SECTION 1

Les groupes

Définition d'un groupe

Comme son nom l'indique, un groupe désigne un ensemble d'éléments. Mais pour que cet ensemble soit promu groupe, on doit le munir d'une **loi de composition interne** (un truc qui dit comment les éléments jouent entre eux et rien qu'entre eux). Quand on compose un élément du groupe avec un autre élément du groupe, on obtient encore un élément du groupe. C'est surtout ça un groupe !

Techniquement, un groupe $\{G : a,b,c\}$ est bien un groupe si :

- $\forall\ (a,b) \in G^2,\ a \cdot b \in G$
- la loi de composition interne est **associative** $((a \cdot b) \cdot c = a \cdot (b \cdot c))$
- G contient un **élément neutre** e (tel que : $\forall\ a \in G,\ a \cdot e = a$)
- pour chaque $a \in G$, il existe un **élément symétrique** a^{-1} (tel que $a \cdot a^{-1} = e$)

Remarque : on dira indifféremment loi de composition interne ou loi de multiplication interne.

Exemple de groupe ultra simple *:* $\mathbf{C_2}$: {1,-1} avec la multiplication ordinaire comme loi de composition interne. 1×1, 1×(-1), (-1)×(-1), font bien tous parti de C_2 puisque le résultat est toujours 1 ou -1. La permutations entre deux éléments associée à l'identité forme un groupe en tout point similaire, c'est aussi C_2. De la même façon, l'identité et l'inversion spatiale (parité), ie $\boldsymbol{x} \rightarrow \boldsymbol{-x}$, forment encore C_2. Un même groupe peut donc être décrit différemment !

Groupes et symétries sont fortement liés, ce qui explique l'importance de leur étude en physique étant donné que les symétries sont au centre de notre compréhension physique du monde.
Imaginons un système $\mathcal{S}$ laissé invariant par deux symétries différentes A et B. La loi de composition interne $A \cdot B$ correspond, dans le cas des symétries, à l'application

successive de A et de B sur $\mathcal{S}$. Et l'application successive des symétries sur le système continue nécessairement à le laisser invariant donc $A \cdot B$ est aussi une symétrie de $\mathcal{S}$. La loi de composition interne étant interprétée comme une succession d'opérations de symétrie, l'associativité en découle ; on aura forcément $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ (mais attention, l'ordre doit rester le même).
Enfin, laisser $\mathcal{S}$ tel quel constitue l'élément neutre de toutes les symétries et chaque action d'une symétrie peut être inversée.
Les **opérations de symétrie** sur un système forment donc toujours un groupe !

Un peu de vocabulaire :

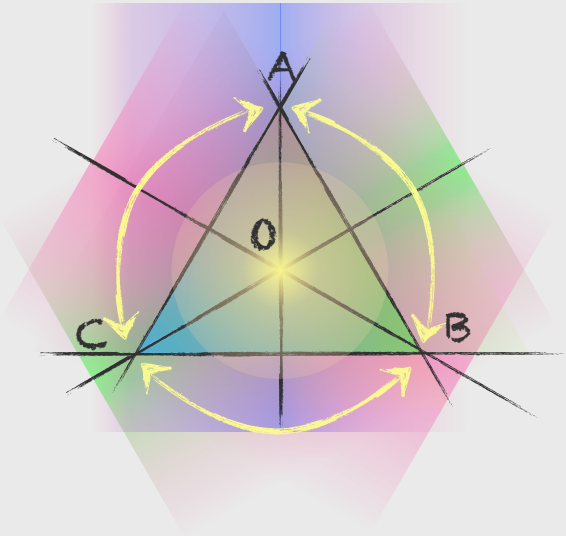
L'ordre ou le **cardinal** d'un groupe est son nombre d'éléments.

Un groupe est dit **abélien** lorsque la loi de composition est commutative :
$ab = ba$, pour tout $a, b \in G$

C_2 est à l'évidence abélien.

Exemple :

Le plus petit groupe non abélien est le groupe des symétries du triangle équilatéral appelé groupe diédral D_3.



6 transformations laissent le triangle invariant :
l'identité (e), les rotations de $2\pi/3$ et $4\pi/3$ (R_1 et R_2), et les réflexions par rapport aux hauteurs (S_A, S_B et S_C).
Elles sont toutes inversibles et la table de multiplication entre ces transformations finit de prouver qu'il s'agit bien d'un groupe.

Le caractère non abélien est évident si on compare, par exemple, R_1S_A qui amène A en C, B en B et C en A (on applique les transformations de la droite vers la gauche) et S_AR_1 qui amène A en B, B en A et C en C.

La **table de multiplication** d'un groupe permet de savoir comment chacun des éléments joue entre eux et permet donc de le décrire entièrement.

Exemple :

Pour D_3, la table de multiplication ressemble à :

·	e	R_1	R_2	S_A	S_B	S_C
e	e	R_1	R_2	S_A	S_B	S_C
R_1	R_1	R_2	e	S_B	S_C	S_A
R_2	R_2	e	R_1	S_C	S_A	S_B
S_A	S_A	S_C	S_B	e	R_2	R_1
S_B	S_B	S_A	S_C	R_1	e	R_2
S_C	S_C	S_B	S_A	R_2	R_1	e

Deux grandes dynasties de groupe se partagent le royaume :

- les groupes cycliques qui peuvent décomposer tous les groupes abéliens.
- les groupes symétriques auxquels peuvent se rapporter tout groupe d'ordre fini.

Groupes cycliques et groupes symétriques

➡ Le **groupe cyclique C_n** (dont on a déjà côtoyé un membre avec C_2) a la structure générale $\{e,a,a^2,\ldots,a^{n-1};a^n=e\}$ avec n un entier positif quelconque. On le note aussi $<a>$.

a générant tous les éléments du groupe est appelé… **générateur** du groupe.

On appelle **période** ou **ordre d'un élément** a d'un groupe le plus petit entier positif tel que $a^m = e$. Si m n'existe pas, a est dit d'ordre infini.

Le générateur a de C_n est donc, par définition, de période (ou d'ordre) n.

L'ordre d'un groupe cyclique coïncide avec l'ordre de son générateur (ce qui explique l'utilisation du termes ordre au lieu de période pour un élément).

Tous les groupes cycliques sont abéliens (car $a^i a^j = a^j a^i = a^{i+j}$)

Les racines n-ième de l'unité $\{e^{i2\pi/n}\}$ munies de la règle usuelle de multiplication sont l'exemple concret le plus direct d'un groupe cyclique.

Les lignes et colonnes de la table de multiplication de ces groupes sont en permutation circulaire (telle que l'ordre reste le même) les unes par rapport aux autres, d'où son nom.

Exemple :

Table de multiplication de C_2 :

·	e	a
e	e	a
a	a	e

Table de multiplication de C_3 :

·	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

➡ Le **groupe symétrique S_n** est formé de toutes les **permutations** possibles entre n éléments différents et est donc d'ordre $n!$.

On peut représenter de manière générale les permutations de n éléments sur deux lignes :

$$p = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ p_1 & p_2 & p_3 & \cdots & p_n \end{pmatrix}$$

Une permutation suivie d'une seconde en forme bien sûr une troisième, ce qui définit la loi de composition du groupe.

L'identité correspond à l'absence de permutation :

$$e = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

Et l'inverse de p est logiquement :

$$p^{-1} = \begin{pmatrix} p_1 & p_2 & p_3 & \cdots & p_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

Exemple :

S_3 est d'ordre 3!=6. Les 6 permutations sont :

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Le premier élément n'est autre que *e* (rien n'a bougé). Les trois éléments suivants sont obtenus en permutant deux éléments du trio et en laissant le troisième tranquille. Les deux derniers éléments sont obtenus en permutant circulairement les trois éléments.

Pour une écriture plus compacte, on décompose les permutations en 1-cycle (pas de permutations), 2-cycle (permutations 2 à 2), 3-cycle (permutations circulaires à 3 éléments), etc.

Cela donne pour les 6 permutations du groupe S_3 :
e = (1)(2)(3),
(12)(3), (1)(23), (2)(31),
(123), (321).
L'ordre d'écriture est indifférent et il est d'usage d'omettre les 1-cycle ou éléments non permutés ((12)(3)=(12)).

Lorsqu'on multiplie deux permutations, on part de la permutation la plus à droite et on regarde où arrive successivement chacun des éléments.

Exemple :

(23)·(13) = ?

- $1 \rightarrow ?$: (13) est tel que $1 \rightarrow 3$ et (23) est tel que $3 \rightarrow 2$, donc 1 est envoyé sur 2 ($1 \rightarrow 2$) par le produit des permutations.
- $2 \rightarrow ?$: (13) est tel que $2 \rightarrow 2$ et (23) est tel que $2 \rightarrow 3$, donc 2 est envoyé sur 3 ($2 \rightarrow 3$).
- $3 \rightarrow ?$: (13) est tel que $3 \rightarrow 1$ et (23) est tel que $1 \rightarrow 1$, donc 3 est envoyé sur 1 ($3 \rightarrow 1$).

On obtient bien la permutation cyclique (123) dans laquelle $1 \rightarrow 2 \rightarrow 3 \rightarrow 1$. Donc (23)·(13) = (123)

Autre exemple : (321)·(12) = (1)(23)(2) = (23)

Sous-groupes, morphismes, classes et groupes quotients

Un sous-ensemble de G qui forme un groupe avec la même loi de multiplication est un **sous-groupe** de G.

Tout élément a différent de e d'un groupe G d'ordre fini forme un sous-groupe cyclique de G.

Preuve :

$a \cdot a = a^2$ est dans G par propriété des groupes et vaut soit e soit un élément différent de a (car seul $a \cdot e$ donne a). De même, si $a^2 \neq e$, alors $a^2 \cdot a = a^3$ vaut soit e, soit un élément différent à la fois de a et a^2 puisqu'ils sont tous deux différents de e. En continuant ainsi, on obtient un ensemble $\{a, a^2, a^3, a^4, a^5, \ldots\}$ s'arrêtant pour a^p valant e (et cela arrive nécessairement puisque le groupe G est fini). On obtient alors un groupe cyclique d'ordre p.

Un **homomorphisme** entre un groupe G et un groupe G' est une application envoyant les éléments de G vers G' tout en préservant la loi de composition :
si $g_i \in G \mapsto g_i' \in G'$ et $g_1 g_2 = g_3$, alors $g_1' g_2' = g_3'$

Quand l'application est bijective, un élément pour un élément, on parle d'**isomorphisme** (on le note symboliquement $G \simeq G'$)

Si on appelle f l'homomorphisme $G \xrightarrow{f} G'$, on a alors :

- $f(g_1)f(g_2) = f(g_3) = f(g_1 g_2)$ par définition
- $f(g)f(e) = f(g) \Rightarrow f(e) = e'$.
  L'élément neutre de G est envoyé sur l'élément neutre de G'.
- $f(g^{-1}) = f^{-1}(g)$ puisque $f(g^{-1})f(g) = f(e) = e'$.

Cela montre que :

l'**image** de l'**homomorphisme** f de G à G' définit comme $\mathrm{Im}(f) \equiv f(G) \equiv \{f(g); g \in G\}$ est un **sous-groupe** de G'.

Preuve :

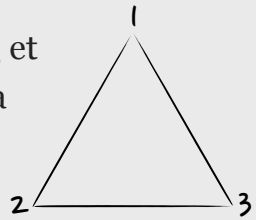
En effet,

- $e' \in \mathrm{Im}(f)$,
- $f(g_1)f(g_2) = f(g_1 g_2) \in \mathrm{Im}(f)$ pour tout $g_1, g_2 \in G$
- $f^{-1}(g) = f(g^{-1}) \in \mathrm{Im}(f)$ pour tout élément de G.

Construisons la table de multiplication du groupe S_3 :

·	e	(12)	(23)	(31)	(123)	(321)
e	e	(12)	(23)	(31)	(123)	(321)
(12)	(12)	e	(123)	(321)	(23)	(31)
(23)	(23)	(321)	e	(123)	(31)	(12)
(31)	(31)	(123)	(321)	e	(12)	(23)
(123)	(123)	(31)	(12)	(23)	(321)	e
(321)	(321)	(23)	(31)	(12)	e	(123)

On remarque qu'en identifiant les deux permutations circulaires aux rotations de D_3 et les 2-cycle aux réflexions, on a exactement la même table de multiplication. Cela montre que S_3 et D_3 sont isomorphes ($S_3 \simeq D_3$).



L'exemple précédent est généralisable :

le **théorème de Cayley** stipule en effet que tout groupe G d'ordre n est isomorphe à un sous groupe de S_n.

Preuve :

Les éléments de G sont étiquetés $\{g_i\ ; i = 1,\cdots,n\}$.
Pour un élément a dans G, ag_i est un élément de G déterminé par la règle de composition interne. On peut très bien appelé a_i l'indice entier qui désigne cet élément : $g_{a_i} \equiv ag_i$, ce qui détermine une séquence de nombres entiers $(a_1, \cdots, a_n)$.
Comme $ag_i = ag_k$ seulement pour $i = k$ (suffit de multiplier par a^{-1} pour s'en assurer), tous les entiers $\{a_1, \cdots, a_n\}$ sont différents. Ils forment donc une permutation de $(1,2,\cdots,n)$.

Plus simplement, on peut voir l'action de a sur l'ensemble des $g \in G$ comme une translation (à gauche) des éléments du groupe (ga serait la translation à droite, différente par défaut).

On peut par conséquent envoyer G sur S_n :

$$a \in G \longrightarrow p_a = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \in S_n$$

Si $ab=c$ dans G, on a :

$$p_a p_b = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & \cdots & n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$$
$$= \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_{b_1} & a_{b_2} & \cdots & a_{b_n} \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & \cdots & n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_{b_1} & a_{b_2} & \cdots & a_{b_n} \end{pmatrix}$$

Or $g_{a_{b_i}} = ag_{b_i} = a(bg_i) = (ab)g_i = cg_i = g_{c_i}$
Donc

$$p_a p_b = p_c = \begin{pmatrix} 1 & 2 & \cdots & n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix} \in S_n$$

On a donc montré que l'application $a \in G \longrightarrow p_a \in S_n$ préserve la loi de composition interne, ie c'est un homomorphisme.
Et comme on a commencé par dire que l'application envoyait un antécédent sur une image unique, il s'agit d'un isomorphisme.
L'ensemble des p_a (pour tous les a de G) forme donc un sous-groupe de S_n isomorphe à G.

Deux éléments a et b de G sont dit **conjugués** s'il existe un troisième élément p de G tel que $b=pap^{-1}$. On écrit $b \sim a$ car il s'agit d'une **relation d'équivalence**.

Une relation d'équivalence se doit d'être symétrique ($a \sim b \Rightarrow b \sim a$), réflexive ($a \sim a$) et transitive (si on a $a \sim b$ et $b \sim c$ alors $a \sim c$), ce qu'on vérifie bien avec la relation de conjugaison.

Des éléments conjugués les uns par rapport aux autres forment une **classe de conjugaison**.

L'identité (élément neutre) forme une classe à elle seule.

Et dans le groupe symétrique, les cycle d'une même longueur appartienne à une même classe.

Preuve :

soit p un cycle de longueur donnée et q une permutation quelconque du même groupe de symétrie alors :

$$\begin{aligned} qpq^{-1} &= (q_i \leftarrow i)(p_i \leftarrow i)(i \leftarrow q_i) \\ &= (q_i \leftarrow i)(p_i \leftarrow q_i) \\ &= (q_{p_i} \leftarrow p_i)(p_i \leftarrow q_i) \\ &= (q_{p_i} \leftarrow q_i) \\ &= q[p] \end{aligned}$$

On n'a fait qu'étiqueter différemment la permutation p :

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ p_1 & p_2 & p_3 & \cdots & p_n \end{pmatrix} \text{ devient } \begin{pmatrix} q_1 & q_2 & q_3 & \cdots & q_n \\ p_{q_1} & p_{q_2} & p_{q_3} & \cdots & p_{q_n} \end{pmatrix}$$

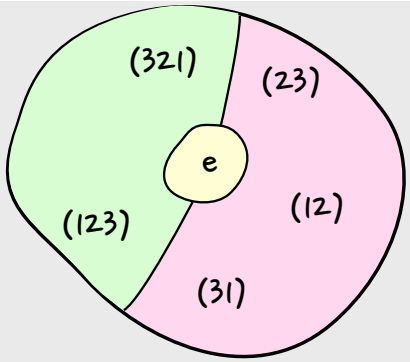
L'ordre change mais pas ce que devient chacune des valeurs. La structure des cycles est donc nécessairement la même.

Exemple :

S_3 est donc constitué de 3 classes :

- e
- {(12),(23),(13)}
- {(123),(321)}

Comme l'isomorphisme entre D_3 et S_3 l'impose, ces classes trouves bien leurs correspondances dans D_3 puisqu'on peut vérifier que l'identité, les deux rotations et les trois réflexions forment là encore trois classes de conjugaison.



Chaque élément d'un groupe appartient à une et une seule classe puisque l'action de conjugaison consiste en une translation à gauche et une translation à droite (composer tous les éléments du groupe par un même élément revient à les décaler (ou permuter) tous de la même façon) et donc associe un élément conjugué différent à chaque élément différent du groupe (c'est une bijection).
Et d'autre part, deux classes différentes sont disjointes par transitivité (si elle ne sont pas disjointes, elles coïncident).
Par conséquent, l'union de toutes les classes d'un groupe reforme le groupe, ou dit autrement, **les classes forment une partition du groupe**.

Un **sous-groupe** H de G est dit **invariant**, ou **normal**, ou distingué, s'il est identique à ses sous-groupes conjugués ($H = g^{-1}Hg$ pour $g \in G$).

Remarque :

un sous-groupe invariant est nécessairement une union de classes conjuguées dont l'identité (un groupe doit la contenir).

Exemple :

Le sous-groupe $\{e, (123), (321)\}$ de S_3 forme un sous-groupe invariant puisqu'il contient l'identité et la classe entière des 3-cycles. Tout élément conjugué de cet ensemble appartient à une de ces deux classes et se trouve donc dans l'ensemble de départ.

Les classes de conjugaison ne sont pas les seules à savoir découper un groupe. Leurs concurrentes : les **classes latérales** dites à gauche ou à droite issues d'un sous-groupe donné.
Cette partition diffère de la précédente sur deux points : elle n'est pas nécessairement unique et les classes latérales entrant dans la partition comportent chacune le même nombre d'éléments.

Soit $H=\{h_1,h_2,...\}$ un sous-groupe de G et p un élément de G (qui n'est pas dans H). Alors l'ensemble $pH=\{ph_1,ph_2,...\}$ est appelé **classe à gauche** de G suivant H.
De même, Hp est une **classe à droite** suivant H.

Remarques :

- si p est dans H, on récupère H ($pH=H=Hp$) par définition d'un sous-groupe.
- une classe à gauche (ou à droite), comme une classe tout court, n'est généralement pas un groupe (on doit contenir l'identité pour en être un !).

Deux classes à gauche (ou à droite) d'un même sous-groupe soit coïncident complètement, soit n'ont aucun élément en commun.

Preuve :

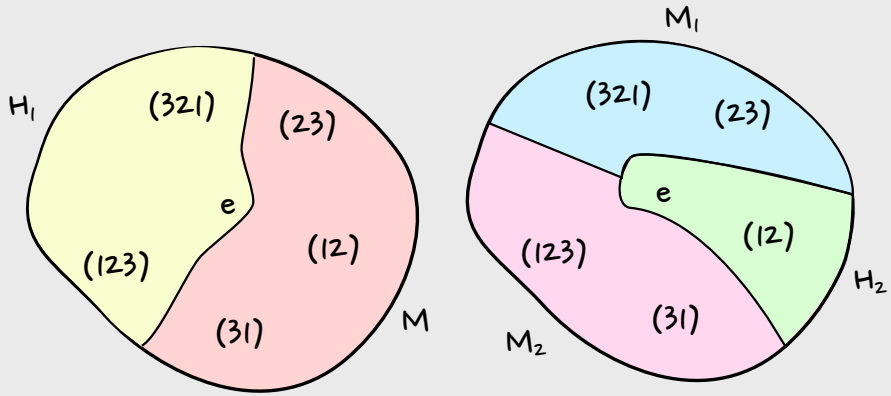
Soient pH et qH deux classes à gauche et supposons qu'on ait, pour un certain h_i, et un certain h_j pris dans H, $ph_i=qh_j$, donc pH et qH ont au moins un élément en commun.
Comme $q^{-1}p=h_jh_i^{-1}$, $q^{-1}p$ est un élément de H. Par conséquent, $q^{-1}pH=H$ (puisque H est un sous-groupe donc un groupe).
Conclusion : $pH=qH$.
Pour ne pas être dans ce cas, il faut aucun h_i et h_j tels que $ph_i=qh_j$, autrement dit, pH et qH doivent être disjoints.

Et chaque classe à gauche (ou à droite) suivant un sous-groupe H a nécessairement autant d'éléments que H.

On en déduit que pour un sous-groupe H d'ordre n_H, l'ensemble des classes à gauche (ou à droite) forme une partition des éléments de H en ensembles disjoints de n_H éléments chacun.

Exemple :

Le sous-groupe $\{H_1 : e, (123), (321)\}$ de S_3 possède une classe à gauche $\{M : (12), (23), (31)\}$ obtenue en multipliant à gauche les éléments de H_1 par (12), ou par (23), ou encore par (31).



Le sous-groupe $\{H_2 : e, (12)\}$ de S_3 possède, lui, deux classes à gauche :

- $\{M_1 : (23), (321)\}$ obtenue en multipliant à gauche les éléments de H_2 soit par (23), soit par (321),
- $\{M_2 : (31), (123)\}$ obtenue en multipliant à gauche les éléments de H_2 soit par (31), soit par (123).

Le **théorème de Lagrange** en découle : l'ordre d'un groupe fini doit être un multiple entier de l'ordre de n'importe lequel de ses sous-groupes.
Cela entraîne que tout groupe d'ordre premier est cyclique et donc abélien.
Plutôt joli, non ?

Preuve :

Soit a un élément de G différent de e. Alors a forme un sous-groupe cyclique de G d'ordre au moins 2. Or cet ordre doit diviser l'ordre G. Seul solution, il vaut l'ordre G, ce qui implique que G est cyclique et par conséquent abélien.

Les classes à gauche ou à droite issues d'un sous-groupe invariant sont particulièrement simples et utiles. Déjà, classes à gauche et classes à droite coïncident ($pHp^{-1}=H$ implique $pH=Hp$). De plus, la partition obtenue est unique et une «factorisation» de G basée sur cette partition devient naturelle.

L'ensemble des classes issues d'un sous-groupe invariant H d'un groupe G a la propriété de former lui-même un groupe, appelé **groupe quotient** G/H, d'ordre n_G/n_H.

Preuve :

- La loi de composition interne entre deux classes latérales pH et qH est définie comme l'ensemble des produits $ph_iqh_j=(pq)h_k$ avec $h_k=(q^{-1}h_iq)h_j$ appartenant bien à H (puisque H est un sous-groupe invariant).
  Plus simplement : $pHqH=pqH$.
- $H=eH$ joue le rôle de l'élément neutre.
- $p^{-1}H$ est l'inverse de pH.
- $pH\cdot(qH\cdot rH)=(pH\cdot qH)\cdot rH=(pqr)H$

Exemple 1 :

Considérons $\mathbb{Z}/2\mathbb{Z}$ où $\mathbb{Z}$ est l'ensemble des entiers relatifs munis de l'addition comme loi de composition interne. $2\mathbb{Z}$ est donc l'ensemble des entiers relatifs pairs. Et par conséquent, $\mathbb{Z}/2\mathbb{Z}$ est formé de deux sous-groupes distincts : les entiers pairs et les entiers impairs. Le groupe quotient $\mathbb{Z}/2\mathbb{Z}$ est donc isomorphe au groupe cyclique à deux éléments C_2. Il correspond aussi à l'ensemble {0,1} muni de l'addition modulo 2.
On peut généraliser en disant que $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au groupe cyclique C_n et correspond aussi à l'ensemble des restes dans la division euclidienne de k par n, soit l'ensemble {0,1,...,n} muni de l'addition modulo n.

L'exemple précédent permet de mieux comprendre pourquoi G/H se lit G **modulo** H.

Exemple 2 :

Dans le cas de S_3, H={e,(123),(321)} est un sous-groupe invariant.
G/H contient deux éléments : H et M={(12),(23),(31)}.
H est l'ensemble des permutations paires à 3 éléments (l'identité correspond à aucune permutation et les 3 cycles à des permutations doubles). On appelle aussi H A_3, groupe alterné d'ordre 3. M est l'ensemble des permutations impaires.
On voit facilement que la composition de deux permutations impaires ou paires donne une permutation paire alors qu'une composition mixte donne une permutation impaire :
$HM=MH=M$, $HH=H$ et $MM=H$.
On en déduit que G/H est isomorphe à C_2 (H est envoyé sur l'identité et M correspond à l'autre élément)

Le morphisme $f : G \to G/H, g \mapsto gH$ est appelé **morphisme canonique** ou projection canonique.

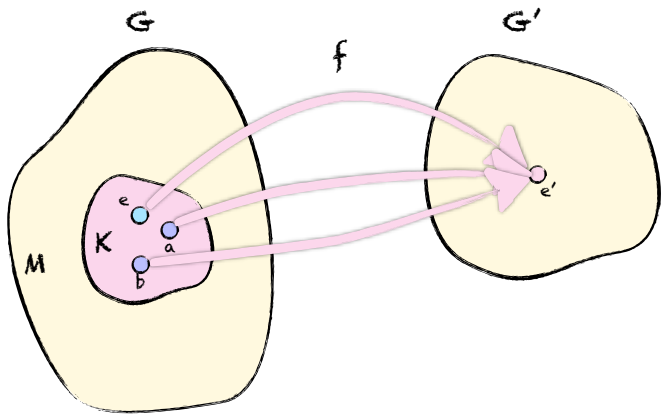
Le deuxième exemple illustre un théorème qui va se révéler bien utile mais définissons d'abord le noyau d'un homomorphisme :

Soit f un homomorphisme de G à G'. On appelle **noyau** K de cet **homomorphisme** l'ensemble des éléments de G qui sont envoyé sur l'élément neutre de G' ($K=\{g \in G\,;\, g \overset{f}{\longmapsto} e' \in G'\}$).

Théorème d'isomorphisme (premier) :

Soit f un homomorphisme de G à G' de noyau K.

- K forme alors un sous-groupe invariant de G.
- Le groupe quotient G/K est isomorphe à G'.
  Autrement dit, on rend f injectif en quotientant G par son noyau.
  Cela se note symboliquement :
  $G/K \simeq G'$ ou encore $G/\mathrm{Ker}(f) \simeq f(G)$ où $\mathrm{Ker}(f)$ désigne le noyau de f et $f(G)$ est l'image de f.

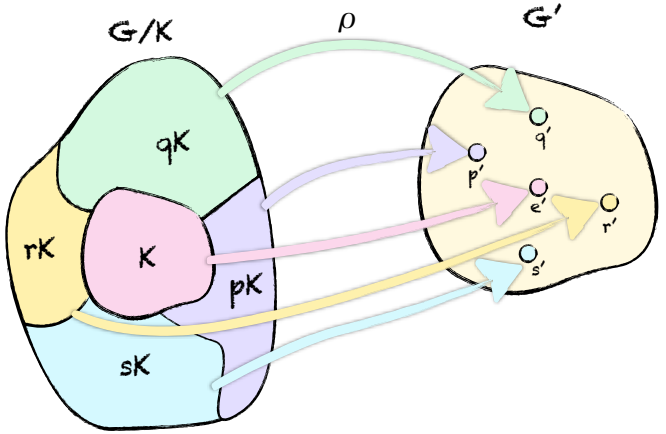


Preuve :

- Montrons que K est un sous-groupe :
  pour a et b dans K, $a \cdot b \longrightarrow e' \cdot e' = e'$, donc $a{\cdot}b$ est aussi dans K. La préservation de la loi de composition par l'homomorphisme assure que pour $g \xrightarrow{f} g'$, on a aussi $e \xrightarrow{f} e'$ et $g^{-1} \xrightarrow{f} g'^{-1}$. D'où $e \in K$, et si $a \in K$, alors a^{-1} est aussi dans K (car $a^{-1} \xrightarrow{f} e'^{-1} = e'$).

- Montrons que K est indépendant :
  prenons a dans K et g dans G. $gag^{-1} \xrightarrow{f} g'e'g'^{-1} = e'$. Donc $gag^{-1} \in K$ pour tout $g \in G$.

- Montrons que G/K est isomorphe à G' :
  les éléments du groupe quotient G/K sont les classes latérales pK. Considérons l'application envoyant les classes latérales vers l'image de f
  $pK \xrightarrow{\rho} f(p) = p' \in G'$.
  - ρ est bien définie : si $pK{=}qK$ pour un p et un q dans K, alors $q^{-1}p$ est aussi dans K et donc
    $$\begin{aligned} f(q^{-1}p) &= 1 \\ &= f(q^{-1})f(p) \quad \text{comme } f \text{ est un homomorphisme} \\ &= f^{-1}(q)f(p) \end{aligned}$$
    Et finalement, $f(q){=}f(p)$.
  - ρ est bien un homomorphisme :
    $$\begin{aligned} \rho(pK \cdot qK) &= \rho(pqK) \\ &= f(pq) \\ &= f(p)f(q) \\ &= \rho(pK)\rho(qK) \end{aligned}$$
  - Si $\rho(pK) = \rho(qK)$ alors $\rho(q^{-1}pK) = \rho(q^{-1}K \cdot pK)$ (à nouveau, le groupe quotient est un groupe), et par action de groupe de l'homomorphisme,
    $\rho(q^{-1}K \cdot pK) = \rho(q^{-1}K)\rho(pK) = \rho^{-1}(qK)\rho(pK) = e'$, ce qui implique $q^{-1}pK = K$ ou $qK = pK$.
    L'application est bien bijective.



Le dessin ci-dessus illustre le cas d'un groupe G contenant 15 éléments avec un noyau K en contenant 3. G/K et G' sont alors tous deux d'ordre 5.

Exemple :

on a vu dans un exemple précédent que l'homomorphisme de S_3 sur C_2 devient un isomorphisme si on quotiente S_3 par le sous groupe invariant $H{=}\{e,(123),(321)\}$: $S_3/H \simeq C_2$. Or H n'étant autre que le noyau K de l'homomorphisme comme le prévoit le théorème d'isomorphisme.

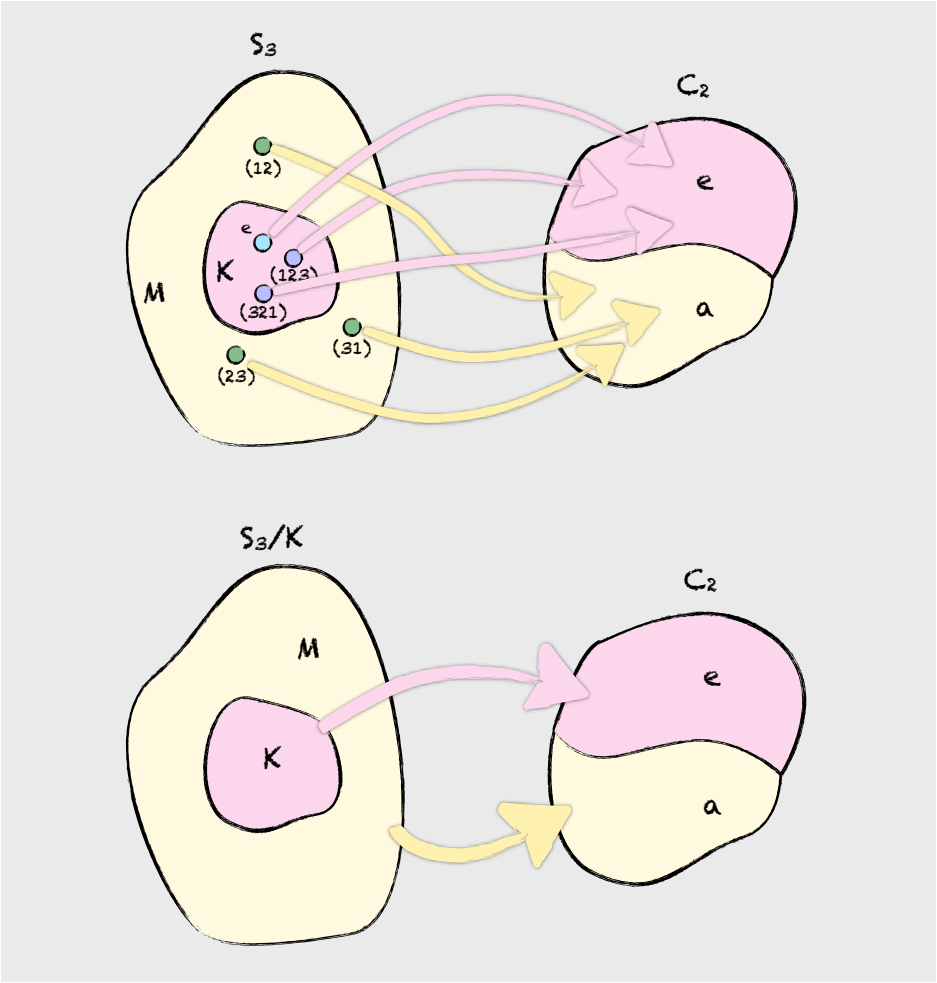


Image et noyau nous disent beaucoup sur les homomorphismes, en effet :

Pour un homomorphisme f tel que $G \xrightarrow{f} G'$
- f est **injectif** si et seulement si $\mathrm{Ker}(f) = e$
- f est **surjectif** si et seulement si $\mathrm{Im}(f) = G'$

Produit direct de deux groupes

Soit H_1 et H_2 deux sous-groupes du groupe G avec les deux propriétés suivantes :
- les éléments de H_1 commutent avec les éléments de H_2.
- chaque élément de $g \in G$ peut s'écrire $g = h_1 h_2$ avec $h_1 \in H_1$ et $h_2 \in H_2$.

G est alors le **produit direct** de H_1 et H_2 : $G = H_1 \otimes H_2$.

Exemple :

Décomposons $C_6 = \{e = a^6, a, a^2, a^3, a^4, a^5\}$ en $H_1 = \{e, a^3\}$ et $H_2 = \{e, a^2, a^4\}$.
Comme C_6 est abélien, le premier critère est respecté.
Et $e = ee$, $a = a^3a^4$, $a^2 = ea^2$, $a^3 = a^3e$, $a^4 = ea^4$, $a^5 = a^3a^2$.
$H_1 \simeq C_2$ et $H_2 \simeq C_3$ donc $C_6 \simeq C_2 \otimes C_3$.

Si $G = H_1 \otimes H_2$, alors H_1 et H_2 doivent être invariants.

Preuve :

pour $a_1 \in H_1$,
$ga_1g^{-1} = h_1h_2a_1(h_1h_2)^{-1} = h_1h_2a_1h_2^{-1}h_1^{-1} = h_1a_1h_1^{-1} \in H_1$ (on peut bien sûr faire pareil avec a_2 dans H_2).

On peut donc construire les groupes quotient G/H_1 et G/H_2. On montre alors que $G/H_1 \simeq H_2$ et $G/H_2 \simeq H_1$, ce qui éclaire un peu plus le terme de groupe quotient.