Théorie des groupes

Bcp de monde . . .

September 2024

Table des matières

Exemples en tout genres

0.1 Section1

Définition :
distance mdr a definition d'une distance

0.1.1 Sous-section1

Preuve :

exemple de preuve

□

0.1.2 Comment faire un lemme

Lemme :
avec la box noire sans nom

Lemme : nom
sasn la box mais avec le nom

Chapitre 1

Notion de groupe, morphisme, produit direct

1.1 Groupes, sous-groupes, exemples

1.1.1 Définitions

Définition :
Groupe Un groupe est un ensemble non vide G munis d'une loi $*$ telle que :

(i) $*$ est associative
(ii) $*$ possède un neutre $e \in G$
(iii) Tout élément possède un inverse pour $*$

Définition : Groupe abélien
Un groupe G est dit abélien si : $\forall (x, y) \in G,\ xy = yx$

1.1.2 Sous-groupes

Définition : Sous-groupe
Un sous-ensemble H de G est appelé sous-groupe si :

- $e \in H$
- $\forall x, y \in H, xy^1 \in H$

Définition : Groupe fini
G est dit fini si il est cardinal fini, on note alors $o(G) = |G|$, appelé ordre de G.

1.1.3 Sous-groupe engendré

Définition : Sous-groupe engendré par une partie
Soient G un groupe et $S \subset G$
Soit G_S l'ensemble des sous groupes de G qui contiennent S.

On appelle sous groupe engendré par S l'ensemble : $\langle S \rangle := \bigcap_{H \in G_S} H$

Si de plus $\langle S \rangle = G$ on dit que S est une partie génératrice de G ou que S engendre G

Définition : Groupe de type fini
Si G est engendré par un singleton, on dit que G est monogène.
Un groupe monogène fini est dit cyclique.
Si il existe une partie finie $S \subseteq G$ qui engendre G, on dit que G est de type fini.

Définition : Ordre d'un élément

- Si $\langle x \rangle$ est infini, on dit que x est d'ordre infini.
- Si $\langle x \rangle$ est fini, on dit que x est d'ordre $|\langle x \rangle|$

Si $x^n = e$ alors $o(x)|n$

1.2 morphismes de groupes

Définition : Morphisme de groupe
Soit $(G, *), (H, \cdot)$ deux groupes. Un morphisme de groupes de G dans H est une application
$f : \quad G \quad \longrightarrow \quad H$ tel que $\forall x, y \in G, f(x * y) = f(x) \cdot f(y)$

Exercice :

1. $f(e_G) = e_H$
2. $f^{-1}(x) = f(x^{-1})$
3. $\forall n \in \mathbb{N}\ ,\ f^n(x) = f(x^n)$
4. Si $K < G$, alors $f(K) < H$
5. Si $K < H$, alors $f^{-1}(K) < G$

Exemple :

1. $\epsilon : \quad \mathbb{S}_n \quad \longrightarrow \quad \{-1, 1\}$
2. $det : \quad \mathbb{GL}_n(\mathbb{R}) \quad \longrightarrow \quad \mathbb{R}^*$
3. $exp : \quad \mathbb{C} \quad \longrightarrow \quad \mathbb{C}^*$
4. Mais $exp : \quad \mathcal{M}_2(\mathbb{R}) \quad \longrightarrow \quad (\mathbb{GL}_2(\mathbb{R}), \times)$

1.2.1 Isomorphismes

Définition : Isomorphisme

1. Un isomorphisme de G dans H est un morphisme de groupes bijectif.
2. G et H sont isomorphe ssi il existe un isomorphisme entre les deux.

Exercice :
Si f est un isomorphisme alors f^{-1} aussi

Exercice :

1. $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphe
2. $\mathbb{Z}/6\mathbb{Z}$ et $\mathbb{S}_n$ ne sont pas isomorphe (car l'un est abélien et l'autre non).
3. $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphe ssi $m \wedge n = 1$

Définition : Automorphisme
Un automorphisme est un isomorphisme d'un groupe G dans lui-même. L'ensemble des automorphismes de G se note $Aut(G)$.

Exercice :
Montrer que $Aut(G) < \mathbb{S}_G$, où $\mathbb{S}_G$ désigne l'ensemble des bijections de G dans lui même

Exercice :
$\forall g \in G$, on note $\sigma_g : \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array} \right.$ (automorphisme intérieur associé à g), montrer que $\sigma_g \in Aut(G)$

Exercice :
On note $Int(G)$ l'ensemble des automorphismes intérieurs de G, montrer que $Int(G) < Aut(G)$

Théorème : Théorème de Cayley
Tout groupe G est isomorphe à un sous-groupe de $\mathbb{S}_G$. En particulier, si $|G| = n$, alors G est isomorphe à un sous-groupe de $\mathbb{S}_n$.

Preuve :

Pour tout $g \in G$, on pose $\tau_g : \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gx \end{array} \right.$ τ_g est une bijection de G dans G. Notons $T_G := \{\tau_g, g \in G\} \subseteq \mathbb{S}_G$.

Vérifions que :

1. $T_G < \mathbb{S}_G$
2. G est isomorphe à T_G

Preuve de 1 :

- $Id_G = \tau_e \in T_G (T_G \neq \emptyset)$
- $\forall g_1, g_2 \in G, \forall x \in G, \tau_{g_1 g_2}(x) = g_1 g_2 x = g_1(g_2 x) = \tau_{g_1}(\tau_{g_2}(x))$, donc on a bien $\tau_{g_1 g_2} = \tau_{g_1}\tau_{g_2}$
- $\forall g \in G, \tau_{g^{-1}} \circ \tau_g = \tau_g \circ \tau_{g^{-1}} = Id_G$ Donc $(\tau_g)^{-1} = \tau_{g^{-1}} \in T_G$

Preuve de 2 :

Notons $\phi : \left| \begin{array}{ccc} G & \longrightarrow & T_G \\ g & \longmapsto & \tau_g \end{array} \right.$ Alors ϕ est un morphisme (d'après la preuve de 1) ϕ est immédiatement surjectif, mais il est également injectif :
Soit $g \in G$ tel que $\tau_g = Id_G$. Alors $\forall x \in G, gx = x$. Si on prend $x = e_G$, on obtient $g = e_G$. Donc $\ker(\phi) = e_G$, et donc ϕ est injectif.

$\square$

1.3 Produits directs

Définition : Produit direct
Le groupe "produit direct" de deux groupes G_1, G_2 est l'ensemble $G_1 \times G_2$ muni de la loi :
$$\cdot : \left| \begin{array}{ccc} (G_1 \times G_2) \times (G_1 \times G_2 & \longrightarrow & G_1 \times G_2 \\ ((x_1, x_2), (y_1, y_2)) & \longmapsto & (x_1 y_1, x_2 y_2) \end{array} \right.$$

Exercice :
vérifier que $G_1 \times G_2$ muni de cette loi est bien un groupe.

Définition : Projections et injections canoniques

1. Projections canoniques $p_i : \left| \begin{array}{ccc} G_1 \times G_2 & \longrightarrow & G_i \\ (x_1, x_2) & \longmapsto & x_i \end{array} \right.$.
2. Injections canoniques : $q_1 : \left| \begin{array}{ccc} G_1 & \longrightarrow & G_1 \times G_2 \\ x_1 & \longmapsto & (x_1, e_2) \end{array} \right.$ et $q_2 : \left| \begin{array}{ccc} G_2 & \longrightarrow & G_1 \times G_2 \\ x_2 & \longmapsto & (e_1, x_2) \end{array} \right.$

Remarque :

$\mathrm{Im}(q_i)$ est isomorphe à G_i. Ainsi $G1 \times G_2$ contient un sous-groupe isomorphe à G_1, de même pour G_2.

Remarque :

$\forall\ x = (x_1, x_2) \in G_1 \times G_2$, on a :

$x = (p_1(x), p_2(x)) = (x_1, x_2) = (x_1, e_2)(e_1, x_2) = (e_1, x_2)(x_1, e_2) = q_1(x_1)q_2(x_2) = q_2(x_2)q_2(x_1)$

Théorème :
Un groupe G est isomorphe au produit direct $G1 \times G_2$ ssi G contient deux sous-groupes H_1, H_2 tel que :

1. H_i est isomorphe à $G_i (i = 1, 2)$
2. $h_1 h_2 = h_2 h_1, \forall h_1 \in H_1, \forall h_2 \in H_2$
3. $G = H_1 H_2$
4. $H_1 \cap H_2 = \{e_G\}$

Preuve :

$\boxed{\Rightarrow}$ Supposons qu'il existe $\phi : \ G_1 \times G_2 \longrightarrow G$ isomorphe.

1. On a que $G_1 \simeq \{G_1, e_2\} \simeq \phi(\{G_1, e_2\}) := H_1$ il suffit alors de remarquer que H_1 est un sous groupe de G. On construit de même H_2
2. $\forall (h_1, h_2) \in H_1 \times H_2$, on note $h_1' = (h_1, e_2)$ idem pour h_2', on a alors :
$$h_1 h_2 = \phi(h_1' h_2') = \phi(h_2' h_1') = h_2 h_1$$
3. $\forall x \in G, \exists!\ x' = (h_1, h_2) \in G_1 \times G_2$ tel que $\phi(x') = x$. On a alors :
$$x = \phi(x') = \phi(h_1' h_2') = h_1 h_2$$
4. Immédiat

$\boxed{\Leftarrow}$ Construisons un isomorphisme de G dans $G_1 \times G_2$
Fait : $\forall g \in G, \exists! (h_1, h_2) \in H_1 \times H_2$ tel que $g = h_1 h_2$
En effet : l'existence vient de 3), l'unicité vient de 4) :$g = h_1 h_2 = k_1 k_2$ alors $(k_1)^{-1} h_1 = k_2 (h_2)^{-1}$.
Comme $H_1 \cap H_2 = \{e\}$ on obtient $(k_1)^{-1} h_1 = k_2 (h_2)^{-1} = e_G \Rightarrow h_1 = k_1$ et $h_2 = k_2$
Notons $\phi_1 : \ H_1 \longrightarrow G_1$ et $\phi_2 : \ H_2 \longrightarrow G_2$ les isomorphismes données par 1).
Posons $\phi : \left| \begin{array}{ccc} G & \longrightarrow & G_1 \times G_2 \\ h_1 h_2 & \longmapsto & (\phi_1(h_1), \phi_2(h_2)) \end{array} \right.$
Mq ϕ est un morphisme (α), injectif (β), surjectif γ
(α) : $\phi(h_1 h_2 h_1' h_2') = \phi(h_1 h_1' h_2 h_2') = (\phi_1(h_1 h_1'), \phi_2(h_2 h_2')) = (\phi_1(h_1), \phi_1(h_1'), \phi_2(h_2)\phi_2(h_2')) = (\phi_1(h_1), \phi_2(h_2))(\phi_1(h_1'), \phi_2(h_2')) = \phi(g)\phi(g')$
(β) : Soit $x = h_1 h_2$ tel que $\phi(x) = (\phi_1(h_1), \phi_2(h_2)) = (e_1, e_2)$
Alors $\phi_1(h_1) = e_1$ et $\phi_2(h_2) = e_2 \Rightarrow h_1 = h_2 = e_G$
(γ) : Soit $x = (x_1, x_2) \in G_1 \times G_2$, soit (h_1, h_2) tel que $\phi_i(h_i) = x_i$, alors $x = (\phi_1(h_1), \phi_2(h_2)) = \phi(h_1, h_2)$, cela montre la surjectivité de ϕ.

|

$\square$

Exemple :
$(\mathbb{Z}/2^\alpha\mathbb{Z},+,\times)$ est anneau. On note $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ l'ensemble des éléments inversibles de l'anneau (pour la loi $\times$). Si $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/2^{\alpha-2}\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

Chapitre 2

Classes modulo un sous-groupe, sous-groupes distingués

2.1 Classes à droite, classes à gauche

Soit $H < G$. On définit $x\mathcal{R}_H y \iff xy^{-1} \in H$ et $x\,{}_H\mathcal{R} y \iff x^{-1}y \in H$

Exemple :

1. $\mathcal{R}_H$ et ${}_H\mathcal{R}$ définissent deux relations d'équivalences
2. La classe d'équivalence de x pour $\mathcal{R}_H$ est Hx appelée classe à droite de x modulo H, idem pour ${}_H\mathcal{R}$

Exemple :
On se place dans $\mathcal{S}_3$, on pose $\sigma = (1,2,3)$ et $\tau = (1,2)$, on a alors $\mathbb{S}_3 = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \sigma\tau\}$.
Pour $H = \{e, \tau\}$, on a :
$H\sigma = \{\sigma, \tau\sigma\}, H\sigma^2 = \{\sigma^2, \tau\sigma^2(= \sigma\tau)\}$
$\sigma H = \{\sigma, \sigma\tau\}, \sigma^2 H = \{\sigma^2, \sigma^2\tau(= \tau\sigma)\}$
donc $\sigma H \neq H\sigma$.

Exemple :
Si G est abélien, on a $xH = Hx, \forall x \in G$.

Remarque :

$\forall g \in G$, $\tau_g : \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gx \end{array} \right.$ est une bijection. En particulier, $\tau_g|_H$ est une bijection de H sur gH. De même, $\rho_g : \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & xg \end{array} \right.$, alors $\rho_g|_H$ est une bijection de H sur Hg.

Remarque :

Soit $\{e\} \cup \{x_i, i \in I\}$ un système de représentants des classes à gauche modulo H. On a alors $G = H \sqcup \bigsqcup_{i \in I} x_i H$ (union disjointe).

Remarque :

L'application : $x_i H \longrightarrow H(x_i)^{-1}$ est une bijection de l'ensemble des classes à gauche sur l'ensemble des classes à droite.

Définition : Indice de H dans G
L'indice de H dans G est le cardinal (fini ou infini) de l'ensemble des classes à gauche (= cardinal de l'ensemble des classes à droite), il est noté $[G : H]$

On en déduit le théorème de Lagrange :

Théorème : Théorème de Lagrange
Soit G un groupe fini et $H < G$. Alors :

1. $|G| = |H|[G : H]$
2. $\forall x \in G, o(x) \mid |G|$

2.2 Sous-groupes distingués

Définition :
Soit G un groupe fini, $H < G$ est dit distingué (ou normal) dans G ssi $\forall x \in G, xH = Hx$.
Le cas échéant on note : $H \triangleleft G$

Définition :
Un groupe G est dit simple ssi ses seuls sous-groupes distingué sont $\{e\}$ et G.

Remarque :

Si G est abélien, tout $H < G$ est distingué.

Exemple :
Soit $H < G$. Alors $H \triangleleft G \iff \forall g \in G, gHg^{-1} = H$

Propriété :
Soit $H\backslash G$ l'ensemble des classes à gauche modulo H.
L'application : $(xH, yH) \longrightarrow xyH$ est bien définie ssi $H \triangleleft G$.
Idem pour les classes à droites G/H.

Preuve :

$\Rightarrow$: Soit $h \in H, y \in G$, l'application est bien définie, donc $egH = hgH$ donc $yH = hgH$ donc $H = y^{-1}hyH$, donc $y^{-1}hy \in H$.
$\Leftarrow$: Si $x, x' \in G$ tel que $xH = x'H$, et si $y, y' \in G$ tel que $yH = y'H$, alors on a $h, h' \in H$ vérifiant : $x' = xh$ et $y' = yh'$. Donc $x'y' = xyy^{-1}hyh'$, avec $y^{-1}hyh' \in H$ car $H \triangleleft G$. Donc $x'y'H \subseteq xyH$, par symétrie on a $\supseteq$

$\square$

Théorème : Groupe quotient
Soit G un groupe, $H \triangleleft G$. On note $\bar{x}$ la classe de x modulo H, $\frac{G}{H}$ l'ensemble des classes modulo H. Alors :

1. L'application $* : \left| \begin{array}{ccc} (\frac{G}{H}) \times (\frac{G}{H}) & \longrightarrow & \frac{G}{H} \\ (\bar{x}, \bar{y}) & \longmapsto & \bar{x} * \bar{y} := \bar{xy} \end{array} \right.$ munit $\frac{G}{H}$ d'une structure de groupe tel que $\bar{e} = H$ est l'élément neutre.
2. En particulier, l'application $\pi : \; G \longrightarrow \frac{G}{H}$ est un morphisme de groupes de noyau H.

2.2.1 Sous-groupes distinguées et noyaux

Propriété :
Si $\phi : G \longrightarrow G'$ un morphisme, alors $\ker(\phi) \triangleleft G$.

Preuve :

Si $h \in \ker(\phi), g \in G, \phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_{G'}$, donc $ghg^{-1} \in \ker(\phi)$.

$\square$

Théorème : Groupes distingués et morphismes
Soit G un groupe. Alors $H \triangleleft G$ ssi $\exists G'$ groupe, $\exists\ \phi : G \longrightarrow G'$ morphisme tel que $H = \ker(\phi)$

Exemple :

1. $\varepsilon : \mathbb{S}_n \longrightarrow -1, 1$ (*signature*), alors $A_n := \ker(\varepsilon) \triangleleft \mathbb{S}_n$
2. $det : \mathbb{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$, alors $\mathbb{SL}_n(\mathbb{R}) := \ker(det) \triangleleft \mathbb{GL}_n(\mathbb{R})$

Théorème : Premier théorème d'isomorphisme
Soit $\phi : G \longrightarrow G'$ un morphisme de groupe. Alors, $G/\ker(\phi)$ est isomorphe à $Im(\phi)$.

Chapitre 3

Étude de $\mathbb{Z}/n\mathbb{Z}$, de $\mathbb{S}_n$, de $\mathbb{D}_n$

3.1 J'ai pas le nom...

3.1.1 Autres exemples de sous groupes normaux

- j'ai pas le premier...
- Le centre d'un groupe $Z(G) = \{g \in G,\ gx = gx\ \forall x \in G\}$ est un sous groupe normal de G. (preuve en exercice (feuille 3)). $Z(G)$ est en fait caractéristique c'est à dire qu'il est invariant par tout automorphisme intérieur
- Le groupe dérivé de G est le sous-groupe (noté D(G)) qui est engendré par les commutateurs de G c'est à dire les éléments de la forme $[a, b] = aba^{-1}b^{-1}$ est aussi un sous-groupe normal.

Exemple :

1. Si G est abélien alors $Z(G) = G$
2. Si $n \leq 3$ alors $Z(S_n) = \{e\}$

Preuve :

Preuve du deuxième point :
Soit $\sigma \in \mathbb{S}_n$ avec $\sigma \neq e$.
Soit alors $i \in [\![1, n]\!]$ tel que l'on ait $\sigma(i) := j \neq i$
Soit enfin $k \in [\![1, n]\!] \setminus \{i, j\}$, on pose $\tau = (j, k)$.
On à bien $\sigma\tau \neq \tau\sigma$, car $\sigma\tau(i) = j \neq \tau\sigma(j) = k$

$\square$

Exercice :

- $D(G) \lhd G$ et $G/D(G)$ est abélien
- Soit $H \lhd$ alors G/H est abélien$\Leftrightarrow D(G) < H$
- D(G) est un sous groupe caractéristique de G
- $\forall n \leq 3 \quad D(S_n) = A_n$ ou A_n est le groupe alterné, désigne les permutations de signature paire

Définition : Normalisateur d'un sous-groupe
Soit $H < G$, on note$N_G(H) = \{g \in G,\ gH = Hg\}$, on l'appelle le normalisateur de H dans G

Exercice :
Mq $H \triangleleft N_g(H)$ et que $N_g(H) < G$

Exemple :
Dans A_4
Soit $H = \{e, (1,2), (3,4)\} < A_4$, $|H| = 2$.
O a $H < D(A_4)$ et $H \triangleleft D(A_4)$ car $\dfrac{|D(A_4)|}{|H|} = 2$.
Verifier que $N_{A_4}(H) = D(A_4)$:
Soit $N = N_{A_4}(H)$ pour simplifier. On sait que $D(A_4) < N$ donc $|D(A_4| = 4$ divise $|N|$ donc $|N| \in \{4, 8, 12\}$, mais vu $N < A_4$, $|N|$ divise 12, donc $|N| = 4$ où $|N| = 12$. Mais $N \neq A_4$ car $(1,2,3)H(1,2,3) \neq H$

3.2 Groupes Monogènes, cycliques, symétriques, diédraux

3.2.1 Groupes Monogènes

Définition : Groupe monogène
Un groupe G est dit *monogène* s'il est engendré par une unique élément

Théorème :
Soit G un groupe monogène alors :

- Ou bien G est isomorphe à $\mathbb{Z}$
- Ou bien G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$

Preuve :

Soit $G = \langle x \rangle$ et soit $\psi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & x^k \end{array} \right.$. ψ est un morphisme de groupe, il est surjectif.

Si il est injectif on à bien $G \simeq \mathbb{Z}$.

Sinon, il existe $n \in \mathbb{N}$ tq $\ker \psi = n\mathbb{Z}$

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\psi"] \arrow[d, "\pi"'] & G \\ \mathbb{Z}/n\mathbb{Z} \arrow[ur, "\tilde{\psi}"'] & \end{tikzcd}$$

Et d'après le premier théorème d'isomorphisme, il existe un isomorphisme de groupe $\tilde{\psi} : \mathbb{Z}/n\mathbb{Z} \longrightarrow Im(\psi) = G$ tel que le diagramme ci-dessus commute.

□

Propriété :
Tout groupe fini d'ordre p avec p premier est cyclique

Preuve :

Il suffit d'utiliser le théorème de Lagrange.

□

3.2.2 Sous-groupes d'un groupe monogène

Propriété :

1. Tout sous-groupe non trivial d'un groupe monogène infini est infini
2. Tout sous groupe d'un groupe cyclique est monogène et cyclique

Preuve :

1. Ici $G \simeq \mathbb{Z}$, donc tout $H < G$ est isomorphe à un sous-groupe de $\mathbb{Z}$ ie. un groupe de la forme $n\mathbb{Z}$ pour $n \neq 0$, donc H est infini
2. On reprend le diagramme :

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\psi"] \arrow[d, "\pi"'] & G \\
\mathbb{Z}/n\mathbb{Z} \arrow[ur, "\tilde{\psi}"'] &
\end{tikzcd}$$

Soit $K < G = \mathbb{Z}/n\mathbb{Z}$ on à $K = \pi(\pi^{-1}(K))$ car π est surjective. Comme $\pi^{-1}(K)$ est un sous groupe de $\mathbb{Z}$ il existe $k > 0$ tq $\pi^{-1}(K) = k\mathbb{Z}$.
Alors $K = \pi(k\mathbb{Z})$ est le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\pi(k)$, K est donc monogène et fini

$\square$

Remarque :

Si on reprend la preuve précédente on à $\pi^{-1}(0) = n\mathbb{Z} \subset \pi^{-1}(K) = k\mathbb{Z}$.
Ainsi, $n\mathbb{Z} \subset k\mathbb{Z}$ et donc $k|n$. Par conséquent, pour tout sous-groupe K de $\mathbb{Z}/n\mathbb{Z}$, il existe un diviseur k de n tel que $\pi(k)$ engendre K, l'ordre de $\pi(k)$ étant $\dfrac{n}{k}$, on a $|K| = \dfrac{n}{k}$ en particulier ce diviseur est unique on à donc le théorème suivant.

Théorème :
Soit $G = \langle x \rangle$ un groupe cyclique d'ordre n alors :
Pour tout diviseur d de n, il existe un unique sous groupe d'ordre d de G et ce sous groupe est engendré par $x^{n/d}$

Propriété :
Soit G un groupe non trivial alors :
G n'a pas de d'autres sous-groupes que G et $\{e\} \iff$ G est cyclique d'ordre p premier

Preuve :

$\boxed{\Leftarrow}$ évident par Lagrange

$\boxed{\Rightarrow}$ Soit$x \in G \setminus \{e\}$ alors $\langle x >= G$ par hypothèse. Si G était infini, il posséderait des sous-groupes non triviaux de type $n\mathbb{Z}$, donc G est fini. Comme il n'a pas d'autres sous-groupes que $\{e\}$ et G on a forcément $|G| = p$ premier par le théorème précédent.

$\square$

Théorème :
Soit G un groupe monogène : $G = \langle x \rangle$

1. Si G est infini, alors les seuls générateurs de G sont x et x^{-1}
2. Si G est fini (il est cyclique d'ordre n) alors l'ensemble de ses générateurs est donné par $\{x^k : k \in \mathbb{Z}, k \wedge n = 1\}$

Preuve :

1. Soit $\psi : k \in \mathbb{Z} \to x^k \in G$ (vue précédemment) qui est un isomorphisme de groupes. En particulier, ψ échange les générateurs. Comme les seuls générateurs de $\mathbb{Z}$ sont 1 et -1, on conclut.
2. Soit $k \in \mathbb{Z}$, alors :

$$\begin{aligned} G = \langle x \rangle &\iff \exists m \in \mathbb{Z}, x^{km} = x \\ &\iff \exists m \in \mathbb{Z}, n | km - 1 \\ &\iff \exists (m, q) \in \mathbb{Z}, km - nq = 1 \\ &\iff pgcd(k, n) = 1 \end{aligned}$$

□

Exercice :
L'ensemble des générateurs de $G \simeq \mathbb{Z}/n\mathbb{Z}$ est aussi égal à $\{\bar{k} \in \mathbb{Z}/n\mathbb{Z} : 0 \leq k \leq n-1, k \wedge n = 1\}$

Définition : Fonction d'Euler
La fonction d'Euler est la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ telle que :

— $\varphi(1) = 1$
— $\varphi(n) = |\{k \in \mathbb{N} : 1 \leq k \leq n, k \wedge n = 1\}|$

3.3 Anneau $\mathbb{Z}/n\mathbb{Z}$

On rappelle que les opérations d'addition et de multiplication sont bien définies sur $\mathbb{Z}/n\mathbb{Z}$ (pas de dépendance des représentants) et que cet anneau est unitaire.

Définition : Inverse modulo n
On dit que $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible s'il existe $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{k}\bar{m} = \bar{1}$

Propriété :
Soit $n \geq 2$. Les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont exactements les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$
L'ensemble des éléments inversibles est alors un groupe abélien fini d'ordre $\varphi(n)$.

Preuve :

Utiliser la caractérisation précédente avec Bézout.

□

3.4 Produits directs de groupes cycliques, calcul de $\varphi(n)$

On considère le morphisme d'anneaux unitaires :

$$f : k \in \mathbb{Z} \to (\bar{k}, \bar{\bar{k}}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Théorème :
Le morphisme d'anneaux unitaires f induit par passage au quotient par son noyau un isomorphisme d'anneaux unitaires $\bar{f} : \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ si et seulement si $m \wedge n = 1$

Preuve :

Il faut vérifier $\bar{f}$ est bijective ssi $m \wedge n = 1$:

$$\begin{aligned} f \text{ est surjective} &\iff |Im(f)| = mn \\ &\iff |\mathbb{Z}/\ker(f)| = mn \textit{ (grâce au théorème d'isomorphisme)} \\ &\iff \ker(f) = mn\mathbb{Z} \\ &\iff m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z} \\ &\iff m \wedge n = 1 \end{aligned}$$

□

Propriété :
Si $m \wedge n = 1$, alors $\varphi(nm) = \varphi(n)\varphi(m)$

Théorème :
Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, décomposé en facteur premiers. Alors :

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \times \cdots \times \left(1 - \frac{1}{p_k}\right)$$

Preuve :

Il nous suffit de calculer $\varphi(p^\alpha)$ pour p premier et $\alpha \geq 1$. On a :

$$\begin{aligned} \varphi(p^\alpha) &= |\{k \in \{1, \cdots, p^\alpha\} : k \wedge p^\alpha = 1\}| \\ &= |\{1, \cdots, p^\alpha\} \setminus \{p, 2p, \cdots, p^{\alpha-1}p\}| \\ &= p^\alpha - p^{\alpha-1} \end{aligned}$$

□

3.5 Structure des groupes abéliens finis (admis)

Référence : Livre de F. Ulmer "Théorie des groupes" chapitre 12

Soit G un groupe fini abélien d'ordre N. Il existe une décomposition unique $N = d_1 \cdots d_n$ avec $d_n \geq 2$ et $d_{i+1} | d_i$ telle que :

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$$

Exemple :
On peut lister, à isomorphisme près, tous les groupes abéliens d'ordre $72 = 3^2 \times 2^3$ avec les séquences suivantes : $(3^2 \times 2^2, 2), (3 \times 2, 3 \times 2, 2), (3 \times 2^3, 3), (2^2 \times 3, 2 \times 3), (3^2 \times 2, 2, 2)$

3.6 Groupes symétriques

On note $\mathbb{S}_n$ l'ensemble des permutations de $\{1, 2, ..., n\}$ que l'on munit de la loi de composition : c'est un groupe d'ordre $n!$

3.6.1 Support et Orbite

Définition : Support
Le support de $\sigma \in \mathbb{S}_n$ est l'ensemble $\{i \in \{1, ..., n\} \ ; \ \sigma(i) \neq i\}$

Exercice :
Soit $\sigma \in \mathbb{S}_n$. Montrer que

- σ et σ^{-1} ont le même support
- Deux permutations dont les supports sont disjoints commutent

Définition : Orbite
Soit $\sigma \in \mathbb{S}_n$. On définit la relation d'équivalence sur $\{1, ..., n\}$:

$$i\mathcal{R}j \iff \exists r \in \mathbb{Z} \mid \sigma^r(i) = j.$$

La classe de i est notée $\Omega(i) = \{\sigma^r(i), r \in \mathbb{Z}\}$ et est appelée σ-orbite de i.

3.6.2 Notion de cycle

Définition : r-cycle
$\sigma \in \mathbb{S}_n$ est un r-cycle si il existe $j_1, ..., j_r$ dans $\{1, ..., n\}$ tq $\sigma(j_1) = j_2, ..., \sigma(j_{r-1}) = j_r, \sigma(j_r) = j_1$, et si pour $k \notin \{j_1, ..., j_r\}, \sigma(k) = k$.
Alors le support de σ est $\{j_1, ..., j_r\}$. On notera $\sigma = (j_1, ..., j_r)$

Définition : Transposition et permutation circulaire

1. Un 2-cycle est appelé transposition
2. le n-cycle $(1, ..., n)$ est appelé permutation circulaire

Exemple :
Si $\sigma_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 5 & 4 \end{pmatrix} \begin{matrix} \leftarrow & i \\ \leftarrow & \sigma_0(i) \end{matrix}$
alors $\sigma_0 = (1, 3, 2)(4, 6)$.

Théorème :
Toute permutation $\sigma \in \mathbb{S}_n \setminus \{e\}$ se décompose sous la forme $\sigma = \gamma_1 \circ \gamma_2 \circ ... \circ \gamma_s$ où $s \in \mathbb{N}^*$, et où les γ_i sont des cycles différents de e dont les supports sont disjoints deux à deux. Cette décomposition est unique à l'ordre près des facteurs.

Exercice :

1. Montrer que l'ordre de σ est égal au ppcm des longueurs des cycles $\gamma_1, ..., \gamma_s$.
2. Calculer σ_0^{1000}.

3.6.3 Formules importantes

Propriété :
Pour tout $\tau \in \mathbb{S}_n$, $\tau(j_1, ..., j_r)\tau^{-1} = (\tau(j_1), ..., \tau(j_r))$.

Propriété :
On a : $(j_1, ..., j_r) = (j_1, j_2)(j_2, j_3)...(j_{r-1}, j_r)$

Cas particulier : $(a, b, c) = (a, b)(b, c)$

Applications de ces deux propriétés :

1. Deux r-cycles de $\mathbb{S}_n$ sont conjugués dans $\mathbb{S}_n$
2. $(1, i)(1, j)(1, i) = (1, i)(1, j)(1, i)^{-1} = (i, j)$
3. $\mathbb{S}_n$ est engendré par les transpositions du type $(j, j+1)$ où $j \in \{1, ..., n-1\}$
   preuve : laissée en exercice au lecteur, l'idée est de montrer que (i, j) est un produit de transpositions du type $(k, k+1)$ par récurrence sur $j-1$ en utilisant $(i, j) = (j-1, j)(i, j-1)(j-1, j)$
4. $\mathbb{S}_n$ est engendré par $(1, 2)$ et $\eta = (1, 2, ..., n)$
   preuve : $\eta^i(1, 2)\eta^{-i} = (i+1, i+2)$

3.6.4 Générateurs

Soit $n \geq 2$.

Théorème :

1. $\mathbb{S}_n$ est engendré par les transpositions
2. $\mathbb{S}_n$ est engendré par les transpositions du type $(1, j)$ où $j \in \{2, ..., n\}$

3.6.5 Centre

Théorème :
$Z(\mathbb{S}_n) = \{e\}$ pour $n = 1$ et $n \geq 3$.

3.6.6 Signature

Définition : Signature
Soit $\sigma \in \mathbb{S}_n$. On pose $\epsilon(\sigma) = (-1)^{n-t}$ où t est le nombre de σ-orbites différentes.

Exemple :

- $\sigma = e$: on a $\sigma(i) = i$ pour tout $i \in \{1, ..., n\}$, chaque point est une orbite donc $t = n$ et $\epsilon(\sigma) = 1$
- $\sigma = (1, 2)$: ici il y a $n-2$ éléments fixés qui donnent chacun une orbite, et $\{1, 2\}$ est une autre orbite donc $\epsilon(\sigma) = -1$.
- $\sigma = (1, ..., r)$: $\epsilon(\sigma) = (-1)^{r-1}$

Propriété :
Soit $\sigma \in \mathbb{S}_n$ où $n \geq 2$. Alors $\epsilon(\sigma \circ \tau) = (-1) \times \epsilon(\sigma)$ pour toute transposition $\tau \in \mathbb{S}_n$.
En particulier, si σ est un produit de k transpositions, on a $\epsilon(\sigma) = (-1)^k$.

Remarque :

Ainsi, la parité du nombre de transpositions nécessaires pour décomposer σ ne dépend que de σ.

Théorème :
Si $n \geq 2$, $\epsilon : \mathbb{S}_n \longrightarrow \{1, -1\}$ est un morphisme de groupes surjectif.

Preuve :

Soient $\sigma, \sigma' \in \mathbb{S}_n$. On décompose $\sigma = \tau_1 \circ ... \circ \tau_k$ et $\sigma' = \tau'_1 \circ ... \circ \tau'_{k'}$ en produits de transpositions. Alors $\epsilon(\sigma \circ \sigma') = (-1)^{k+k'} = \epsilon(\sigma) \times \epsilon(\sigma')$.

□

Définition : Groupe alterné
Soit $n \geq 2$. $\mathcal{A}_n$ est le noyau de ϵ, on le nomme groupe alterné.

Remarque :

C'est un sous groupe distingué de $\mathbb{S}_n$ d'indice 2, car le noyau d'un morphisme

Remarque :

Si τ est une transposition, $(\tau\mathcal{A}_n) \cap \mathcal{A}_n = \emptyset$, d'où $\mathbb{S}_n = (\tau\mathcal{A}_n) \sqcup \mathcal{A}_n$.

Théorème :

1. Si $n \geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles.
2. Si $n \geq 5$, deux 3-cycles sont conjugués dans $\mathcal{A}_n$
3. Si $n \geq 2$, alors $D(\mathbb{S}_n) = \mathcal{A}_n$, si $n \geq 5$ alors $D(\mathcal{A}_n) = \mathcal{A}_n$.

Preuve :

1. Soit $\sigma \in \mathcal{A}_n$, σ est un produit d'un nombre pair de transpositions, or $(i,j)(j,k) = (i,j,k)$ et $(i,j)(k,l) = (i,j,k)(j,k,l)$.
2. Soient $(i,j,k), (i',j',k')$ deux 3-cycles. Il existe $\sigma \in \mathbb{S}_n$ tel que $\sigma(i) = i', \sigma(j) = j', \sigma(k) = k'$. Alors $\sigma(i,j,k)\sigma^{-1} = (i',j',k')$. Sans perte de généralité, on peut supposer que $\sigma \in \mathcal{A}_n$, en effet $n \geq 5$, donc il existe une transposition $\tau = (r,s)$ avec $r, s \notin \{i,j,k\}$, et on peut remplacer σ par $\sigma\tau$.
3. $D(\mathcal{A}_n) \subset D(\mathbb{S}_n) \subset \mathcal{A}_n$ car si $a, b \in \mathbb{S}_n$, alors $\epsilon([a,b]) = 1$.
   Montrons que si $n \geq 5$, les 3-cycles, qui engendrent $\mathcal{A}_n$, sont des commutateurs (de $\mathcal{A}_n$).
   Soit $\sigma = (i,j,k)$ un 3-cycle. σ^2 est aussi un 3-cycle donc d'après 2. les deux sont conjugués : il existe $\eta \in \mathcal{A}_n$ tel que $\sigma^2 = \eta\sigma\eta^{-1}$ i.e. $\sigma = [\eta, \sigma]$.

□

Cas particuliers :

1. $D(\mathcal{A}_3) = \{e\}$
2. $D(\mathcal{A}_4) = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$

Preuve :

1. $\mathcal{A}_3 = \langle(1,2,3)\rangle$ donc $\mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$ est abélien
2. On note $V = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, c'est un sous groupe distingué de $\mathcal{A}_4$. Alors le groupe quotient $\mathcal{A}_4/V$ est d'ordre 3 donc isomorphe à $\mathbb{Z}/3\mathbb{Z}$ qui est abélien. Ainsi $D(\mathcal{A}_4)$ est un sous-groupe de V. Par le théorème de Lagrange, $D(\mathcal{A}_4)$ est de cardinal 1, 2, ou 4. $\mathcal{A}_4$ n'est pas abélien donc ce n'est pas 1. Si c'était 2, $D(\mathcal{A}_4)$ serait de la forme $\{e, (i,j)(k,l)\}$ qui n'est pas distingué.

□

Propriété :
Soit $\sigma \in \mathbb{S}_n$,avec $n \neq 2$ alors : $\epsilon(\sigma \circ \tau) = (-1)\epsilon(\sigma)$

Preuve :

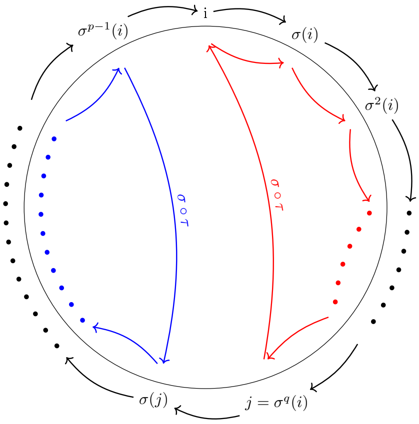
On veut étudier les orbites de $\sigma \circ \tau$. Seules les σ-orbites qui contiennent i ou j seront modifiées par τ. τ agit comme l'identité sur les autres orbites.

- Premier cas : i et j appartiennent a la même orbite O :

  $O = \{i, \sigma(i), \sigma^2(i), ..., \sigma^q(i) = j, \sigma^{q+1}(i), ..., \sigma^{p-1}$, ou $p = |O|$. Vérifions alors que $\sigma \circ \tau$ sépare O en deux $\sigma \circ \tau$-orbites :

  — L'orbite de i par $\sigma \circ \tau$ noté O_i vaut : $\boxed{O_i = \{i, \sigma \circ \tau(i) = \sigma(j) = \sigma^{q+1}(i), ..., \sigma^{p-1}(i)\}}$

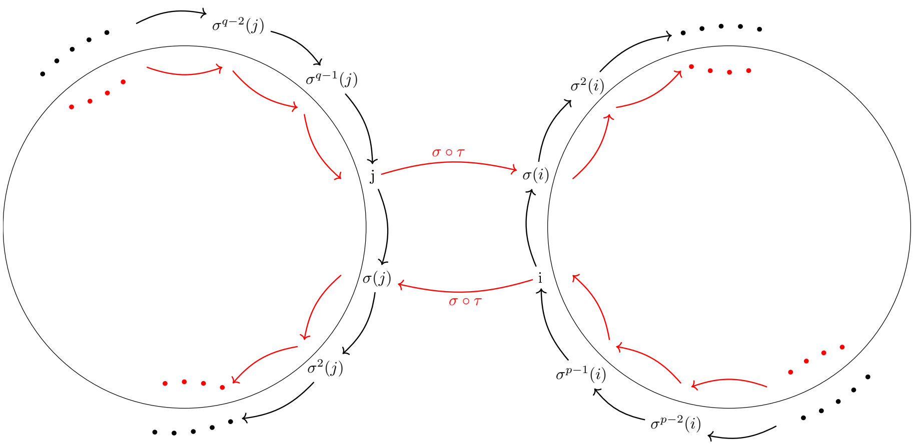
  — L'orbite de i par $\sigma \circ \tau$ noté O_j vaut : $\boxed{O_j = \{j, \sigma \circ \tau(j) = \sigma(i), \cdots, \sigma^{q-1}(i)\}}$



  On a bien montrer que $O_i \bigcap O_j = \emptyset$

- Deuxième cas, i et j sont dans deux orbites différentes :

  On note $O' = \{j, \sigma(j), \cdots, \sigma^{q-1}(j)\}$ l'orbite de j sous σ et $O = \{i, \sigma(i), \cdots, \sigma^{p-1}(i)\}$ l'orbite de i sous σ. A compléter...



□

3.7 Groupes Diédraux

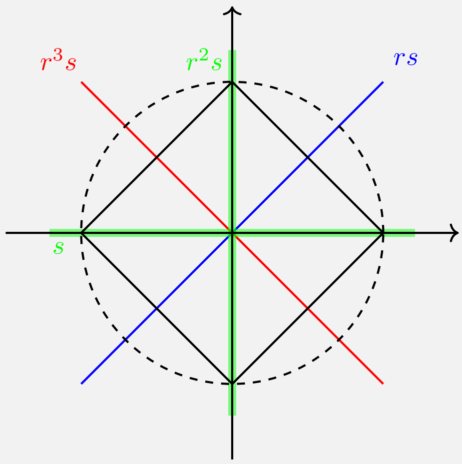
$\Omega = \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$ est la rotation d'angle $\dfrac{2\pi}{n}$. On note aussi $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ la symétrie d'axe (O_x)

Propriété :

1. $\Omega^n = e$ et $S^2 = e$
2. $S\Omega S = \Omega^{-1}$, et donc $S\Omega^{-1} = \Omega S$

Exemple :

- $n = 2$: $D_2 \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
- $n = 3$:
  On a $\Omega^{-1}S\Omega = S\Omega^2 = Sr^{-1} = rS$ et
  $r^{-2}sr^2 = r^{-2}r^{-2}s = r^2s$
  Et donc $D_3 \simeq \mathcal{S}_3$
- $n = 4$:



Théorème :
Soit $n \neq 2$, $D_n =< s, r >$ alors :

$$D_n = \{e, r, r^2, \cdots, r^{n-1}, s, rs, \cdots, r^{n-1}s\}$$

En particulier, $|D_n| = 2n$ et $< r >$ est distingué dans D_n

Preuve :

Les éléments $e, r, r^2, \cdots, r^{n-1}$ sont distincts deux à deux, de même que le sont $s, sr, sr^2, \cdots, sr^{n-1}$. Il reste alors qu'a remarquer que ces deux ensembles sont disjoints, par exemple au moyen d'un déterminant de matrice.

$\square$

Soit $g \in < r, s >$: c'est un mot en r, s, r^{-1},, en utilisant $sr = r^{-1}s$ on se ramène à un mot de "réduit" de la forme $e, r, r^2, \cdots, r^{n-1}$ ou $s, sr, sr^2, \cdots, sr^{n-1}$.

Remarque :

D_n est aussi engendré par r et rs, en effet $r = rs \cdots$

Exercice :
Soit G un groupe engendré par deux éléments a et b qui vérifient, $o(a) = n$, $o(b) = 2$ et $o(ab) = 2$ alors G est isomorphe à D_n

Preuve :

$ab = ba^{-1} \Rightarrow b \notin < a >$ et $G = \{e, a, a^2, \cdots, a^{n-1}, b, ba, \cdots, a^{n-1}b\}$ Par exemple J calais (Chapitre groupes diédraux)

□

Remarque :

En TD on identifiera la liste des sous groupes normaux de D_n

Exercice :

- Soit $n \neq 3$, alors $Z(D_n) = \{e, r^{n/2}\}$ si n est pair et e sinon.
- $D(D_1) = \{e\}$ et $D(D_2) = \{e\}$
- $\forall n \neq 3,\ D(D_n) = \langle r^2 \rangle$

Preuve :

— $[r^i, r^j] = e$
— $[r^i, r^j s] = r^i r^j s r^{-i} (r^j s)^{-1} = r^{i+j} s r^{-i} s r^{-j} = r^{2i}$
— $[r^i s, r^j s] = r^{i-j}$ On a bien $D(D_n) = \langle r^2 \rangle$

□

3.8 Classification des groupe d'ordre 8

3.8.1 Définition de Q_8

$Q_8 = \langle I, J \rangle$ où $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, et $I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

Propriété :

1. $o(I) = 4,\ J^2 = -I (\Leftarrow o(J) = 4$
2. $JI = I^{-1} J$

Propriété :
$Q_8 = \{e, I, I^2, I^3, J, IJ, I^2 J, I^3 J\}$

Preuve :

Similaire à celle faite pour D_n

□

Théorème :
Soit G un groupe non abélien d'ordre 8.
Si G possède un seul élément d'ordre 2 alors : $G \simeq Q_8$, sinon, $G \simeq D_4$

Preuve :

Tout les éléments de G ne peuvent être abéliens à la fois, car G est non abélien. Dès lors, il existe un élément i d'ordre 4 (8 étant exclu car $G \neq \mathbb{Z}/8\mathbb{Z}$ abélien). On note $H := \langle i \rangle$

Soit $j \in G$, $j \notin H$, on a $G = \{1, i, i^2, i^3\} \cup \{j, ji, ji^2, ji^3\} = H \cup jH$.

Comme $H \triangleleft G$ vu $[G : H] = 2$, on a $jij^{-1} \in H$

1. Si G possède un seul élément d'ordre 2, c'est $i^2 \in \langle i \rangle$. On a de plus $o(j) = o(ij) = o(i^2 j) = o(ij^3) = 4$, et $ji = i^{-1}j$, on vérifie alors que $G \simeq Q_8$
2. Si G possède au moins 2 éléments d'ordre 2 alors il existe dans $\{j, ji, ji^2, ji^3\}$ un élément d'ordre 2, notons le j_0, (par exemple$i^2 j$ fonctionne) Comme précédemment

□

Chapitre 4

Action de groupes

4.1 Définition et exemples

Définition : Action
Soit G un groupe et X un ensemble non vide. Une opération de G sur un ensemble X est une application $G \times X \longrightarrow X,\ (g, x) \mapsto g \cdot x$ qui vérifie

— $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x,\ \forall g_1, g_2 \in G,\ \forall x \in G$
— $e \cdot x = x,\ \forall x \in X$

Remarque :

On a défini ici une action de G à gauche. On peut définir une action de G à droite en demandant cette fois ci : $(x \cdot g_1) \cdot g_2 = x \cdot (g_1 g_2)$

Propriété :

— $\forall g \in G$, l'application $\gamma_g : X \longrightarrow X,\ x \mapsto g \cdot x$ est une bijection (d'inverse $\gamma_{g^{-1}}$)
— L'application $G \longrightarrow \mathrm{Bij}(X),\ x \mapsto \gamma_x$ est un morphisme de groupes. Réciproquement, tout morphisme de groupes $\lambda : G \longrightarrow \mathrm{Bij}(X)$ définit une action de G sur X en posant $g \cdot x = (\lambda(g))(x)$.

Remarque :

On étudira le cas particulier où $X = G$, il s'agit d'un cas très intéressant. On peut avoir $G \longrightarrow \mathrm{Bij}(G)$ et même des exercices où $G \longrightarrow \mathrm{Aut}(G)$.

Exemple :

1) G opère sur G par translation à gauche $G \times G,\ (g, x) \longrightarrow g \cdot x = gx$.
2) G opère sur G par conjugaison $G \times G \longrightarrow G,\ (g, x) \mapsto g \cdot x = gxg^{-1}$. Ici, l'application $G \longrightarrow G,\ x \mapsto gxg^{-1}$ est un automorphisme de G. Donc on a ici $G \longrightarrow \mathrm{Aut}(G)$.

Définition : automorphisme intérieur
L'application $i_g : G \longrightarrow G,\ x \mapsto gxg^{-1}$ s'appelle l'automorphisme intérieur associé à g.

Exercice. L'ensemble $\mathrm{Int}(G)$ des automorphismes intérieurs de G forme un sous-groupe de $\mathrm{Aut})(G)$.

Lemme. $\mathrm{Int}(G) \simeq G/Z(G)$

Preuve :

On considère le morphisme

$$\varphi : \left| \begin{array}{ccc} G & \longrightarrow & \mathrm{Int}(G) \\ g & \longmapsto & i_g \end{array} \right.$$

— L'application φ est évidemment surjective.

—

$$\begin{aligned} g \in \ker(\varphi) &\iff i_g = \mathrm{Id}_G \\ &\iff \forall x \in G,\ i_g(x) = gxg^{-1} = x \\ &\iff \forall x \in G,\ gx = xg \\ &\iff g \in Z(G). \end{aligned}$$

On conclut en appliquant le 1er théorème d'isomorphisme.

□

Exemple :
(Suite des exemples)

3) Soit $H < G$ (pas forcément distingué). Soit l'application

$$f : \left| \begin{array}{ccc} G \times (G/H)_{\text{gauche}} & \longrightarrow & (G/H)_{\text{gauche}} \\ (g, xH) & \longmapsto & (gx)H \end{array} \right.$$

Cette application est bien définie. En effet, si $gH = xH$ alors $y = xh$ où $k \in H$, et ensuite $g(yH) = g(xhH) = g(xH) = (gx)H$.

4) $G := \mathrm{SL}_2(\mathbb{R})$ agit sur $\mathbb{H} := \{z \in \mathbb{C},\ \mathrm{Im}(z) > 0\}$ via

$$f : \left| \begin{array}{ccc} G \times \mathbb{H} & \longrightarrow & \mathbb{H} \\ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) & \longmapsto & \frac{az+b}{cz+d} \end{array} \right.$$

5) $O_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}),\ M^\top M = I_n\}$ agit sur $\mathbb{S}^n := \{(x_1, \cdots, x_n) \in \mathbb{R}^n,\ x_1^2 + \cdots + x_n^2 = 1\}$ via

$$g : \left| \begin{array}{ccc} \mathrm{GL}_n(\mathbb{R}) \times \mathbb{S}^n & \longrightarrow & \mathbb{S}^n \\ (M, x) & \longmapsto & Mx \end{array} \right.$$

6) D_n (groupe diédral) agit sur l'ensemble des sommets du polygôle régulier à n côtés.

7) $\mathrm{GL}_n(\mathbb{R})$ agit sur l'ensemble des matrices symétriques $S_n(\mathbb{R})$ via

$$h : \left| \begin{array}{ccc} \mathrm{GL}_n(\mathbb{R}) \times S_n(\mathbb{R}) & \longrightarrow & \mathbb{S}^n \\ (g, x) & \longmapsto & g^\top xg \end{array} \right.$$

4.2 Stabilisateur, orbite

Définition : stabilisateur
Soit $x \in X$. Le stabilisateur de x dans G est

$$\mathrm{Stab}_G(x) := \{g \in G,\ g \cdot x = x\}.$$

Exercice. $\mathrm{Stab}_G(x) < G$.

Maintenant, introduisons la relation sur X suivante :

$$x\mathcal{R}y \iff \exists g \in G,\ y = g \cdot x.$$

Exercice. $\mathcal{R}$ est une relation d'équivalence.

Définition :
Soit $x \in X$. $\mathrm{Orb}_G(x)$ est la classe d'équivalence de x par la relation $\mathcal{R}$. Autrement dit :

$$\mathrm{Orb}_G(x) = \{g \cdot x,\ g \in G\}$$

Retour sur les 7 exemples.

1) $\mathrm{Stab}_G(x) = \{x\}n\ \mathrm{Orb}_G(x) = G$.
2) $\mathrm{Stab}_G(x) = \{g \in G,\ gxg^{-1} = x\} = \{g \in G,\ gx = xg\}$, appelé le "centraliseur" de x, noté $C_G(x)$.

$$\mathrm{Orb}_G(x) := \{gxg^{-1},\ g \in G\}$$

est la "classe de conjugaison" de x.

3)

$$f : \left| \begin{array}{ccc} G \times (G/H)_{\text{gauche}} & \longrightarrow & (G/H)_{\text{gauche}} \\ (g, xH) & \longmapsto & (gx)H \end{array} \right.$$

$$\mathrm{Stab}_G(xH) = xHx^{-1}$$

$$\mathrm{Orb}_G(xH) := (G/H)_{\text{gauche}}$$

4)

$$f : \left| \begin{array}{ccc} \mathrm{SL}_2(\mathbb{R}) \times \mathbb{H} & \longrightarrow & \mathbb{H} \\ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) & \longmapsto & \frac{az+b}{cz+d} \end{array} \right.$$

$$\mathrm{Stab}_G(i) = \left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix},\ a^2 + b^2 = 1\right\} \simeq \mathrm{SO}_n(\mathbb{R}) = \left\{\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix},\ \theta \in \mathbb{R}\right\}$$

$$\mathrm{Orb}_G(i) := \mathbb{H}.$$

6)
7)

$$h : \left| \begin{array}{ccc} \mathrm{GL}_n(\mathbb{R}) \times S_n(\mathbb{R}) & \longrightarrow & \mathbb{S}^n \\ (g, M) & \longmapsto & g^\top M g \end{array} \right.$$

$$\mathrm{Stab}_G(M) = \{\text{groupes des isométries par la forme quadratique induite par } M\}$$

$$\mathrm{Orb}_G(xH) := \{M^\top \in S_n(\mathbb{R}),\ \text{signature}(M) = \text{signature}(M')\}$$

Fait important : Si $y \in \mathrm{Orb}_G(x)$ alors on peut relier $\mathrm{Stab}_G(x)$ et $\mathrm{Orb}_G(y)$. On a

$$\mathrm{Stab}_G(x) = g\mathrm{Stab}_G(x)g^{-1}.$$

Autre propriété importante :

Théorème :
Soit $x \in X$. L'application

$$V : \left| \begin{array}{ccc} (G/\mathrm{Stab}_G(x))_{\text{gauche}} & \longrightarrow & \mathrm{Orb}_G(x) \\ g\mathrm{Stab}_G(x) & \longmapsto & g \cdot x \end{array} \right.$$

est bien définie et c'est une bijection. Attention, V n'est pas un morphisme de groupes.

Preuve :

Soit $S := \mathrm{Stab}_G(x)$. Soit $(g, g') \in G^2$ tel que $g'S = Sg$. Alors $g' = gS$ où $s \in S$. Ainsi, $g' \cdot x = (gS) \cdot x = g \cdot (x \cdot s) = g \cdot x$.

V est surjective par définition.

V est injective : : Soit $(g, g') \in G^2$ tel que $g \cdot x = g' \cdot x$. On a $(g')^{-1} \cdot (g \cdot x) = x$. Or $(g')^{-1} \cdot (g \cdot x) = ((g')^{-1}g) \cdot x$, donc $(g')^{-1}g \in S$, donc $g \in g'S$, donc $gS = g'S$.

$\square$

Corollaire :
Si G est un groupe fini

1) $\forall x \in X,\ |\mathrm{Orb}_G(x)| = \frac{|G|}{|\mathrm{Stab}_G(x)|} = [G : \mathrm{Stab}_G(x)]$.
2) Si X est fini et si $\{x_1, \cdots, x_r\}$ est un ensemble de représentants des orbites par la relation $\mathcal{R}$, alors
$$|X| = \sum_{i=1}^{r} |\mathrm{Orb}_G(x_i)| = \sum_{i=1}^{r} \frac{|G|}{|\mathrm{Stab}_G(x_i)|}.$$

4.3 Action d'un groupe G sur lui même par conjugaison

On rappel que l'action de G par conjugaison sur lui même est défini par :

$$\varphi : \left| \begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & gxg^{-1} \end{array} \right.$$

On défini alors :

— $\mathrm{Orb}_G(x) = \{gxg^{-1},\ g \in G\}$ appelé classe de conjugaison.
— $C_G(x) := \mathrm{Stab}_G(x) = \{g \in G, gxg^{-1} = x\}$ appelé centralisateur de x

Remarque :

$\mathrm{Orb}(e) = \{e\}$ ainsi $\{e\}$ est toujours une classe de conjugaison de cardinal 1.

Lemme :
Soit $x \in G$, $|\mathrm{Orb}_G(x)| = 1 \iff x \in Z(G)$

Dans ce contexte l'équation aux classes devient :

$$\begin{aligned} |G| &= \sum_{i=1}^{r} |\mathrm{Orb}_G(x_i)| \\ &= |Z(G)| + \sum_{\substack{i=1 \\ |\mathrm{Orb}_G(x_i)| \geq 2}}^{r} |\mathrm{Orb}_G(x_i)| \end{aligned}$$

Corollaire :
Soit G un groupe fini d'ordre p^α ou p est un nombre premier et $\alpha >= 1$. $Z(G)$ n'est pas réduit à $\{e\}$

Preuve :

Déjà remarquons que$|Z(G)| = \sum_{ß=1|\mathrm{Orb}_G(x_i)|>=2}^{r} -|\mathrm{Orb}_G(x_i)|$. Ensuite il suffit de monter que que si $|\mathrm{Orb}_G(x_i)| >= 2$ alors $p| \ \ |\mathrm{Orb}_G(x_i)|$

□

Corollaire :
Tout groupe d'ordre p^2 est abélien

Preuve :

Nous l'avons monter dans le TD n°3, ex 3. Dans l'idée : si $|Z(G)| = p^2$, on a finit. Si $|Z(G)| = p$ on obtient une contradiction en remarquant que $G/Z(G)$ est d'ordre p donc monogène et que donc G est abélien

$\square$

On peut donc monter grâce à ce corollaire et le théorème de structure des groupes abélien fini que :

- Pour $p = 2$, tout groupe G d'ordre 4 on à soit $G \simeq \mathbb{Z}/4\mathbb{Z}$ soit, $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
- Pour $p = 3$, tout groupe G d'ordre 9 on à soi $G \simeq \mathbb{Z}/9\mathbb{Z}$ soit $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Théorème :
Si H est un sous groupe de G on à :
En posant $I(H) = \{i \in [\![1, r]\!] \mid \mathrm{Orb}_G(x_i) \cap H \neq \emptyset\}$

$$H \triangleleft G \Longleftrightarrow H = \bigcup_{\substack{i=1 \\ i \in I(H)}}^{r} \mathrm{Orb}_G(x_i)$$

Autrement dit :

$$H \triangleleft H \Longleftrightarrow H \text{est une union (disjointe) de classe de conjugaisons}$$

Preuve :

$\boxed{\Leftarrow}$

Il suffit de remarquer que les classes de conjugaison sont stables par conjugaison.

$\boxed{\Rightarrow}$

Commençons par écrire $H = \bigcup_{i=1}^{r} \mathrm{Orb}_G(x_i) \cap H$, ce qui découle immédiatement du fait que les orbites forment une partition de G. Il suffit alors de montrer que pour tout $i \in I(H)$ on à $\mathrm{Orb}_G(x_i) \subset H$.

Soit donc $i \in I(H)$ et $y \in \mathrm{Orb}_G(x_i)$:

Par définition de $I(H)$ il existe $x \in H \cap \mathrm{Orb}_G(x_i)$. Et, x parcours tout $\mathrm{Orb}_G(x_i)$ sous l'action de notre action de groupe (conjugaison). IL suffit alors de se rappeler que H est normal et l'on obtient bien $\mathrm{Orb}_G(x_i) \subset H$.

$\square$

4.4 Actions transitives, actions fidèles

Définition :
Soit G un groupe qui agit sur X. On dit que l'action de G sur X est transitive si :

$$\forall x \in X, \forall y \in X, \exists g \in G, y = g \cdot x$$

Autrement dit, il n'y a qu'une seule orbite. On dit alors que X est G-homogène.

Exemple :
1) G opère sur lui-même par translation transitivement. En effet, $\forall x, y \in G, y = (yx\hat{}-1) \cdot x$
2) Si G opère sur lui-même par conjugaison, on a l'équivalence : l'action est transtive $\Leftrightarrow$ G est le groupe trivial (en effet, $\mathrm{Orb}_G(1) = 1$) 3) L'action $\begin{cases} G \times (G/H)_g \to (G/H)_g \\ (g, xH) \mapsto gxH \end{cases}$ est transitive.
4)On considère l'action : $\begin{cases} \mathrm{SL}_2(\mathbb{R}) \times \mathbb{H} \to \mathbb{H}(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z) \mapsto \frac{az+b}{cz+d} \end{cases}$ Nous allons montrer qu'elle est transitive. Il suffit pour cela de montrer que $\mathrm{Orb}_{\mathrm{SL}_2(\mathbb{R})}(i) = \mathbb{H}$. Soit $z \in \mathbb{H}$. On écrit $z = x + iy$ où $y > 0, x \in \mathbb{R}$. On relie d'abord z à y par la translation $g' = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$. On relie ensuite y à i par une homothétie bien choisie. Pour que celle-ci soit dans $\mathrm{SL}_2(\mathbb{R})$, on ajuste les coefficients diagonaux de la manière suivante : $g'' = \begin{pmatrix} 1/\sqrt{y} & 0 \\ 0 & \sqrt{y} \end{pmatrix}$ Enfin, en composant ces deux opérations, on obtient que pour $g = g''g' \in \mathrm{SL}_2(\mathbb{R})$, $g \cdot z = i$.
5) L'action de $\mathrm{O}_n(\mathbb{R})$ sur $S\hat{}n-1$ est transitive. 6) Le groupe diédral d'ordre $2n$ D_n agit transitivement sur les sommets du polygône régulier à n côtés.

Définition :
Soit G un groupe agissant sur X. On dit que l'action de G sur X est fidèle si le morphisme correspondant :

$$\gamma : \begin{cases} G \to \mathcal{S}_X g \mapsto (x \mapsto g \cdot x) \end{cases}$$

est injectif.

Rq : Il revient au même de demander : $\forall g \in G, (\forall x \in X, g \cdot x = x \Rightarrow g = 1$

Exemple :
1) L'action de translation à gauche d'un groupe sur lui-même est fidèle. En effet, si $g \in \ker\gamma$, alors $\forall x \in G, g \cdot x = x$ donc $g = g \cdot e = e$.
2) L'action par conjugaison fournit le noyau d'action : $\ker\gamma = \mathrm{Z}(G)$
3) $\mathrm{SL}_2(\mathbb{R})$ n'agit pas fidèlement sur $\mathbb{H}$. En effet, si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, alors :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \ker\gamma \Leftrightarrow \forall z \in \mathbb{H}, \frac{az+b}{cz+d} = z \Leftrightarrow \forall z \in \mathbb{H}, cz\hat{}2 + (d-a)z - b = 0 \Leftrightarrow \begin{cases} c = b = 0 \\ a = d = \pm 1 \end{cases}$$

Rq : On peut toujours se ramener à une action fidèle quitte à quotienter G par le noyau de l'action.

Chapitre 5

Produit semi-direct

5.0.1 Produit semi-direct interne

Rappel : G_1, G_2 deux groupes. $G_1 \times G_2$ est un groupe pour la loi $(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2')$

Théorème :
Un groupe G est isomorphe au produit direct $G_1 \times G_2$ si et seulement si on peut trouver H_1, H_2 deux sous-groupes de G vérifiant :

$$-H_i estisomorphe G_i - H_1, H_2 commutent - H_1 H_2 = G - H_1 \cap H_2 \text{est trivial}$$

Application (TD) : $(\mathbb{Z}/2\hat{}\alpha\mathbb{Z})\hat{}* \simeq \mathbb{Z}/2\hat{}\alpha - 2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Définition : produit semi-direct interne
Soit G un groupe et N, H deux sous-groupes de G. On dit que G est produit semi-direct interne de N par H si :

1. $N \lhd G$
2. $G = NH$
3. $N \cap H$est trivial

Exemple :
Dans S_n, pour $N = \mathcal{A}_n, H = \{\mathrm{Id}, \tau\}$ où τ est une transposition quelconque, on voit directement (cf chapitre sur le groupe symétrique) que S_n est p.s.d.i de N par H.

Remarque :

On dit alors que H est un complément de N dans G. (il n'est en général pas unique : c'est l'analogue des supplémentaires en algèbre linéaire)

Par ailleurs, un sous-groupe distingué N n'admet pas nécessairement de complément.

Remarque :

Supposons $i), ii)$ et $iii)$ vérifiés pour N, H et G. Soient $n_1 h_1, n_2 h_2 \in G$. Alors :

$$n_1 h_1 n_2 h_2 = \underbrace{n_1 h_1 n_2 h_1\hat{}-1}\in N \underbrace{h_1 h_2}\in H$$

C'est la décomposition "NH" du produit $n_1 h_1 n_2 h_2$. Cela implique qu'on introduit une nouvelle opération dans G, donnée par :

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 h_1 n_2 h_1\hat{}-1, h_1 h_2)$$

Ainsi, $N \times H$ muni de la loi $(x_1, h_1) \cdot (x_2, y_2) := (x_1 h_1 x_2 h_1^{-1}, h_1 h_2)$ est isomorphe à $(G, \cdot)$

Cela montre que G est iso au produit semi-direct externe de N par H (N et H n'étant maintenant plus unis comme sous-groupe de G, mais comme groupe "abstraits") où :

$$\phi : \left| \begin{array}{ccc} H & \longrightarrow & \mathrm{Aut}(N) \\ h & \longmapsto & \phi_h : \left| \begin{array}{ccc} N & \longrightarrow & N \\ x & \longmapsto & hxh^{-1} \end{array} \right. \end{array} \right.$$

Exemple :
[Groupe diédral] $D_n = \{\underbrace{\mathrm{Id}, r, \ldots, r\hat{\ } n_1}\, rotations, \underbrace{s, \ldots, sr\hat{\ } n_1}\, symtries\}$ On note N le sous-groupe normal engendré par r, et on pose $H = \{\mathrm{Id}, s\}$. Alors D_n est p.s.d.i de N par H.

IL faut insert ce qui manque ici

5.0.2 Produit semi-direct externe

Soient N, H deux groupes et $\phi : H \to \mathrm{Aut}(N)$ un morphisme. L'action correspondante à ϕ est :

$$\begin{cases} H \times N \to N \\ (h, x) \mapsto \phi(h)(x) = \phi_h(x) \end{cases}$$

Propriété :
L'ensemble $N \times H$ munit de la loi $(x, h) \cdot_\phi (y, k) = (x\phi_h(y), hk)$ est un groupe, appelé le produit semi-direct externe de N par H relativement à ϕ. On le note $N \rtimes_\phi H$.

Preuve :

Il faut vérifier l'associativité, l'existence d'un élèment neutre (qui se trouve être $(1_N, 1_H)$ et l'existence d'un inverse pour chaque élèment : $(x, h)\hat{\ }{-1} = (\phi_{h\hat{\ }-1}(x\hat{\ }{-1}), h\hat{\ }{-1})$

□

Propriété :
Soit $G = N \rtimes_\phi H$ le produit semi-direct externe de N par H, relatif à $\phi : H \to \mathrm{Aut}(N)$. On note $*_\phi$ la loi de groupe.
On pose deux applications :

$$I_N : \left| \begin{array}{ccc} N & \longrightarrow & G \\ x & \longmapsto & (x, e_H) \end{array} \right. \quad \text{et} \quad I_H : \left| \begin{array}{ccc} H & \longrightarrow & G \\ h & \longmapsto & (e_N, h) \end{array} \right.$$

$N' = \mathrm{Im}(I_N)$ est un sous-groupe de G isomorphe à N, et $H' = \mathrm{Im}(I_H)$ est un sous-groupe de G iso à H.
Alors G est produit semi-direct interne de N' par H' et on à :
$I_N(\phi_h(x)) = I_H(h) * \phi I_N(x) *_\phi (I_H(h))^{-1}$

Remarque :

Si on note avec les images de I_N et I_H (les réalisations N' de N dans G, et H' de H dans G)

$(\phi_h(x))' = h' *_\phi x' *_\phi (h')^{-1}$

Ainsi, l'action du morphisme ϕ est celle de la conjugaison quitte à employer la loi $*_\phi$ pour le groupe $G = N \times H$.

Preuve :

On veut montrer que G est p.s.d.i. de N' par H'. Il nous faut donc vérifier trois points :

1. $N' \lhd G$
2. $G = N'H'$
3. $N' \cap H' = \{e\}$

$N' = \{(x, e_H), x \in N\}$ et $H' = \{(e_N, h), h \in H\}$, on a donc : $N' \cap H' = \{e_G\}$

Soit $(x, h) \in G$

Alors $(x, h) = (x, e_H) *_\phi (e_N, h)$ (exercice)

Soit $(x, e_H) \in N'$ et soit $(y, k) \in G$
$(y, k) *_\phi (x, e_H) *_\phi (y, k)^{-1} =$

$(y, k) *_\phi (x, e_H) *_\phi (\phi_{k^{-1}}(y^{-1}, k^{-1}) =$

$(y, k) *_\phi (x\phi_{e_H}(\phi_{k^{-1}}(y^{-1}), k^{-1}) =$

$(y, k) *_\phi (x\phi_{k^{-1}}(y^{-1}), k^{-1}) =$

$(y\phi_k(x\phi_{k^{-1}}(y^{-1})), kk^{-1}) =$

$(y\phi_k(x)\phi_k(\phi_{k^{-1}}(y^{-1})), e_H) =$

$(y\phi_k(x)y^{-1}, e_H) \in N'$

On note $x' := (x, e_H) \in N'$
$h' := (e_N, h) \in H'$
On a : $x' *_\phi h' = (x, h) \in G$ (exercice !)

$x'_1 *_\phi h'_1 *_\phi x'_2 *_\phi h'_2 = (x_1, h_1) *_\phi (x_2, h_2) = (x_1\phi_{h_1}(x_2), h_1h_2) = (x_1\phi_{h_1}(x_2))' *_\phi (h_1h_2)'$

On obtient deux décompositions "N, H", on identifie les coordonnées :

$$\begin{cases} x'_1 *_\phi h'_1 *_\phi x'_2 *_\phi (h'_1)^{-1} = (x_1 *_N \phi_{h_1}(x_2))' \\ h'_1 *_\phi h'_2 = (h_1 *_H h_2)' \end{cases}$$

En faisant $x_1 = e_N$, on obtient avec la première ligne : $h'_1 *_\phi x'_2 *_\phi (h'_1)^{-1} = (\phi_{h_1}(x_2))'$

$\square$

On reviendra sur la notion de p.s.d après la preuve du théorème de Sylow. En effet, on montrera le théorème suivant : classification des groupes d'ordre pq où p et q sont premiers,
ou bien $p \nmid q - 1$, dans ce cas $G \simeq \mathbb{Z}/pq\mathbb{Z}$,
ou bien p divise $q - 1$, dans ce cas $G \simeq \mathbb{Z}/pq\mathbb{Z}$ ou $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Chapitre 6

Théorèmes de Sylow

Définition :
Soit G un groupe d'ordre $p^\alpha m$ où p est premier, $\alpha \geq 1, m \in \mathbb{N}^*, \text{pgcd}(p,m) = 1$.
Un p-Sylow de G est un sous-groupe d'ordre p^α.

Théorème :

1. G possède au moins un p-Sylow
2. Si H p-sous-groupe de G (il existe $\beta \in \{1, ..., \alpha\}$ tel que $|H| = p^\beta$), alors il existe un p-Sylow S (de G) tel que $H \subseteq S$
3. Les p-Sylow sont conjugués : si S_1, S_2 sont deux p-Sylow, il existe $g \in G, S_2 = gS_1g^{-1}$.
4. Soit s_p le nombre de p-Sylow. On a : $s_p \mid n$ où $(n = |G|)$
5. $s_p = 1 \bmod p$, en particulier (d'après 4), on a $s_p \mid m$.

6.1 Démonstration du point 1 :

Direction artistique :

i) Soit $|G| = p^\alpha m =: n$ Alors G se plonge dans $GL_n(\mathbb{Z}/p\mathbb{Z})$

ii) Posons $K = GL_n(\mathbb{Z}/p\mathbb{Z})$. Alors K possède un p-Sylow Σ, $|K| = p^\gamma l$, où $\text{pgcd}(p,l) = 1$

iii) Lemme : Soit K un groupe tel que, $|K| = p^\gamma l$, $\text{pgcd}(p,l) = 1$.

Soit G' sous-groupe de K et soit Σ un p-Sylow de K. Alors il existe $k \in K$ tel que $k\Sigma k^{-1} \cap G'$ est un p-Sylow de G'.

G se plonge dans $GL_n(\mathbb{Z}/p\mathbb{Z})$

G se plonge dans $\mathbb{S}_n$ par le plongement de Caley. On considère ensuite :

$$\phi : \left| \begin{array}{ccc} \mathbb{S}_n & \longrightarrow & GL_n(\mathbb{Z}/p\mathbb{Z}) \\ \sigma & \longmapsto & u_\sigma \end{array} \right. \quad \text{où } u_\sigma \text{ désigne l'application : } u_\sigma = \left\{ \begin{array}{l} (\mathbb{Z}/p\mathbb{Z})^n \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n \\ u_\sigma(e_i) = e_{\sigma(i)} \end{array} \right.$$

Quand $(e_1, ...e_n)$ est la base canonique de $(\mathbb{Z}/p\mathbb{Z})^n$ et u_σ un application linéaire.

Il suffit alors de montrer que ϕ est un morphisme injectif (exercice laissé au lecteur) et de composer ces deux plongement pour obtenir le résultat voulu.

6.1.1 $GL_n(\mathbb{Z}/p\mathbb{Z})$ possède un p-Sylow

1. **Cardinal de $GL_n(\mathbb{Z}/p\mathbb{Z})$:**

   Pour cela, on énumère les bases de $(\mathbb{Z}/p\mathbb{Z})^n$:

- Il y a $p^n - 1$ possibilités pour le 1er vecteur $\vec{u_1}$.
- Il y a $p^n - p$ possibilités pour le 2nd vecteur $\vec{u_2}$. En effet, $\vec{u_2} \in (\mathbb{Z}/p\mathbb{Z})^n \setminus \mathrm{Vect}(\vec{u_1})$. Or $\mathrm{Vect}(\vec{u_1})$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})$ donc de cardinal p.

  $\vdots$
- Il y a $p^n - p^{n-1}$ possibilités pour le n-ème vecteur $\vec{u_n}$.
  En effet, $\vec{u_n} \in (\mathbb{Z}/p\mathbb{Z})^n \setminus \mathrm{Vect}(\vec{u_1}, \dots, \vec{u}_{n-1})$ et $\mathrm{Vect}(\vec{u_1}, \dots, \vec{u}_{n-1}) \simeq (\mathbb{Z}/p\mathbb{Z})^{n-1}$ donc de cardinal p^{n-1}.

Ainsi :
$|GL_n(\mathbb{Z}/p\mathbb{Z})| = (p^n-1)(p^n-p)\dots(p^n-p^{n-1}) = (p^n-1)(p^{n-1}-1)p \times \dots \times (p-1)p^{n-1}$.

Autrement dit,

$|GL_n(\mathbb{Z}/p\mathbb{Z})| = (p^n-1)\dots(p-1) \times (1 \times p \times \dots \times p^{n-1}) = (p^n-1)\dots(p-1) \times p^{\frac{n(n-1)}{2}}$

avec $(p^n-1)\dots(p-1)$ non divisible par p. Un p-Sylow de $GL_n(\mathbb{Z}/p\mathbb{Z})$ est donc d'ordre $p^{\frac{n(n-1)}{2}}$.

2. **Exhibons un sous-groupe de $GL_n(\mathbb{Z}/p\mathbb{Z})$ d'ordre $p^{\frac{n(n-1)}{2}}$.**

Notons $H = \left\{ \begin{pmatrix} 1 & * & \dots & * \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & 1 \end{pmatrix} \;\middle|\; * \in \mathbb{Z}/p\mathbb{Z} \right\} < GL_n(\mathbb{Z}/p\mathbb{Z})$. On a alors $|H| = p^{\frac{n(n-1)}{2}}$

Ainsi, H est un p-Sylow de $GL_n(\mathbb{Z}/p\mathbb{Z})$.

3. **Une fois le lemme suivant établi, on aura démontré le 1) du théorème de Sylow, avec**

$$s := (\phi \circ \mathrm{Cayley})^{-1}\left(G' \cap k\Sigma k^{-1}\right).$$

> **Lemme :**
> Soit K un groupe tel que $|K| = p^\alpha l$. Soit $G' < K$ et soit Σ un p-Sylow. Alors il existe $k \in K$ tel que $k\Sigma k^{-1} \cap G'$ soit un p-Sylow de G'.

On s'intéresse à l'action $: \left| \begin{array}{ccc} K \times K/\Sigma & \longrightarrow & K/\Sigma \\ (g, k\Sigma) & \longmapsto & gk\Sigma \end{array} \right.$

On restreint cette action à G' $: \left| \begin{array}{ccc} G' \times K/\Sigma & \longrightarrow & K/\Sigma \\ (g, k\Sigma) & \longmapsto & gk\Sigma \end{array} \right.$

On obtient alors : $Stab_K(k\Sigma) = k\Sigma k^{-1}$ et $Stab_{G'}(k\Sigma) = (k\Sigma k^{-1}) \cap G'$.

On souhaite vérifier qu'il existe $k \in K$ tel que $Stab_{G'}(k\Sigma)$ est un p-Sylow de G'.

On note $|G'| = p^{\beta_0} r$. On veut donc montrer qu'il existe $k \in K$ tel que :

$$|k\Sigma k^{-1} \cap G'| = p^{\beta_0}.$$

Autrement dit, il existe $k \in K$ tel que $\frac{|G'|}{|Stab_{G'}(k\Sigma)|}$ n'est pas divisible par p.

On applique l'équation aux classes : on note $k_1\Sigma, \dots, k_N\Sigma$ les représentants des orbites de l'action de G' sur K/Σ. On alors :

$$|K/\Sigma| = \sum_{i=1}^{N} |Orb_{G'}(k_i\Sigma)|$$

car $|K/\Sigma| = \frac{|K|}{|\Sigma|} = \frac{p^\alpha l}{p^\alpha} = l$ non divisible par p. (en effet, si pour tout i, $|Orb_{G'}(k_i\Sigma)|$ est divisible par p, alors $|K/Z|$ le serait aussi, ce qui est impossible)

Ainsi, il existe i tel que $|Orb_{G'}(k_i\Sigma)| = \frac{|G'|}{|Stab_{G'}(k\Sigma)|}$ est non divisible par p qui était le résultat voulu pour conclure.

2) Voici un second lemme dont on se servira :

Lemme :
Soit $H < G$ un $p-$groupe tel que $|H| = p^\beta$ où $\beta \in \{1, \ldots, \alpha\}$. Alors il existe un p-Sylow S de G tel que $H \subset S$.

Preuve :

Soit S' un p-Sylow de G. On applique le lemme avec $K = G, \quad G' = H, \quad \Sigma = S'$. Il existe $g \in G$ tel que $gS'g^{-1} \cap H$ est un p-sylow de H. Comme H est un p-groupe, H un p-Sylow de K coïncide avec K, d'où $K \subset gS'g^{-1}$. On pose alors $S = gS'g^{-1}$: c'est un p-Sylow de G contenant H, d'où le résultat.

$\square$

3) Un lemme et un corollaire intéressants :

Lemme :
Deux p-Sylow S, S' sont conjugués : il existe $g \in G$ tel que $S = gS'g^{-1}$

Preuve :

On reprend la preuve de 2) avec $H = S$. Alors $H \subset gS'g^{-1}$ devient $S \subset gS'g^{-1}$. Comme $|S| = |gS'g^{-1}| = |S'|$, on a $S = gS'g^{-1}$.

$\square$

Corollaire :
Soit G un groupe tel que $|G| = p^\alpha m$. Soit S un p-Sylow de G. Alors on a :

$$S \lhd G \Longleftrightarrow S \text{ est l'unique } p\text{-Sylow de } G$$

Preuve :

$$S \lhd G \quad \Longleftrightarrow \quad \forall g \in G, gSg^{-1} = S \quad \Longleftrightarrow \quad \forall S' \ p\text{-Sylow de } G,\ S = S'$$

Tout cela nous donne finalement que :

$$S \lhd G \Longleftrightarrow S \text{ est l'unique } p\text{-Sylow de } G$$

$\square$

4) Lemme sur la divisibilité par le nombre de p-Sylow

Lemme :
Soit s_p le nombre de p-Sylow de G. Alors $s_p \mid n$ avec $n = p^\alpha m$.

Preuve :

On pose $X := \{\ S \mid S \text{ est un } p\text{-Sylow de } G\}$ et on considère l'action :

$$: \left| \begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, S) & \longmapsto & gSg^{-1} \end{array} \right.$$

Le point 3) dit que cette action est transitive : il y a une seule orbite. Alors : $\forall s \in X$,

$$n = |G| = |Orb_G(s)| \times |Stab_G(s)| = |X| \times |Stab_G(s)| = s_p \times |Stab_G(s)|$$

Donc $s_p \mid n$.

$\square$

5) Second lemme sur la divisibilité par le nombre de p-Sylow

Lemme :
On a de plus que $s_p \equiv 1\ [p]$ et $s_p \mid m$.

Preuve :

On fixe $S' \in X$, et on considère $: \left| \begin{array}{ccc} S' \times X & \longrightarrow & X \\ (g,S) & \longmapsto & gSg^{-1} \end{array} \right.$. L'équation aux classes nous donne :

$$s_p = |X| = \sum_{i=1}^{N} |Orb_{S'}(s_i)|$$

où $S_1, \ldots, S_N$ sont des représentants des orbites. Ainsi :

$$s_p = |Fix| \quad + \sum_{\substack{i=1 \\ Stab_{S'}(s_i) \not\subseteq S'}}^{N} |Orb_{S'}(s_i)|.$$

Où $Fix = \{S \in X \mid \forall g \in S', gSg^{-1} = S\}$.
On remarque que $\displaystyle\sum_{\substack{i=1 \\ Stab_{S'}(s_i) \not\subseteq S'}}^{N} |Orb_{S'}(s_i)| = \frac{|S'|}{|Stab_{S'}(s_i)} = \frac{p^\alpha}{p^{\epsilon_i}}$ avec $\epsilon_i < \alpha$.

Alors $|Orb_{S'}(s_i)|$ est divisible par p. On souhaite maintenant montrer que $s_p \equiv 1\ [p]$. Il suffit de démontrer que $|Fix| = 1$. Autrement dit que $Fix = \{S'\}$. Soit $T \in Fix$, en particulier, T est un p-Sylow. On veut donc montrer que $T = S'$.

Astuce : On regarde le sous-groupe engendré par T et S', que l'on note N. Alors : $T < N$ et $S' < N$.

Remarque :

T et S' sont des p-Sylow de N.

Ainsi on a :

$$\forall a \in T, \quad aTa^{-1} = T \text{ (car } T < N)$$
$$\forall a \in S', \quad aTa^{-1} = T \text{ (car } T \in Fix)$$

Alors : $N =< T, S' >, \quad \forall a \in N, \quad aTa^{-1} = T$. Ainsi, par le corollaire T est normal dans N, donc c'est l'unique p-Sylow de N d'où $T = S'$. En conclusion $|Fix| = 1$ et donc $s_p \equiv 1\ [p]$.

$\square$

Chapitre 7

Applications de cours diverses

7.1 A_5 est simple

Propriété :
A_5 est simple et : $A_5 \lhd S_5$ et $|A_5| = \dfrac{5!}{2} = 60$

On sait que H est réunion de classes de conjugaison. On va montrer que si $H \neq \{e\}$ alors $H = A_5$.

Petite réflexion sur les classes de conjugaisons :
Soit $H \lhd A_5$
Les permutation de A_5 sont du type :

1. (a, b, c), les trois cycles
2. $(a, d)(c, d)$ doubles transpositions
3. (a, b, c, d, e) des 5 cycles

Classes de conjugaisons : Soit $\sigma \in A_5$
On pose : $C(\sigma) = \{g\sigma g^{-1}, g \in A_5\}$

1. Les 3 cycles sont une classe de conjugaison i.e :
   $\forall \sigma_1, \sigma_2$ des trois cycles $\exists g \in A_5, \sigma_2 = g\sigma_1 g^{-1}$. Il y a $\dfrac{5 \times \times 3 \times 4}{3} = 20$ 3-cycles.
2. L'ensemble des doubles transposition est elle aussi une classe de conjugaison :
   Soit $\tau = (a, b)(c, d)$ et $\tau' = (a', b')(c', d')$ deux transpositions. Soit aussi $e, e' \in [\![1, 5]\!]$ tq l'on ait : $\{a, b, c, d, e\} = \{a', b', c', d', e'\} = \{1, 2, 3, 4, 5\}$. On pose alors $\eta \in S_5$ qui envoie a sur a', b sur b' etc...
   On a alors : $\eta\tau\eta^{-1} = \tau'$
   Ici, se présentent alors deux cas : soit $\eta \in A_5$ au quel cas τ et τ' sont bien conjuguées dans A_5. Soit $\eta \notin A_5$.
   On à alors par simple vérification : $(\eta \circ (a, b))\tau(\eta \circ (a, b))^{-1} = \tau'$
   Il y a $\dfrac{5 \times 4 \times 3 \times 2}{2 \times 2 \times 2} = 15$
3. Il y a $\dfrac{5!}{5} = 24$ 5-cycles dans A_5. Ils se répartissent en ceux classes, celle de $(1, 2, 3, 4, 5)$ et celle de $(2, 1, 3, 4, 5)$

Lemme :
Si $H \lhd A_5$ contient un 5-cycle, alors i les contient tous.

Preuve :

Il suffit de remarquer que si σ est un 5-cycle alors $< \sigma >$ est un 5-Sylow. Et d'utiliser le deuxième théorème de Sylow.

$\square$

On à Maintenant tout les outils en main pour attaquer la preuve de la première propriété.

Preuve :

Soit $H \triangleleft A_5$, $H \neq \{e\}$:

- Si H contient un trois cycle alors $|H| >= 20 + 1$. Mais $|H|$ divise 60. Donc H contient un 3-cycle ou un 5-cycle. Dans tout les cas on à $|H| > 30$ donc $|H| = 60$
- Si H contient un 5-cycle, idem
- Si H contient un 3-cycle, idem

$\square$

7.2 Classification des groupes d'ordre pq

Théorème :
Soit G un groupe d'ordre pq, avec p et q premiers.
- Si p ne divise pas q-1, alors où bien : $G \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
- Si p divise q-1 alors, soit $G \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, soit :
$\exists \alpha : \mathbb{Z}/p\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/q\mathbb{Z})$ non trivial tel que $G \simeq \mathbb{Z}/q\mathbb{Z} \times_{\alpha} \mathbb{Z}/p\mathbb{Z}$

De plus si,$\alpha\beta : \mathbb{Z}/p\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/q\mathbb{Z})$ sont non triviaux alors : $\mathbb{Z}/q\mathbb{Z} \times_{\alpha} \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \times_{\alpha} \mathbb{Z}/p\mathbb{Z}$

insere prop manquate

Preuve :

Du théorème Premier cas :

Etude des q-Sylow :

$S_q \equiv 1(q)$ et $S_q|p \Longleftarrow S_q = 1$. Donc il existe un unique q-Sylow, il est distingué dans G, notons le N

Il existe un p-Sylow noté H. G est produit semi direct (interne) de N par H :
- $N \triangleleft G$ on l'a déjà
- $N \cap H = \{e\}$ car si $g \in N \cap H$, alors $o(g)|p$ et $o(g)|q$ donc $o(g) = 1$
- G=NH :

  On pose $function f N * HNH(x^a, h^b)x^a h^b$

$\square$

7.3 Classification des groupes d'ordre pq

Théorème :
Soit G un groupe d'ordre pq, avec p et q premiers.
- Si p ne divise pas q-1, alors : $G \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
- Si p divise q-1 alors, soit $G \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, soit :
$\exists \alpha : \mathbb{Z}/p\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/q\mathbb{Z})$ non trivial tel que $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_{\alpha} \mathbb{Z}/p\mathbb{Z}$

De plus si,$\alpha, \beta : \mathbb{Z}/p\mathbb{Z} \longrightarrow Aut(\mathbb{Z}/q\mathbb{Z})$ sont non triviaux alors : $\mathbb{Z}/q\mathbb{Z} \rtimes_{\alpha} \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_{\beta} \mathbb{Z}/p\mathbb{Z}$

insere prop manquate

Preuve :

Du théorème Premier cas :

Etude des q-Sylow :

$S_q \equiv 1(q)$ et $S_q | p \Longleftarrow S_q = 1$. Donc il existe un unique q-Sylow, il est distingué dans G, notons le N

Il existe un p-Sylow noté H. G est produit semi direct (interne) de N par H :

- $N \triangleleft G$ on l'a déjà
- $N \cap H = \{e\}$ car si $g \in N \cap H$, alors $o(g)|p$ et $o(g)|q$ donc $o(g) = 1$
- G=NH :

  On pose $f : \left| \begin{array}{ccc} N * H & \longrightarrow & NH \\ (x^a, h^b) & \longmapsto & x^a h^b \end{array} \right.$

Deuxième cas :

□

On peut donc compléter notre classification :

$\|G\|$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Nb de sg	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1

7.3.1 Caractérisation de $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ et mêm de $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}$

Propriété :

Soit $n \in \mathbb{N}^*$. L'application $\Psi : \left| \begin{array}{ccc} ((\mathbb{Z}/n\mathbb{Z})^\times, \times) & \longrightarrow & (\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ) \\ s & \longmapsto & \Psi_s : \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ c & \longmapsto & cs \end{array} \right. \end{array} \right.$ est un ismorphisme.

Corollaire :
Si $n = q$ un nombre premier, alors

$$(\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}), \circ) \simeq ((\mathbb{Z}/q\mathbb{Z})^\times, \times) \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +)$$

(cf TD), et si p divise $q - 1$ alors ce groupe possède un unique sous-groupe d'ordre p.

Preuve :

Preuve de la proposition.
Ψ est bien un morphisme de groupes.
Pour tout $s \in (\mathbb{Z}/n\mathbb{Z})^\times, \Psi_s \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.
Reste à montrer que Ψ est injectif et surjectif.
Ψ injectif :
$\ker(\Psi) = \{s \in (\mathbb{Z}/n\mathbb{Z})^\times, \Psi_s = \mathrm{Id}\}$.
surjectivité :
Soit $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}, +)$, c'est un morphisme bijectif de $(\mathbb{Z}/n\mathbb{Z}, +)$.
$\forall c \in \{0, ..., n-1\}, \varphi(\bar{c}) = \varphi(\bar{1} + ... + \bar{1}) = c\varphi(\bar{1}) = \bar{c}\varphi(\bar{1})$
Est-ce que $\varphi(\bar{1})$ joue le rôle de s ?
Oui!!! Car $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, φ permute les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$. Comme $\bar{1} \in (\mathbb{Z}/n\mathbb{Z})^\times$, on a bien $\varphi(\bar{1}) \in (\mathbb{Z}/n\mathbb{Z})^\times$. Cela établit la surjectivité de Ψ.

□

7.3.2 Sur les morphismes $\alpha : \mathbb{Z}/p\mathbb{Z} \mapsto \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$

Propriété :

- Ou bien p ne divise pas $q-1$, dans ce cas α est trivial
- ou bien p divise $q-1$, alors ou bien α est trivial, ou bien α est injectif et son image est l'unique sous-groupe d'ordre p dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$

Preuve :

$o(\alpha(\overline{1})$ divise $o(\overline{1}) = p$ et divise $|\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})| = q-1$.
Si p ne divise pas $q-1$, alors $o(\alpha(\overline{1})) = 1$, et dans ce cas α est trivial.
Si p divise $q-1$, on a les deux possibilités : $o(\overline{\alpha(\overline{1})}) = 1$ ou $o(\alpha(\overline{1})) = p$.
Dans le permier cas, α est trivial, dans le deuxième cas, α est alors injectif et comme $|\mathrm{im}(\alpha)| = p$, $\mathrm{im}(\alpha)$ est bien l'unique sous-groupe d'ordre p de $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$

□

Propriété :
Soient $\alpha, \beta : (\mathbb{Z}/p\mathbb{Z}, +) \mapsto (\mathrm{Aut}(K), \circ)$ (où K est un groupe général) deux morphismes.
Si $\mathrm{im}(\alpha) = \mathrm{im}(\beta)$, alors il existe $\rho \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ tel que $\beta = \alpha \circ \rho$.

Corollaire :
Soient $\alpha, \beta : (\mathbb{Z}/p\mathbb{Z}, +) \mapsto (\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}), \circ)$ deux morphismes non triviaux.
Alors $\mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\beta \mathbb{Z}/p\mathbb{Z}$.

Preuve :

Pour montrer que les deux p.s.d isomorphes, il suffit de montrer que $\mathrm{im}(\alpha) = \mathrm{im}(\beta)$ (utiliser ici la proposition 2 et un exercice du TD).
Comme α est non trivial, on a $\ker(\alpha) \neq \mathbb{Z}/p\mathbb{Z}$. Mais $\mathbb{Z}/p\mathbb{Z}$ ne possède que deux sous-groupes. Donc $\ker(\alpha) = \{e\}$. De même $\ker(\beta) = \{e\}$.
Ainsi $|\mathrm{Im}(\alpha)| = |\mathrm{Im}(\beta)| = |\mathbb{Z}/p\mathbb{Z}| = p$. Donc les deux sous-groupes $\mathrm{Im}(\alpha), \mathrm{Im}(\beta)$ de $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ coincident avec l'unique sous-groupe d'ordre p de $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +)$.

□

Preuve :

Comme $\mathrm{Im}(\alpha) = \mathrm{Im}(\beta)$ par hypothèse, α et β sont simultanément triviaux ou pas.
<u>Permier cas</u> :
Si α et β sont triviaux, alors on peut prendre $\rho = \mathrm{Id}$, on a bien $\beta = \alpha \circ \rho$.
<u>Deuxième cas</u> :
α, β ne sont pas tous les deux triviaux.
Si j'appelle $J = \mathrm{Im}(\alpha) = \mathrm{Im}(\beta)$, on a $J \simeq \mathbb{Z}/p\mathbb{Z}$ (le voir comme un "autre" $\mathbb{Z}/p\mathbb{Z}$). On a $\alpha(\overline{1}) \neq \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$ car α n'est pas trivial.
Donc $\alpha(\overline{1})$ est un générateur de $(\mathbb{Z}/p\mathbb{Z}, +)$. Mais $\beta(\overline{1}) \in \mathbb{Z}/p\mathbb{Z}$, donc il existe $k \in \{0, ..., p-1\}$ tel que $\beta(\overline{1}) = k\alpha(\overline{1})$. Mais $\beta(\overline{1}) \neq 0$, donc $k \in \{0, ..., p-1\}$.
Posons $\rho : \left| \begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \overline{b} & \longmapsto & \overline{b} \times \overline{k} \end{array} \right.$. Alors $\rho \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$, car $\overline{k} \in (\mathbb{Z}/p\mathbb{Z})^\times$. De plus, $\alpha \circ \bar{\rho}(1) = \alpha(\overline{k} = k\alpha(\overline{1}) = \beta(\overline{1})$. Donc $\alpha \circ \rho = \beta$.

□

7.3.3 Compléments

Propriété :
Soit $n \in \mathbb{N} \setminus \{0, 1, 2\}$, avec $n \neq 6$. Alors $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n \simeq \mathfrak{S}_n$.
Autrement dit : $\forall \rho \in \mathrm{Aut}(\mathfrak{S}_n), \exists ! \sigma \in \mathfrak{S}_n$ tel que $\rho(\eta) = \sigma\eta\sigma^{-1}$ ("Tout autour de $\mathfrak{S}_n$ est intérieur")
Si $n = 6$, alors $[\mathrm{Aut}(\mathfrak{S}_n); \mathrm{Int}(\mathfrak{S}_n)] = 2$.

Remarque :

Voir Perrin.

$J_k := \{\eta \in S_n, \eta$ est un produit de k transpositions à support disjoints$\}$.

Lemme : S
oit $\rho \in \mathrm{Aut}(S_n)$.

- $\exists k \in \mathbb{N}^*, \rho(J_k) = J_k$
- $\rho \in \mathrm{Int}(S_n) \iff \rho(J_1) = J_1$

Lemme : S
oit $n \geq 1, k \geq 2$ tel que $n \geq 2k$.
Soit $\rho \in \mathrm{Aut}(S_n)$.
Alors $\rho(J_1) = J_k$ implique $n = 6$ et $k = 3$.