GROUPES OPÉRANT

Soit X un ensemble quelconque et G un groupe.

I. GÉNÉRALITÉS SUR LES OPÉRATIONS

① DÉFINITIONS

1.1.1. G **opère** (ou **agit**) **à gauche** sur X s'il existe une application $\phi : G\times X \to X$

$$(g, x) \mapsto \phi(g, x) \text{ vérifiant : } \begin{cases} \text{(i)}\ \phi\big(g'; \phi(g; x)\big) = \phi(g'g; x) \\ \text{(ii)}\ \phi(e; x) = x \end{cases}$$

ϕ est appelée **opération** (ou **action**) **à gauche** de G sur X.

2. $\phi(g, x)$ sera noté ${}^g x$.

3. L'existence d'une action à gauche équivaut à celle d'un morphisme φ de G dans $S(X)$, ensemble des permutations de X.

On a alors : $\varphi : G \to S(X)$

$$g \mapsto \varphi(g) : X \to X$$
$$x \mapsto {}^g x$$

📖 On définit de même une **opération à droite**, l'axiome *(i)* devant être alors remplacé par : *(i')* $\phi\big(g', \phi(g, x)\big) = \phi(gg', x)$.
$\phi(g, x)$ sera dans ce cas noté x^g.

Contrairement à une opération à gauche, on ne peut avoir la définition **1.1.3.** équivalente (et bien plus agréable !) au moyen d'un morphisme (en effet, l'application φ définie devrait vérifier : $\varphi(g)\circ\varphi(g') = \varphi(g'g)$). C'est pourquoi la plupart des manuels se borne à étudier les opérations à gauche, ce que nous feront également (sans plus préciser "à gauche").

✋ Pour désigner ϕ ou φ, le mot « action », moins courant, serait préférable au mot « opération », qui désigne plutôt une loi de composition interne. En effet, ${}^g x$ n'est pas le résultat d'une loi interne puisqu'il est construit à partir de $(g, x) \in G\times X$.

On se méfiera donc de certains manuels qui notent $g.x$ pour ${}^g x$. On prendra alors garde à ne pas y voir de loi entre g et x (sauf dans le cas très particulier où X est un groupe dont G est un sous-groupe).

1.2. OPÉRATIONS NATURELLES :

Sur tout ensemble X, le groupe $\big(S(X), \circ\big)$ **opère naturellement** par $\phi : S(X)\times X \to X$

$$(f, x) \mapsto f(x).$$

Le morphisme φ est alors $Id : S(X) \to S(X)$.

☝ En particulier, S_n opère naturellement sur $\{1, ..., n\}$.

Plus généralement, tout groupe de bijections (sous-groupe de $S(X)$) opère naturellement sur X.

📖 On reconnaît, en les axiomes $\cdot$ *(i)* ${}^{g'}({}^g x) = {}^{(g'.g)}x$ et $\cdot$ *(ii)* ${}^e x = x$, ceux que doit respecter le groupe multiplicatif d'un corps $(K, +, .)$ pour qu'un groupe $(E, +)$ soit un K-espace vectoriel.

② PROPRIÉTÉS

2.1. G opère **fidèlement** sur X si $\varphi : G \to S(X)$ est injective

i.e. si : $(\forall\, x \in X\ ;\ {}^g x = x) \Rightarrow g = e$ (e est le seul élément de G qui laisse invariant tout élément de X).

✍ Par exemple, S_n opère fidèlement sur $\{1, ..., n\}$.

☝ G étant alors isomorphe à $Im(\varphi)$, partie de $S(X)$, on peut le plonger dans $S(X)$.

☝ Fidélisation : d'après la décomposition canonique d'un morphisme, $G/Ker(\varphi)$ opère toujours fidèlement sur X.

2.2. G opère **transitivement** sur X si : $\forall\, x, y \in X\ ;\ \exists\, g \in G\ ;\ {}^g x = y$.

✍ Par exemple, S_n opère transitivement sur $\{1, ..., n\}$.

II. EXEMPLES

① OPÉRATIONS DE G SUR LUI-MÊME

1.1. Comme groupe formé de bijections de G sur G, $Aut(G)$ opère naturellement sur le groupe G par : $Aut(G)\times G \to G$

$$(\varphi, g) \mapsto \varphi(g).$$

1.2. On appelle **translation à gauche de** G **sur** G l'opération : $G\times G \to G$

$$(g, x) \mapsto gx.$$

📖 La translation à droite se définit de la même manière par : $(g, x) \mapsto xg$, mais attention : c'est une opération à droite.

☝ La translation à gauche est fidèle.

On en déduit le théorème de Cayley : tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n (voir chapitre 3 - **IV**).

1.3. On appelle **conjugaison de** G **sur** G l'opération : $G\times G \to G$

$$(g, x) \mapsto gxg^{-1}, \text{ appelé } \textbf{conjugué de } x \textbf{ par } g.$$

$\varphi(g) : x \mapsto gxg^{-1}$ est appelé **automorphisme intérieur** associé à g.

a et b sont **conjugués** si : $\exists\, g \in G\ ;\ b = gag^{-1}$.

✋ La conjugaison de G sur G n'opère en général ni fidèlement ni transitivement.

② OPÉRATIONS DE G SUR DES PARTIES DE G

Les opérations définies sur G s'étendent à $\mathscr{P}(G)$ ou à une partie de $\mathscr{P}(G)$.

2.1. Convenons que $\varphi(\varnothing) = \varnothing$, que $g\varnothing = \varnothing$, et que : $g\varnothing g^{-1} = \varnothing$.

1. $Aut(G)$ opère sur $\mathscr{P}(G)$ par : $Aut(G)\times\mathscr{P}(G) \to \mathscr{P}(G)$, $(\varphi, A) \mapsto \varphi(A)$

2. G opère par translation sur $\mathscr{P}(G)$ par : $G\times\mathscr{P}(G) \to \mathscr{P}(G)$, $(g, A) \mapsto gA$

3. G opère par conjugaison sur $\mathscr{P}(G)$ par : $G\times\mathscr{P}(G) \to \mathscr{P}(G)$, $(g, A) \mapsto gAg^{-1}$

2.2. G opère par conjugaison sur l'ensemble des sous-groupes de G.

✋ Pas de translation.

2.3. Sur $(G/H)_g$, ensemble des classes à gauche modulo H, G opère par translation mais seulement à gauche.

✋ Pas de conjugaison.

③ OPÉRATIONS EN GÉOMÉTRIE

3.1.1. $GL(E)$ opère naturellement sur l'espace vectoriel E.

2. $GL(E)$ opère sur l'ensemble des sous-espaces vectoriels de E et sur l'ensemble des sous-espaces vectoriels de dimension fixée de E par : $(u, F) \mapsto u(F)$.

3. $GL(E)$ opère sur l'ensemble des bases de E par : $(u, (e_1, ..., e_n)) \mapsto (u(e_1), ..., u(e_n))$.

☝ En tant que sous-groupes, $SL(E)$, $O(E)$ et $O^+(E)$ opèrent sur les mêmes ensembles que $GL(E)$.

3.2.1. $O(E)$ et $O^+(E)$ opèrent naturellement sur le $\mathbb{R}$-espace euclidien E.

2. $O(E)$ opère sur la sphère unité de E par : $(u, x) \mapsto u(x)$.

3. $O(E)$ opère sur l'ensemble des bases orthonormées de E.

4. $O^+(E)$ opère sur l'ensemble des bases orthonormées de même sens de E.

☝ Remarquons que $O^-(E)$ n'opère pas (il est certes inclus dans $S(G)$, mais ce n'est pas un groupe).

☝ $U(E)$ opère sur le $\mathbb{C}$-espace hermitien E.

3.3.1. $GL_n(K)\times GL_p(K)$ opère sur $\mathscr{M}_{p\times n}(K)$ par : $((P, Q), A) \mapsto QAP$ (relation d'**équivalence**).

2. $GL_n(K)$ opère sur $\mathscr{M}_n(K)$ par conjugaison : $(P, A) \mapsto PAP^{-1}$ (relation de **similitude**).

3. $GL_n(K)$ opère sur $\mathscr{S}_n(K)$, ensemble des matrices symétriques, par : $(P, A) \mapsto PAP^*$ (relation de **congruence**).

3.4.1. $GA(\mathcal{E})$ et tous ses sous-groupes usuels opèrent naturellement sur l'espace affine $\mathcal{E}$.

2. $\vec{\mathcal{E}}$ opère sur $\mathcal{E}$ par : $(\vec{u}, M) \mapsto M + \vec{u}$.

🕮 Et citons l'action par homographie de $SL(\mathbb{R}^2)$ sur le demi-plan de Poincaré $\{z \in \mathbb{C} ; \mathrm{Im}(z) > 0\}$: $(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, z) \mapsto \dfrac{az+b}{cz+d}$, opération à la base de la géométrie hyperbolique.

III. QUOTIENTAGE

① ORBITES

1.2.1. La relation $\mathscr{R}$ définie par ($x \mathscr{R} y$ si : $\exists\, g \in G ; y = {}^g x$) est une relation d'équivalence sur X.

2. Pour $x \in X$, la classe $\omega(x)$ de x est l'ensemble des valeurs prises par les ${}^g x$ quand g parcourt G.
$\omega(x) = \{{}^g x ; g \in G\}$.
On l'appelle la G-**orbite** (ou **trajectoire**) de x.

3. Les G-orbites forment une partition de X.

☝ Certains manuels, notant $g.x$ pour ${}^g x$, notent $G.x$ la G-orbite de x.

☝ Deux éléments d'une même orbite sont parfois dits G-**équivalents**.

☝ Si G opère transitivement, il n'y a qu'une orbite, X.
Le nombre de G-orbites « mesure » en quelque sorte l'intransitivité de l'opération (plus il y a d'orbites, plus on s'éloigne d'une situation de transitivité).
$\mathscr{R}$ et les G-orbites sont parfois appelées respectivement **relation** et **classes d'intransitivité**.

L'ensemble X se trouve donc en partition de classes dont la forme est étroitement liée au groupe G opérant sur X.
On dira que G **quotiente** X et on notera X/G l'ensemble des classes.

☝ Nous avons vu au chapitre 2 comment un sous-groupe H quotiente à gauche un groupe G.
Ce n'est qu'un cas particulier d'un quotientage par opération.
En effet, H opère sur G par translation à droite : $H\times G \to G$, $(h, g) \mapsto gh$.
La H-orbite d'un élément g de G est $\omega(g) = \{gh ; h \in H\} = gH$, qui est bien la classe à gauche de g modulo H.
Et on retrouve les classes à droite en faisant opérer par translation à gauche $(h, g) \mapsto hg$.

Nous avons longuement étudié comment la structure de groupe de G ne se transporte pas à l'ensemble-quotient pour peu que H ne soit pas distingué.

Le problème peut se poser pour tout type de structure possédée par l'ensemble X.

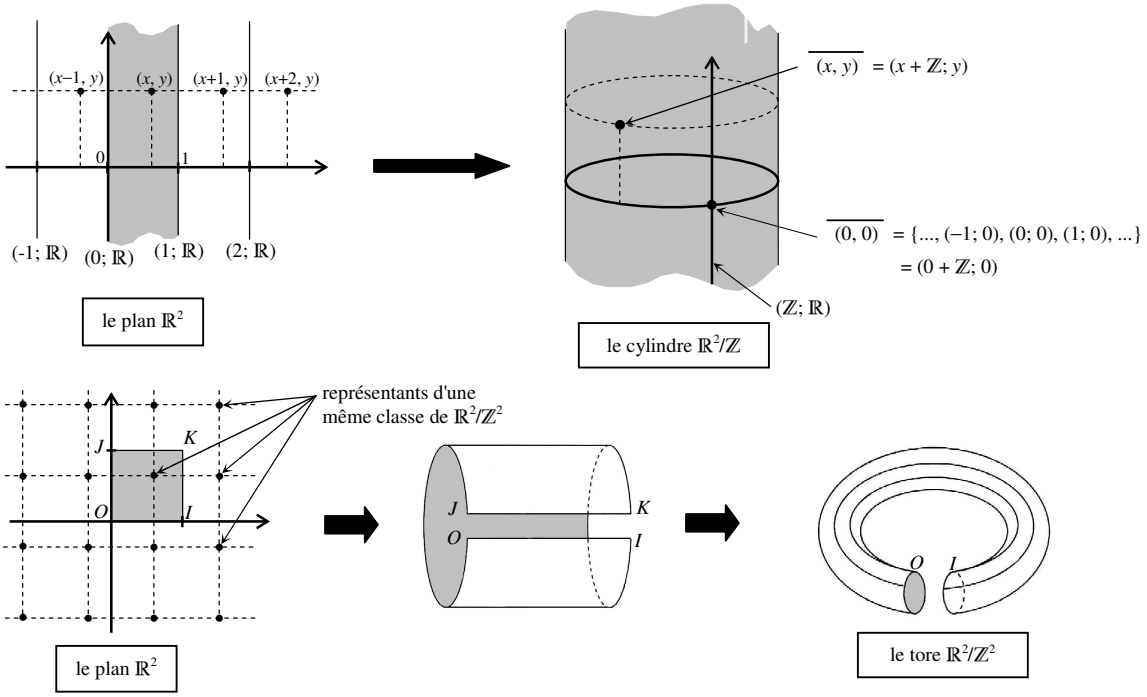
En particulier si X est un espace topologique, il est possible de faire descendre de façon naturelle la topologie de X sur l'espace des orbites X/G pour peu que chaque application $X \to X$

$$x \mapsto {}^g x \text{ soit continue.}$$

☝ En faisant opérer les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}^2, +)$ sur l'espace topologique $\mathbb{R}^2$ par translations :

$\mathbb{Z}\times\mathbb{R}^2 \to \mathbb{R}^2$ et $\mathbb{Z}^2\times\mathbb{R}^2 \to \mathbb{R}^2$

$(n, (x, y)) \mapsto (x + n, y)$ $((n, m), (x, y)) \mapsto (x + n, y + m)$, on dote le cylindre $\mathbb{R}^2/\mathbb{Z}$ et le tore $\mathbb{R}^2/\mathbb{Z}^2$ d'une topologie.



📖 Signalons qu'en quotientant $\mathbb{R}^2/\mathbb{Z}^2$ par $\mathbb{Z}/2\mathbb{Z}$, on obtient une topologie sur la fameuse bouteille de Klein.

② STABILISATEURS

2.1. Le **stabilisateur** de x (ou **groupe d'isotropie** de x) est $S(x) = \{g \in G \,;\, {}^g x = x\}$.

2.2. $S(x)$ est un sous-groupe de G.

2.3. Si la G-orbite $\omega(x)$ est finie :
$Card(\omega(x)) = [G : S(x)]$.

☝ En particulier, quand G est fini, on a : $|G| = |S(x)|.Card(\omega(x))$.

☝ Lorsque G opère par conjugaison sur l'ensemble des sous-groupes de G, le stabilisateur $\{a \in G \,;\, aHa^{-1} = H\}$ d'un sous-groupe H est noté $N(H)$ et appelé **normalisateur** de H.

③ ÉQUATION AUX CLASSES

On appelle **paramétrage** (ou **transversale**) des orbites toute partie de X contenant un et un seul représentant de chacune des G-orbites. On pourra noter $\{\omega(x)\}_{x \in \Omega}$ une partition de X.

3.1. Soit G opérant sur X fini, et Ω un paramétrage des G-orbites.
Alors : $Card(X) = \sum_{x \in \Omega} [G : S(x)]$.

④ CAS PARTICULIER : LA CONJUGAISON DE G SUR LUI-MÊME

4.1.1. Les orbites sont appelées **classes de conjugaison**.

2. Le stabilisateur de g est $C(g) = \{a \in G \,;\, aga^{-1} = g\}$, appelé **centralisateur** de g.

3. $\omega(g)$ est ponctuelle $\Leftrightarrow g \in Z(G) \Leftrightarrow C(g) = G$.

4. ÉQUATION AUX CLASSES DE CONJUGAISON :
Soit Ω^* un paramétrage des classes de conjugaison non ponctuelles.
Alors : $|G| = |Z(G)| + \sum_{x \in \Omega^*} [G : C(x)]$.

✋ Notons que l'étude de la conjugaison n'a de sens que lorsque G est non commutatif.

Si G est commutatif, toutes les orbites sont ponctuelles, les centralisateurs valent tous G, Ω^* est vide et l'équation aux classes nous apprend que : $|G| = |Z(G)|$, ce qui n'est pas très enrichissant...

On réglera donc le cas commutatif avant d'utiliser l'équation.

☝ Dans G non commutatif et pour un élément $g \notin Z(G)$:

- $\omega(g)$ contient au moins 2 éléments : g (conjugué de g par lui-même) et aga^{-1} où a est un élément qui ne commute pas avec g.
- $C(g)$ contient au moins 2 éléments : g (qui commute avec lui-même) et e (qui commute avec tout le monde).

On pourra s'amuser à retrouver que $|G| \geq 4$, ce qui n'est pas vraiment surprenant...

⑤ CLASSIFICATIONS

5.1.1. Une propriété commune à tous les éléments d'une même classe d'équivalence est appelée **invariant**.
2. Une propriété caractéristique de tous les éléments d'une même classe d'équivalence est appelée **invariant total** ou **classifiant**.

☝ On a vu dans le chapitre 2 - **XI** ① **1.5.1.** *b)* que, dans un groupe fini, deux éléments conjugués ont le même ordre. L'ordre est un invariant de conjugaison.

☝ On a vu ainsi dans le chapitre 3 – **II** ④ **4.2.** que deux permutations de S_n sont conjuguées si et seulement si elles sont de même type. Le type est un classifiant de conjugaison dans S_n.

De manière générale, un classifiant permettra la **classification** de l'ensemble X, c'est-à-dire :
- de distinguer facilement les différentes classes
- de les compter
- de trouver un représentant aussi simple que possible de chaque classe.

📖 CLASSIFICATIONS DES OPÉRATIONS DU **II** ③ **3.3.** EN ALGEBRE LINEAIRE :

◆ L'équivalence :

Soit A et B dans $\mathcal{M}_{p\times n}(K)$.

$A \sim B \Leftrightarrow A$ et B représentent la même application linéaire (dans des couples de bases différents).

Le rang est un classifiant d'équivalence : $A \sim B \Leftrightarrow \text{rg}(A) = \text{rg}(B)$.

On en déduit que : - il y a $\inf(n, p) + 1$ classes d'équivalence,

- chaque classe possède un représentant du type $\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$.

◆ La similitude :

Soit A et B dans $GL_n(K)$.

$A \approx B \Leftrightarrow A$ et B représentent le même endomorphisme (dans des bases différentes).

Le rang, le déterminant, la trace et le polynôme caractéristique sont des invariants d'une classe de similitude.

Mais la classification est l'objet de la partie « réduction des endomorphismes » du cours d'algèbre linéaire.

Si K est algébriquement clos (par exemple $\mathbb{C}$) :

$A \approx B \Leftrightarrow A$ et B ont mêmes "réduites de Jordan".

Si $K = \mathbb{R}$, le problème est plus épineux.

Si $n = 2$ ou 3 : $A \approx B \Leftrightarrow A$ et B ont même polynôme caractéristique et même polynôme minimal.

☝ Une autre réduction, celle de Frobenius, amène à la construction d'une suite de polynômes qui se trouvent être invariants de similitude.

◆ La congruence :

Soit A et B dans $\mathcal{S}_n(K)$.

$A \equiv B \Leftrightarrow A$ et B représentent la même forme quadratique.

Si K est algébriquement clos (par exemple $\mathbb{C}$) :

Comme pour l'équivalence, le rang est un classifiant de congruence.

Si $K = \mathbb{R}$:

La signature est un classifiant de congruence : $A \equiv B \Leftrightarrow A$ et B ont même signature.

On en déduit que : - il y a $\frac{(n+1)(n+2)}{2}$ classes de congruence,

-chaque classe possède un représentant du type $\begin{bmatrix} I_s & 0 & 0 \\ 0 & -I_t & 0 \\ 0 & 0 & 0 \end{bmatrix}$.

IV. Exercices

① REMISE À NIVEAU

1.1.1. Étudier la fidélité et la transitivité de la translation à gauche de G sur G.

2. Trouver une condition nécessaire et suffisante sur G pour que la conjugaison de G sur lui-même opère transitivement.
Même question avec fidèlement.

3. Étudier la fidélité et la transitivité de la translation à gauche de G sur $\mathcal{P}(G)$.
Même question avec la conjugaison.

4. Étudier la fidélité et la transitivité de la translation à gauche de G sur $(G/H)_g$.

1.2. Étudier la fidélité et la transitivité des opérations du **II** ③.

1.3. Soit H un sous-groupe de G. On fait opérer H sur G par translation à gauche.
Caractériser les orbites.

1.4. Soit σ, une permutation de S_n.

a) Démontrer que les $<\sigma>$-orbites sont les supports des cycles disjoints de la décomposition de σ.

b) En déduire que : $<\sigma>$ opère transitivement dans $\{1, ..., n\} \Leftrightarrow \sigma$ est un n-cycle.

② AUTRES EXERCICES

2.1. Montrer que si x et y sont dans la même G-orbite, alors les stabilisateurs $S(x)$ et $S(y)$ sont conjugués dans G.

2.2. Démontrer que le normalisateur $N(H)$ est le plus grand sous-groupe de G dans lequel H est distingué.

2.3. THÉORÈME DE CAUCHY :

Si G est un groupe fini et p un diviseur premier de $|G|$, alors il existe un élément d'ordre p.

On l'a déjà montré dans le chapitre 2 - **XII** ③ lorsque G est commutatif.
Le cas non commutatif pourra être traité comme dans le **V** ① **1.4.** *b)* et *c)*. Montrons une autre présentation :

On pose : $S = \{(a_1, ..., a_p) \in G^p \ ; \ a_1...a_p = e\}$, et γ désigne le cycle $(12 \ ... \ p)$.
On fait opérer naturellement $<\gamma>$ sur S en posant : $\forall \ \sigma \in <\gamma> \ ; \ \sigma(a_1, ..., a_p) = (a_{\sigma(1)}, ..., a_{\sigma(p)})$.

a) Déterminer $Card(S)$.

b) Démontrer que les $<\gamma>$-orbites sont ponctuelles ou ont p éléments.

c) Démontrer que le nombre d'orbites ponctuelles est un multiple de p.
(Utiliser l'équation aux classes.)

d) En déduire le théorème de Cauchy : le nombre de solutions dans G de l'équation $x^p = e$ est un multiple de p,
(Utiliser l'équation aux classes.)
puis que tout diviseur premier de $|G|$ est l'ordre d'un élément de G.

- Un théorème de Frobenius affirme que le théorème reste vrai en remplaçant p par un diviseur quelconque de $|G|$.
- C'est faux pour un diviseur non premier : $(\mathbb{Z}/2\mathbb{Z})^4$ a bien des éléments d'ordre 2, mais pas d'ordre 4, 8 ou 16.

2.4. DÉFINITIONS D'UN ESPACE AFFINE :

Soit E un espace vectoriel.
$\mathcal{E}$ est dit **espace affine** de direction E si le groupe $(E, +)$ opère fidèlement et transitivement sur $\mathcal{E}$.

a) Montrer que : $\mathcal{E}$ espace affine de direction $E \Leftrightarrow$ il existe un isomorphisme φ de $(E, +)$ dans un sous-groupe T de $S(E)$ opérant transitivement sur $\mathcal{E}$.

b) Montrer que : $\mathcal{E}$ espace affine de direction $E \Leftrightarrow$ il existe une application $\theta : \mathcal{E} \times \mathcal{E} \to E$ telle que :

- *(i)* pour tout x de E, $\theta_x : y \mapsto \theta(x, y)$ est une bijection de $\mathcal{E} \mapsto E$
- *(ii)* pour tous x, y, z de E : $\theta(x, y) + \theta(y, z) = \theta(x, z)$

- $\theta(x, y)$ est généralement noté $x - y$, ou $\overrightarrow{xy}$.
- L'axiome *(ii)* est appelé "relation de Chasles".

c) Montrer que E peut être considéré comme espace affine de direction E.
(On trouvera un sous-groupe de** $S(E)$ **isomorphe à** $(E, +)$ **et opérant transitivement sur** E.**)

V. Sujets d'étude

① LE THÉORÈME DE BURNSIDE ET SES APPLICATIONS

1.1. LE THÉORÈME DE BURNSIDE :

p étant un nombre premier, on appelle **p-groupe** tout groupe d'ordre p^α, avec $\alpha \in \mathbb{N}^*$.

Démontrer le théorème de Burnside : G est un p-groupe $\Rightarrow Z(G) \neq \{e\}$.

(Étudier l'ordre de $C(x)$ pour $x \in \Omega^*$, puis utiliser l'équation aux classes de conjugaison.)

1.2. 1ère APPLICATION : Montrer que tout groupe d'ordre p^2 est commutatif.

(Raisonner par l'absurde en supposant que l'ordre de $Z(G)$ n'est pas p^2 :

- ***1ère méthode : utiliser le fait que si $G/Z(G)$ est cyclique, alors G est commutatif (voir*** chapitre 2 – **XI ② 2.1.)**
- ***2ème méthode : étudier l'ordre $C(x)$ pour $x \notin Z(G)$.)***

1.3. 2ème APPLICATION : UN CAS PARTICULIER DU THÉORÈME DE SYLOW.

G est un p-groupe $\Rightarrow$ tout diviseur de $|G|$ est l'ordre d'un sous-groupe de G.

a) Supposons le résultat vrai pour tout groupe d'ordre p^α.
Soit G d'ordre $p^{\alpha+1}$ et p^m, avec $m \neq 0$, un diviseur de $p^{\alpha+1}$.
α) Justifier l'existence d'un élément x dans $Z(G) - \{e\}$.
β) Trouver un élément d'ordre p dans $< x >$. On pose H le sous-groupe qu'il engendre.
(On peut exhiber l'élément ou assurer son existence en appliquant à $Z(G)$ le résultat du chapitre 2 - **XII ③.)**
γ) Justifier qu'on peut quotienter G par H et qu'il existe un sous-groupe K de G/H d'ordre p^{m-1}.
(On pourra se demander pourquoi ne pas avoir appliqué le résultat du* IV ② 2.3. *directement à G pour avoir un élément d'ordre p dans le β) !)
δ) Si φ désigne le morphisme canonique de G dans G/H, montrer que $\varphi^{-1}(K)$ est d'ordre p^m.
b) Montrer par récurrence sur α le résultat.

1.4. 3ème APPLICATION : LE THÉORÈME DE SYLOW :

Si G est un groupe fini et p^n un diviseur de $|G|$ avec p premier, alors il existe un sous-groupe d'ordre p^n.

On utilisera un résultat vu dans le chapitre 2 - **XII** ③ : si G un groupe commutatif fini, alors tout diviseur premier de $|G|$ est l'ordre d'un sous-groupe de G.

a) Montrer le théorème de Sylow lorsque G est commutatif.
(Utiliser le résultat du chapitre 2 ***puis raisonner comme dans le* 3.1. *c) α) 3) et 4).)***
b) Soit G non commutatif et supposons le théorème de Sylow vrai pour les groupes d'ordre $< |G|$.
α) Montrer le théorème si p^n divise l'ordre d'un centralisateur.
β) Montrer le théorème si p^n ne divise aucun des ordres de centralisateurs.
(Utiliser l'équation aux classes de conjugaison pour appliquer le résultat du chapitre 2 ***sur $Z(G)$.)***
c) Conclure.

1.5. 4ème APPLICATION : RÉSOLUBILITÉ DES p-GROUPES

a) Montrer que si G est d'ordre p^n avec p premier, alors :
il existe une suite décroissante de sous-groupes distingués $G_n = \{e\} \subseteq G_{n-1} \subseteq ... \subseteq G_0 = G$ telle que :
$\forall\ 0 \leq k \leq n\ ;\ |G_k| = p^{n-k}$.
(Raisonner par récurrence sur α et raisonner comme dans le* 1.3. *a) β) et γ) pour descendre l'exposant.)
b) En déduire que tout p-groupe est résoluble.

② LES 6 TYPES DE SOUS-GROUPES FINIS DE $O^+(3)$

Rappelons que $O^+(3)$ est composé des rotations « axiales ».
Soit G un sous-groupe fini propre (c'est-à-dire distinct de $\{Id\}$) de $O^+(3)$ et n son ordre.
On appelle pôles d'une rotation les deux points d'intersection de son axe et de la sphère unité S^2 de $\mathbb{R}^3$.
On pose $\mathcal{P}$ l'ensemble des pôles de toutes les rotations de G - $\{Id\}$.
On fait opérer naturellement G sur $\mathcal{P}$, et pour tout P de $\mathcal{P}$, on note S_P son stabilisateur et ω_P son orbite.
On rappelle que, pour tout P : $|S_P|.Card(\omega_P) = n$.
Donc, tous les stabilisateurs des pôles d'une même orbite ω_k ont même cardinal, que nous noterons s_k.
Soit A un paramétrage des orbites, contenant un et un seul point de chaque orbite.

2.1. Montrer que : $2(1-\frac{1}{n}) = \sum_{P \in A} (1-\frac{1}{|S_P|})$.

(Dénombrer, de deux manières différentes, les couples (rotation r, pôle de r) ***de*** $(G - \{Id\}) \times \mathcal{P}$ ***:***

- ***en comptant les rotations, puis le nombre de pôles de chacune***
- ***en comptant les points d'une orbite, puis le nombre de rotations dont chaque point est pôle.)***

2.2. Montrer qu'il n'y a que 2 ou 3 orbites.

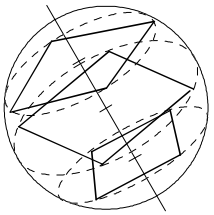
(Montrer puis utiliser le fait que tout stabilisateur contient au moins 2 éléments.)

2.3. Cas où il y a 2 orbites :

a) Montrer que chaque orbite est ponctuelle.

b) En déduire que G est cyclique.

(Utiliser la nature des sous-groupes finis de $O^+(2)$: voir cours sur les groupes.)



cas $n = 4$

☝ G est engendré par une rotation d'angle $\frac{2\pi}{n}$.

Ses rotations laissent stables tous les n-gones réguliers plans inscrits dans S^2 ayant leur centre sur l'axe commun à ces rotations.

Attention, pour ce qui est du n-gone de même centre que S^2, G n'est que la « moitié » du sous-groupe de $O^+(3)$ contenant toutes les rotations le laissant stable (voir **2.5.**).

2.4. Détermination des cas où il y a 3 orbites :

On pose désormais : $s_1 \leq s_2 \leq s_3$.

a) Montrer que : $s_1 = 2$.

b) Montrer que : $s_2 = 2 \Rightarrow 2s_3 = n$.

c) Montrer que : $s_2 = s_3 = 3 \Rightarrow n = 12$.

d) Montrer que : $s_2 = 3$ et $s_3 = 4 \Rightarrow n = 24$.

e) Montrer que : $s_2 = 3$ et $s_3 = 5 \Rightarrow n = 60$.

f) Montrer qu'il est impossible d'avoir : $s_2 = 3$ et $s_3 \geq 6$.

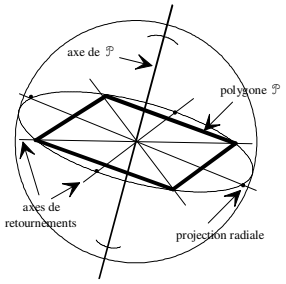
g) Montrer qu'il est impossible d'avoir : $s_2 \geq 4$ et $s_3 \geq 4$.

2.5. 1er cas : $s_1 = s_2 = 2$ et $s_3 = \frac{n}{2}$

a) Soit $P \in \omega_3$. Posons r un élément de S_P et ρ un élément de $G - S_P$.

Montrer que : $r^{n/2} = \rho^2 = r\rho r\rho = e$.

b) En déduire que G est isomorphe au groupe diédral $D_{n/2}$.



cas $n = 8$

☝ De $G \approx D_{n/2}$, on déduit que G est le sous-groupe de $O^+(3)$ constitué de toutes les rotations laissant stable un $(n/2)$-gone régulier plan $\mathcal{P}$ inscrit dans S^2 et de même centre que S^2.

Attention, ce n'est qu'une isomorphie : $D_{n/2}$ est composé d'éléments de $O^+(2)$ et de $O^-(2)$, restrictions au plan de $\mathcal{P}$ des éléments de G, qui sont bien dans $O^+(3)$.

Les éléments de G sont :

- les $\frac{n}{2}$ rotations engendrées par la rotation d'angle $\frac{2\pi}{n}$ et dont l'axe est celui de $\mathcal{P}$ (dont les restrictions sont les rotations de $D_{n/2}$),
- les $\frac{n}{2}$ retournements autour des droites reliant le centre de $\mathcal{P}$ et les sommets et les milieux de côté de $\mathcal{P}$ (dont les restrictions sont les symétries de $D_{n/2}$).

Les 3 orbites sont :

- ω_1, formée des $\frac{n}{2}$ sommets de $\mathcal{P}$, reliés deux à deux par une des rotations d'angles $\frac{2k\pi}{n}$.
- ω_2, formée des $\frac{n}{2}$ projections radiales sur S^2 des milieux de côté de $\mathcal{P}$, reliés deux à deux par un des retournements.

  ($s_1 = s_2 = 2$: chaque sommet P de ω_1 ou de ω_2 est invariant par Id et par le retournement d'axe passant par P.)
- ω_3, formée des 2 points d'intersection de S^2 avec l'axe de $\mathcal{P}$, reliés par n'importe lequel des retournements.

  ($s_3 = n/2$: chaque sommet P de ω_3 est invariant par les $\frac{n}{2}$ rotations d'angles $\frac{2k\pi}{n}$.)

2.6. 2ème cas : $s_1 = 2$, $s_2 = s_3 = 3$ et $n = 12$

a) Posons : $\omega_2 = \{P_1, P_2, P_3, P_4\}$.

Soit $\varphi : G \to S(\omega_2)$ le morphisme défini par : $\varphi(r) = \begin{pmatrix} P_1 & P_2 & P_3 & P_4 \\ r(P_1) & r(P_2) & r(P_3) & r(P_4) \end{pmatrix}$.

Montrer que φ est injectif

b) En déduire que G est isomorphe au groupe alterné A_4.

☝ De $G \approx A_4$, on déduit que G est le sous-groupe de $O^+(3)$ constitué de toutes les rotations laissant stable un tétraèdre régulier inscrit dans S^2.

2.7. 3ème cas : $s_1 = 2$, $s_2 = 3$, $s_3 = 4$ et $n = 24$

Montrer, en utilisant le morphisme φ de **2.6.**, que G est isomorphe au groupe symétrique S_4.

☝ De $G \approx S_4$, on déduit que G est le sous-groupe de $O^+(3)$ constitué de toutes les rotations laissant stable un cube (ou son octaèdre régulier dual) inscrit dans S^2.

2.8. 4ème cas : $s_1 = 2$, $s_2 = 3$, $s_3 = 5$ et $n = 60$

Montrer, en utilisant le morphisme φ de **2.6.**, que G est isomorphe au groupe alterné A_5.

☝ De $G \approx A_5$, on déduit que G est le sous-groupe de $O^+(3)$ constitué de toutes les rotations laissant stable un icosaèdre régulier (ou son dodécaèdre dual) inscrit dans S^2.

Bibliographie

Arnaudiès, Fraysse	*Cours de mathématiques - Algèbre*	Dunod	Théorie complète, des exemples, théorème de Burnside.
Berger	*Géométrie Tome 1*	Nathan	Théorie complète, des exemples, et les sous-groupes finis de $O^+(3)$.
Bouvier, Richard	*Groupes*	Hermann	Théorie complète, théorème de Burnside, théorème de Sylow, existence d'un élément d'ordre un diviseur premier de $\|G\|$, définitions d'un espace affine, étude détaillée des sous-groupes finis de $O^+(3)$.
Calais	*Éléments de théorie des groupes*	PUF	Théorie complète, théorème de Burnside et ses applications.
Francinou, Gianella	*Exercices de mathématiques pour l'agrégation*	Masson	Pas de cours, quelques exercices bien faits sur les p-groupes.
Frenkel	*Géométrie pour l'élève-professeur*	Hermann	Rappels théoriques, définitions d'un espace affine.
Gourdon	*Algèbre*	Ellipses	Théorie complète, théorème de Burnside et ses applications, existence d'un élément d'ordre un diviseur premier de $\|G\|$, théorème de Sylow, théorème de Wedderburn.
Lafon	*Algèbre*	Hermann	Étude des sous-groupes finis de $O^+(3)$, théorème de Wedderburn.
Lelong-Ferrand, Arnaudiès	*Algèbre*	Dunod	Théorie complète.
Perrin	*Cours d'algèbre*	Ellipses	Théorie complète, exemples, théorème de Burnside.
Ramis, Deschamps, Odoux	*Cours de mathématiques spéciales - Algèbre*	Masson	Théorie complète.