# Algèbre

J. Mellac

Mai 2016

## Table des matières



# 1 Classification des groupes abéliens finis

Rappels : Soit $G$ un groupe fini.
L'ordre de $G$ est son cardinal.
L'ordre de $x \in G$ est l'ordre du sous groupe engendré par cet élément.
L'exposant de $G$ est le plus petit entier $n \in \mathbb{N}^*$ tel que $\forall x \in G,\ x^n = e$, où $e$ est l'élément neutre du groupe.

Dans la suite de ce paragraphe, les groupes sont supposés abéliens finis et sont notés additivement.

## 1.1 Décomposition d'un groupe abélien fini en somme directe de composantes primaires

**Définition.** Soit $p$ un nombre premier.

1. Un groupe $G$ est $p$-primaire ou est un groupe de $p$-torsion si tout élément de $G$ a pour ordre une puissance de $p$.
2. Un groupe $G$ est un $p$-groupe si son ordre est une puissance de $p$.

**Proposition.** Les deux définitions précédentes sont équivalentes.

**Démonstration.** L'implication (2) $\Rightarrow$ (1) est immédiate, l'implication réciproque est démontrée par récurrence sur le cardinal de $G$ en prenant $G' = G/\mathbb{Z}x$ car $|\mathbb{Z}x| = p^k$ avec $k \in \mathbb{N}^*$ si $x \neq 0$.

**Définition.** Soit $G$ un groupe abélien fini quelconque et $p$ un nombre premier. L'ensmble $T_p(G)$ défini par :
$T_p(G) = \{x \in G | \exists k \in \mathbb{N}^*,\ p^k x = 0\}$ est un sous groupe $p$-primaire de $G$, appelé sous groupe de $p$-torsion de $G$.

**Remarque.** En notant $|G| = n = \prod_{i=1}^{r} p_i^{\alpha_i}$, si $p \neq p_i,\ i \in [\![1, r]\!]$ on a $T_p(G) = \{0\}$.

**Théorème.** Théorème de décomposition.
Tout groupe abélien fini est somme directe de ses sous groupes de $p$-torsion.

**Démonstration.** $|G| = n = \prod_{i=1}^{r} p_i^{\alpha_i}$. En supposant $r = 2$, $G = T_{p_1}(G) \oplus T_{p_2}(G)$. En effet en notant $m = p_1^{\alpha_1},\ n = p_2^{\alpha_2}$, l'égalité de Bezout entraine l'existence de $a, b \in \mathbb{Z}$, tels que : $am + bn = 1$. Soit $x \in G$, $x = (am + bn)x = a(mx) + b(nx)$ or $mx \in T_{p_2}(G)$ et $nx \in T_{p_1}(G)$. De plus si $y \in T_{p_1}(G) \cap T_{p_2}(G)$, $mx = 0$ et $nx = 0$ entraine $x = (am + bn)x = a(mx) + b(nx) = 0$, d'où la conclusion. On termine en faisant une récurrence sur $r$.

## 1.2 Structure d'un groupe abélien fini

**Théorème.** Tout groupe fini $G$ $p$-primaire est somme directe de groupes cycliques $p$-primaires.

La démonstration repose sur le lemme suivant

**Lemme.** Soit $x \in G$ d'ordre maximal $p^n$. Le groupe $G/\mathbb{Z}x$ est $p$-primaire et tous ses éléments ont un ordre $p^m,\ m \leq n$. De plus si $\overline{y} \in G/\mathbb{Z}x$ est d'ordre $p^m$, il existe $z \in G$, élément de la classe de $y$, dont l'ordre est également $p^m$.

**Démonstration.** Avec les notations précédentes, $p^m \overline{y} = 0 \Longleftrightarrow p^m y = kx$, l'ordre de $kx$ étant un diviseur de $p^{n-m}$ on en déduit $p^{n-m}k = lp^n$, l'élément $z = y - lx$ est alors dans la classe de $y$ et est d'ordre $p^m$.
La démonstration du théorème se fait par récurrence sur le cardinal du groupe en utilisant l'hypothèse de récurrence sur $G/\mathbb{Z}x$.

Soit $G = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_s$ un groupe $p$-primaire, avec $|\mathbb{Z}a_i| = p^{e_i},\ i \in [\![1, s]\!]$

**Proposition.** Unicité.
Deux décompositions de $G$ en somme directe ont le même nombre de composantes et la suite des ordres des sous groupes cycliques est la même dans les deux cas.

**Définition.** La suite $p^{e_1}, p^{e_2}, \cdots, p^{e_s}$ est la suite des facteurs invariants du groupe $p$-primaire $G$.

**Théorème.** Un groupe abélien fini $G$ est somme directe de groupes cycliques, $G = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_t$, $|\mathbb{Z}b_i| = n_i,\ i \in [\![1,t]\!]$, tels que $n_{i+1}|n_i,\ i \in [\![1,t-1]\!]$. La suite $n_1, n_2, \cdots n_t$ est la suite des facteurs invariants, elle est unique.

**Démonstration.** En utilisant le théorème de décomposition, $|G| = n = \prod_{i=1}^{r} p_i^{e_i}$, en notant

$G_i = T_{p_i}(G),\ i \in [\![1,r]\!]$, on a

$G = G_1 \oplus G_2 \oplus \cdots \oplus G_r$ puis en utilisant le théorème précédent on a

$G_i = \mathbb{Z}a_{i1} \oplus \cdots \oplus \mathbb{Z}a_{ih_i}$ avec $|\mathbb{Z}a_{i1}| = p_i^{e_{i1}} \geq |\mathbb{Z}a_{i2}| = p_i^{e_{i2}} \geq |\mathbb{Z}a_{ih_i}| = p_i^{e_{ih_i}}$. le résultat en découle, où

$\mathbb{Z}b_i = \mathbb{Z}a_{1i} \oplus \cdots \oplus \mathbb{Z}a_{ri},\ i \in [\![1,t]\!],\ n_i = |\mathbb{Z}b_i| = p_1^{e_{1i}} \cdots p_r^{e_{ri}}$.

**Remarque.** L'exposant du groupe $G$ est $n_1$.

**Définition.** En reprenant $n_i = p_1^{e_{1i}} \cdots p_r^{e_{ri}}$, les $p_j^{e_{ji}},\ (i,j) \in [\![1,t]\!] \times [\![1,r]\!]$ sont appelés diviseurs élémentaires de $G$.

**Théorème.** Deux groupes abéliens finis sont isomorphes si et seulement si ils ont mêmes facteurs invariants.

**Exemples .** 1) Déterminons à un isomorphisme près le groupe admettant $2, 2^2, 2^3, 3, 3^2, 5$ comme diviseurs élémentaires. Ses facteur invariants sont alors

$n_1 = 2^3\, 3^2\, 5 = 360$, $n_2 = 2^2\, 3 = 12$ et $n_3 = 2$, on a alors

$G \simeq \mathbb{Z}/360\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2) Déterminer les diviseurs élémentaires et less facteurs invariants de $G = \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}$.

Le théorème chinois donne : $\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/42\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, les diviseurs élémentaires sont 2,4,3,3 et 7.

Les facteurs invariants sont alors : $n_1 = 4.3.7 = 84,\ n_2 = 2.3 = 6$, $G \simeq \mathbb{Z}/84\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

3) Déterminer à un isomorphisme près tous les groupes abélien d'ordre 300.

$300 = 4.3.25 = 2^2.3.5^2$. Les diviseurs élémentaires possibles sont :

a) $2^2$,3,$5^2$ ou b) 2,2,3,$5^2$ ou c) 4,3,5,5 ou d) 2,2,3,5,5 ce qui donne les facteurs invariants :

a) $n_1 = 300$ b) $n_1 = 150,\ n_2 = 2$ c) $n_1 = 60,\ n_2 = 5$ d) $n_1 = 30,\ n_2 = 10$.

# 2 Groupes finis. Groupe symétrique

Dans ce paragraphe, les groupes, qui ne seront plus nécéssairement abéliens, seront finis et notés multiplicativement, à part $\mathbb{Z}$ ainsi que les groupes additifs des corps. Les notions d'homomorphismes (ou simplement morphismes), noyau, image sont supposées connues.

**Définition.** Soit $H$ un sous groupe d'un groupe $G$. On appelle classe à gauche (respectivement à droite) de l'élément $a \in G$ relativement à $H$, le sous ensemble

$$aH = \{g \in G \mid \exists h \in G,\ g = ah\} \text{ resp. } Ha = \{g \in G \mid \exists h \in G,\ g = ha\}.$$

Les classes à gauche forment une partition de $G$, leur ensemble est noté $G/H$, ce n'est pas un groupe en général. Le cardinal de $G/H$ est noté $(G : H)$ et est appelé l'indice de $H$ dans $G$

**Théorème.** De Lagrange.
Si $H$ est un sous groupe du groupe fini $G$, on a

$$|G| = |G/H|\,|H| = (G : H)|H|.$$

En particulier l'ordre d'un élément de $G$ divise l'ordre de $G$.

## 2.1 Sous groupes distingués

**Définition.** Soit $G$ un groupe et $a \in G$. L'application $\phi_a : G \longrightarrow G,\ x \longmapsto axa^{-1}$ est un automorphisme de $G$, appelé automorphime intérieur.

1) Un sous groupe $H$ de $G$ est normal ou distingué s'il est stable par automorphisme intérieur, c'est à dire si :
$\forall a \in G,\ aHa^{-1} = H$. Ceci est équivalent à dire qu'il y a égalité entre les classes à gauche et les classes à droite. On note $H \lhd G$.

2) Un sous groupe $H$ de $G$ est caractéristique s'il est stable par tout automorphisme de $G$. Un tel groupe est normal.

3) On dit qu'un groupe est simple s'il n'a que deux sous groupes normaux : $\{1\}$ et $G$.

**Proposition.** Un sous groupe $H$ est normal si et seulement si $G/H$ a une structure de groupe pour le produit défini par :
$\forall a, b \in G,\ aH.bH = ab.H$

**Remarques.**

**Définition.** 1) Une suite exacte $G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_4} \cdots \xrightarrow{f_{n-1}} G_n$ signifie que les $f_i$ sont des morphismes de groupes tels que $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1},\ i \in [\![1, n-1]\!]$.
La définition d'un sous groupe normal conduit à la suite exacte courte :

$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{p} G/H \longrightarrow 1$, $i$ est injectif et $p$ est surjectif.

2) Soit $f : G \longrightarrow G'$ un morphisme de groupes, $\operatorname{Ker} f$ est un sous groupe normal de $G$ et
$G/\operatorname{Ker} f \simeq \operatorname{Im} f$.

3) Tout sous groupe d'un groupe abélien est normal, la réciproque est fausse comme le montre le groupe des quaternions, dont tous les sous groupes sont distingués ( et cycliques à par $\{1\}$ et $H_8$) mais qui n'est pas abélien.

**Définition.** 1) Soit $A$ une partie de $G$, on note $< A >$ le sous groupe de $G$ engendré par $A$, c'est le plus petit sous groupe de $G$ contenant $A$. En notant $A^{-1} = \{a^{-1} | a \in A\}$ on a
$< A >= \{a_1 a_2 \cdots a_n | n \in \mathbb{N}, a_i \in A \cup A^{-1}\}$.

2) On définit le centre d'un groupe $G$ par $Z = C(G) = \{a \in G | \forall b \in G,\ ab = ba\}$ c'est l'ensemble des éléments de $G$ qui ommutent avec tous les éléments de $G$.

3) On définit le sous groupe dérivé de $G$ comme le sous groupe engendré par les commutateurs de $G$, c'est à dire les élments de la forme $aba^{-1}b^{-1}$ avec $a, b \in G$, il est noté $D(G)$.

**Proposition.** Le centre et le sous groupe dérivé de $G$ sont des sous groupes distingués de $G$, de plus $G/D(G)$ est abélien et si $K$ est un sous groupe distingué de $G$ tel que $G/K$ soit abélien alors $D(G) \subset K$.

## 2.2 Groupe symétrique

**Définition.** Le groupe symétrique de l'ensemble $[\![1, n]\!]$ est l'ensemble des bijections de cet ensemble sur lui même muni de la composition des applications. Il est noté $\mathcal{S}_n$ ou $\mathfrak{G}_n$. Ce groupe n'est pas commutatif si $n > 2$.

**Définition.**
1. Soit $(i, j) \in [\![1, n]\!]^2,\ i \neq j$.
   Une transposition $\tau$ est un élément de $\mathcal{S}_n$ défini par : $\tau(i) = j,\ \tau(j) = i,\ \forall x \notin \{i, j\},\ \tau(x) = x$.
   Cette transposition est notée $\tau = (i, j)$
2. Soient $x_1, x_2, \cdots, x_p$ $p$ éléments distincts de $[\![1, n]\!]$. Un $p$-cycle ou cycle d'ordre $p$ est un élément $\sigma$ de $\mathcal{S}_n$ défini par :
   $\forall x \notin \{x_1, x_2, \cdots, x_p\},\ \sigma(x) = x,\ \forall i \in [\![1, p-1]\!],\ \sigma(x_i) = x_{i+1},$ et $\sigma(x_p) = x_1$.
   Ce $p$-cycle est noté $\sigma = (x_1, x_2, \cdots, x_p)$. L'ensemble $\{x_1, x_2, \cdots, x_p\}$ est appelé support du $p$-cycle.
   Un $n$-cycle est appelé permutation circulaire.

**Remarque.** 1) Une transposition est un 2-cycle. $(i, j)(i, j) = Id_{[\![1,n]\!]} = Id$.
2) Deux cycles de supports disjoints commutent. $n = 6,\ (1, 2, 3)(4, 6) = (4, 6)(1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$.

**Exemple.** n=3, $(1, 2)(1, 3) = (1, 3, 2)$, $(1, 3)(1, 2) = (1, 2, 3)$ ces transpositions ne commutent pas, leurs supports ont 1 en commun.

**Proposition.** 1) Soit $\sigma \in \mathcal{S}_n$ On définit sur $[\![1, n]\!]$ la relation $xR_\sigma y \iff \exists k \in \mathbb{Z},\ y = \sigma^k(x)$. Cette relation est une relation d'équivalence sur $[\![1, n]\!]$.
2) Soit $x \in [\![1, n]\!]$. Il existe un entier $p \in \mathbb{N}^*$ tels que $x, \sigma(x), \cdots, \sigma^{p-1}(x)$ sont deux à deux distincts et que $\sigma^p(x) = x$. La classe d'équivalence de $x$ pour la relation $R_\sigma$ est l'ensemble $\{x, \sigma(x), \cdots, \sigma^{p-1}(x)\}$ elle est appelée orbite de $x$ pour la permutation $\sigma$ (voir paragraphe suivant), de plus $(x, \sigma(x), \cdots, \sigma^{p-1}(x))$ est un $p$-cycle.

**Proposition.** Toute permutation de $\mathcal{S}_n$ est un produit de transpositions.

**Démonstration.** Si $n = 1$ ou $n = 2$ c'est immédiat, supposons $n \geq 3$ et le résultat vrai pour $n - 1$.
Soit $\sigma \in \mathcal{S}_n$.
Si $\sigma(n) = n$ $\sigma|_{[\![1,n-1]\!]} \in \mathcal{S}_{n-1}$ et le résultat résute de l'ypothèse de récurrence.
Si $\sigma(n) = k < n$, $\mu = (k, n)\sigma$ vérifie $\mu(n) = n$, d'où $\mu = \tau_1\tau_2 \cdots \tau_r \Longrightarrow \sigma = (k, n)\tau_1\tau_2 \cdots \tau_r$.

**Définition.** 1) Soit $\sigma \in \mathcal{S}_n$, un couple $(i,j) \in [\![1,n]\!]^2$ est une inversion de $\sigma$ si $i<j$ et $\sigma(i)>\sigma(j)$. On note $I(\sigma)$ le nombre d'inversions de $\sigma$.
2) La signature de $\sigma \in \mathcal{S}_n$ est définie par $\epsilon(\sigma) = (-1)^{I(\sigma)} \in \{-1,1\}$.
3) Une permutation est paire (respectivement impaire) si $\epsilon(\sigma)=1$ (respectivement -1).

**Proposition.** L'ensemble des permutations paires est un sous groupe de $\mathcal{S}_n$ appelé groupe alterné et noté $\mathcal{A}_n$. Ce sous groupe est engendré par les cycles d'ordre 3 pour $n \geq 3$.

En effet, $\mathcal{A}_n$ est engendré par les produits pairs de transposition et : $(a,b)(b,c) = (a,b,c),\ (a,b)(a,c) = (a,c,b),\ (a,b)(c,d) = (a,c,b)(a,c,d)$.

**Exemple.** $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $(1,3),\ (1,4),\ (2,3),\ (2,4)$ sont les inversions de $\sigma$. $I(\sigma)=4,\ \epsilon(\sigma)=1,\ \sigma$ est une permutation paire de $\mathcal{S}_4$.

**Proposition.** 1) Si $\tau$ est une transposition, $\epsilon(\tau) = -1$.
2) $\sigma_1,\ \sigma_2 \in \mathcal{S}_n$ on a $\epsilon(\sigma_1,\sigma_2) = \epsilon(\sigma_1)\,\epsilon(\sigma_2)$, autrement dit $\epsilon$ est un morphisme de groupes entre $(\mathcal{S}_n,\ \circ)$ et $(\{-1,1\},\times)$ et $\mathcal{A}_n = \operatorname{Ker}\epsilon$. On a donc $\mathcal{A}_n \lhd \mathcal{S}_n$

**Exemple.** 1) $\mathcal{S}_2 = \{Id,(1,2)\},\ \mathcal{A}_2 = \{Id\}$.
2) $\mathcal{S}_3 = \{Id,(1,2),(1,3),(2,3),(1,2,3),(1,3,2)\},\ \mathcal{A}_3 = \{Id,(1,2,3),(1,3,2)\}$.

**Proposition.** 1) Soit $\sigma = (a_1,\cdots,a_p)$ un cycle d'ordre $p$ de $\mathcal{S}_n$ et $\tau \in \mathcal{S}_n$. On a :

$$\tau\sigma\tau^{-1} = (\tau(a_1),\cdots,\tau(a_p))$$

ce qui entraine que dans $\mathcal{S}_n$ tous les cycles d'ordre $p$ sont conjugués.
2) Si $n \geq 5$, les cycles d'ordre 3 sont conjugués dans $\mathcal{A}_n$.

**Démonstration.** Soit $n \geq 5$ et $i,j,k,i',j',k' \in [\![1,n]\!]$, $i,j,k$ distincts, de même que $i',j',k'$.
Il existe $\tau \in \mathcal{S}_n$ tel que $\tau(i)=i', \tau(j)=j', \tau(k)=k'$. On a $\tau\sigma\tau^{-1} = (\tau(i),\tau(j),\tau(k))$, si $\tau \in \mathcal{A}_n$ c'est terminé, sinon il existe deux éléments $l,m \in [\![1,n]\!]$ distincts de $i,j,k$. Dans ce cas on remplace $\tau$ par le produit $\tau(l,m) \in \mathcal{A}_n$.

# 3 Groupe opérant sur un ensemble.

## 3.1 Généralités

**Définition.** On dit qu'un groupe $G$ opère sur un ensemble $X$ s'il y a une application :

$$G \times X \longrightarrow X,\ \ (g,x) \longmapsto g.x$$

vérifiant les propriétés suivantes :
$\forall g,g' \in G,\ \forall x \in X,\ g.(g'.x) = (gg').x$
$\forall x \in X,\ 1.x = x$
Il est équivalent de se donner un morphisme $\phi : G \longrightarrow \mathcal{S}(X)$, où $\mathcal{S}(X)$ désigne le groupe des bijections de $X$. Il suffit de poser $g.x = \phi(g)(x)$.

On dit que le groupe opère transitivement sur $X$ si : $\forall (x,y) \in X^2,\ \exists g \in G,\ g.x = y$.
On dit que le groupe opère fidèlement sur $X$ si le morphisme $\phi$ est injectif : $\forall x \in X,\ g.x = x \Rightarrow g = 1$.
On peut noter que $G/\operatorname{Ker}\phi$ opère fidèlement sur $X$.

**Définition.** Soit $x \in G$, l'orbite de $x$ est l'ensemble $\omega(x) = G.x = \{y \in X | \exists g \in G,\ g.x = y\}$. Ceci peut permettre de définir une relation d'équivalence sur $X$ :
$x\mathcal{R}y \iff y \in \omega(x)$. On peut noter que $G$ opère transitivement sur $\omega(x)$.

**Proposition.** Toute permutation de $\mathcal{S}_n$ est un produit de cycles disjoints.

**Démonstration.** Soit $\sigma \in \mathcal{S}_n$ et $G =< \sigma >$. $G$ opère sur $[\![1, n]\!]$ et les orbites sont les classes définies pour la relation $R_\sigma$ précédente.
en appelant $F_1, \cdots, F_r$ ces classes, et $\sigma_i = \sigma|_{F_i}$, on a $\sigma = \sigma_1 \cdots \sigma_r$ ces produits commutant entre eux.

**Exemple.** $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 3 & 5 & 1 & 8 & 2 & 7 \end{pmatrix} = (1,4,5)(2,6,8,7) = (1,4)(4,5)(2,6)(6,8)(8,7)$, les éléments invariants (ici 3) ne sont pas précisés dans le produit.

**Définition.** Soit $G$ un groupe opérant sur l'ensemble $X$ et $x \in X$. Le stabilisateur de $x$ ou sous groupe d'isotropie de $x$ est le sous groupe de $G$ défini par $H_x = \{g \in G | g.x = x\}$.

**Exemples .** 1) Dans l'opération de $\mathcal{S}_n$ sur $[\![1, n]\!]$, le stabilisateur d'un point est isomorphe à $\mathcal{S}_{n-1}$.

2) Soit $X$ une droite affine définie sur un corps $\mathbb{K}$ et $G$ le groupe des similitudes

$$G = \{x \longmapsto ax + b,\ a \in \mathbb{K}^*,\ b \in K\}$$

Le groupe $G$ opère transitivement sur $X$ et si $x \in X$, le stabilisateur $H_x$ est le groupe des homothéties centrées en $x$.

3) Le groupe $G$ opère sur lui même par translation à gauche $g.a = ga$. Il opère transitivement et fidèlement, ce qui donne un morphisme injectif $\phi : G \longrightarrow \mathcal{S}(G)$.
Ceci conduit au thèorème de Cayley :

**Théorème.** Soit $G$ un groupe fini de cardinal $n$, $G$ est isomorphe à un sous groupe de $\mathcal{S}_n$.

4) Soit $H$ un sous groupe (quelconque) de $G$. Le groupe $G$ opère par translation à gauche sur $G/H$ : $g.(aH) = (ga)H$. Cette opération est transitive. Le stabilisateur de $aH$ est le conjugué de $H$, $aHa^{-1}$. En considérant le morphisme $\phi : G \longrightarrow \mathcal{S}(G/H)$ on a donc $\operatorname{Ker}\phi = \bigcap_{a \in G} aHa^{-1}$ ce qui montre que l'opération n'est pas fidèle en général.

5) Le groupe $G$ opère sur lui même par automorphismes intérieurs : $g.a = gag^{-1}$. Le stabilisateur de $a$, $H_a = \{g \in G | gag^{-1} = a\}$ est l'ensemble des éléments de $G$ commutant avec $a$, il est appelé centralisateur de $a$.

6) $G$ opère sur l'ensemble de ses sous groupes par conjuguaison : $g.H = gHg^{-1}$. Le stabilisateur de $H$ est noté $N_G(H) = \{g \in G | gHg^{-1} = H\}$ et est appelé normalisateur du sous groupe $H$, c'est le plus grand sous groupe de $G$ dans lequel $H$ est normal.

**Proposition.** 1) Soit $G$ un groupe opérant sur l'ensemble $X$ et $x \in X$ l'application $G/H_x \longrightarrow \omega(x),\ g \longmapsto gH_x$ est une bijection.

2) Si le groupe $G$ est fini $|\omega(x)| = [G : H_x] = \dfrac{|G|}{|H_x|}$.

3) Si le groupe $G$ et $X$ sont finis en notant $X = \bigcup_{i\in I} \omega(x_i)$, réunion d'orbites deux à deux disjointes, on a :

$$|X| = \sum_{i\in I}[G : H_{x_i}] = \sum_{i\in I} \frac{|G|}{|H_{x_i}|}$$

**Démonstration.** $g.x = h.x \iff h \in gH_x$ établit la conclusion.

Une conséquence importante de la proposition précédente est l'équation des classes.

**Proposition.** Equation des classes
Soit $G$ un groupe fini, opérant sur lui même par automorphismes intérieurs et $Z$ le centre du groupe. En utilisant les hypothèses du 3) de la proposition précédente on a :

$$|G| = |Z| + \sum_{i\in J}[G : C(y_i)]$$

où $\{y_i,\ i \in J\}$ est un ensemble de représentants des classes de conjugaison distinctes contenant plus d'un élément et $C(y_i)$ est le centralisateur de l'élément $y_i$.

## 3.2 Application : Sous groupes finis de $SO_3(\mathbb{R})$

**Théorème.** Tout sous groupe fini de $SO_3(\mathbb{R})$ est soit cyclique, engendré par une rotation d'axe $\Delta$ et d'angle $\dfrac{2\pi}{n},\ n \in \mathbb{N}^*$, soit un groupe $D_n$, soit isomorphe à $\mathcal{A}_4$ ou à $\mathcal{S}_4$ ou à $\mathcal{A}_5$.

**Lemme.** Les sous groupes finis de $SO_2(\mathbb{R})$ sont cycliques.

**Démonstration.** Il suffit didentifier $SO_2(\mathbb{R})$ et $\mathbb{U}$, ensemble des nombres complexes de module 1, par l'isomorphisme $g \longmapsto a$ qui à la rotation $g$ associe $a \in \mathbb{U}$ où $z \longmapsto az$ est la forme complexe de $g$. On utilise alors le résultat : Tous sous groupe multiplicatif fini d'un corps est cyclique (Voir 8 exercice 1)

**Démonstration.** Théorème
Soit $G$ un tel groupe non réduit à $Id_{\mathbb{R}^3}$, on note $n$ son ordre et $Id_{\mathbb{R}^3}$ sera noté $e$, la sphère unité sera notée $S$. L'axe de toute rotation $g$ différente de $e$ coupe $S$ en deux points appelés pôles de $g$, on note $P$ l'ensemble de ces pôles et $A$ l'ensemble des couples $(g, x)$,où $g$ est une rotation différente de $e$ et $x$ un pôle relatif à $g$, $|A| = 2(n-1)$.
Le groupe $G$ opère sur $P$ car si $x$ est un pôle de $g$ et $h \in G$, $h(x)$ est un pôle de $hgh^{-1}$, on notera $G_x$ le stabilisateur de $x$, ce sous groupe est cyclique et $|G_x| \geq 2$, la deuxième affirmation est immédiate, pour montrer la première on considère $g \in G,\ g \neq e$ dont $x$ est un pôle notons $P = (\mathbb{R}x)^\perp$, $P$ est stable par $g$ et $g|_P \in SO(P)$, le morphisme $G_x \longrightarrow SO(P), g \longmapsto g|_P$ est injectif car $\mathbb{R}^3 = (\mathbb{R}x)^\perp \oplus P$, $G_x$ est isomorphe à un sous groupe fini de $SO(P)$, il est donc cyclique d'après le lemme précédent.
On appelle $(\Omega)_{i\in[\![1,r]\!]}$ les orbites de $P$ sous $G$ avec $|\Omega_1| \geq \cdots \geq |\Omega_r|$ et $|G_x|$ ne dépend que de $i$ car si $y = h(x),\ h \in G,\ h \neq e$ on a alors $G_y = hG_xh^{-1}$, on notera $n_i = |G_x|,\ x \in \Omega_i$. On a $2 \leq n_1 \cdots \leq n_r$ car

$|\Omega_i| = \dfrac{|G|}{|G_x|}$.

Le nombre de couples de $A$ dans $\Omega_i$ est $(n_i-1)|\Omega_i| = \dfrac{n(n_i-1)}{n_i} = n\left(1-\dfrac{1}{n_i}\right)$, ce qui entraine

$|A| = n\sum_{i=1}^{r}\left(1-\dfrac{1}{n_i}\right) = 2(n-1)$ $(E)$.

$r = 1 \Longrightarrow 2(n-1) < n$ or $n = 1$ est exclu, donc $r > 1$. De plus $\left(1-\dfrac{1}{n_i}\right) \geq 1-\dfrac{1}{2}$ ce qui entraine avec $r \geq 4$, $2(n-1) = n\sum_{i=1}^{r}\left(1-\dfrac{1}{n_i}\right) \geq 2n$ les seules valeurs possibles sont donc $r = 2$ ou $r = 3$.

Si $r = 2$, on obtient à partir de $(E)$ $\dfrac{n}{n_1}+\dfrac{n}{n_2} = 2 \Longrightarrow n_1 = n_2 = n$. Soit $x_1 \in \Omega_1$ et $x_2 \in \Omega_2$, $G_{x_1} = G_{x_2} = G$, toute rotation $g \neq e$ a pour point fixe $x_1$et $x_2$, donc $x_2 = -x_1$ et $g$ est une rotation d'axe $(x_1, x_2)$. Le morphisme précédent $g \longmapsto g|_P$ montre que $G$ est cyclique, il est donc engendré par une rotation d'axe $(x_1, x_2)$ et d'angle $\dfrac{2\pi}{n}$.

Si $r = 3$ $n_1 = 2$. en effet si $n_1 \geq 3$ on a $n\sum_{i=1}^{3}\left(1-\dfrac{1}{n_i}\right) = 2(n-1) \geq 3n\left(1-\dfrac{1}{3}\right) = 2n$, ce qui est impossible.

Si $n_2 = 2$ alors $(E)$ entraine $n = 2n_3$. Le groupe $G$ est alors isomorphe au groupe diédral $D_{\frac{n}{2}}$. Montrons ce résultat.

Soit $x \in \Omega_3$, $G_x$ est un sous groupe cyclique d'ordre $n_3 = \dfrac{n}{2}$ engendré par $h$ et l'orbite de $x$ contient $\dfrac{|G|}{|G_x|} = 2$ éléments $x$ et $y \neq x$. Soit $g \in G - G_x$, $g(x) \neq x \Longrightarrow g(x) = y$ et on a aussi $g(y) = x$, d'où $g^2(x) = x$ et $g^2(y) = y$. Soit $z \notin \{x, y\}$ un pôle de $g$, donc de $g^2$, cette dernière rotation laissant plus deux fixes sur $S$, on a alors $g^2 = e$. On a alors $hg \notin G_x$ sinon $g \in G_x$, on a alors, comme pour $g$, $(hg)^2 = hghg = e$.

$[G : G_x] = 2$ et $g \notin G_x \Longrightarrow G = G_x \cup gG_x$. On a les relations :

$g^2 = e$, $h^{\frac{n}{2}} = e$, $hghg = e$, $G$ engendré par $h, g$, ce qui entraine $G \simeq D_{\frac{n}{2}}$.

Si $n_1 = 2, n_2 = 3$, on obtient à partir de $(E)$, $\dfrac{1}{n_3} = \dfrac{1}{6}+\dfrac{2}{n}$, il y a trois possibilités

a) $n_3 = 3$ donc $n = 12$, b) $n_3 = 4$ donc $n = 24$, c) $n_3 = 5$ donc $n = 60$.

a) $|\Omega_1| = 6$, $x \in \Omega_1 \Rightarrow |G_x| = 2 = n_1$, $|\Omega_2| = 4$, $y \in \Omega_2 \Rightarrow |G_y| = 3 = n_2$

$|\Omega_3| = 4$, $z \in \Omega_3 \Rightarrow |G_z| = 3 = n_3$.

Les éléments de $G$ non triviaux de $G$ sont donc d'ordre 2 ou 3. Notons $\Omega_2 = \{a, b, c, d\}$, l'action de $g$ sur $\Omega_2$ induit un morphisme de $G$ dans $\mathcal{S}_4$, injectif car si $g$ laisse quatre points fixes c'est l'identité, or l'unique sous groupe de $\mathcal{S}_4$ d'ordre 12 est $\mathcal{A}_4$, on a donc $G \simeq \mathcal{A}_4$.

b) On a $\Omega_2 = \{(a,-a),(b,-b),(c,-c),(d,-d)\}$, $G$ agit sur ces couples car l'ordre de $G_a$, $a \in \Omega_2$ est égal à 3, différents des deux autres cas.

On otient alors un morphisme injectif $G$ dans $\mathcal{S}_4$, car si $g$ fixe quatre paires, il laisse globalement invariantes quatre droites de l'espace engendrant au moins un plan sur lequel $g$ est une homothétie, en complétant une base orthonormale du plan pour avoir une base orthonormale de l'espace, on obtient le résultat à partir de l'écriture canonique de $g$. d'où $G \simeq \mathcal{S}_4$.

c) On a $\Omega_2 = \{(x_i, -x_i),\ i \in [\![1, 15]\!]\}$, comme dans b) $G$ agit sur ces couples de pôles. Soit $\{(x,-x) \in \Omega_2^2\}$, pôles de $g \in G$. $G$ opère transitivement sur $\Omega_2$, il existe donc $g' \in G$ telle que $g'(x) = -x$. Les quatres rotations $e, g, g', gg'$ laissent $\{x, -x\}$ globalement invariant, ce sont les seules. Si $g''(x) = x, g \in G_x = \{e, g\}$, si $g''(x) = -x$, $g''g'^{-1} \in G_x$ d'où $g'' = g'$ ou $g'' = gg' = g'g$.

Soit $y$ et $-y$ les pôles de $g'$, on a $gg'(y) = g(y) = g'g(y) \Longrightarrow g(y) = \pm y$, chacune des trois rotations $g, g', gg'$

conserve globalement les couples de leurs pôles respectifs. Soient $y$ et $-y$ pôles de $g'$ et $x$ et $-x$ ceux de $g$. $gg'(y) = g(y) = -x = g'g(y)$, $g(y)$ est donc un pôle de $g'$. On peut répartir les 3 pôles d'ordre 2 en cinq ensembles de six pôles $P_2^i,\ i \in [\![1,5]\!]$, formant un ensemble $E$ sur lequel $G$ opère (le vérifier). On peut alors etablir un morphisme de groupes :
$\phi : G \longrightarrow \mathcal{S}_5$ qui à $g \in G$ associe une permutation des $P_2^i$. On montre comme précédement que ce morphisme est injectif, $\mathcal{A}_5$ étant le seul sous groupe d'ordre 60 de $\mathcal{S}_5$, on a bien $G \simeq \mathcal{A}_5$.

# 4 Théorèmes de Sylow

Le théorème de Lagrange montre que si $H$ est un sous groupe du groupe fini, $|H| \mid |G|$, la réciproque est fausse en général. ainsi $|\mathcal{A}_4| = 12$ mais il n'admet aucun sous groupe de cardinal 6. Il existe un cas où la propriété est vraie.

**Définition.** Soit $G$ un groupe fini de cardinal $n = p^e\, m$ avec $p$ premier et $p \wedge m = 1$. Un sous groupe de Sylow de $G$ est un sous groupe de cardinal $p^e$. Autrement dit $H$ est un $p$-groupe tel que $[G : H]$ est premier avec $p$.

**Exemple.** Soit $\mathbb{K} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $p$ premier et $G = GL(n, \mathbb{K})$. en comptant les bases de $\mathbb{K}^n$, on obtient :

$$|G| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}) = mp^{\frac{n(n-1)}{2}},\ \ p \wedge m = 1.$$

L'ensemble des matrices triangulaires supérieures strictes est un sous groupe de Sylow de $G$.

$$H = \{A = (a_{ij}) | a_{ii} = 1,\ i > j \Longrightarrow a_{ij} = 0\},\ \ |H| = p.p^2.\cdots.p^{n-1} = p^{\frac{n(n-1)}{2}}.$$

**Lemme.** Soit $G$ un groupe abélien et $p \in \mathbb{N}$ premier tel que $p \mid |G|$ alors $G$ contient un élément d'ordre $p$.

**Démonstration.** On fait une récurrence sur $|G|$. Si $|G| = p$ c'est immédiat. Si $|G| > p$ soit $a \in G$. Si $p|O(a)$ où $O(a)$ est l'ordre de a, soit $O(a) = p.r$ alors $a^r$ a pour ordre $p$. sinon on considère $G' = G/ < a >$ qui a un ordre strictement plus petit que celui de $G$ et $p||G'|$. L'hypothése de récurrence entraine l'existence d'un élément $b < a >$ d'ordre $p$ auquel cas $p|O(b)$ et on est ramené au premier cas.

**Théorème.** de Sylow I
Soit $G$ un groupe fini et $p \in \mathbb{N}$ premier. Si $p^k \mid |G|,\ k \in \mathbb{N}^*$ alors $G$ contient un sous groupe d'ordre $p^k$, donc en particulier un sous groupe de Sylow.

**Démonstration.** On fait une récurrence sur $|G|$. Si $|G| = p$ c'est immédiat. Supposons $|G| = p^e m$ avec $e \in \mathbb{N}^*,\ m \wedge p = 1$.
en appelant $Z$ le centre de $G$ et en utilisant l'équation des classes :

$$|G| = |Z| + \sum_{i \in J} [G : C(y_i)]$$

Soit $p \not| |Z|$, dans ce cas il existe $i \in J$ tel que $p \not| [G : C(y_i)]$ alors $p^k | C(y_i)$ et $|C(y_i)| < |G|$ d'où le résultat dans ce cas.
Soit $p \mid |Z|$, dans ce cas le lemme précédent montre l'existence de $c \in Z$ d'ordre $p$, or $< c >$ est un sous groupe normal de $G$ d'ordre $p$ le groupe quotient $G/ < c >$ est tel que son ordre est divisible par $p^{k-1}$, il contient donc, d'après l'hypothèse de récurrence un sous groupe de la forme $H/ < c >$ d'ordre $p^{k-1}$, le sous groupe $H$ de $G$ est alors de cardinal $p^k$.

**Théorème.** de Sylow II
1) Deux $p$ sous groupes de Sylow sont conjugués dans $G$.
2) Le nombre de $p$ sous groupes de Sylow divise l'indice de n'importe quel $p$ sous groupe de Sylow et est congru à 1 modulo $p$.
3) Tout sous groupe d'ordre $p^k$ est inclus dans un $p$ sous groupe de Sylow.

**Lemme.** Soit $P$ un sous groupe de Sylow de $G$ et $H$ un sous groupe de cardinal $p^k$ inclus dans le normalisateur $N(P)$ de $P$. On a alors $H \subset P$.

**Démonstration.** $P \lhd N(P)$ entraine que $HP$ est un sous groupe de $N(P)$ et on a $HP/P \simeq H/(H \cap P)$ (théorème d'isomorphisme). ceci entraine que $HP/P$ a un ordre de la forme $p^l$ et $|HP| = p^l|P|$, or $P$ étant un $p$ sous groupe de Sylow on a $l = 0$, $HP = P$ ce qui entraine que $H \subset P$.

**Démonstration.** Théorème
On appelle $\Gamma$ l'ensemble des $p$ sous groupes de Sylow et on fait opérer $G$ par conjuguaison sur $\Gamma$. On considère $\Sigma$ une orbite pour cette opération et $P \in \Sigma$. Faisons opérer le $p$ sous groupe de Sylow $P$ sur $\Sigma$. L'orbite de $P$ est alors réduite à $\{P\}$, c'est la seule qui contient un seul élément : Si $\{P'\}$ était une telle orbite, on aurait $P \subset N(P')$ soit $P = P'$ d'aprés le lemme. Chaque autre $P$ orbite a un cardinal qui divise $|P|$ donc une puissance de $p$, on a donc bien $|\Sigma| \equiv 1$ modulo $p$ . Suppsons qu'il existe un $p$ sous groupe de Sylow $Q$ qui n'est pas élément de $\Sigma$ en faisant $Q$ opérer sur $\Sigma$, on obtiendrait, $|\Sigma| \equiv 0$ modulo $p$ en utilisant le même raisonnement, ce qui est contradictoire. Les $p$ sous groupe de Sylow sont donc tous conjugués.

On a $[G : P] = [G : N(P)][N(P) : P]$ or $[G : N(P)]$ est le nombre d'éléments dans l'orbite du $p$ sous groupe de Sylow $P$. Soit $H$ sous groupe de cardinal $p^k,\ k \in \mathbb{N}$, faisons opérer $H$ sur $\Sigma$. Les orbites contiennent un nombre d'éléments de la forme $p^l,\ l \in \mathbb{N}$ et $|\Sigma| \equiv 1$ modulo $p$ entraine qu'une orbite a un seul élément $P$, on a donc $H \subset P$ d'après le lemme.

**Remarque.** En posant $|G| = p^e\, m,\ p \wedge m = 1$, le nombre de $p$ Sylow de $G$ est un diviseur de $m$. On a $[G : P] = m \Longrightarrow [G : N(P)]|m$.

**Exemple.** Application.
Un groupe $G$ de cardinal 63 n'est pas simple. Etudions les 7 sous groupes de $G$. Leur nombre $k$ est congru à 1 modulo 7 et $k$ divise 9 ce qui entraine que $k = 1$. ce qui montre que ce 7 sous groupe de Sylow est normal, il est le seul élément de l'orbite.

# 5 Automorphismes de $\mathbb{Z}/n\mathbb{Z}$

## 5.1 Eléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

**Proposition.** Les conditions suivantes sont équivalentes
- $\overline{x}$ est inversible dans $\mathbb{Z}/a\mathbb{Z}$.
- $\overline{x}$ n'est pas diviseur de zéro dans $\mathbb{Z}/a\mathbb{Z}$.
- $x$ est premier avec $a$.

**Démonstration.** Supposons $\overline{x}$ inversible dans $\mathbb{Z}/a\mathbb{Z}$.
Soit $\overline{y}$ tel que $\overline{x}.\overline{y} = 0$. On a alors $\overline{x}^{-1}.(\overline{x}.\overline{y}) = 0$ c'est à dire $\overline{y} = 0$, $\overline{x}$ n'est donc pas diviseur de zéro.
Supposons que $x$ ne soit pas premier avec $a$, soit $d = a \wedge x \neq 1$
$x = dx_1$, $a = da_1 \Rightarrow \overline{x}.\overline{a_1} = \overline{x_1}.\overline{a} = \overline{0}$ et $\overline{x}$ est diviseur de zéro dans $\mathbb{Z}/a\mathbb{Z}$.
Supposons $x$ premier avec $a$. En utilisant le théorème de Bezout, il existe des entiers relatifs $k$ et $l$ tels que $kx + la = 1$ ce qui entraîne $\overline{k}.\overline{x} = \overline{1}$, $\overline{x}$ est donc inversible.

**Définition.** On appelle fonction d'Euler et on note $\phi(n)$ le nombre d'entiers $k$ tels que $1 \leq k \leq n$ et $k \wedge n = 1$.

**Proposition.** Soit $n = \prod_{i=1}^{r} p_i^{e_i}$, on a $\phi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

**Démonstration.** Dans le cas où $p$ est premier, $\phi(p) = p - 1$ car $\mathbb{Z}/p\mathbb{Z}$ est un corps
$\phi(p^e) = p^e - p^{e-1} = p^e \left(1 - \frac{1}{p}\right)$.
$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p^{e_i}\mathbb{Z})^*$ où $(\mathbb{Z}/n\mathbb{Z})^*$ est l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

**Proposition.** On a $\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$, l'automorphisme étant caractérisé par $u \in \mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z}) \longmapsto u(1)$.

## 5.2 Applications

**Théorème-définition.** Soient $H$ et $N$ deux groupes et $\mathrm{Aut}(N)$ le groupe des automorphismes de groupe de $N$ et $\phi : H \longrightarrow \mathrm{Aut}(N)$ un morphisme de groupes. On définit sur $N \times H$ une loi définie par :

$$(n, h)(n', h') = (n\phi(h)(n'), hh')$$

Muni de cette loi $N \times H$ a une structure de groupe, appelé produit semi direct de $N$ par $H$ relativement à $\phi$, il est noté : $N \rtimes_\phi H$

**Remarque.** Sous les hypothéses précédentes on a la suite exacte :

$$1 \longrightarrow N \xrightarrow{i} N \rtimes_\phi H \xrightarrow{p} H \longrightarrow 1$$

où $i : n \longmapsto (n, 1)$ est injective et $p : (n, h) \longmapsto h$ est surjective. En notant $\overline{H} = \{(1, h) | h \in H\}$ et $s : H \longrightarrow \overline{H},\ h \longmapsto (1, h)$. On traduit ceci en disant que $N \rtimes_\phi H$ est une extension du groupe $N$ par le groupe $H$. On a $p \circ s = Id_H$, ce qui signifie que l'extension de groupes est scindée.

**Proposition.** Soient un groupe $G$ et $H, N$ deux sous groupes de $G$ tels que a) $N \lhd G$
b) $N \cap H = \{1\}$, c) $G = NH$. $G$ est un produit semi direct $N \rtimes_\phi H$ où $\phi : H \longrightarrow \mathrm{Aut}\,(N)$ est défini par $\phi(h)(n) = hnh^{-1} \in N$.

**Démonstration.** Tout élément de $G$ s'écrit de manière unique sous la forme $g = nh$, l'unicité étant une conséquence de b). On a de plus, avec $(n, n') \in N^2,\ (h, h') \in H^2$
$(nh)(n'h') = n(hn'h^{-1})hh'$ et $hn'h^{-1} \in N$

**Corollaire.** A toute suite exacte scindée

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

correspond un morphisme de groupes $\phi : H \longrightarrow \mathrm{Aut}(N)$ tel que $G \simeq N \rtimes_\phi H$.

**Démonstration.** Avec les notations précédentes, $G \simeq N' \rtimes_\phi H'$ où $N' = i(N)$ et $H' = s(H)$, vérifiant les propriétés de la proposition précédente.

**Exemple.** Groupe diédral $D_n$ engendré par la rotation $r$ et la réflexion $s$. On a alors la suite exacte scindée :

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{i} D_n \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

où $s(\overline{1}) = s$.
$i(\overline{k}) = r^k,\ p(r^k) = \overline{0},\ p(sr^k) = \overline{1}$.
On a donc $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

**Théorème.** Groupes d'ordre $pq$.
Soit $G$ un groupe d'ordre $pq$ où $p < q$ sont des nombres premiers.

1. Si $q$ n'est pas congru à 1 modulo $p$, $G \simeq \mathbb{Z}/pq\mathbb{Z}$.
2. Si $q$ est congru à 1 modulo $p$, $G$ a deux structures possibles, à isomorphisme près. Ou bien $G \simeq \mathbb{Z}/pq\mathbb{Z}$
   ou bien $G$ n'est pas commutatif et dans ce cas. $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$.

**Démonstration.** D'après les théorèmes de Sylow, il existe un sous groupe de Sylow $H$ d'ordre $q$ et un sous groupe de Sylow $K$ d'ordre $p$. D'aprés le theorème de Sylow II, Il existe un seul un sous groupe de Sylow d'ordre $q$, il est donc normal, de plus $|H \cap K|$ divise $p$ et $q$ et donc $H \cap K = \{1\}$ ce qui entraine que $|HK| = |H||K| = pq$ d'où $G = HK$, $G$ est donc produit semi direct de $H$ par $K$.
1) Supposons que $q$ n'est pas congru à 1 modulo $p$, il y a alors un seul groupe de Sylow d'ordre $p$, soit $K$ et donc $K \lhd G$, ce qui entraine que $G \simeq H \times K$, produit direct des groupes avec $H \simeq \mathbb{Z}/q\mathbb{Z}$ et $K \simeq \mathbb{Z}/p\mathbb{Z}$ d'où $G \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$ car $p \wedge q = 1$.

2) Si $q$ est congru à 1 modulo $p$, l'ordre de l'image de $\phi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Aut}\,(\mathbb{Z}/q\mathbb{Z})$ divise $p$, elle vaut donc 1 ou $p$, dans le premier cas $\forall \overline{k} \in \mathbb{Z}/p\mathbb{Z},\ \phi(\overline{k}) = Id$ et le produit de $H$ par $K$ est direct.
Dans le deuxième cas,, il existe dans $\mathrm{Aut}\,(\mathbb{Z}/q\mathbb{Z})$ un unique sous groupe $\Gamma$ d'ordre $p$, $\phi$ est un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur $\Gamma$, déterminé par le choix de $\phi(\overline{1}) = \gamma$ parmi les $p-1$ générateurs de $\Gamma$. Si $\phi'$ est un autre isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur $\Gamma$, $\alpha = \phi'^{-1} \circ \phi$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, il existe alors un isomorphisme de $H \rtimes_\phi K$ sur $H \rtimes_{\phi'} K$.

**Remarque.** Soit $q > 2$ premier, ce résultat permet de retrouver $D_q \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

# 6 Simplicité de $\mathcal{A}_n$

**Théorème.** Si $n \geq 5$, le groupe alterné $\mathcal{A}_n$ est simple.

**Démonstration.** Soit $N$ un sous groupe normal de $\mathcal{A}_n$, montrons que $N$ contient un cycle d'ordre 3, il les contiendra tous dans ce cas car ils sont conjugués.
Soit $\sigma \in N,\ \sigma \neq Id$ tel que $\sigma$ admette un nombre maximal de points fixes. Décomposons $[\![1, n]\!]$ comme réunion d'orbites disjointes du groupe $< \sigma >$, certaines orbites ont au moins deux éléments. Supposons que toutes les orbites ont deux éléments, en dehors des points fixes. Il en existe au moins deux car la permutation est paire. Soit $\sigma = (i, j)(r, s)$.
Soit $k \neq i, j, r, s$ et $\tau = (r, s, k)$, on considère $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$ et $\sigma'$ laisse $i, j$ fixés, ainsi que tout élément fixés par $\sigma$, à part $k$, ce qui contredit l'hypothèse car $\sigma'$ a plus de points fixes que $\sigma$.

On est ramené au cas où au moins une orbite de $< \sigma >$ a 3 ou plus de 3 éléments. Si $\sigma$ n'est pas réduit au cycle $(i,j,k)$, il existe au moins deux autres éléments $r,s$ modifiés par $\sigma$, car $\sigma$ est paire. Soit $\tau = (k,r,s)$ et $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$ comme précédement. On a $\sigma'(i) = i$ et tous les points fixés par $\sigma$ le sont par $\sigma'$, ce qui contredit à nouveau l'hypothèse et qui montre que $\sigma$ est un cycle d'ordre 3.

**Corollaire.** On a $D(\mathcal{A}_n) = \mathcal{A}_n$ si $n \geq 5$ et $D(\mathcal{S}_n) = \mathcal{A}_n$ pour $n \geq 2$.

**Proposition.** 1) Les sous groupes distingués de $\mathcal{A}_4$ sont
$\{Id\}$, $V = \{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, $V$ étant commutatif et $\mathcal{A}_4$.
Ce qui montre que $\mathcal{A}_4$ n'est pas simple.
2) On a $D(\mathcal{A}_4) = V$.

**Démonstration.** 1) Soit $H \lhd \mathcal{A}_4$. Il suffit de distinguer les cas où $H$ contient un cycle d'ordre 3 ou non.

2) On remarque que le groupe $\mathcal{A}_4/V$ est de cardinal 3, donc commutatif, ce qui entraine que $D(\mathcal{A}_4) \subset V$, or $\mathcal{A}_4$ n'éatant pas commutatif ceci entraine que $\mathcal{A}_4 = V$.

**Proposition.** Si $n \geq 5$ les sous groupes distingués de $\mathcal{S}_n$ sont $\{Id\}, \mathcal{A}_n$ et $\mathcal{S}_n$.

**Démonstration.** Soit $H \lhd \mathcal{S}_n$, on a alors $H \cap \mathcal{A}_n = \{Id\}$ ou $\mathcal{A}_n$, dans le deuxième cas ceci entraine soit $H = \mathcal{A}_n$, soit $H = \mathcal{S}_n$.

Si $H \cap \mathcal{A}_n = \{Id\}$, $H\mathcal{A}_n$ est un sous groupe de $\mathcal{S}_n$ isomorphe à $H \times \mathcal{A}_n$ car ces deux sous groupes sont nornaux dans $\mathcal{S}_n$, ceci entraine que $|H| \leq 2$ sinon on aurait $|H\mathcal{A}_n| > 2|\mathcal{A}_n| = n!$. si $H \neq \{Id\}$, $|H| = 2$, soit $H = \{Id, (i,j)\}$ mais dans ce cas $H$, qui est distingué contiendrait tous les conjugués de $(i,j)$, c'est à dire toutes les transpositions, ce qui est contradictoire.

# 7 Exercices

**Exercice 1.** 1) Montrer que le groupe multiplicatif d'un corps fini est cyclique. en déduire que $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.
2) Montrer que si $p$ est un nombre premier supérieur ou égal à 3 et $\alpha$ un entier supérieur ou égal à 2 on a $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$ où $\phi(p^\alpha) = p^{\alpha-1}(p-1)$.
On montrera que $1+p$ est un élément d'ordre $p^{\alpha-1}$ de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ puis qu'il existe un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.

**Exercice 2.** soit $G$ un groupe fini dont tout sous groupe propre est cyclique.
1) $G$ est il cyclique ? abélien ?
2) Si $G$ est abélien, est il cyclique ?

**Exercice 3.** 1) Montrer que tout groupe simple $G$ d'ordre soixante est isomorphe à $\mathcal{A}_5$.
2) en utilisant le résultat précédent redémontrer le cas $n = 60$ dans l'étude des sous groupes finis de $SO_3(\mathbb{R})$.

**Exercice 4.** Formule de Burnside.
Soit $G$ un groupe fini opérant sur un ensemble fini $X$. Pour tout $g \in G$ on définit $\mathrm{Fix}_X(g) = \{x \in X | g.x = x\}$ et on note $\mathrm{Orb}_X(G)$ l'esemble des $G$-orbites dans $X$.
Montrer que

$$|\mathrm{Orb}_X(G)| = \frac{1}{|G|}\sum_{g\in G} |\mathrm{Fix}_X(g)|.$$

**Exercice 5.** Théorème de Cauchy.
Soit $G$ un groupe fini dont l'ordre est divisible par $p$ premier.
On définit $X = \{(x_1, \cdots, x_p) | x_1 \cdots x_p = e\}$. On fait $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$ opérer sur $X$ par
$\overline{k}.(x_1, \cdots, x_p) = (x_{\overline{1+k}}, \cdots, x_{\overline{p+k}})$.
1) Montrer que $|X| = |G|^{p-1}$. Vérifier que la définition précédente permet bien d'obtenir une opération de $\mathbb{K}$ sur $X$.
2) Montrer que l'orbite de $a = (e, \cdots, e) \in X$ contient un seul élément. Montrer que si l'orbite de $b = (x_1, \cdots, x_p) \in X,\ b \neq a$ admet un seul élément alors $x_1$ est élément d'ordre $p$ de $G$.
3) Montrer qu'il est impossible que $a$ soit le seul élément de $G$ dont l'orbite ne contient que lui même en remarquant que dans le cas contraire chaque orbite, sauf une, contient $p$ éléments.
Ceci démontre, sans l'utilisation de théorème de Sylow, que $G$ contient un élément d'ordre $p$.

**Exercice 6.** Soient $G$ un groupe fini, $p$ un nombre premier divisant l'ordre de $G$ et $H$ un sous groupe de $G$. Montrer que si $P$ est un $p$-sous groupe de Sylow de $G$ tel que $N_G(P) \subset H$, alors $N_G(H) = H$.

**Exercice 7.** Soient $G$ un groupe fini, $N$ un sous groupe normal de $G$ et $p$ un nombre premier divisant l'ordre de $N$. Montrer que si $P$ est un $p$-sous groupe de Sylow de $N$, alors
$G = N.N_G(P)$.

**Exercice 8.** Montrer qu'un groupe d'ordre $pqr$, avec $p, q, r$ nombres premiers distincts n'est pas simple.

**Exercice 9.** Montrer qu'il n'existe aucun groupe simple d'ordre 300.

**Exercice 10.** Le but de cet exercice est de montrer que pour $n \neq 6$ les automorphismes de $\mathcal{S}_n$ sont les automorphismes intérieurs.
1) Soit $\phi$ un automorphisme de $\mathcal{S}_n,\ n \neq 6$, montrer que l'image d'une transposition est une transposition en utilisant un argument de cardinalité.
2) Pour tout $i \in [\![2, n]\!]$, on pose $\tau_i = (1, i)$ et $\phi(\tau_i) = (a_i, b_i)$.
Montrer que si $i \neq j$, on a $\{a_i, b_i\} \cap \{a_j, b_j\} \neq \emptyset$.
3) On suppose, quitte à échanger $a_3$et $b_3$ que $a_2 = a_3$. Montrer que $a_3$ appartient au support de $\phi(\tau_i)$ pour tout $i \in [\![3, n]\!]$. On raisonnera par récurrence.
4) En déduire que $\phi$ est un automorphisme intérieur.

# 8 Correction

**Solution 1.** 1) On utilise le résultat suivant que l'on laisse au lecteur le soin de vérifier.
Soient $x, y$ éléments de $\mathbb{K}^*$, sous groupe multiplicatif de $K$, d'ordres respectifs $m$ et $n$ premiers entre eux, l'ordre de $xy$ est $mn$. Il existe donc un élément $x \in \mathbb{F}_q^*$ dont l'ordre est le plus petit commun multiple $\alpha$ des ordres de tous les éléments, $\alpha$ correspond au facteur invariant $n_t$ du théorème de la page 3.
Montrons un résultat plus général : Tout sous groupe fini $G$ du groupe multiplicatif d'un corps est cyclique.
Soit $|G| = q$ D'une part $\forall u \in G\ ,\ u^\alpha = 1$, d'autre part $\forall u \in G\ ,\ u^q = 1$, $\alpha$ étant d'après sa définition le plus petit entier vérifiant cette propriété, on a $\alpha \leq q$. Le polynôme $X^\alpha - 1$ ayant au plus $\alpha$ racines distinctes dans le corps $\mathbb{K}$, on a $q \leq \alpha$ ce qui entraîne l'égalité entre ces deux nombres. Ceci démontre que $x$ engendre le groupe multiplicatif $G$, tout élément de ce groupe est donc une puissance de $x$.

2) On montre par récurrence le résultat : Si $k \in \mathbb{N}$, $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec $\lambda \in \mathbb{N}^*$ premier avec $p$.

$$2 \leq i < p,\ p^3 | \binom{p}{i} p^i \text{ et si } p \geq 3,\ p^3 | p^p \Longrightarrow (1+p)^p = 1 + p^2 + up^3 = 1 + p^2(1+up)$$

d'où $\lambda = 1 + up \wedge p = 1$. le résultat est vrai pour $k = 1$. Supposons le résultat vrai au rang $k$.

$$(1+p)^{p^{k+1}} = \left(1 + \lambda p^{k+1}\right)^p = 1 + \sum_{i-1}^{p-1} \binom{p}{i} \lambda^i p^{(k+1)i} + \lambda^p p^{(k+1)p}.$$

Pour $i \geq 3$ on a $p^{k+3}$ en facteur, donc

$$(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda + up) \Rightarrow (1+p)^{p^{\alpha-1}} = 1 + \lambda p^{\alpha} \text{ et } (1+p)^{p^{\alpha-2}} = 1 + \lambda p^{\alpha-1}$$

ce qui montre que $(1+p)^{p^{\alpha-1}}$ est bien dordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^*$.

On considère alors le morphisme surjectif $\psi : (\mathbb{Z}/p^{\alpha}\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$ et on choisit dans $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^*$ un élément $x$ tel que $\psi(x)$ engendre le groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$. L'ordre de $x$ est un multiple de $p-1$ et il existe $y \in < x >$ d'ordre $p-1$ et ceci entraine que l'ordre de $y(1+p)$ est $p^{\alpha-1}(p-1)$ car leurs ordres sont premiers entre eux.

**Solution 2.** 1) Réponse négative . Exemple $\mathcal{S}_3$ dont les sous groupes propres sont d'ordre deux ou trois et donc cycliques.
2) Réponse négative . Exemple $(\mathbb{Z}/p\mathbb{Z})^2$.

**Solution 3.** 1) On a $60 = 2^2.3.5$, le nombre de 5-sylow est $n_5 = 1+5k$ et $n_5|12$, d'où $n_5 = 1$ ou 6, et $n_5 = 6$ sinon le 5-sylow serait normal dans $G$. Le groupe $G$ agit transitivement par conjuguaison sur l'ensemble des 5-sylow, ce qui entraine l'existence d'un morphisme $\Sigma : G \longrightarrow \mathcal{S}_6$ non trivial car l'action est transitive, on
$\operatorname{Ker}\Sigma = \{e\}$ car $G$ est simple, $G$ est donc isomorphe à un sous groupe de $\mathcal{S}_6$.
$D(G) = G \subset D(\mathcal{S}_6 = \mathcal{A}_6)$ car $G$ n'est pas commutatif et est simple. $G$ n'est pas distindué dans $\mathcal{A}_6$ car ce derneir groupe est simple (voir cours). Notons $X$ l'ensemble des classes à gauche de $\mathcal{A}_6$ relativement à $G$ (où $G$ et $\Sigma(G)$ sont confondus) ; $|X| = 6$. $G$ agit par translations à gauche sur $X$ par :

$$\phi : G \longrightarrow \mathcal{S}_{\mathcal{X}} \simeq \mathcal{S}_6,\ g \longmapsto (xG \mapsto (gx)G)$$

, le morphisme étnt non trivial car $G$ n'est pas distingué

dans $\mathcal{S}_6$, on a donc $G \simeq \phi(G)$ or $\forall g \in G,\ \phi(g)(G) = G$, $g$ est fixe pour tous les éléments de $\phi(G)$ ce qui entraine que $\phi(G)$ est isomorphe à un sous groupe de $\mathcal{S}_5$, d'où $\phi(G) \subset D(\mathcal{S}_5) = \mathcal{A}_5$ d'où $G \simeq \mathcal{A}_5$ par égalité des cardinaux.

2) Soit $g \in G$, $g$ a deux pôles, donc $g \in G_a$ et $g$ est d'ordre 2,3 ou 5. Les pôles d'une orbite étant deux à deux opposés, il existe 15 sous groupes d'ordre deux (car $|\Omega_1| = 30$), 10 sous groupes d'ordre 3 et 6 sous groupes d'ordre 5, ce sont les seuls sous groupes de $G$. Notons $G(p)$ l'ensemble des éléments de $G$ d'ordre $p \in \{2,3,5\}$, $|G(2)| = 15$, $|G(3)| = 20$, $|G(5)| = 24$. Soit $H \lhd G$. Si $H$ contient un sous groupe d'ordre 5 (qui est un 5-sylow), il les contient tous car ils sont conjugués donc $6|\ |H|$, de même s'il contient un 3-sylow il les contient tous, dans ce cas $10|\ |H|$ et dans ce dernier cas, il contient donc un élément d'ordre 5 (théorème de sylow II ou théorème de Cauchy), donc les 24 éléments d'ordre 5, autrement dit il contient $G(3) \cup G(5)$ ce qui entraine $|H| \geq 20 + 24 = 44$ d'où $H = G$, de même si $2|\ |H|$, alors $15|\ |H|$ et on en conclut à nouveau que $H = G$, d'où $G$ est simple et $G \simeq \mathcal{A}_5$.

**Solution 4.** Supposons dans un premier temps que l'oération soit transitive et notons
$S = \{(g,x) \in G \times X | g.x = x\}$. On a d'une part $|S| = \sum_{g \in G} |\operatorname{Fix}_X(g)|$, d'autre part
$|S| = \sum_{x \in X} |G_x| = |X|\frac{|G|}{|X|} = |G|$, $G_x$ étant le stabilisateur de $x \in X$. ce qui entraine
$1 = |\operatorname{Orb}_X(G)| = \frac{1}{|G|}\sum_{g \in G} |\operatorname{Fix}_X(g)|$.
Dans le cas général, appelons $\Omega_1, \cdots, \Omega_k$ les $k$ orbites, on a alors :

$$\operatorname{Fix}_X(g) = \bigcup_{i=1}^{k} \operatorname{Fix}_{\Omega_i}(g),\ |\operatorname{Fix}_X(g)| = \sum_{i=1}^{k} |\operatorname{Fix}_{\Omega_i}(g)|$$

d'où

$$\frac{1}{|G|}\sum_{g \in G} |\operatorname{Fix}_X(g)| = \frac{1}{|G|}\sum_{g \in G}\sum_{i=1}^{k} |\operatorname{Fix}_{\Omega_i}(g)| = \sum_{i=1}^{k} \frac{1}{|G|}\sum_{g \in G} |\operatorname{Fix}_{\Omega_i}(g)| = k$$

**Solution 5.** 1) $x = (x_1, \cdots, x_p) \in X \Longleftrightarrow x_p = x_1^{-1} \cdots x_{p-1}^{-1}$ d'où $|X| = |G|^{p-1}$. On vérifie aisément que

$$\overline{k}.\left(\overline{l}.x\right) = (\overline{k+l}).x,\ \overline{0}.x = x$$

2) On a bien $\overline{k}.a = a$. Si $x = (x_1, \cdots, x_p) \in X, x \neq a$ tel que $\forall k \in \mathbb{K},\ \overline{k}.x = x$, alors
$\forall k \in \mathbb{K},\ x_{\overline{1+k}} = x_1$, d'où $x_1 = x_2 = \cdots = x_p$ d'où $x_1^p = 1$ et $x_1 \neq e$.

3) Si $a$ est le seul élément de $X$ dont l'orbite contient un seul élément et $x \neq e$ l'ordre de $\Omega_x$, orbite de $x$ est $p$ car $p|\ |\Omega_x|$ et $|\Omega_x| \neq 1$ d'où $|X| = 1 + mp$, $m$ étant le nombre de telles orbites, or ceci est impossible car $p|\ |X|$.

**Solution 6.** Il suffit de montrer que $N_G(H) \subset H$. $P$ est un $p$-sous groupe de Sylow de $H$.
Soit $n \in N_G(H)$, $P \subset H \Longrightarrow nPn^{-1} \subset H$ et $|nPn^{-1}| = |P|$ donc $nPn^{-1}$ est un $p$-sous groupe de Sylow de $H$, il est donc conjugué avec $P$.
$\exists h \in H,\ P = h(nPn^{-1})h^{-1}$, on a donc $hn \in N_G(P),\ hn = h' \in N_G(P)$, d'où $n = h^{-1}h' \in H$.

**Solution 7.** Soit $g \in G$, on a : $P \subset N$ et $N \lhd G \Longrightarrow gPg^{-1} \subset N$, le sous groupe $gPg^{-1}$ est donc un $p$-sous groupe de sylow de $N$, il est donc conjougué avec $P$ dans $N$ :
$\exists n \in N,\ n(gPg^{-1})n^{-1} = P \Longrightarrow ng \in N_G(P)$, on a donc $g \in n^{-1}N_G(P) \subset N.N_G(P)$ ce qui montre que $G \subset N.N_G(P)$ et donc l'égalité entre ces groupes.

**Solution 8.** On suppose $p > q > r$ et on appelle $n_p, n_q, n_r$ respectivement le nombre de $p$ (respectivement $q$, respectivement $r$) sous groupes de Sylow. L'intersection d'un $p$-sous groupe de Sylow et d'un $q$-sous groupe de Sylow est réduite à l'élément neutre, même chose pour les deux autres cas . Supposons
$n_p > 1,\ n_q > 1,\ n_r > 1$. L'ensemble de ces sous groupes de Sylow contient
$N = n_p(p-1)+n_q(q-1)+n_r(r-1)+1$ éléments. Le deuxième théorème de Sylow entraine que $n_p \in \{q, r, qr\}$ et $n_p$ étant congru à 1 modulo $p$ et $p > q > r$ on a donc $n_p = qr$. On établit de la même manière que $n_q > p$ et $n_r > q$, d'où $N > qr(p-1) + p(q-1) + q(r-1) = pqr + (p-1)(q-1)$, d'où $N > pqr$, cette contradiction entraine que $n_p$ ou $n_q$ ou $n_r$ est égal à 1 et que le groupe n'est pas simple.

**Solution 9.** On a $300 = 2^2.3.5^2$. Le nombre $n_5$ de 5-sylow est 1 ou 6 (théorème de Sylow II). Si $n_5 = 1$, le sous groupe en question est normal dans $G$ qui n'est pas simple.
Si $n_5 = 6$ , on fait opérer $G$ sur l'ensemble des 5-Sylow par conjugaison. En notant $S_5(G)$ l'ensemble de ces six sous groupes, ceci permet de définir un morphisme
$\phi : G \longrightarrow \mathcal{S}_{S_5(G)} \simeq \mathcal{S}_6$, et $\operatorname{Ker}\phi$ est normal dans $G$.
Si $\operatorname{Ker}\phi = \{e\}$ $\phi$ est injectif et donc $G$ est isomorphe à un sous groupe de $\mathcal{S}_{S_5(G)}$ de cardinal 720, or $|G| = 300$, ce n'est donc pas possible.
Si $\operatorname{Ker}\phi = G$, alors si $P \in S_5(G)$, $P$ est normal (car $\forall g \in G,\ \phi(g) = Id$) et dans ce cas $n_5 = 1$, ce qui est contradictoire.
Finalement dans ce cas on a $\{e\} \subsetneq \operatorname{Ker}\phi \subsetneq G$ et $\operatorname{Ker}\phi$ est normal non trivial et $G$ n'est pas simple.

**Solution 10.** 1) Soit $\tau$ une transposition de $\mathcal{S}_n$, $\phi(\tau)$ est d'ordre deux, c'est donc un produit de transpositions à supports distincts. Notons $T_k$ l'ensemble des permutations produit de $k$ transpositions à support disjoints ($2k \leq n$), on a $|\phi(T_k)| = |T_k|$.
Chaque $T_k$ est une classe de conjugaison de $\mathcal{S}_n$, donc $\phi(T_1)$ est un des $T_k$, car l'image d'une classe de conjugaison par $\phi$ est une classe de conjugaison. Supposons $n \neq 6$.

$$|T_1| = \binom{n}{2} = \frac{n(n-1)}{2},\ |T_k| = \frac{\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2k+2}{2}}{k!} = \frac{n(n-1)\cdots(n-2k+1)}{2^k k!}$$

la division par $k!$ vient du fait que l'ordre des transpositions n'intervient pas car elles commutent.
On a :

$$|T_k| = |T_1| \Longleftrightarrow k!\,2^{k-1} = (n-2)(n-3)\cdots(n-2k+1).$$

Pour $k=2$ on a $(n-2)(n-3)=4$ qui n'a pas de solution dans $\mathbb{N}$, pour $k\geq 3$ on obtient

$$|T_k|=|T_1|\Longleftrightarrow (n-2)\cdots(n-k+1)\binom{n-k}{k}=2^{k-1}$$

ce qui n'est possible que si $n-k+1=n-2$, sinon le terme de gauche a un facteur impair, ce qui entraine $k=3$ mais $(n-2)\binom{n-3}{3}=4\Longrightarrow n=6$ ce qui est exclu. ceci montre que $\phi(T_1)=T_1$.

2) On a $\tau_i\tau_j=(1,j,i)$, $\tau_j\tau_i=(1,i,j)$ d'où si $i\neq j$, $\phi(\tau_i)\phi[\tau_j)\neq\phi(\tau_j)\phi(\tau_i)$, ce qui entraine que $\{a_i,b_i\}\cap\{a_j,b_j\}\neq\emptyset$, car deux transpositions à supports disjoints commutent.

3) Supposons que $a_2\notin\{a_i,b_i\}, i\in[\![4,n]\!]$. En appliquant ce qui précède à $j=2$ et $j=3$ on a alors $\{a_i,b_i\}=\{b_2,b_3\}$., on en déduit que
$\phi(\tau_2\tau_3\tau_i)=(a_2,b_3)=\phi(\tau_3)$, or $\tau_2\tau_3\tau_i=(1,i,3,2)\neq\tau_3$, ce qui entraine que $\phi(\tau_i)=(a_2,b_i)$.

4) Considérons $\sigma\in\mathcal{S}_n$ définie par $\sigma(i)=b_i$ où $b_1=a_2$, les $b_i$ sont deux à deux distincts car $\phi$ est injectif.
$\phi(\tau_i)=(a_2,b_i)=\sigma\tau_i\sigma^{-1}$, $\mathcal{S}_n$ est engendré par les $\tau_i$, si $\psi\in\mathcal{S}_n$, on a
$\psi=\tau_{i_1}\cdots\tau_{i_k}$, on a $\phi(\psi)=\sigma\tau_{i_1}\cdots\tau_{i_k}\sigma^{-1}=\sigma\psi\sigma^{-1}$, $\phi$ est un automorphisme intérieur.