Théorie des groupes

Sous-groupes engendré:

On se propose de montrer que le sous-groupe de G engendré par une partie P défini ci-dessous est bien **le plus petit sous-groupe qui contient** P:

$$H = \langle P \rangle := \left\{ h_1^{k_1} h_2^{k_2} \dots h_n^{k_n} \ ; \ n \in \mathbb{N} \ , \ h_i \in H \ , \ k_i \in \mathbb{Z} \right\}$$

On montre facilement que le plus petit sous-groupe qui contient P est l'intersection ci-dessous, reste à montrer l'égalité suivant:

$$H = \bigcap_{\substack{P \subseteq Q \\ Q < G}} Q$$

On appelle $\widetilde{H}$ l'interesection ci-dessus puis on procède par double inclusion:

- Le sous-groupe H est un sous-groupe qui contient P trivialement, donc en particulier, on a par les propriétés de l'intersection que $\widetilde{H} \subseteq H$.
- Le sous-groupe $\widetilde{H}$ contient tout les élément de P, donc par stabilité, il contient nécéssairement toutes les combinaisons trouvées dans H, ie on a bien $H \subseteq \widetilde{H}$.

Sous-groupes monogène d'un groupe fini:

On se donne G un groupe fini, et $g \in G$, alors il existe un entier positif tel que:

$$g^k = 1$$

En effet l'ensemble $\{g^k, k \in \mathbb{N}\}$ ne prends qu'un nombre fini de valeurs, donc il existe nécessairement deux indices $n > p$ tel que:

$$g^n = g^p$$

Et donc $g^{n-p} = 1$

Image d'une partie génératrice:

On se donne un groupe $G = \langle P \rangle$ pour P une partie de G, ainsi qu'un morphisme $\phi : G \longrightarrow H$, on veut alors montrer que l'image d'une partie génératrice est génératrice, ie que:

$$f(G) = \langle f(P) \rangle$$

On se donne un élément $f(g) \in f(G)$, alors on a que g se décompose en produit **fini** de puissances d'éléments de P et donc on a:

$$f(g) = f\left(\prod_{p_i \in P} p_i^{k_i} \right) = \prod_{p_i \in P} f(p_i)^{k_i}$$

Fininalement on a bien que $f(g)$ s'écrit comme produit **fini** de puissances d'éléments de $f(P)$ donc on a bien le résultat.

Théorème de Cayley:

On se propose de démontrer que tout groupe G est **isomorphe à un groupe d'automorphismes**, on définit l'application suivante:

$$\Phi : G \longrightarrow \mathrm{Aut}(G, G)$$
$$g \longmapsto \phi_g$$

Où $\phi_g(x) = gx$, ie on associe à chaque élément de G la fonction qui translate tout les éléments de G par celui-ci, alors:

- Cette application est facilement un **morphisme de groupes**.
- Cette application est facilement **injective**.

Finalement, on a bien que $G \cong \mathrm{Im}(\Phi) < \mathrm{Aut}(G, G)$ comme souhaité.

Sous-groupes de $\mathbb{Z}$:

On se propose de montrer la propriété suivante:

$$H < \mathbb{Z} \iff \exists n \in \mathbb{Z}\ ;\ H = n\mathbb{Z}$$

On se donne un sous groupe $H < \mathbb{Z}$ et on distingue deux cas:

- Si H est trivial, alors $H = 0\mathbb{Z}$ qui convient.
- Sinon H contient un élément non-nul, donc un élément **positif** h.

Dans ce cas, la partie $H \cap \mathbb{N}^*$ est non-vide, et donc elle contient un plus petit élément qu'on notera n. On va alors montrer que tout élement du groupe est un multiple de cet élément.

En effet soit $h \in H$, alors on effectue la division euclidienne de h par n et on obtient:

$$h = nq + r\ ;\ r \in [\![0\ ;\ n-1]\!]$$

Mais alors par construction on a $r < n$ et $r \in H \cap \mathbb{N}^*$ par opérations, donc nécéssairement $r = 0$, car sinon, n ne serait pas le plus petit élément de la partie considérée.

Classificiation des groupes cycliques:

On se propose de classifier les groupes cycliques G, engendrés pas un élément $g \in G$, alors on définit:

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow G \\ n &\longmapsto g^n \end{aligned}$$

Alors cette application est **un morphisme de groupe surjectif**, aussi le noyau de ϕ est un sous-groupe normal, et on sait que les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$, on distingue alors deux cas:

- Soit $\mathrm{Ker}\phi$ est trivial et alors ϕ est un isomorphisme: $G \cong \mathbb{Z}$.
- Soit $\mathrm{Ker}\phi = n\mathbb{Z}$ et alors ϕ induit un isomorphisme par passage au quotient: $G \cong \mathbb{Z}/n\mathbb{Z}$

Finalement on a bien montré qu'il n'y a bien qu'un seul groupe cyclique d'ordre n qui est $\mathbb{Z}/n\mathbb{Z}$ et qu'un seul groupe cyclique d'ordre infini qui est $\mathbb{Z}$.

Groupe Symétrique

On note S_n l'ensemble des bijections sur $\{1, \dots, n\}$ et on montre facilement que c'est un groupe pour la composition.

Cardinal de S_n

Montrons par récurrence sur n la propriété suivante:

$$|A| = |B| = n \implies \left|\mathrm{Bij}(A, B)\right| = n!$$

L'initialisation est triviale, en effet si les deux ensembles sont vides, il n'existe qu'une seule application bijective du vide dans lui-même.

Soit ϕ une bijection de A' dans B' ensembles de cardinal $n+1$, alors il existe $n+1$ choix possibles pour l'image de l'élément a_1, on considère alors la restriction:

$$\begin{aligned} \widetilde{\phi} : A' \backslash \{a_1\} &\longrightarrow B' \\ x &\longmapsto \phi(x) \end{aligned}$$

Alors $\phi(a_1)$ n'est pas dans l'image de cette fonction car sinon cela contredirait l'injectivité de ϕ, on peut donc restreindre à l'arrivée en une fonction bijective:

$$\begin{aligned} \widetilde{\phi} : A' \backslash \{a_1\} &\longrightarrow B' \backslash \{\phi(a_1)\} \\ x &\longmapsto \phi(x) \end{aligned}$$

C'est une fonction bijective entre deux ensembles de cardinal n, il ya donc par hypothèse de récurrence $n!$ choix possibles pour une telle fonction. Finalement par dénombrement, on a bien qu'il y a $(n+1)n! = (n+1)!$ choix possibles de fonctions bijectives entre ensembles de taille $n+1$.

On conclut sur le groupe symétrique en prenant $A = B = \{1, \dots, n\}$

Isomorphisme sur les ensembles de même cardinal

On se donne X un ensemble de cardinal n, montrons que $S(X) \cong S_n$. On sait qu'il y a une bijection i entre X et $\{1, \dots, n\}$ donnée par:

$$i : k \in \{1, \dots, n\} \mapsto x_k \in X$$

On pose $\sigma \in S_n$ et $\tau \in S(X)$ et on considère le diagramme commutatif suivant:

$$\begin{array}{ccc} \{1, \dots, n\} & \xrightarrow{\sigma} & \{1, \dots, n\} \\ \downarrow{\scriptstyle i} & & \uparrow{\scriptstyle i^{-1}} \\ X & \xrightarrow{\tau} & X \end{array}$$

Ceci nous donne directement l'isomorphisme, en effet on pose:

$$\phi : \tau \in S(X) \mapsto i^{-1} \circ \tau \circ i \in S_n$$

Alors ϕ est bien une bijection de $S(X)$ sur S_n, et on montre facilement que c'est un morphisme car:

$$\phi(\tau_1 \tau_2) = i^{-1}(\tau_1 \tau_2) i = i^{-1} \tau_1 i i^{-1} \tau_2 i = \phi(\tau_1)\phi(\tau_2)$$

Non-commutativité

On se propose de montrer que S_n n'est pas commutatif pour $n \geq 3$, on montre pour cela que son centre est trivial ie:

$$Z(S_n) = \{Id\}$$

Supposons par l'absurde qu'il soit non-trivial, alors il existe une permutation $\sigma \neq Id$ qui commute avec toutes les autres. Elle admet au moins un point x tel que $\sigma(x) \neq x$, mais alors il y a 3 éléments distincts dans S_n donc il existe $y \in \{1, \ldots, n\}$ tel que:

$$\begin{cases} y \neq x \\ y \neq \sigma(x) \end{cases}$$

On définit alors σ' comme une permutation telle que:

$$\begin{cases} \sigma'(x) = x \\ \sigma'(\phi(x)) = y \end{cases}$$

Alors on a que nécessairement:

$$\begin{cases} \sigma\sigma'(x) = \sigma(x) \\ \sigma'\sigma(x) = y \end{cases}$$

Ce qui est absurde car σ devrai commuter, donc le centre est bien trivial.

Propriétés du support

1. On considère σ, τ deux permutations de S_n, montrons que:

   $$\text{Supp}(\sigma\tau) \subseteq \text{Supp}(\sigma) \cup \text{Supp}(\tau)$$

   Passons au complémentaire, on obtient que la propriété est équivalente à:

   $$\text{Fix}(\sigma) \cap \text{Fix}(\tau) \subseteq \text{Fix}(\sigma\tau)$$

   Qui est trivialement vérifiée.

2. Un lemme utile pour la suite:

   $$x \in \text{Supp}(\sigma) \implies \sigma(x) \in \text{Supp}(\sigma)$$

   C'est évident car sinon σ ne serait pas injective.

3. Supposons maintenant que:

   $$\text{Supp}(\sigma) \cap \text{Supp}(\tau) = \emptyset$$

   Alors on a égalité, en effet si x est fixé par τ mais pas par σ, alors on a:

   $$\sigma\tau(x) = \sigma(x) \neq x$$

   Donc il est bien dans le support du produit, et si x est fixé par σ mais pas par τ, alors on a:

   $$\sigma\tau(x) = \tau(x) \neq x$$

   Car $\tau(x)$ est dans le support de τ par le lemme, et donc est fixé par σ.

Les permutations à supports disjoints commutent

Soit deux permutations σ, τ à supports disjoints et $x \in \{1, \dots, n\}$, alors on distingue deux cas:

- Si x est dans le support de τ, alors il est fixé par σ par hypothèse et $\tau(x)$ est fixé par σ par le lemme précédent donc on a:
$$\tau(\sigma(x)) = \tau(x) \quad \text{et} \quad \sigma(\tau(x)) = \tau(x)$$
- Si x n'est pas dans le support de τ, alors par symétrie, il est dans le support de σ et on conclut par le même calcul.

En particulier si on a:
$$\sigma\tau = \mathrm{Id}$$
Alors les deux permutations sont l'identité car:

- Si x est dans le support de τ, alors il est fixé par σ mais alors on a une absurdité, donc le support est vide.
- Si x n'est pas dans le support de τ, alors par symétrie, il est dans le support de σ mais alors on a aussi une absurdité, donc le support est vide.

Décomposition en cycles à supports disjoints

Soit $\sigma \in S_n$, alors on définit l'ensemble suivant appelé σ-orbite de $x \in [\![1\ ;\ n]\!]$ par:
$$\mathcal{O}_x := \{\sigma^k(x)\ ;\ k \in \mathbb{N}\}$$
Alors par un simple raisonnement sur l'ordre et les propriétés de cet ensemble on montre facilement que:
$$\forall x, y \in [\![1\ ;\ n]\!]\ ;\ \mathcal{O}_x \cap \mathcal{O}_y = \emptyset \text{ ou } \mathcal{O}_x = \mathcal{O}_y$$
En outre si on définit la relation d'équivalence sur $[\![1\ ;\ n]\!]$ par:
$$x \sim y \iff \mathcal{O}_x = \mathcal{O}_y$$
On peut alors **partitionner** $[\![1\ ;\ n]\!]$ en $k \leq n$ orbites, et donc il existe une famille de représentants $(x_1, \dots x_k) \in [\![1\ ;\ n]\!]$ tels que:
$$[\![1\ ;\ n]\!] = \bigcup_{i \leq k} \mathcal{O}_{x_k}$$
On pose alors:
$$\tau = (x_1 \dots \sigma^{l_1}(x_1)) \dots (x_k \dots \sigma^{l_k}(x_k)) = c_1 \dots c_k$$
Alors les supports de ces cycles sont exactement les orbites prédéfinies et il suffit de montrer que $\sigma = \tau$:

- Si $x \notin \mathrm{Supp}(\sigma)$ alors son orbite est un singleton et $\sigma(x) = \tau(x) = x$
- Si $x \in \mathrm{Supp}(\sigma)$ alors il appartient à un unique cycle c_i et on a $\tau(x) = \sigma(x)$ par définition de ces cyles.

Ordre d'une permutation

Sois σ une permutation sur $\{1, \dots, n\}$, alors on a d'aprés la propriété précédente que pour $k \leq n$ il existe une famille $(c_j)_{j \leq k}$ de cycles à supports disjoints tels que:

$$\sigma = c_1 \dots c_k$$

Soit $i \in \mathbb{N}$, alors on sait que les supports sont disjoints donc on a:

$$\sigma^i = \mathrm{Id} \implies c_1^i \dots c_k^i = \mathrm{Id} \implies \forall c \in (c_j)\ ;\ i \in \mathrm{ord}(c)\mathbb{N} \tag{1}$$

En d'autres termes i doit être un multiple de l'ordre de chaque cycle, en effet supposons l'inverse ie qu'il existe un cycle $c \in (c_j)$ tel que $\mathrm{ord}(c) \nmid k$, alors pour x dans le support de ce cycle, on aurait:

$$\sigma^i(x) = c^i(x) \neq x \implies \sigma^i \neq \mathrm{Id}$$

En reformulant la dernière partie de (1), on trouve donc que:

$$\sigma^i = \mathrm{Id} \implies i \in \bigcap_{c \in (c_j)} \mathrm{ord}(c)\mathbb{N}$$

Or le plus petit i qui vérifie $\sigma^i = \mathrm{Id}$ est donc le plus petit élément de l'ensemble ci-dessus des multiples communs des ordres, qui est par définition le plus petit commun multiple des ordres des (c_j).

Conjugaison d'un cycle

On considère un cycle $c = (a_1 \dots a_k)$ de S_n, ainsi qu'une permutation quelconque σ. Cherchons à caractériser la permutation τ suivante:

$$\tau = \sigma(a_1 \dots a_k)\sigma^{-1}$$

Soit $x \in \{1, \dots, n\}$, alors on considère deux cas:

- Si $\sigma^{-1}(x)$ n'est pas dans le support de c.
- Si $\sigma^{-1}(x)$ est dans le support de c.

Le premier cas est trivial[1], examinons donc le second, on a tout d'abord que:

$$\exists i \in \{1, \dots, k\}\ ;\ \sigma^{-1}(x) = a_i \tag{2}$$

Or par définition d'un cycle on a que:

$$c\sigma^{-1}(x) = a_{i+1}$$

Et donc finalement:

$$\tau(x) = \sigma(a_{i+1})$$

Mais en reprenant l'équation obtenue en (2), on obtient aussi que:

$$x = \sigma(a_i)$$

Donc finalement on trouve que sur le support de τ est exactement l'image des (a_i) par σ et que la permutation effectuée correspond au cycle:

$$\tau = (\sigma(a_1) \dots \sigma(a_k))$$

Le conjugué d'un cycle est donc un cycle de même longueur. En outre si deux permutations sont conjuguées, alors elle sont de même type, en effet si:

$$\sigma' = \tau\sigma\tau^{-1}$$

[1] En effet si $c\sigma^{-1}(x) = \sigma^{-1}(x)$, alors on a directement que $\tau(x) = x$