Chapitre 1

Éléments de la théorie des groupes

1.1 Introduction/Notions de base

Notions fondamentales:

- Groupes
- Morphismes
- Réalisations et Représentations
- Symétries

1.1.1 Groupes

Des groupes, des corps, des espaces vectoriels, des algèbres, etc. sont des **structures algébriques**, c.à.d. des n-uplets formés par:

- un ou plusieurs ensembles (non-vides)
- une ou plusieures lois de composition internes et/ou externes
- des règles pour les lois de composition

Définition 1.1 (Groupe)**.** Soit $G \neq \emptyset$ un ensemble muni d'une loi de composition interne, c'est-à-dire une application $\star : G \times G \to G$. Le couple $(G, \star)$ est appelé **groupe** lorsque les règles suivantes sont satisfaites:

(G1) $\forall a, b, c \in G : a \star (b \star c) = (a \star b) \star c$ (associativité)

(G2) $\exists e \in G : \forall a \in G : e \star a = a \star e$ (élément neutre)

(G3) $\forall a \in G : \exists a^{-1} \in G : a \star a^{-1} = a^{-1} \star a = e$ (inverse)

Le groupe est dit **commutatif** ou **abélien** si la loi de composition est commutative:

(G4) $\forall a, b \in G : a \star b = b \star a$ (commutativité)

Remarques 1.1. Déf. groupe:

1. La définition inclut le fait que le produit $a \star b$ est aussi un membre de G. C'est parfois formulé comme axiom separé G0 (fermeture).

2. Notation: $\star(a, b) = a \star b = ab$.

3. Autres symboles utilisés pour la loi de composition: $\circ, *, \cdot, \perp, f_1, f_2, f_3, \ldots$.

4. Dans le cas abélien la composition est souvent notée "+", l'élément neutre est noté "0" et l'élément inverse de a est noté "$-a$".

5. Souvent l'ensemble G est identifié avec le groupe $(G, \star)$ (avec la loi de composition sous-entendu).

6. L'ensemble G peut être **fini**, **infini dénombrable** ou **non-dénombrable**; le nombre d'éléments, $|G|$, est appelé **l'ordre** du groupe. On parle aussi d'un **groupe discret** (G dénombrable) et d'un **groupe continu** (G non-dénombrable).

7. L'élément neutre e d'un groupe est unique. Le symétrique y de tout élément x est également unique. Voir l'exercice 1.1.

8. Pour des raffinements minimalistes dans la définition 1.1 voir l'exercice 1.2.

Exemple 1.1. Exemples de groupes discrets

1. $C_2 = \{e, a\}$ avec $a^2 = e$: $|C_2| = 2$, abélien.
2. $C_3 = \{e, c, c^2\}$ avec $c^3 = e$: $|C_3| = 3$, abélien.
3. $(\{1, i, -1, -i\}, \cdot)$: $|G| = 4$, abélien
4. S_n, les permutations de n objets: $|S_n| = n!$, non-abélien pour $n \geq 3$.
5. $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$: $|G| = \infty$, dénombrable, abélien.
6. $(\mathbf{Q} - \{0\}, \cdot)$: $|G| = \infty$, dénombrable, abélien.

Exemple 1.2. Exemples de groupes continus

1. $(\mathbf{R}, +)$, $(\mathbf{C}, +)$: $|G| = \infty$, non-dénombrable, abélien.
2. $(\mathbf{R} - \{0\}, \cdot)$, $(\mathbf{C} - \{0\}, \cdot)$: $|G| = \infty$, non-dénombrable, abélien.
3. Translations: abélien
4. Rotations du plan SO(2): abélien, compact
5. Rotations de E_3, SO(3): non-abélien, compact
6. Groupe de Galilée G(3)
7. Groupe de Lorentz O(1, 3): non-abélien, non-compact
8. Groupe de Poincaré P(4): non-abélien, non-compact

Exemple 1.3. Contrexemples

1. $(\mathbf{Z}, \cdot)$ n'est pas un groupe: $1/n \notin \mathbf{Z}$.
2. $(\mathbf{Q}, \cdot)$, $(\mathbf{R}, \cdot)$, $(\mathbf{C}, \cdot)$ ne sont pas des groupes: 0 n'a pas d'inverse.

Discussion 1.1. Structure:

1. La définition 1.1 est abstraite dans le sens que *ce n'est pas nécessaire* (mais possible) de spécifier les éléments du groupe G. Par exemple, pour le groupe C_2 (voir exemple 1.1) les éléments e et a ne sont pas décrits. L'information essentielle (concernant la structure) est contenue dans la loi de composition: $a^2 = e$.

2. La **structure** d'un groupe est donc la déscription de tous les résultats de toutes les combinaisons possibles de paires d'éléments de groupe.

3. Pour un groupe fini $G = \{g_1, \cdots, g_n\}$ on peut décrire la loi de composition (c.à.d. la structure) par une **table de groupe** $T = (t_{ij})$, où $t_{ij} = g_i g_j \in G$. T est une matrice $n \times n$ sur G.

4. Pour les groupes infinis il faut donner une règle/prescription pour la loi de composition.

Exemple 1.4. Table de groupe pour C_2
Il y a exactement un groupe abstrait de l'ordre 2: $C_2 = \{e, a\}$ avec $a^2 = e$. C'est le plus simple groupe non trivial. Il est abélien.
La table de groupe:

C_2	e	a
e	$e^2 = e$	$ea = a$
a	$ae = a$	$a^2 = e$

$=$

C_2	e	a
e	e	a
a	a	e

ou $\begin{pmatrix} \mathrm{e} & \mathrm{a} \\ \mathrm{a} & \mathrm{e} \end{pmatrix}$

Exemple 1.5. Table de groupe pour C_3
$C_3 = \{e, a, a^2\}$ avec $a^3 = e$.
La table de groupe:

C_3	e	a	$b(= a^2)$
e	e	a	b
a	a	b	e
b	b	e	a

Remarques 1.2. Table de groupe

1. La table de groupe est symétrique par rapport à l'axe principal $\Leftrightarrow$ Le groupe est abélien: $t_{ij} = g_i g_j = t_{ji} = g_j g_i$.
   (Voir exemples 1.4 et 1.5.)

2. **Carré latin**: Chaque élément apparaît exactement une fois dans chaque ligne et chaque colonne. Par conséquent, les lignes (colonnes) sont des permutations de la première ligne (colonne).
   "Preuve": Soit $G = \{g_1, \ldots, g_n\}$. Supposons l'élément g apparaît deux fois dans la même ligne i, disons dans les colonnes j et k, c.à.d.:

   $$t_{ij} = g_i g_j = t_{ik} = g_i g_k = g \quad \text{avec} \quad g_j \neq g_k \,.$$

   Multiplication à gauche avec g_i^{-1} donne $g_i^{-1} g = g_j = g_k$ en contradiction avec la supposition. Similaire pour les colonnes.

3. La propriété du carré latin est nécessaire mais non pas suffisante pour être une table de groupe valable. Il faut de plus vérifier l'associativité.

Définition 1.2 (Sous-Groupe)**.** Soit $H \subseteq G$. Le couple $(H, \star)$ est un **sous-groupe** de $(G, \star)$ si $(H, \star)$ est un groupe.

- Les **sous-groupes triviaux** sont $\{e\}$ et G
- Les **sous-groupes propres** ne sont ni $\{e\}$ ni G
- Si $H \subseteq (H \subset G)$ est un sous-groupe de G, on écrit: $H \leq G$ $(H < G)$.

Remarques 1.3. Déf. sous-groupe:
Comme l'associativité est heritée, il faut surtout vérifier la fermeture quand on multiplie, et que les inverses et l'élément neutre restent dans H.

Exemple 1.6. Sous-groupes

1. Nous allons voir que chaque groupe fini de l'ordre n est un sous-groupe de S_n.
2. $(Z_2, \cdot) = (\{1, -1\}, \cdot) < (\{1, i, -1, -i\}, \cdot)$.
3. $(\mathbf{Z}, +) < (\mathbf{Q}, +) < (\mathbf{R}, +) < (\mathbf{C}, +)$.
4. $\mathrm{SO}(2) < \mathrm{SO}(3)$.

5. $C_3 < \mathrm{SO}(2)$. Les rotations avec angle $\theta = 0°, 120°, 240°$.
   C'est un exemple pour un sous-groupe fini d'un groupe continu.

6. Pour la classification des sous-groupes finis de $SO(3)$, voir par exemple, [1, 2].

Théorème 1.1. *Soit G un groupe. $H \subset G$ est un sous-groupe $\Leftrightarrow \forall x, y \in H : xy^{-1} \in H$.*

Proof. (Théorème 1.1)
"⇒": Trivial. $(x, y \in H \Rightarrow y^{-1} \in H \Rightarrow xy^{-1} \in H)$
"⇐": $y \in H \Rightarrow yy^{-1} = e \in H$ (Identité), $e, y \in H \Rightarrow ey^{-1} = y^{-1} \in H$ (Inverse), $x, y^{-1} \in H \Rightarrow xy \in H$ (Fermeture). □

1.1.2 Morphismes

Un homomorphisme est une application f d'un ensemble A dans un ensemble B ($f : A \to B$) en *preservant une structure* donnée. C'est une notion cléf dans létude des structures algébriques.

Définition 1.3 (Homomorphisme de groupes)**.** Soient $(G, \circ)$ et $(G', \circ')$ des groupes. Une application $\phi : G \to G'$ avec $g \mapsto \phi(g)$ est un **homomorphisme de groupes** de G dans G' si $\phi(g_1 \circ g_2) = \phi(g_1) \circ' \phi(g_2)$.

Soient $X \subseteq G$ et $Y \subseteq G'$. On appele:

- **Image de X**: $\phi(X) := \{\phi(g) | g \in X\} \subseteq G'$.
- **Antécédent de Y**: $\phi^{-1}(Y) := \{g \in G | \phi(g) \in Y\} \subseteq G$.
- **Image de ϕ**: $\mathrm{Im}(\phi) := \phi(G) = \{\phi(x) | x \in G\} \subseteq G'$.
- **Noyau de ϕ**: $\mathrm{Ker}(\phi) := \phi^{-1}(\{e'\}) = \{x \in G | \phi(x) = e'\} \subseteq G$
  où e' est l'élément neutre de G'.

Un homomorphisme est appelé

- **Epimorphisme** $:\Leftrightarrow \phi$ surjectif: $\phi(G) = G'$
- **Monomorphisme** $:\Leftrightarrow \phi$ injectif: $g_1 \neq g_2 \Rightarrow \phi(g_1) \neq \phi(g_2)$
- **Isomorphisme** $:\Leftrightarrow \phi$ bijectif: à la fois surjectif et injectif
  Les deux groupes sont dits **isomorphes**, et l'on écrit: $G \cong G'$.
- **Endomorphisme** $:\Leftrightarrow G' = G$
- **Automorphisme** $:\Leftrightarrow G' = G$ et ϕ bijectif

Quelques conséquences des axiomes de groupe:

Proposition 1.2. *Soient G, G' des groupes, $\phi : G \to G'$ un homomorphisme et $e \in G$ l'élément neutre de G. C'est vrai que*

a) $\phi(e)$ *est l'élément neutre de* G'.

b) $\forall a \in G : \phi(a^{-1}) = [\phi(a)]^{-1}$.

c) $\forall a \in G, n \in \mathbf{Z} : \phi(a^n) = [\phi(a)]^n$.

d) $H \leq G \Rightarrow \phi(H) \leq G'$.

e) $H' \leq G' \Rightarrow \phi^{-1}(H') \leq G$.

Proof. (Esquisse)
a) $\phi(e) = \phi(ee) = \phi(e)\phi(e)$. Mais $a^2 = a \Rightarrow a = e$.
b) $\phi(e) = \phi(a^{-1}a) = \phi(a^{-1})\phi(a)$. Le symétrique de $\phi(a)$ est unique et $[\phi(a)]^{-1} = \phi(a^{-1})$.
c) Pour $n = 0$ c'est l'assertion a). Pour $n > 0$: par induction. Pour $n < 0$: $\phi(a^n) = \phi((a^{-1})^{-n}) = [\phi(a^{-1})]^{-n} = ([\phi(a)]^{-1})^{-n} = [\phi(a)]^n$.
d) Exercice.
e) Exercice. □

Remarques 1.4. Quelques remarques

1. Notez que "a)" et "b)" sont des cas particuliers de "c)" qui sont souvent utilisés.
2. Cas particulier de "d)": $\phi(G)$ est un sous-groupe de G'.
3. Cas particulier de "e)": $\phi^{-1}(G')$ et $\mathrm{Ker}(\phi)$ sont des sous-groupes de G.

Exemple 1.7. Homomorphismes

1. $f : G \to G'$, $\forall g \in G : f(g) = e'$: trivial, non-fidèle.
2. $f : G \to G$, $\forall g \in G : f(g) = g$: trivial, isomorphisme.
3. $\mathrm{Aut}(G) \equiv \mathrm{I}(G) := \{\rho_g | g \in G\}$ avec $\rho_g : G \to G$, $\rho_g(h) = ghg^{-1}$ est appelé automorphisme intérieur effectuant la conjugaison par l'élément fixe $g \in G$.

   $f : G \to \mathrm{Aut}(G)$, $g \mapsto \rho_g$ est un homomorphisme.
   $\rho_{g_1 g_2}(h) = g_1 g_2 h g_2^{-1} g_1^{-1} = g_1(g_2 h g_2^{-1})g_1^{-1} = \rho_{g_1}(g_2 h g_2^{-1}) = \rho_{g_1}(\rho_{g_2}(h)) = (\rho_{g_1} \circ \rho_{g_2})(h)$
   $\Rightarrow f(g_1 g_2) = \rho_{g_1 g_2} = \rho_{g_1} \circ \rho_{g_2} = f(g_1) f(g_2)$

   Exerice: Vérifier que a) ρ_g est un automorphisme et b) $\mathrm{Aut}(G)$ est un groupe ($\to$ TD2).
4. ...

Discussion. Noyau et image:
L'image peut être considerée comme mesure de la surjectivité, le noyau comme mesure de l'injectivité d'un homomorphisme.

Proposition 1.3. *Un homomorphisme de groupe $\phi : G \to H$ est injectif $\Leftrightarrow$ $Ker(\phi) = \{e\}$ (avec e l'élément neutre de G).*

Proof. "$\Rightarrow$": Soit $x \in \mathrm{Ker}(\phi)$, c.à.d. $\phi(x) = e' = \phi(e)$. ϕ injectif $\Rightarrow x = e \Rightarrow \mathrm{Ker}(\phi) = \{e\}$.
"$\Leftarrow$": Soit $\mathrm{Ker}(\phi) = \{e\}$ et supposons il y a $x, y \in G$, $x \neq y$: $\phi(x) = \phi(y)$. On a $e' = \phi(y)\phi(x)^{-1} = \phi(y)\phi(x^{-1}) = \phi(yx^{-1})$. Alors, $yx^{-1} \in \mathrm{Ker}(\phi) = \{e\}$, c.à.d. $yx^{-1} = e$ ou $y = x$ en contradiction avec la supposition. □

Presque trivial mais important:

Proposition 1.4. *Soient $\phi : G \to H$ et $\psi : H \to K$ des homomorphismes de groupe.*

a) $\psi \circ \phi : G \to K$ est un homomorphisme.

b) ϕ est un isomorphisme $\Rightarrow \phi^{-1} : H \to G$ est un isomorphisme.

c) ϕ, ψ sont des isomorphismes $\Rightarrow \psi \circ \phi$ est un isomorphisme.

d) L'identité $Id : G \to G$, $x \mapsto x$, est un automorphisme.

1.1.3 Représentations

But: Réalisation d'un groupe abstrait comme *groupe de transformations* agissant sur un objet($\leftrightarrow$ensemble).

Soit $M \neq \emptyset$ un ensemble. Une **transformation** sur M est une application bijective $T : M \to M, x \mapsto T(x)$. On définit le **groupe symétrique/groupe de permutations** comme ensemble de toutes les transformations sur M (avec la composition d'applications comme loi interne):

$$\mathrm{S}(M) := \{T | T : M \to M \text{ bijective}\}.$$

Définition 1.4 (Représentation)**.** Soit G un groupe et $M \neq \emptyset$ un ensemble. Une **représentation** de G sur M est un homomorphisme de groupe $\alpha : G \to \mathrm{S}(M)$.

Remarques 1.5. Représentation

- $g \in G$ est donc envoyé sur un opérateur $\alpha(g) \in \mathrm{S}(M)$ agissant sur l'ensemble M. Notation: $\alpha(g)(m) =: g \cdot m$.
- $\alpha(gg') = \alpha(g) \circ \alpha(g') \rightsquigarrow \alpha(gg')(m) = \alpha(g)(\alpha(g')(m)) \rightsquigarrow (gg') \cdot m = g \cdot (g' \cdot m)$.
- $\alpha(e) = Id \rightsquigarrow \alpha(e)(m) = m \rightsquigarrow e \cdot m = m$.
- L'**orbite** de $m \in M$ est l'ensemble $\{g \cdot m | g \in G\}$.

Soit $(V, +, *)$ un espace vectoriel sur un corps $\mathbf{K}$.
Rappel: un **homomorphisme linéaire** est une application $f : V \to V$ telle que $\forall a, b \in \mathbf{K} : \forall \vec{v}, \vec{w} \in V : f(a * \vec{v} + b * \vec{w}) = a * f(\vec{v}) + b * f(\vec{w})$.

L'ensemble de tous les isomorphismes linéaires de V est un groupe, appelé **groupe général linéaire** $\mathrm{GL}(V, \mathbf{K})$:

$$\mathrm{GL}(V, \mathbf{K}) := \{A | A \text{ automorphisme linéaire de } V\} \subset \mathrm{S}(V)\,.$$

Exercice: Vérifier que $\mathrm{GL}(V, \mathbf{K})$ est un groupe.

En pratique, V est construit sur $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$. Pour un espace vectoriel de dimension n finie un homomorphisme linéaire peut être representé par une matrice $n \times n$ inversible à coefficients dans $\mathbf{K}$ en choisissant une base. $\mathrm{GL}(V, \mathbf{K})$ peut être consideré comme l'ensemble de toutes les matrices $n \times n$ inversibles ($\det \neq 0$) à coefficients dans $\mathbf{K}$.

Définition 1.5 (Représentation linéaire)**.** Une **représentation linéaire du groupe** G **sur le K-espace vectoriel** V est un homomorphisme de groupe $\rho : G \to \mathrm{GL}(V, \mathbf{K})$.

1. $\dim(V)$: **le degré/la dimension** de la représentation ρ.
2. Une représentation est **fidèle** $:\Leftrightarrow \rho$ est injectif.

Remarques 1.6. Représentation linéaire

1. Il s'agit d'une représentation où: $M = V$(=espace vectoriel) et (plus important) les transformations sont linéaires, c.à.d. éléments de $\mathrm{GL}(V, \mathbf{K}) \subset \mathrm{S}(V)$.

2. La notion de représentation linéaire d'un groupe est *fondamentale* en mathématiques et en physique.

3. Très souvent: "représentation" = "représentation linéaire".

4. Des réalisations non-linéaires jouent un rôle important dans la brisure spontanée d'une symétrie.

1.1.4 Symétries

Groupe $\rightarrow$ Action de groupe sur on objet.

L'objet va être modelisé par un ensemble; Réalisation de groupe comme opérateurs agissant sur cet ensemble.

Groupe de symétrie $\rightarrow$ L'action de groupe ne change pas des observables.

Exercice: [$\rightarrow$ TD1] Faire une liste avec des exemples de groupes/symétries en physique.

- Sur quels objets est-ce que le groupe agit?
- Dans le cas d'une symétrie: quels invariants y a-t-il?

La **brisure d'une symétrie** joue également un rôle très important en physique.

Exercice: Imaginez de quelle manière une symétrie peut être brisée.

1.2 Exemples

1.2.1 Exemples de groupes discrets

Pour $g \in G$ on définit:

$$\begin{aligned} g^0 &:= e, g^1 := g, \ldots, g^{n+1} := (g^n)g \quad \text{pour} \quad n \in \mathbf{N} \\ g^{-n} &:= (g^n)^{-1} = \underbrace{g^{-1} \cdots g^{-1}}_{n \text{ fois}} . \end{aligned}$$

Définition 1.6 (L'ordre d'un élément)**.** Un élément $g \in G$ est dit **d'ordre** n ($n \geq 2$) si $g^n = e$ et $g^m \neq e$ pour $1 \leq m \leq n-1$.

Définition 1.7 (Sous-groupe engendré)**.** Soit $X = \{x_1, \ldots, x_j\} \subseteq G$ avec $0 < j \leq |G|$. Le **sous-groupe engendré** par X est:

$$\langle X \rangle = \langle x_1, \ldots, x_j \rangle := \{x_1^{z_1} \cdots x_j^{z_j} | x_i \in X, z_i \in \mathbf{Z}, i = 1, \ldots, j\}.$$

C'est le plus petit sous-groupe de G contenant le sous-ensemble X.

Exemple 1.8. Groupe cyclique: $C_n := \{e, c, c^2, \ldots, c^{n-1}\}$ avec $c^n = e$

- $|C_n| = n$.
- $C_n = \langle c \rangle < S_n$.
- C_n est abélien ($c^r c^s = c^{r+s} = c^{s+r} = c^s c^r$).
- Réalisations fidèles (isomorphe)
  1. C_n = Rotations d'un polygone régulier avec $n \geq 2$ côtés *oriéntés*. (Le cas $n = 2$ est dégeneré.)
  2. Le groupe de rotations du plan d'angles $\frac{k2\pi}{n}, 0 \leq k \leq n-1$.
  3. Le groupe des nombres complexes, $(\{e^{2ikx/n} | 0 \leq k \leq n-1\}, \cdot)$.
  4. $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$ avec l'addition.

Exemple 1.9. Groupe diédral: $D_n := \langle c, b \rangle$ avec $c^n = b^2 = (bc)^2 = e$

- $|D_n| = 2n$. Éléments: $\{e, c, c^2, \ldots, c^{n-1}, b, bc, \ldots, bc^{n-1}\}$.
- $C_n < D_n \leq S_n$. ($D_n < S_n$ pour $n > 3$).
- Réalisations fidèles (isomorphe)
  1. D_n = Rotations d'un polygone régulier avec $n \geq 2$ côtés *non-oriéntés*.

Exemple 1.10. Groupe D_3: $D_3 := \langle c, b \rangle$ avec $c^3 = b^2 = (bc)^2 = e$

- Symétrie d'un triangle régulier et non-orienté. (Figur).

- $|D_3| = 6$. Éléments: $\{e, c, c^2, b, bc, bc^2\}$.
- Contient les éléments e, c, c^2 de C_3 (rotations de $2\pi/3$ antihoraire). Donc: $C_3 < D_3 \leq S_3$.
- Non-orienté: éléments supplémentaires $\leftrightarrow$ rotations de π autour des axes $0A$, OB, OC. $\rightsquigarrow$ nouveaux genérateurs b_1, b_2, b_3 avec $b_i^2 = e$.
- c envoie chaque axe sur un autre axe: Par exemple, $c(AO) = BO$, c.à.d. b_1 et b_2 sont liés par c.
- Ici, $b_2 = cb_1c^{-1}$. Vérification: $b_2(ABC) = CBA$, $cb_1c^{-1}(ABC) = cb_1(BCA) = c(BAC) = CBA$.
- De même: $b_3 = c^{-1}b_1c$.
- En plus, $b_2 = b_1c$: $b_2(ABC) = CBA$, $b_1c(ABC) = b_1(CAB) = CBA$.
- Donc, $b_1 \equiv b$ suffit et $D_3 = \langle b, c\rangle$ avec $c^3 = b^2 = e$.
- Il faut aussi dire comment b et c commutent! $b_2 = cb_1c^{-1} \stackrel{!}{=} b_1c \Rightarrow cb = bc^2$. Alternativement: $(bc)^2 = b(cb)c = b(bc^2)c = b^2c^3 = e$.
- Resultat final: $D_3 = \langle b, c\rangle$ avec $c^3 = b^2 = (bc)^2 = e$.
- Table de multiplication: voir TD1.

Exemple 1.11. Groupe D_4: voir Jones, p. 10, 11.

Remarques. C_n, D_n en physique
Pour $n = 2, 3, 4, 6$, C_n et D_n appraissent comme groupes de symétrie de certains cristaux. (voir Table 7.3 dans N.W. Ashcroft, N.D.Mermin, Solid State Physics, 1976.)

Exemple 1.12. Le groupe des permutations S_n
Physique: Particules identiques, La statistique des fermions et des bosons

Définition 1.8 (Groupe de permutations)**.** Le **groupe des permutations** de n objets est noté S_n. Un élément $a \in S_n$ est une application $a : \{1, \ldots, n\} \to \{1, \ldots, n\}$ tel que $1 \mapsto a(1)$, $2 \mapsto a(2)$, $\ldots n \mapsto a(n)$. L'élément le plus général peut donc être décrit par

$$a = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}.$$

- L'ordre des colonnes n'est pas pertinent.
- $|S_n| = n!$
- Non-abélien (pour $n \geq 3$):

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{mais} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

- Le symétrique (l'élément inverse):

$$a^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

On peut introduire une notation plus compacte:

Définition 1.9 (Cycle)**.** Un r**-cycle** ($1 \leq r \leq n$) est une permutation de S_n qui est une permutation circulaire de r éléments ($a_1\ a_2\ \dots\ a_r$) et laisse fixe les $n - r$ autres, c.à.d., $a_1 \mapsto a_2, a_2 \mapsto a_3, \dots, a_{r-1} \mapsto a_r, a_r \mapsto a_1$ et $a_j \mapsto a_j$ sinon:

$$(a_1\ a_2\ \dots\ a_r) \equiv \begin{pmatrix} a_1 & a_2 & \dots & a_{r-1} & a_r & a_{r+1} & \dots & a_n \\ a_2 & a_3 & \dots & a_r & a_1 & a_{r+1} & \dots & a_n \end{pmatrix}$$

Pour transformer une permutation en notation cyclique il faut:

a) Réarranger les colonnes (voir exemple)

b) Diviser les cycles

c) Supprimer la ligne en bas

d) Supprimer les 1-cycles

Exemple:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \overset{a)}{=} \left(\begin{array}{cccc|c} 1 & 2 & 4 & | & 3 \\ 2 & 4 & 1 & | & 3 \end{array}\right) \overset{b)}{=} \begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 3 \end{pmatrix} \overset{c)}{=} (1\ 2\ 4)(3) \overset{d)}{=} (1\ 2\ 4)$$

Remarques. Cycles:

1. Permutation générale = Produit de cycles disjoints. [voir Exo. 1.3 a)]

2. Éléments disjoints ⇒ Les cycles commutent.
   On peut donc réarranger les cycles par longeur.

3. L'ordre d'un cycle = Longeur du cycle.
   Par exemple: $(1\ 3\ 2)^3 = (1)(2)(3) \equiv () = e$.

4. L'ordre d'un élément = ppmc(Longeurs des cycles).
   (ppmc = plus petit des multiples communs)

Exemple 1.13. Groupe S_2

- $S_2 = \{(), (1\ 2)\}$. $() = (1)(2)$ est l'identité.
- $|S_2| = 2$.
- $S_2 \cong C_2$: $() \mapsto e, (1\ 2) \mapsto c$.

Exemple 1.14. Groupe S_3

- $S_3 = \{(), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.
- $|S_3| = 3! = 6$.
- $S_3 \cong D_3$: Identifier les trois sommets A, B, C avec 1, 2, 3.
  $() \mapsto e$, $(1\ 2\ 3) \mapsto c$, $(1\ 3\ 2) \mapsto c^2$,
  $(2\ 3) \mapsto b \equiv b_1$, $(1\ 3) \mapsto bc \equiv b_2$, $(1\ 2) \mapsto bc^2 \equiv b_3$.
- Figure!

Exemple 1.15. Groupe S_4

- $S_4 = \{(); 6(\cdot\ \cdot); 3(\cdot\ \cdot)(\cdot\ \cdot); 8(\cdot\ \cdot\ \cdot); 6(\cdot\ \cdot\ \cdot\ \cdot)\}$.
- $|S_4| = 4! = 24$.

On peut écrire chaque r-cycle comme produit de $(r-1)$ 2-cycles (transpositions):

$$(n_1\ n_2\ \ldots\ n_r) = (n_1\ n_2)(n_2\ n_3)\ldots(n_{r-1}\ n_r)\,.$$

Une permutation est dite **paire** (**impaire**) si le nombre de 2-cycles/transpositions est paire (impaire). On définit le signe d'une permutation P:

$$\mathrm{sign}(P) = (-1)^{\text{nombre de transpositions}} = \begin{cases} +1 & \text{P est paire} \\ -1 & \text{P est impaire} \end{cases}.$$

Exemple 1.16. Le **groupe alternante** $A_n := \{P \in S_n | \mathrm{sign}(P) = +1\}$.

- Le groupe A_4 est un candidat pour une symétrie entre les trois générations du modèle standard [3].
- $A_n < S_n$.
- $|A_n| = |S_n|/2 = n!/2$ (voir TD2, ex. 3).

Théorème 1.5 (Cayley)**.** *Chaque groupe fini de l'ordre n est isomorphe à un sous-groupe de S_n.*

Preuve. La multiplication avec $g \in G$ correspond à une permutation (voir table de multiplication). On propose alors come homorphisme

$$\Pi : G \to S_n, \quad g \mapsto \Pi(g) = \begin{pmatrix} e & a & \cdots \\ g & ga & \cdots \end{pmatrix}.$$

Cette application est un homomorphisme:

$$\begin{aligned} \Pi(g_2)\Pi(g_1) &= \begin{pmatrix} e & a & \cdots \\ g_2 & g_2a & \cdots \end{pmatrix}\begin{pmatrix} e & a & \cdots \\ g_1 & g_1a & \cdots \end{pmatrix} \\ &= \begin{pmatrix} g_1 & g_1a & \cdots \\ g_2g_1 & g_2g_1a & \cdots \end{pmatrix}\begin{pmatrix} e & a & \cdots \\ g_1 & g_1a & \cdots \end{pmatrix} \\ &= \begin{pmatrix} e & a & \cdots \\ g_2g_1 & g_2g_1a & \cdots \end{pmatrix} = \Pi(g_2g_1)\,. \end{aligned}$$

L'application est injective:
Supposons $\Pi(g) = \Pi(g')$ pour $g \neq g'$. Alors, $gg_i = g'g_i \Rightarrow g = g'$ en contradiction avec la supposition.
On a donc $G \cong \Pi(G) \leq S_n$. □

Exemple 1.17. $C_3 < S_3$
$C_3 = \{e, c, c^2\}, c^3 = e$

C_3	e	c	c^2
e	e	c	c^2
c	c	c^2	e
c^2	c^2	e	c

$\Pi(e) = \begin{pmatrix} e & c & c^2 \\ e & c & c^2 \end{pmatrix} = (), \Pi(c) = \begin{pmatrix} e & c & c^2 \\ c & c^2 & e \end{pmatrix} = (1\ 2\ 3), \Pi(c^2) = \begin{pmatrix} e & c & c^2 \\ c^2 & e & c \end{pmatrix} = (1\ 3\ 2).$
$\Rightarrow C_3 \cong A_3 < S_3$.

1.2.2 Exemples de groupes continus

- Groupe fini: $g_i \equiv g(i)$, $i = 1, \ldots, n$.
- Groupe infini denombrable: $g_i \equiv g(i)$, $i \in \mathbf{N}$.
- Groupe continu: $g(\alpha_1, \ldots, \alpha_n) \equiv g(\vec{\alpha})$, $\alpha_i \in I_i \subseteq \mathbf{R}$.
  (Plus général: $\vec{\alpha} \in U$ où U est une sous-variété du $\mathbf{R}^n$.)

  On a donc une description par n paramètres continus. Si la parametrisation est minimale (c.à.d. il n y a pas de parametrisation du groupe avec $n-1$ paramètres), n est la **dimension** du groupe.

  Dans le cas continu, ce n'est pas possible de décrire la structure par une table de multiplication. Au lieu de cela, il faut directement spécifier la loi de composition:
  $$g(\vec{\beta}) * g(\vec{\alpha}) = g(\vec{\gamma}), \quad \text{avec } \vec{\gamma} = \vec{\gamma}(\vec{\alpha}, \vec{\beta}).$$

  Le groupe est **compact** si l'interval $I_1 \times I_2 \times \ldots \times I_n \subset \mathbf{R}^n$ (ou la variété $U \subset \mathbf{R}^n$) est compact.

Exemple 1.18. Groupes classiques (=groupes de matrices)

Soit $(V, +, *)$ un espace vectoriel de dimension n sur le corps $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$. Rappel: un **homomorphisme linéaire** est une application $f : V \to V$ telle que $\forall a, b \in \mathbf{K} : \forall \vec{v}, \vec{w} \in V : f(a\vec{v} + b\vec{w}) = af(\vec{v}) + bf(\vec{w})$.
L'ensemble de tous les isomorphismes linéaires de V est un groupe, appelé **groupe général linéaire** $\mathrm{GL}(n, \mathbf{K})$. Un homomorphisme linéaire peut être representé par une matrice $n \times n$ à coefficients dans $\mathbf{K}$ en choisissant une base. $\mathrm{GL}(n, \mathbf{K})$ peut être consideré comme l'ensemble de toutes les matrices $n \times n$ inversibles ($\det \neq 0$) à coefficients dans $\mathbf{K}$. Les groupes classiques sont des sous-groupes de $\mathrm{GL}(n, \mathbf{K})$ qui est le plus large groupe de matrices.

1. **Groupe général linéaire:** $\mathrm{GL}(n, \mathbf{K}) := \{A \in M_n(\mathbf{K}) | \det A \neq 0\}$

   - Dimension: $\mathrm{GL}(n, \mathbf{C})$ a n^2 paramètres complexes, c.à.d. $2n^2$ paramètres réels. On écrit: $\dim_{\mathbf{R}}\{\mathrm{GL}(n, \mathbf{C})\} = 2n^2$ et $\dim_{\mathbf{R}}\{\mathrm{GL}(n, \mathbf{R})\} = n^2$.
   - Sous-groupes: $\mathrm{GL}(n, \mathbf{R}) < \mathrm{GL}(n, \mathbf{C})$.

2. **Groupe spécial linéaire:** $\mathrm{SL}(n, \mathbf{K}) := \{A \in \mathrm{GL}(n, \mathbf{K}) | \det A = 1\}$.

   - Dimension: $\dim_{\mathbf{R}}\{\mathrm{SL}(n, \mathbf{C})\} = 2(n^2 - 1)$ et $\dim_{\mathbf{R}}\{\mathrm{SL}(n, \mathbf{R})\} = n^2 - 1$.
   - Sous-groupes: $\mathrm{SL}(n, \mathbf{R}) < \mathrm{GL}(n, \mathbf{R}) < \mathrm{GL}(n, \mathbf{C})$, $\mathrm{SL}(n, \mathbf{C}) < \mathrm{GL}(n, \mathbf{C})$, $\mathrm{SL}(n, \mathbf{R}) < \mathrm{SL}(n, \mathbf{C})$.

3. **Groupe orthogonal:** $\mathrm{O}(n) := \{A \in \mathrm{GL}(n, \mathbf{R}) | AI_nA^T = A^TI_nA = I_n\}$.

   - $AA^T = I_n \Rightarrow \det(A)^2 = 1 \Rightarrow \det(A) = \pm 1$.
   - Dimension: $\dim_{\mathbf{R}}\{\mathrm{O}(n)\} = n(n-1)/2 = \binom{n}{2}$.
     Le nombre de plans indépendants que l'on peut choisir.
   - Sous-groupes: $\mathrm{O}(n) < \mathrm{GL}(n, \mathbf{R})$.
   - $\mathrm{O}(n)$ est un groupe **compact**.

4. **Groupe spécial orthogonal:** $\mathrm{SO}(n) := \{A \in \mathrm{O}(n) | \det A = 1\}$.

- Dimension: $\dim_{\mathbf{R}}\{\mathrm{SO}(n)\} = \dim_{\mathbf{R}}\{\mathrm{O}(n)\} = \binom{n}{2}$.
  Dans le cas réel la condition $\det A = +1$ ne change pas le nombre de paramètres continus libres.
- Sous-groupes: $\mathrm{SO}(n) = \mathrm{O}(n) \cap \mathrm{SL}(n, \mathbf{R}) \Rightarrow \mathrm{SO}(n) < \mathrm{O}(n)$, $\mathrm{SO}(n) < \mathrm{SL}(n, \mathbf{R})$.
- $\mathrm{SO}(n)$ est **compact**.

5. **Groupe unitaire:** $\mathrm{U}(n) := \{A \in \mathrm{GL}(n, \mathbf{C}) | AI_nA^\dagger = A^\dagger I_n A = I_n\}$.
   - $AA^\dagger = I_n \Rightarrow \det(A)^2 = 1 \Rightarrow \det(A) = e^{i\phi}$.
   - Dimension: $\dim_{\mathbf{R}}\{\mathrm{U}(n)\} = n^2$.
   - Sous-groupes: $\mathrm{U}(n) < \mathrm{GL}(n, \mathbf{C})$.
   - $\mathrm{U}(n)$ est un groupe **compact**.
6. **Groupe spécial unitaire:** $\mathrm{SU}(n) := \{A \in \mathrm{U}(n) | \det A = 1\}$.
   - Dimension: $\dim_{\mathbf{R}}\{\mathrm{SU}(n)\} = \dim_{\mathbf{R}}\{\mathrm{U}(n)\} - 1 = n^2 - 1$.
     Dans le cas complex la condition $\det A = +1$ fixe la phase ϕ et le nombre de paramètres continus libres est reduit par un.
   - Sous-groupes: $\mathrm{SU}(n) = \mathrm{U}(n) \cap \mathrm{SL}(n, \mathbf{C}) \Rightarrow \mathrm{SU}(n) < \mathrm{U}(n)$, $\mathrm{SU}(n) < \mathrm{SL}(n, \mathbf{C})$.
   - $\mathrm{SU}(n)$ est **compact**.
7. **Groupe pseudo-orthogonal:** $\mathrm{O}(n, m) := \{A \in \mathrm{GL}(n + m, \mathbf{R}) | A^T I_{n,m} A = I_{n,m}\}$ avec
$$I_{n,m} := \mathrm{diag}(I_n, -I_m) \equiv \begin{pmatrix} I_n & 0 \\ 0 & -I_m \end{pmatrix}.$$
   - $\mathrm{O}(n, 0) \equiv \mathrm{O}(n)$, le groupe orthogonal. $\mathrm{O}(1, 3)$ est le groupe de Lorentz.
   - Dimension: $\dim_{\mathbf{R}}\{\mathrm{O}(n, m)\} = \dim_{\mathbf{R}}\{\mathrm{O}(n + m)\} = d(d-1)/2$ avec $d = n + m$.
   - Sous-groupes: $\mathrm{O}(n, m) < \mathrm{GL}(n + m, \mathbf{R})$.
   - Non compact (pour $m > 0$).
8. **Groupe spécial pseudo-orthogonal:** $\mathrm{SO}(n, m) := \{A \in \mathrm{O}(n, m) | \det A = 1\}$.
   - $\mathrm{SO}(n, 0) \equiv \mathrm{SO}(n)$, le groupe spécial orthogonal.

- Dimension: $\dim_{\mathbf{R}}\{\mathrm{SO}(n,m)\} = \dim_{\mathbf{R}}\{\mathrm{SO}(n+m)\} = d(d-1)/2$ avec $d = n+m$.
- Sous-groupes: $\mathrm{SO}(n,m) = \mathrm{O}(n,m) \cap \mathrm{SL}(n+m,\mathbf{R}) < \mathrm{GL}(n+m,\mathbf{R})$.
- Non compact (pour $m > 0$).

9. **Groupe pseudo-unitaire:** $\mathrm{U}(n,m) := \{A \in \mathrm{GL}(n+m,\mathbf{C}) | A^\dagger I_{n,m} A = I_{n,m}\}$.
   - $\mathrm{U}(n,0) \equiv \mathrm{U}(n)$, le groupe unitaire.
   - Dimension: $\dim_{\mathbf{R}}\{\mathrm{U}(n,m)\} = \dim_{\mathbf{R}}\{\mathrm{U}(n+m)\} = d^2$ avec $d = n+m$.
   - Sous-groupes: $\mathrm{U}(n,m) < \mathrm{GL}(n+m,\mathbf{C})$.
   - Non compact (pour $m > 0$).
10. **Groupe spécial pseudo-unitaire:** $\mathrm{SU}(n,m) := \{A \in \mathrm{U}(n,m) | \det A = 1\}$.
    - $\mathrm{SU}(n,0) \equiv \mathrm{SU}(n)$, le groupe spécial unitaire.
    - Dimension: $\dim_{\mathbf{R}}\{\mathrm{SU}(n,m)\} = \dim_{\mathbf{R}}\{\mathrm{SU}(n+m)\} = d^2 - 1$ avec $d = n+m$.
    - Sous-groupes: $\mathrm{SU}(n,m) = \mathrm{U}(n,m) \cap \mathrm{SL}(n+m,\mathbf{C}) < \mathrm{GL}(n+m,\mathbf{C})$.
    - Non compact (pour $m > 0$).
11. **Groupe symplectique:** $\mathrm{Sp}(2m,\mathbf{K}) := \{A \in \mathrm{GL}(2m,\mathbf{K}) | A^\dagger J A = J\}$ avec

$$J := \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix} .$$

    - Groupe de transformations canoniques d'un système Hamiltonien.
    - Dimension: $\dim_{\mathbf{R}}\{\mathrm{Sp}(2m,\mathbf{R})\} = m(2m+1)$, $\dim_{\mathbf{R}}\{\mathrm{Sp}(2m,\mathbf{C})\} = 2m(2m+1)$.
      Par exemple: $\dim_{\mathbf{R}}\{\mathrm{Sp}(2m,\mathbf{R})\} = \dim_{\mathbf{R}}\{\mathrm{GL}(2m,\mathbf{R})\} -$ contraintes.
      Contraintes:

$$A = \begin{pmatrix} C & D \\ E & F \end{pmatrix}$$

      avec C, D, E, F des matrices $m \times m$. La condition $A^\dagger J A = J$ donne des contraintes:

      (a) $C^\dagger E = (C^\dagger E)^\dagger$:

      Le triangle au-dessous de la diagonale de $C^\dagger E$ est entièrement determiné. Cela donne $1 + 2 + \ldots + m - 1 = m(m-1)/2$ contraintes.

(b) $C^\dagger F - E^\dagger D = I_m$: m^2 contraintes.

(c) $(C^\dagger F - E^\dagger D)^\dagger = I_m$: Équivalent à b).
Il n'y a pas de contraintes supplémentaires.

(d) $D^\dagger F = (F^\dagger D)^\dagger$: Même nombre de contraintes que a): $m(m-1)/2$.

Au total: $\dim_{\mathbf{R}}\{\mathrm{Sp}(2m,\mathbf{R})\} = 4m^2 - 2 \times m(m-1)/2 - m^2 = 2m^2 + m = m(2m+1)$.

- Non compact.

12. **Groupe spécial symplectique:** $\mathrm{SSp}(2m,\mathbf{K}) := \{A \in \mathrm{Sp}(2m,\mathbf{K}) | \det A = 1\}$.

- Dimension: $\dim_{\mathbf{R}}\{\mathrm{SSp}(2m,\mathbf{R})\} = m(2m+1)$, $\dim_{\mathbf{R}}\{\mathrm{SSp}(2m,\mathbf{C})\} = 2m(2m+1) - 1$.
- Sous-groupes: $\mathrm{SSp}(2m,\mathbf{K}) = \mathrm{Sp}(2m,\mathbf{K}) \cap \mathrm{SL}(2m,\mathbf{K})$.
- Non compact.

Exemple 1.19. Groupe de translations sur $\mathbf{R}^m$: $\mathrm{T}(m) := \{\tau(\vec{a}) | \vec{a} \in \mathbf{R}^m\}$
avec

$$\tau(\vec{a}) : \mathbf{R}^m \to \mathbf{R}^m \,,\, \tau(\vec{a}) : \vec{x} \mapsto \vec{x}' = \vec{x} + \vec{a}$$

- Loi de composition: $\tau(\vec{a}') \cdot \tau(\vec{a}) = \tau(\vec{a} + \vec{a}') = \tau(\vec{a}' + \vec{a}) = \tau(\vec{a}) \cdot \tau(\vec{a}')$ (abélien).
- Identité: $e = \tau(\vec{0})$
- Inverse: $\tau(\vec{a})^{-1} = \tau(-\vec{a})$
- Dimension: $\dim_{\mathbf{R}}\{\mathrm{T}(m)\} = m$.
- Non compact.

Exemple 1.20. Groupe affine sur $\mathbf{R}^{n+m}$: $\mathrm{GA}(n,m) := \{g(A,\vec{a}) | A \in \mathrm{O}(n,m), \vec{a} \in \mathbf{R}^{n+m}\} = \mathrm{O}(n,m) \bigwedge \mathrm{T}(n+m)$ (où $\bigwedge$ est le produit semi-direct)
avec

$$g(A,\vec{a}) : \mathbf{R}^{n+m} \to \mathbf{R}^{n+m} \,,\, g(A,\vec{a}) : \vec{x} \mapsto \vec{x}' = A\vec{x} + \vec{a}$$

- Loi de composition (produit semi-direct): $g(A', \vec{a}') \cdot g(A, \vec{a}) = g(A'A, A'\vec{a} + \vec{a}')$
- Identité: $e = g(I_{n+m}, \vec{0})$.
- Inverse: $g(A, \vec{a})^{-1} = g(A^{-1}, -A^{-1}\vec{a})$.

  Dérivation: $g(A'A, A'\vec{a} + \vec{a}') \stackrel{!}{=} g(I_{n+m}, \vec{0}) \Rightarrow A'A \stackrel{!}{=} I_{n+m}, A'\vec{a} + \vec{a}' \stackrel{!}{=} \vec{0} \Rightarrow A' = A^{-1}, \vec{a}' = -A'\vec{a} = -A^{-1}\vec{a}$.
- Dimension: $\dim_{\mathbf{R}}\{\mathrm{GA}(n,m)\} = \dim_{\mathbf{R}}\{\mathrm{O}(n,m)\} + \dim_{\mathbf{R}}\{\mathrm{T}(n+m)\} = d(d-1)/2 + d = d(d+1)/2$ avec $d = n + m$.
- Sous-groupes: $\mathrm{GA}(n,m) = \mathrm{O}(n,m) \bigwedge \mathrm{T}(n+m) \Rightarrow \mathrm{O}(n,m) < \mathrm{GA}(n,m)$, $\mathrm{T}(n+m) < \mathrm{GA}(n,m)$.
- **Groupe Euclidién**: $\mathrm{E}(n) \equiv \mathrm{GA}(n,0) = \mathrm{O}(n) \bigwedge \mathrm{T}(n)$.
  $\mathrm{E}(n)$ est le groupe de symétrie de E^n, c.à.d. E^n est isotrope autour de 0 (toutes les directions sont équivalentes, $\mathrm{O}(n) < \mathrm{E}(n)$) et E^n est homogène (tous les points sont équivalents, $\mathrm{T}(n) < \mathrm{E}(n)$).
- **Groupe de Poincaré**: $\mathrm{P}(n) \equiv \mathrm{GA}(1, n-1) = \mathrm{O}(1, n-1) \bigwedge \mathrm{T}(n)$.
  Symétrie de l'espace-temps!

Exemple 1.21. Groupe de Galilée: $\mathrm{G}(m) := \{g(A, \vec{a}, \tau, \vec{u}) | A \in \mathrm{O}(m), \vec{u}, \vec{a} \in \mathbf{R}^m, \tau \in \mathbf{R}\}$ avec

$$g(A, \vec{a}, \tau, \vec{u}) : \mathbf{R}^{m+1} \to \mathbf{R}^{m+1}\,, \begin{pmatrix} t \\ \vec{x} \end{pmatrix} \mapsto \begin{pmatrix} t' = t + \tau \\ \vec{x}' = A\vec{x} + \vec{a} + \vec{u}t \end{pmatrix}.$$

Ici, $\vec{u}$ est la vitesse relative entre les référentiels (frames).

- Composition: $g(A', \vec{a}', \tau', \vec{u}') \cdot g(A, \vec{a}, \tau, \vec{u}) = g(A'A, A'\vec{a} + \vec{a}' + \vec{u}'\tau, \tau + \tau', A'\vec{u} + \vec{u}')$.
  Exercice: Check!
- Identité: $e = g(I_m, \vec{0}, 0, \vec{0})$.
- Inverse: $g(A, \vec{a}, \tau, \vec{u})^{-1} = g(A^{-1}, -A^{-1}(\vec{a} - \vec{u}\tau), -\tau, -A^{-1}\vec{u})$.

  Exercice: Determinez $A', \vec{a}', \tau', \vec{u}'$ en utilisant $g(A'A, A'\vec{a}+\vec{a}'+\vec{u}'\tau, \tau+\tau', A'\vec{u}+\vec{u}') \stackrel{!}{=} g(I_m, \vec{0}, 0, \vec{0})$.

- Dimension: $\dim_{\mathbf{R}}\{\mathrm{G}(m)\} = \dim_{\mathbf{R}}\{\mathrm{O}(m)\} + 2m + 1 = (m+1)(m+2)/2$.
  Notez: La dimension du groupe de Galilée sur le $\mathbf{R}^{m+1}$ est égale à la dimension du groupe de Poincaré sur le $\mathbf{R}^{m+1}$ comme il faut: $\dim_{\mathbf{R}}\{\mathrm{G}(m)\} = \dim_{\mathbf{R}}\{\mathrm{P}(m+1)\}$.
- Relativité galiléenne, G(3) symétrie maximale de la mécanique de Newton.
- Non affine (on ne peut pas écrire $\vec{x}' = A\vec{x} + \vec{a}$ avec $A \in \mathrm{O}(m)$).
- Non compact.

1.3 Propriétés générales de groupes

1.3.1 Conjugaison et classes de conjugaison

Définition 1.10 (Conjugaison)**.** Deux éléments $a, b \in G$ sont **conjugués** $:\Leftrightarrow \exists g \in G :$ $a = gbg^{-1}$. On écrit: $a \sim b$.

Remarques. En général g va dépendre de a et b mais n'est pas unique.
Par exemple: $D_3 = \{e, c, c^2, b, b_2 = bc, b_3 = bc^2\}$ avec $c^3 = b^2 = (bc)^2 = e$.
$c \sim c^2 : c = bc^2b^{-1} = b_2c^2b_2^{-1} = b_3c^2b_3^{-1}$ (voir TD1).

Définition 1.11 (Relation d'équivalence)**.** Soit S un ensemble.
Un sous-ensemble $R \subset S \times S$ est une **relation d'équivalence** si

(i) $\forall x \in S : (x, x) \in R$ (Reflexivité)

(ii) $(x, y) \in R \Rightarrow (y, x) \in R$ (Symétrie)

(iii) $(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$ (Transitivité)

On écrit $x \sim y$ si $(x, y) \in R$. Avec cette notation:

(i) $\forall x \in S : x \sim x$ (Reflexivité)

(ii) $x \sim y \Rightarrow y \sim x$ (Symétrie)

(iii) $x \sim y \wedge y \sim z \Rightarrow x \sim z$ (Transitivité)

Exemple 1.22 (Relation d'équivalence)**.**

1. Conjugaison: $a \sim b$ si $\exists g \in G : a = gbg^{-1}$. (Check axiomes)
2. Deux personnes avec les mêmes parents. (Check axiomes)
3. $D_3 : b \sim b_2 = cbc^{-1} \sim b_3 = c^{-1}bc$.

Exemple 1.23. Contrexemples

1. Deux personnes avec la même nationalité (double-nationalité):
   X: Français, Y: Français et Allemand, Z: Allemand
   $X \sim Y, Y \sim Z$ mais $X \not\sim Z$.

Discussion (Conjugaison). $a \sim b \Rightarrow a$ et b sont similaires (avec des propriétés similaires).

Exemple: Rotation
Soit b une rotation par un angle α autour d'un axe $\hat{n}$:

$$b\vec{v} = \vec{v}' .$$

L'élément conjugué gbg^{-1} correspond à une rotation par le même angle α autour de l'axe $g\hat{n}$:

$$(gbg^{-1})(g\vec{v}) = g\vec{v}' .$$

L'espace enter a été tourné par g.

Attention:

- Rotations conjuguées $\Rightarrow$ même angle.
- Même angle $\Rightarrow$ rotation conjuguée?
  Oui pour le groupe entier SO(3).
  Non pour des sous-groupes comme $D_4 < \mathrm{SO}(3)$! Le nouveau axe $g\hat{n}$ peut être hors du sous-groupe (c.à.d. il n'y a aucun élément du sous-groupe qui correspond à une rotation autour de cette axe).

Définition 1.12 (Classe d'équivalence)**.** La **classe déquivalence** de $a \in S$ est l'ensemble $[a] := \{b \in S | b \sim a\}$.

Remarques. Important:

- Les classes d'équivalence sont disjointes:

$$[a] \cap [b] = \begin{cases} \emptyset & \text{si} \quad a \not\sim b \\ [a] = [b] & \text{si} \quad a \sim b \end{cases} .$$

- Une relation d'équivalence sur $S \rightsquigarrow$ **Partition** de S en classes disjointes:

$$\dot{\cup}_{a \in S}\ [a] = S$$

Définition 1.13 (Classe de conjugaison)**.** Soit G un groupe, $a \in G$.
La **classe de conjugaison** est l'ensemble $[a] := \{b \in G | \exists g \in G : b = gag^{-1}\}$.

Exemple 1.24 (Classe de conjugaison)**.**

1. La classe de conjugaison de e est $\{e\}$. (Trivial)
2. Si G est abélien, la classe de conjugaison de $g \in G$ est $\{g\}$. (Trivial)
3. C_n: $[g] = \{g\}\ \forall g \in G$ car C_n est abélien.
4. D_3: Classes:
   - $[e] = \{e\}$,
   - $[c] = \{c, c^2\}$, par ex., $bcb^{-1} = b(cb) = b(bc^2) = c^2$.
   - $[b] = \{b, bc, bc^2\} = \{b \equiv b_1, b_2, b_3\}$
5. S_n:
   - Une permutation $P \in S_n$ possède une decomposition en cycles. Une permutation avec k_1 cycles de longueur l_1, k_2 cycles de longueur l_2 etc. aurait la forme
   $$(l_1)^{k_1}(l_2)^{k_2} \ldots (l_r)^{k_r}$$
   où (sans restriction) $l_1 \geq l_2 \geq \ldots \geq l_r$. Il faut ici inclure les 1-cycles tel que
   $$\sum_{i=1}^{r} k_i l_i = n\,.$$
   Les l_i fournissent donc une partition du nombre entier $n \in \mathbf{N}$.
   - Deux permutations P_1 et P_2 sont conjuguées: $P_1 \sim P_2 \Leftrightarrow P_1$ et P_2 ont la même decomposition en cycles (voir l'exercice 1.3).

- Exemple S_3:

Partition	Permutation	Classe de conjugaison	Corresp. avec $D_3 \cong S_3$
$3 = 1+1+1$	$(1)^3$	$()$	e
$3 = 2+1$	$(2)^1(1)^1$	$(2\ 3), (1\ 3), (1\ 2)$	$b = b_1, b_2, b_3$
$3 = 3$	$(3)^1$	$(1\ 2\ 3), (1\ 3\ 2)$	c, c^2

- Exemple S_4:

Partition	Permutation	Classe de conjugaison	Nombre d'éléments
$4 = 1+1+1+1$	$(1)^4$	$()$	1
$4 = 2+1+1$	$(2)^1(1)^2$	$(\cdot\ \cdot)$	$6 = \binom{4}{2}$
$4 = 2+2$	$(2)^2$	$(\cdot\ \cdot)(\cdot\ \cdot)$	$3 = \frac{1}{2}\binom{4}{2,2}$
$4 = 3+1$	$(3)^1(1)^1$	$(\cdot\ \cdot\ \cdot)$	$8 = \binom{4}{3}$
$4 = 4$	$(4)^1$	$(\cdot\ \cdot\ \cdot\ \cdot)$	$6 = 4!/4$

6. Soit $A \in GL(n, \mathbf{K})$. La classe de conjugaison $[A] = \{PAP^{-1} |\ P \in GL(n, \mathbf{K})\}$ consiste des matrices qui sont semblables à A.

1.3.2 Sous-groupes

Rappel: Soit G un groupe.
$H \subset G$ est un sous-groupe $:\Leftrightarrow$ H est un groupe. On écrit $H < G$.

Définition 1.14 (Classe à gauche ou co-ensemble (coset))**.**
Soit $H < G$. Les **classes à gauche** de H sont les ensembles gH, $g \in G$.
Notation: $gH \equiv [g] = \{gh | h \in H\}$, $G/H := \{gH | g \in G\}$.

Similaire: les **classes à droite**.

Exemple 1.25. Soit $H = \{h_1, h_2, h_3\}$ sous-groupe de G. $gH = \{gh_1, gh_2, gh_3\}$. Notamment: $|gH| = |H|$.

Proposition 1.6.

a) Les classes à gauche sont des classes d'équivalence: $g \sim g' \Leftrightarrow g' \in gH$.

b) $G = \dot{\cup}_{g \in G}\, gH$ *(Partition de G)*

c) $gH \cap g'H \neq \emptyset \Leftrightarrow gH = g'H$

d) $g \sim g' \Leftrightarrow g^{-1}g' \in H \Leftrightarrow gH = g'H$

e) $g \in H \Leftrightarrow gH = H$

Preuve.

a) On a bien une relation d'équivalence:

- Reflexivité: $e \in H \Rightarrow g = ge \in gH \Rightarrow g \sim g$
- Symétrie: $g \sim g' \Rightarrow \exists h \in H : g' = gh \Rightarrow g = g'h^{-1} \Rightarrow g \in g'H \Rightarrow g' \sim g$
- Transitivité:

$$\begin{aligned} g \sim g' &\Rightarrow g' = gh_1\,,\ h_1 \in H \\ g' \sim g'' &\Rightarrow g'' = g'h_2\,,\ h_2 \in H \\ \Rightarrow g'' &= gh_1h_2 = gh_3\,,\ h_3 \in H \Rightarrow g'' \in gH \end{aligned}$$

b),c) Verifié pour chaque relation d'équivalence: a) $\Rightarrow$ b), c)

d) trivial

e) trivial

□

Lemme 1.7. *L'application* $\alpha : [g_1] \to [g_2]\,,\ g_1h \mapsto g_2h$ *est bijective.*

Preuve.

- α est surjectif. [For $g \in [g_2]\, \exists h \in H : g = g_2h$. L'antecédent de g est donc g_1h.]

- α est injectif.
  Soit $g, g' \in [g_1]$ avec $g \neq g'$. À montrer: $\alpha(g) \neq \alpha(g')$.
  $g = g_1 h$, $g' = g_1 h'$ avec $h \neq h' \Rightarrow \alpha(g) = g_2 h \neq \alpha(g') = g_2 h'$.
- α est donc bijectif et $|[g]| = |[e]| = |H|$ $\forall g \in G$.

□

Discussion.

a) Chaque classe à gauche contient le même nombre d'éléments: $\forall g \in G : |gH| = |H|$.

b) De plus, on a $s \equiv |G : H|$ classes à gauche disjointes. On appelle s l'index de H en G.

Par conséquent, $|H|$ doit être un diviseur de $|G|$.

Théorème 1.8 (Lagrange)**.** *Soit G un groupe. $H < G$ un sous-groupe. Si deux parmi les trois grandeurs $|G|$, $|H|$ et $|G : H|$ sont finies, alors la troisième est finie et*

$$|G| = |G : H| \cdot |H| .$$

Preuve. $G = \dot{\cup}_{g \in G} gH$, $|gH| = |H| \Rightarrow |G| = |G : H| \cdot |H|$. □

Corollaire. *$|G| = p$ nombre premier $\Rightarrow$ Il n'y a pas de sous-groupes propres de G.*

Discussion. La structure d'un groupe est très régulier!

Exemple 1.26.

- C_p, p nombre premier. $|C_p| = p$. Il n'y a pas de sous-groupes propres.
- D_3:
  - $|D_3| = 6$.
  - Lagrange: $6 = 3 \cdot 2$: $|H| = 2$, 3 classes à gauche.
  - Lagrange: $6 = 2 \cdot 3$: $|H| = 3$, 2 classes à gauche.
  - Par exemple, $H = \{e, b\}$: $eH = H$, $cH = \{c, cb\}$, $c^2 H = \{c^2, c^2 b = bc\}$.

1.3.3 Sous-groupes normaux

Les classes de conjugaison et les classes à gauche (sous-groupes) partitionnent le groupe mais sont très différentes sinon.

Définition 1.15 (Sous-groupe normal ou invariant)**.**
Un sous-groupe $H \leq G$ est **normal** $:\Leftrightarrow \forall h \in H \forall g \in G : ghg^{-1} \in H$
$:\Leftrightarrow \forall g \in G : gHg^{-1} \subseteq H$
(H inv. sous conjugaison)
On écrit $H \trianglelefteq G$ ($H \lhd G$ pour $H \neq G$).

Proposition 1.9. *$H \trianglelefteq G \Leftrightarrow \forall g \in G : gH = Hg$ (classes à gauche = classes à droite)*

Preuve. Trivial. [$gHg^{-1} \subseteq H \Rightarrow gH \subseteq Hg$. $g^{-1}Hg \subseteq H \Rightarrow Hg \subseteq gH$.] □

Exemple 1.27. D_3

- $C_2 = \{e, b\}$ un sous-groupe normal de D_3?
  Non: La classe de conjugaison de b est $[b] = \{b, bc, bc^2\} \not\subseteq C_2$.
- $C_3 = \{e, c, c^2\}$ un sous-groupe normal de D_3?
  Oui: La classe de conjugaison de c est $[c] = \{c, c^2\} \subset C_3$. Donc $C_3 = [e] \cup [c]$

Définition 1.16 (Groupe quotient G/H)**.** Soit H un sous-groupe *normal* d'un groupe G. L'ensemble des co-ensembles $G/H := \{gH | g \in G\}$ avec le produit $(g_1H)(g_2H) := g_1g_2H$ est un groupe, appelé **groupe quotient**.

Remarques 1.7. Groupe quotient:

- Produit bien défini? Oui:
  Pour $[g_1] = [g_1'], [g_2] = [g_2']$: $[g_1g_2] = [g_1'g_2']$? Oui. $g_1' = g_1h_1$, $g_2' = g_2h_2$. $g_1'g_2'H = g_1h_1g_2h_2H = g_1h_1Hg_2 = g_1Hg_2 = g_1g_2H$.
- Axiomes de groupe sont satisfaits? Oui:
  - G0: $g_1g_2H \in G/H$? OK.

- G1: $[g_1]([g_2][g_3]) = \ldots = ([g_1][g_2])[g_3]$. OK.
- G2: $(eH)(gH) = (eg)H = gH$. Élément neutre $eH \equiv [e]$. OK.
- G3: $(gH)(g^{-1}H) = (gg^{-1})H = eH$. Donc $[g]^{-1} = [g^{-1}]$. OK.

Exemple 1.28. D_3 et $H = \{e, c, c^2\} = C_3 \lhd D_3$
Co-ensembles: $E \equiv \{e, c, c^2\}$ et $B \equiv \{b, bc, bc^2\}$. Est-ce que $\{E, B\}$ forme un groupe?
$E^2 = (eH)(eH) = (ee)H = eH = H = E$
$EB = (eH)(bH) = ebH = bH = B$
De même $BE = B$
$B^2 = (bH)(bH) = b^2H = eH = E$
C'est donc un groupe isomorphe à $C_2 = \{e, b\}$: $D_3/C_3 \cong C_2$.

Exemple 1.29. Contrexemple: D_3 et $H = \{e, b\} = C_2$
$H = \{e, b\} = C_2$ n'est pas un sous-groupe normal. Pour cette raison G/H ne devrait pas être un groupe. Considerons, par ex., $(cH)(cH) = \{c, cb\}\{c, cb\} = \{c^2, c^2b; cbc = b, e\} = c^2H \cup eH$. Ce n'est pas un co-ensemble: $[c][c] = [c^2] \neq [cb][c] = [cbc] = [b]$ (pas bien défini car le résultat dépend du représentant de la classe!)

Définition 1.17 (Produit direct)**.** Soient $G_1, \ldots, G_n$ des groupes. Dans l'ensemble $G = G_1 \times \ldots \times G_n = \{(a_1, \ldots, a_n) | a_i \in G_i (1 \leq i \leq n)\}$ on définit une multiplication par $(a_1, \ldots, a_n)(b_1, \ldots, b_n) := (a_1b_1, \ldots, a_nb_n)$. L'ensemble G avec cette multiplication est un groupe, le **produit direct** des groupes $G_1, \ldots, G_n$.

Remarques.

- Interpretation: Les G_i sont indépendantes. Les éléments de G_i et de G_j $(i \neq j)$ commutent. Plus précisement: G_i' et G_j' commutent avec $G_k' := E_1 \times \ldots E_{k-1} \times G_k \times E_{k+1} \times \ldots \times E_n$ où $E_j = \{e_j\}$.
- Chaque élément $g \in G$ peut être écrit d'une façon unique comme $g = (a_1, \ldots, a_n)$ avec $a_i \in G_i$.
- $G_i \cong G_i'$ $(\forall i = 1, \ldots, n)$.

- $G_i' \lhd G$ $(\forall i = 1, \ldots, n)$.
- $G/G_i' \cong G_1 \times \ldots G_{i-1} \times G_{i+1} \times \ldots \times G_n$.
- $n = 2$: $G = A \times B$, $G/A \cong B$, $G/B \cong A$.
- Problème inverse: Un groupe G donné, ainsi que des sous-groupes A et B il faut vérifier si
  (1) A et B commutent et
  (2) Chaque élément $g \in G$ peut être écrit d'une façon unique comme $g = ab$ avec $a \in A$ et $b \in B$.
  Si c'est le cas, alors, $G \cong A \times B$ et $A \lhd G$, $B \lhd G$.

Exemple 1.30. $D_2 = \langle a, b \rangle$ avec $a^2 = b^2 = (ab)^2 = e$
Sous-groupes: $A = \langle a \rangle \cong C_2 \lhd D_2$ et $B = \langle b \rangle \cong C_2 \lhd D_2$.
A et B commutent car $ab = ba$. $D_2 = \{e, a, b, ab\}$ et chaque élément de D_2 peut être écrit d'une façon unique comme $g = a_i b_j$, $a_i \in A$, $b_j \in B$. Alors, $D_2/C_2 = C_2$ et $D_2 = C_2 \times C_2$.

Exemple 1.31. Contrexemple D_3
Sous-groupes: C_2, C_3 et $D_3/C_3 = C_2$.
Par contre, $D_3 \neq C_2 \times C_3$ car $C_2 \times C_3$ est abélien mais D_3 est non-abélien.
($C_2 \not\lhd D_3$. Bien sûr $C_2 \lhd C_2 \times C_3$.)

1.3.4 Théorème d'isomorphisme

Proposition 1.10. *Soit $f : G \to G'$ un homomorphisme de groupes. Dans ce cas: $Ker(f) \trianglelefteq G$.*

Preuve. $K \equiv \mathrm{Ker}(f) \leq G$. [voir Rem. 1.4]
Soit $g \in G, h \in K$ tel que $f(h) = e'$. On a $ghg^{-1} \in K$ car $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(gg^{-1}) = f(e) = e'$. K est alors un sous-groupe invariant: $K \trianglelefteq G$. □

Théorème 1.11. *Soit $f : G \to G'$ un homomorphisme de groupes. On a*

$$Im(f) \cong G/Ker(f)\,.$$

"Preuve". Il y a une correspondance 1:1: $f(g) \leftrightarrow gK$ avec $K = \mathrm{Ker}(f)$ (image $\leftrightarrow$ co-ensemble)
(i) Est $f(g) \mapsto gK$ bien définit?
Supposons il y a $g, g' \in G$ avec $f(g) = f(g')$ mais $gK \neq g'K$. $\Rightarrow f(g'g^{-1}) = e \Rightarrow g'g^{-1} \in K \Rightarrow g'K = gK$ in contradiction avec la supposition.
(ii) Est $gK \mapsto f(g)$ bien définit?
Supposons il y a $gK = g'K$ avec $f(g) \neq f(g')$. $\Rightarrow g'g^{-1} \in K \Rightarrow f(g') = f(g)$. Contradiction.
(iii) $f(g)f(g') \mapsto (gK)(g'K)$?
f est un homomorphisme: $f(g)f(g') = f(gg')$, $f(gg') \mapsto gg'K = (gK)(g'K)$ □

Resumé: Un homomorphisme de groupes est très régulier!

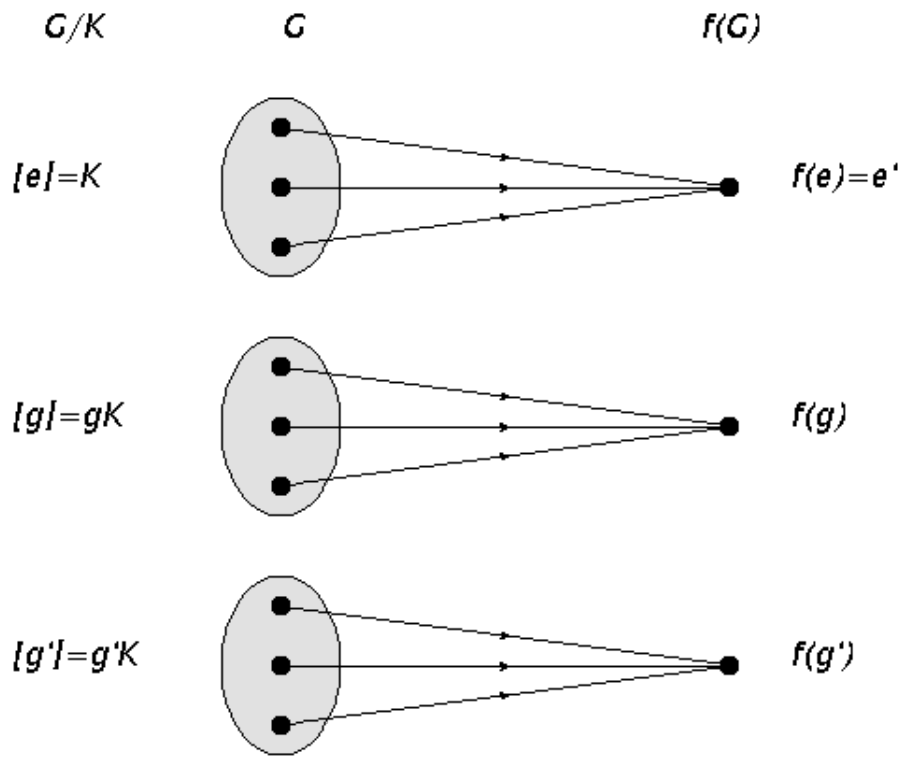

Figure 1.1: *Représentation graphique du théorème d'isomorphisme.*

Corollaire. *Soit $f : G \to G'$ un homomorphisme de groupes. On a*

a) $|Im(f)| = |G|/|Ker(f)|$.

b) L'application f est r:1 avec $r = |Ker(f)|$ car co-ensembles sont imagés en bloque et chaque co-ensemble contient r éléments.

Exercices

Exercice 1.1. Montrer que l'élément neutre e d'un groupe est unique. Montrer ensuite que le symétrique y de tout élément x est également unique.

Exercice 1.2. Montrer qu'un ensemble $G \neq \emptyset$ muni d'une loi de composition interne associative est un groupe si et seulement si

(G2') $\exists e \in G : \forall a \in G : e \star a = a$ (élément neutre à gauche)

(G3') $\forall a \in G : \exists a^{-1} \in G : a^{-1} \star a = e$ (inverse à gauche)

Autrement dit, il suffit qu'il existe un élément neutre à gauche et un élément inverse à gauche.

Exercice 1.3. Classes de conjugaison de S_n
On appelle **cycle** de longueur $k(1 \leq k \leq n)$ une permutation de S_n qui est une permutation circulaire de k éléments et laisse fixe les $n - k$ autres.

a) Montrer que toute permutation est la composition de cycles disjointes. Cette décomposition est-elle unique?

b) Montrer que dans S_n deux éléments sont conjugués si et seulement s'ils ont la même décomposition en cycles. En déduire que le nombre de classes de conjugaison de S_n est le nombre de partitions de l'entier n, c'est-à-dire de suites d'entiers, $\lambda_1, \lambda_2, \ldots, \lambda_l$, tels que $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_l > 0$, et $\sum_{i=1}^{l} \lambda_i = n$.