftrightarrow$ la classe $H$ de l'élément neutre est un sous-groupe distingué de $G$ et $R$ est définie par :*

$$xRy \Leftrightarrow y \in Hx = xH.$$

**Preuve.**
On suppose que $R$ est compatible avec la loi de $G$, alors $H = \{x \in G / xRe\}$ est un sous-groupe de $G$. De plus si $x \in H$ alors $xRe \Rightarrow \forall z \in G,\ \ z.xRz \Rightarrow z.x.z^{-1}Rz.z^{-1} \Rightarrow z.x.z^{-1}Re \Rightarrow zxz^{-1} \in H$. Donc $H$ est distinguée et on a $xRx^{'} \Leftrightarrow x.x^{'-1}Re \Leftrightarrow x.x^{\prime-1} \in H \Leftrightarrow x' \in Hx = xH$. Inversement si $xRy$ alors $x.y^{-1} \in H$. Comme $H$ est distingué alors $\forall z,\ z.x.y^{-1}.z^{-1}Re \Rightarrow zx \in Hzy \Rightarrow$

$zxRzy$. De même si $xRy$ alors $x.y^{-1}Re$, donc $x.z.z^{-1}.y^{-1} = x.z.(y.z)^{-1} \in H$. Par suite $x.z \in Hy.z$ et donc $x.zRy.z$. D'où la compatibilité.

THÉORÈME 2. *( 1er th. d'isomorphisme)*
*Soient $G$ et $G^{'}$ deux groupes, $f$ un homomorphisme de $G$ dans $G^{'}$, $p$ la surjection canonique de $G$ dans $G/kerf$ et $i$ l'injection canonique de $f(G)$ dans $G^{'}$ alors il existe un isomorphisme $\overline{f}$ de $G/kerf$ dans $f(G)$ tel que :*

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

Preuve. $G/kerf$ est l'ensemble quotient de $G$ par la relation $R$ définie par :
$xRy \Leftrightarrow xy^{-1} \in Kerf \Leftrightarrow f(x) = f(y)$, donc $R$ est la relation d'équivalence associée à $f$. Par suite il existe $\overline{f_1}$ telle que $f = \overline{f_1} \circ p$ où :

$$\overline{f_1} : G/Kerf \to G^{'}$$

$$\overline{x} \to f(x)$$

Soit $\overline{f}$ de $G/kerf$ dans $f(G)$ qui à $\overline{x}$ fait correspondre $f(x)$. Alors $\overline{f}$ est un isomorphisme de groupe et $\overline{f_1} = i \circ \overline{f}$, d'où $f = i \circ \overline{f} \circ p$.
**Remarque**: On obtient une décomposition semblable à celle de la proposition 1, si on remplace $Kerf$ par un sous-groupe distingué $N$ de $G$ tel que $N \subset Kerf$. Mais dans le Théorème précédent, $\overline{f}$ n'est injective que si $N = Ker(f)$.

## 3. Théorèmes d'isomorphismes

PROPOSITION 4. *Soient $G$, $G^{'}$ et $G^{''}$ 3 groupes, $f$ un homomorphisme de $G$ dans $G^{'}$ et $g$ un homomorphisme surjectif de $G$ dans $G^{''}$; alors il existe un homomorphisme $\phi$ de $G^{''}$ dans $G^{'}$ tel que: $f = \phi \circ g$ si et seulement si $Kerg \subset Kerf$.*

Preuve.
La première implication est évidente; inversement soit $y \in G^{''}$; comme $g$ est surjective, il existe $x \in G$ tel que $y = g(x)$. On pose : $\phi(y) = f(x)$. Montrons que $\phi$ est une application.
Si $y = g(x) = g(x')$ alors $g(x).g(x')^{-1} = e'' = g(x.x'^{-1}) = e'' \Rightarrow x.x'^{-1} \in Kerg$.
D'où $x.x'^{-1} \in Kerf \Rightarrow f(x.x'^{-1}) = e' \Rightarrow f(x) = f(x')$. Donc $\phi(y) = \phi(y')$.
Donc $\phi$ est bien une application. On vérifie aussi que $\phi$ est un homomorphisme de groupe: si $y = g(x)$ et $y' = g(x')$; alors $\phi(y.y') = f(x.x') = f(x).f(x') = \phi(y).\phi(y')$.

PROPOSITION 5. *Soient $G$ un groupe et $H$ et $K$ deux sous-groupes de $G$. Alors on a :*
*1) $HK$ est un sous-groupe de $G$ si et seulement si $HK = KH$.*
*2) Si $H$ est un sous-groupe distingué de $G$ alors $HK$ est un sous-groupe de $G$.*
*3) Si $H$ est un sous-groupe distingué de $G$ alors $H \cap K$ est distingué dans $K$.*

Preuve.
1) On suppose que $HK$ est un sous-groupe de $G$, montrons que $HK = KH$.
Soit $h.k \in H.K$, puisque $H.K$ est un sous-groupe on a $k^{-1}h^{-1} \in HK \Rightarrow k^{-1}h^{-1} = h'k' \Rightarrow hk = k'^{-1}h'^{-1} \in KH$; donc $HK \subset KH$.
Soit $kh \in KH$, on a $h^{-1}k^{-1} \in HK \Rightarrow (h^{-1}k^{-1})^{-1} \in HK \Rightarrow kh \in HK$ d'où $KH \subset HK$.
Inversement, soient $hk$, $h'k' \in HK$. On a :
$a = hk.(h'k')^{-1} = hk.(k'^{-1}h'^{-1}) = hk''h'^{-1}$ ou $k'' = kk'^{-1}$, $k''h'^{-1} = h''k'''$ d'où $a = h.h''k''' \in HK$. Ceci entraine que $HK$ est un sous-groupe de $G$.
2) Si $H$ est distingué dans $G$ alors $HK$ est un sous-groupe de $G$:
pour cela, montrons que $HK = KH$.
Comme $H$ est distingué alors $\forall k \in K$ on a $kH = Hk$, d'où $HK = KH$.
3) Soient $x \in H \cap K$ et $k \in K$ on a :
$kxk^{-1} \in K$ et puisque $H$ distingué on a $kxk^{-1} \in H$; donc $kxk^{-1} \in H \cap K$, d'où $H \cap K$ est un sous-groupe distingué de $K$.

THÉORÈME 3. *(2**ème** **th. d'isomorphisme** )*
*Soient $G$ un groupe, $H$ un sous-groupe distingué de $G$ et $K$ un sous-groupe de $G$ alors $K/H \cap K \simeq H.K/H$.*

Preuve.
Comme $H$ est un sous-groupe distingué de $G$, alors $H.K$ est un sous-groupe de $G$. Donc $H$ est un sous-groupe distingué de $H.K$.
Soit

$$p : K \longrightarrow H.K/H$$
$$x \longrightarrow \overline{x} = H.x$$

$p$ est un homomorphisme surjectif, d'où $K/Kerp \simeq H.K/H$.
$Kerp = \{x \in K/H.x = H\} = \{x \in K/x \in H\} = K \cap H$. Par suite $K/K \cap H \simeq H.K/H$

THÉORÈME 4. *(3**ème** **th. d'isomorphisme** )*
*Soient $G$ un groupe, $H$ et $K$ deux sous-groupes distingués de $G$ tels que $H \subset K$; alors $G/K \simeq (G/H)/(K/H)$.*

Preuve.
Soit $p$ la surjection canonique de $G$ dans $G/H$ et $p'$ la surjection canonique de $G$

dans $G/K$. Comme $Ker(p) \subset Ker(p')$, alors d'après la proposition 4, il existe une application $\phi$ de $G/H$ dans $G/K$ tel que $p' = \phi \circ p$.
L'application $\phi$ est l'application qui à $xH$ fait correspondre $xK$. Il est claire que $\phi$ est une surjection. De plus, $Ker\phi = \{xH/xK = K\} = \{xH/x \in K\} = K/H$.
D'où $K/H$ est un sous-groupe distingué de $G/H$ et $(G/H)/(K/H) \simeq G/K$.

THÉORÈME 5. *(4***ème** **th. d'isomorphisme ou th. de correspondance)**.
*Soient $G$ un groupe et $H$ un sous-groupe distingué de $G$ et $T$ un sous-groupe de $G/H$, alors il existe un sous-groupe $R \supset H$ tel que $T = R/H$.*

Preuve.
Soient $p$ la surjection canonique de $G$ vers $G/H$ et $R = p^{-1}(T)$. Alors $R$ est un sous-groupe de $G$ qui contient $H$ et on a : $T = R/H$
**Exercice :** Montrer que $R/H$ est un sous-groupe distingué de $G/H \Leftrightarrow R$ est un sous-groupe distingué de $G$.
**Applications :**
1. Sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ . D'après le théorème de correspondance les sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $R/n\mathbb{Z}$ où $R$ est un sous-groupe de $\mathbb{Z}$ tel que $n\mathbb{Z} \subset R$. Comme $R$ est un sous groupe de $\mathbb{Z}$ alors $R = d\mathbb{Z}$ et puisque $n\mathbb{Z} \subset R$ alors $d/n$. Par suite les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont $d\mathbb{Z}/n\mathbb{Z}$ où $d/n$.
2. Soient $m$, $n$ et $d$ des entiers naturels tels que $m = nd$, $n$ et $d$ sont premiers entre eux et $\phi$ l'application de $\mathbb{Z}$ dans $d\mathbb{Z}/m\mathbb{Z}$ qui fait correspondre à $i$ la classe de $di$. Alors $\phi$ est une surjection et $Ker\phi = n\mathbb{Z}$. Par suite on a

$$d\mathbb{Z}/m\mathbb{Z} = d\mathbb{Z}/nd\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}.$$

CHAPITRE 4

# Complèment sur les groupes

## 1. Groupe opérant sur un ensemble

DÉFINITION 4. Soient $G$ un groupe et $E$ un ensemble; une opération de $G$ sur $E$ est une application, qu'on note par ., de $G \times E$ dans $E$ telle que :

$$\begin{aligned} . \ G \times E &\to E \\ (g, x) &\mapsto g.x \end{aligned}$$

i) $\forall (g_1, g_2) \in G^2, \ \forall x \in E, (g_1 g_2).x = g_1.(g_2.x)$,
ii) si $e$ est l'élément neutre de $G$ alors: $\forall x \in E, \ e.x = x$.
On dit que $G$ opère à gauche sur $E$ si et seulement si il existe une opération de $G$ sur $E$; on dit alors que $E$ est un G-ensemble.

PROPOSITION 6. *Soient $G$ un groupe et $E$ un ensemble alors; $E$ est un G-ensemble $\Leftrightarrow$ il existe un homomorphisme $T$ de $G$ dans le groupe symétrique $S(E)$ de $E$.*

Preuve.
* Si $G \subset S(E)$ on définit une opération naturelle de $G$ sur $E$ par:

$$\begin{aligned} G \times E &\to E \\ (g, x) &\mapsto g.x = g(x) \end{aligned}$$

En effet, on a bien une application et:
- $\forall (g_1, g_2) \in G^2, \ \forall x \in E, \ (g_1 \circ g_2).x = (g_1 \circ g_2)(x) = g_1(g_2(x)) = g_1.g_2(x) = g_1.(g_2.x)$,
- $Id.x = Id(x) = x$.
* On suppose qu'il existe un homomorphisme $T$ de $G$ dans $S(E)$; on définit une opération de $G$ sur $E$ par:

$$\begin{aligned} . \ G \times E &\to E \\ (g, x) &\mapsto g.x = T(g)(x). \end{aligned}$$

La fonction . est bien une application et de plus:
- $\forall (g_1, g_2) \in G^2,\ \ \forall x \in E,\ \ (g_1 g_2).x = T(g_1 g_2)(x) = ((T(g_1)) \circ (T(g_2))(x) = T(g_1)(T(g_2)(x)) = g_1.(T(g_2)(x)) = g_1.(g_2.x)$,
- $\forall x \in E,\ \ e.x = T(e)(x) = Id(x) = x$.
Donc l'application qu'on vient de définir est bien une opération et $E$ est un G-ensemble.
* Inversement, on suppose que $G$ opère sur $E$. Soit $T$ définie par :

$$\begin{aligned} T:\ G &\to S(E) \\ g \mapsto T(g) = T_g &: E \to E \\ x &\mapsto g.x \end{aligned}$$

- $T_g$ est bien une bijection : En effet si $g.x = g.x' \Rightarrow g^{-1}.(g.x) = g^{-1}.(g.x')$
Donc $(g^{-1}g).x = (g^{-1}g).x' \Rightarrow e.x = e.x' \Rightarrow x = x'$. Ainsi $T_g$ est une injection de plus elle est surjective car:
$\forall y \in E,\ \ y = g.(g^{-1}.y) = T_g(g^{-1}.y)$.
Donc $T$ est bien une application de $G$ dans $S(E)$.
- $T$ est un homomorphisme de groupe :
$\forall (g_1, g_2) \in G^2, T(g_1 g_2)(x) = (g_1 g_2).x = g_1.(g_2.x) = T_{g_1}(g_2.x) = T_{g_1}(T_{g_2}(x)) = T_{g_1} \circ T_{g_2}(x)$.
Par suite, $T(g_1 g_2) = T_{g_1} \circ T_{g_2}$.

DÉFINITION 5. Si l'homomorphisme précédent $T$ est injectif, on dit alors que $G$ opère fidèlement sur $E$.

**Exemples :**
1) Soient $E = \{1, 2, 3, \cdots, n\}$ et $G = S_n$ le groupe symétrique de $E$ . Alors $G$ opère sur $E$ et l'opération est définie comme suit :

$$\begin{aligned} G \times E &\to E \\ (\sigma, p) &\mapsto \sigma(p) \end{aligned}$$

2) Soient $G$ un groupe et $N$ un sous-groupe distingué de $G$; alors $G$ opère sur $N$ de la façon suivante :

$$\begin{aligned} . \ G \times N &\to N \\ (g, n) &\mapsto g.n = gng^{-1}. \end{aligned}$$

La fonction . est bien une application et vérifie les deux propriétés i et ii).
3) Soit $G$ un groupe, alors $G$ opère sur lui même et l'opération est définie par :

$$\begin{aligned} . \ G \times G &\to G \\ (g, x) &\mapsto gxg^{-1} = g.x. \end{aligned}$$

La fonction . est bien une opération car c'est une application et de plus :
- $\forall (g_1, g_2) \in G^2, \ \ \forall x \in G$ :
$g_1.(g_2.x) = g_1.(g_2 x g_2^{-1}) = g_1.(g_2 x g_2^{-1}) g_1^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1} = (g_1 g_2).x$,
- $\forall x \in G, \ e.x = exe = x$.
Donc . est bien une opération qu'on appelle conjugaison. On dit que $G$ opère sur lui même par conjugaison.
4) Soient $G$ un groupe et $A$ l'ensemble de tous les sous-groupes de $G$ ; alors $G$ opère sur $A$ de la façon suivante :

$$\begin{aligned} . \ G \times A &\to A \\ (g, N) &\mapsto gNg^{-1} \end{aligned}$$

La fonction . est bien une opération.
**Orbite d'un élément**
Soit $E$ un G-ensemble. On définit sur $E$ une relation $T$ par :
$xTy \Leftrightarrow y \in G.x = \{g.x / g \in G\}$ ; $T$ est une relation d'équivalence. On appelle orbite de $x$ la classe d'équivalence $O_x$ de $x$ modulo T et on a $O_x = G.x$.
**Exemple:**
On prend le cas où $G$ opère sur lui même par conjugaison ; alors pour tout $x$, $O_x = \{gxg^{-1} / g \in G\}$. Si l'élément $x$ commute avec tout élément de $G$ alors $O_x = \{x\}$.
L'ensemble $C$ des éléments de $G$ qui commutent avec tout élément de $G$ est un sous-groupe de $G$ qu'on appelle centre de $G$ et qu'on note par $C$ ou par $Z(G)$.
**Stabilisateur d'un élément**
Soient $E$ un G-ensemble et $x$ un élément de $E$, l'ensemble $\sum_x = \{g \in G / g.x = x\}$ est un sous-groupe de $G$ qu'on appelle stabilisateur de $x$.
**Exemples :**
1) Si $G$ opère par conjugaison sur lui même.
$\sum_x = \{g \in G / g.x = x\} = \{g \in G / gxg^{-1} = x\} = \{g \in G / gx = xg\}$. Dans ce cas $\sum_x$ est aussi appelé centralisateur de $x$. D'autre part, l'ensemble des éléments de $G$ qui commutent avec tout élément de $G$ est un sous-groupe de $G$ qu'on note par $Z(G)$ et de plus on a $Z(G) = \cap_{x \in G} \sum_x$.
2) Si $G$ opère sur $A$( l'ensemble de tous les sous groupes de G) par conjugaison alors : $\sum_N = \{g \in G / gNg^{-1} = N\}$, $\sum_N$ est appelée normalisateur de $N$.
3) Soient $S_4$ le groupe des permutations des entiers de $1$ à $4$ et $\Sigma_4$ le stabilisateur de $4$: $\Sigma_4 = \{\sigma \in S_4 | \sigma(4) = 4\}$. Il est clair que $\Sigma_4 \simeq S_3$.

THÉORÈME 6. *Soient $E$ un G-ensemble et $x$ un élément de $E$, alors il existe une bijection entre l'orbite de $x$ et l'ensemble des classes d'équivalence à gauche modulo $\sum_x$.*

Preuve.
Soient $(G/\sum_x)_g$ l'ensemble des classes à gauche de $\sum_x$ et $\phi : (G/\sum_x)_g \longrightarrow$

$O_x = G.x$ qui à $f\sum_x \longmapsto f.x$. On a :
$f\sum_x = f'\sum_x \Leftrightarrow f'^{-1}f \in \sum_x \Leftrightarrow f'^{-1}f.x = x \Leftrightarrow f.x = f'.x$. Donc $\phi$ est une application injective. De plus elle est surjective par construction :
$\forall y \in G.x,\ \exists f \in G \,|\, y = fx \Rightarrow \phi(f\sum_x) = y$. Donc $\phi$ est une bijection.

COROLLAIRE 1. *On suppose de plus que $G$ est fini ; alors pour tout $x$, $O_x$ est fini et $cardO_x$ divise l'ordre de $G$.*

Preuve.
Si $G$ est fini alors $(G/\sum_x)_g$ est fini donc $O_x$ est fini et $cardO_x = [G : \sum_x]$ donc $cardO_x$ divise $|G|$.

COROLLAIRE 2. *Soit $X$ l'ensemble constitué d'un représentant de chaque orbite. On suppose que $E$ est un G-ensemble fini alors :*

$$cardE = \sum_{x\in X}[G : \sum_x].$$

Preuve.
Ceci vient du fait que

$$E = U_{x\in X}O_x \Rightarrow |E| = \sum_{x\in X}|O_x| = \sum_{x\in X}[G : \sum_x].$$

## 2. Applications

**Théorème de Cauchy :**
Soient $G$ un groupe d'ordre $n$ et $p$ un nombre premier divisant $n$ ; alors il existe un élément $x$ de $G$ dont l'ordre est égal à $p$.
Preuve.
* Soit

$$E = \{(x_1, x_2, \cdots, x_p) \in G^p / x_1.x_2....x_p = e\}.$$

On va montrer que le cardinal de $E$ est égal à $n^{(p-1)}$.
Soit

$$f : E \to G^{p-1}$$
$$(x_1, x_2, \cdots, x_p) \mapsto (x_1, x_2, \cdots, x_{p-1})$$

$f$ est bien une application. De plus si on a :
$f(x_1, x_2, \cdots, x_p) = f(x'_1, x'_2, \cdots, x'_p)$
$\Rightarrow (x_1, x_2, \cdots, x_{p-1}) = (x'_1, x'_2, \cdots, x'_{p-1})$
$\Rightarrow x_1 = x'_1,\ \ x_2 = x'_2 = \cdots = x_{p-1} = x'_{p-1}$
De plus comme $x_1.x_2.\cdots.x_p = e$ et $x'_1.x'_2.\cdots.x'_p = e \Rightarrow x_p = x'_p$ donc $f$ est

injective. L'application $f$ est surjective car : $\forall(x_1, x_2, \cdots, x_{p-1}) \in G^{p-1}$ on a :

$$f(x_1, x_2, \cdots, x_{p-1}, x_p) = (x_1, x_2, \cdots, x_{p-1})$$

où $x_p = (x_1.x_2.\cdots.x_{p-1})^{-1}$.
D'où : $cardE = CardG^{p-1} = n^{p-1}$.
* Soit

$$\sigma : E \to E$$

$$(x_1, x_2, \cdots, x_p) \mapsto (x_2, x_3, \cdots, x_p, x_1) \in E.$$

Donc $\sigma$ est une application injective d'où bijective puisque $cardE$ est fini. De plus on a:

$$\sigma^p = idE.$$

Donc l'ordre de $\sigma$ est égal à $1$ ou à $p$.
- Si $Ordre(\sigma) = 1 \Rightarrow \sigma = id \Rightarrow \forall y \in E, \ \ \sigma(y) = y$.
Soit:
$y = (x_1, x_2, \cdots, x_p) \neq (e, e, \cdots, e)$
On a: $\sigma(y) = (x_2, x_3, \cdots, x_p, x_1) = (x_1, x_2, \cdots, x_p)$
Donc

$$x_1 = x_2 = \cdots = x_p = x \neq e.$$

Comme $(x_1, x_2, \cdots, x_p) \in E \Rightarrow x_1.x_2.\cdots.x_p = x^p = e \Rightarrow x$ est d'ordre $p$.
- Si $Ordre(\sigma) = p$, soit $C = \{ide, \sigma, \sigma^2, \cdots, \sigma^{p-1}\} \subset S(E)$.
$C$ opère d'une manière naturel sur $E$, d'où on a :

$$|E| = \sum_{x \in X} |O_x|$$

et $|O_x|$ est un diviseur de l'ordre de $C$ qui est égal à $p$.
Donc on a 2 possibilités : $|O_x| = 1$ ou bien $|O_x| = p$. On suppose qu'il existe $r$ éléments dont le cardinal est égal à 1 et $S$ éléments dont le cardinal est égal à $p$.

$$O(e, e, \cdots, e) = C.(e, e, \cdots, e) = \{(e, e, \cdots, e)\} \Rightarrow r \geq 1.$$

Donc $|E| = r + Sp = n^{p-1}$. On a donc $p/n$ et $n^{p-1} = r + Sp$; ce qui implique $p/r \Rightarrow r \geq p$. Par suite il existe $(x_1, x_2, \cdots, x_p) \in E$ tel que :
$(x_1, x_2, \cdots, x_p) \neq (e, e, \cdots, e)$ et
$O(x_1, x_2, \cdots, x_p) = C.(x_1, x_2, \cdots, x_p) = \{(x_1, x_2, \cdots, x_p)\}$.
Donc $\sigma(x_1, x_2, \cdots, x_p) = (x_1, x_2, \cdots, x_p) = (x_2, x_3, \cdots, x_p, x_1) \Rightarrow x_1 = x_2 = \cdots = x_p = x \neq e$. Et comme $(x_1, x_2, \cdots, x_p) \in E \Rightarrow x^p = e \Rightarrow \exists x$ d'ordre $p$.
**p-Groupes:**
Soient $G$ un groupe et $p$ un nombre premier. On dit que G est un p-groupe si et seulement si tout élément de $G$ est d'ordre une puissance de $p$.

PROPOSITION 7. *Soit $G$ un groupe fini; alors $G$ est un p-groupe $\Leftrightarrow$ l'ordre de $G$ est une puissance de $p$.*

Preuve.
Soit $n = |G|$ et $q$ un diviseur premier de $n$. D'après le Théorème de Cauchy $\exists x \in G$ tel que ordre de $x = q$; mais par hypothèse tout élément est d'ordre une puissance de $p \Rightarrow ordre(x) = p^i \Rightarrow q/p^i \Rightarrow q/p \Rightarrow q = p$.
Donc $p$ est le seul diviseur premier de $n$ donc $n = p^j$.
L'implication inverse est évidente.

**Equation des classes**
Soit $G$ un groupe fini ; on fait opérer $G$ sur lui même par conjugaison, alors on a :

$$|G| = \sum_{x \in X} [G : \sum_x].$$

De plus $[G : \sum_x] = 1 \Leftrightarrow G = \sum_x = \{g/gxg^{-1} = x\} \Leftrightarrow x \in Z(G)$.
Si $x \in Z(G) \Rightarrow O_x = \{gxg^{-1}/g \in G\} = \{x\} \Rightarrow Z(G) \subset X$( $X$ est l'ensemble constitué d'un représentant de chaque orbites).
Ainsi $|G| = \sum_{x \in Z(G)} [G : \sum_x] + \sum_{x \notin Z(G)} [G : \sum_x] = |Z(G)| + \sum_{x \notin Z(G)} [G : \sum_x]$
Cette dernière équation s'appelle équation des classes.

THÉORÈME 7. *(Théorème de Burnside) Soit $G$ un p-groupe fini ; alors le centre de $G$ n'est pas réduit à l'élément neutre.*

Preuve.
On sait que $[G : \sum_x]$ est un diviseur de $|G| = p^i$, d'autre part si $x \notin Z(G)$ alors $[G : \sum_x] \neq 1$ donc dans ce cas, $p$ divise $[G : \sum_x]$ par suite $p$ divise $\sum_{x \notin Z(G)} [G : \sum_x]$. Comme $p$ divise $|G|$, on conclue que $p$ divise aussi $|Z(G)|$ ce qui veut dire que $Z(G)$ contient au moins $p$ éléments; d'où $Z(G)$ n'est pas réduit à l'élément neutre.
**Théorèmes de Sylow** :
Soient $G$ un groupe d'ordre $n$ et $d$ un diviseur de $n = |G|$; existe t'il un sous groupe de $G$ d'ordre $d$ ? dans la suite on va essayer de répondre à cette questions en plus d'autres.

THÉORÈME 8. *(théorme 1) Soit $G$ un groupe d'ordre $n = p^h m$ où $p$ est un nombre premier qui ne divise pas $m$; alors $\forall k \leq h$, il existe un sous-groupe de $G$ d'ordre $p^k$.*

Preuve.
On raisonne par récurrence sur $n$ pour $n = 1, 2, 3, 4$ le résultat est vraie. On

suppose que le résultat est vrai pour $\forall i < n$ et on va le montrer pour $n$.
On a :

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} [G : \sum\nolimits_x]$$

* On suppose que $p$ ne divise pas $|Z(G)|$, alors $\exists y \notin Z(G)$ tel que $p$ ne divise pas $[G : \sum_y]$, donc $p^k$ ne divise pas $[G : \sum_y]$, mais on a $|G| = |\sum_y|.[G : \sum_y]$. Par suite comme $p^k$ divise $|G|$ et il ne divise pas $[G : \sum_y]$, et $p$ est premier avec $[G : \sum_y]$, alors on a $p^k$ divise $|\sum_y|$.
On a $|\sum_y| \neq n$ car sinon $[G : \sum_y] = 1 \Rightarrow y \in Z(G)$. Donc $[\sum_y] < n$. D'après l'hypothèse de récurrence, il existe un sous groupe de $\sum_y$ d'ordre $p^k$ d'où le résultat.
* Si $p$ divise $|Z(G)|$, d'après le théorème de Cauchy il existe un élément $a \in Z(G)$ tel que $a$ est d'ordre $p$. Soit $H$ le sous groupe engendré par $a$ dans $G$, $H$ est un s-groupe distingué de $G$ car $a$ est un élément du centre. Donc $G/H$ est un s-groupe dont l'ordre est strictement inférieur à celui de $G$. Donc on a si $k \leq h,\ p^{k-1}$ divise l'ordre de $G/H$ donc il existe un s-groupe $T$ de $G/H$ d'ordre $p^{k-1}$. D'après le Théorème de correspondance, il existe un sous-groupe $R$ de $G$ qui contient $H$ et tel que $T = R/H$. Par suite on a $|R| = |T|.|H| = p^k$, donc il existe un sous groupe de $G$ d'ordre $p^k$.

DÉFINITION 6. Soit $G$ un groupe d'ordre $n = p^h m$ où $p$ et $m$ sont premiers entre eux et $p$ un nombre premier. Alors il existe un p-s-groupe de $G$ d'ordre $p^h$. Un p-s-groupe de Sylow de $G$ est un sous groupe de $G$ dont l'ordre est égal à $p^h$.($p^h$ est la plus grande puissance de $p$ divisant l'ordre de $G$.)

**Remarque :** Un p-s-groupe de Sylow est un élément maximal dans l'ensemble des p-s-groupes de $G$ ; en effet si $H$ est un p-s-groupe de Sylow et $K$ un p-s-groupe de $G$ tel que $H \subset K$ alors on a $|K| = p^i$ et $|H| = p^h$.
$H \subset K \Rightarrow h \leq i$ et comme $h$ est la plus grande valeur telle que $p^h/|G|$ alors $i = h$. D'où $H = K$.

THÉORÈME 9. *(théorème 2) Soient $G$ un groupe d'ordre $n$ et $p$ un diviseur premier de $n$ alors:*
*a) Si $H$ est un p-s-groupe de Sylow de $G$ alors $\forall a \in G,\ aHa^{-1}$ est un p-s-groupe de Sylow.*
*b) Si $H$ est le seul p-s-groupe de Sylow de $G$ alors $H$ est distingué dans $G$.*

Preuve.
a) Soit

$$\phi_a : G \to G$$

$$x \mapsto axa^{-1}$$

$\phi_a$ est un automorphisme de groupe. De plus on a $\phi_a(H) = aHa^{-1}$ est un s-groupe de $G$ isomorphe à $H$; donc ils ont un même nombre d'éléments et ainsi $|H| = |aHa^{-1}| = p^h$ la plus grande puissance de $p$ divisant $n$. Par suite $\forall a \in G,\ aHa^{-1}$ est un p-s-groupe de Sylow de $G$.
b) Si $H$ est le seul p-s-groupe de Sylow, alors d'après a), on a $\forall a \in G,\ \ H = aHa^{-1}$, donc $H$ est distingué.

LEMME 1. *Soit $H$ un p-sous groupe de Sylow de $G$. Alors $H$ est le seul élément de $N(H)/H$ dont l'ordre est une puissance de $p$.*

Preuve.
Comme $N(H) = \{g \in G / gHg^{-1} = H\}$, il est clair que $H$ est distingué dans $N(H)$. On va montrer que si $aH$ est d'ordre une puissance de $p$ alors $aH = H$.
Soit $T$ le s-groupe de $N(H)/H$ engendré par $aH$. Si $\phi : N(H) \longrightarrow N(H)/H$ est la projection canonique et $R = \phi^{-1}(T)$ alors $T = R/H$.
Puisque $T$ est un p-groupe alors $R$ est aussi un p-s-groupe de $G$:
Soit $t \in R,\ \ tH \in T \Rightarrow \exists k$ tel que : $(tH)^{pk} = H = t^{pk}H \Rightarrow t^{pk} \in H$.
Comme $H$ est un p-s-groupe de Sylow alors $H$ est d'ordre $p^h$; d'où $(t^{pk})^{ph} = e = t^{(p^{k+h})}$
Donc $R$ est un p-s-groupe et comme $H \subset R$ et $H$ est maximale dans l'ensemble des p-s-groupe de $G$ alors $H = R$. Donc $T = H/H = \{H\} \Rightarrow aH = H$.

LEMME 2. *Soient $H$ un p-s-groupe de Sylow et $a$ un élément de $G$ d'ordre une puissance de $p$ tel que $aHa^{-1} = H$, alors $a \in H$.*

Preuve.
Comme $aHa^{-1} = H$, alors $a \in N(H)$ et comme $a$ est d'ordre une puissance de $p \Rightarrow aH$ est d'ordre une puissance de $p$ dans $N(H)/H$, mais d'après le lemme précédent $H$ est le seul élément d'ordre une puissance de $p$; d'où $aH = H$ et donc $a \in H$.

THÉORÈME 10. *(Théorème 3) Soient $G$ un groupe d'ordre $n$ et $p$ un diviseur premier de $n$, alors:*
*a) Le nombre des p-s-groupe de Sylow de $G$ est congru à 1 modulo $p$ et c'est un diviseur de $|G|$.*
*b) Tous les p-s-groupe de Sylow sont conjugués.*

Preuve.
Soient $H$ un p-sous-groupe de Sylow de $G$ et $A = \{H, H_1, H_2, \cdots, H_r\}$ l'ensemble de tous les conjugués de $H$, on a: $G$ opère sur $A$ par conjugaison c.à.d:

$$G \times A \to A$$
$$(g, H_j) \mapsto gH_jg^{-1}$$

C'est bien une opération. De même, si $K$ est un s-groupe de $G$ alors $K$ opère sur $A$ de la même façon et on a le cardinal de chaque orbite divise l'ordre de $K$.
Si $K = H$, on a $|A| = \sum_{x \in X} |O_x|$ et $|O_x|$ divise $|H| = p^h$.
- $O_H = \{g.H/g \in H\} = \{gHg^{-1}/g \in H\} = \{H\}$, donc $O_H$ contient un seul élément.
- Soit $H_i \in A$, on va montrer que $O_{H_i} \neq \{H_i\}$. Sinon :
$O_{H_i} = \{H_i\} \Rightarrow \forall a \in H,\ aH_ia^{-1} = H_i$, $H_i$ est un p-s-groupe de Sylow et $a \in H$, donc il est d'ordre une puissance de $p$; d'après le lemme 2, $a \in H_i$; d'où $H \subset H_i$ et puisque ce sont des sous-groupes de Sylow ils ont même ordre et donc $H = H_i$. Contradiction.
Donc $|A| = 1 + P^{\alpha_1} + P^{\alpha_2} + \cdots + P^{\alpha_r}$ où les $\alpha_i$ ne sont pas nuls. Donc le nombre des éléments de $A$ est congru à 1 mod $p$.
Soit $H_0$ un p-s-groupe de Sylow, on suppose que $H_0 \notin A$.
$H_0$ opère sur $A$ et les orbites sont de cardinaux diviseurs de $|H_0|$. Montrons qu'il n'existe pas d'orbite qui contient un seul élément.
Sinon soit $K \in A$ tel que $O_K = \{K\} \Rightarrow \forall a \in H_0,\ aKa^{-1} = K \Rightarrow H_0 \subset K \Rightarrow H_0 = K$. Ce qui est impossible, donc toutes les orbites ont un cardinal plus grand que 1, d'où:
$|A| = P^{\alpha_1} + P^{\alpha_2} + \cdots + P^{\alpha_{r+1}}$ avec $\alpha_i \neq 0 \Rightarrow |A| \equiv 0 \bmod p$; contradiction. Donc $H_0 \in A$.
Par suite $A$ est l'ensemble de tous les p-s-groupes de Sylow de $G$ et le nombre des éléments de $A$ est congru à 1 modulo $p$.
Soit

$$f : A = \{H, a_1Ha_1^{-1}, \cdots, a_rHa_r^{-1}\} \longrightarrow (G/N(H))_g$$
$$a_iHa_i^{-1} \longmapsto a_iN(H).$$

On a $a_iHa_i^{-1} = a_jHa_j^{-1} \Leftrightarrow a_j^{-1}a_iHa_i^{-1}a_j = H \Leftrightarrow a_j^{-1}a_i \in N(H) \Leftrightarrow a_j^{-1}a_iN(H) = N(H) \Leftrightarrow a_iN(H) = a_jN(H)$. Donc $f$ est une application injective de plus elle est surjective car:
Soit $aN(H) \in (G/N(H))_g$, si $a = e$, alors $f(H) = N(H)$. Si $a \notin N(H)$ on a $aHa^{-1} \neq H \Rightarrow aHa^{-1} \in A \Rightarrow f(aHa^{-1}) = aN(H)$. Donc $f$ est une bijection et $card(A) = [G : N(H)]$.

THÉORÈME 11. *(Théorème 4) Soient $G$ un groupe fini et $p$ un diviseur premier de $|G|$. Alors tout p-s-groupe de $G$ est inclus dans un p-s-groupe de Sylow de $G$.*

Preuve.
Soient $K$ un p-sous-groupe de $G$, $H$ un p-sous-groupe de Sylow de $G$ et $A = \{H = H_0, H_1, H_2, \cdots, H_r\}$ l'ensemble de tous les p-sous-groupe de Sylow de

$G$, on a: $K$ opère sur $A$ par conjugaison .
Comme , $|A| = \sum_{x \in X} |O_x|$, $|O_x|$ divise $|K| = p^k$ et $|A| \equiv 1 \bmod p$; alors il existe $i$ tel que $O_{H_i} = \{gH_ig^{-1}/g \in K\} = \{H_i\}$. Ceci veut dire que $\forall a \in K$, $aH_ia^{-1} = H_i$. D'après le lemme 2, cette dernière propriété implique que $K \subset H_i$.

THÉORÈME 12. *(Théorème 5) Soient $G$ un groupe fini et $p$ un diviseur premier de $|G|$. Alors on a : $H$ est un p-s-groupe de Sylow de $G \Leftrightarrow H$ est maximal dans l'ensemble des p-s-groupe de $G$.*

Preuve.
La première implication est démontré dans une remarque précédente. D'après le Théorème précédent tout p-s-groupe $K$ de $G$ est inclus dans un p-s-groupe de Sylow $H$ de $G$; si de plus $K$ est maximal alors il coincide avec le p-sous-groupe de Sylow $H$. D'où l'implication inverse.
**Exemple**
Soient $G$ un groupe d'ordre 6 et $N_p$ le nombre des p-sous-groupes de Sylow de $G$.
a) Si $G$ est abélien alors $N_2 = N_3 = 1$, car tout sous-groupe de $G$ est distingué dans $G$.
b) Si $N_2 = N_3 = 1$, alors $G$ possède deux sous-groupes propres qui sont un 2-sous-groupe de Sylow et un 3-sous-groupe de Sylow et ces deux sous-groupes sont distingués et leurs produit c'est $G$. Ceci implique que $G$ est abélien.

c) Si $G$ est non abélien alors, puisque $N_p \equiv 1 \bmod p$ et $N_p$ divise $|G|$, on a $N_2 = 1$ ou 3 et $N_3 = 1$. Si $N_2 = 1$, et puisque $N_3 = 1$, alors $G$ sera abélien, ce qui est contraire à notre hypotèse. Donc $N_2 = 3$. Ceci implique en particulier qu'il existe un seul 3-sous-groupe de Sylow et qu'il est distingué dans $G$.
Si $G = S_3$ le groupe symétrique, qui n'est pas abélien, alors $N_2 = 3$; car on a 3 2-sous-groupes de Sylow de $S_3$ qui sont ceux engendré par les trois transpositions.

## 3. Groupes résolubles:

**Suite dérivée d'un groupe:**
Soient $G$ un groupe et $a$ et $b$ deux éléments de $G$; l'élément $[a, b] = aba^{-1}b^{-}$ est appelé commutateur de $a$ et $b$.
On désigne par $D(G)$ le groupe $[G, G]$ engendré par les commutateurs de $G$, appelé aussi le groupe dérivé de $G$. On définit par récurrence sur $n$ le $n^{eme}$ groupe dérivé $D^n(G)$ par $D^n(G) = D(D^{n-1}(G))$.

**Propriétés :**
1) Soient $G$ et $G'$ deux groupes et $\phi$ un homomorphisme de $G$ dans $G'$. Alors on a:

$$\phi(D(G)) = D(\phi(G)) \subset D(G').$$

Si $\phi$ est une surjection, alors

$$\phi(D(G)) = D(G').$$

Par récurrence, on vérifie que:

$$\phi(D^n(G)) = (D^n(\phi(G))) \subset D^n(G').$$

Et si $\phi$ est une surjection alors :

$$\phi(D^n(G)) = D^n(G').$$

2) Soient $H$ un sous-groupe de $G$ et $i : H \longrightarrow G$, l'injection canonique d'après 1), on a:

$$i(D^n(H)) = D^n(H) \subset D^n(G).$$

3) Si de plus $H$ est distinguée dans $G$ on a:

$$p : G \to G/H$$

$$x \mapsto \overline{x}.$$

$p(D^n(G)) = (D^n(G/H))$ car $p$ est une surjection. De plus:

$$p(D^n(G)) = H.D^n(G)/H.$$

4) Soient $G$ un groupe et $H$ un sous groupe distingué de $G$ tel que $G/H$ est abélien; alors $D(G) \subset H$:
Soient $a$ et $b$ deux éléments de $G$; alors $aba^{-1}b^{-1} \in H$, car puisque $G/H$ est abélien, on a

$$\overline{aba^{-1}b^{-1}} = \overline{a}.\overline{b}.\overline{a^{-1}}.\overline{b^{-1}} = H.$$

D'où $aba^{-1}b^{-1} \in H$ et donc $D(G) \subset H$.
**Remarque :** Comme on a:

$$\phi(D(G)) \subset D(G')$$

pour tout homomorphisme, alors en particulier si $G' = G$ et $\phi$ est un automorphisme intérieur ceci reste vrai. D'où $D(G)$ sera distinguée dans $G$. Il en est de même pour $D^n(G) = D(D^{n-1}(G))$ avec $D^{n-1}(G)$.

**Suite normale d'un groupe :**
Soient $G$ un groupe et

$$G = G_0 = G_1 \supset G_2 \supset \cdots \supset G_k \cdots \supset G_n = \{e\}$$

une suite de sous groupe de $G$. On dit que $(G_j)$ est normal si et seulement si $(G_{i+1})$ est distingué dans $G_i$ pour $0 \leq i \leq n-1$.

**Exemple :**
Soient $S_4$ le groupe des permutations de $\{1,2,3,4\}$, $A_4$ le sous groupe des permutations paires et

$$V_4 = \{\sigma \in A_4 / \sigma^2 = ide\}$$

Alors on a:
$V_4 \lhd A_4$ et $A_4 \lhd S_4$, d'où la suite $S_4 \supset A_4 \supset V_4 \supset \{e\}$ est une suite normale.
**Groupes résolubles:**
Soit $G$ un groupe, on dit que $G$ est résoluble si et seulement si il existe une suite normale :
$G = G_0 \supset G_1 \supset \cdots \supset G_k \cdots \supset G_n = \{e\}$ telle que $G_i/G_{i+1}$ est abélien pour tout $i,\ 0 \leq i \leq n-1$.
**Exemples :**
i) Le groupe $S_4$ est résoluble car $S_n/A_n$ est abélien, $A_4/V_4$ est abélien et $V_4/\{e\}$ est abélien.
ii) Un groupe abélien est résoluble.

THÉORÈME 13. *Soient $G$ un groupe. Alors $G$ est résoluble si et seulement si il existe un entier $n$ tel que $D^n(G) = \{e\}$.*

Preuve.
On suppose qu'il existe $n$ tel que $D^n(G) = \{e\}$ alors la suite :
$G = G_0 \supset D(G) \supset D^2(G) \supset \cdots \supset D^n(G) = \{e\}$ est une suite normale et on a :

$$D^i(G)/D(D^i(G))$$

est abélien donc $G$ est résoluble.
On suppose que $G$ est résoluble. Il existe une suite normale $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ telle que $G_i/G_{i+1}$ est abélien. En particulier $G/G_1$ est abélien. D'où $G_1 \supset D(G)$ et comme $G_2 \subset G_1$ et $G_1/G_2$ est abélien alors $G_2 \supset D(G_1)$ donc:

$$G_2 \supset D(G_1) \supset D(D(G)) = D^2(G).$$

Ainsi on montre par réccurence que $\forall i,\ G_i \supset D^i(G)$. Donc $G_n \supset D^n\{G\}$. Mais $G_n = \{e\} \Rightarrow D^n(G) = \{e\}$.

THÉORÈME 14. *Soient $G$ un groupe et $H$ un sous groupe distingué de $G$. Alors $G$ est résoluble si et seulement si $H$ et $G/H$ sont résolubles.*

Preuve
On suppose que $H$ et $G/H$ sont résolubles. Alors il existe $n$ tel que:

$$D^n(G/H) = \{H\}$$

et un entier $m$ tel que:

$$D^m(H) = \{e\}.$$

Or $D^n(G/H) = H.D^n(G)/H$ d'où $H.D^n(G) = H \Rightarrow D^n(G) \subset H$.
Par suite:

$$D^{m+n}(G) = D^m(D^n(G)) \subset D^m(H) = \{e\}.$$

D'où $G$ est résoluble.
Si $G$ est résoluble alors $\exists n$ tel que $D^n(G) = \{e\}$.
$D^n(H) \subset D^n(G) = \{e\} \Rightarrow H$ est résoluble.
$D^n(G/H) = H.D^n(G)/H = \{H\} \Rightarrow G/H$ est résoluble.
**Remarque :**
Soit $G$ un p-groupe fini, alors $G$ est résoluble. En effet:
On raisonne par récurrence sur $n$ où $|G| = p^n$
Si $n = 0, 1, \cdots$ c'est évident.
On suppose que le théorème est vrai pour $\forall i \leq n$.
Si $G = Z(G)$ alors $G$ est résoluble. Sinon alors $Z(G)$ est résoluble et $G/Z(G)$ est d'ordre $p^k$ où $k < n$. Donc d'après l'hypothèse de récurrence $G/Z(G)$ est résoluble. D'où $G$ est résoluble.

## 4. Structures des groupes abéliens finis

DÉFINITION 7. Soient $G$ un groupe abélien fini et $A_1$, $A_2$, $\cdots$, $A_n$ des sous-groupes de $G$. On dit que $G$ se décompose en produit directe des sous-groupes $A_i$ si et seulement si:
1. $G = A_1 \dot{A}_2 \cdots A_n$,
2. Pour tout $i$, $i = 1, \cdots n-1$ on a $A_i \cap A_{i+1} \cdots \cap A_n = \{e\}$. Une fois ces deux conditions vérifiés, $G$ sera noté comme suit

$$G = A_1 \times A_2 \times \cdots \times A_n.$$

THÉORÈME 15. *Soit $G$ un groupe abélien d'ordre $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Alors $G$ est produit directe de ses sous-groupes $S_1, \cdots, S_r$ où $S_i$ est l'ensemble des éléments de $G$ dont l'ordre est une puissance de $p_i$.*

Preuve. On va démontrer le théorème dans le cas où $n = n_1 n_2$ avec $n_1$ et $n_2$ premiers entre eux. Soit $A_i$ l'ensemble des éléments de $G$ dont l'ordre est un diviseur de $n_i$. Montrons que $G$ est produit directe de $A_1$ et de $A_2$. Comme $n_1$ et $n_2$ sont premiers entre eux, alors il existe $u$ et $v$ deux entiers tels que $1 = un_1 + vn_2$. Par suite pour tout $x$ de $G$ on a

$$x = x^{un_1 + vn_2} = x^{un_1} x^{vn_2};$$

l'élément $x^{un_1}$ est d'ordre un diviseur de $n_2$ et $x^{vn_2}$ est d'ordre un diviseur de $n_1$. Donc on a $G = A_1 A_2$. Comme $n_1$ et $n_2$ sont premiers entre eux, alors $A_1 \cap A_2$ est réduit à l'élément neutre. Ainsi $G$ est produit directe de $A_1$ et de $A_2$. Pour démontrer le théorème dans le cas général, il suffit de raisonner par récurence

et appliquer le résultat qu'on vient de démontrer.

THÉORÈME 16. *Soit $G$ un p-groupe abélien fini; alors $G$ est produit direct de sous-groupes cycliques.*

Preuve.
On va commencer par citer quelques résultats qu'on va utiliser pour la preuve de ce Théorème.
1. Soient $G$ un p-groupe fini, $k$ un entier non nul et $b$ un élément de $G$ tel que $b^{p^k}$ est différent de l'élément neutre. Si $b^{p^k}$ est d'ordre $p^m$, alors $b$ est d'ordre $p^{k+m}$.
2. Soient $a_1$ un élément de $G$ dont l'ordre est maximal et $G_1$ le sous groupe de $G$ engendré par $a_1$. Si $\overline{b}$ est d'ordre $p^k$ dans $G/G_1$, alors il existe un élément $a \in \overline{b}$ dont l'ordre est exactement $p^k$. Il suffit d'utiliser le résultat précédent et définir le bon élément de $\overline{b}$ dont l'ordre est égal à $p^k$.
Alors à l'aide de ce dernier résultat et en utilisant un raisonnement par récurence, on arrive à montrer le théorème. Il suffit d'appliquer l'hypotèse de récurence sur le groupe quotient $G/G_1$. Donc il va exister des sous-groupes cycliques $\overline{G_2}, \cdots, \overline{G_n}$ tels que

$$G/G_1 \simeq \overline{G_2} \times \cdots \times \overline{G_n}.$$

Chaque $\overline{G_i}$ est engendré par un élément $\overline{b_i}$ qui a le même ordre que l'un de ses éléments $a_i$( d'après le résultat 2, rappelé au début de cette preuve). Soit $G_i$ le sous groupe de $G$ engendré par $a_i$, alors, en utilisant le raisonnement par recurence, on montre que

$$G \simeq G_1 \times G_2 \times \cdots \times G_n.$$

On peut vérifier de plus, qu'une telle décomposition avec $|G_i| = p^{r_i}$ et $r_n \leq r_{n-1} \leq \cdots \leq r_1$, est unique.

CHAPITRE 5

# Les structures Quotients

## 1. Les Anneauxs Quotients

Soient $A$ un Anneau, $I$ un idéal bilatère de $A$ et $A/I$ le groupe quotient de $A$ par $I$. On muni $A/I$ d'une multiplication définie par $\forall \overline{x} \in A/I \ \ \forall \overline{y} \in A/I$, $\overline{x}.\overline{y} = \overline{xy}$. Muni de l'addition en plus de cette dernière loi, $A/I$ est un anneau qu'on appelle anneau quotient de $A$ par $I$. Les différents Théorèmes d'isomorphismes qu'on a vu pour les groupes restent valables pour les anneaux. Les démonstrations de ces Théorèmes est presque la même que pour les groupes; il suffit de vérifier que les homomorphismes de groupes utilisé dans les preuves sont aussi des homomorphismes d'anneaux.

THÉORÈME 17. *( 1er th. d'isomorphisme)*
*Soient $A$ et $B$ deux anneaux, $f$ un homomorphisme d'anneaux de $A$ dans $B$, $p$ la surjection canonique de $A$ dans $A/kerf$ et $i$ l'injection canonique de $f(A)$ dans $B$ alors il existe un isomorphisme $\overline{f}$ de $A/kerf$ dans $f(A)$ tel que :*

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

PROPOSITION 8. *: Soient $A$, $B$ et $C$ 3 anneaux, $f$ un homomorphisme de $A$ dans $B$ et $g$ un homomorphisme surjective de $A$ dans $C$; alors il existe un homomorphisme $\phi$ de $C$ dans $B$ tel que: $f = \phi \circ g$ si et seulement si $Kerg \subset Kerf$.*

THÉORÈME 18. *(2**ème** **th. d'isomorphisme** )*
*Soient $A$ un anneau, $I$ et $J$ deux idéaux bilatères de $A$, alors $J/I \cap J \simeq I + J/I$.*

THÉORÈME 19. *(3**ème** **th. d'isomorphisme** )*
*Soient $A$ un anneau, $I$ et $J$ deux idéaux bilatères de $A$ tels que $I \subset J$; alors $A/J \simeq (A/I)/(J/I)$.*

THÉORÈME 20. *(4**ème** **th. d'isomorphisme ou th. de correspondance)**.*
*Soient $A$ un anneau, $I$ un idéal bilatère de $A$ et $T$ un sous-anneaux de $A/I$, alors il existe un sous-anneau de $A$, $R \supset I$ tel que $T = R/I$.*

## 2. Espaces Vectoriels Quotients

Soient $K$ un corps commutatif, $E$ un K-espace vectoriel, $F$ un sous-espace vectoriel de $E$ et $E/F$ le groupe quotient de $E$ par $F$. On muni $E/F$ d'une multiplication externe définie par $\forall a \in K \ \ \forall \overline{x} \in E/F$, $a.\overline{x} = \overline{ax}$. Muni de l'addition en plus de cette dernière loi, $E/F$ est un K-espace vectoriel qu'on appelle espace vectoriel quotient de $E$ par $F$. Les différents Théorèmes d'isomorphismes qu'on a vu pour les groupes restent valables pour les espaces vectoriels. Les démonstrations de ces Théorèmes sont presque les mêmes que pour les groupes; il suffit de vérifier que les homomorphismes de groupes utilisé dans les preuves sont aussi des homomorphismes d'espaces vectoriels.

THÉORÈME 21. *( 1er th. d'isomorphisme)*
*Soient $E$ et $F$ deux K-espaces vectoriels, $f$ une application linéaire de $E$ dans $F$, $p$ la surjection canonique de $E$ dans $E/kerf$ et $i$ l'injection canonique de $f(E)$ dans $F$ alors il existe un isomorphisme $\overline{f}$ de $E/kerf$ dans $f(E)$ tel que :*

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

PROPOSITION 9. *: Soient $E$, $E'$ et $E"$ 3 K-espaces vectoriels, $f$ une application linéaire de $E$ dans $E'$ et $g$ une application linéaire surjective de $E$ dans $E"$; alors il existe une application linéaire $\phi$ de $E"$ dans $E'$ tel que: $f = \phi \circ g$ si et seulement si $Kerg \subset Kerf$.*

THÉORÈME 22. *($2^{\text{ème}}$ **th. d'isomorphisme** )*
*Soient $E$ un K-espace vectoriel, $F$ et $G$ deux sous-espaces vectoriels de $E$, alors $G/(F \cap G) \simeq (F+G)/F$.*

THÉORÈME 23. *($3^{\text{ème}}$ **th. d'isomorphisme** )*
*Soient $E$ un K-espace vectoriel, $F$ et $G$ deux sous-espaces vectoriels de $E$ tels que $F \subset G$; alors $E/G \simeq (E/F)/(G/F)$.*

THÉORÈME 24. *($4^{\text{ème}}$ **th. d'isomorphisme ou th. de correspondance)**.*
*Soient $E$ un K-espace vectoriel, $F$ un sous-espace vectoriel de $E$ et $T$ un sous-espace vectoriel de $E/F$, alors il existe un sous-espace vectoriel de $E$, $R \supset F$ tel que $T = R/F$.*