Université des Sciences et Technologies de Lille
U.F.R. de Mathématiques Pures et Appliquées

M308 : Théorie des groupes

Clément BOULONNE

Avec la participation de Jean-Yves PALLARO,
d'après des notes de cours données par Chenxi GUO.

Cours dispensé par Pierre Debes

L3 Mathématiques 2008 - 2009

Table des matières

Chapitre 1

Structures de groupe

1.1 Généralités

Définition 1.1. *On appelle groupe la donnée $(G, \circ)$ d'un ensemble G et d'une loi (ou opération) de composition interne, c'est-à-dire une application*

$$\begin{array}{ccc} G \times G & \mapsto & G \\ (g_1, g_2) & \to & g_1.g_2 \end{array}.$$

vérifiant :

1. *Associativité : $x \circ (y \circ z) = (x \circ y) \circ z$*
2. *Élément neutre : il existe $e \in G$ tel que $e \circ x = x \circ e = x$*
3. *Élément symétrique : $\forall x \in G$, il existe $x' \in G$ tel que $x \circ x' = x' \circ x = e$. On note $x' = x^{-1}$.*

Remarque 1.2. Si en plus, on a la commutativité : $x \circ y = y \circ x$, le groupe est *commutatif* ou *abélien*. Dans ce cas, en général, la loi est notée $+$.

Exemples 1.3.
1. $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathbb{Q}^*, \times)$,$(\mathbb{Z}, +)$ sont abéliens.
2. $(\mathrm{GL}_m(\mathbb{C}), \times)$ et $(S_n, \circ)$ sont non abéliens.

Remarque 1.4. Si G est un groupe, alors on a : $\forall a, n, b \in G$

$$\begin{array}{ccc} a.n = b & \Longleftrightarrow & n = a^{-1}b \\ \Downarrow & \nearrow & \\ a^{-1}.(a.n) = a^{-1}.b & & \end{array}$$

et

$$a.n = a.y \Leftrightarrow n = y,$$
$$n.a = y.a \Leftrightarrow n = y.$$

Définition 1.5. *On appelle ordre du groupe G le cardinal du groupe G. On note $|G| = \mathrm{card}(G)$.*

1.2 Structure induite

Définition 1.6. *Étant donné un groupe $(G, \circ)$, un sous-groupe de G est la donnée d'un sous-ensemble H de G tel que H muni de la loi induite (ou restriction) de G à H soit un groupe, c'est-à-dire :*

- $H \times H \to G$ *soit à valeurs dans* H.
- passage à l'inverse *:*

$$\begin{array}{ccc} H & \mapsto & G \\ n & \to & n^{-1} \end{array}$$

soit à valeurs dans H,
- $1 \in H$ *(en particulier* $H \neq \emptyset$*).*

Proposition 1.7. *Si* G *est un groupe,* $H \subset G$ *est un sous-groupe si et seulement si :*

1. $\forall x, y \in H, x.y^{-1} \in H$,
2. $H \neq \emptyset$.

Remarque 1.8. Les sous-groupes triviaux de G sont G et 1.

Proposition 1.9. *L'intersection d'une famille* $(H_i)_{i\in I}$ *de sous-groupes d'un groupe* G *est un sous-groupe de* G.

Démonstration. Soit $H = \bigcap_{i\in I} H_i$.
- $H \subset G$
- $H \neq \emptyset$ car $1 \in H_i \quad \forall i \in I$
- Soient x, y. Par définition de H, $x, y \in H_i$, $i \in I$, d'où $xy^{-1} \in H_i$, $i \in I$. (car H_i sous-groupe de G) c'est-à-dire $xy^{-1} \in H$.

□

Définition 1.10. *Soient* $(G, \circ)$ *un groupe et* $S \subset G$ *sous-ensemble. Alors l'intersection de tous les sous-groupes de* G *qui contiennent* S *est un sous-groupe de* G *qui contient* S*. On l'appelle les sous-groupe de* G *engendré par* S *et on le note* $< S >$*. C'est* le plus petit sous-groupe de G qui contient S.

Proposition 1.11. *On a*

$$< S >= \{g_1^{n_1} \dots g_s^{n_s},\ g_i \in S,\ s \in \mathbb{N},\ n_1, \dots, n_s \in \mathbb{Z}\backslash\{0\}\}.$$

Démonstration. Montrons que $< S >= H_s$.
- H_s est un sous-groupe de G
  1. $H_s \subset G$,
  2. $H_s \neq \emptyset$,
  3. stabilité.
- $H_s \supset S$ car si $g \in S$, on peut écrire $g = g^{-1}$, d'où $< S > \subset H_s$ car on sait que $< S >$ est le plus petit sous-groupe. Si $g_1 \dots g_s \in S \subset < S >$ et $n_1, \dots, n_s \in \mathbb{Z}\backslash\{0\}$, alors $g_1^{n_1} \dots g_s^{n_s} \in < S >$, d'où $H_s \subset < S >$ car $< S >$ est un sous-groupe.

□

Remarques 1.12. 1. $< \emptyset >= \{1\}$

2. On dit qu'un groupe G est :
   - de type fini s'il existe $S \subset G$ fini tel que $G =< S >$.
   - monogène s'il existe $g \in G$ tel que $G =< g >$, soit $G = \{g^n,\ n \in \mathbb{Z}\}$.

   Si de plus, G est fini, alors il est dit cyclique.

Définition 1.13. *Si* G *est un groupe et* $g \in G$*, alors on appelle ordre de* g *le nombre* $| < g > |$.

Théorème 1.14 (Théorème de Lagrange)**.** *Soient G un groupe* fini *et H un sous-groupe de G. On a $|H|$ divise $|G|$.*

Démonstration. Les classes à droite de G modulo un sous-groupe H sont telles que, pour $x, y \in G$, on pose $x \sim y$ si $yx^{-1} \in H$, qui est une relation d'équivalence. La classe d'équivalence de x est alors :

$$\begin{aligned}\overline{x} = \{y \in G,\, yx^{-1} \in H\} &\iff yx^{-1} = h \in H \\ &\iff y = hx,\, h \in H \\ &\iff y \in Hx = \{h.x,\, h \in H\}.\end{aligned}$$

Donc $\overline{x} = H.x$. □

Exemples 1.15. 1. $g\mathbb{Z} = \overline{1} = 1 + g\mathbb{Z}$

2. Montrer que la preuve par g correspond à compter modulo g, c'est-à-dire dans la situation $g\mathbb{Z} \subset \mathbb{Z}$.

Lemme 1.16. *Si G et fini, alors $\forall x \in G$,* $\mathrm{card}(H.x) = |H|$.

Démonstration. L'application

$$\begin{array}{ccc} H & \mapsto & Hx \\ h & \to & hx \end{array}$$

est bijective. On dit que Hx, H, et xH sont équipotents. □

Preuve du théorème de Lagrange. Les classes à droite de G modulo H forment une partition de G, d'où

$$\begin{aligned} |G| &= \text{ somme des cardinaux des classes d'équivalences} \\ \Rightarrow |G| &= \{\text{nombre de classes}\} \times |H|. \end{aligned}$$

□

Proposition 1.17. *Soit G un groupe et x un élément de G d'ordre fini n. Alors n est le plus petit entier > 0 tel que $x^n = 1$.*

Démonstration. Par définition, $n = |< x >| = |\{x^m,\, m \in \mathbb{Z}\}|$. Comme $< x >$ est fini, il existe $m, m' \in \mathbb{Z}$, $m < m'$ tel que $x^m = x^{m'}$. On a alors $x^{m'-m} = 1$. Considérons l'ensemble

$$\mathcal{N} = \{h \in \mathbb{N} / \, h \neq 0,\, x^h = 1\}.$$

On a :
- $\mathcal{N} \subset \mathbb{N}\backslash\{0\}$.
- $\mathcal{N} \neq \emptyset$ car $m' - m \in \mathbb{N}$.

On note ν son plus petit élément. Il s'agit donc de montrer que $m = \nu$. Si $h \in \mathcal{N}$ alors $x^h = 1$. On fait la division euclidienne de h par ν, c'est-à-dire $h = \nu q + r$, avec $0 \leqslant r < \nu$. On a alors :

$$\begin{aligned} x^h = x^{\nu q + r} &= (x^\nu)^q.x^r \\ &= 1.x^r = x^r, \end{aligned}$$

d'où $x^r = 1$ et $r < \nu$. Impossible. Ce qui entraîne $r = 0$ donc ν divise h. On en déduit : pour $h, h' \in \mathbb{Z}$ tels que $h' \geqslant h$, on a :

$$\begin{aligned} x^h = x^{h'} &\iff x^{h'-h} = 1 \iff \nu | h' - h, \\ n = |\{x^h, \quad h \in \mathbb{Z}\}| &= (\text{nombre de puissance de } x \text{ distinctes}), \\ < x > = \{1, x, x^2, ..., x^{\nu-1}\}&. \end{aligned}$$

Conclusion : $| < x > | = \nu$, c'est-à-dire $n = \nu$. □

Remarque 1.18. Pour tout $g \in G$, l'ordre de g divise celui de G, en particulier $g^{|G|} = 1$.

Définition 1.19. *Soient G un groupe et H un sous-groupe de G ($H < G$). On note $[G : H]$ l'indice de H dans G :*

$$[G : H] = \frac{\text{card}(G)}{\text{card}(H)}.$$

Théorème 1.20. *Dans un groupe, l'intersection d'un nombre fini de sous-groupes d'indices finis est un sous-groupe d'indice fini.*

$$(H_1 \cap H_2)_x = H_{1x} \cap H_{2x} \Rightarrow [G : H_1 \cap H_2] \leqslant [G : H_1][G : H_2].$$

Théorème 1.21 (Formule des indices)**.** *Si H est un sous-groupe d'indice fini dans un groupe G et si K est un sous-groupe de G contenant H, alors K est d'indice fini dans G et :*

$$[G : H] = [G : K][K : H].$$

1.3 Morphisme de groupe

Définition 1.22. *On appelle et on note* $\text{Hom}(G_1, G_2)$*, morphisme (ou homomoprhisme) de groupe entre deux groupes G_1 et G_2 l'application :*

$$\begin{array}{rccc} f & : & G_1 & \to & G_2 \\ & & f(x.y) & \mapsto & f(x).f(y) \end{array}.$$

En particulier :
- $f(1_{G_1}) = 1_{G_2}$,
- $f(x^{-1}) = f(x)^{-1}$.

Exemples 1.23. 1. $a \in (\mathbb{Z}, +, 0)$, $n \in \mathbb{Z}$. Alors :

$$\begin{array}{rccc} \phi_a & : & \mathbb{Z} & \to & \mathbb{Z} \\ & & n & \mapsto & an \end{array}$$

est un morphisme.

2. $(G, \circ)$ pour $g \in G$.

$$\begin{array}{rccc} \varphi_g & : & (\mathbb{Z}, +) & \to & (G, \circ) \\ & & n & \mapsto & g^n \end{array}.$$

$$\varphi_g(n + m) = g^{m+n} = g^n.g^m = \varphi_{g(n)}.\varphi_{g(m)}.$$

3.

$$\begin{array}{rccc} \det & : & (\text{GL}_n(\mathbb{C}), \circ) & \to & (\mathbb{C}^*, \times) \\ & & A & \mapsto & \det A \end{array}.$$

4. L'application signature :
$$\begin{array}{ccc}(\mathcal{S}_n,\times) & \mapsto & (\{1,-1\},\times)\\ \omega & \to & \sigma(\omega)\end{array}.$$

Définition 1.24. *On appelle endomorphisme d'un groupe G, un morphisme (ou un homomorphisme) $f : G \to G$. On note* $\mathrm{End}(G)$*, l'ensemble des endomorphismes du groupe G.*

Définition 1.25. *Un automorphisme d'un groupe G est un endomorphisme bijective de G. On note* $\mathrm{Aut}(G)$*, l'ensemble des automorphismes du groupe G.*

Définition 1.26. *L'ensemble des monomorphismes de G_1 vers G_2 est défini comme suivant :*
$$\mathrm{Mono}(G_1,G_2) = \{f \in \mathrm{Hom}(G_1,G_2) \text{ tel que } f \text{ injective}\}.$$

Définition 1.27. *On définit l'ensemble des épimorphismes :*
$$\mathrm{Epi}(G_1,G_2) = \{f \in \mathrm{Hom}(G_1,G_2) \text{ tel que } f \text{ surjective}\}.$$

Proposition 1.28. *Si $f \in \mathrm{Hom}(G_1,G_2)$ et*

1. *Si $H_1 < G_1$, alors $f(H_1) < G_2$.*
2. *Si $H_2 < G_2$, alors $f^{-1}(H_2) < G_1$.*

Cas particulier :

(a) Soit $H_1 = G_1$, on appelle groupe image de f , $f(G_1)$.

(b) Soit $H_2 = \{1\}$, on appelle noyau de f et on note $\mathrm{Ker}(f)$, $f^{-1}(\{1\})$.

Démonstration. 1. en exercice
$$f^{-1}(H_2) \subset G_1 \xrightarrow{f} G_2 \supset H_2.$$

2.
$$f^{-1}(H_2) = \{g \in G_1 | f(g) \in H_2\}$$
$$f^{-1}(H_2) < G_1$$

et égalité ssi f est bijective.

I/ $f^{-1}(H_2) \subset G_1$ (par construction).

II/ $1_{G_1} \in f^{-1}(H_2)$ car $f(1_{G_1}) \in H_2$ alors $f^{-1}(H_2) = (f^{-1})(H_2)$, image pas réciproque.

III/ Soient $g,h \in f^{-1}(H_2)$. Alors $f(gh) = f(g)f(h) \in H_2$, donc $gh \in f^{-1}(H_2)$.

IV/ Si $g \in f^{-1}(H_2)$, $f(g^{-1}) = f(g)^{-1}$; d'où $g^{-1} \in f^{-1}(H_2)$.

□

Proposition 1.29. *Si $f \in \mathrm{Hom}(G_1,G_2)$, alors*

1. *f est surjective $\Leftrightarrow f(G_1) = G_2$.*
2. *f injective $\Leftrightarrow \mathrm{Ker}(f) = \{1_{G_1}\}$*

Démonstration. 1. Définition

2. Exercice

□

1.4 Structure produit direct

Définition 1.30. *Soient G_1 et G_2 deux groupes. La loi sur $G_1 \times G_2$ définie par*

$$(g_1, g_2) \times (g_1', g_2') \overset{déf}{=} (g_1 g_1', g_2 g_2').$$

donne à $G_1 \times G_2$ une structure de groupe.

Définition 1.31. *Les applications :*

$$\begin{array}{rccc} pr_1 & : & G_1 \times G_2 & \to & G_1 \\ & & (g_1, g_2) & \mapsto & g_1 \end{array} \quad et \quad \begin{array}{rccc} pr_2 & : & G_1 \times G_2 & \to & G_2 \\ & & (g_1, g_2) & \mapsto & g_2 \end{array} \quad \textit{sont surjectives,}$$

et

$$\begin{array}{rccc} i_1 & : & G_1 & \to & G_1 \times G_2 \\ & & g_1 & \mapsto & (g_1, g_2) \end{array} \quad et \quad \begin{array}{rccc} i_2 & : & G_2 & \to & G_1 \times G_2 \\ & & g_2 & \mapsto & (g_1, g_2) \end{array} \quad \textit{sont injectives.}$$

Ce sont des morphismes de groupes (vérification en exemples).

Définition 1.32. *Cette construction du produit se généralise au produit de n groupes, $G_1, ..., G_n$, et même d'une famille $(G_i)_{i \in I}$ avec*

$$(g_i)_{i \in I} \times (h_i)_{i \in I} \overset{déf}{=} (g_i h_i)_{i \in I}.$$

Le produit des groupes G_i où $i \in I$ se note $\prod_{i \in I} G_i$.

Exemple 1.33.

$$\prod_{n \in \mathbb{N}} \mathbb{R} = \{\text{suites réelles}\} = \mathbb{R}^{\mathbb{N}}.$$

1.5 Structure quotient

Définition 1.34. *Soit G un groupe. H sous-groupe de G. On définit deux relations sur G :*

1. *Pour $g, h \in G$,*
$$g \sim_g h \text{ si } h^{-1} g \in H.$$
2. *Pour $g, h \in G$,*
$$g \sim_d \text{ si } g h^{-1} \in H.$$

Ce sont des relations d'équivalence.

Remarque 1.35. Si $h^{-1} g \in H$,

$$(h^{-1} g)^{-1} = g^{-1} h \in H.$$

Définition 1.36. *On définit la classe de x, $\overline{x}$:*

$$\overline{x} = \{h \in G | h \sim_g x\} = \{h \in G | x^{-1} h \in H\} = \{h \in G | h \in xH\}.$$

Les classes à gauche sont les sous-ensembles xH où $x \in G$. Les classes à droite sont les sous-ensembles Hx où $x \in G$.

Remarque 1.37.

$$xH = yH \Leftrightarrow x \sim_g y \Leftrightarrow y^{-1} x \in H.$$

On pose :

$$G/.H = \{xH,\ x \in G\} \qquad \text{(ensemble des classes à gauche)},$$
$$G/H. = \{Hx,\ x \in G\} \qquad \text{(ensemble des classes à droite)}.$$

Remarque 1.38. Si G est abélien, $xH = Hx$.

Soient $g_1H,\ g_2H \in G/.H$. $g_1Hg_2H = \{g_1hg_2k | h \in H, k \in H\}$ n'est pas en général de la forme g_1g_2H (ou même gH avec $g \in G$). Ce n'est pas un élément de $G/.H$.

Définition 1.39. *Le sous-groupe H est dit normal (ou distingué ou invariant) dans G si pour tout sous-groupe H de G, pour tout $h \in H$ et tout $g \in G$, on a $ghg^{-1} \in H$. On note : $H \triangleleft G$.*

Remarque 1.40. Si G est abélien, $ghg^{-1} = h \in H$. Donc tout sous-groupe est distingué,

Propriété 1.41. *Si $H \triangleleft G$, les classes à droite coïncident avec les classes à gauche : $xH = Hx$ $(\forall x \in G)$.*

Démonstration. Soit $xh \in xH$, $(h \in H)$.

$$xh = \underbrace{xhx^{-1}}_{\text{dans } H \text{ car } H \triangleleft G} x \in Hx,$$

donc $xH \subset Hx$. □

1.
$$\begin{aligned} g_1Hg_2H &= g_1(Hg_2)H \\ &= g_1(g_2H)H \\ &= g_1g_2HH = g_1g_2H. \qquad (HH = H) \end{aligned}$$

2.
$$\begin{aligned} (gH)^{-1} &= H^{-1}g^{-1} \\ &= Hg^{-1} = g^{-1}H. \end{aligned}$$

On pose :
$$G/.H = G/H. = G/H$$
On a une loi de groupe sur G/H (qui provient de celle de G) : $g_1H \circ g_2H = g_1g_2H$.

Définition 1.42. *L'application*
$$\begin{array}{ccc} G & \mapsto & G/H \\ g & \to & gH \end{array}$$
est un morphisme surjectif qu'on appelle surjection canonique.

Exemples 1.43.
1. Pour $(\mathbb{Z}, +)$, les sous-groupes sont les $n\mathbb{Z}$ $(n \in \mathbb{N})$. Ils sont distingués, d'où le groupe quotient $\mathbb{Z}/n\mathbb{Z}$.
2. Pour $(\mathcal{S}_d, \circ)$, on définit :
$$\mathcal{A}_d = \{\omega \in \mathcal{S}_d \,|\, \Sigma_d(\omega) = 1\}.$$
où S_d est l'application signature définie aux exemples 1.23 et 1.46. On a ainsi :
– $\mathcal{A}_d < \mathcal{S}_d$,
– $\mathcal{A}_d \triangleleft \mathcal{S}_d$: si $\omega \in \mathcal{A}_d$ et $g \in \mathcal{S}_d$, alors $\Sigma(g\omega g^{-1}) = \Sigma(g)\Sigma(\omega)\Sigma(g)^{-1} = 1$.

On a : $\mathcal{S}_n/\mathcal{A}_n = \{+1, -1\}$.

Définition 1.44. *On dit que G_1 et G_2 sont isomorphes si on peut trouver un isomorphisme f (un morphisme bijective) tel que $f : G_1 \to G_2$. On note $G_1 \simeq G_2$ si G_1 et G_2 sont isomorphes.*

Proposition 1.45. *Si $f \in \mathrm{Hom}(G, G')$, alors $\mathrm{Ker}(f) \triangleleft G$ et $G/\mathrm{Ker}(f) \simeq f(G)$.*

Exemple 1.46. Soit σ l'application signature :

$$\sigma : \mathcal{S}_n \to \{\pm 1\},$$

- $\mathcal{A}_n \triangleleft \mathcal{S}_n$,
- $\mathcal{S}_n/\mathcal{A}_n \simeq \sigma(\mathcal{S}_n) = \{\pm 1\}$.

Démonstration. On veut montrer que $\mathrm{Ker}(f) \triangleleft G$: soient $h \in \mathrm{Ker}\, f$ et $g \in G$. On veut ainsi montrer que $ghg^{-1} \in \mathrm{Ker}(f)$.

$$f(ghg^{-1}) = f(g)\underbrace{f(h)}_{=1}f(g)^{-1} = f(g)f(g)^{-1} = 1.$$

Donc : $ghg^{-1} \in \mathrm{Ker}\, f$.

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & G' \\ {\scriptstyle s}\downarrow & & \uparrow{\scriptstyle i} \\ G/\mathrm{Ker}(f) & \xrightarrow{\ \overline{f}\ } & f(G) \end{array} .$$

On a construit $\overline{f} \in \mathrm{Isom}(G/\mathrm{Ker}(f), f(G))$, avec $i \circ \overline{f} \circ s = f$. On pose

$$\overline{f}(x\,\mathrm{Ker}(f)) \overset{\text{déf}}{=} f(x).$$

Les problèmes sont :

1. si $x\,\mathrm{Ker}(f) = y\,\mathrm{Ker}(f)$, a-t-on $f(x) = f(y)$?
2. La définition dépend-elle du nombre de représentants de la classe ?

La réponse est oui car :

$$x\,\mathrm{Ker}(f) = y\,\mathrm{Ker}(f) \Leftrightarrow x^{-1}y \in \mathrm{Ker}(f) \Leftrightarrow f(x^{-1}y) = 1 \Leftrightarrow f(x)^{-1}f(y) = \ 1 \Leftrightarrow f(y) = f(x).$$

- Soit $g \in G$.

$$(i \circ \overline{f} \circ s)(g) = i \circ \overline{f}(s(g)) = i \circ \overline{f}(g\,\mathrm{Ker}(f)) = i(f(g)) = f(g).$$

- *Surjectivité de $\overline{f}$:* Soit $f(g)$ un élément quelconque de $f(G)$, $f(g) = \overline{f}(g\,\mathrm{Ker}(f))$.
- *Injectivité :* Soit $g\,\mathrm{Ker}(f)$ un élément quelconque de $G/\mathrm{Ker}\, f$, tel que $\overline{f}(g\,\mathrm{Ker}(f)) = 1$. On veut savoir si $\overline{f}$ est injective, soit :

$$g\,\mathrm{Ker}(f) = 1\,\mathrm{Ker}(f) = \mathrm{Ker}(f).$$

On a : $f(g) = 1$ donc $g \in \mathrm{Ker}(f)$. $g1^{-1} \in \mathrm{Ker}(f)$. $g \sim 1$, c'est-à-dire $g\,\mathrm{Ker}(f) = 1\,\mathrm{Ker}(f)$. □

Remarque 1.47. $g \in H \Leftrightarrow g$ est dans la classe de 1.

Proposition 1.48. *Soit $f \in \mathrm{Hom}(G, G')$ et $H < \mathrm{Ker}(f)$ tel que $H \triangleleft G$.*
Alors :

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow{\scriptstyle s} & & \uparrow{\scriptstyle i} \\ G/H & \xrightarrow{\overline{f}} & f(G) \end{array} .$$

- $f = i \circ \overline{f} \circ s$.
- $\overline{f}(G/H) = f(G)$
- $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/H$

Il existe $\overline{f} \in \mathrm{Hom}(G/H, f(G))$ tel que $f = i \circ \overline{f} \circ s$. On dit que « f se factorise à travers *G/H ».*

Exemple 1.49. Soit le diagramme suivant :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/2\mathbb{Z} \\ \downarrow{\scriptstyle s} & \nearrow{\scriptstyle \overline{f}} & \\ \mathbb{Z}/6\mathbb{Z} & & \end{array} .$$

Alors $\mathrm{Ker}(f) = 2\mathbb{Z}$, soit $H = 6\mathbb{Z}$, $H = 6\mathbb{Z} \subset 2\mathbb{Z}$.

Remarque 1.50. Pour $H = \mathrm{Ker}(f)$, on obtient

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow & & \uparrow{\scriptstyle i} \\ G/Ker(f) & \xrightarrow{\overline{f}} & f(G) \end{array}$$

avec $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/\mathrm{Ker}(f) = \{1\}$, c'est-à-dire $\overline{f}$ est surjective donc $f(G) : G/\mathrm{Ker}(f) \to f(G)$.

Démonstration. On pose $\overline{f}(gH) = f(g)$.

- On vérifie que $\overline{f}$ est bien définie donc on veut savoir si $gH = g'H \Rightarrow f(g) = f(g')$. Si $gH = g'H$, alors $g^{-1}g' \in H \subset \mathrm{Ker}(f)$. Donc $f(g^{-1}g') = 1$ d'où $f(g) = f(g')$,
- $f(G) = \overline{f}(G/H)$

- $i \circ f \circ s = f$.

Soit $g \in G$.

$$i \circ \overline{f} \circ s(g) = i \circ \overline{f}(gH) = i(f(g)) = f(g).$$

$\mathrm{Ker}(\overline{f})$. Soit $gH \in G/H$. On veut savoir à quelle condition $\overline{f}(gH) = 1_G$?

$$\overline{f}(gH) = f(g) = 1 \Leftrightarrow g \in \mathrm{Ker}(f) \Leftrightarrow gH \in \underbrace{\{kH, k \in \mathrm{Ker}(f)\}}_{\text{déf. de } \mathrm{Ker}(f)/H}$$

donc $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/H$. □

Théorèmes d'isomorphisme

Théorème 1.51 (Premier théorème d'isomorphisme)**.** *Soit H et K deux sous-groupes de G et $H \triangleleft G$ alors :*
- $HK = KH =< H \cup K >$
- $H \triangleleft KH$ *et* $H \cap K \triangleleft K$
- $KH/H \simeq K/H \cap K$.

Démonstration. – Il est toujours vrai que :

$$HK \subset < H \cup K >$$
$$KH \subset < H \cup K > .$$

– Soit $h \in H$ et $k \in K$.

$$hk = \underbrace{k}_{\in K}\underbrace{k^{-1}hk}_{\in H} \in KH.$$

D'où $HK \subset KH$, de même $KH \subset HK$.

– On montre que HK est un sous-groupe de G. Soient $h, h' \in H$ et $k, k' \in K$.

$$hkh'k' = h(kh')k' = h(h''k'')k',$$

donc HK est stable. Soit $h \in H$, et $k \in K$.

$$(hk)^{-1} = k^{-1}h^{-1} \in KH = HK.$$

Donc $HK < G$.

–
$$\left.\begin{array}{l} H \subset HK \\ K \subset HK \end{array}\right\} \text{ d'où } < H \cup K > \subset HK.$$

– On a : $H \triangleleft HK$ car $H \triangleleft G$. Pour montrer que $H \cap K \triangleleft K$, soit $x \in H \cap K$ et $k \in K$. Ainsi $kxk^{-1} \in K$ car $x, k \in K$ et $kxk^{-1} \in H$ car $x \in H \triangleleft G$. Donc $kxk^{-1} \in H \cap K$ et donc $H \cap K \triangleleft K$.

– On part de l'injection canonique qu'on compose avec la surjection canonique.

$$\begin{array}{ccc} K & \xrightarrow{\ i\ } & KH \\ & & \downarrow s \\ & & KH/H \end{array} .$$

– $s \circ i$ est surjective : soit khH un élément de KH/H.
On a

$$\begin{aligned} khH &= kH \quad (h \in H) \\ &= s(k). \end{aligned}$$

– Noyau de $s \circ i$: soit $k \in K$. On a

$$s \circ i(k) = 1_{KH/H} = H \Leftrightarrow kH = H \Leftrightarrow k \in H,$$

d'où $\mathrm{Ker}(s \circ i) = \{k \in K | k \in H\} = H \cap K$.

Conclusion : $K/\operatorname{Ker}(s\circ i)\simeq s\circ i(K)$ donne

$$K/H\cap K\simeq KH/H.$$

□

Théorème 1.52 (Second théorème d'isomorphisme)**.** *Soit H_1, H_2 deux sous-groupes de G tel que $H_1\subset H_2$ et $H_1\subset G$, $H_2\lhd G$, alors*[1]

$$G/H_2\simeq (G/H_1)/(H_2/H_1),$$

ce qui sous-entend que $H_2/H_1\lhd G/H_1$.

Démonstration. $H_2/H_1\lhd G/H_1$. On définit :

$$s : G\to G/H_2$$

la surjection canonique. On a :

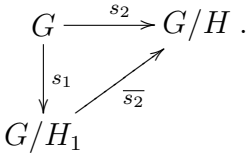
$$G/H_2=s(G),\quad H_2/H_1=s(H_2).$$

En particulier $H_2/H_1<G/H_1$. De plus, si $gH_2\in G/H_2$ et $h_2H_1\in H_2/H_1$,

$$gH_1h_2H_1(gH_1)^{-1}\in H_2/H_1.$$

Comme s est un morphisme peut-on écrire que c'est $s(gh_2g^{-1})\in H_2/H_1$? Oui car $gh_2g^{-1}\in H_2$ $(H_2\lhd G)$.

– On part de



$\overline{s_2}$ existe d'après la proposition 1.48, on a bien $H_1\subset Ker(s_2)=H_2$.

–
$$\overline{s_2}(G/H_1)=s_2(G)=G/H_2 \text{ et } \operatorname{Ker}(\overline{s_2})=\operatorname{Ker}(s_2)/H_1=H_2/H_1,$$

d'où $(G/H_1)/(H_2/H_1)\simeq G/H_2$.

□

Exemples 1.53. Soient $G=\mathbb{Z}$, $H=m\mathbb{Z}$, $K=n\mathbb{Z}$. Alors

$$\begin{aligned} H\cap K=m\mathbb{Z}\cap n\mathbb{Z}=\mu\mathbb{Z} \qquad & \text{où } \mu=\operatorname{PPCM}(m,n),\\ HK=m\mathbb{Z}+n\mathbb{Z}=\delta\mathbb{Z} \qquad & \text{avec } \delta=\operatorname{PGCD}(m,n),\end{aligned}$$

d'où $\delta\mathbb{Z}/m\mathbb{Z}\simeq n\mathbb{Z}/\mu\mathbb{Z}$. Si $d|n$, $d\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}/nd^{-1}\mathbb{Z}$. En particulier,

$$\frac{m}{\delta}=\frac{\mu}{n}\Leftrightarrow mn=\delta\mu.$$

[1] $H_1\lhd H_2$, évident

Solution.

$$\mathbb{Z} \xrightarrow{\mu} d\mathbb{Z}$$

$$\begin{array}{ccc} x & \longrightarrow & dx \\ & & \downarrow s \\ & & d\mathbb{Z}/n\mathbb{Z} \end{array} \qquad \begin{array}{c} dx \\ \downarrow \\ \text{classe de } dx \mod n \end{array}$$

μ et s sont surjectives donc $s \circ \mu$ aussi. On cherche $\mathrm{Ker}(s \circ \mu)$.

$$s \circ \mu(x) = 0, \qquad x \in \mathbb{Z}.$$

$$\begin{aligned} s(dx) = 0 &\iff dx \text{ est divisible par } n \\ &\iff \text{il existe } h \in \mathbb{Z} \text{ tel que } dx = nh \\ &\qquad \text{ce qui donne } x = nhd^{-1}, \end{aligned}$$

d'où $Ker(s \circ \mu) = nd^{-1}\mathbb{Z}$. □

Propriété 1.54 (Sous-groupes de G/H)**.** *Soit G un groupe et $H \triangleleft G$, alors les sous-groupes de G/H sont les groupes K/H où K est un sous-groupe de G qui contient H.*

Exemple 1.55. Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont $n\mathbb{Z}/6\mathbb{Z}$ avec $n\mathbb{Z} \supset 6\mathbb{Z}$ (c'est-à-dire $n|6$), c'est-à-dire

$$\mathbb{Z}/6\mathbb{Z}, \quad \{0\}, \quad 2\mathbb{Z}/6\mathbb{Z}, \quad 3\mathbb{Z}/6\mathbb{Z}.$$

Démonstration. On introduit la surjection canonique $s : G \longrightarrow G/H$. Si K est un sous-groupe de G contenant H alors $K/H = s(K)$ est un sous-groupe de G/H. Soit $\mathcal{H}$ un sous-groupe de G/H.

$$s : G \longrightarrow \underbrace{G/H}_{\supset \mathcal{H}}.$$

On pose $K = s^{-1}(\mathcal{H})$. On a alors :
- $K < G$,
- $K = s^{-1}(\mathcal{H}) \supset s^{-1}(\{1\}) = \mathrm{Ker}(s)$,
- $K/H = \mathcal{H}$[2] $= s(s^{-1}(\mathcal{H}))$, d'où $\mathcal{H} = s(K) = K/H$.

□

1.6 Groupes monogènes

Définition 1.56. *Un groupe monogène est un groupe contenant un élément a tel que, pour tout élément x du groupe, il existe un entier n vérifiant $x = a^n$.*

Exemples 1.57. 1. $\mathbb{Z} =< 1 >$,

[2] Pour une application f, on a toujours les inclusions suivantes :
- $f(f^{-1}(A) \subset A$ et égalité si f surjective,
- $f^{-1}(f(A)) \subset A$, et égalité si f injective.

donc
- ($\subset$) vrai car s est surjective,
- ($\supset$) toujours vrai.

2. $\mathbb{Z}/n\mathbb{Z} =< \overline{1} >$.

Proposition 1.58. *1. Un groupe monogène infini est isomorphe à $\mathbb{Z}$.*

2. Un groupe cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où $n = |G|$.

Démonstration. Soit G un groupe monogène, soit g un générateur de $G =< g >$. L'application

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \to & G =< g > \\ & & h & \mapsto & g^h \end{array}$$

est :
- un morphisme,
- surjective car $G =< g >= \{g^h | h \in \mathbb{Z}\}$

On cherche $\mathrm{Ker}(\varphi)$: c'est un sous-groupe de $\mathbb{Z}$ de la forme $a\mathbb{Z}$, d'où $\mathbb{Z}/a\mathbb{Z} \simeq G$.
- Si $a \neq 0$, G est fini donc cyclique et d'ordre a.
- Si $a = 0$, $G \simeq \mathbb{Z}/0\mathbb{Z}$, G infini.

□

Proposition 1.59. *Soit G un groupe cyclique d'ordre n :*

1. Si H sous-groupe de G, alors H et G/H sont cycliques.

2. $d|n \Leftrightarrow$ il existe un unique sous-groupe G_d de G d'ordre d, quotient Q_d de G d'ordre d.

3.

$$\begin{aligned} |G/H| = d &\iff |G||H|^{-1} = d \\ &\iff H \text{ est un sous-groupe de } G \text{ d'ordre } n/d \\ &\iff G/H = G/G_{n/d} = G_d. \end{aligned}$$

Démonstration. 1. en exercice.

2. ($\Leftarrow$) $|G_d| = d$ divise $n = |G|$, d'après le théorème 1.14 de Lagrange.
($\Rightarrow$) Soit g un générateur de G et φ le morphisme :

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \to & G \\ & & m & \mapsto & g^m \end{array}.$$

Existence : Si $m|n$, g^m d'ordre $\frac{n}{m}$ donc $< g^{n/d} >$ est un sous-groupe d'ordre d car n/d divise n.

Unicité : Soit $H \subset G$ d'ordre d. On a

$$\begin{aligned} H &= \varphi(\varphi^{-1}(H))^{3} && \text{car } \varphi \text{ est surjectif,} \\ &= \varphi(a\mathbb{Z}) = \{g^{ah} | h \in \mathbb{Z}\} =< g^a > . \end{aligned}$$

On obtient en particulier que H est cyclique. D'autre part,

$$\varphi^{-1}(H) = a\mathbb{Z} \supset \varphi^{-1}(\{1\}) = \{\text{multiple de l'ordre de } g\} = n\mathbb{Z},$$

c'est-à-dire a divise $|G|$ et alors H d'ordre $\frac{n}{a} = d$.

Conclusion : Nécessairement $H = \varphi(nd^{-1}\mathbb{Z})$.

□

[3] $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ donc de la forme $a\mathbb{Z}$.

Proposition 1.60 (Isomorphismes). *1. $f \in \mathrm{Hom}(G, G')$ et f bijectif $\Leftrightarrow$ f isomorphisme.*

2. f est un isomorphisme $\Rightarrow$ f^{-1} isomorphisme.

Définition 1.61. *Si E est non vide, on note $\mathfrak{S}(E)$, le groupe symétrique de E qui est l'ensemble des applications bijectives de E dans E.*

Lemme 1.62. *Si E est équipotent à E'*[4] *alors $\mathfrak{S}(E) \simeq \mathfrak{S}(E')$.*

Démonstration.

$$\begin{array}{rcl} \mathfrak{S}_E & \mapsto & \mathfrak{S}_{E'} \\ \sigma & \to & f \circ \sigma \circ f^{-1} \end{array},$$

(f est une bijection de E sur E'). □

Indicateur d'Euler :

Soit $n > 0$, $n \in \mathbb{N}$ fixé, $a \in \mathbb{Z}$ et

$$\overline{a} = \text{ classes de } a \mod n.$$

$$\begin{array}{ccccc} \overline{a} \text{ engendre } (\mathbb{Z}/n\mathbb{Z}, +) & \Longleftrightarrow & 1 \in < \overline{a} > & \Longleftrightarrow & \exists m \in \mathbb{Z} \text{ tel que } m\overline{a} = 1 \\ \Updownarrow & & & & \Updownarrow \\ & & & & \exists l, m \in \mathbb{Z},\ ma + ln = 1 \\ & & & & \Updownarrow \\ \overline{a} \text{ est inversible dans } \mathbb{Z}/n\mathbb{Z} \text{ pour } \times & & \Longleftrightarrow & & a \text{ et } n \text{ sont premiers entre eux} \end{array}$$

Conclusion :

$$\begin{aligned} \{\text{générateurs de } (\mathbb{Z}/n\mathbb{Z}, +)\} &= \{\text{classe d'entiers} > 0 \text{ premiers à } n \text{ et} \leqslant n\} \\ &\Longleftrightarrow \{\text{inversibles de } (\mathbb{Z}/n\mathbb{Z}, \times)\} \end{aligned}$$

On note $\varphi(n)$ le nombre d'éléments de ces ensembles.

1.7 Automorphismes intérieurs, groupes simples

Définition 1.63. *Soient G un groupe et $g \in G$. L'application*

$$\begin{array}{rcccl} C_g & : & G & \to & G \\ & & x & \mapsto & gxg^{-1} \end{array}$$

est

- *un morphisme ($gxyg^{-1} = gxg^{-1}gyg^{-1}$),*
- *bijectif ($(C_g)^{-1} = C_{g^{-1}}$).*

C'est donc un automorphisme, appelé conjugaison par g. Ces automorphismes sont appelés automorphismes intérieurs. On note $\mathrm{Int}(G)$ *leur ensemble.*

Proposition 1.64. *On a* $\mathrm{Int}(G) < \mathrm{Aut}(G)$ *car* $C_{g_1} \circ C_{g_2} = C_{g_1 g_2}$.

[4] c'est-à-dire qu'il existe une bijection de E à E'.

Plus précisément, l'application

$$\begin{array}{rccc} \Gamma & : & G & \to & \mathrm{Aut}(G) \\ & & g & \mapsto & C_g \end{array}$$

est un morphisme et $\Gamma(G) = \mathrm{Int}(G)$. Le noyeau de Γ, $\mathrm{Ker}(\Gamma)$ est l'ensemble :

$$Z(G) = \{g \in G,\, xg = gx, \quad x \in G\},$$

appelé centre de G. D'où aussi : $G/Z(G) \simeq \mathrm{Int}(G)$.

Remarque 1.65. Un sous-groupe $H < G$ est distingué ssi pour tout $g \in G$, $C_g(H) \subset H$ ssi H est invariant par tout automorphisme intérieur. On dit que H est un sous-groupe caractéristique et on note $H \sqsubset G$ si H est invariant par tout automorphisme de G. Donc $H \sqsubset G \Rightarrow H \triangleleft G$.

Définition 1.66. *Un groupe G est dit simple si ses seuls sous-groupes distingués sont G et $\{1\}$.*

Exemple 1.67. $(\mathbb{Z}/n\mathbb{Z}, +)$ est simple si et seulement si n est premier.

Proposition 1.68. *Tout groupe fini d'ordre premier p est cyclique.*

Chapitre 2

Groupe opérant sur un ensemble

2.1 Groupe de permutations

Définition 2.1. *Si X est un ensemble, l'ensemble*

$$\mathrm{Per}(X) = \{\textit{bijection/permutation : } X \to X\}$$

est un groupe pour la composition. Si $X = \{1, \dots, d\}$ alors

$$\mathrm{Per}(X) = \mathcal{S}_d \qquad \textit{(groupe symétrique d'ordre } d\textit{)}$$

est non abélien pour $n > 2$, en général.

Théorème 2.2 (Cayley)**.** *Tout groupe est isomorphe à un sous-groupe de permutation.*

Démonstration.

$$\begin{array}{ccccccc} G & \mapsto & \mathrm{Per}(G) & & & & \\ g & \to & \gamma_g & : & G & \to & G \\ & & & & x & \mapsto & gx \end{array}$$

est un morphisme injectif. Vérifions-le :

- $\gamma_{g_1 g_2} = \gamma_{g_1} \circ \gamma_{g_2}$ car $g_1 g_2 x = g_1(g_2 x)$,
- $\gamma_g = \mathrm{id}$ alors $g = 1$,
-

$$\underbrace{G/\{1\}}_{=G} \simeq \gamma(G) \subset \mathrm{Per}(G).$$

□

Remarque 2.3. γ représente les représentations régulières à gauche de G.

Définition 2.4. *Pour $s \in \mathrm{Per}(X)$, On définit le support de s :*

$$\mathrm{supp}(s) = \{x \in X,\ s(x) \neq x\}.$$

Remarque 2.5. $s(\mathrm{supp}(s)) = \mathrm{supp}(s)$.

Démonstration. En effet,

($\subset$) Si $x \in \mathrm{supp}(s)$ alors

$$\begin{aligned} s(x) \notin \mathrm{supp}(s) &\Leftrightarrow s(s(x)) = s(x) \\ &\Leftrightarrow s(x) = x \Leftrightarrow x \notin \mathrm{supp}(s) \end{aligned}$$

d'où ($\subset$).

($\supset$) On veut montrer que $\text{supp}(s) \subset s(\text{supp}(s))$. D'après la précédente inclusion,

$$s^{-1}(\text{supp}(s^{-1}) \subset \text{supp}(s^{-1}),$$

d'où $\text{supp}(s^{-1}) \subset s(\text{supp}(s^{-1}))$, c'est-à-dire $\text{supp}(s) \subset s(\text{supp}(s))$.

En conséquence, $s|_{\text{supp}(s)} \in \text{Per}(\text{supp}(s))$. □

Définition 2.6. *Pour $x \in X$, on pose $O_s(x) = \{s^n(x) | n \in \mathbb{Z}\}$, l'orbite de x sous s.*

Remarque 2.7. Si $\{x_1, \ldots, x_n\}$ est une famille de représentants des σ-orbites, alors $\{O_s(x_i)\}_i$ forme une partition.

Si X est fini,

$$O_s(x) = \{x, s(x), \ldots, s^{p-1}(x)\},$$

où p est le plus petit entier > 0 tel que $s^p(x) = x$.

$$s|_{O_s(x)} = \begin{pmatrix} x & s(x) & \cdots & s^{p-1}(x) \\ s(x) & s^2(x) & \cdots & x \end{pmatrix}$$

permute les éléments de $O_s(x)$ de façon circulaire. On dit que c'est un cycle de longueur pour un p-cycle.

Définition 2.8. *Un p-cycle de X est une permutation de X qui n'a qu'une orbite de longeur $\geqslant 2$.*

On utilise la notation suivante : $(x_1\ x_2\ \ldots\ x_p)$ veut dire que
- $x_1 \to x_2$ (x_1 s'envoie sur x_2),
- $x_2 \to x_3$ (x_2 s'envoie sur x_3),
- $\vdots$
- $x_p \to x_1$ (x_p s'envoie sur x_1).

Exemples 2.9. Dans $\mathcal{S}_4$, s : (1 2 3 4) est un cycle de longueur 4.

$$O_s(1) = \{1, 2, 3, 4\}, \qquad O_s(2) = \{2, 3, 4, 1\}$$

Soit maintenant

$$s = (1\ 2) \circ (3\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Alors

$$O_s(1) = O_s(2) = \{1, 2\}, \qquad O_s(4) = O_s(3) = \{3, 4\}.$$

Ce n'est donc pas un cycle.

Proposition 2.10. *Soient deux permutations $s, s' \in \text{Per}(X)$ telles que $\text{supp}(s) \cap \text{supp}(s') = \emptyset$. Alors ces deux permutations commutent.*

Démonstration. Soit $x \in X$.
- Si $x \in \text{supp}(s)$

$$ss'(x) = s(x) \quad (\text{car } x \in \text{supp}(s) \Rightarrow x \notin \text{supp}(s')),$$
$$s's(x) = s(x) \quad (\text{car } x \in \text{supp}(x) \Rightarrow s(x) \in \text{supp}(s) \Rightarrow s(x) \notin \text{supp}(s')).$$

– Si $x \in \mathrm{supp}(s')$, idem.
– Si $x \notin \mathrm{supp}(s), s \notin \mathrm{supp}(s')$ alors $ss'(x) = x = s's(x)$.

□

Exemples 2.11. 1. $(1\ 2)(3\ 4) = (3\ 4)(1\ 2)$.

$$\left.\begin{array}{l}(1\ 2\ 3)(2\ 3) = (1\ 2)\\ (2\ 3)(1\ 2\ 3) = (1\ 3)\end{array}\right\} \Rightarrow \mathrm{supp}(x) \cap \mathrm{supp}(s') = \emptyset.$$

2.

$$s = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\\ 6 & 4 & 5 & 10 & 7 & 1 & 2 & 3 & 8 & 9\end{pmatrix} = (1\ 6)(2\ 4\ 10\ 9\ 8\ 3\ 5\ 7)$$
$$= (2\ 4\ 10\ 9\ 8\ 3\ 5\ 7)(1\ 6)$$

Théorème 2.12. *Soit X fini. Tout élément $s \in Per(X)$ s'écrit sous la forme $s = p_1 \dots p_i$, où les p_i sont des cycles à supports disjoints. De plus l'écriture est unique à l'ordre près.*

Démonstration. *Existence :* pour $x, y \in X$, on pose $x \sim y$ s'il existe $n \in \mathbb{Z}$ tel que $y \in s^n(x)$. $\sim$ est une relation d'équivalence (le montrer). Pour $x \in X$, la classe de $x \equiv O_s(x)$. Les orbites $O_s(x)$ sont soit égales, soit disjointes. Notons $O_1, \dots, O_r$ les orbites de longueur $\geqslant 2$ et posons $s|_{O_i} = p_i$. c'est un cycle de longueur $\mathrm{card}(O_i)$. On a $s = p_1, \dots, p_r$ vérifiant : soit $x \in X$.Si $s(x) \neq x$, alors $x \in O_i$ pour un certain i, $s^i(x) = s(x)$.

$$p_1, \dots, p_r(x) = p_i(x) = s|_{O_i(x)} = s(x).$$

Si $s(x) = x$, alors $x \notin \bigcup_{i=1}^r O_i$, $p_1 \dots p_r(x) = x$, $s(x) = x$.
Unicité : supposons $s = p_1 \dots p_r$ comme dans l'énoncé. On a $s|_{\mathrm{supp}(p_i)} = p_i$. Si $x \in \mathrm{supp}(p_i)$, $O_s(x) = \mathrm{supp}(p_i)$.
Conclusion : si $s = p_1 \dots p_r$, alors $p_i = s|_{O(x)}$ où $x \in \mathrm{supp}(s)$.

□

Remarque 2.13. $(x_1, x_2, \dots, x_n) = (x_1, x_2)(x_2, x_3) \dots (x_{n-1}, x_n)$.

Conséquence 2.14. *$\mathcal{S}_d$ est engendré par les 2-cycles (appelés aussi les transpositions).*

Définition 2.15.

$$\mathcal{A}_d = \{s \in \mathcal{S}_d,\ s \text{ s'écrit comme produit d'un nombre pair de transpositions}\}.$$

Exemple 2.16. $\mathcal{A}_d$ est engendré par les 3-cycles ($d \geqslant 3$).

Théorème 2.17. *Il existe un unique morphisme (non trivial) $\varepsilon : \mathcal{S}_d \to \{-1, 1\}$ tel que si s est un 2-cycle, alors $\varepsilon(s) = 1$.*

Corollaire 2.18. *1.* $\mathrm{Ker}(\varepsilon) = \mathcal{A}_d \triangleleft \mathcal{S}_d$.
2. $\mathcal{S}_d/\mathcal{A}_d \simeq \{-1, 1\}$.

Preuve du théorème 2.17. *Existence :* Pour $s \in \mathcal{S}_d$, on pose

$$\varepsilon(s) = \prod_{\substack{(i,j)\in\{1,\dots,d\}^2\\ i\neq j}} \frac{X_{s(i)} - X_{s(j)}}{X_i - X_j} = \pm 1.$$

On a $\varepsilon(st) = \varepsilon(s)\varepsilon(t)$ et si s est un 2-cycle, alors $\varepsilon(s) = -1$.

Unicité : Si ε non trivial, il existe un 2-cycle s tel que $\varepsilon(s) = -1$. Si s, s' sont deux 2-cycles alors il existe $w \in \mathcal{S}_d$ tel que $s' = wsw^{-1}$ et donc $\varepsilon(s) = \varepsilon(s')$. D'où l'unicité.

□

Autre démonstration pour montrer l'unicité de ε dans le théorème 2.17. Soit $\varepsilon : \mathcal{S}_n \to \{-1, 1\}$ un morphisme non trivial. Alors il existe un 2-cycle τ_0 tel que $\varepsilon(\tau_0) = -1$ (car sinon comme les 2-cycles engendrent $\mathcal{S}_n$, on aurait $\varepsilon(\omega) = 1$ pour $\omega \in (\mathcal{S}_n)$. En fait, $\varepsilon(\tau) = -1$ pour tout 2-cycle τ. Notons que si $\tau_0 = (a\ b)$ et si $\omega \in \mathcal{S}_n$:

$$\omega\tau_0\omega^{-1} = (\omega(a)\ \omega(b)).$$

On a en particulier :

$$\varepsilon(\omega(a)\ \omega(b)) = \varepsilon(\omega)\varepsilon(\tau_0)\varepsilon(\omega)^{-1} = -1.$$

Si $\tau = (a'\ b')$ est un 2-cycle on peut toujours l'écrire

$$\tau = \omega\tau_0\omega^{-1}.$$

Il suffit de prendre pour ω une bijection de $\{1, \ldots, n\}$ qui envoie a sur a', et b sur b'. Donc $\varepsilon(\tau) = -1$. Les 2-cycles engendrent S_n, alors la connaissance de ε sur les 2-cycles détermine ε. On a de plus $\mathrm{Ker}(\varepsilon) = \mathcal{A}_n$.

($\supset$) évident.

($\subset$) On observe que :

1. $[\mathcal{S}_d : \mathrm{Ker}\,\varepsilon] = 2$ car $\mathcal{S}_d/\mathrm{Ker}\,\varepsilon \simeq \varepsilon(\mathcal{S}_d) = \{\pm 1\}$ (d'après le premier théorème d'isomorphisme, en cosidérant le morphisme ε).
2. $[\mathcal{S}_d : \mathcal{A}_d] = 2$. On veut le montrer. Soit $\omega \in \mathcal{S}_d$ tel que $\omega = \tau_1 \ldots \tau_m$ avec τ des transpositions. Si m est pair alors $\omega \in \mathcal{A}_n$, sinon

   $$\omega\tau_m = \tau_1 \ldots \tau_{m-1} \in \mathcal{A}_n.$$

   Donc soit $\omega \in \mathcal{A}_n$ ou soit $\omega\tau_m \in \mathcal{A}_n$. Il y a donc 2 classes à gauche de $\mathcal{S}_n$ modulo $\mathcal{A}_n$:
   – la classe triviale $\mathcal{A}_n$,
   – la classes des 2-cycles $\tau_0\mathcal{A}_n$.
   D'où $[\mathcal{S}_d : \mathcal{A}_d] = 2$.

Ainsi :

$$\frac{|\mathcal{S}_d|}{|\mathcal{A}_d|} = 2 = \frac{|\mathcal{S}_d|}{|\mathrm{Ker}\,\varepsilon|},$$

d'où $|\mathcal{A}_d| = |\mathrm{Ker}\,\varepsilon|$. On a

$$\mathcal{A}_d \subset \ker\varepsilon$$

et comme : $|\mathcal{A}_d| = |\mathrm{Ker}\,\varepsilon|$ alors $\mathcal{A}_d = \mathrm{Ker}\,\varepsilon$. □

Remarque 2.19. En particulier, on a :

$$\mathcal{A}_d \triangleleft \mathcal{S}_d.$$

car $\mathrm{Ker}(\varepsilon) = \mathcal{A}_d$ est distingué dans $\mathcal{S}_d$.

Définition 2.20. *On définit* $[G : H]$

$$[G : H] = \frac{|G|}{|H|}$$

comme étant le nombre de classes à gauche (ou à droite) modulo H.

Exemple 2.21. Soient $n = 3$ et $\sigma = (1\ 2\ 3)$ alors

$$\varepsilon(\sigma) = \frac{(x_2 - x_3)(x_3 - x_1)(x_2 - x_1)}{(x_1 - x_2)(x_2 - x_3)(x_1 - x_3)} = 1.$$

- Si $\sigma \in \mathcal{S}_n$, $\varepsilon(\sigma) \in \{\pm 1\}$
- Si σ est un 2-cycle, $\varepsilon(\sigma) = -1$.

Soient $\sigma, \tau \in \mathcal{S}_n$. Alors

$$\begin{aligned}
\varepsilon(\sigma\tau) &= \prod_{(i,j)\in\mathcal{P}_n} \frac{x_{\sigma(\tau(i))} - x_{\sigma(\tau(j))}}{x_i - x_j} = \prod_{(i,j)\in\mathcal{P}_n} \frac{x_{\sigma(\tau(i))} - x_{\sigma(\tau(j))}}{x_{\tau(i)} - x_{\tau(j)}} . \frac{x_{\tau(i)} - x_{\tau(j)}}{x_i - x_j} \\
&= \prod_{(i,j)\in\mathcal{P}_n} \frac{x_{\tau(i)} - x_{\tau(j)}}{x_i - x_j} \times \prod_{(i,j)\in\mathcal{P}_n} \frac{x_{\sigma(\tau(i))} - x_{\sigma(\tau(j))}}{x_{\tau(i)} - x_{\tau(j)}} \\
&= \varepsilon(\tau) \prod_{(i',j')\in Z(\mathcal{P}_n)} \frac{x_{\sigma(i')} - x_{\sigma(j')}}{x_{i'} - x_{j'}} \\
&= \varepsilon(\tau)\varepsilon(\sigma)
\end{aligned}$$

où $Z(\mathcal{P}_n)$ désigne l'ensemble des couples où chaque paire n'est représentée qu'une seule fois.

2.2 Action d'un groupe

Définition 2.22. *Soit G un groupe et E un ensemble. On définit l'action du groupe G sur l'ensemble E, l'application :*

$$\begin{array}{rcl} G \times E & \mapsto & E \\ (g, x) & \to & g.x \end{array}$$

qui a les propriétés suivantes :

1. $\forall (g_1, g_2) \in G \times G,\ \forall x \in E,\ g_1 g_2 x = g_1(g_2 x)$,
2. $\forall x \in E,\ e.x = x$.

On dit aussi que E est muni d'une loi de composition externe à gauche à opérateurs dans G.

Définition 2.23. *Pour $H \leqslant G$, on peut définir l'action de G par translation à gauche sur $Q_H = (G/H)_g$.*

En effet :

$$\begin{aligned}
gxH \in xH &\iff gxH = xH \\
&\iff gx \in xH \iff g \in xHx^{-1}.
\end{aligned}$$

On peut préciser le résultat. Avant cela, on rappelle la définition du noyau d'une action :

Définition 2.24. *Soient G un groupe et E un ensemble. Soit γ une action de G sur E. On définit le* noyau *de l'action :*

$$\operatorname{Ker}\gamma = \{g \in G,\ \gamma(g) = \mathrm{id}_E\}.$$

Proposition 2.25. *Soient un groupe G et $H \leqslant G$ alors le noyau de l'action γ de G sur $Q_H = (G/H)_g$ est :*

$$\operatorname{Ker}\gamma = \{g \in G,\ g.xH = xH,\ \forall x\}$$

et c'est le plus grand sous-groupe de G, normal dans G et contenu dans H.

Proposition 2.26. *Soient G un groupe et E un ensemble et soit γ une action de G sur E.*

1. *Si $H \triangleleft G$ tel que $x^{-1}Hx = H$ alors* $\operatorname{Ker}\gamma = H$.
2. *Si G est simple, $G \simeq \operatorname{Im}\gamma$ et* $\operatorname{Ker}\gamma = \{e\}$. *Il est « évident » que $\bigcap_{x\in G} xHx^{-1} \triangleleft G$.*

Proposition 2.27. *Si G est un groupe fini d'ordre $n = 1$, contenant un sous-groupe propre H tel que $[G : H] = k > 1$ et n ne divise pas $k!$, alors G n'est pas simple.*

Définition 2.28. *Soit G un groupe et E un ensemble. On appelle* action de G sur E *la donnée d'un homomorphisme*

$$\begin{array}{rcccl} \rho & : & G & \to & \mathrm{Per}(E) \\ & & g & \mapsto & \rho(g) \ : \ E \to E \\ & & & & \qquad\quad x \mapsto \rho(g)(x) = g.x \end{array} .$$

Exemples 2.29.

1. Si E est un ensemble $\rho : \mathrm{Per}(E) \to \mathrm{Per}(E)$ induit une action de $G = \mathrm{Per}(E)$ sur E : Si $g \in \mathrm{Per}(E)$ et $x \in E$, $\rho(g)(x) = g.x$.
2. $E = \{1, \ldots, n\}$, $\mathcal{S}_n$ agit sur $\{1, \ldots, n\}$.
3. Si $G_n < \mathcal{S}_n$, le morphisme $G \to \mathcal{S}_n$ qu'on appelle injection canonique induit une action de G sur $\{1, \ldots, n\}$.
4. Soit G un groupe. Le morphisme

$$\begin{array}{rcccl} \gamma & : & G & \to & \mathrm{Per}(G) \\ & & g & \mapsto & \gamma(g) \ : \ G \to G \\ & & & & \qquad\quad x \mapsto g.x \end{array}$$

   de représentation régulière à gauche de G induit une action de G sur lui-même.
5. Une action de $\mathcal{S}_4$ sur $\{1, \ldots, 6\}$: Tout élément $\omega \in \mathcal{S}_4$ agit sur les paires $\{i, j\}$ formées d'éléments de $\{1, 2, 3, 4\}$:

$$\omega(\{i, j\}) = \{\omega(i), \omega(j)\}, \qquad \omega = (1\ 2\ 3\ 4),$$

$$\begin{aligned} \dot{1} = \{1, 2\} &\longrightarrow \{2, 3\} \\ \dot{2} = \{1, 3\} &\longrightarrow \{2, 4\} \\ \dot{3} = \{1, 4\} &\longrightarrow \{2, 1\} \\ \dot{4} = \{2, 3\} &\longrightarrow \{3, 4\} \\ \dot{5} = \{2, 4\} &\longrightarrow \{3, 1\} \\ \dot{6} = \{3, 4\} &\longrightarrow \{4, 1\} \end{aligned}$$

   On a $\omega = (\dot{1}\ \dot{4}\ \dot{6}\ \dot{3})(\dot{2}\ \dot{5})$. De façon générale, moyennant ces notations, tout élément ω agissant sur les paires de $\{1, 2, 3, 4\}$ s'écrit comme un élément de $\mathcal{S}_6$. On a aussi l'action suivante $\mathcal{S}_4 \to \mathcal{S}_6$.

Définition 2.30. *Étant donnée une action $\rho : G \to \mathrm{Per}(E)$ pour tout $x \in E$, on pose*

$$O_\rho(x) = \{\rho(g)(x) | g \in G\} \subset E$$

qu'on appelle l'orbite de x dans l'action de G sur E et

$$G_\rho(x) = \{g \in G \quad | \quad \rho(g)(x) = x\} \subset G,$$

qu'on appelle le fixateur *de x dans l'action de G sur E (on a $G_\rho(x) < G$).*

$$g_1, g_2 \in G_\rho(x), \quad \rho(g_1 g_2)(x) = \rho(g_1) \circ \rho(g_2)(x) = \rho(g_1)[\rho(g_2)(x)] = \rho(g_1)(x) = x.$$

Remarque 2.31. Pour $s \in \mathrm{Per}(E)$ et $x \in E$, on a déjà défini l'orbite de x sous s comme $O_s(x) = \{s^n(x) | n \in \mathbb{Z}\}$. En fait, $O_s(x)$ correspond à l'orbite nouvellement définie de x dans l'action $< s > \xrightarrow{\rho} \mathrm{Per}(E)$ (injection canonique)

Proposition 2.32. *Si G fini, on a*

$$\mathrm{card}(O_\rho(x)) = \frac{|G|}{|G_\rho(x)|}.$$

Démonstration. On considère l'application

$$\begin{array}{ccc} G & \mapsto & O_p(x) \\ g & \to & \rho(g)(x) \end{array}.$$

Elle est
- bien définie (par définition),
- injective (par définition).

On définit pour $g_1, g_2 \in G$,

$$g_1 \sim g_2 \Rightarrow \rho(g_1)(x) = \rho(g_2)(x).$$

C'est une relation d'équivalence.

$$\begin{array}{rl} g_1 \sim g_2 & \iff \rho(g_2)^{-1}\rho(g_1)(x) = x \\ & \iff \rho(g_2^{-1}g_1)(x) = x \\ & \iff g_2^{-1}g_1 \in G_\rho(x) \iff g_1 G_\rho(x) = g_2 G_\rho(x). \end{array}$$

La relation $\sim$ est une relation d'équivalence associée avec classes à gauche de G modulo son sous-groupe $G_\rho(x)$. On définit l'application :

$$\begin{array}{ccccc} \varphi & : & G/.G_\rho(x) & \to & O_\rho(x) \\ & & gG_\rho(x) & \mapsto & \rho(g)(x) \end{array}.$$

- φ est bien définie : si g_1, g_2 sont 2 représentants de la même classe, alors $g_1 \sim g_2$, c'est-à-dire $\rho(g_1)(x) = \rho(g_2)(x)$.
- φ est surjective : évident.
- φ est injective : soient $g_1 G_\rho(x), g_2 G_\rho(x)$ tels que $\rho(g_1)(x) = \rho(g_2)(x)$. On a donc : $g_1 \sim g_2$, c'est-à-dire $g_1 G_\rho(x) = g_2 G_\rho(x)$.

$\Rightarrow \varphi$ est donc bijective d'où

$$\mathrm{card}(O_\rho(x)) = \mathrm{card}(G/G_\rho(x)) = [G : G_\rho(x)] = \frac{|G|}{|G_\rho(x)|}.$$

□

Proposition 2.33 (Formule des classes)**.** *Soit $\rho : G \to \mathrm{Per}(E)$ une action. On pose, pour $x, y \in E$, $x \sim y$ s'il existe $g \in G$ tel que $y = \rho(g)(x)$. $\sim$ est une relation d'équivalence. Pour tout $x \in E$, la classe d'équivalence de x est $O_\rho(x)$. Les classes forment une partition de l'ensemble E. Si E fini, on déduit :*

$$\mathrm{card}(E) = \sum_{i=1}^{r} \mathrm{card}(O_i) \tag{2.1}$$

où $O_1, \ldots, O_r$ sont les orbites distinctes.

Remarque 2.34.

$$\text{card}(O_\rho(x)) = 1 \iff O_\rho(x) = \{x\} \iff \forall g \in G,\ \rho(g)(x) = x.$$

Définition 2.35. *On pose* $E_G = \{x \in E | \rho(g)(x) = x\} \subset E$ *qu'on appelle ensemble des points fixes de l'action. L'égalité* (2.1) *se réecrit :*

$$\text{card}(E) = |\Sigma| + \text{card}(E_G).$$

où Σ *est la somme des cardinaux des orbites de cardinal* 2*.*

Définition 2.36. Une action $\rho : G \to \text{Per}(E)$ est dite fidèle si ρ est injectif.

Remarque 2.37. Une définition équivalente à la définition 2.36 est la suivante :

$$g \in G \text{ et } gx = x,\ \forall x \in E \Rightarrow g = e.$$

Exemple 2.38. L'action suivante est fidèle :

$$\begin{array}{ccccc} \gamma & : & G & \to & \text{Per}(G) \\ & & g & \mapsto & \gamma_g \end{array} \quad \text{où} \quad \begin{array}{ccccc} \gamma_g & : & G & \to & G \\ & & x & \mapsto & gx \end{array}.$$

On appelle cette action, représentation régulière de G à gauche.

Définition 2.39. ρ est dite transitive s'il n'existe qu'une seule orbite *(c'est-à-dire tous les éléments de* E *sont dans la même orbite ou* c'est-à-dire pour tout $x \in E$, pour tout $y \in E$, il existe $g \in G$ tel que $\rho(g)(x) = y$.

Exemples 2.40.

1. γ est transtive car si $x, y \in G$, $\gamma_g(x) = y$ pour $g = yx^{-1}$.
2. $\sigma = (1, 2, 3)$ dans $\mathcal{S}_4$. L'action de $< \sigma >$ sur $\{1, 2, 3, 4\}$ n'est pas transitive (les orbites sont $\{1, 2, 3\}$ et $\{4\}$).

Définition 2.41. ρ *est dite* n*-transitive si pour tout* $(x_1, ..., x_n) \in E^n$ *tel que les* x_i *sont deux à deux distinctes et pour tout* $(y_1, ..., y_n) \in E^n$ *tel que les* y_i *sont deux à deux distinctes, il existe* $g \in G$ *tel que* $gx_i = y_i$*,* $i = 1, ..., n$*.*

Remarques 2.42.

1. Pour $n \geq m \geq 1$, n-transitif $\Rightarrow$ m-transitive $\Rightarrow$ 1-transitif (= transitif).
2. $\mathcal{S}_d$ est d-transitif (dans son action sur $\{1, ..., d\}$) si $(x_1, ..., x_d)$, $(y_1, ..., y_d)$ vérifient la condition de la définition 2.41. L'application σ qui envoie x_i sur y_i pour $i = 1, ..., d$ est une permutation de $\{1, ..., d\}$.
3. $$\begin{aligned} \mathcal{H} &= \{\text{homographie bijective}\} \\ &= \left\{ z \xrightarrow{h} \frac{az + b}{cz + d} \,|\, a, b, c, d \in \mathbb{C},\ (c, d) \neq (0, 0) \right\}. \end{aligned}$$

   $\mathcal{H}$ opère sur $\mathbb{C} \cup \{\infty\}$

   $$\begin{array}{ccccc} \rho & : & \mathcal{H} & \to & \text{Per}(\mathbb{C}) \\ & & h & \mapsto & h : \mathbb{C} \to \mathbb{C} \end{array}.$$

   $\mathcal{H}$ est bien sûr un groupe et ρ. $\mathcal{H}$ est 3-transitif.

Justification. Soient $(a,b,c) \in (\mathbb{C}\cup\{\infty\})^3$ (avec a,b,c deux à deux distincts) et $(a',b',c') \in (\mathbb{C}\cup\{\infty\})^3$ (avec a',b',c' deux à deux distincts) alors il existe une homographie h tel que :

$$\begin{cases} h(a) &= a', \\ h(b) &= b', \\ h(c) &= c'. \end{cases}$$

□

Définition 2.43. *L'action ρ est dite imprimitive si ρ est* transitive *et il existe une partition de E (non triviale, c'est-à-dire* $\mathrm{card}(E_i) \geq 2$ *et $i \geq 2$) en sous-ensembles $(E_i)_{i\in I}$ (*automatiquement de même cardinal*) qui soit invariante par l'action (de tout élément $\rho(g)$). De façon plus explicite, on doit avoir : si $g \in G$, pour tout $i \in I$, si $x,y \in E_i$ alors $\rho(g)(x)$ et $\rho(g)(y)$ sont un même E_j qu'on note $E_{i(g)}$.*

Remarque 2.44. $\rho(g) : E_{i(g)} \to E_i$ est une *bijection.*

Exemples 2.45. 1. $G =< \underbrace{(123456)}_{\sigma} >\subset \mathcal{S}_6$ opère sur $\{1,2,3,4,5,6\}$. L'action est :

- transitive,
- imprimitive : on écrit

$$\underbrace{\{1,2,3,4,5,6\}}_{E} = \underbrace{\{1,3,5\}}_{E_1} \cup \underbrace{\{2,4,6\}}_{E_2}$$

et on a

$$\sigma^{2k+1}(E_1) = \{2,4,6\} = E_2$$
$$\sigma^{2k+1}(E_2) = \{3,5,1\} = E_1.$$

σ transforme la partition E_1, E_2 de E en la partition E_2, E_1 (c'est-à-dire la même).

2. Soit G un groupe. *Soient $\gamma : G \to \mathrm{Per}(G)$ (représentation regulière à gauche) et $H < G$.* Les classes xH de G modulo H forment une partition de G. Cette partition est *invariante* pour tout élément de G : soit $g \in G$, soient $x,y \in G$ tel que $y \in xH$. On a $gy \in gH$. Comme γ est aussi transitive, elle est imprimitive.

Définition 2.46. *L'action ρ est dite* primitive *si ρ est transitive et non imprimitive.*

Proposition 2.47. *Soient $\rho : G \to \mathrm{Per}(E)$ une action* transitive *et $x_0 \in E$. On a ρ imprimitive si et seulement si il existe un sous groupe de H tel que $G(x_0) \subseteq H \subseteq G$.*

Démonstration. ($\Rightarrow$) Soit $(E_i)_{i\in I}$ une partition non triviale de E invariante par l'action. Soit $i_0 \in I$ tel que $x_0 \in E_{i_0}$. On pose

$$H = \{g \in G,\ \rho(g)(E_{i_0}) = E_{i_0}\} = \mathrm{Stab}_G(E_{i_0}),$$

et

- $H < G$,
- $G_{x_0} \subset H$: soit $g \in G_{x_0}$ c'est-à-dire $\rho(g)(x_0) = x_0 \in E_{i_0}$, ce qui entraine $\rho(g)(E_{i_0}) = E_{i_0}$ car ρ lasse la partition invariante, tous les élémnets images de E_{i_0} sont dans le même sous-ensemble de la partition.

– $H \neq G$: si $H = G$ alors

$$\rho(g)(E_{i_0}) = E_{i_0} \qquad \text{pour tout } g \in G \tag{2.2}$$

Cela contredit la transitivité de ρ car (2.2) $\Rightarrow$ l'orbite de x_0 est contenue dans $E_{i_0} \neq E$.
– $Gx_0 \neq H$. Soit $h \in G$ tel que $\rho(h)(x_0) \in E_{i_0} \backslash \{x_0\}$ (h existe par *transitivité* de l'action) $h \notin Gx$ et $h \in H$ (par *imprimitivité* et par définition de H).

($\Leftarrow$) On considère les classes à gauche de G modulo H, $g_1H, ..., g_nH$ et on pose

$$E_i = \{\rho(g_ih)(x_0),\ h \in H\}.$$

On montre que ces E_i, $i = 1, ..., n$ constituent une partition de E.
– Soient $i \neq j$ et $h \in H$,

$$\rho(g_ih)(x_0) \iff \rho(g_jh)(x_0).$$

$$\begin{aligned} x_0 &= \rho(g_jh)^{-1}(\rho(g_ih)(x_0)) \\ &= \rho((g_jh)^{-1}(g_ih))(x_0) \quad (\text{car } \rho \text{ est un morphisme}) \\ &= \rho(h^{-1}g_j^{-1}g_ih)(x_0). \end{aligned}$$

Ainsi, $h^{-1}g_j^{-1}g_ih \in G_{x_0}$. Comme $G_{x_0} \subset H$, on a $h^{-1}g_j^{-1}g_ih \in H$ et donc $g_j^{-1}g_i \in H$ d'où $g_j^{-1}g_i = h' \in H$, soit $g_i = g_jH$, d'où g_i et g_j sont dans la même classe. Ce qui contredit l'hypothèse $g_iH \neq g_jH$. Donc $E_i \cap E_j = \emptyset$.
– $\bigcup_{i=1} E_i = E$.
($\supset$) Soit $x \in E$. Par transitivité (ρ est transitive par hypothèse), il existe $g \in G$ tel que $\rho(g)(x_0) = x$. L'élément $g \in G$ est une classe à gauche g_iH, pour $i \in \{1, \ldots, n\}$ car g_iH forment une partition de G, donc s'écrit $g = g_ih$ pour un $h \in H$. D'où,

$$x = \rho(g)(x_0) = \rho(g_ih)(x_0) \in E_i.$$

– La partition de E en la réunion des E_i est invariante par l'action. Soit $g \in G$

$$\rho(g)(E_i) = \{\rho(gg_ih)(x_0),\ h \in H\}$$

et

$$E_i = \{\rho(g_ih)(x_0),\ h \in H\}.$$

Quand h décrit H, g_ih décrit g_iH et gg_ih décrit la classe gg_iH qui est une des classes g_iH où $i = 1, ..., n$. Disons $gg_ih = g_kH$. Alors $\rho(g)(E_i) = E_k$. $\rho(g)$ permute les ensembles $E_1, ..., E_n$.
– La partition est non triviale : soient $h_1Gx_0, ..., h_mGx_0$ la liste des classes à gauche de H modulo G_{x_0}. Ces classes forment une partition de H, donc pour un $h \in H$, on peut écrire : $h \in h_i\gamma$ avec $\gamma \in G_{x_0}$. Donc pour un g_k, représentant d'une classe de H, on a :

$$\rho(g_kh)(x_0) = \rho(g_kh_i\gamma)(x_0) = \rho(g_k)\rho(h_i)(x_0) = \rho(g_kh_i)(x_0).$$

Donc lorsque h parcourt H, $\rho(g_ih)(x_0)$ sera égal à l'un des $\rho(g_ih_j)$ (d'où m possibilités). Donc

$$E_i = \{\rho(g_ih_j)(x_0),\ j = 1, ..., m\}.$$

Si $j \neq j'$,

$$\rho(g_ih_j)(x_0) \neq \rho(g_ih_{j'})(x_0)$$

car sinon

$$(g_i h_j)^{-1}(g_i h_j) \in Gx_0 \quad \text{et} \quad h_j^{-1} h_j \in Gx_0.$$

Contradiction. Donc, s'il existe au moins deux h_i distincts de deux classes différentes, alors E_i a au moins deux éléments distincts. Voyons que c'est effectivement le cas :

$$\operatorname{card}(E_i) = m = [H : G_{x_0}]$$

d'après l'explication ci-dessus, quand h parcourt H. Chaque E_i contient autant d'élément qu'il y a de classes modulo G_{x_0}, soit m éléments.

$$= \frac{|H|}{|G_{x_0}|} \begin{cases} \neq 1 & \text{car } H \supsetneq Gx_0 \text{ par hyp. Donc } \operatorname{card}(E_i) \geq 2 \\ \neq \operatorname{card}(E) & \text{car } \operatorname{card} E = [G : Gx_0] = \frac{|G|}{|Gx_0|} \text{ et que } |H| \neq |G| \\ & \text{toujours par hypothèse. Donc } \operatorname{card}(I) \geq 2. \end{cases} .$$

On a donc les deux critères d'une parition non triviale : $\operatorname{card}(E_i) \geq 2$ et $\operatorname{card}(I) \geq 2$. □

Proposition 2.48. *Soit $\rho : G \to \mathrm{Per}(X)$ une action et soit $x \in X$. Alors ρ est imprimitive $\iff$ il existe H un sous-groupe de G tel que $G(x) \subsetneq H \subsetneq G$.*

Remarque 2.49. La condition ne dépend pas de x. Soit $x' \in X$, il existe $\sigma \in \mathrm{Per}(X)$ *tel que* $\sigma(x) = x'$. Alors $G(\sigma(x)) = \sigma G(x)\sigma^{-1}$.

Démonstration. ($\supset$) Si $\tau \in G(x)$ c'est-à-dire si $\tau.x = x$ soit $\rho(\tau)(x) = \tau$

$$(\sigma\tau\sigma^{-1})(\sigma(x)) = \sigma(x).$$

Donc $\sigma\tau\sigma^{-1} \in G(\sigma(x))$.

($\subset$) Il faut écrire ($\supset$) pour σ^{-1} à la place de σ. Si $G(x) \subsetneq H \subsetneq G$ alors $G(x') \subsetneq \sigma H \sigma^{-1} \subsetneq G$. □

Exemple 2.50. Soit $\gamma : G \to \mathrm{Per}(G)$ une représentation regulière à gauche. Si $x \in G$:

$$G(x) = \{g \in G \,|\, gx = x\} = \{1\}.$$

L'action est imprimitive d'après le critère de la proposition 2.48, il suffit de montrer $H < G$ tel que

$$\{1\} \subsetneq H \subsetneq G,$$

ce qui est possible sauf si $|G|$ premier.

Démonstration. Si $|G|$ n'est pas premier, disons $|G| = d$, il existe $r|d$ et il existe x tel que

$$| < x > | = r,$$

sinon $\forall x$, l'ordre de $| < x > | = d \Rightarrow (x^r)^{d/r} = e$

$$| < x^r > | = d/r < d,$$

(contradiction). □

Proposition 2.51. *Soit $\rho : G \to \mathcal{S}_n$ une action (on suppose ρ transitive). ρ est 2-transitive $\iff$ $G(1)$ agit transitivement sur $\{2, ..., n-1\}$.*

Proposition 2.52. *Soit $\rho : G \to \mathcal{S}_n$ une action. on a ρ 2-transitive $\Rightarrow$ ρ primitive.*

Démonstration de la proposition 2.51. ($\Rightarrow$) Il s'agit de montrer : *pour tout $j \in \{2, ..., n-1\}$, il existe $g(1) \in G$ tel que $g(2) = j$*, c'est-à-dire :

$$g(1) = 1, \qquad g(2) = j.$$

Ce qui est possible par définition 2.41 (de la 2-transitivité).

($\Leftarrow$) Il s'agit de démontrer *pour tout (a, b) avec $a, b \in \{1, ..., n\}$, $a \neq b$, il existe $g \in G$ tel que*

$$\begin{cases} g(1) & = a, \\ g(2) & = b. \end{cases} .$$

L'action est transitive donc il existe $g \in G$ tel que $g(1) = a$. Soit $g(2) = b'$. Par hypothèse, $G(1)$ agit transitivement sur $\{2, ..., n-1\}$ dont il existe $g' \in G(1)$ tel que $g'(b') = b$. On a :

$$\begin{cases} g'g(1) & = g'(a) = a \\ g'g(2) & = g'(b') = b \end{cases} .$$

□

Démonstration de la proposition 2.52. On suppose que ρ 2-transitive.

- ρ est transitive.
- Si ρ est imprimitive, il existe une partition $(E_i)_{i \in I}$ non triviale qui soit invariante par l'action .Soient $a, b \in E_{i_0}$, $a \neq b$, Par la 2-transitivité, il existe $g \in G$ tel que $g(a) \in E_{i_0}$ et $g(b) \notin E_{i_0}$.
  Ce qui contredit l'imprimitivité.

□

Proposition 2.53. *Soit $\rho : G \subset \mathcal{S}_n \to \mathcal{S}_n$ action transitive. On suppose que G* est engendré par des cycles de longueur première. Alors l'action est primitive.

Démonstration. Supposons ρ imprimitive : il existe une partition $(X_i)_{i \in I}$ de $\{1, ..., d\}$ invariante par l'action. Soit g un cycle dans g, soit $i \in \{1, ..., n\}$ quelconque. Supposons $g(X_i) \not\subset X_i$ alors il existe $x_i \in X_i$ tel que $g(x_i) \notin X_i$. Par imprimitivité, on a :

$$g(x) \notin X_i \qquad \text{pour tout } x \in X_i$$

et donc $X_i \subset \text{supp}(g)$ car il n'y a aucun point fixe.

Supposons $g(X_1) \not\subset X_1$, ce qui entraine, d'après ci-dessus, que :

$$X_1 \subset \text{supp}(g) \tag{2.3}$$

Soit $i \neq 1$, on a soit :

$$g(X_i) \neq X_i \tag{2.4}$$

ou bien

$$g|_{X_i} = \text{id} \tag{2.5}$$

En effet, si $g(X_i) = X_i$ et $g|_{X_i} \neq \text{id}$, c'est-à-dire il existe $x \in X_i$ tel que $g(x) \neq x$. Alors

$$\text{supp}(g) = g_{\circlearrowleft}(x) = \{x, g(x), g^2(x), \ldots, g^k(x)\} \subset X_i \quad \text{car } g \text{ est un cycle} \tag{2.6}$$

On en déduit de (2.3) et (2.6) que $X_1 \subset X_i$. Contradiction avec $\{X_i\}_i$, partition de $\{1, \dots, d\}$.

Montrons maintenant (2.5) : si $g(X_i) \neq X_i$ alors, par imprimitivité, $X_i \subset \operatorname{supp}(g)$ et si $g|_{X_i} = \mathrm{id}$ alors $X_i \cap \operatorname{supp}(g) = \emptyset$. Donc on a soit $g(X_i) \neq X_i$, soit $g|_{X_i} = \mathrm{id}$.

Conclusion : $\operatorname{supp}(g)$ *est réunion d'un certain nombre* ≥ 1 *de* X_i :

$$|\operatorname{supp}(g)| = d = k|X_i| \qquad \text{où } d \text{ est premier}$$

Si g est cycle de longueur un nombre premier, cela ne peut pas se produire. Contradiction dans ce cas.

On obtient donc :

$$g(X_i) \subset X_i \quad \text{pour tout } g \text{ cycle de longueur un nombre premier}$$

$$g(X_i) \subset X_i \qquad \text{pour tout } g \in G$$

Ce qui contredit la transitivité de l'action. Donc ρ est primitive. □

Définition 2.54. *Deux actions* $\rho : G \to \mathrm{Per}(X)$ *et* $\rho' : G \to \mathrm{Per}(X')$ *sont dites équivalentes si « les actions sont les mêmes à la numérotation près des éléments de l'ensemble » c'est-à-dire il existe une bijection* $\gamma : X \to X'$ tel que pour tout $g \in G$, *ce diagramme :*

$$\begin{array}{ccc} X & \xrightarrow{\rho(g)} & X \\ {\scriptstyle\gamma}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\gamma} \\ X' & \xrightarrow[\rho'(g)]{} & X' \end{array}$$

commute c'est-à-dire :

$$\rho'(g) \circ \gamma = \gamma \circ \rho(g)$$

(ou autrement si $\rho(g)(x) = y$ *alors* $\rho'(g)(\gamma(x) = \gamma(y))$*).*

Soit G un groupe et soit $H < G$. On a déjà introduit l'action :

$$\begin{array}{rcccl} T\gamma & : & G & \to & \mathrm{Per}(G/H) \\ & & g & \mapsto & \gamma(g) \ : \ G/H \to G/H \\ & & & & \qquad\quad xH \mapsto gxH \end{array}$$

Cette fonction est transitive (dite de translation à gauche sur le classes à gauche).

Proposition 2.55. *Réciproquement si* $\rho : G \to \mathrm{Per}(X)$ *est une action* transitive *alors* ρ *est équivalente à l'action* $T\gamma$ *précédente pour* $H = G_{\rho(x)}$ *(où* $x \in X$*).*

Démonstration. On pose :

$$\begin{array}{rcccl} \gamma & : & G/G(x) & \to & X \\ & & gG(x) & \mapsto & \rho(g)(x) \end{array}$$

On vérifie que γ est :

- bien définie. Si g et g' sont dans la même classe : $g^{-1}g'$ est dans G_x. Donc

$$\begin{aligned} \rho(g^{-1}g')(x) = x &\iff \rho(g^{-1})\rho(g')(x) = x \\ &\iff \rho(g^{-1})(\rho(g')(x)) = x \iff \rho(g'(x)) = \rho(g)(x), \end{aligned}$$

  en composant à gauche par $\rho(g)$. Or : $\gamma(g(G(x)) = \rho(g)(x)$ et $\gamma(g'(G(x))) = \rho(g')(x)$ et ces images sont égales d'après ci-dessus, d'où γ est bien une application.

- injective :

$$\rho(g)(x) = \rho(g')(x) \iff g^{-1}g' \in G(x) \qquad g \in G$$

surjective (transitivité).

$$\begin{array}{ccc} G/G(x) & \xrightarrow{T(g)} & G/G(x) \\ {\scriptstyle\gamma}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\gamma} \\ X & \xrightarrow[\rho(g)]{} & X \end{array}$$

$$\rho'(g) \circ \gamma = \gamma \circ \rho(g)$$

Soit $g'G(x) \in G/G(x)$

$$\rho(g) \circ \gamma(g'G(x)) = \rho(g)(\rho(g')(x) = \rho(gg')(x)$$

$$\gamma \circ T(g)(g'G(x)) = \gamma(gg'G(x)) = \rho(gg')(x)$$

□

Définition 2.56 (Action par conjugaison)**.** *Soit G un groupe. L'application*

$$\begin{array}{rcl} C : G & \to & \mathrm{Per}(G) \\ g & \mapsto & \begin{array}{rcl} C_g : G & \to & G \\ x & \mapsto & gxg^{-1} \end{array} \end{array}$$

définit une action de G sur lui-même.

En effet, C_g est bijective car $(C_g)^{-1} = C_{g^{-1}}$. $g \to C_g$ morphisme car

$$C_{g_1 g_2} = C_{g_1} \circ C_{g_2}.$$

En effet,

$$\begin{aligned} C_{g_1 g_2} &= g_1 g_2 x (g_1 g_2)^{-1} \\ &= g_1 (g_2 x g_2^{-1}) g_1^{-1} = C_{g_1} \circ (C_{g_2})(x). \end{aligned}$$

Remarque 2.57. $C_g \in \mathrm{Aut}(G)$

$$\begin{aligned} C_g(xy) &= gxyg^{-1} \\ &= gxg^{-1}gyg^{-1} = C_g(x)C_g(y) \end{aligned}$$

Pour $x \in G$,

$$O(x) = \text{orbite de } x = \{gxg^{-1},\ g \in G\},$$

classe de conjugaison de x dans G ;

$$G_x = \text{fixateur de } x = \{g \in G,\ gxg^{-1} = x\},$$

commutant de x dans G. On a si G fini

$$\mathrm{card}(O(x)) = \frac{|G|}{|G_x|}$$

Classes de conjugaison de $\mathcal{S}_n$

Soit $w \in \mathcal{S}_n$, la classe de conjugaison de w est

$$\{g\omega g^{-1},\ g \in \mathcal{S}_n\}.$$

Définition 2.58. *On dit que w est de type $1^{r_1}2^{r_2}...n^{r_n}$ si dans la décomposition de w en produit de cycles à supports disjoints figurent*

$$\begin{aligned} &r_1 \text{ points fixes},\\ &r_2 \text{ cycle de longueur } 2,\\ &\vdots\\ &r_n \text{ cycle de longueur } n. \end{aligned}$$

Exemple 2.59.

$$w = (123)(45)(6789)(12\ 13\ 14)$$

est de type $1^2 2^1 3^2 4^1$.

Proposition 2.60. *Deux permutations $w, w' \in \mathcal{S}_n$ sont conjuguées si et seulement si w et w' ont le même type de décomposition en cycles à supports disjoints*

Exemple 2.61 (Dans $\mathcal{S}_8$)**.**

$$2^2.3.1 = \{\text{produits 2-transpositions, un 3-cycle, un point fixe}\}$$

est une classe de conjugaison de $\mathcal{S}_8$.

Lemme 2.62. *Si $c = (x_1, ..., x_n)$ et $g \in \mathcal{S}_n$ alors*

$$gcg^{-1} = (g(x_1), ..., g(x_n)).$$

Démonstration de la proposition 2.60. ($\Rightarrow$) On suppose

$$w' = gwg^{-1} \text{ avec } g \in \mathcal{S}_n.$$

w s'écrit

$$w = \prod_{i=1} c_i,$$

où les c_i sont des cycles de longueur r_i à supports disjoints. On obtient

$$\begin{aligned} w' = gwg^{-1} &= g \prod_{i=1} c_i g^{-1}\\ &= \prod_{i=1} gc_i g^{-1} \rightarrow \text{ cycle de longueur } r_i. \end{aligned} \tag{2.7}$$

Les cycles gc_ig^{-1} de la forme $(g(x_1), \ldots, g(x_2))$ sont de support $g(\text{supp}(c_i))$ qui sont disjoints car g est bijective et les x_i sont distincts. Conclusion : (2.7) est la décomposition de w' en cycle à supports disjoints. Elle est de même type que celle de w.

($\Leftarrow$) On suppose que w et w' sont de même type. On peut donc écrire

$$w = \prod_{i=1} c_i \quad \text{où les } c_i \text{ sont des cycles à support disjoints,}$$
$$w' = \prod_{i=1} c'_i \quad \text{où les } c'_i \text{ sont des cycles à support disjoints,}$$

et où pour chaque $i \in I$, c_i et c'_i sont des cycles de même longueur. On pose

$$c_i = (\underbrace{x_{i_1}, x_{i_2}, ..., x_{i_{n_i}}}_{n_i \text{ éléments}}),$$
$$c'_i = (x'_{i_1}, x'_{i_2}, ..., x'_{i_{n_i}}).$$

On définit un élément $g \in \mathcal{S}_n$ par

$$g(x_{i_j}) = x'_{i_j},$$

pour tout $i \in I$, pour tout $j = 1, ..., n_i$.
Exemple 2.63.

$$w = (123)(45),$$
$$w' = (341)(25),$$
$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}.$$

En utilisant le lemme 2.62, on obtient :

$$\begin{aligned} gwg^{-1} &= g\left(\prod_{i=1} c_i\right) g^{-1} = \prod_{i=1} gc_ig^{-1} \\ &= \prod_{i=1} g(x_{i_1}, ..., x_{i_{n_i}})g^{-1} \\ &= \prod_{i=1} (g(x_{i_1}), ..., g(x_{i_{n_i}})) \\ &= \prod_{i=1} (x'_{i_1}, x'_{i_2}, ..., x'_{i_{n_i}}) \\ &= \prod_{i=1} c'_i = w'. \end{aligned}$$

Conclusion : $gwg^{-1} = w'$.

□

2.3 Produit semi-direct

On se donne deux groupes G et H et une action $\rho : G \to \mathrm{Aut}(H)$.

Définition 2.64. *Le produit semi-direct $H \rtimes G$ est l'ensemble $H \times G$ muni de la loi*

$$(h.g).(h', g') = (h\rho(g)(h'), gg') \in H \times G.$$

On obtient aussi un groupe.

Vérification. – loi interne,
– élément symétrique,

– élément neutre (ρ est un automorphisme donc $\rho(g)(e) = e$),
– associativité

$$\begin{aligned}((h.g).(h',g')).(h'',g'') &= (h\rho(g)(h').\rho(gg')'h''), (gg')g'')\\ (h,g).((h',g').(h'',g'')) &= (h.g).(h'\rho(g')(h''), g'g'')\\ &= (h\rho(g)(h'\rho(g')(h''), g(g'g'')).\end{aligned}$$

On a que $\rho(g)$ est un automorphisme donc

$$\rho(g)(h_1h_2) = \rho(g)(h_1)\rho(g)(h_2).$$

Ainsi,

$$\begin{aligned}\rho(g)(h'\rho(g')(h'')) &= \rho(g)(h')\rho(g)(\rho(g')(h''))\\ &= \rho(g)(h')\rho(gg')(h'').\end{aligned}$$

On a ainsi que le symétrique est :

$$(h,g)^{-1} = (\rho(g^{-1})(h^{-1}), g^{-1}).$$

□

Remarques 2.65. 1. $H \rtimes G$ n'est pas commutatif.

2. Le produit direct $H \times G$ correspond au produit semi-direct où $G \to \mathrm{Aut}(H)$ est l'action triviale, c'est-à-dire $\rho(g) = \mathrm{id}_H$.

Exemple 2.66 (groupe diédral)**.** $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, avec l'action

$$\begin{array}{rccl}\rho & : & \mathbb{Z}/2\mathbb{Z} & \longmapsto & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})\\ & & \dot{0} & \longrightarrow & \mathrm{id}\\ & & \dot{1} & \longrightarrow & -\mathrm{id}\\ & & \dot{s} & \longrightarrow & (-1)^s\,\mathrm{id}\,.\end{array}$$

$$(m,s)(m',s') = (m + (-1)^s m', s + s').$$

Application pour $n = 7$:

$$\begin{aligned}(3,1)(2,1) &= (3-2, 1+1) = (1,0)\\ (2,1)(3.1) &= (2-3, 1+1) = (6,0).\end{aligned}$$

Proposition 2.67. *1. L'application*

$$\begin{array}{rccl}i & : & H & \to & H \rtimes G\\ & & h & \mapsto & (h,1)\end{array}$$

est un isomorphisme *de H sur un sous-groupe* distingué *H' de $H \rtimes G$.*

2. L'applcation

$$\begin{array}{rccl}j & : & G & \to & H \rtimes G\\ & & g & \mapsto & (1,g)\end{array}$$

est un isomorphisme *de G sur un sous-groupe G' de $H \rtimes G$.*

3. *L'application*
$$\begin{array}{rccc} \rho_2 & : & H \rtimes G & \to & G \\ & & (h,g) & \mapsto & g \end{array}$$
est un morphisme surjectif.

4. *De plus, on a :*
$$H \rtimes G = H'G',$$
avec H' est un sous groupe distingué de $H \rtimes G$, G' est un sous-groupe de $H \rtimes G$, $H' \cap G' = \{1\}$ et
$$j(g)i(h)j(g)^{-1} = i(\rho(g)(h)) \quad \text{pour } g \in G,\ h \in H.$$

Démonstration. 1. On montre que i, j et ρ_2 sont des morphismes :

(a) Pour l'application i :
$$\begin{aligned} i(hh') &= (hh', 1), \\ i(h)i(h') &= (h,1)(h',1) = (h\rho(1)(h'), 1.1) = (hh', 1). \end{aligned} \tag{2.8}$$

(b) Pour l'application j, faire la même chose que (2.8).

(c) Pour l'application ρ_2,
$$\begin{aligned} \rho_2((h,g)(h',g')) &= \rho_2(h\rho(g)(h'), gg') = gg' \\ &= \rho_2((h,g))\rho_2((h',g')). \end{aligned}$$

(d) Par contre ρ_1 n'est pas un morphisme :
$$\begin{aligned} \rho_1((h,g)(h'g')) &= \rho_1(h\rho(g)(h'), gg') \\ &= h\rho(g)(h') \\ &\neq hh' = \rho_1(h,g)\rho_1(h',g'). \end{aligned}$$

2. (a) On montre que i et j sont injectives :
$$\begin{aligned} H &\simeq i(H) = H' < H \rtimes G, \\ G &\simeq j(G) = G' < H \rtimes G. \end{aligned}$$

(b) On montre que ρ_2 est surjective.

3. On montre que H' est un sous-groupe distingué de $H \rtimes G$. Soit $(h,1) \in H'$ tel que $h \in H$. Soit $(k,g) \in H \rtimes G$ avec $k \in H$ et $g \in G$). On veut montrer que $(k,g)(h,1)(k,g)^{-1} \in H'$.
$$\begin{aligned} (k,g)(h,1)(k,g)^{-1} &= (k,1)(1,g)(h,1)\Big((k,1)(1-g)\Big)^{-1} \\ &= (k,1)(1,g)(h,1)(1,g)^{-1}(k,1)^{-1} \\ &= (k,1)(\rho(g)(h),g)(1,g^{-1})(k,1)^{-1} \\ &= (k,1)(\rho(g)(h),1)(k,1)^{-1} \in H'. \end{aligned}$$

D'autre part, le calcul montre que
$$j(g)i(h)j(g)^{-1} = i(\rho(g)(h)),$$
donc $H' \lhd H \rtimes G$.

4. Reste à voir que

$$\begin{aligned} H' \cap G' &= \{(1,1)\} \quad \text{(par définition)}, \\ H \rtimes G &= H'G'. \end{aligned} \tag{2.9}$$

(2.9)—($\supset$) évident.
(2.9)—($\subset$) $(h,g) = (h,1)(1,g)$.

□

Remarques 2.68. 1.

$$\begin{array}{ccccccc} H & \xrightarrow{i} & H' & \subset & H \times G & \supset & G' & \xleftarrow{j} & G\,. \\ h & \longmapsto & (h,1) & & & & (1,g) & \longmapsto & g \end{array}$$

2. On identifie H à H' (h à $i(h)$, i à une inclusion) et G à G' (g à $j(g)$, j à une inclusion).
3. Tout élément $(h,g) \in H \rtimes G$ s'écrit

$$(h,g) = (h,1)(1,g) = hg.$$

4. $j(g)i(h)j(g)^{-1} = i(\rho(g)(h))$ donc

$$ghg^{-1} = \rho(g)h.$$

5. Le produit

$$(h,g)(h',g') = (h\rho(g)(h'), gg')$$

se réécrit

$$hg.h'g' = h\rho(g)(h').gg' = h(gh'g^{-1})gg'.$$

Définition 2.69. *On appelle suite exacte (courte), la donnée*

$$1 \xrightarrow{i} H \xrightarrow{f} G \xrightarrow{g} K \xrightarrow{\rho} 1\,, \tag{2.10}$$

où H, G, K sont des groupes, $1 = \{1\}$, $i \in \mathrm{Hom}(1,H)$ avec $i(1) = 1$, $\rho \in \mathrm{Hom}(K,1)$ avec $\rho(k) = 1$, $f \in \mathrm{Hom}(H,G)$, $g \in \mathrm{Hom}(G,K)$ et où l'image d'un morphisme est le noyau du morphisme suivant :

$$\begin{aligned} f(H) = \mathrm{Ker}(g) &\Rightarrow g \circ f = 1, \\ i(1) = \mathrm{Ker}(f) &\iff f \textit{ injective}, \\ g(G) = \mathrm{Ker}(\rho) &\Rightarrow g \textit{ injective}. \end{aligned}$$

Exemples 2.70. 1. Si $K \triangleleft$ G, on a la suite exacte suivante :

$$1 \longrightarrow K \longrightarrow G \longrightarrow G/K \longrightarrow 1\,.$$

2. Si G opère sur H, on a la suite exacte suivante :

$$1 \longrightarrow H \xrightarrow{i} G \rtimes H \xrightarrow{\rho_2} G \longrightarrow 1\,,$$

avec

$$i(H) = H',\ G = \mathrm{Ker}(\rho_2),\ (h,g) \xrightarrow{\rho_2} g.$$

Définition 2.71. *Étant donnée une suite exacte* (2.10)*, on appelle section* un morphisme $s : G \to E$ *tel que* $\rho \circ s = \mathrm{id}_G$*. La suite exacte est dites scindée s'il existe une section.*

Remarque 2.72. Le morphisme ρ est *surjectif*, donc pour $g \in G$, il existe un antécédent $s_g \in E$ de g par ρ (on a $\rho(s_g) = g$). La correspondance :

$$g \to s_g$$

n'est une section que si

$$s_g g' = s_g s_{g'} \quad \text{(morphisme)}.$$

Exemples 2.73.

1. Soit $\rho : G \to \mathrm{Aut}(H)$ donnée par la suite exacte suivante :

$$1 \longrightarrow H \longrightarrow H \rtimes G \underset{\rho}{\overset{s}{\rightleftarrows}} G \longrightarrow 1 .$$

Plus précisément,

$$\begin{array}{rccc} \rho & : & H \rtimes G & \to & G \\ & & (h, g) & \mapsto & g \end{array}$$

et s un morphisme :

$$\begin{array}{rccc} s & : & G & \to & H \rtimes G \\ & & g & \mapsto & (1, g) \end{array} .$$

s est une section.

2. *Exemple d'une suite exacte non scindée.* Soit la suite exacte suivante :

$$0 \longrightarrow 2\mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{\rho} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 .$$

Supposons qu'il existe une section $s : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$

$$0 \xrightarrow{s} 0 \xrightarrow{\rho} 0$$

$$1 \longrightarrow 2 \longrightarrow 0 \neq 1$$

La deuxième ligne se justifie par :

$$s(1 + 1) = s1 + s1 = 4.$$

On aboutit ainsi à une contradiction.

Remarque 2.74. Une section $s : G \to E$ est *toujours injective* si $s(g) = 1_E$ alors

$$\rho(\underbrace{s(g)}_{=g}) = \rho(1_E) = 1_G,$$

d'où $\mathrm{Ker}(s) = \{1_G\}$.

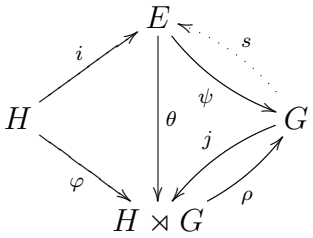
Proposition 2.75. *Étant donnée une suite exacte,*

$$1 \longrightarrow H \xrightarrow{\varphi} E \xrightarrow{\psi} G \longrightarrow 1 ,$$

les assertions suivantes sont équivalentes :

(i) il existe une section $s : G \to E$,

(ii) il existe une action $\rho : G \to \mathrm{Aut}(H)$ et un isomorphisme $\theta : E \to H \rtimes G$ qui rend commutatif le diagramme suivant :



avec

$$\rho \circ \theta = \psi \text{ et } \theta^{-1} \circ \varphi = i.$$

Démonstration. (ii) $\Rightarrow$ (i) On pose $s = \theta^{-1} \circ j$.

– $s \in \mathrm{Hom}(G, E)$

–

$$\begin{aligned} \psi \circ s &= \psi \circ (\theta^{-1} \circ j) \\ &= (\psi \circ \theta^{-1}) \circ j \\ &= \rho \circ j = \mathrm{id}_G . \end{aligned}$$

(i) $\Rightarrow$ (ii) On définit une action $\rho : G \to \mathrm{Aut}(H)$ par $\rho(g)(h) = s(g)hs(g)^{-1}$, avec $g \in G$ et $h \in H$. Autrement dit $\rho(g)$ est la conjugaison sur H par $s(g)$ (*où on identifie $h \in H$ à $\varphi(h) \in G$*). On a bien

$$\rho(g)(H) = H,$$

c'est-à-dire $s(g)Hs(g)^{-1} = H$ car $H = \mathrm{Ker}(\psi) \triangleleft E$. On considère $H \rtimes G$ et on définit :

$$\begin{array}{rccl} \theta & : & E & \to & H \rtimes G \\ & & x & \mapsto & \theta(x) = (x(s(\psi(x))^{-1}), \psi(x)) \end{array},$$

avec $\psi(x) \in G$ et $x(s(\psi(x)))^{-1} \in H = \mathrm{Ker}\,\psi$[1]. On montre que θ est un morphisme, c'est-à-dire $\theta(x_1x_2) = \theta(x_1)\theta(x_2)$.

$$\theta(x_1x_2) = \Big(x_1x_2(s(\psi(x_1x_2)))^{-1}, \psi(x_1x_2)\Big),$$

$$\begin{aligned} \theta(x_1)\theta(x_2) &= \Big(x_1(s(\psi(x_1)))^{-1}, \psi(x_1)\Big).\Big(x_2(s(\psi(x_2)))^{-1}, \psi(x_2)\Big) \\ &= \Big(x_1s(\psi(x_1))^{-1}.s(\psi(x_1))x_2(\psi(x_1))^{-1}s(\psi(x_2))^{-1}, \psi(x_1)\psi(x_2)\Big) \\ &= \Big(x_1x_2s(\psi(x_1))^{-1}s(\psi(x_2))^{-1}, \psi(x_1)\psi(x_2)\Big). \end{aligned}$$

Or

$$x_1x_2s(\psi(x_1))^{-1}s(\psi(x_2))^{-1} = x_1x_2(s(\psi(x_2)\psi(x_1)))^{-1} \text{ et } \psi(x_1x_2) = \psi(x_1)\psi(x_2).$$

[1] En effet (en rappelant que $\psi(s(x)) = x$),

$$\begin{aligned} \psi(xs(\psi(x))^{-1}) &= \psi(x).\psi(s(\psi(x)))^{-1} \\ &= \psi(x)\psi(x)^{-1} = 1. \end{aligned}$$

Donc : θ est un morphisme, on montre maintenant qu'il est bijectif. θ a pour réciproque

$$\begin{array}{rccc} \theta' & : & H \rtimes G & \to & E \\ & & (h,g) & \mapsto & hs(g) \end{array}$$

qui lui aussi est un morphisme :

$$\begin{aligned} \theta'\Big((h_1,g_1),(h_2,g_2)\Big) &= \theta'(h_1 s(g_1) h_2 s(g_1)^{-1}, g_1 g_2) \\ &= h_1 s(g_1) h_2 s(g_1)^{-1}.s(g_1 g_2) \\ &= h_1 s(g_1) h_2 s(g_2) \\ &= \theta'\Big((h_1,g_1)\Big)\theta'\Big((h_2,g_2)\Big). \end{aligned}$$

En effet,

$$\begin{aligned} \theta' \circ \theta(x) &= \theta'(x(s(\psi(x)))^{-1}, \psi(x)) \\ &= xs(\psi(x))^{-1} xs\psi(x) = x \\ \theta \circ \theta'(h,g) &= \theta(hs(g)) = \Big(hs(g)s(\psi(hs(g)))^{-1}, \psi(hs(g))\Big) \\ &= \Big(hs(g)s(\psi(s(g)))^{-1}, \psi(s(g))\Big) = (h,g). \end{aligned}$$

□

Chapitre 3

Théorèmes de Sylow

3.1 p-groupes

Définition 3.1. *Pour p un nombre premier, un p-groupe $\neq \{1\}$ est un groupe dont l'ordre est une puissance de p.*

Proposition 3.2. *Soit P un p-groupe. Si P opère sur un ensemble X fini alors si*

$$X^p = \{\textit{points fixes de l'action}\},$$

on a

$$\operatorname{card}(X^p) \equiv \operatorname{card}(X) \pmod{p}.$$

Démonstration. Utiliser la formule des classes. □

Corollaire 3.3. *Le centre d'un p-groupe P est $\neq \{1\}$.*

Démonstration. On considère l'action

$$\begin{array}{rccl} \rho & : & P & \to & \operatorname{Per}(P) \\ & & g & \mapsto & C_g \ : \ x \to gxg^{-1} \\ & & & & \qquad\ p \mapsto p \end{array}.$$

La proposition 3.2 donne

$$\operatorname{card}(P) \equiv \operatorname{card}(Z(p)) \pmod{p},$$

d'où $\operatorname{card}(Z(G)) = 0 \pmod{p}$. Comme $1 \in Z(G)$, on a $\operatorname{card}(Z(G)) = p$. □

Proposition 3.4. *Soient G un p-groupe et H un sous-groupe d'indice p. Alors $G \rhd H$.*

Démonstration. On considère l'action

$$\begin{array}{rccl} \rho & : & G & \to & \operatorname{Per}(G/H) \\ & & g & \mapsto & \rho(g) : xH \to gxH \end{array} \qquad \text{où } H = \operatorname{Ker}\rho.$$

Par translation à gauche sur les classes à gauche modulo H :

$$G/\operatorname{Ker}(P) \simeq \rho(G) \subset \operatorname{Per}(G/H) \simeq S_P.$$

Donc :

$$\operatorname{card}(G/\operatorname{Ker}(\rho)) = p^\alpha | p!$$

et donc $p^{\alpha-1}|(p-1)!$ que donne :

$$\alpha - 1 = 0 \quad \Longleftrightarrow \quad \alpha = 1.$$

Donc :

$$\text{card}(G/\operatorname{Ker}(\rho)) = p = \text{card}(G/H). \tag{3.1}$$

Or $\operatorname{Ker}(\rho) \subset H$. Combiné à (3.1) qui se réécrit $\text{card}(H) = \text{card}(\operatorname{Ker}\rho)$, cela donne :

$$H = \operatorname{Ker}(\rho) \lhd G.$$

□

On peut ajouter une précision par rapport à (3.1) : $Z(G)$ contient un élément d'ordre p.

Démonstration. Soit $z \in Z(G)$ tel que $z \neq 1$. Cet élément z est d'ordre p^β avec $\beta \geq 1$. Posons alors $x = z^{p^\beta}$, alors $x \in Z(G)$ et est d'ordre p. □

Proposition 3.5. *Soit G un p-groupe d'ordre p^n. Alors il existe une suite de sous-groupe*

$$\{1\} = G_0 \subset G_1 \subset ... \subset G_n = G$$

tel que $\text{card}(G_i) = p^i$*, pour* $i = 0, 1, ..., n$ *et* $G_i \lhd G$.

Démonstration. On fait une démonstration par récurrence sur n.

- Pour $n = 0$, on a $G = \{1\}$.
- Supposons $n \geq 0$. D'après le corollaire 3.3, il existe $x \in Z(G)$ tel que x est d'ordre p. On a : $< x > \lhd G$ (car $x \in Z(G)$). Le groupe $G/ < x >$ est d'ordre p^{n-1}. D'après l'hypothèse de récurrence, il existe une suite :

  $$\{1\} = H_0 \subset H_1 \subset ... \subset H_{n-1} = G/ < x >$$

  de sous-groupes de $G/ < x >$ tel que $\text{card}(H_i) = p^i$ et $H_i \lhd G/ < x >$ pour $i = 0, ..., n-1$. Notons $s : G \to G/ < x >$ la surjection canonique. On pose :

  $$G_i = s^{-1}(H_{i-1}), \qquad i = 1, ..., n.$$

  Posons $G_0 = \{1\}$. On a ainsi

  $$G_0 \subset G_1 \subset ... \subset G_n$$

  tel que $G_i \lhd G$ pour $i = 1, ..., n$.

  $$s^{-1}(H_{i-1}) \lhd s^{-1}(G/ < x >) \iff H_{i-1} \lhd G/ < x > .$$

  On cherche maintenant $\text{card}(G_i)$ pour $i = 1, .., n$. On a $G_i = s^{-1}(H_{i-1})$, c'est-à-dire $s(G_i) = H_{i-1} \Rightarrow G_i/ < x >= H_{i-1}$. Donc $\text{card}(G_i) = \text{card}(H_{i-1}). < x >= p^{i-1}p = p^i$.

□

Proposition 3.6. *Soit G un p-groupe d'ordre p^n. Soit $s < n$ et H un sous-groupe d'ordre p^s. Alors il existe un sous-groupe K d'ordre p^{s+1} tel qe $K \supset H$.*

Démonstration. La preuve de cette proposition se fait par réccurrence sur n. Au rang $n = 0$ et $n = 1$, la propriété est vraie. Soit G d'ordre p^{n+1}, soit $s < n + 1$ et soit H un sous-groupe p^s. Il existe $x \in Z(G)$ d'ordre P.

1er cas Si $x \notin H$ alors $H < x >$ est un sous-groupe (car $x \in Z(G)$) qui contient H et est d'ordre :

$$\frac{\text{card}(H) < x >}{\text{card}(H \cap < x >)} = \frac{p^s p}{1}.$$

2ème cas Si $x \in H$, on a :

$$H < x > / < x > \simeq H/(H \cap < x >) = H/ < x > \text{ sous-groupe de } G/ < x >,$$

$$\text{card}(H/ < x >) = p^{s-1}, \qquad \text{card}(G/ < x >) = p^{n+1-1} = p^n,$$

et $s-1 < n$. D'après l'hypothèse de réccurrence, il existe un sous-groupe $\mathcal{H}/ < x > < G < x >$ (où $\mathcal{H} < G$ et $\mathcal{H} \supset < x >$) tel que $H/ < x > \subset \mathcal{H}/ < x >$ et $\text{card}(\mathcal{H}/ < x >) = p^s$. On a ainsi $\mathcal{H} < G$, $\mathcal{H} \supset H$ et :

$$\text{card}(\mathcal{H}) = p^s.p = p^{s+1}.$$

□

3.2 Théorèmes de Sylow

Soit p un nombre premier.

Définition 3.7. *Si G est un groupe fini d'ordre mp^n où $p \nmid m$, on appelle sous-groupe de Sylow de G, H un sous-groupe de G d'ordre p^n.*

Théorème 3.8 (Théorèmes de Sylow)**.** *Soit $p \mid \text{card}(G)$,*

1. *il existe au moins un p-sous-groupe de Sylow ;*
2. *tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow ;*
3. *tous les p-sous-groupes de Sylow sont conjugués (c'est-à-dire si S et S' sont des p-Sylow, il existe $g \in G$ tel que $s' = gsg^{-1}$) ;*
4. *Le nombre de p-sous-groupes de Sylow divise m et est congru à 1 modulo p.*

3.3 Applications

Théorème 3.9 (Cauchy)**.** *Soit G un groupe fini arbitraire, si $p \mid \text{card}(G)$ alors il existe $g \in G$ d'ordre p.*

Démonstration. On a $\text{card}(G) = p^k m$ avec $k \geq 1$ et $p \nmid m$. Soit un S un p-sylow d'ordre p^k. Soit $y \in S$, $y \neq 1$, y est d'ordre p^l avec $l \leq k$. Alors $g = y^{p^{(l-1)}}$ est d'ordre p. □

Théorème 3.10. *Soient p et q deux nombrees premiers tel que $p > q$. Soit G un groupe d'ordre pq. Alors G est isomorphe au produit semi-direct d'un sous-groupe dinstingué H d'ordre p et d'un sous-groupe K d'ordre q. En particulier, G n'est pas un groupe simple (car $H \triangleleft G$).*

Démonstration. Le nombre de p-Sylow de $G \equiv 1 \bmod p$ et divise q. Donc c'est 1 (puisque $p > q$). *Il existe un unique p-Sylow noté S_p.* Il est automatiquement distingué[1]. On pose $H = S_p$ et on

[1]En effet si $g \in G$, gS_Pg^{-1} est un p-Sylow et donc

$$gS_pg^{-1} = S_p.$$

choisit un q-Sylow K. Alors HK est un sous-groupe d'ordre $\operatorname{card}(H)\operatorname{card}(K)/\operatorname{card}(H\cap K) = pq$. Donc $G = HK$. On a une suite exacte

$$1 \longrightarrow H \longrightarrow HK \underset{}{\overset{s}{\rightleftarrows}} HK/H \longrightarrow 1$$

et $HK/H \simeq K/(H\cap K) = K$. *L'isomorphisme* $s : HK/H \to K \subset HK$ est une section de la suite exacte. D'après la proposition 2.75,

$$HK \simeq H \rtimes KH/H \simeq H \rtimes K.$$

□

Théorème 3.11. *Soient G un groupe fini et S un p-Sylow. On défint* $\operatorname{Nor}_G(S)$, *le* normalisateur *de S dans G :*

$$\operatorname{Nor}_G(S) = \{g \in G,\ gSg^{-1} = S\}.$$

On a :
- $S \subset \operatorname{Nor}_G(S)$,
- $\operatorname{Nor}_G(S) = G \iff S \lhd G$,
- $\operatorname{Nor}_G(S)$ *est un sous-groupe de G.*
- *De plus,* $\operatorname{Nor}_G(S)$ *est* le plus grand *sous-groupe de G qui contient S et dans lequel S est* distingué.

Ainsi :

$$\operatorname{Nor}_G(\operatorname{Nor}_G(S)) = \operatorname{Nor}_G(S).$$

Démonstration. – $\operatorname{Nor}_G(S) \subset \operatorname{Nor}_G(\operatorname{Nor}_G(S))$.
- Soit $n \in \operatorname{Nor}_G(\operatorname{Nor}_G(S))$,

$$\begin{aligned} nSn^{-1} &\subset n\operatorname{Nor}_G(S)n^{-1} \quad \text{car } S \subset \operatorname{Nor}_G(S),\\ &\subset \operatorname{Nor}_G(S). \end{aligned}$$

Le sous-groupe S est un p-Sylow de G qui est contenu dans $\operatorname{Nor}_G(S)$. S est donc aussi un p-Sylow de $\operatorname{Nor}_G(S)$.

$$S \subset \operatorname{Nor}_G(S) \subset G,$$

avec
- S est d'ordre pk,
- Nor_G est d'ordre $p^{k'}m'$ avec $k' \leq k$,
- $\operatorname{card}(G) = p^k n$.

Nécessairement $k' = k$ et S p-Sylow de $\operatorname{Nor}_G(S)$. De même, nSn^{-1} est un p-Sylow de $\operatorname{Nor}_G(S)$. D'après les théorèmes 3.8 de Sylow, S et nSn^{-1} sont conjugués dans $\operatorname{Nor}_G(S)$, c'est-à-dire il existe $h \in \operatorname{Nor}_G(S)$ tel que $nSn^{-1} = hSh^{-1}$ ou encore $h^{-1}nS(h^{-1}n)^{-1} = S$ donc $h^{-1}n \in \operatorname{Nor}_G(S)$. En conclusion

$$n = h.h^{-1}n \in \operatorname{Nor}_G(S),$$

donc $n \in \operatorname{Nor}_G(S)$. □

Chapitre 4

Groupes abéliens, groupes nilpotents, résolubles

4.1 Groupes abéliens

Proposition 4.1. *Soit G un groupe* abélien *d'ordre $m = p_1^{\alpha_1}...p_r^{\alpha_r}$. Alors G est isomorphe au produit direct de ses p-sylows S_i pour $i = 1, ..., r$. De plus, si*

$$\begin{array}{rccc} m_i & : & G & \to & G \\ & & g & \mapsto & p_i^{\alpha_i} g \end{array},$$

$$S_i = \mathrm{Ker}(m_i) = \left(\prod_{j \neq i} p_j^{\alpha_j} \right) G.$$

Démonstration. ($\supset$) On veut montrer que $\mathrm{Ker}(m_i) \subset S_i$. L'inclusion est claire, d'après la proposition 1.17 et la remarque 1.18 car pour un élément $h \in \prod_{j \neq i} p_j \alpha_j$, on a que l'image de h par m_i vaut :

$$p_i^{\alpha_i} = \left(\prod_{j \neq i} p_j^{\alpha_j} \right) g = |G| g = 0.$$

($\supset$) On veut montrer que $S_i \subset \mathrm{Ker}(m_i)$. L'inclusion est claire car $|S_i| = p_i^{\alpha_i}$.
Soit $G_i = \mathrm{Ker}(m_i)$, on considère :

$$\begin{array}{rccc} \phi & : & G_1 \times ... \times G_r & \to & G \\ & & (g_1, ..., g_r) & \mapsto & g_1 + ... + g_r \end{array}.$$

- ϕ est un morphisme.
- ϕ est injective : soit $(g_1, .., g_n) \in \mathrm{Ker}(\phi)$ c'est-à-dire $g_1 + ... + g_r = 0$. On multiplie pour i par $\prod_{j \neq i} p_j^{\alpha^j}$. On obtient

$$\prod_{j \neq i} p_j^{\alpha_j} g_i = 0.$$

car pour $k \neq i$, $g_k \in G_k$ donc s'écrit :

$$\prod_{j \neq k} p_j^{\alpha_j} g', \text{ où } g' \in G,$$

alors en multipliant par $\prod_{j \neq i} p_j^{\alpha_j}$, chaque terme autre que celui en i, contiennent le $\prod_{1 \leq j \leq r} p_j^{\alpha_j} g'$, qui vaut 0, d'après la remarque 1.18. On sait aussi $p_i^{\alpha_i} g_i = 0$ car $g_i \in \mathrm{Ker}(m_i)$, avec $m_i(g) = p_i^{\alpha_i} g$. Par Bezout, il existe $u_i, v_i \in \mathbb{Z}$ tel que

$$u_i \prod_{j \neq i} p_j^{\alpha_j} + v_i p_i^{\alpha_i} = 1.$$

Cela donne $1g_i = 0 + 0$,

$$g_i = 0, \quad i = 1, ..., r,$$

donc $\mathrm{Ker}(\phi) = \{(0, 0, \ldots, 0)\}$.

– ϕ surjectif : les nombres $\prod_{j\neq 1} p_j^{\alpha_j}$, $\prod_{j\neq 2} p_j^{\alpha_j}$, ..., $\prod_{j\neq r} p_j^{\alpha_j}$ sont premiers entre eux. Il existe donc $u_1, .., u_r \in \mathbb{Z}$ tel que

$$u_1 \prod_{j\neq 1} p_j^{\alpha_j} + \cdots + u_r \prod_{j\neq r} p_j^{\alpha_j} = 1.$$

Ce qui donne pour tout $g \in G$,

$$g = u_1 \prod_{j\neq 1} p_j^{\alpha_j} g + \cdots + u_r \prod_{j\neq r} p_j^{\alpha_j} g.$$

Or pour $i = 1, .., r$.

$$\left(\prod_{j\neq i} p_j^{\alpha_j}\right) g \in G_i = \mathrm{Ker}(m_i), \tag{4.1}$$

car $p_i^{\alpha_i} \left(\prod_{j\neq i} p_j^{\alpha_j}\right) .g = |G|g = 0$. D'où ϕ est surjectif. Ainsi ϕ est un isomorphisme.

(4.1) prouve également $G_i \subset \left(\prod_{j\neq i} p_j^{\alpha_j}\right) G$. En effet, pour $g_i \in G_i$, (4.1) s'écrit :

$$g_i = 0 + \cdots + 0 + \left(\prod_{j\neq i} p_j^{\alpha_j}\right) g + 0 + \cdots + 0,$$

d'où $g_i \in \left(\prod_{j\neq i} p_j^{\alpha_j}\right) G$. Donc $G \simeq G_1 \times \cdots \times G_r$. Reste à montrer que $G_i \subset S_i$. On sait que $S_i \subset G_i$ et $|S_i| = p_i^{\alpha_i}$. S'il existe i_0 tel que $S_{i_0} \subset G_{i_0}$, on a :

$$|G| = |G_1 \times ... \times G_r| > p_1^{\alpha_1} \ldots p_r^{\alpha_r} = |G|.$$

car un G_{i_0} contient strictement un S_{i_0}, et S_i est de cardinal $p_i^{\alpha_i}$ pour tout i. D'où la contradiction donc $G_i = S_i$ pour tout i.

□

Définition 4.2. *On dit qu'un groupe fini est nilpotent s'il est isomorphe au produit direct de ses p-Sylows ou de façon équivalente s'il est isomorphe à un produit direct de p-groupes.*

Remarques 4.3.

1. Si un groupe est abélien alors il est nilpotent.
2. Un p-Sylow d'un groupe nilpotent est nécessairement distingué (et donc à p fixé, il n'y a qu'un p-Sylow.

Proposition 4.4. *Si S ($S \lhd S \times T$[1]) est le p-Sylow alors*

1. *$G \simeq S \times T$ (produit des autres p-Sylow),*
2. *$G \lhd S$,*
3. *$S \simeq S \times \{1\}$,*
4. *$S \times T \lhd S \times \{1\}$.*

[1] Soit $s \in S$ et $t \in T$ alors

$$(1, t)(s, 1)(1, t)^{-1} = (s, 1) \in S.$$

Théorème 4.5 (Admis). *(a)* p-groupes abéliens *: Soit G un p-groupe abélien fini. Alors G est isomorphe à un produit de p-groupes cycliques :*

$$\mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_j}\mathbb{Z},$$

avec $\alpha_1 \leq \cdots \leq \alpha_j$. De plus, il y a unicité de $\alpha_1 \leq \cdots \leq \alpha_j$.

(b) groupe abélien *: Soit G un groupe abélien fini. Alors G est isomorphe à un produit direct de groupes cycliques :*

$$\mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z},$$

avec $d_1|d_2$, $d_2|d_3$, ..., $d_{\ell-1}|d_\ell$. De plus, il y a unicité de la suite $d_1, \ldots, d_\ell$.

Exemple 4.6. Soit un groupe G abélien d'ordre $360 = 2^3 \times 3^2 \times 5$. D'après le proposition 4.1, $G \simeq S_2 \times S_3 \times S_5$ (où S_2, S_3 et S_5 sont des Sylows). En utilisant les propositions (a) et (b) du théorème 4.5, on obtient :

possibilité pour S_2	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
possibilité pour S_3	$\mathbb{Z}/9\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	
possibilité pour S_5	$\mathbb{Z}/5\mathbb{Z}$		
possibilité pour G	$\mathbb{Z}/360\mathbb{Z}$[2]		

Remarque 4.7. Avec les notations du théorème 4.5(b),

$$|G| = d_1 \times d_2 \times \cdots \times d_\ell.$$

On définit $\exp(G)$, l'exposant de G qui est le plus petit entier $n \geq 0$ tel que $ng = 0$, pour tout $g \in G$. Ici, $\exp(G) = d_\ell$.

Lemme 4.8 (Lemme chinois). *Si $p_1, \ldots, p_\ell$ sont des nombres premiers distincts 2 à 2 et $\alpha_1, \ldots, \alpha_\ell$ des entiers ≥ 1 alors*

$$\mathbb{Z}/p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{\alpha_\ell}\mathbb{Z}.$$

Attention ! $\mathbb{Z}/p^2\mathbb{Z} \not\simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Démonstration.

$$\begin{array}{ccc} Z & \mapsto & \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \ldots \mathbb{Z}/p_\ell^{\alpha_\ell}\mathbb{Z} \\ n & \to & \overline{n} \pmod{p_1^{\alpha_1}}, \ldots, \overline{n} \pmod{p_\ell^{\alpha_\ell}} \end{array}$$

a pour noyau

$$\{n \in \mathbb{Z},\ p_1^{\alpha_1}|n, \ldots, p_\ell^{\alpha_\ell}|n\} = p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}\mathbb{Z},$$

d'où un morphisme injectif

$$\mathbb{Z}/p_1^{\alpha_1} \ldots p_\ell^{\alpha_\ell}\mathbb{Z} \to \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{\alpha_\ell}\mathbb{Z}$$

qui est un isomorphisme car les p_i-groupes ont le même ordre. On peut voir aussi d'après le théorème 4.5(a) que

$$\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_m^{\alpha_m}\mathbb{Z} \quad \text{avec } \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_m$$

[2]

$$\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \times & \mathbb{Z}/4\mathbb{Z} \\ \mathbb{Z}/3\mathbb{Z} & \times & \mathbb{Z}/3\mathbb{Z} \\ & & \mathbb{Z}/5\mathbb{Z} \\ \hline \mathbb{Z}/6\mathbb{Z} & \times & \mathbb{Z}/60\mathbb{Z} \end{array}$$

et $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \simeq \mathbb{Z}/360\mathbb{Z}$.

est unique et elle détermine le groupe à isomorphisme près, voir l'exemple 4.9. Le même raisonnement peut aussi se faire grâce au théorème 4.5(b) :

$$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_\ell\mathbb{Z} \quad \text{avec } d_1|d_2|\ldots|d_\ell.$$

Il y a unicité de la suite $d_1|d_2|\ldots|d_\ell$ qui détermine le groupe à l'isomorphisme près. □

Exemple 4.9.

$$\underbrace{\mathbb{Z}/3\mathbb{Z}}_{3^1} \times \underbrace{\mathbb{Z}/27\mathbb{Z}}_{3^3} \simeq \underbrace{\mathbb{Z}/9\mathbb{Z}}_{3^2} \times \underbrace{\mathbb{Z}/9\mathbb{Z}}_{3^2}.$$

4.2 Commutateurs et groupes dérivés

Définition 4.10. *Soit G un groupe. Soient H et K deux sous-groupe. On pose :*

$$[H,K] \stackrel{\text{def}}{=} < \{hkh^{-1}k^{-1},\ h \in H,\ k \in K\} >$$

qu'on appelle le groupe des commutateurs de H et K.

Lemme 4.11. *Soient $H, K < G$ et soit $f \in \mathrm{Hom}(G,G)$. On a :*

(i) $[H,K] = [K,H]$,

(ii) $f([H,K]) = [f(H), f(K)]$,

(iii) $H \triangleleft G$ *et* $K \triangleleft G \Rightarrow [H,K] \triangleleft G$,

(iv) $H \sqsubset G$ *et* $K \sqsubset G \Rightarrow [H,K] \sqsubset G$,

(v) $K < \mathrm{Nor}_G(H) \Rightarrow [H,K] \subset H$.

Démonstration. (i) Soient $x \in H$ et $y \in K$

$$xyx^{-1}y^{-1} = (yxy^{-1}x^{-1})^{-1} \in [K,H]^{-1} = [K,H],$$

donc $\{xyx^{-1}y^{-1},\ x \in H, y \in K\} \subset [K,H]$, donc $[H,K] \subset [K,H]$. La démonstration de l'autre inclusion est similaire.

(ii) Soient $x \in H$ et $y \in K$,

$$f(xyx^{-1}y^{-1}) = f(x)f(y)f^{-1}(x)f^{-1}(y).$$

Donc si $A = \{xyx^{-1}y^{-1},\ x \in H, y \in K\}$,

$$f(A) = \{[u,v],\ u \in f(H), v \in f(K)\}.$$

On sait $f(< A >) =< f(A) >$, d'où $f([H,K]) = [f(H), f(K)]$.

(iii) Soient $g \in G$ et C_g l'action intérieur correspondant. D'après (ii),

$$C_g([H,K]) = [C_g(H), C_g(K)] \subset [H,K].$$

(iv) Soit χ une action de G,

$$\chi([H,K]) = [\chi(H), \chi(K)] \subset [H,K].$$

(v) Soit $h \in H$ et soit $k \in K$. On a $hkh^{-1}k^{-1} \in H$.

□

Définition 4.12. *Si G est un groupe, on appelle groupe dérivé, le groupe $D(G) = [G, G] \subset G$.*

Définition 4.13. *Un groupe fini est dit résoluble s'il existe n tel que $D^n(G) = \{1\}$.*

Remarque 4.14. $D(G) \sqsubset G$.

Proposition 4.15. *(a) $D(G)$ est le plus petit sous-groupe distingué de G tel que $G/D(G)$ abélien.*

(b) Si A est un groupe abélien et $\varphi \in \mathrm{Hom}(G, A)$ alors $D(G) \subset \mathrm{Ker}(\varphi)$ et φ se factorise à travers $G/D(G)$.

Démonstration. (a) Soit $H \triangleleft G$, alors

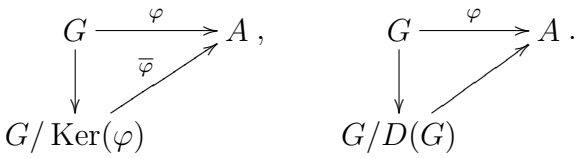
$$G/H \text{ abélien} \iff D(G) \subset H. \tag{4.2}$$

Soient $x, y \in G$ et $\overline{x}, \overline{y}$ leur classe mod H,

$$\begin{aligned} \overline{xy} = \overline{yx} &\iff \overline{xyx}^{-1}\overline{y}^{-1} = 1 \\ &\iff \overline{xyx^{-1}y^1} = 1 \\ &\iff xyx^{-1}y^{-1} \in H \quad \text{(pour tous } x, y \in G\text{)}. \end{aligned}$$

Pour $H = D(G)$, (4.2) montre que $G/D(G)$ est abélien. Si H est un sous-groupe distingué tel que G/H est abélien alors (4.2) montre que $D(G) \subset H$, d'où (a).

(b) $\varphi : G \to A$ induit un morphisme injectif $G/\mathrm{Ker}(\varphi) \to A$. Donc $G/\mathrm{Ker}(\varphi)$ est isomorphe à un sous groupe de A et est donc *abélien*. (4.2) montre que $D(G) \subset \mathrm{Ker}(\varphi)$. On sait alors que φ se factorise par $D(G)$.



□

Définition 4.16. *On pose :*

$$\begin{cases} D_0(G) = G, \\ D_{n+1}(G) = D(D_n(G)). \end{cases}$$

Donc

- $D_1(G) = D(G)$,
- $D_2(G) = D(D(G))$.

Remarques 4.17.

1. $D_n(G) \sqsubset \cdots \sqsubset D_2(G) \sqsubset D_1(G) \sqsubset G$. En particulier, $D_n(G) \sqsubset G$.
2. $D_n(G)/D_{n-1}(G)$ est abélien.

Définition 4.18. *Un groupe G est dit résoluble s'il existe $n \geq 0$ tel que $D_n(G) = \{1\}$.*

Exemples 4.19.

1. Si un groupe est *abélien* alors il est *résoluble*.
2. $\mathcal{D}_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est résoluble. On a, pour $h, h' \in \mathbb{Z}/n\mathbb{Z}$ et $s, s' \in \mathbb{Z}/2\mathbb{Z}$,

$$\begin{aligned} (h, s)(h', s')(h, s)^{-1}(h', s')^{-1} &= (\ldots, s + s - s - s') \\ &= (\ldots, 0). \end{aligned}$$

Ce qui donne $D(\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \subset \mathbb{Z}/n\mathbb{Z}$ et donc $D_2(\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}) \subset D(\mathbb{Z}/n\mathbb{Z}) = \{1\}$.

3. Un groupe G simple résoluble est nécessairement isomorphe à $\mathbb{Z}/p\mathbb{Z}$ avec p premier.

Démonstration. $D(G) \sqsubset G$, donc $D(G) = \{1\}$ ou $D(G) = G$. Si $D(G) = G$ alors $D_n(G) = G$, ce qui est impossible. Donc $D(G) = \{1\}$, c'est-à-dire G abélien. On sait que les groupes abéliens simples sont les groupes $\mathbb{Z}/p\mathbb{Z}$ avec p premier. □

Proposition 4.20. *La classe des groupes résolubles est stable par sous-groupe, par quotient et par produit semi-direct.*

Démonstration.
– Soit $H \subset G$ avec G résoluble. On a $D_n(H) \subset D_n(G)$. Donc si $D_N(G) = \{1\}$ alors $D_N(H) = \{1\}$, d'où H est résoluble.
– Soient G résoluble et $H \triangleleft G$. On a si $s : G \to G/H$ est la surjection canonique :

$$\begin{aligned} D_n(G/H) &= D_n(s(G)) \\ &= s(D_n(G)). \end{aligned} \tag{4.3}$$

Si $D_N(G) = \{1\}$ alors $D_N(G/H) = \{\overline{1}\}$ et donc G/H résoluble. On vérifie tout de même l'égalité (4.3). Pour $n = 1$

$$D(s(G)) = s(D(G))$$

D'après la propriété (ii) du lemme 4.11,

$$[s(G), s(G)] = s([G, G]).$$

On suppose la propriété vraie pour n, on veut la montrer pour $n + 1$:

$$\begin{aligned} D_{n+1}(s(G)) &= D(D_n(s(G)) = D(s(D_n(G))) \qquad \text{(hypothèse de récurrence)} \\ &= s(D(D_n(G))) \\ &= s(D_{n+1}(G)). \end{aligned}$$

– Soit $G \rtimes H$, un produit semi-direct d'un groupe G résoluble et d'un groupe H résoluble. Pour $g, g' \in G$ et $h, h' \in H$,

$$(g, h)(g', h')(g, h)^{-1}(g', h')^{-1} = (\dots, hh'h^{-1}(h')^{-1}).$$

Cela montre que $D(G \rtimes H) = G \rtimes D(H)$. On en déduit $D_n(G \rtimes H) \subset G \rtimes D_n(H)$. Si $D_N(H) = \{1\}$, on obtient $D_N(G \rtimes H) \subset G$. Si $D_M(G) = \{1\}$, $D_{M+N}(G \rtimes H) \subset D_M(G) = \{1\}$, d'où $G \rtimes H$ résoluble.

□

Remarque 4.21. Il est plus généralement vrai que pour G un groupe et $H \triangleleft G$,

$$G \text{ résoluble} \iff H \text{ résoluble et } G/H \text{ résoluble.}$$

Corollaire 4.22. *On a :*

(i) Si un groupe est abélien alors il est nilpotent.

(ii) Si un groupe est nilpotent alors il est résoluble.

Les réciproques sont fausses.

Démonstration. (i) Voir les remarques 4.3.

(ii) Un groupe nilpotent est isomorphe à un produit direct de p-groupes ; Il suffit de montrer qu'un p^2-groupe est résoluble. Soit G un p-groupe d'ordre p^n. On fait une récurrence p^n. Les propriétés sont vraies pour $n = 0$ et $n = 1$. Elle est vraie aussi pour $n = 2$ car tout groupe d'ordre p^ℓ est abélien. Si G est d'ordre p^{n+1}, on sait qu'il existe $H \triangleleft G$ tel que $|H| = p^n$. Ainsi $|G/H| = p$ et donc G/H est cyclique donc abélien, ce qui donne $D(G) \subset H$. Par l'hypothèse de récurrence, H est résoluble donc il existe N tel que $D_N(H) = \{1\}$. D'où $D_{N+1}(G) = \{1\}$.

□

Démonstration des réciproques fausses. (i) On a déjà vu que la réciproque est fausse.
(ii) $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est résoluble et n'est pas nilpotent car s'il était nilpotent $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ serait abélien.

□

Remarque 4.23. Le théorème de Rait-Thompson nous dit que tout groupe d'ordre impaire est résoluble.

Exemple 4.24. Soit $\mathcal{S}_n$ le groupe de n-permutaions et $\mathcal{A}_n$ le groupe alterné.
$n = 5$, $\mathcal{A}_n$ est simple et donc non résoluble. $\mathcal{A}_n$ n'est donc pas nilpotent. $\mathcal{S}_n$ n'est pas résoluble car son sous-groupe $\mathcal{A}_n$ ne l'est pas.
$n = 2$, $\mathcal{A}_2 = \{1\}$ et $\mathcal{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$.
$n = 3$, $\mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$, $\mathcal{S}_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ sont résoluble mais non nilpotent (donc non abélien).
$n = 4$, $\mathcal{A}_4$ est d'ordre $12 = 2^2 \times 3$.

$$\text{3-Sylow} : S_3 = \mathbb{Z}/3\mathbb{Z},$$
$$\text{2-Sylow} : S_2 = \mathbb{Z}/4\mathbb{Z} \text{ ou } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Si $\mathcal{A}_4$ est nilpotent alors $A_4 \simeq S_3 \times S_2$ serait abélien. Donc $\mathcal{A}_4$ n'est pas nilpotent. $\mathcal{S}_4$ est d'ordre 24 :

$$\text{3-Sylow} : S_3 \simeq \mathbb{Z}/3\mathbb{Z},$$
$$\text{2-Sylow} : S_2 \text{ est d'ordre } 8.$$

Si $\mathcal{S}_4$ est nilpotent alors $\mathcal{S}_4 \simeq S_3 \times S_2$ et les élément de S_3 commutent à cause de S_2. Tout 3-cycle est dans un 3-Sylow et tout 2-cycle est dans un 3-Sylow car il existe un 3-cycle et un 2-cycle qui ne commutent pas. Donc $\mathcal{S}_4$ n'est pas nilpotent. On cherche à savoir si $\mathcal{S}_4$ et $\mathcal{A}_4$ sont résolubles. On a :

$$D(\mathcal{A}_4) = V_4 \qquad \text{abélien} \tag{4.4}$$

donc $D_2(\mathcal{A}_4) = \{1\}$ d'où $\mathcal{A}_4$ est résoluble

Démonstration de l'égalité (4.4). ($\subset$) $V_4 \triangleleft \mathcal{A}_4$ et $\mathcal{A}_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$ abélien donne que $D(A_4) \subset \mathcal{A}_4$.
($\supset$) résulte de la formule

$$(xyz)(xyt)(xyz)^{-1}(xyt)^{-1} = (xy)(zt).$$

□

On finit l'exemple en donnant une preuve comme quoi $\mathcal{S}_4$ est résoluble. $D(\mathcal{S}_4) \subset \mathcal{A}_4$ car $s(xyx^{-1}y^{-1}) = s(x)s(y)s(x)^{-1}s(y)^{-1} = 1$, ce qui donne finalement

$$D_3(\mathcal{S}_4) \subset D_2(\mathcal{A}_4) = \{1\}$$

qui montre bien que $\mathcal{S}_4$ est résoluble.