UFR MATHÉMATIQUES
Université Clermont Auvergne

Master de mathématiques
première année

ALGÈBRE 1
Première partie : groupes

Notes de cours de François DUMAS - année 2020-2021

Table des matières

version provisoire du 6 juillet 2020

Ces notes correspondent au programme d'une unité d'enseignement de première année de master. Elles ne constituent pas un cours d'algèbre autonome et complet sur les notions présentées, mais s'insèrent entre le contenu d'enseignements préalables de licence et d'enseignements ultérieurs pour le master ou l'agrégation. Elles incluent donc autour des résultats principaux à fois quelques rappels synthétiques sur des prérequis essentiels et quelques compléments ouvrant sur des prolongements possibles.

Le mode de rédaction n'est pas celui d'un traité, mais de simples notes destinées à servir de support au travail personnel des étudiants, à compléter évidemment par des exercices et des problèmes.

Les ouvrages d'enseignement en français sur ces sujets classiques sont nombreux, et ces notes les utilisent. Citons entre autres :

Serge Lang, *Algèbre*, éditions Dunod,
Patrice Tauvel, *Algèbre (agrégation, master)*, éditions Dunod,
Daniel Perrin, *Cours d'algèbre*, éditions Ellipses,
Collectif (sous la direction de Aviva Szpirglas), *Mathématiques Algèbre*, éditions Pearson,
Jean Delcourt, *Théorie des groupes*, éditions Dunod,
Josette Calais, *Eléments de théorie des groupes*, éditions PUF,
Josette Calais, *Eléments de théorie des anneaux*, éditions PUF,
Jean Querré, *Cours d'algèbre*, éditions Masson,
Daniel Guin, *Algèbre, tome 1 : groupes et anneaux*, éditions Belin.

Ces notes contiennent immanquablement des coquilles ou des erreurs. Merci de m'en faire part.

Francois.Dumas@uca.fr

Chapitre 1

Groupes abéliens finis

1.1 Rappels sur les groupes cycliques

1.1.1 Ordre d'un sous-groupe, ordre d'un élément

Définitions. Un groupe G est dit *fini* lorsqu'il n'a qu'un nombre fini d'éléments. Dans ce cas, le nombre d'éléments de G est appelé l'*ordre* de G. On le note $o(G)$, ou encore $|G|$. C'est un entier naturel non-nul.

Théorème de Lagrange. *Soit H un sous-groupe d'un groupe fini G. Alors H est fini, et l'ordre de H divise l'ordre de G.*

> *Preuve.* Notons $|G| = n$. Il est clair que H est fini. Notons $|H| = m$. Pour tout $x \in G$, notons $xH = \{xy\,;\, y \in H\}$ la classe de x à gauche modulo H. Il est facile de vérifier que l'ensemble des classes xH lorsque x décrit G est une partition de G. Comme chaque classe xH est d'ordre m, on conclut que n est égal au produit de m par le nombre de classes distinctes. □

Proposition et définition. *Soit G un groupe fini. Pour tout $x \in G$ distinct du neutre e, il existe un entier $n \geq 2$ unique tel que :*

$$x^n = e \quad \text{et} \quad x^k \neq e \text{ pour tout } 1 \leq k < n.$$

Le sous-groupe de G engendré par x est alors :

$$\langle x \rangle = \{e, x, x^2, x^3, \ldots, x^{n-1}\}.$$

L'entier n est l'ordre du sous-groupe $\langle x \rangle$ et est appelé l'ordre de l'élément x de G. On le note $|x|$. C'est un diviseur de l'ordre de G. Dans le cas où $x = e$, on a $\langle e \rangle = \{e\}$, et $|e| = 1$.

> *Preuve.* Evidente, laissée au lecteur (voir le cours de L3). □

1.1.2 Groupes isomorphes

Définition. Deux groupes G_1 et G_2 sont dits *isomorphes* lorsqu'il existe un isomorphisme de groupes de l'un sur l'autre.

> • *Remarques.* Lorsque deux groupes sont isomorphes : si l'un est abélien, alors l'autre l'est aussi ; si l'un est fini, l'autre l'est aussi et ils sont de même ordre ; ils ont le même nombre de sous-groupes d'ordre donné ; leurs centres, leurs groupes dérivés, leurs groupes d'automorphismes,... sont isomorphes. Deux groupes finis de même ordre sont isomorphes si et seulement si leur tables sont identiques à une permutation près des éléments.

• *Exemple.* Soit G_1 le groupe des racines quatrièmes de l'unité dans $\mathbb{C}$. On a : $G_1 = \{1, i, -1, -i\}$. La loi de groupe est ici la multiplication des complexes.

Soit G_2 le groupe des rotations affines du plan euclidien conservant un carré. Il est constitué de la rotation r de centre le centre O du carré et d'angle $\frac{\pi}{2}$, de la symétrie centrale s de centre O, de la rotation r' de centre O et d'angle $-\frac{\pi}{2}$, et de l'identité id. On a : $G_2 = \{\mathrm{id}, r, s, r'\}$. La loi de groupe est ici la loi $\circ$ de composition des applications.

Soit G_3 le groupe $\mathbb{Z}/4\mathbb{Z}$ des classes de congruences modulo 4. On a : $G_3 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. La loi de groupe est ici l'addition des classes de congruence.

G_1	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

G_2	id	r	s	r'
id	id	r	s	r'
r	r	s	r'	id
s	s	r'	id	r
r'	r'	id	r	s

G_3	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Il est clair qu'ils sont isomorphes, via les isomorphismes :

$$1 \mapsto \mathrm{id} \mapsto \overline{0}, \qquad i \mapsto r \mapsto \overline{1}, \qquad -1 \mapsto s \mapsto \overline{2}, \qquad -i \mapsto r' \mapsto \overline{3}.$$

• *Exemple.* Il est bien connu (voir cours de L3) qu'il n'existe à isomorphisme près que deux groupes d'ordre 4. L'un est le groupe cyclique d'ordre 4, noté C_4 (voir ci-dessous), l'autre est appelé groupe de Klein, noté V. Les deux sont abéliens.

C_4	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

V	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

D'une part $C_4 = \{e, a, b, c\}$ avec $b = a^2$ et $c = a^3 = a^{-1}$; il contient, outre le neutre d'ordre 1, deux éléments d'ordre 4 et un élément d'ordre 2. D'autre part $V = \{e, a, b, c\}$ avec $b = ac$ et $c = ab$; il contient, outre le neutre d'ordre 1, trois éléments d'ordre 2.

1.1.3 Groupe cyclique

Définition. Un groupe fini est dit *cyclique* lorsqu'il est engendré par un élément.

Remarques.

1. Dire qu'un groupe fini G d'ordre n est cyclique signifie qu'il existe dans G un élément a qui est d'ordre n, de sorte que $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.
2. Un groupe cyclique est nécessairement abélien.
3. Pour tout entier $n \geq 1$, il existe à isomorphisme près un unique groupe cyclique d'ordre n, noté C_n. Ce groupe C_n est isomorphe par exemple au groupe multiplicatif $\mathbb{U}_n$ des racines n-ièmes de l'unité dans $\mathbb{C}$, ou encore au groupe additif $\mathbb{Z}/n\mathbb{Z}$ des classes de congruences modulo n, ou encore à beaucoup d'autres groupes que l'on rencontre dans divers domaines des mathématiques.

Pour certaines valeurs de n, il existe des groupes abéliens non cycliques. On a vu par exemple ci-dessus que pour $n = 4$, le groupe de Klein V n'est pas cyclique puisqu'il ne contient pas d'éléments d'ordre 4. Le théorème suivant montre au contraire que, pour certaines valeurs de n, le groupe C_n est à isomorphisme près le seul groupe d'ordre n.

THÉORÈME. *Tout groupe fini d'ordre premier est cyclique.*

En d'autres termes, pour tout nombre premier p, il existe à isomorphisme près un et un seul groupe d'ordre p, qui est le groupe cyclique (donc abélien) C_p.

> *Preuve.* Soient p un nombre premier et G un groupe d'ordre p. Soit a un élément de G distinct du neutre e. Considérons dans G le sous-groupe $\langle a \rangle$ engendré par a. D'après le théorème de Lagrange, son ordre $|a|$ divise p. Comme p est premier, on ne peut avoir que deux cas : ou bien $|a| = 1$, mais alors $a = e$, ce qui est exclu ; ou bien $|a| = p$, mais alors $\langle a \rangle$ est inclus dans G et de même ordre que G, donc il est égal à G. On conclut que $G = \langle a \rangle$ est cyclique. □

> *Questions.* Soit $C_n = \{e, a, a^2, \ldots, a^{n-1}\}$ le groupe cyclique d'ordre n. Peut-on déterminer parmi ses éléments ceux qui engendrent C_n (outre a bien entendu) ? Peut-on déterminer tous ses sous-groupes ? Prenons par exemple $n = 6$. Dans $C_6 = \{e, a, a^2, a^3, a^4, a^5\}$, les différents éléments engendrent les sous-groupes suivants : $\langle e \rangle = \{e\}$ d'ordre 1, $\langle a^3 \rangle = \{e, a^3\}$ d'ordre 2, $\langle a^2 \rangle = \langle a^4 \rangle = \{e, a^2, a^4\}$ d'ordre 3, et $\langle a \rangle = \langle a^5 \rangle = \{e, a, a^2, a^3, a^4, a^5\}$ d'ordre 6. La dernière égalité provient du fait que $(a^5)^2 = a^4$, $(a^5)^3 = a^3$, $(a^5)^4 = a^2$, et $(a^5)^6 = e$.

Le résultat général est le suivant :

PROPOSITION. *Soit n un entier naturel non-nul. Soit $C_n = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ le groupe cyclique d'ordre n.*

(i) *Pour tout diviseur d de n, il existe un et un seul sous-groupe d'ordre d de C_n ; il est cyclique, engendré par a^k pour $k = \frac{n}{d}$.*

(ii) *Les générateurs de C_n sont tous les éléments a^k tels que k et n sont premiers entre eux.*

> *Preuve.* Repose sur des considérations simples d'arithmétique élémentaire, en particulier le théorème de Bézout pour le point (ii). Laissée au lecteur (voir le cours de L3). □

1.1.4 Produit direct de groupes

PROPOSITION ET DÉFINITION. *Soit r un entier naturel non-nul. Soient $G_1, G_2, \ldots, G_r$ des groupes, d'éléments neutres respectifs $e_1, e_2, \ldots, e_r$. Le produit cartésien :*

$$\prod_{i=1}^{r} G_i = G_1 \times G_2 \times \cdots \times G_r = \{(x_1, x_2, \ldots, x_r),\ x_1 \in G_1,\ x_2 \in G_2, \ldots, x_r \in G_r\}$$

est un groupe pour la loi définie par :

$$(x_1, x_2, \ldots, x_r).(y_1, y_2, \ldots, y_r) = (x_1 y_1, x_2 y_2, \ldots, x_r y_r) \quad \text{pour tous } x_i, y_i \in G_i,\ 1 \leq i \leq r.$$

Ce groupe est appelé le produit direct des groupes G_i. Son élément neutre est $(e_1, e_2, \ldots, e_r)$.

> *Preuve.* Simple vérification, vue en L3 et laissée au lecteur. □

REMARQUES. Il est clair que :

1. le produit direct $\prod_{i=1}^{r} G_i$ est fini si et seulement si G_i est fini pour tout $1 \leq i \leq r$, et l'on a alors $|\prod_{i=1}^{r} G_i| = \prod_{i=1}^{r} |G_i|$;
2. le produit direct $\prod_{i=1}^{r} G_i$ est abélien si et seulement si G_i est abélien pour tout $1 \leq i \leq r$;
3. le produit direct $\prod_{i=1}^{r} G_i$ est isomorphe au produit direct $\prod_{i=1}^{r} G_{\sigma(i)}$ pour tout permutation σ des indices $\{1, 2, \ldots, r\}$.

Rappelons (en l'énonçant seulement dans le cas abélien) le résultat suivant, qui sera utile un peu plus loin.

LEMME. *Soient G_1 et G_2 deux groupes abéliens et $G = G_1 \times G_2$ leur produit direct. Soient $H = G_1 \times \{e_2\}$ et $K = \{e_1\} \times G_2$. Alors :*

(i) *H et K sont deux sous-groupes de G, avec $H \simeq G_1$, $K \simeq G_2$, et $H \cap K = \{(e_1, e_2)\}$;*

(ii) *tout élément $g \in G$ s'écrit de façon unique $g = hk$ avec $h \in H$ et $k \in K$;*

(iii) *$G/H \simeq K \simeq G_2$.*

Preuve. Simple vérification, vue en L3 et laissée au lecteur. □

1.1.5 Produit direct de groupes cycliques

La question étudiée ici est celle de savoir à quelles conditions un produit de groupes cycliques est cyclique.

THÉORÈME (dit théorème des restes chinois). *Soient $G_1, G_2, \ldots, G_r$ des groupes cycliques d'ordres respectifs $n_1, n_2, \ldots, n_r$. Alors, le produit direct $\prod_{i=1}^r G_i$ est cyclique si et seulement si les entiers n_i sont deux à deux premiers entre eux.*

Preuve. Pour tout $1 \leq i \leq r$, notons $G_i = \langle a_i \rangle \simeq C_{n_i}$ avec a_i d'ordre n_i. Posons $G := \prod_{i=1}^r G_i$ et $e = (e_1, e_2, \ldots, e_n)$ son élément neutre. Supposons que les n_i sont deux à deux premiers entre eux. Considérons dans G l'élément $x = (a_1, a_2, \ldots, a_r)$. Quel que soit $k \in \mathbb{Z}$, on a $x^k = e$ si et seulement si $a_i^k = e_i$ pour tout $1 \leq i \leq r$, ce qui équivaut à dire que k est multiple de chaque n_i, et donc de leur ppcm. Or ce ppcm est ici le produit $N := n_1 n_2 \ldots n_r$. Donc $x^N = e$ et $x^k \neq e$ pour tout $1 \leq k < N$. On conclut que l'élément x est d'ordre N dans G. Or on sait que G est formé de N éléments ; on conclut que $G = \langle x \rangle \simeq C_N$. La réciproque est laissée au lecteur (voir cours de L3). □

REMARQUE. Avec les notations multiplicatives utilisées ici, le théorème s'énonce sous la forme :

$$C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r} \simeq C_{n_1 n_2 \ldots n_r} \iff \text{les } n_i \text{ sont deux à deux premiers entre eux.}$$

Avec les notations additives usuelles en arithmétique, le théorème s'énonce sous la forme :

$$\prod_{i=1}^{r} (\mathbb{Z}/n_i\mathbb{Z}) \simeq \mathbb{Z}/(n_1 n_2 \ldots n_r)\mathbb{Z} \iff \text{les } n_i \text{ sont deux à deux premiers entre eux.}$$

LEMME (théorème de Cauchy dans le cas abélien). *Soit G est un groupe fini abélien. Alors, pour tout diviseur premier p de l'ordre de G, il existe un élément de G d'ordre p.*

Preuve. Considérons $x_1, \ldots, x_r$ une famille finie de générateurs de G. Notons G_i le groupe cyclique engendré par x_i pour tout $1 \leq i \leq r$. Parce que G est abélien, l'application $\varphi : \Pi_{i=1}^r G_i \to G$ qui à tout r-uplet $(y_1, y_2, \cdots, y_r)$ associe le produit $y_1 y_2 \cdots y_r$ est un morphisme de groupes surjectif. Donc en utilisant le premier théorème d'isomorphisme sur les groupes (voir cours de L3), l'ordre de G divise l'ordre du groupe produit $\Pi_{i=1}^r G_i$. Donc tout diviseur premier p de $|G|$ divise $|G_i|$ pour un indice $1 \leq i \leq r$ au moins, ce qui implique qu'une puissance de x_i est d'ordre p dans G. □

On verra plus tard au corollaire 4.1.1 que ce résultat reste vrai pour tout groupe fini même non abélien.

1.2 Structure des groupes abéliens finis

1.2.1 Exposant d'un groupe abélien

• *Remarque préliminaire.* On sait d'après le théorème de Lagrange que, dans un groupe fini G, l'ordre de tout élément g (c'est-à-dire l'ordre du groupe cyclique engendré par g) est un diviseur de l'ordre de G. On sait aussi que réciproquement, si d est un diviseur donné de l'ordre de G, il n'existe pas forcément dans G d'élément d'ordre d (par exemple, voir plus loin en 2.1.1, le groupe alterné A_4 d'ordre 12 contient le neutre e qui est d'ordre 1, trois éléments d'ordre 2 qui sont les produits de deux transpositions disjointes, et huit 3-cycles : il ne contient donc pas d'élément d'ordre 4 ni d'ordre 6). D'où le sens de la définition suivante.

Définition. Soit G un groupe fini. On appelle *exposant* de G le plus petit entier strictement positif n tel que $g^n = e$ pour tout $g \in G$.

Propriétés immédiates. Il est clair que :
- ✓ l'exposant de G est le ppcm des ordres des éléments de G,
- ✓ l'ordre de tout élément de G divise l'exposant de G,
- ✓ l'exposant de G est un diviseur de l'ordre de G.

Le groupe alterné A_4 d'ordre 12 est d'exposant 6 et ne contient pas d'élément d'ordre 6 ; c'est un fait qui ne peut pas se produire pour un groupe fini abélien d'après la proposition suivante.

Proposition. *Si G est un groupe fini abélien, alors l'exposant de G est le maximum des ordres des éléments de G ; en particulier, il existe alors au moins un élément de G dont l'ordre est égal à l'exposant de G.*

Preuve. Supposons G abélien fini. Soient g et h deux éléments de G d'ordres respectifs ℓ et m premiers entre eux. D'une part $(gh)^{\ell m} = (g^\ell)^m (h^m)^\ell = e$, donc l'ordre de gh divise ℓm. D'autre part, si k est un entier tel que $(gh)^k = e$, alors l'élément $g^k = h^{-k}$ appartient à la fois au groupe cyclique $\langle g \rangle$ d'ordre ℓ et au groupe cyclique $\langle h \rangle$ d'ordre m, et donc vaut e puisque ℓ et m sont premier entre eux ; il en résulte que k est un multiple de ℓ et un multiple de m, donc un multiple de leur ppcm ℓm. On conclut que l'ordre de gh est égal à ℓm.

Ceci étant, appelons n le maximum des ordres des éléments de G, et g un élément de G dont l'ordre vaut n. Notons par ailleurs N le ppcm des ordres des éléments de G, c'est-à-dire l'exposant de G. Puisque g est d'ordre n, il est clair que n divise N.

Par l'absurde, supposons qu'il existe un élément $h \in G$ dont l'ordre q ne soit pas un diviseur de n. Il existerait alors un nombre premier p et des entiers n', q', α, β tels que $n = p^\alpha n'$ et $q = p^\beta q'$ avec p qui ne divise ni n' ni q', et $\beta > \alpha$. Les élements g^{p^α} et $h^{q'}$ seraient d'ordres respectifs n' et p^β, qui sont premiers entre eux. En appliquant la première étape de la preuve, l'élément $g^{p^\alpha} h^{q'}$ serait dordre $p^\beta n' > n$, ce qui serait contradictoire avec la définition de n. Ainsi l'ordre de tout élément de G divise n, donc n est un multiple du ppcm N. On conclut que $n = N$, ce qui achève la preuve. □

Remarque. *Si G est un groupe fini abélien, alors l'exposant de G a exactement les mêmes diviseurs premiers que l'ordre de G.*

En effet, cela résulte directement du lemme final de 1.1.5 et des propriétés immédiates de l'exposant. □

En d'autres termes, si $|G| = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ est la décompositon de $|G|$ en produit de facteurs premiers, avec $\alpha_i \geq 1$ pour tout $1 \leq i \leq s$, alors l'exposant de G est de la forme $= p_1^{\beta_1} \cdots ps^{\beta_s}$ avec $1 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq s$.

1.2.2 Dual d'un groupe abélien fini

DÉFINITION ET PROPOSITION. *Pour tout groupe fini G (abélien ou non), on appelle caractère de G tout morphisme de groupes de G dans le groupe multiplicatif $\mathbb{C}^*$. Les caractères de G forment un groupe abélien fini appelé le dual de G et noté $\widehat{G}$.*

Preuve. Notons n l'ordre de G. Soit χ un caractère de G. Pour tout $g \in G$, on a $\chi(g)^n = \chi(g^n) = \chi(e) = 1$, ce qui prouve que l'image de χ est un sous-groupe du groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité dans $\mathbb{C}$. L'ensemble $\widehat{G}$ des caractères de G est donc inclus dans l'ensemble $\mathbb{U}_n^G$ des applications de G dans $\mathbb{U}_n$.

Une conséquence de cette observation est que, pour tout $g \in G$, on a $|\chi(g)| = 1$ donc $\chi(g)^{-1} = \overline{\chi(g)}$. En définissant naturellement le produit de deux caractères χ et χ' par $\chi\chi'(g) = \chi(g)\chi'(g)$ pour tout $g \in G$, on obtient sur $\widehat{G}$ une structure de groupe abélien, dont le neutre est le caractère χ_0 qui à tout $g \in G$ associe 1, et tel que l'inverse χ^{-1} d'un caractère χ associe à tout $g \in G$ le complexe $\chi^{-1}(g) = \overline{\chi(g)}$.

Enfin, en rappelant que l'ensemble F^E des applications d'un ensemble fini E dans un ensemble fini F est fini de cardinal $(\operatorname{card} F)^{\operatorname{card} E}$, il est clair que $\widehat{G}$ est fini d'ordre $\leq n^n$. □

LEMME. *Si G est un groupe cyclique, ou plus généralement un produit direct de groupes cycliques, alors le groupe dual $\widehat{G}$ est isomorphe à G.*

Preuve. Supposons que $G \simeq C_n$ est cyclique d'ordre n. Notons $G = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ où a est un générateur de G. Il est clair qu'un caractère χ de G est entièrement déterminé par la donnée de la valeur $\chi(a)$, puisqu'alors $\chi(a^k) = \chi(a)^k$ pour tout élément $a^k \in G$ avec $0 \leq k \leq n-1$. Le morphisme d'évaluation $\widehat{G} \to \mathbb{U}_n, \chi \mapsto \chi(a)$ est donc bijectif, et détermine un isomorphisme entre $\widehat{G}$ et $\mathbb{U}_n$.

Considérons maintenant deux groupes abéliens finis G et H, et leur produit direct $G \times H$. Il est facile de vérifier directement que l'application $\phi : \widehat{G \times H} \to \widehat{G} \times \widehat{H}$ définie par :

$$\phi(\chi)(g,h) = (\chi(g, e_H), \chi(e_G, h)) \text{ pour tout } \chi \in \widehat{G \times H} \text{ et tout } (g,h) \in G \times H$$

est un morphisme de groupes, et qu'il est bijectif de bijection réciproque ϕ^{-1} définie par :

$$\phi^{-1}(\chi_1, \chi_2)(g,h) = (\chi_1(g), \chi_2(h)) \text{ pour tous } (\chi_1, \chi_2) \in \widehat{G} \times \widehat{H} \text{ et tout } (g,h) \in G \times H.$$

On a donc un isomorphisme $\widehat{G \times H} \simeq \widehat{G} \times \widehat{H}$, ce qui achève la preuve en appliquant la première étape. □

Ce lemme est en fait une étape vers le résultat plus général que l'on montrera plus loin en 1.2.3 suivant lequel l'isomorphisme entre G et $\widehat{G}$ est vrai pour tout groupe abélien fini. On a pour cela besoin d'un autre résultat intermédiaire non trivial, qui est le lemme suivant.

LEMME (dit lemme de prolongement des caractères). *Soient G un groupe abélien fini, et H un sous-groupe de G. Alors tout caractère de H se prolonge en un caractère de G. En d'autres termes, l'application canonique de restriction $\widehat{G} \to \widehat{H}$ est surjective.*

Preuve. On procède par récurrence sur l'indice $r = [G : H]$ de H dans G. Rappelons que r est l'ordre du groupe quotient G/H. Si $r = 1$, alors $H = G$ et le résultat est clair. Supposons $r \geq 2$ et supposons le résultat du lemme vrai pour tous les sous-groupes d'indice strictement inférieur à r. Comme $H \neq G$, on peut choisir un élément $g \in G$ tel que $g \notin H$. Soit K le sous-groupe de G engendré par H et par g. Le principe de la preuve consiste à construire pour tout caractère χ de H un caractère χ' de K prolongeant χ. Puisque $[G : K] < [G : H] = r$,

on peut alors appliquer à K l'hypothèse de récurrence pour prolonger χ' en un caractère χ'' de G.

Comme G/H est d'ordre r, on a $g^r \in H$; notons m le plus petit entier strictement positif tel que $g^m \in H$, c'est-à-dire l'ordre de $\overline{g}$ dans G/H, qui divise donc r. Puisque $g^m \in H$, on peut considérer $\omega = \chi(g^m) \in \mathbb{C}^*$. Tout élément de $k \in K$ peut s'écrire sous la forme $k = hg^\ell$ avec $h \in H$ et ℓ entier tel que $0 \leq \ell < m$. Cette écriture est unique car si $hg^\ell = h'g^{\ell'}$, alors $g^{\ell-\ell'} = h'h^{-1} \in H$, d'où $\ell - \ell' = 0$ par minimalité de m, et finalement $\ell = \ell'$ et $h = h'$. On pose alors $\chi'(k) = \chi'(hg^\ell) = \chi(h)\zeta^\ell$ où ζ désigne une racine m-ième de ω arbitrairement choisie, ce qui définit bien une application $\chi' : K \to \mathbb{C}^*$ dont la restriction à H est χ.

Pour montrer que χ' un morphisme de groupes, considérons deux éléments quelconques $k, k' \in K$. Il existe $h, h' \in H$ et $\ell, \ell' \in \{0, 1, \ldots, m-1\}$ tels que $k = hg^\ell$ et $k' = h'g^{\ell'}$. Parce que G est abélien, on a $kk' = hh'g^{\ell+\ell'}$. Deux cas sont possibles. Si $0 \leq \ell + \ell' < m$, on calcule directement :

$$\chi'(kk') = \chi'(hh'g^{\ell+\ell'}) = \chi(hh')\zeta^{\ell+\ell'} = \chi(h)\chi(h')\zeta^\ell\zeta^{\ell'} = \chi(h)\zeta^\ell\chi(h')\zeta^{\ell'} = \chi'(k)\chi'(k').$$

Si $m \leq \ell + \ell' < 2m$, alors $0 \leq \ell + \ell' - m < m$, et on calcule en utilisant le fait que $g^m \in H$:

$$\chi'(kk') = \chi'(hh'g^{\ell+\ell'}) = \chi'(hh'g^m g^{\ell+\ell'-m}) = \chi(hh'g^m)\zeta^{\ell+\ell'-m} = \chi(h)\chi(h')\chi(g^m)\zeta^{\ell+\ell'-m},$$

puis comme $\chi(g^m) = \zeta^m$:

$$\chi'(kk') = \chi(h)\chi(h')\zeta^m\zeta^{\ell+\ell'-m} = \chi(h)\chi(h')\zeta^{\ell+\ell'} = \chi'(k)\chi'(k').$$

On a ainsi montré que χ' est un caractère de K qui prolonge χ. On applique l'hypothèse de récurrence pour conclure, comme indiqué au début de la preuve, qu'il existe un caractère χ'' de G dont la restriction à K est χ', et donc dont la restriction à H est χ. □

1.2.3 Théorème de Kronecker

THÉORÈME ET DÉFINITION. *Soit G un groupe abélien fini d'ordre $n \geq 2$. Il existe un unique entier $r \geq 1$ et des entiers $d_1, \ldots, d_r \geq 2$ uniques, dont le produit vaut n, et qui vérifient :*

(1) *d_i divise d_{i+1} pour tout $1 \leq i \leq r-1$,*

(2) *G est isomorphe au produit direct de groupes cycliques $C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r}$.*

On dit que ces entiers $d_1, d_2, \ldots, d_r$, qui caractérisent G à isomorphisme près, forment la suite des facteurs invariants de G.

Preuve : On procède par récurrence sur l'ordre de G. Si G est d'ordre 2, alors $G \simeq C_2$ et le résultat est évident. Considérons maintenant un groupe G d'ordre $n \geq 3$ et supposons le théorème vrai pour tout groupe d'ordre strictement inférieur à n.

Désignons par d l'exposant de G. D'après la proposition 1.2.1, il existe dans G un élément x d'ordre d. Le groupe cyclique $H = \langle x \rangle$ est isomorphe au sous-groupe $\mathbb{U}_d$ de $\mathbb{C}^*$. Prenons un isomorphisme de groupes $\chi : H \to \mathbb{U}_d$; c'est en particulier un caractère de H. D'après le second lemme de 1.2.2, il existe un caractère $\widetilde{\chi}$ de G prolongeant χ. Parce que d'après la proposition 1.2.1 tout élément de G est d'ordre divisant d, le caractère $\widetilde{\chi}$ est en fait à valeurs dans $\mathbb{U}_d$; il définit donc un morphisme de groupes $\widetilde{\chi} : G \to \mathbb{U}_d$. Ceci permet d'introduire l'application :

$$\begin{array}{rccc} \phi & : & G & \to & (G/H) \times H \\ & & g & \mapsto & (\overline{g}\,,\, \chi^{-1} \circ \widetilde{\chi}(g)) \end{array}.$$

Il est clair que ϕ est un morphisme de groupes. Soit $g \in \operatorname{Ker}\phi$. On a $\overline{g} = \overline{e}$ c'est-à-dire $g \in H$, donc $\widetilde{\chi}(g) = \chi(g)$, donc $\chi^{-1}(\widetilde{\chi}(g)) = g$, d'où $g = e$. Ainsi ϕ est injectif. Les groupes finis G

et $(G/H) \times H$ étant de même ordre, cela suffit pour déduire que ϕ est bijectif, et détermine donc un isomorphisme de groupes de G sur $(G/H) \times H$.

Puisque $|G/H| < |G|$, l'hypothèse de récurrence implique l'existence d'entiers $d_1, d_2, \ldots, d_{r-1}$ supérieurs ou égaux à 2 tels que d_i divise d_{i+1} et $G/H \simeq C_{d_1} \times C_{d_2} \times \cdots \times C_{d_{r-1}}$. On pose de plus $d_r = d$. Comme $H \simeq C_{d_r}$, il vient :

$$G \simeq (G/H) \times H \simeq C_{d_1} \times C_{d_2} \times \cdots \times C_{d_{r-1}} \times C_{d_r}.$$

Il est clair que, si l'on désigne par a un générateur du groupe $C_{d_{r-1}}$ et par e_i l'élément neutre de C_{d_i} pour tout $1 \leq i \leq r$, l'élément $(e_1, e_2, \ldots, e_{r-2}, a, e_r)$ est d'ordre d_{r-1}. On a déjà vu que l'ordre de tout élément de G divise l'exposant d_r, donc ici d_{r-1} divise d_r, ce qui achève la preuve de l'existence de la décomposition.

Pour l'unicité, supposons qu'il existe un isomorphisme de groupes θ de G sur un produit de groupes cycliques $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s}$ avec $s \geq 1$ et n_i qui divise n_{i+1} pour tout $1 \leq i \leq s-1$. Pour tout $1 \leq i \leq s$, notons a_i un générateur de C_{n_i} et e_i l'élément neutre de C_{n_i}. Il est clair que l'élément $(e_1, \ldots, e_{s-1}, a_s$ est d'ordre n_s dans K. De plus $a_i^{n_s} = e_i$ pour tout $1 \leq i \leq s$ puisque n_i divise n_s ; il en résulte que tout élément de K est d'ordre inférieur ou égal à n_s. En d'autres termes n_s est l'exposant de K. On en déduit via l'isomorphisme θ que $n_s = d_r$ et donc :

$$C_{d_1} \times C_{d_2} \times \cdots \times C_{d_{r-1}} \times C_{d_r} \simeq C_{n_1} \times C_{n_2} \times \cdots \times C_{n_{s-1}} \times C_{d_r},$$

d'où il résulte par passage au quotient (voir point (iii) du lemme 1.1.4) que :

$$C_{d_1} \times C_{d_2} \times \cdots \times C_{d_{r-1}} \simeq C_{n_1} \times C_{n_2} \times \cdots \times C_{n_{s-1}}.$$

L'hypothèse de récurrence permet alors de conclure que $s - 1 = r - 1$ et $n_i = d_i$ pour tout $1 \leq i \leq r-1$, ce qui achève la preuve. □

COROLLAIRE. *Pour tout groupe abélien fini G , le groupe dual $\widehat{G}$ est isomorphe à G.*

Preuve. Résulte immédiatement du théorème précédent et du premier lemme de 1.2.2. □

1.2.4 Facteurs invariants et diviseurs élémentaires

► En utilisant le théorème ci-dessus et le théorème des restes chinois, on déduit par exemple qu'il existe à isomorphisme près quatre groupes abéliens d'ordre 36, qui sont :

$$C_{36} \simeq C_9 \times C_4, \qquad C_3 \times C_{12} \simeq C_3 \times C_3 \times C_4,$$
$$C_2 \times C_{18} \simeq C_2 \times C_2 \times C_9, \qquad C_6 \times C_6 \simeq C_3 \times C_3 \times C_2 \times C_2 \simeq C_6 \times C_3 \times C_2,$$

ou encore que tous les groupes abéliens d'ordre ≤ 12 sont, à isomorphisme près, donnés par :

$n = 1$	C_1		
$n = 2$	C_2		
$n = 3$	C_3		
$n = 4$	C_4	$C_2 \times C_2$	
$n = 5$	C_5		
$n = 6$	$C_6 \simeq C_2 \times C_3$		

$n = 7$	C_7		
$n = 8$	C_8	$C_2 \times C_4$	$C_2 \times C_2 \times C_2$
$n = 9$	C_9	$C_3 \times C_3$	
$n = 10$	$C_{10} \simeq C_2 \times C_5$		
$n = 11$	C_{11}		
$n = 12$	$C_{12} \simeq C_3 \times C_4$	$C_2 \times C_6 \simeq C_2 \times C_2 \times C_3$	

► Plus généralement, si l'on considère un groupe abélien fini G donné par sa décomposition suivant les facteurs invariants $d_1, \ldots, d_r$, on peut décomposer chaque groupe cyclique C_{d_i} en produit de groupes cycliques dont l'ordre est une puissance d'un nombre premier. En notant $d_i = \prod_j p_j^{\alpha_{i,j}}$ la décomposition en facteurs premiers de d_i, les entiers $d_{ij} = p_j^{\alpha_{i,j}}$ s'appellent les *diviseurs élémentaires* de G. *Le théorème des restes chinois permet de passer de la décomposition suivant les facteurs invariants à la décomposition suivant les diviseurs élémentaires et réciproquement.*

Sans formaliser d'énoncé sur ce point, donnons quelques exemples.

Considérons le groupe $G = C_{54} \times C_{360}$ d'ordre 19440. On a $C_{54} \simeq C_2 \times C_{27}$ et $C_{360} \simeq C_8 \times C_9 \times C_5$. La suite des diviseurs élémentaires de G est $2, 2^3, 3^2, 3^3, 5$. On en déduit les facteurs invariants $d_1 = 2 \times 3^2 \times 5^0 = 18$ qui divise $d_2 = 2^3 \times 3^3 \times 5 = 1080$, d'où la décomposition $G \simeq C_{18} \times C_{1080}$.

Soit G un groupe abélien d'ordre 360. On déduit de $360 = 2^3 \times 3^2 \times 5$ les différentes possibilités pour les diviseurs élémentaires et les facteurs invariants de G ; à isomorphisme prés, six cas sont possibles :

$$\begin{aligned} C_8 \times C_9 \times C_5 &\simeq C_{360} \\ C_8 \times C_3 \times C_3 \times C_5 &\simeq C_3 \times C_{120} \\ C_2 \times C_4 \times C_9 \times C_5 &\simeq C_2 \times C_{180} \\ C_2 \times C_4 \times C_3 \times C_3 \times C_5 &\simeq C_6 \times C_{60} \\ C_2 \times C_2 \times C_2 \times C_9 \times C_5 &\simeq C_2 \times C_2 \times C_{90} \\ C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5 &\simeq C_2 \times C_6 \times C_{30} \end{aligned}$$

Citons pour finir à titre d'exemple une autre application du théorème de Kronecker, qui est la version simple (dans le cas des groupes abéliens) d'un résultat important de la théorie des caractères pour les groupes finis quelconques.

1.2.5 Espace hermitien des fonctions complexes sur un groupe abélien fini

Soit G un groupe fini. On note $\mathbb{C}^G$ l'ensemble des applications de G dans $\mathbb{C}$. C'est de façon évidente un espace vectoriel de dimension finie $n = |G|$. Il est bien connu et facile de vérifier que $\mathbb{C}^G$ est muni d'un produit hermitien défini par :

$$\langle \varphi, \psi \rangle = \tfrac{1}{|G|} \sum_{g \in G} \overline{\varphi(g)} \psi(g), \quad \text{pour tous } \varphi, \psi \in \mathbb{C}^G.$$

PROPOSITION. *Soit G un groupe fini. Avec les notations ci-dessus :*

(i) *le groupe dual $\widehat{G}$ est une famille orthonormale dans $\mathbb{C}^G$;*

(ii) *si de plus G est abélien, le groupe dual $\widehat{G}$ est une base orthonormale de $\mathbb{C}^G$.*

Preuve. Rappelons (voir 1.2.2) que, dans le groupe $\widehat{G}$:

$$\begin{cases} \text{l'élément neutre } \chi_0 \text{ est le caractère constant égal à 1,} \\ \text{l'inverse } \chi^{-1} \text{ d'un caractère } \chi \text{ est égal au conjugué } \overline{\chi} \text{ de } \chi. \end{cases}$$

Pour tous $\chi, \chi' \in \widehat{G}$, on a $\langle \chi, \chi' \rangle = \langle \chi_0, \overline{\chi}\chi' \rangle = \langle \chi_0, \chi^{-1}\chi' \rangle$. Comme $\langle \chi_0, \chi_0 \rangle = 1$, il suffit pour montrer (i) de vérifier que $\langle \chi_0, \chi \rangle = 0$ pour tout $\chi \in \widehat{G}$ distinct de χ_0.

Soit donc χ un caractère de G distinct de χ_0. Il existe $h \in G$ tel que $\chi(h) \neq 1$. On calcule :

$$\chi(h)\langle \chi_0, \chi \rangle = \chi(h) \tfrac{1}{|G|} \sum_{g \in G} \chi(g) = \tfrac{1}{|G|} \sum_{g \in G} \chi(h)\chi(g) = \tfrac{1}{|G|} \sum_{g \in G} \chi(hg) = \tfrac{1}{|G|} \sum_{g' \in G} \chi(g').$$

Donc $\chi(h)\langle \chi_0, \chi \rangle = \langle \chi_0, \chi \rangle$, d'où $\langle \chi_0, \chi \rangle = 0$, ce qui montre le résultat voulu.

Puisque la famille formée des éléments de $\widehat{G}$ est orthonormale, elle est libre. Si l'on suppose de plus que G est abélien, il résulte du corollaire 1.2.3 que le cardinal de cette famille est égale à $|G|$, qui n'est autre que la dimension de $\mathbb{C}^G$, de sorte $\widehat{G}$ est une base de $\mathbb{C}^G$. □

Chapitre 2

Rappels et compléments sur les groupes non abéliens

2.1 Exemples de références

2.1.1 Groupes symétriques

PROPOSITION ET DÉFINITION. *Pour tout entier $n \geq 1$, l'ensemble des bijections d'un ensemble fini à n éléments sur lui-même est un groupe fini d'ordre $n!$ pour loi $\circ$. On l'appelle le n-ième groupe symétrique et on le note S_n. Les éléments de S_n sont appelés les permutations sur n éléments.*

Preuve. Vue en L3 ; à réviser. □

EXEMPLE. Pour $n = 1$, le groupe S_1 est le groupe trivial $\{e\}$ d'ordre 1. Pour $n = 2$, le groupe S_2 est d'ordre 2, donc $S_2 = C_2 = \{e, \tau\}$ où $e = \left(\begin{smallmatrix}1&2\\1&2\end{smallmatrix}\right)$ et $\tau = \left(\begin{smallmatrix}1&2\\2&1\end{smallmatrix}\right)$, qui vérifie bien $\tau^2 = e$.

EXEMPLE. Pour $n = 3$, le groupe S_3 est d'ordre 6. On a : $S_3 = \{e, \gamma, \gamma^2, \tau_1, \tau_2, \tau_3\}$ avec :

$$e = \left(\begin{smallmatrix}1&2&3\\1&2&3\end{smallmatrix}\right), \quad \gamma = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right), \quad \gamma^2 = \left(\begin{smallmatrix}1&2&3\\3&1&2\end{smallmatrix}\right), \quad \tau_1 = \left(\begin{smallmatrix}1&2&3\\1&3&2\end{smallmatrix}\right), \quad \tau_2 = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right), \quad \tau_3 = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right).$$

	e	γ	γ^2	τ_1	τ_2	τ_3
e	e	γ	γ^2	τ_1	τ_2	τ_3
γ	γ	γ^2	e	τ_3	τ_1	τ_2
γ^2	γ^2	e	γ	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	γ	γ^2
τ_2	τ_2	τ_3	τ_1	γ^2	e	γ
τ_3	τ_3	τ_1	τ_2	γ	γ^2	e

Le groupe S_3 n'est pas abélien. C'est le plus petit groupe non abélien (car les groupes d'ordre 2, 3 ou 5 sont abéliens car cycliques d'après le théorème 1.1.3, et les deux seuls groupes d'ordre 4 sont abéliens comme on l'a rappelé en 1.1.2.

Il admet trois sous-groupes d'ordre 2 qui sont $\{e, \tau_1\}$, $\{e, \tau_2\}$ et $\{e, \tau_3\}$, et un sous-groupe d'ordre 3 qui est $\{e, \gamma, \gamma^2\}$.

DÉFINITION. On appelle *transposition* de S_n toute permutation τ qui échange deux éléments i et j en laissant fixe les $n - 2$ autres. On note alors $\tau = [i, j]$. On a de façon évidente $\tau^2 = e$.

THÉORÈME. *Toute permutation de S_n est un produit de transpositions. En d'autres termes, le groupe S_n est engendré par ses transpositions.*

Preuve. Vue en L3 ; à réviser. On pourra procéder par récurrence sur n. □

• *Remarque.* Il n'y a pas unicité de la décomposition d'une permutation en produit de transpositions. Par exemple, dans S_4, on a $[2,4][1,4][4,2][1,3] = [2,3][1,2]$. Néanmoins, on a le lemme suivant.

THÉORÈME ET DÉFINITIONS.

(i) *Si une même permutation σ de S_n se décompose d'une part en un produit de m transpositions, d'autre part en un produit de m' transpositions, alors les entiers naturels m et m' sont de même parité. On appelle signature de σ le nombre $(-1)^m$, où m désigne le nombre de transpositions d'une décomposition quelconque de σ en produit de transpositions. On la note $\varepsilon(\sigma)$.*

(ii) *L'application signature $\varepsilon : S_n \to \{-1, 1\}$ est un morphisme de groupes.*

(iii) *L'ensemble des permutations de signature 1 (ie. qui se décomposent en un nombre pair de transpositions) est un sous-groupe de S_n appelé groupe alterné, noté A_n, d'ordre $\frac{n!}{2}$.*

Preuve. Vue dans le cours de L3. A réviser. □

EXEMPLE. Pour $n = 2$, on a $A_2 = \{e\}$. Pour $n = 3$, on a $A_3 = \{e, \gamma, \gamma^2\}$ avec $\gamma = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$.

EXEMPLE. Pour $n = 4$, le groupe alterné A_4 est d'ordre 12.

Le groupe A_4 contient les trois produits de deux transpositions disjointes :

$$a = [1,2][3,4] = \left(\begin{smallmatrix}1&2&3&4\\2&1&4&3\end{smallmatrix}\right), \quad b = [1,3][2,4] = \left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right), \quad c = [1,4][2,3] = \left(\begin{smallmatrix}1&2&3&4\\4&3&2&1\end{smallmatrix}\right).$$

Il contient aussi les huit permutations qui permutent circulairement trois éléments i, j, k en fixant le quatrième, et qui sont donc de la forme $[i,k][i,j]$. De tels éléments sont appelés des 3-cycles.

$$x_1 = \left(\begin{smallmatrix}1&2&3&4\\1&3&4&2\end{smallmatrix}\right), \quad y_1 = \left(\begin{smallmatrix}1&2&3&4\\1&4&2&3\end{smallmatrix}\right) = x_1^2, \quad x_2 = \left(\begin{smallmatrix}1&2&3&4\\3&2&4&1\end{smallmatrix}\right), \quad y_2 = \left(\begin{smallmatrix}1&2&3&4\\4&2&1&3\end{smallmatrix}\right) = x_2^2,$$
$$x_3 = \left(\begin{smallmatrix}1&2&3&4\\2&4&3&1\end{smallmatrix}\right), \quad y_3 = \left(\begin{smallmatrix}1&2&3&4\\4&1&3&2\end{smallmatrix}\right) = x_3^2, \quad x_4 = \left(\begin{smallmatrix}1&2&3&4\\2&3&1&4\end{smallmatrix}\right), \quad y_4 = \left(\begin{smallmatrix}1&2&3&4\\3&1&2&4\end{smallmatrix}\right) = x_4^2.$$

	e	a	b	c	x_1	y_1	x_2	y_2	x_3	y_3	x_4	y_4
e	e	a	b	c	x_1	y_1	x_2	y_2	x_3	y_3	x_4	y_4
a	a	e	c	b	x_3	x_4	y_3	y_4	x_1	x_2	y_1	y_2
b	b	c	e	a	y_4	x_2	y_1	x_3	y_2	x_4	y_3	x_1
c	c	b	a	e	y_2	y_3	x_4	x_1	y_4	y_1	x_2	x_3
x_1	x_1	y_4	y_2	x_3	y_1	e	c	x_4	x_2	a	b	y_3
y_1	y_1	y_3	x_4	x_2	e	x_1	x_3	b	c	y_4	y_2	a
x_2	x_2	x_4	y_3	y_1	b	y_4	y_2	e	a	x_1	x_3	c
y_2	y_2	x_3	x_1	y_4	y_3	c	e	x_2	x_4	b	a	y_1
x_3	x_3	y_2	y_4	x_1	x_4	a	b	y_1	y_3	e	c	x_2
y_3	y_3	y_1	x_2	x_4	c	y_2	y_4	a	e	x_3	x_1	b
x_4	x_4	x_2	y_1	y_3	a	x_3	x_1	c	b	y_2	y_4	e
y_4	y_4	x_1	x_3	y_2	x_2	b	a	y_3	y_1	c	e	x_4

Les trois éléments a, b, c sont d'ordre 2, et le sous-groupe $V = \{e, a, b, c\}$ de A_4 est le groupe de Klein.

Les huit 3-cycles x_i, y_i pour $1 \leq i \leq 4$ sont d'ordre 3. On obtient donc quatre sous-groupes cycliques $G_i = \{e, x_i, y_i\}$, pour $1 \leq i \leq 4$.

On observe au passage que, bien que 4 et 6 soient des diviseurs de $|A_4| = 12$, le groupe A_4 ne contient pas d'élément d'ordre 4 ni 6, puisqu'il est formé de huit éléments d'ordre 3, trois éléments d'ordre 2, et du neutre e d'ordre 1.

On montrera plus loin que, non seulement A_4 n'admet pas d'élément d'ordre 6, mais qu'il n'admet en fait pas de sous-groupe d'ordre 6 ; en revanche, A_4 admet le sous-groupe V d'ordre 4 bien qu'il n'admette pas d'élément d'ordre 4.

2.1.2 Groupes diédraux

EXEMPLE. Soit $\mathbb{D}_6$ le sous-groupe des isométries du plan affine euclidien conservant un triangle équilatéral (ABC).

On montre aisément que $\mathbb{D}_6$ est formé de l'identité e, de la rotation r de centre l'isobarycentre O de (ABC) et d'angle $2\pi/3$, de la rotation r^2 de centre O et d'angle $4\pi/3$, et des réflexions s_1, s_2, s_3 par rapport aux trois médianes (ou hauteurs) du triangle (faire un dessin !).

Il est clair que $\mathbb{D}_6$ est isomorphe au groupe symétrique S_3.

	e	r	r^2	s_1	s_2	s_3
e	e	r	r^2	s_1	s_2	s_3
r	r	r^2	e	s_3	s_1	s_2
r^2	r^2	e	r	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	r	r^2
s_2	s_2	s_3	s_1	r^2	e	r
s_3	s_3	s_1	s_2	r	r^2	e

EXEMPLE. Soit $\mathbb{D}_8$ le sous-groupe des isométries du plan affine euclidien conservant un carré $(ABCD)$.

On montre que $\mathbb{D}_8$ est formé de l'identité e, de la rotation r de centre le centre O du carré et d'angle $\pi/2$, de la symétrie centrale r^2 de centre O, de la rotation r^3 de centre O et d'angle $3\pi/2$, des réflexions s_1, s_2 par rapport aux deux médianes du carré, et des réflexions t_1, t_2 par rapport aux deux diagonales (faire un dessin).

On a $t_1 = rs_1$, $s_2 = r^2 s_1$, $t_2 = r^3 s_1$, donc $\mathbb{D}_8$ est engendré par les deux éléments r et s_1.

	e	r	r^2	r^3	s_1	s_2	t_1	t_2
e	e	r	r^2	r^3	s_1	s_2	t_1	t_2
r	r	r^2	r^3	e	t_1	t_2	s_2	s_1
r^2	r^2	r^3	e	r	s_2	s_1	t_2	t_1
r^3	r^3	e	r	r^2	t_2	t_1	s_1	s_2
s_1	s_1	t_2	s_2	t_1	e	r^2	r^3	r
s_2	s_2	t_1	s_1	t_2	r^2	e	r	r^3
t_1	t_1	s_1	t_2	s_2	r	r^3	e	r^2
t_2	t_2	s_2	t_1	s_1	r^3	r	r^2	e

DÉFINITION. Pour tout entier $n \geq 2$, on appelle groupe diédral d'ordre $2n$, noté $\mathbb{D}_{2n}$, le sous-groupe des isométries affines conservant un polygone régulier à n côtés.

On montre en géométrie que $\mathbb{D}_{2n}$ est formé de $2n$ éléments distincts :

$$\mathbb{D}_{2n} = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\},$$

engendré par deux éléments r et s vérifiant les relations :

$$r^n = e, \qquad s^2 = e, \qquad sr^k = r^{n-k}s \quad \text{pour tout } 1 \leq k \leq n.$$

CONVENTION. Dans le cas $n = 2$, $\mathbb{D}_4$ est le groupe des isométries conservant un segment ; il est clair que $\mathbb{D}_4$ est isomorphe au groupe de Klein V.

2.1.3 Exemple de groupe quaternionique

EXEMPLE. Le sous-ensemble Q_8 de $\mathrm{GL}_2(\mathbb{C})$ formé des huit matrices :

$$e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \quad -e = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \quad j = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right),$$
$$-j = \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right), \quad k = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \quad -k = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right),$$
$$\ell = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right), \quad -\ell = \left(\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix}\right).$$

est un groupe, d'ordre 8, non abélien, appelé *groupe des quaternions.*

	e	$-e$	j	$-j$	k	$-k$	ℓ	$-\ell$
e	e	$-e$	j	$-j$	k	$-k$	ℓ	$-\ell$
$-e$	$-e$	e	$-j$	j	$-k$	k	$-\ell$	ℓ
j	j	$-j$	$-e$	e	ℓ	$-\ell$	$-k$	k
$-j$	$-j$	j	e	$-e$	$-\ell$	ℓ	k	$-k$
k	k	$-k$	$-\ell$	ℓ	$-e$	e	j	$-j$
$-k$	$-k$	k	ℓ	$-\ell$	e	$-e$	$-j$	j
ℓ	ℓ	$-\ell$	k	$-k$	$-j$	j	$-e$	e
$-\ell$	$-\ell$	ℓ	$-k$	k	j	$-j$	e	$-e$

Le groupe Q_8 n'est pas isomorphe à $\mathbb{D}_8$; en effet Q_8 ne contient qu'un élément d'ordre 2, alors que $\mathbb{D}_8$ en contient cinq.

2.2 Groupes quotients

2.2.1 Classes modulo un sous-groupe, indice d'un sous-groupe

RAPPELS. Soit G un groupe. Soit H un sous-groupe. Pour tout $x \in G$, on note :

$$xH = \{xh\,;\, h \in H\} \quad \text{et} \quad Hx = \{hx\,;\, h \in H\}.$$

1. Le sous-ensemble xH s'appelle la *classe à gauche* de x modulo H. Le sous-ensemble Hx s'appelle la *classe à droite* de x modulo H. Pour tout $x \in G$, H est équipotent à xH via la bijection $h \mapsto xh$ de H sur xH, et à Hx via la bijection $h \mapsto hx$ de H sur Hx.

2. En particulier, pour $x = e$, on a : $eH = He = H$.

3. On vérifie (rappeler la démonstration) que les classes à gauche forment une partition de G, de même que les classes à droite.

4. On démontre ensuite (faites-le) que l'ensemble des classes à droite modulo H est équipotent à l'ensemble des classes à gauche modulo H via la bijection $Hx \mapsto x^{-1}H$.

DÉFINITION. Soient G un groupe et H un sous-groupe de G. On appelle *indice de H dans G*, noté $[G : H]$, le cardinal de l'ensemble des classes modulo H (à droite ou à gauche). On dit que H est d'indice fini lorsque ce cardinal est fini.

REMARQUE. Si G est un groupe fini, alors tout sous-groupe H de G est d'indice fini dans G, et on a d'après le théorème de Lagrange l'égalité :

$$|G| = |H| \times [G : H].$$

A noter qu'un sous-groupe infini H d'un groupe infini G peut très bien être d'indice fini (prendre par exemple $G = \mathrm{O}_n(\mathbb{R})$ et $H = \mathrm{SO}_n(\mathbb{R})$).

2.2.2 Sous-groupe normal

Les notions rappelées ici ont été vues en L3. On ne redonne pas ici les démonstrations : les reprendre en exercice.

DÉFINITION. Soient G un groupe et H un sous-groupe de G. On dit que H est *normal dans G*, ou encore *distingué dans G*, lorsque, pour tout $x \in G$, on a : $xH = Hx$. On note alors $H \triangleleft G$.

REMARQUES (deux autres traductions équivalentes de la définition).

- L'égalité $xH = Hx$ ne signifie par que $xh = hx$ pour tout $h \in H$, mais que, pour tout $h \in H$, il existe $h' \in H$ tel que $xh = h'x$ et $h'' \in H$ tel que $hx = xh''$. On en déduit donc la caractérisation pratique suivante :
$$H \triangleleft G \quad \Leftrightarrow \quad \forall\, h \in H,\ \forall\, x \in G,\ xhx^{-1} \in H.$$

- Pour tout $x \in G$, notons $xHx^{-1} = \{xhx^{-1}\,;\, h \in H\}$. Si $xHx^{-1} \subset H$ pour tout $x \in G$, alors $H \subset yHy^{-1}$ pour tout $y \in G$, puisque tout $h \in H$ peut s'écrire $h = y(y^{-1}hy)y^{-1}$. On en déduit donc la caractérisation suivante :
$$H \triangleleft G \quad \Leftrightarrow \quad \forall\, x \in G,\ xHx^{-1} = H.$$

Remarque terminologique. On dit parfois sous-groupe *distingué* pour sous-groupe normal : les deux termes sont absolument synonymes.

Exemples généraux de sous-groupes normaux

1. Quel que soit le groupe G, les sous-groupes $\{e\}$ et G sont toujours des sous-groupes normaux de G.
2. Si G est abélien, tout sous-groupe de G est normal dans G.
3. Tout sous-groupe d'indice 2 dans un groupe G est normal dans G.
4. Pour tout morphisme $f : G \to G'$ d'un groupe G dans un groupe G', le noyau $\operatorname{Ker} f$ est normal dans G.
5. Si $H \lhd G$ et $K \lhd G$, alors $H \cap K \lhd G$.

Exemples d'applications.

• *Exemple.* Pour tout $n \geq 2$, le groupe alterné A_n est normal dans le groupe symétrique S_n. Cela résulte du point 4 ci-dessus puisque A_n est le noyau du morphisme signature, ou encore du point 3 puisque $[S_n : A_n] = 2$.

• *Exemple.* Considérons le groupe symétrique $S_3 = \{e, \gamma, \gamma^2, \tau_1, \tau_2, \tau_3\}$, avec les notations de 2.1.1. Le sous-groupe $A_3 = \{e, \gamma, \gamma^2\}$ est normal dans S_3 comme on vient de le voir. Les trois sous-groupes $H_i = \{e, \tau_i\}$ pour $i = 1, 2, 3$ ne sont pas normaux dans S_3 car, par exemple pour $i = 1$, on a $\gamma\tau_1\gamma^{-1} = \gamma\tau_1\gamma^2 = \gamma\tau_3 = \tau_2 \notin H_1$.

• *Exemple.* Considérons le groupe diédral $\mathbb{D}_{2n} = \{e, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$, avec les notations de 2.1.2. Le sous-groupe cyclique $C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$ est normal dans $\mathbb{D}_{2n}$ car d'indice 2. Dès lors que $n > 2$, le sous-groupe $K = \{e, s\}$ n'est pas normal dans $\mathbb{D}_{2n}$ car $r^{-1}sr = r^{-1}r^{n-1}s = r^{n-2}s \notin K$. A noter que pour $n = 2$, le sous-groupe K est normal puisque $\mathbb{D}_4$ est le groupe de Klein donc abélien.

• *Exercice.* Montrer que le groupe des quaternions Q_8 admet un sous-groupe d'ordre 2 et trois sous-groupes d'ordre 4, et que tous ses sous-groupes sont normaux dans Q_8.

Attention. Soient G un groupe, H et K deux sous-groupes de G tels que K soit un sous-groupe de H. Donc $K \subset H \subset G$. On peut avoir K normal dans H et H normal dans G sans avoir K normal dans G.

Exemple : plaçons-nous dans le groupe alterné A_4, en reprenant toutes les notations 2.1.1. Observons d'abord (écrivez les détails !) que :

pour toute permutation $\sigma \in S_4$ et toute transposition $[i, j]$, on a : $\sigma[i, j]\sigma^{-1} = [\sigma(i), \sigma(j)]$.

Considérons dans A_4 le sous-groupe $V = \{e, a, b, c\}$. Pour tout $\sigma \in A_4$, on a :

$$\sigma a\sigma^{-1} = \sigma[1, 2][3, 4]\sigma^{-1} = \sigma[1, 2]\sigma^{-1}\sigma[3, 4]\sigma^{-1} = [\sigma(1), \sigma(2)][\sigma(3), \sigma(4)] \in V.$$

On montre de même que $\sigma b\sigma^{-1} \in V$ et $\sigma c\sigma^{-1} \in V$ pour tout $\sigma \in A_4$. On conclut que $V \lhd A_4$.

Considérons dans A_4 le sous-groupe $K = \{e, a\}$ de V, donc de A_4. Il n'est pas normal dans A_4, car par exemple, $x_1 a x_1^{-1} = x_1 a y_1 = b \notin K$.

Et pourtant K est évidemment normal dans V puisque V est abélien.

2.2.3 Quotient d'un groupe par un sous-groupe normal

THÉORÈME ET DÉFINITION. *Soient G un groupe et H un sous-groupe normal dans G.*

(i) *La relation $\sim_H$ définie sur G par :*

$$\text{pour tous } x, y \in G, \quad x \sim_H y \quad \Leftrightarrow \quad xy^{-1} \in H,$$

est une relation d'équivalence.

(ii) *Pour tout $x \in G$, la classe d'équivalence $\overline{x}$ de x pour la relation $\sim_H$ est :*

$$\overline{x} = xH = Hx.$$

En particulier, la classe du neutre e est $\overline{e} = H$.

(iii) *La loi de composition interne définie sur l'ensemble quotient $G/\sim_H = \{\overline{x}\,;\, x \in G\}$ par :*

$$\overline{x}.\overline{y} = \overline{xy} \quad \text{pour tous } x, y \in G,$$

est bien définie (indépendamment des représentants choisis) et munit $G/\sim_H$ d'une structure de groupe. On l'appelle le groupe quotient de G par le sous-groupe normal H. On le note G/H.

(iv) *L'application $\pi : G \to G/H$ qui, à tout élément $x \in G$ associe sa classe $\overline{x}$ est un morphisme de groupes surjectif, appelé surjection canonique.*

(v) *Si H est d'indice fini, alors G/H est d'ordre fini, et $|G/H| = [G : H]$.*

En particulier, si G est fini, alors G/H est d'ordre fini, et $|G/H| = \frac{|G|}{|H|}$.

Preuve. Le point (v) résulte directement de la remarque du 2.2.1 ci-dessus. Les points (i) à (iv) ont été démontrés dans le cours de L3 (en reprendre la preuve dans le détail).

Insistons seulement sur le fait que, dans le point (iii), le fait crucial est que la loi de groupe sur G/H est bien définie. L'idée naturelle pour définir la loi interne dans G/H est de poser $\overline{x}.\overline{y} = \overline{xy}$ pour tous $\overline{x}, \overline{y} \in G/H$. Mais il est indispensable pour cela constitue une définition que le produit de deux classes ainsi défini ne dépende pas des représentants x et y choisis. En d'autres termes, si l'on prend d'autres représentants $x' \in \overline{x}$ et $y' \in \overline{y}$, (et il n'y a aucune raison alors pour que $xy = x'y'$) est-il clair que $\overline{xy} = \overline{x'y'}$? C'est effectivement le cas comme le montrent les calculs ci-dessous.

Supposons que $x' \in \overline{x}$ et $y' \in \overline{y}$. Alors $x'x^{-1} \in H$ et $y'y^{-1} \in H$. On a :

$$(x'y')(xy)^{-1} = x'y'y^{-1}x^{-1} = x'y'y^{-1}(x')^{-1}x'x^{-1} = \big[x'(y'y^{-1})(x')^{-1}\big]x'x^{-1}.$$

Or, $y'y^{-1} \in H$ par hypothèse et donc, parce que H est supposé normal dans G (c'est là qu'intervient cette hypothèse fondamentale), on a aussi $x'(y'y^{-1})(x')^{-1} \in H$. Finalement comme par ailleurs $x'x^{-1} \in H$, on conclut que $[x'(y'y^{-1})(x')^{-1}]x'x^{-1}$ appartient à H comme produit de deux éléments de H. On a ainsi vérifié que $(x'y')(xy)^{-1} \in H$, donc $\overline{xy} = \overline{x'y'}$. □

EXEMPLES DE GROUPES QUOTIENTS.

• *Exemple.* Considérons le groupe diédral $\mathbb{D}_{2n} = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\}$, et son sous-groupe normal $C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$. Les deux classes modulo C_n sont :

$$\overline{e} = C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\} \quad \text{et} \quad \overline{s} = sC_n = \{s, sr, sr^2, sr^3, \ldots, sr^{n-1}\},$$

car il est clair que deux éléments quelconques de la forme sr^k et sr^ℓ sont équivalents modulo C_n puisque $sr^k(sr^\ell)^{-1} = sr^k r^{-\ell}s^{-1} = sr^{k-\ell}s = ssr^{n-(k-\ell)} = r^{n-k+\ell} \in C_n$. Le groupe quotient $\mathbb{D}_{2n}/C_n = \{\overline{e}, \overline{s}\}$ est donc le groupe à deux éléments. On écrit : $\mathbb{D}_{2n}/C_n \simeq C_2$.

• *Exemple.* Considérons le groupe des quaternions $Q_8 = \{e, -e, j, -j, k, -k, \ell, -\ell\}$. On a vu en exercice en 2.2.2 que le sous-groupe $H = \{e, -e\}$ est normal. Les classes modulo H sont :

$$\overline{e} = H = \{e, -e\}, \quad \overline{j} = jH = \{j, -j\}, \quad \overline{k} = kH = \{k, -k\}, \ \ \overline{\ell} = \ell H = \{\ell, -\ell\}.$$

Le groupe quotient $Q_8/H = \{\overline{e}, \overline{j}, \overline{k}, \overline{\ell}\}$ est d'ordre 4. Comme $(\overline{j})^2 = (\overline{k})^2 = (\overline{\ell})^2 = \overline{-e} = \overline{e}$, on conclut que Q_8/H est isomorphe au groupe de Klein. On écrit $Q_8/H \simeq V$.

• *Exercice.* Montrer que le sous-groupe $V = \{e, a, b, c\}$ de A_4 est normal dans S_4, et que le groupe quotient S_4/V est isomorphe à S_3 ; (voir fin de 2.1.1 et fin de 2.2.2).

THÉORÈME (dit premier théorème d'isomorphisme). *Soient G et G' deux groupes, et $f : G \to G'$ un morphisme de groupes. Alors le groupe quotient de G par le sous-groupe normal* $\operatorname{Ker} f$ *est isomorphe au sous-groupe* $\operatorname{Im} f = f(G)$ *de G'. On note :*

$$G/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

Preuve (à connaître). Posons $H = \operatorname{Ker} f$. Le principe est de construire une application $\overline{f} : G/H \to \operatorname{Im} f$ en posant $\overline{f}(\overline{x}) = f(x)$ pour tout $\overline{x} \in G/H$.

On commence par montrer que $\overline{f}$ est bien définie, indépendamment des représentants choisis. Pour cela, prenons deux éléments x et x' représentants de la même classe dans G/H, c'est-à-dire tels que $\overline{x} = \overline{x'}$. On a alors $x' \sim_H x$, ou encore $x'x^{-1} \in H = \operatorname{Ker} f$, d'où $f(x'x^{-1}) = e_{G'}$, donc $f(x')f(x)^{-1} = e_{G'}$, et finalement $f(x') = f(x)$ dans $\operatorname{Im} f$. Ce qui permet bien de poser $\overline{f}(\overline{x}) = f(x) = f(x') = \overline{f}(\overline{x}')$.

$\overline{f}$ est un morphisme de groupe car, pour tous $x, y \in G$, on a : $\overline{f}(\overline{x}.\overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$.

Par construction, $\overline{f}$ est surjective car tout élément y de $\operatorname{Im} f$ est de la forme $y = f(x)$ pour au moins un élément $x \in G$, et il existe donc $\overline{x} \in G/H$ tel que $y = \overline{f}(\overline{x})$.

Pour l'injectivité, montrons que $\operatorname{Ker} \overline{f} = \{\overline{e}\}$. Soit donc $\overline{x} \in G/H$ tel que $\overline{f}(\overline{x}) = e_{G'}$. Cela signifie que $f(x) = e_{G'}$, c'est-à-dire $x \in \operatorname{Ker} f$. Mais $x \in H$ est équivalent à $\overline{x} = H = \overline{e}$, ce qui achève la preuve. □

EXEMPLES D'APPLICATION.

• *Exemple.* Soit $n \geq 2$ un entier. Soit $\varepsilon : S_n \to \{-1, 1\}$ le morphisme signature. On a $A_n = \operatorname{Ker} \varepsilon \lhd S_n$. Comme ε est clairement surjectif (il existe dans S_n des permutations de signature -1 et des permutations de signature 1), on a $\operatorname{Im} \varepsilon = \{-1, 1\}$. On conclut que $S_n/A_n \simeq \{-1, 1\}$. On écrit : $S_n/A_n \simeq C_2$.

• *Exemple.* Soit $\mathbb{U}$ le groupe multiplicatif des nombres complexes de module 1. L'application $t \mapsto \exp it$ définit un morphisme de groupes surjectif $f : \mathbb{R} \to \mathbb{U}$, dont le noyau est $\operatorname{Ker} f = 2\pi\mathbb{Z}$. On a donc : $\mathbb{R}/2\pi\mathbb{Z} \simeq \mathbb{U}$. Fixons un entier $n \geq 1$. L'application $k \mapsto \exp \frac{2ik\pi}{n}$ définit un morphisme de groupes $g : \mathbb{Z} \to \mathbb{U}$, de noyau $\operatorname{Ker} g = n\mathbb{Z}$, dont l'image est le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité, de sorte que $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{U}_n$.

• *Exercice.* En utilisant le morphisme déterminant, montrer que :

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R}^* \quad \text{et} \quad \mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}) \simeq C_2.$$

2.2.4 Centre, automorphismes intérieurs, groupe dérivé

On regroupe ici trois notions générales relatives aux groupes quotients qui seront utiles dans la suite. On ne reprend pas ici les démonstrations ; certaines ont été détaillées en L3, d'autres pourront être cherchées en travaux dirigés ou comme exercices personnels.

1. *Centre.* Soit G un groupe.
   (i) On appelle centre de G, noté $Z(G)$, l'ensemble des éléments de G qui commutent avec tous les éléments de G :
   $$Z(G) = \{g \in G\,;\, \forall\, x \in G,\ xg = gx\}.$$
   Le centre $Z(G)$ est un sous-groupe de G, abélien, et normal dans G.
   (ii) Si le groupe $G/Z(G)$ est monogène, alors le groupe G est abélien.

2. *Automorphismes intérieurs.* Soit G un groupe.
   (i) On note $\operatorname{Aut} G$ le groupe des automorphismes du groupe G, pour la loi $\circ$. Pour tout $g \in G$, l'application $\gamma_g : G \to G$ définie par :
   $$\forall\, x \in G,\ \gamma_g(x) = gxg^{-1},$$
   est un élément de $\operatorname{Aut} G$. On l'appelle l'automorphisme intérieur déterminé par g. On note $\operatorname{Inn} G$ l'ensemble des automorphismes intérieurs de G :
   $$\operatorname{Inn} G = \{\gamma_g\,;\, g \in G\}.$$
   $\operatorname{Inn} G$ est un sous-groupe de $\operatorname{Aut} G$, normal dans $\operatorname{Aut} G$.
   (ii) L'application $g \mapsto \gamma_g$ est un morphisme de groupes de G dans $AutG$ et l'on a :
   $$G/Z(G) \simeq \operatorname{Inn} G.$$

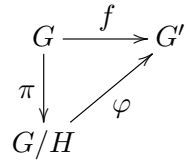
3. *Groupe dérivé et abélianisé.* Soit G un groupe.
   (i) On appelle groupe dérivé de G, noté $D(G)$, le sous-groupe de G engendré par les commutateurs d'éléments de G, c'est-à-dire par tous les éléments de la forme $xyx^{-1}y^{-1}$, avec $x, y \in G$. On a : $D(G)$ est normal dans G, et $G/D(G)$ est abélien.
   (ii) Plus généralement, pour tout sous-groupe H normal dans G, le groupe quotient G/H est abélien si et seulement si $D(G) \subseteq H$.

2.2.5 Propriété universelle du groupe quotient

Le premier théorème d'isomorphisme est un cas particulier du résultat plus général suivant.

Théorème (dit propriété universelle du groupe quotient). *Soient G un groupe, H un sous-groupe normal dans G, et $\pi : G \to G/H$ la surjection canonique.*

(i) *Pour tout groupe G' et tout morphisme de groupes $f : G \to G'$ tel que $H \subseteq \operatorname{Ker} f$, il existe un unique morphisme de groupes $\varphi : G/H \to G'$ tel que $f = \varphi \circ \pi$.*



(ii) *Avec les données ci-dessus, on a de plus :*

$$(\ f \text{ surjectif } \Rightarrow\ \varphi \text{ surjectif }) \quad \text{et} \quad (\ H = \operatorname{Ker} f\ \Rightarrow\ \varphi \text{ injectif }).$$

Preuve. Pour tout $\overline{x} \in G/H$, posons $\varphi(\overline{x}) = f(x) \in G'$. Montrons que cette définition est indépendante du choix du représentant dans $\overline{x}$. Pour cela, considérons $y \in G$ tel que $\overline{y} = \overline{x}$; on a par définition $xy^{-1} \in H$. Puisque $H \subseteq \operatorname{Ker} f$, on déduit que $xy^{-1} \in \operatorname{Ker} f$, donc $f(xy^{-1}) = e$ d'où $f(x)f(y)^{-1} = e'$, c'est-à-dire $f(x) = f(y)$, ou encore $\varphi(\overline{x}) = \varphi(\overline{y})$. On définit donc bien une application :

$$\begin{aligned} \varphi :\ G/H &\longrightarrow G' \\ \overline{x} &\longmapsto f(x) \end{aligned}$$

qui, par définition, vérifie $\varphi \circ \pi = f$ puisque $\varphi(\pi(x)) = \varphi(\overline{x}) = f(x)$ pour tout $x \in G$. Il est clair que φ est un morphisme de groupes car pour tous $\overline{x}, \overline{y} \in G/H$ on a $\varphi(\overline{x}.\overline{y}) = \varphi(\overline{xy}) = f(xy) = f(x)f(y) = \varphi(\overline{x})\varphi(\overline{y})$. Il reste à montrer l'unicité de φ. Soit donc ψ un morphisme $G/H \to G'$ tel que $\psi \circ \pi = f$. Alors, pour tout $\overline{x} \in G/H$, on a : $\psi(\overline{x}) = \psi(\pi(x)) = (\psi \circ \pi)(x) = f(x) = \varphi(\overline{x})$. D'où $\psi = \varphi$, ce qui achève de montrer le point (i).

Pour (ii), supposons d'abord que f est surjective. Soit $x' \in G'$ quelconque. Par surjectivité de f, il existe $x \in G$ tel que $x' = f(x)$. Comme $f(x) = \varphi(\overline{x})$, on déduit qu'il existe $\overline{x} \in G/H$ tel que $x' = \varphi(\overline{x})$. Ce qui prouve que φ est surjective. Supposons enfin que $H = \operatorname{Ker} f$. Soit $\overline{x} \in G/H$ tel que $\overline{x} \in \operatorname{Ker} \varphi$. On a $e' = \varphi(\overline{x}) = f(x)$, d'où $x \in \operatorname{Ker} f$, c'est-à-dire $x \in H$; par suite $\overline{x} = \overline{e}$. Ceci prouve que $\operatorname{Ker} \varphi = \{\overline{e}\}$, et l'injectivité de φ. □

► *Remarque.* Si l'on prend dans le théorème ci-dessus $H = \operatorname{Ker} f$ et $G' = \operatorname{Im} f$, le morphisme φ est à la fois injectif et surjectif, donc est un isomorphisme de $G/\operatorname{Ker} f$ sur $\operatorname{Im} f$, et l'on retrouve le premier théorème d'isomorphisme vu 2.2.3.

Le théorème précédent s'étend lui-même sous la forme suivante.

Lemme de factorisation (fondamental). *Soient G un groupe, H un sous-groupe normal dans G, et π la surjection canonique $G \to G/H$. Soient G' un groupe, H' un sous-groupe normal dans G', et π' la surjection canonique $G' \to G'/H'$. Alors, pour tout morphisme de groupes $f : G \to G'$ vérifiant la condition $f(H) \subseteq H'$, il existe un unique morphisme $\varphi : G/H \to G'/H'$ tel que $\varphi \circ \pi = \pi' \circ f$.*

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\pi}\downarrow & \searrow^{g} & \downarrow{\scriptstyle\pi'} \\ G/H & \xrightarrow[\varphi]{} & G'/H' \end{array}$$

Preuve. Posons $g = \pi' \circ f$, qui est un morphisme de groupes $G \to G'/H'$, comme composé de deux morphismes. Afin d'appliquer le théorème précédent, montrons que $H \subseteq \operatorname{Ker} g$. Soit $x \in H$. On a $f(x) \in f(H)$. L'hypothèse $f(H) \subseteq H'$ implique donc $f(x) \in H'$. D'où $\pi'(f(x)) = \widetilde{e}'$. On déduit que $g(x) = \widetilde{e}'$, c'est-à-dire $x \in \operatorname{Ker} g$. Ainsi $g : G \to G'/H'$ est un morphisme vérifiant $H \subseteq \operatorname{Ker} g$; le théorème précédent assure l'existence d'un unique morphisme $\varphi : G/H \to G'/H'$ tel que $\varphi \circ \pi = g$, d'où le résultat. □

► *Remarque.* Avec les données et notations ci-dessus, on a :

$$(\ \pi' \circ f \text{ surjectif } \Rightarrow\ \varphi \text{ surjectif }) \quad \text{et} \quad (\ H = \operatorname{Ker}(\pi' \circ f)\ \Leftrightarrow\ f^{-1}(H') = H\ \Rightarrow\ \varphi \text{ injectif }).$$

Donnons un exemple d'aplication de ce type de factorisation de morphisme.

THÉORÈME (dit deuxième théorème d'isomorphisme). *Soient G un groupe, H et K deux sous-groupes de G tels que $H \triangleleft G$. On note $HK = \{hk\,;\, h \in H, k \in K\}$. Alors :*

(i) $H \cap K \triangleleft K$, (ii) *HK sous-groupe de G et* $H \triangleleft HK$, (iii) $K/(H \cap K) \simeq HK/H$.

Preuve. Remarquons d'abord que, comme $H \triangleleft G$, tout élément $hk \in HK$ s'écrit aussi $kk^{-1}hk \in KH$, de sorte que $HK = KH$

Il est clair que $H \cap K$ est un sous-groupe de K. Montrons qu'il est normal dans K. Considérons pour cela un élément $x \in H \cap K$. Pour tout $k \in K$, on a $kxk^{-1} \in K$ car $x \in K$ et K est un sous-groupe, et $kxk^{-1} \in H$ car $x \in H$ et $H \triangleleft G$. Donc $kxk^{-1} \in H \cap K$, ce qui montre que $H \cap K \triangleleft K$.

Pour le point (ii), il suffit d'observer que, pour tous $h, h' \in H$ et $k, k' \in K$, on a $hkh'k' = h(kh'k^{-1})kk' \in HK$ et $(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1} \in HK$, donc HK est un sous-groupe de G. Il est clair que H est un sous-groupe de HK et le fait qu'il soit normal dans HK découle du calcul $(hk)^{-1}h'(hk) = k^{-1}(h^{-1}h'h)k \in H$.

Puisque $H \triangleleft HK$, on peut considérer le groupe quotient HK/H et $\pi' : HK \to HK/H$ la surjection canonique. Notons j l'injection canonique $K \to HK$, morphisme défini par $j(k) = ke = k$ pour tout $k \in K$. On a bien sûr $j(H \cap K) \subseteq H$, de sorte que l'application directe du lemme de factorisation assure l'existence d'un morphisme de groupes $\varphi : K/H \cap K \to HK/H$ tel que $\varphi \circ \pi = \pi' \circ j$:

$$\begin{array}{ccc} K & \xrightarrow{\quad j \quad} & HK \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ K/H \cap K & \xrightarrow{\quad\varphi\quad} & HK/H \end{array}$$

Montrons que φ est surjective. Soit $\overline{hk}$ un élément quelconque de HK/H, avec $h \in H, k \in K$. On a $\overline{hk} = \overline{h}\,\overline{k} = \overline{k}$; on déduit que $HK/H = \pi'(K) = (\pi' \circ j)(K)$. Comme on l'a remarqué précédemment, la surjectivité de $\pi' \circ j$ implique celle de φ. Montrons que φ est injective. Soit $k \in K$ un élément quelconque de $\mathrm{Ker}(\pi' \circ j)$. On a $\overline{e} = \pi'(j(k)) = \pi'(k) = \overline{k}$, c'est-à-dire $k \in H$. Donc $k \in H \cap K$; on déduit que $\mathrm{Ker}(\pi' \circ j) \subseteq H \cap K$. L'inclusion réciproque étant claire, on déduit que $\mathrm{Ker}(\pi' \circ j) = H \cap K$. On conclut que φ est injective. Ainsi φ réalise un isomorphisme de $K/H \cap K$ sur HK/H. □

2.2.6 Sous-groupes d'un groupe quotient

PROPOSITION. *Soient G un groupe et H un sous-groupe normal dans G. L'ensemble des sous-groupes de G/H est en bijection avec l'ensemble des sous-groupes de G contenant H.*

Plus précisément, si l'on note $\pi : G \to G/H$ la surjection canonique, il existe pour tout sous-groupe $\overline{K}$ de G/H un unique sous-groupe K de G contenant H tel que $\overline{K} = \pi(K) = K/H$.

Preuve. Soit $\overline{K}$ un sous-groupe de G/H. Posons $K = \pi^{-1}(\overline{K}) = \{x \in G\,;\, \pi(x) \in \overline{K}\}$. En tant qu'image réciproque d'un sous-groupe par un morphisme de groupes, K est un sous-groupe de G. Si $h \in H$, on a $\pi(h) = \overline{e}$, donc $\pi(h) \in \overline{K}$, de sorte que $h \in \pi^{-1}(\overline{K})$, c'est-à-dire $h \in K$. Ceci montre que $H \subseteq K$. Par définition de K, on a $\pi(K) \subseteq \overline{K}$. Réciproquement, soit $\overline{x} \in \overline{K}$, avec $x \in G$; comme $\pi(x) = \overline{x} \in \overline{K}$, on a clairement $x \in \pi^{-1}(\overline{K}) = K$, et donc $\overline{x} = \pi(x) \in \pi(K)$. En résumé, $\overline{K} = \pi(K)$. Enfin, $H \triangleleft G$ implique $H \triangleleft K$, et il est clair alors que $K/H = \pi(K)$.

Montrons maintenant l'unicité. Soit donc K' un sous-groupe de G tel que $H \subseteq K'$ et $\overline{K} = \pi(K')$. On a donc $\pi(K) = \pi(K')$. Quel que soit $k' \in K'$, il existe alors $k \in K$ tel que $\pi(k') = \pi(k)$, donc $k'k^{-1} \in H$; on a $k' = hk$ avec $h \in H$, et l'hypothèse $H \subseteq K$ implique $h \in K$, d'où $k' \in K$ comme produit de deux éléments de K. On conclut que $K' \subseteq K$. L'inclusion réciproque s'obtient de même. □

THÉORÈME (dit troisième théorème d'isomorphisme). *Soient G un groupe et H un sous-groupe normal dans G. Pour tout sous-groupe K normal dans G contenant H, on a :*

$$K/H \lhd G/H, \qquad \text{et} \qquad (G/H)/(K/H) \simeq G/K.$$

Preuve. Notons θ la surjection canonique $G \to G/K$ et π la surjection canonique $G \to G/H$. Il est clair que $K/H = \pi(K)$ est un sous-groupe de G/H (comme image du sous-groupe K par le morphisme de groupes π). Quels que soient $\overline{x} \in G/H$ et $\overline{k} \in K/H$, on a $\overline{x}\overline{k}\overline{x}^{-1} = \pi(xkx^{-1})$; or $xkx^{-1} \in K$ puisque $K \lhd G$, donc $\overline{x}\overline{k}\overline{x}^{-1} \in \pi(K)$. Ceci prouve que $K/H \lhd G/H$. On peut donc considérer le groupe quotient $(G/H)/(K/H)$; notons θ' la surjection canonique $G/H \to (G/H)/(K/H)$. Puisque $\pi(K) = K/H$, on applique le lemme de factorisation pour conclure qu'il existe un morphisme $\varphi : G/K \to (G/H)/(G/K)$ tel que $\varphi \circ \theta = \theta' \circ \pi$.

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ \theta \downarrow & & \downarrow \theta' \\ G/K & \xrightarrow{\varphi} & \dfrac{(G/H)}{(K/H)} \end{array}$$

Le morphisme $\theta' \circ \pi$ est surjectif comme composé de deux surjections, d'où il résulte que φ est surjectif. On a $\mathrm{Ker}(\theta' \circ \pi) = K$, d'où l'on déduit que φ est injectif. On conclut que φ est un isomorphisme de groupes de G/K sur $(G/H)/(K/H)$. □

COROLLAIRE (dit formule des indices). *Sous les hypothèses du théorème précédent, si l'on suppose de plus que H est d'indice fini dans G, alors on a : $[G : H] = [G : K][K : H]$.*

Preuve. Découle directement du théorème et des propriétés de l'indice. □

2.3 Produit direct ou semi-direct

2.3.1 Observations préliminaires

NOTATION. Soient G un groupe, H et K deux sous-groupes de G. On note HK le sous-ensemble de G formé des éléments qui s'écrivent comme produit d'un élément de H par un élément de K.

$$HK = \{hk\,;\, h \in H, k \in K\}.$$

REMARQUES.

1. Si $H \cap K = \{e\}$, tout élément de HK s'écrit *de façon unique* sous la forme hk avec $h \in H, k \in K$.

   En effet, si $h_1k_1 = h_2k_2$ avec $h_1, h_2 \in H$ et $k_1, k_2 \in K$, on a $h_2^{-1}h_1 = k_2k_1^{-1}$. Le premier produit est dans H puisque H est un sous-groupe, et le second est dans K puisque K est un sous-groupe. Donc $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$, c'est-à-dire $h_2^{-1}h_1 = k_2k_1^{-1} = e$, et donc $h_2 = h_1$ et $k_2 = k_1$.

2. Si $H \cap K = \{e\}$, et si H et K sont finis, alors HK est fini et $\operatorname{card} HK = |H| \times |K|$.

   En effet, il résulte du point précédent que HK est alors équipotent à $H \times K$.

3. On a $HK = KH$ si et seulement si, quels que soient $h \in H$ et $k \in K$, il existe $h' \in H$ et $k' \in K$ tels que $hk = k'h'$. Attention, ça n'implique pas que tout élément de H commute avec tout élément de K.

Exemple d'application. Le groupe alterné A_4 ne contient pas de sous-groupe d'ordre 6.

En effet : on a vu en 2.1.1 que A_4 contient 3 éléments a, b, c d'ordre 2, huit éléments d'ordre 3, et le neutre e d'ordre 1. On a vu en 2.2.2 que les trois sous-groupes $\{e, a\}$, $\{e, b\}$ et $\{e, c\}$ ne sont pas normaux dans A_4, mais le sous-groupe $V = \{e, a, b, c\}$ est normal dans A_4.

Supposons par l'absurde qu'il existe dans A_4 un sous-groupe F d'ordre 6. Il serait d'indice 2, donc normal dans A_4. Donc $F \cap V$ serait normal dans A_4 comme intersection de deux sous-groupes normaux. De plus, $F \cap V$ étant un sous-groupe à la fois de F d'ordre 6 et de V d'ordre 4, le théorème de Lagrange impliquerait que $|F \cap V| = 1$ ou 2. Si $|F \cap V| = 1$, alors d'après la remarque 2 ci-dessus, la partie FV de A_4 compterait 24 éléments, ce qui est absurde puisque $|A_4| = 12$. C'est donc que $F \cap V$ est d'ordre 2. Donc $F \cap V$ est l'un des trois sous-groupes $\{e, a\}$, $\{e, b\}$ et $\{e, c\}$. Or ceux-ci ne sont pas normaux dans A_4. D'où une contradiction.

2.3.2 Produit direct ou semi-direct (interne) de deux sous-groupes

Définitions. Soient G un groupe, H et K deux sous-groupes de G. On dit que G est le *produit semi-direct* de H par K lorsque les trois conditions suivantes sont vérifiées :

$$(1)\ \ G = HK, \qquad (2)\ \ H \cap K = \{e\}, \qquad (3)\ \ H \lhd G.$$

On dit que G est le *produit direct* de H par K lorsque les trois conditions suivantes sont vérifiées :

$$(1)\ \ G = HK, \qquad (2)\ \ H \cap K = \{e\}, \qquad (4)\ \ \forall\, h \in H,\ \forall\, k \in K,\ hk = kh.$$

Parce que ces notions sont ici relatives à des sous-groupes d'un même groupe, on parle parfois de produit semi-direct ou direct *interne*.

Lemme. *Soient G un groupe, H et K deux sous-groupes de G.*

(i) *Si G est produit semi-direct de H par K, alors on a : $G = KH = HK$.*

(ii) *Si G est le produit direct de H par K, alors G est produit semi-direct de H par K,*

(iii) *Si G est le produit direct de H par K, alors G est produit direct de K par H,*

(iv) *Si G est le produit direct de H par K, alors H et K sont normaux dans G.*

Preuve. On suppose que les trois conditions (1), (2) et (3) sont vérifiées. On sait déjà que tout élément g de G s'écrit $g = hk$ avec $h \in H$ et $k \in K$. Donc $g = kk^{-1}hk$, et comme $H \lhd G$, le produit $h' = k^{-1}hk$ est un élément de H. D'où $g = kh'$ avec $k \in K$ et $h' \in H$, ce qui montre (i).

Supposons (1), (2) et (4) vérifiées. D'après la remarque 1 ci-dessus, il résulte des hypothèses (1) et (2) que tout élément $g \in G$ s'écrit de façon unique sous la forme $g = hk$ avec $h \in H$ et $k \in K$. Donc pour tout $\ell \in H$, on a : $g\ell g^{-1} = hk\ell k^{-1}h^{-1} = h\ell kk^{-1}h^{-1} = h\ell h^{-1}$ en utilisant l'hypothèse (4). Ce dernier produit étant un élément du sous-groupe H, on a montré que $g\ell g^{-1} \in H$ pour tout $g \in G$ et tout $\ell \in H$. Donc $H \lhd G$ et la condition (3) est vérifiée, ce qui prouve (ii).

Le point (iii) est clair, et le point (iv) en découle par symétrie du rôle joué par H et K. □

REMARQUE. Attention, la réciproque du point (ii) est fausse ; un groupe peut être produit semi-direct de deux sous-groupes sans que ce produit soit direct (voir exemples ci-dessous).

Exemple. Considérons le groupe diédral $\mathbb{D}_{2n} = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\}$, et les sous-groupes $C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$ et $K = \{e, s\}$. Il est clair que $\mathbb{D}_{2n} = C_n K$ et $C_n \cap K = \{e\}$. On a vu que $C_n \lhd \mathbb{D}_{2n}$. Donc $\mathbb{D}_{2n}$ est produit semi-direct de C_n par K. Si $n > 2$, ce produit semi-direct n'est pas direct car $sr^k = r^{n-k}s \neq r^k s$, de sorte que la condition (3) n'est pas vérifiée, et K n'est pas normal dans $\mathbb{D}_{2n}$. Dans le cas particulier où $n = 2$, $\mathbb{D}_4 \simeq V$ est abélien, et il est le produit direct de C_2 par $K \simeq C_2$.

Exercice. Montrer que le groupe des quaternions Q_8 n'est pas produit semi-direct de deux de ses sous-groupes propres (on rappelle que Q_8 n'est pas abélien, et que ses sous-groupes propres sont normaux, d'ordre 2 ou 4).

THÉORÈME. *Soient G un groupe, H un sous-groupe normal de G, et K un sous-groupe de G. On suppose que G est le produit semi-direct de H par K. Alors :*

(i) *Soient g, g' deux éléments quelconques de G. Si $g = hk$ et $g' = h'k'$ sont les décompositions (uniques) de g et g' (avec $h, h' \in H$ et $k, k' \in K$), alors la décomposition du produit gg' est donnée par :*

$$gg' = h\gamma_k(h')kk', \qquad \text{avec } h\gamma_k(h') \in H \text{ et } kk' \in K$$

où γ_k désigne l'automorphisme intérieur de G défini par $x \mapsto kxk^{-1}$.

(ii) *On a : $G/H \simeq K$.*

Preuve. (i) résulte simplement du calcul $gg' = hkh'k' = hkh'k^{-1}kk'$, et du fait que $kh'k^{-1}$ appartient à H puisque $H \lhd G$. Pour (ii), on considère l'application $f : G \to K$ qui, à tout $g \in G$ décomposé de façon unique en $g = hk$ avec $h \in H$ et $k \in K$, associe $f(g) = k$. D'après le point (i) précédent, f est un morphisme de groupes. Il est clair qu'il est surjectif et que son noyau est H. D'où l'isomorphisme voulu d'après le premier théorème d'isomorphisme. □

2.3.3 Produit direct ou semi-direct (externe) de deux groupes

OBSERVATION PRÉLIMINAIRE. On a défini en 1.1.4 le produit direct $G = G_1 \times G_2$ de deux groupes G_1 et G_2. Parce qu'il s'agit ici de construire un nouveau groupe à partir de deux groupes donnés, on parle parfois dans ce cas de produit direct *externe*. Cette notion est canoniquement liée à la notion de produit direct (interne) de deux sous-groupes de la façon suivante : si l'on pose $H = G_1 \times \{e_2\}$ et $K = \{e_1\} \times G_2$, alors H est un sous-groupe de G isomorphe à G_1, K est un sous-groupe de G isomorphe à G_2, et G est le produit direct (interne) des sous-groupes H et K (ceci avait déjè été observé dans le cas de groupes abéliens dans le lemme final de 1.1.4).

Le même correspondance existe pour le produit semi-directe, comme le montre l'énoncé suivant.

PROPOSITION ET DÉFINITION. *Soient G_1 et G_2 deux groupes, et $\gamma : G_2 \to \operatorname{Aut} G_1$ un morphisme de groupes. Pour tout $x_2 \in G_2$, on note γ_{x_2} l'automorphisme de G_1 image de x_2 par γ.*

(i) *Le produit cartésien $G_1 \times G_2 = \{(x_1, x_2),\ x_1 \in G_1,\ x_2 \in G_2\}$ est un groupe pour la loi définie par :*

$$(x_1, x_2).(y_1, y_2) = (x_1\gamma_{x_2}(y_1), x_2y_2) \quad \text{pour tous } x_1, y_1 \in G_1,\ x_2, y_2 \in G_2.$$

Ce groupe est appelé le produit semi-direct (externe) de G_1 par G_2. On le note $G = G_1 \times_\gamma G_2$, ou $G = G_1 \rtimes G_2$.

(ii) *Si l'on note $H = G_1 \times \{e_2\}$ et $K = \{e_1\} \times G_2$, alors H est un sous-groupe de G normal dans G et isomorphe à G_1, K est un sous-groupe de G isomorphe à G_2, et G est le produit semi-direct interne de H par K.*

Preuve. La vérification des axiomes de groupes pour (i) et des isomorphismes pour (ii) est technique mais élémentaire. C'est un excellent exercice, à faire absolument ! □

► *Remarque.* Le produit direct de G_1 et G_2 est un cas particulier de produit semi-direct, correspondant au cas où γ_{x_2} est l'identité de G_1 pour tout $x_2 \in G_2$, c'est-à dire au cas où $\gamma : G_2 \to \operatorname{Aut} G_1$ est le morphisme constant $x_2 \mapsto \mathrm{id}_{G_1}$.

► *Remarque.* Dans le produit semi-direct $G_1 \rtimes G_2$, les groupes G_1 et G_2 ne jouent a priori pas des rôles symétriques. En particulier, même si G_1 et G_2 sont abéliens, $G_1 \rtimes G_2$ n'est en général pas abélien (et de fait il ne l'est que lorsque γ est trivial, c'est-à-dire lorsque le produit est direct). Par exemple, pour $n \geq 3$: les groupes cycliques C_n et C_2 sont abéliens, mais le groupe diédral $\mathbb{D}_{2n} \simeq C_n \rtimes C_2$ ne l'est pas.

Chapitre 3

Groupe opérant sur un ensemble

3.1 Groupe opérant sur un ensemble, exemples

3.1.1 Rappel de quelques notions générales

Définition. Soient G un groupe et E un ensemble non vide. On dit que G *opère* (à gauche) sur E s'il existe une loi externe :

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (g, x) & \longmapsto & g.x \end{array}$$

qui satisfait les deux conditions :

$$(1) \quad \forall\, g, g' \in G,\ \forall\, x \in E,\ g.(g'.x) = (gg').x\,; \qquad (2) \quad \forall\, x \in E,\ e.x = x.$$

On dit aussi que E est un G-*ensemble*, ou que l'on a une *action* de G sur E.

Théorème. *La donnée d'une action d'un groupe G sur un ensemble non-vide E équivaut à la donnée d'un morphisme de groupes de G dans le groupe symétrique $S(E)$.*

> *Preuve.* Supposons donné un morphisme de groupes $\gamma : G \longrightarrow S(E)$; pour tout $g \in G$, notons $\gamma_g \in S(E)$ l'image de g par γ. On définit une loi externe $G \times E \longrightarrow E$ en posant $g.x = \gamma_g(x)$ pour tous $g \in G, x \in E$. En utilisant le fait que $\gamma_g \circ \gamma_{g'} = \gamma_{gg'}$ et $\gamma_e = \mathrm{id}_E$, on vérifie aisément que les deux conditions (1) et (2) d'une action sont vérifiées.
>
> Réciproquement, supposons que G opère sur E par $(g, x) \longmapsto g.x$. Définissons pour tout $g \in G$ une application $\gamma_g : E \longrightarrow E$ en posant $\gamma_g(x) = g.x$ pour tout $x \in E$. On a alors :
>
> $$\forall\, x \in E,\ \forall\, g, h \in G, \quad (\gamma_g \circ \gamma_h)(x) = g.(h.x) = (gh).x = \gamma_{gh}(x) \quad \text{et} \quad \gamma_e(x) = e.x = x,$$
>
> ce qui prouve que $\gamma_g \circ \gamma_h = \gamma_{gh}$ et $\gamma_e = \mathrm{id}_E$. On en déduit que γ_g est bijective pour tout $g \in G$ (en prenant $h = g^{-1}$), puis que l'application $\gamma : G \to S(E)$ est un morphisme de groupes. □

Définition et proposition. *Soit G un groupe opérant sur un ensemble non-vide E. Pour tout $x \in E$, on appelle stabilisateur de x l'ensemble :*

$$G_x = \{g \in G\,;\, g.x = x\} \quad .$$

C'est un sous-groupe de G, appelé aussi sous-groupe d'isotropie de x. On le note parfois $\mathrm{Stab}_G(x)$.

> *Preuve.* On a $e.x = x$ donc $e \in G_x$. De plus, quels que soient $g, h \in G_x$, on calcule : $(gh^{-1}).x = (gh^{-1}).(h.x) = (gh^{-1}h).x = g.x = x$. D'où $gh^{-1} \in G_x$. □

DÉFINITION ET PROPOSITION. *Soit G un groupe opérant sur un ensemble non-vide E. Pour tout $x \in E$, on appelle orbite de x l'ensemble :*

$$\Omega_x = \{g.x\,;\, g \in G\} = \{y \in E\,;\, \exists\, g \in G,\ y = g.x\}.$$

Les orbites des éléments de E sous l'action de G forment une partition de E.

> *Preuve.* La relation $\mathscr{R}$ définie sur E par : $(\forall\, x, y \in E,\ x\ \mathscr{R}\ y \ \Leftrightarrow\ \exists\, g \in G,\ y = g.x)$ est clairement une relation d'équivalence. La classe d'équivalence pour $\mathscr{R}$ d'un élément $x \in E$ n'est autre par définition que l'orbite Ω_x. D'où le résultat puisque les classes d'équivalence forment une partition de E. □

DÉFINITIONS. Soit G un groupe opérant sur un ensemble non-vide E.

1. Le noyau du morphisme $\gamma : G \longrightarrow S(E)$ canoniquement associé à l'action de G sur E est appelé le *noyau de l'action*. Il est clair que c'est l'intersection des stabilisateurs :

$$\operatorname{Ker}\gamma = \{g \in G\,;\, \forall\ x \in E,\ g.x = x\} = \bigcap_{x \in E} G_x \quad .$$

   On dit que l'action est *fidèle* (ou que G opère *fidèlement* sur E) lorsque γ est injectif, c'est-à-dire lorsque le noyau de l'action est $\{e\}$. Si G opère fidèlement sur E, alors G est isomorphe à un sous-groupe de $S(E)$, à savoir $\operatorname{Im}\gamma$.

2. Un élément $x \in E$ est appelé un *point fixe* de l'action de G lorsque $g.x = x$ pour tout $g \in G$. On note E^G ou $\operatorname{Fix}_G(E)$ l'ensemble de ces points fixes. Pour tout $x \in E$, on a :

$$(x \in E^G) \ \Leftrightarrow\ (G_x = G) \ \Leftrightarrow (\Omega_x = \{x\}) \quad \text{(orbite ponctuelle)}.$$

   On dit que l'action est *sans point fixe* lorsque $E^G = \emptyset$.

3. On dit que G opère *transitivement* sur E, ou encore que l'action de G sur E est *transitive*, ou encore que E est un G-ensemble *homogène*, lorsqu'il n'y a qu'une seule orbite :

$$\text{(action transitive)} \ \Leftrightarrow\ (\forall\, x \in E,\ \Omega_x = E) \ \Leftrightarrow\ (\forall\, x, y \in E,\ \exists\, g \in G,\ y = g.x).$$

3.1.2 Exemples généraux d'actions

▶ Action d'un groupe sur lui-même par translation

Tout groupe G opère sur lui-même par translation à gauche :
$$\left|\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & g.x = gx \end{array}\right.$$

1. Pour tout $x \in G$, $G_x = \{g \in G\,;\, gx = x\} = \{e\}$.

   On en déduit que $\operatorname{Ker}\gamma = \bigcap_{x \in G} G_x = \{e\}$, donc l'action est fidèle.

2. Pour tout $x \in G$, $\Omega_x = \{gx\,;\, g \in G\} = G$ (car tout $y \in G$ s'écrit $y = (yx^{-1})x$).

   On en déduit qu'il n'y a qu'une seule orbite, donc l'action est transitive.

   De plus, dès lors que $G \neq \{e\}$, on a $\Omega_x = G$ non ponctuelle pour tout $x \in G$, donc l'action est sans point fixe.

▶ **Action d'un groupe sur lui-même par conjugaison**

Tout groupe G opère sur lui même par conjugaison : $\left|\begin{array}{ccc} G\times G & \longrightarrow & G \\ (g,x) & \longmapsto & g.x = gxg^{-1} \end{array}\right.$

1. Pour tout $x \in G$, $G_x = \{g \in G\,;\, gx = xg\}$ est le *centralisateur* de x, noté $C_G(x)$.
   Donc $\operatorname{Ker}\gamma = \bigcap_{x\in G} G_x = \{g \in G\,;\, \forall\, x \in G,\ gx = xg\}$ est le *centre* de G, noté $Z(G)$.
   En particulier l'action est fidèle si et seulement si $Z(G) = \{e\}$.

2. Pour tout $x \in G$, l'orbite $\Omega_x = \{gxg^{-1}\,;\, g \in G\}$ est la *classe de conjugaison* de x.
   On en déduit que Ω_x est ponctuelle si et seulement si x est central ; donc l'ensemble des points fixes E^G est non-vide et égal au centre $Z(G)$.
   De plus $\Omega_e = \{e\}$, donc $\Omega_e \neq G$ dès lors que $G \neq \{e\}$, et l'action n'est alors pas transitive.

▶ **Action d'un groupe sur l'ensemble de ses parties par conjugaison**

Tout groupe G opère sur $\mathscr{P}(G)$ par conjugaison : $\left|\begin{array}{ccc} G\times \mathscr{P}(G) & \longrightarrow & \mathscr{P}(G) \\ (g,X) & \longmapsto & g.X = gXg^{-1} \end{array}\right.$

1. Pour tout $X \subseteq G$, $G_X = \{g \in G\,;\, gXg^{-1} = X\}$ est le *normalisateur* de X, noté $N_G(X)$.

   • *Remarque.* Dans le cas où $X = H$ est un sous-groupe de G, on montre que H est un sous-groupe de $N_G(H)$, que $H \lhd N_G(H)$, et que $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal ; en particulier $H \lhd G$ si et seulement si $N_G(H) = G$.

2. On en déduit que $X \in \mathscr{P}(G)^G$ si et seulement si $N_G(X) = G$.

   • *Remarque.* Dans le cas où $X = H$ est un sous-groupe de G, cela signifie que $H \lhd G$.

3. On en déduit aussi que $\operatorname{Ker}\gamma = Z(G)$.

   • *En effet,* $\operatorname{Ker}\gamma = \bigcap_{X\subseteq G} G_X = \bigcap_{X\subseteq G} N_G(X)$. En considérant parmi les $X \subseteq G$ celles qui sont des singletons, il vient : $\operatorname{Ker}\gamma \subseteq \bigcap_{x\in G} N_G(\{x\}) = \bigcap_{x\in G} C_G(x) = Z(G)$. L'inclusion réciproque est claire.

4. Pour $X \in \mathscr{P}(G)$, $\Omega_X = \{gXg^{-1}\,;\, g \in G\}$ est la classe de conjugaison de X dans $\mathscr{P}(G)$.
   En particulier l'action n'est pas transitive (car $\Omega_\emptyset = \{\emptyset\} \neq \mathscr{P}(G)$).

3.2 Equation aux classes, applications aux p-groupes

3.2.1 Indice des stabilisateurs

PROPOSITION. *Soit G un groupe opérant sur un ensemble E. Si deux éléments x et y de E appartiennent à une même orbite, alors leurs stabilisateurs G_x et G_y sont conjugués dans G.*

Preuve. Soient $x \in E$ et $y \in \Omega_x$; il existe donc $g \in G$ tel que $y = g.x$. Montrons que $G_y = gG_xg^{-1}$. Soit $h \in G_y$. On a $y = h.y$, c'est-à-dire $g.x = h.(g.x) = hg.x$. On en tire : $x = e.x = g^{-1}g.x = g^{-1}.(g.x) = g^{-1}.(hg.x) = (g^{-1}hg).x$, donc $g^{-1}hg \in G_x$, ou encore $h \in gG_xg^{-1}$. Réciproquement, soit $k \in gG_xg^{-1}$. On a $g^{-1}kg \in G_x$, donc $(g^{-1}kg).x = x$, d'où $kg.x = g.x$, c'est-à-dire $k.y = y$, ou encore $k \in G_y$. □

► Convention de notation. Il existe plusieurs notations usuelles pour le cardinal d'un ensemble fini X, par exemple $\mathrm{card}\,(X)$, ou $\#X$, ou $|X|$. On utilise dans ce qui suit $|X|$, que X soit ou non un groupe (auquel cas $|X|$ est l'ordre de X). On sera donc vigilant dans les formules qui suivent à bien identifier les sous-groupes et les simples sous-ensembles.

Théorème. *Soit G un groupe opérant sur un ensemble E.*

(i) *Pour tout $x \in E$, le cardinal de l'orbite Ω_x est égal à l'indice du stabilisateur G_x. On note :*
$$|\Omega_x| = [G : G_x] \quad .$$

(ii) *En particulier, si G est fini, $|\Omega_x|$ divise $|G|$.*

Preuve. On fixe $x \in E$. Soit Q_{G_x} l'ensemble des classes à gauche modulo le sous-groupe G_x, dont le cardinal est par définition l'indice du sous-groupe G_x dans G (voir 2.2.1). On montre que Ω_x et Q_{G_x} sont équipotents en construisant une bijection λ de Ω_x sur Q_{G_x}.

Un élément de Ω_x est de la forme $g.x$, où $g \in G$; on pose $\lambda(g.x) = gG_x$. Montrons que l'on définit bien ainsi une application $\lambda : \Omega_x \longrightarrow Q_{G_x}$, indépendamment de l'élément g choisi. Pour cela, considérons $h, g \in G$ tels que $g.x = h.x$; alors $h^{-1}.(g.x) = h^{-1}.(h.x)$, donc $(h^{-1}g).x = (h^{-1}.h).x = e.x = x$; on conclut que $h^{-1}g \in G_x$, d'où $gG_x = hG_x$.

L'application λ est surjective par construction, car tout élément de Q_{G_x} est de la forme gG_x pour un $g \in G$, et donc $\lambda(g.x) = gG_x$. Pour l'injectivité, considérons $g, h \in G$ quelconques tels que $\lambda(g.x) = \lambda(h.x)$ Alors $gG_x = hG_x$, donc $h^{-1}g \in G_x$, c'est-à-dire $(h^{-1}g).x = x$; d'où $h.x = h.((h^{-1}g).x) = (hh^{-1}g).x = g.x$. Ceci prouve que λ est injective et achève la preuve du point (i). Le point (ii) en découle d'après la remarque 2.2.1. □

Corollaire. *Soit G un groupe opérant sur un ensemble fini E. Soit $\{x_i\}_{1 \leq i \leq r}$ une famille de représentants des orbites distinctes. On a :*
$$|E| = \sum_{i=1}^{r} [G : G_{x_i}] \quad .$$

Preuve. L'ensemble E étant fini, il y a un nombre fini r d'orbites distinctes. Choisissons un représentant x_i dans chacune de ces r orbites. Les Ω_{x_i} pour $1 \leq i \leq r$ forment une partition de E, donc $|E| = \sum_{i=1}^{r} |\Omega_{x_i}|$, d'où le résultat en appliquant le théorème précédent. □

Exemples d'application.

(i) *Si G est un groupe fini d'ordre 33 opérant sur un ensemble E fini de cardinal 19, alors l'action admet forcément des points fixes.*

En effet, toute orbite est de cardinal 1, 3, 11 ou 33. Comme $33 > |E|$, seuls 1, 3 et 11 restent possibles. Si E^G était vide, il n'y aurait pas d'orbite ponctuelle, et on aurait donc en tout et pour tout n orbites à 3 éléments et m orbites à 11 éléments, d'où $3n + 11m = 19$. Cette équation n'ayant pas de solutions dans $\mathbb{N}$, on conclut que $E^G \neq \emptyset$.

(ii) *Soit G un groupe fini d'ordre 15 opérant sans point fixe sur un ensemble E fini de cardinal 17 ; donner le nombre d'orbites et le cardinal de chacune d'elles.*

En effet, puisqu'il n'y a pas de points fixes donc pas d'orbites ponctuelles, toute orbite est de cardinal 3, 5 ou 15. S'il y avait une orbite à 15 éléments (il ne peut de toute façon pas y en avoir plus...), les deux éléments restants de E ne pourraient pas former une orbite. C'est donc qu'il n'y a pas d'orbites à 15 éléments. On a donc en tout et pour tout n orbites à 3 éléments et m orbites à 5 éléments, d'où $3n + 5m = 17$. La seule solution dans $\mathbb{N}$ est $n = 4$ et $m = 1$.

3.2.2 Formule de Burnside

PROPOSITION. *Soit G un groupe fini opérant sur un ensemble fini E. Pour tout $g \in G$, on note $E^g = \{x \in E\,;\, g.x = x\}$ l'ensemble des points de E fixés par g. Alors le nombre r d'orbites distinctes est donné par :*

$$r = \tfrac{1}{|G|} \sum_{g \in G} |E^g|.$$

Preuve. Comme dans le corollaire précédent, il y a un nombre fini r d'orbites distinctes et l'on peut choisir un représentant x_i dans chacune d'elles. Les orbites Ω_{x_i} pour $1 \leq i \leq r$ formant une partition de E, on calcule :

$$\sum_{x \in E} |G_x| = \sum_{i=1}^{r} \sum_{x \in \Omega_{x_i}} |G_x| = \sum_{i=1}^{r} |\Omega_{x_i}|\,|G_{x_i}| = r|G|$$

en utilisant d'abord que $|G_x|$ est constant sur une même orbite d'après la proposition 3.2.1, puis le théorème 3.2.1. On conclut en remarquant que $\sum_{x \in E} |G_x| = \sum_{g \in G} |E^g|$, ce qui correspond à deux façons de compter les couples $(x, g) \in E \times G$ tels que $g.x = x$. □

3.2.3 Equation aux classes pour un groupe fini

THÉORÈME. *Soit G un groupe fini. Pour tout $x \in G$, on note $C_G(x)$ le centralisateur de x dans G. On note $Z(G)$ le centre de G.*

(i) *Le cardinal de la classe de conjugaison de tout élément de G divise $|G|$.*

(ii) *Soit $\{x_i\}_{1 \leq i \leq r}$ une famille de représentants des classes de conjugaison distinctes dans G. Alors :*

$$|G| = \sum_{i=1}^{r} [G : C_G(x_i)] \quad .$$

(iii) *Soit $\{x_i\}_{1 \leq i \leq k}$ une famille de représentants des classes de conjugaison distinctes* non ponctuelles *dans G. Alors :*

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)] \quad .$$

Preuve. Pour l'action de G sur lui-même par conjugaison (voir 3.1.2), l'orbite d'un élément $x \in G$ est sa classe de conjugaison Ω_x, et son stabilisateur est son centralisateur $C_G(x)$. Les points (i) et (ii) résultent donc du théorème et du corollaire de 3.2.1.

Pour montrer (iii), rappelons d'abord (voir 3.1.2) que l'orbite d'un élément $x \in G$ est ponctuelle si et seulement si $x \in Z(G)$. Notons alors $x_1, \ldots, x_k$ des représentants des orbites non ponctuelles (il peut ne pas y en avoir, auquel cas $k = 0$ et G est abélien), et $x_{k+1}, \ldots, x_r$ des représentants des orbites ponctuelles (il y en a toujours au moins une, celle de e, donc $k < r$). Pour $k + 1 \leq i \leq r$, on a $x_i \in Z(G)$ et $|\Omega_{x_i}| = 1$. Pour $1 \leq i \leq k$, on a $x_i \notin Z(G)$ et $|\Omega_{x_i}| = [G : C_G(x_i)] \neq 1$. Donc :

$$|G| = \sum_{i=1}^{k} |\Omega_{x_i}| + \sum_{i=k+1}^{r} |\Omega_{x_i}| = \sum_{i=1}^{k} [G : C_G(x_i)] + |Z(G)|. \qquad \square$$

3.2.4 Applications aux p-groupes

DÉFINITION. Soit p un nombre premier. Un groupe fini est appelé un *p-groupe* lorsque son ordre est une puissance de p.

Le lemme suivant est à la base de l'étude des p-groupes, et en particulier des théorèmes de Sylow qui seront vus plus tard.

LEMME. *Si G est un p-groupe non trivial opérant sur un ensemble fini non-vide E, alors : $|E^G| \equiv |E| \bmod p$.*

> *Preuve.* On sait que $|E^G|$ est le nombre d'orbites ponctuelles. Si toutes les orbites sont ponctuelles, alors $|E| = |E^G|$ et le résultat est clair. Sinon, on note $\Omega_{x_1}, \ldots, \Omega_{x_k}$ les orbites non ponctuelles. Donc : $|E| = |E^G| + \sum_{i=1}^{k} |\Omega_{x_i}|$. Pour tout $1 \leq i \leq k$, $|\Omega_{x_i}|$ divise $|G|$ d'après 3.2.1. Puisque $|G|$ est de la forme p^n avec $n \in \mathbb{N}^*$, on déduit que $|\Omega_{x_i}| = p^{m_i}$ avec $m_i \leq n$. Mais de plus $m_i \geq 1$ puisque $|\Omega_{x_i}| \neq 1$. On conclut que $|E| - |E^G| = \sum_{i=1}^{k} p^{m_i}$ est divisible par p. □

PROPOSITION. *Le centre d'un p-groupe non trivial est non trivial.*

> *Preuve.* On applique ce qui précède à l'action de G sur lui-même par conjugaison : $E = G$ et $E^G = Z(G)$. Le lemme implique donc que $|G| - |Z(G)|$ est divisible par p. Comme $|G|$ est divisible par p, on conclut que $|Z(G)|$ est divisible par p. Donc $|Z(G)| \neq 1$. □

COROLLAIRE (groupes d'ordre p^2). *Si p est un nombre premier, tout groupe d'ordre p^2 est abélien.*

> *Preuve.* Soit G un groupe d'ordre p^2. D'après le théorème de Lagrange, $|Z(G)|$ divise p^2. Comme $|Z(G)| \neq 1$ d'après la proposition précédente, on a donc $|Z(G)| = p$ ou $|Z(G)| = p^2$. Si $|Z(G)| = p^2$, alors $G = Z(G)$, donc G est abélien. Si $|Z(G)| = p$, alors $|G/Z(G)| = p$, donc le groupe $G/Z(G)$ est cyclique (voir 1.1.3). Or $G/Z(G)$ monogène implique G abélien (voir 2.2.4). □

EXERCICE (groupes d'ordre p^3). *Si G est un groupe non-abélien d'ordre p^3 avec p premier, alors, quels que soient $x \in G$ et $y \in G$ tels que $xy \neq yx$, le groupe G est engendré par x et y.*

> *Solution.* Soit $H = \langle x, y \rangle$ le sous-groupe engendré par x et y dans G. Son ordre divise p^3. En appliquant le corollaire précédent, $|H| \neq p^2$ car H non abélien puisque $xy \neq yx$. De plus $|H| \neq p$ car sinon H serait cyclique donc abélien. Enfin $|H| \neq 1$ car H contient au moins x et y. On conclut que $|H| = p^3$, donc $H = G$. □

3.3 Actions transitives, applications à la non simplicité

3.3.1 Exemple fondamental d'action transitive

Soient G un groupe et H un sous-groupe propre de G. On note Q_H l'ensemble des classes à gauche relativement à H. Donc $Q_H = \{xH \,;\, x \in G\}$.

- G opère sur l'ensemble Q_H par translation à gauche : $\left| \begin{array}{ccc} G \times Q_H & \longrightarrow & Q_H \\ (g, xH) & \longmapsto & g.xH = gxH \end{array} \right.$

> *En effet.* Les deux conditions définissant une action sont clairement vérifiées. Le seul problème est de vérifier que l'application ci-dessus est bien définie, indépendamment du représentant de classe à gauche choisi. Pour cela, soit y un autre représentant de xH. On a donc $xH = yH$, ou encore $y^{-1}x \in H$. Pour tout $g \in G$, on a : $(gy)^{-1}(gx) = y^{-1}g^{-1}gx = y^{-1}x$; d'où $(gy)^{-1}(gx) \in H$, c'est-à dire $gyH = gxH$. □

- Cette action est transitive et sans point fixe.

  En effet. L'orbite de $eH = H$ est $\Omega_{eH} = \{geH\,;\, g \in G\} = \{gH\,;\, g \in G\} = Q_H$. Donc l'action est transitive. De plus, comme $H \neq G$, il existe $x \in G$ tel que $x \notin H$, donc $xH \neq H$, de sorte que Q_H n'est pas un singleton. Ainsi l'unique orbite ci-dessus n'est pas ponctuelle : l'action est sans point fixe. □

- Le stabilisateur d'un élément $xH \in Q_H$ est $G_{xH} = xHx^{-1}$.

  En effet. On a : $g \in G_{xH} \Leftrightarrow gxH = xH \Leftrightarrow gx \in xH \Leftrightarrow g \in xHx^{-1}$. □

- Le noyau du morphisme $\gamma : G \to S(Q_H)$ canoniquement associé à l'action est égal à $\bigcap_{x\in G} xHx^{-1}$, qui est le plus grand sous-groupe normal de G contenu dans H.

  En effet. On sait que $\operatorname{Ker}\gamma = \bigcap_{xH\in Q_H} G_{xH}$ donc ici $\operatorname{Ker}\gamma = \bigcap_{x\in G} xHx^{-1}$. Il est clair qu'il est normal dans G (c'est un noyau !) et que $\operatorname{Ker}\gamma \subset H$ (car $g \in \operatorname{Ker}\gamma$ implique qu'en particulier pour $x = e$, on a $g \in eHe^{-1} = H$). Enfin, soit N un sous-groupe normal de G contenu dans H. Pour tout $x \in G$, on a : $xNx^{-1} = N$ et $xNx^{-1} \subset xHx^{-1}$, donc $N \subset xHx^{-1}$. Ceci étant vrai pour tout $x \in G$, on obtient $N \subset \bigcap_{x\in G} xHx^{-1}$. Donc $\operatorname{Ker}\gamma$ est le plus grand sous-groupe normal de G contenu dans H. □

3.3.2 Théorème de Frobenius

Définition. Un groupe G est dit *simple* lorsque $G \neq \{e\}$ et que G n'admet pas de sous-groupes normaux autres que $\{e\}$ et G.

Lemme. *Si G est un groupe simple, et si H est un sous-groupe de G distinct de G, alors l'action de G sur Q_H par translation à gauche est fidèle.*

Preuve. On a vu que $\operatorname{Ker}\gamma$ est un sous-groupe normal de G contenu dans H. La simplicité de G implique donc que $\operatorname{Ker}\gamma = \{e\}$ ou $\operatorname{Ker}\gamma = G$. Si on avait $\operatorname{Ker}\gamma = G$, comme $\operatorname{Ker}\gamma \subset H$, on aurait $G = H$, ce qui est exclu. Donc $\operatorname{Ker}\gamma = \{e\}$. □

Corollaire. *Soit G un groupe fini. Soit H un sous-groupe de G d'indice $k \geq 2$. Si $|G|$ ne divise pas $k!$, alors G n'est pas simple.*

Preuve. Comme $[G : H] \geq 2$, le sous-groupe H est distinct de G. Si G était simple, il résulterait du lemme précédent que le noyau $\operatorname{Ker}\gamma$ de l'action de G sur Q_H par translation serait réduit à $\{e\}$. On aurait donc $G \simeq G/\operatorname{Ker}\gamma \simeq \operatorname{Im}\gamma$. Ainsi, G serait isomorphe à un sous-groupe de $S(Q_H)$, et donc $|G|$ diviserait $|S(Q_H)|$. Mais par définition de l'indice, on a $k = [G : H] = |Q_H|$, et donc $|S(Q_H)| = k!$ □

Remarque. Soient G un groupe et H un sous-groupe propre de G. On peut considérer la restriction à H de l'action considérée en 3.3.1, c'est-à-dire faire opérer H sur Q_H par translation à gauche :

$$\left|\begin{array}{ccc} H \times Q_H & \longrightarrow & Q_H \\ (h, xH) & \longmapsto & h.xH = hxH \end{array}\right.$$

Cette action n'est plus transitive.

En effet. Pour tout $xH \in Q_H$, c'est-à-dire pour tout $x \in G$, l'orbite de xH est $\Omega_{xH} = \{hxH\,;\, h \in H\}$. En particulier $\Omega_{eH} = \Omega_H = \{hH\,;\, h \in H\} = \{H\}$. Si l'action ci-dessus était transitive, on aurait pour tout $x \in G$: $\Omega_{xH} = \Omega_{eH}$, donc $xH = H$, donc $x \in H$. Ce qui contredirait l'hypothèse $H \neq G$.

THÉORÈME. *Soit G un groupe fini. Soit H un sous-groupe de G dont l'indice $p = [G : H]$ est le plus petit diviseur premier de $|G|$. Alors H est normal dans G.*

> *Preuve.* Considérons l'action de H sur Q_H par translation à gauche. Comme on vient de le voir, elle n'est pas transitive. Il existe donc un nombre $r \geq 2$ d'orbites distinctes $\Omega_{x_1 H}, \ldots, \Omega_{x_r H}$. Notons $q_i = |\Omega_{x_i H}|$ pour tout $1 \leq i \leq r$. D'une part les orbites forment une partition de Q_H, donc $p = [G : H] = |Q_H| = q_1 + \cdots + q_r$. D'autre part chaque q_i divise $|G|$. Si l'un des q_i n'est pas 1, il est forcément $\geq p$ (car p est le plus petit diviseur > 1 de $|G|$) et, comme $r \geq 2$, cela contredit l'égalité $p = q_1 + \cdots + q_r$. C'est donc que chaque q_i vaut 1 et que $r = p$. En d'autres termes, pour tout $1 \leq i \leq p$, le stabilisateur $H_{x_i H}$ est égal à H.
>
> Soit $x \in G$. Il existe un unique $1 \leq i \leq p$ tel que $\Omega_{xH} = \Omega_{x_i H}$, ce qui, comme on l'a vu en 3.2.1, implique que les stabilisateurs H_{xH} et $H_{x_i H}$ sont conjugués dans H (le groupe qui opère est ici H). Il existe donc $h \in H$ tel que $H_{xH} = h H_{x_i H} h^{-1}$. Or on a vu ci-dessus que $H_{x_i H} = H$. Donc $H_{xH} = hHh^{-1} = H$. Ainsi tout $h \in H$ vérifie $h.xH = xH$, c'est-à-dire $x^{-1}hx \in H$, ou encore $h \in xHx^{-1}$. Ceci prouve que $H \subset xHx^{-1}$.
>
> On en déduit que, pour tout $x \in G$, on a : $x^{-1}Hx \subseteq x^{-1}(xHx^{-1})x = H$. On conclut : $H \lhd G$. □

REMARQUE. Pour $p = 2$, on retrouve le fait que tout sous-groupe d'indice 2 est normal.

Chapitre 4

Théorèmes de Sylow et applications

4.1 Les théorèmes de Sylow

4.1.1 Premier théorème de Sylow

Remarque préliminaire. Il n'y a pas de réciproque naïve au théorème de Lagrange, au sens où, pour un diviseur m de l'ordre n d'un groupe fini G, il n'existe pas forcément de sous-groupe d'ordre m dans G. On a vu par exemple que le groupe alterné A_4, qui est d'ordre 12, ne contient pas de sous-groupe d'ordre 6. Le premier théorème de Sylow montre que ce type de situation ne peut pas se produire lorsque m est une puissance d'un nombre premier.

Lemme technique. *Soit p un nombre premier. Soient r, s, n trois entiers naturels non-nuls tels que $r \leq n$ et p ne divise pas s. Alors le coefficient binomial $\binom{sp^n}{p^r}$ est de la forme kp^{n-r} pour un entier $k \geq 1$ non divisible par p.*

Preuve. On calcule : $\binom{sp^n}{p^r} = \dfrac{(sp^n)!}{p^r!(sp^n-p^r)!} = \dfrac{sp^n(sp^n-1)(sp^n-2)\dots(sp^n-p^r+1)}{p^r(p^r-1)\times\cdots\times 2\times 1}$

$$= \frac{sp^n}{p^r}\times\frac{sp^n-1}{1}\times\frac{sp^n-2}{2}\times\cdots\frac{sp^n-(p^r-1)}{p^r-1} = p^{n-r}\times\underbrace{s\times\prod_{j=1}^{p^r-1}\frac{sp^n-j}{j}}_{\text{soit } k}$$

Considérons un entier $1 \leq j \leq p^r-1$. Ecrivons-le sous la forme $j = b_j p^{t_j}$ avec $t_j \in \mathbb{N}$ et b_j non divisible par p. Comme $j < p^r$, on a nécessairement $t_j < r$, et donc $n - t_j \geq r - t_j \geq 1$. On écrit :

$$\frac{sp^n-j}{j} = \frac{sp^n-b_jp^{t_j}}{b_jp^{t_j}} = \frac{sp^{n-t_j}-b_j}{b_j} := \frac{a_j}{b_j}, \quad \text{en posant } a_j := sp^{n-t_j}-b_j.$$

Comme p ne divise pas b_j, il ne divise pas non plus a_j. Parce que p est premier, cela implique que p ne divise pas les entiers $a := a_1\times\cdots\times a_{p^r-1}$ et $b := b_1\times\cdots\times b_{p^r-1}$. En résumé, $k = \frac{sa}{b}$, où p ne divise ni s, ni a, ni b.

On a l'égalité : $sap^{n-r} = b\binom{sp^n}{p^r}$. Donc p^{n-r} divise $b\binom{sp^n}{p^r}$. Mais p^{n-r} est premier avec b puisque p est premier ne divisant pas b. On déduit avec le lemme de Gauss que p^{n-r} divise $\binom{sp^n}{p^r}$, donc $k = \dfrac{1}{p^{n-r}}\binom{sp^n}{p^r}$ est entier. Enfin, puisque p ne divise pas sa, il résulte de l'égalité $sa = kb$ et du lemme de Gauss que p ne divise pas k. □

THÉORÈME (dit premier théorème de Sylow). *Soit G un groupe fini. Soit p un nombre premier divisant $|G|$. Notons $|G| = sp^n$ avec $n \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$ non divisible par p. Alors, pour tout entier $1 \leq r \leq n$, il existe un sous-groupe de G d'ordre p^r.*

Preuve. Fixons $1 \leq r \leq n$ et notons E l'ensemble des parties de G à p^r éléments. Donc $|E| = \binom{|G|}{p^r} = \binom{sp^n}{p^r}$. D'après le lemme, il existe $k \in \mathbb{N}^*$ non-divisible par p tel que $|E| = kp^{n-r}$.

Pour tout $A \in E$ et tout $g \in G$, on a $|gA| = |A| = p^r$, donc G opère sur E par translation :

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (g, A) & \longmapsto & gA. \end{array}$$

Soit $\{A_i\}_{1 \leq i \leq m}$ une famille de représentants des orbites distinctes pour cette action. On sait (voir 3.2.1) que $\sum_{i=1}^{m} [G : G_{A_i}] = |E| = kp^{n-r}$, où G_{A_i} est le stabilisateur de A_i. Si p^{n-r+1} divisait tous les $[G : G_{A_i}]$, il diviserait kp^{n-r}, donc p diviserait k, ce qui n'est pas le cas.

On a ainsi montré qu'il existe un entier $1 \leq h \leq m$ tel que p^{n-r+1} ne divise pas $[G : G_{A_h}]$. Pour cet entier h, notons H le stabilisateur G_{A_h}. On se propose de montrer que H est un des sous-groupes d'ordre p^r cherché.

On a : $[G : H] \times |H| = |G| = sp^n$. Si l'on note $[G : H] = s'p^\alpha$ et $|H| = s''p^\beta$, avec $\alpha, \beta \in \mathbb{N}$, et $s', s'' \in \mathbb{N}^*$ non divisibles par p, on a donc : $s's'' = s$ et $\alpha + \beta = n$. La condition $[G : H]$ non divisible par p^{n-r+1} se traduit en outre par l'inégalité $\alpha \leq n - r$. Il en résulte que $r \leq n - \alpha \leq n$, c'est-à-dire $r \leq \beta \leq n$, donc p^r divise p^β, et donc p^r divise $|H|$.

Par ailleurs, par définition du stabilisateur $G_{A_h} = H$, on a $gA_h = A_h$ pour tout $g \in H$. Ceci permet de considérer, pour un élément $a \in A_h$ fixé quelconque, l'application $f : H \to A_h$ définie par $f(g) = ga$ pour tout $g \in H$. Elle est clairement injective, donc $|H| \leq |A_h|$. Mais $|A_h| = p^r$ puisque $A_h \in E$. Ainsi $|H| \leq p^r$. On a vu précédemment que p^r divise $|H|$. On conclut que $|H| = p^r$. □

COROLLAIRE (dit théorème de Cauchy). *Soit G un groupe fini. Pour tout nombre premier p divisant $|G|$, il existe dans G un élément d'ordre p.*

Preuve. On applique le théorème pour $r = 1$. Il existe dans G un sous-groupe H d'ordre p. Comme H est d'ordre premier, il est cyclique, engendré par un élément d'ordre p. □

4.1.2 Sous-groupes de Sylow

DÉFINITIONS. Soit G un groupe fini. Soit p un nombre premier divisant $|G|$. Notons $|G| = sp^n$ avec $n \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$ non divisible par p.

1. On appelle *p-sous-groupe* de G tout sous-groupe de G dont l'ordre est une puissance de p, c'est-à-dire tout sous-groupe H de G tel que $|H| = p^r$ avec $0 \leq r \leq n$.

2. On appelle *p-sous-groupe de Sylow* de G tout p-sous-groupe de G d'ordre maximal, c'est-à-dire tout sous-groupe H de G tel que $|H| = p^n$.

   Exemple. Soit G un groupe fini d'ordre 72. Il existe dans G des sous-groupes d'ordre 2, 4 et 8. Parmi eux, les 2-sous-groupes de Sylow sont ceux d'ordre 8. Il existe aussi dans G des sous-groupes d'ordre 3 et 9. Parmi eux, les 3-sous-groupes de Sylow sont ceux d'ordre 9.

Le théorème suivant a pour objet de préciser la structure des p-sous-groupes de Sylow dont le théorème précédent a établi l'existence.

4.1.3 Second théorème de Sylow

LEMME 1. *Si G est un p-groupe non trivial opérant sur un ensemble fini non-vide E, alors :* $|E^G| \equiv |E| \bmod p$.

Preuve. Démontré en 3.2.4. □

LEMME 2. *Soit G un groupe. Soit p un nombre premier. On suppose qu'il existe dans G un sous-groupe K d'ordre p^r, avec $r \geq 1$, et un sous-groupe H d'indice s non divisible par p. Alors K est inclus dans un conjugué de H.*

Preuve. Soit Q_H l'ensemble des classes à gauche modulo H ; donc $Q_H = \{xH\,;\, x \in G\}$. Considérons l'action de K sur Q_H par translation à gauche :

$$\begin{array}{ccc} K \times Q_H & \longrightarrow & Q_H \\ (g\,,\, xH) & \longmapsto & gxH. \end{array}$$

En appliquant le lemme 1 au p-groupe K, on a $|(Q_H)^K| \equiv |Q_H| \bmod p$. Or $|Q_H| = [G : H] = s$, qui n'est pas divisible par p. On en tire : $|(Q_H)^K| \neq 0$, c'est-à-dire $(Q_H)^K \neq \emptyset$. Il existe donc $x \in G$ tel que la classe à gauche xH soit un point fixe de l'action. On a :

$$(xH \in (Q_H)^K) \;\Leftrightarrow\; (\forall\, g \in K,\; gxH = xH) \;\Leftrightarrow\; (\forall\, g \in K,\; gx \in xH) \;\Leftrightarrow\; (K \subseteq xHx^{-1}),$$

d'où le résultat. □

LEMME 3. *Soient G un groupe fini, et p un nombre premier divisant $|G|$. Si H est un p-sous-groupe de Sylow de G, alors H est l'unique p-sous-groupe de Sylow de son normalisateur.*

Preuve. Notons $|G| = sp^n$ avec $n \geq 1$ et $s \geq 1$ non divisible par p. On a donc $|H| = p^n$. Considérons le normalisateur $N_G(H)$ de H dans G. C'est un sous-groupe de G, donc son ordre divise $|G| = sp^n$. Posons $|N_G(H)| = s'p^\alpha$ avec $s' \in \mathbb{N}^*$ non divisible par p et $0 \leq \alpha \leq n$. Par ailleurs, H est un sous-groupe de $N_G(H)$, donc $|H| = p^n$ divise $|N_G(H)| = s'p^\alpha$. On a donc finalement $|N_G(H)| = s'p^n$, d'où $[N_G(H) : H] = s'$.

Soit K un p-sous-groupe de Sylow de $N_G(H)$. On a donc $|K| = p^n$. En appliquant le lemme 2 aux sous-groupes H et K du groupe $N_G(H)$, on déduit qu'il existe $x \in N_G(H)$ tel que $K \subseteq xHx^{-1}$. Mais $H \lhd N_G(H)$, de sorte que $xHx^{-1} = H$. On conclut que $K \subseteq H$, ce qui, comme les deux groupes sont de même ordre p^n, permet de conclure que $K = H$. □

THÉORÈME (dit second théorème de Sylow). *Soit G un groupe fini. Soit p un nombre premier divisant $|G|$. Notons $|G| = sp^n$ avec $n \in \mathbb{N}^*$ et $s \in \mathbb{N}^*$ non divisible par p. Alors :*

(i) *tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow ;*

(ii) *les p-sous-groupes de Sylow de G sont conjugués dans G ;*

(iii) *le nombre N_p des p-sous-groupes de Sylow de G vérifie :*

$$N_p \text{ divise } s, \qquad \text{et} \qquad N_p \equiv 1 \bmod p.$$

Preuve. (i). Soit K un p-sous-groupe de G non trivial ; notons $|K| = p^r$ avec $1 \leq r \leq n$. Soit H un p-sous-groupe de Sylow de G ; donc $|H| = p^n$, d'où $[G : H] = s$. Comme p ne divise pas s, on peut appliquer le lemme 2 : il existe $x \in G$ tel que $K \subseteq xHx^{-1}$. Mais $|xHx^{-1}| = |H| = p^n$, de sorte que xHx^{-1} est lui-même un p-sous-groupe de Sylow de G.

(ii). Si H et H' sont deux p-sous-groupes de Sylow de G, le raisonnement ci-dessus appliqué à $K = H'$ montre que $H' \subseteq xHx^{-1}$ pour un certain $x \in G$. Mais $|H'| = p^n = |H| = |xHx^{-1}|$, donc $H' = xHx^{-1}$.

(iii). Notons $\mathscr{S}$ l'ensemble des p-sous-groupes de Sylow de G, et $N_p = |\mathscr{S}|$. Il résulte du point (ii) ci-dessus que G opère transitivement par conjugaison sur $\mathscr{S}$. Il n'y a donc qu'une seule orbite :

$$\text{pour tout } H \in \mathscr{S}, \text{ on a } \mathscr{S} = \Omega_H \text{ et } N_p = |\mathscr{S}| = |\Omega_H| = [G : G_H].$$

Fixons un p-sous-groupe de Sylow $H \in \mathscr{S}$. Le stabilisateur G_H est ici $\{x \in G\,;\, xHx^{-1} = H\}$, qui n'est autre que le normalisateur $N_G(H)$ de H dans G. D'où : $N_p = [G : N_G(H)] = |G|/|N_G(H)|$. Comme $|H|$ divise $|N_G(H)|$, l'entier $|G|/|N_G(H)|$ divise l'entier $|G|/|H| = s$. On a ainsi montré que N_p divise s.

Par ailleurs, il est clair que H opère sur $\mathscr{S}$ par conjugaison. En appliquant le lemme 1, on obtient $|\mathscr{S}^H| \equiv |\mathscr{S}| \bmod p$, c'est-à-dire $N_p \equiv |\mathscr{S}^H| \bmod p$. Or $\mathscr{S}^H$ est l'ensemble des éléments $H' \in \mathscr{S}$ tels que $H' = xH'x^{-1}$ pour tout $x \in H$, c'est-à-dire tels que $H \subset N_G(H')$. Mais d'après le lemme 3, le seul p-sous-groupe de Sylow de G contenu dans $N_G(H')$ est H'. On conclut que $H' = H$, donc $|\mathscr{S}^H| = 1$. Ce qui achève la preuve du point (iii). □

COROLLAIRE. *Soient G un groupe fini et p un diviseur premier de $|G|$.*

(i) *Soit H un p-sous-groupe de Sylow de G ; alors H est le seul p-sous-groupe de Sylow de G si et seulement si H est normal dans G.*

(ii) *Si G est abélien, il n'existe dans G qu'un seul p-sous-groupe de Sylow.*

Preuve. Le point (i) est une conséquence immédiate du point (ii) du théorème précédent. Le point (ii) découle immédiatement de (i). □

4.2 Exemples d'applications

4.2.1 Sous-groupes de Sylow d'un groupe abélien

REMARQUE PRÉLIMINAIRE. On a rappelé au chapitre 2 la notion de produit direct de deux sous-groupes d'un groupe. Cette notion se généralise aisément à un nombre fini quelconque de sous-groupes, de la façon suivante : soient G un groupe, et $H_1, \ldots, H_k$ des sous-groupes de G ; on dit que G est le produit direct des sous-groupes $H_1, \ldots, H_k$ lorsque :

(1) $G = H_1 H_2 \ldots H_k$,

(2) $H_i \cap (H_1 \ldots H_{i-1} H_{i+1} \ldots H_k) = \{e\}$ pour tout $1 \leq i \leq k$;

(3) $h_i h_j = h_j h_i$ pour tous $h_i \in H_i, h_j \in H_j$, quels que soient $1 \leq i \neq j \leq k$.

Dans ce cas, tout élément de G s'écrit de façon unique comme un produit $h_1 h_2 \ldots h_k$ avec $h_1 \in H_1, h_2 \in H_2, \ldots, h_k \in H_k$.

Il est clair que, si $G_1, \ldots, G_k$ sont k groupes quelconques, un groupe G est isomorphe au produit direct externe $G_1 \times \cdots \times G_k$ (au sens de 1.1.4) et seulement s'il existe dans G des sous-groupes $H_1, \ldots, H_k$ tels que G soit le produit direct (interne) des sous-groupes $H_1, \ldots, H_k$ et tels que $H_i \simeq G_i$ pour tout $1 \leq i \leq k$.

LEMME. *Soit G un groupe fini non trivial. Soit $|G| = p_1^{n_1} \ldots p_k^{n_k}$ la décomposition en facteurs premiers de l'ordre de G, avec les p_i premiers deux à deux distincts et les n_i entiers ≥ 1.*
Si G admet pour tout $1 \leq i \leq k$ un unique p_i-sous-groupe de Sylow H_i, alors G est le produit direct des H_i.

Preuve. Remarquons d'abord que, pour tous $1 \leq i \neq j \leq k$, on a $H_i \cap H_j = \{e\}$ d'après le théorème de Lagrange. De plus $H_i \triangleleft G$ pour tout $1 \leq i \leq k$ d'après le point (i) du dernier corollaire de 4.1.3. Dès lors, pour tous $h_i \in H_i$ et $h_j \in H_j$:

$$h_j^{-1}h_ih_jh_i^{-1} = h_j^{-1}(h_ih_jh_i^{-1}) \in H_j \quad \text{et} \quad h_j^{-1}h_ih_jh_i^{-1} = (h_j^{-1}h_ih_j)h_i^{-1} \in H_i,$$

de sorte que $h_j^{-1}h_ih_jh_i^{-1} \in H_i \cap H_j = \{e\}$ et donc $h_ih_j = h_jh_i$. Les autres conditions assurant que G est le produit direct $H_1H_2 \dots H_k$ sont alors claires en raisonnant sur les ordres. □

THÉORÈME. *Tout groupe abélien fini non trivial est produit direct de ses sous-groupes de Sylow.*

Preuve. D'après le point (ii) du dernier corollaire de 4.1.3, on est dans les conditions d'application du lemme précédent, qui donne immédiatement le résultat voulu. □

► *Remarque :* Soit G un groupe abélien fini non trivial. Soit $|G| = p_1^{n_1} \dots p_k^{n_k}$ la décomposition en facteurs premiers de l'ordre de G, avec les p_i premiers deux à deux distincts et les $n_i \geq 1$. Fixons $1 \leq i \leq k$ quelconque. Le p_i-sous-groupe de Sylow H_i de G, qui est d'ordre $p_i^{n_i}$, s'exprime d'après le théorème 1.2.3 comme un produit de groupes cycliques $C_{p_i^{r_1}}C_{p_i^{r_2}} \cdots C_{p_i^{r_m}}$ pour des entiers $1 \leq r_1 \leq r_2 \leq \cdots \leq r_m$ uniques, satisfaisant $r_1 + r_2 + \cdots + r_m = n_i$. On retrouve ainsi les liens entre décomposition suivant les facteurs invariants et décomposition suivant les diviseurs élémentaires pour les groupes abéliens finis.

4.2.2 Quelques résultats de non-simplicité

PROPOSITION 1. *Tout groupe d'ordre pq avec p et q deux nombres premiers distincts est non simple.*

Preuve. Soit G un groupe d'ordre pq. Quitte à échanger les rôles de p et q, on peut sans restriction supposer que $p > q$. On sait par le second théorème de Sylow que le nombre N_p de p-sous-groupes de Sylow de G divise q, et vérifie $N_p \equiv 1 \bmod p$. Comme q est premier, on ne peut avoir que $N_p = 1$ ou $N_p = q$. Si l'on avait $N_p = q$, on aurait $q \equiv 1 \bmod p$, donc p diviserait $q - 1$, ce qui contredit l'hypothèse $p > q$. C'est donc que $N_p = 1$. Il y a un seul p-sous-groupe de Sylow ; on sait qu'il est alors normal dans G, et donc G n'est pas simple. □

PROPOSITION 2. *Tout groupe d'ordre p^2q avec p et q deux nombres premiers distincts est non simple.*

Preuve. Soit G un groupe d'ordre p^2q. D'après le second théorème de Sylow, le nombre N_q de q-sous-groupes de Sylow de G divisant p^2, trois cas sont possibles.

Si $N_q = 1$, l'unique q-sous-groupe de Sylow est normal, donc G n'est pas simple.

Si $N_q = p$, il résulte de la condition $N_q \equiv 1 \bmod q$ qu'il existe $\lambda \in \mathbb{N}$ tel que $p = \lambda q + 1$. Comme $p \neq 1$, on a $\lambda \geq 1$, donc $p \geq q + 1$. Par ailleurs, le nombre N_p de p-sous-groupes de Sylow divise q, donc vaut 1 ou q. Supposons que l'on ait $N_p = q$. La condition $N_p \equiv 1 \bmod p$ devenant $q \equiv 1 \bmod p$, on déduit comme ci-dessus que $q \geq p+1$, d'où une contradiction avec l'inégalité $p \geq q+1$ précédente. C'est donc que $N_p = 1$; l'unique p-sous-groupe de Sylow est alors normal, donc G n'est pas simple.

Si $N_q = p^2$, notons $(S_i)_{1 \leq i \leq p^2}$ les q-sous-groupes de Sylow. Chacun est d'ordre q premier, donc cyclique, donc formé du neutre e et de $(q-1)$ éléments d'ordre q. Comme les S_i sont d'intersection deux à deux réduite à $\{e\}$, (cela résulte immédiatement du théorème de

Lagrange), la réunion des S_i comprend $p^2 \times (q-1)$ éléments d'ordre q, (plus le neutre e d'ordre 1). Le cardinal de l'ensemble des éléments de G qui ne sont pas d'ordre q est donc : $|G| - p^2(q-1) = p^2q - p^2(q-1) = p^2$. Ce cardinal p^2 ne permet dans G que l'existence d'un seul p-sous-groupe de Sylow. Ce dernier est alors normal, donc G n'est pas simple. □

PROPOSITION 3. *Tout groupe d'ordre pqr avec p, q et r trois nombres premiers distincts est non simple.*

Preuve. Soit G un groupe d'ordre pqr. Quitte à permuter, on peut sans restriction supposer que $p > q > r$. Soit N_p, N_q, N_r les nombres respectifs de p-sous-groupes, q-sous-groupes et r-sous-groupes de Sylow de G.

Montrons d'abord que l'on a l'inégalité : (*) $\quad pqr \geq N_p(p-1) + N_q(q-1) + N_r(r-1)$.

Désignons par S_i, pour $1 \leq i \leq N_p$ les p-sous-groupes de Sylow de G. Chacun d'eux est d'ordre p, donc contient $p-1$ éléments d'ordre p (plus le neutre e qui est d'ordre 1). Comme les S_i sont d'intersection deux à deux réduite à $\{e\}$, (cela résulte immédiatement du théorème de Lagrange), la réunion des S_i comprend $N_p \times (p-1)$ éléments d'ordre p, (plus le neutre e d'ordre 1). Donc G contient $N_p(p-1)$ éléments d'ordre p, et de même bien sûr $N_q(q-1)$ éléments d'ordre q et $N_r(r-1)$ éléments d'ordre r. Comme $|G| = pqr$, on obtient l'inégalité (*) voulue.

Faisons maintenant l'hypothèse : (H) $\quad N_p > 1$ et $N_q > 1$ et $N_r > 1$.

(1) On sait que N_p divise qr. D'après (H), le cas $N_p = 1$ est exclu. Supposons que $N_p = q$; on aurait alors $q \equiv 1 \bmod p$, ce qui impliquerait (comme on l'a vu dans la preuve de la proposition 2) que $q \geq p+1$. Ceci est contraire aux hypothèses de départ, ce qui prouve que $N_p = q$ est impossible. De même $N_p = r$ conduirait à $r \geq p+1$ et une contradiction. On conclut donc finalement que : $N_p = qr$.
(2) On sait que N_q divise pr. D'après (H), le cas $N_q = 1$ est exclu. Supposons que $N_q = r$; on aurait alors $r \equiv 1 \bmod q$, ce qui impliquerait (comme on l'a vu dans la preuve de la proposition 2) que $r \geq q+1$. Ceci est contraire aux hypothèses de départ, ce qui prouve que $N_q = r$ est impossible. Donc, $N_q = p$ ou pr. Dans les deux cas, on a : $N_q \geq p$.
(3) On sait que N_r divise pq. D'après (H), le cas $N_r = 1$ est exclu. Donc, $N_r = p$ ou q ou pq. Dans les trois cas, on a : $N_r \geq q$.

Il résulte de (1), (2) et (3) que $N_p(p-1)+N_q(q-1)+N_r(r-1) \geq qr(p-1)+p(q-1)+q(r-1) = pqr + pq - p - q$. L'inégalité (*) implique alors $p+q \geq pq$. Ceci est impossible, ce qui prouve que la condition (H) est absurde. On a donc $N_p = 1$ ou $N_q = 1$ ou $N_r = 1$. On sait que l'unique sous-groupe de Sylow est alors normal, et donc G n'est pas simple. □

LEMME 4. *Soit G un groupe d'ordre p^nq avec p et q deux nombres premiers distincts et $n \geq 2$. Si $p > q$, ou si p^n ne divise pas $(q-1)!$, alors G n'est pas simple.*

Preuve. Supposons d'abord $p > q$. Soit N_p le nombre de p-sous-groupes de Sylow de G. On sait que N_p divise q, donc vaut q ou 1. Si $N_p = q$, la condition $N_p \equiv 1 \bmod p$ devient $q \equiv 1 \bmod p$, et il existe donc $\lambda \in \mathbb{N}$ tel que $q = \lambda p + 1$. L'entier λ est non-nul car $q \neq 1$, donc $q > p$, ce qui contredit l'hypothèse $p > q$. C'est donc que $N_p = 1$; l'unique p-sous-groupe de Sylow est alors normal, donc G n'est pas simple. (On peut aussi utiliser directement le théorème de Frobenius).

Supposons maintenant que p^n ne divise pas $(q-1)!$. Soit H un p-sous-groupe de Sylow de G. Il est d'ordre p^n donc $[G : H] = |G||H|^{-1} = p^nqp^{-n} = q \geq 2$. Par ailleurs l'hypothèse faite implique que $p^nq = |G|$ ne divise pas $q!$. On applique alors le corollaire de 3.3.2 pour conclure que G n'est pas simple. □

PROPOSITION 5. *Les groupes abéliens simples sont les groupes cycliques d'ordre premier.*

Preuve. Soit G un groupe abélien simple. Il n'admet donc aucun sous-groupe hormis $\{e\}$ et G. Soient x un élément quelconque de G distinct de e, et $\langle x\rangle$ le sous-groupe monogène engendré par x. Comme $\langle x\rangle \neq \{e\}$, on a nécessairement $G = \langle x\rangle$, de sorte que G est monogène. Si G était infini, il serait isomorphe au groupe additif $\mathbb{Z}$, qui n'est évidemment pas simple (tout $n\mathbb{Z}$ avec $n \in \mathbb{Z}$ est un sous-groupe). C'est donc que G est fini. On conclut que G est cyclique. Soit $p = |G| = |x|$. Pour tout diviseur d de p dans $\mathbb{N}$, l'élément x^d engendre un sous-groupe de G d'ordre pd^{-1}. La simplicité de G implique que $d = 1$ ou $d = p$, ce qui prouve que p est premier. Il est clair réciproquement que tout groupe cyclique d'ordre premier est abélien simple. □

COROLLAIRE 6. *Tout groupe d'ordre p^n avec p premier et $n \geq 2$ n'est pas simple.*

Preuve. Par l'absurde, supposons que G soit simple d'ordre p^n avec p premier et $n \geq 2$. On sait d'après la proposition 3.2.4 que son centre $Z(G)$ n'est pas réduit à $\{e\}$. Comme $Z(G) \triangleleft G$, la simplicité de G implique alors $Z(G) = G$. Donc G est abélien. Mais alors la proposition 6 implique que G est d'ordre premier, d'où la contradiction puisque $n \geq 2$. □

EXERCICE 7. *Soit G un groupe d'ordre $p^n q^m$ avec p et q deux nombres premiers distincts et $n, m \geq 1$. Si $p^n < q + 1$, alors G n'est pas simple.*

Solution. Soit N_q le nombre de q-sous-groupes de Sylow de G. On sait que N_q divise p^n ; il existe donc un entier $0 \leq \alpha \leq n$ tel que $N_q = p^\alpha$. De plus la condition $N_q \equiv 1 \bmod q$ implique qu'il existe $\lambda \in \mathbb{N}$ tel que $N_q = \lambda q + 1$. Ainsi $p^\alpha = \lambda q + 1$. Mais $p^\alpha \leq p^n$ qui est, par hypothèse, strictement inférieur à $q+1$. Donc $\lambda q < q$, c'est-à-dire $\lambda = 0$. On conclut que $N_q = 1$; l'unique q-sous-groupe de Sylow est alors normal, et donc G n'est pas simple. □

EXERCICE 8. Montrer que tout groupe d'ordre 36, 40, ou 56, n'est pas simple.

Solution. Observons d'abord que ces trois entiers ne satisfont les hypothèses d'aucun des résultats précédents, et nécessitent donc une étude particulière.

Si $|G| = 40 = 5 \times 2^3$, on a N_5 qui divise 2^3, donc vaut $1, 2, 4$ ou 8. La condition $N_5 \equiv 1 \bmod 5$ n'est vérifiée que pour $N_5 = 1$. L'unique 5-sous-groupe de Sylow est alors normal dans G. Donc G n'est pas simple.

Si $|G| = 56 = 7 \times 2^3$, on a N_7 qui divise 2^3, donc vaut $1, 2, 4$ ou 8. La condition $N_7 \equiv 1 \bmod 7$ n'est vérifiée que pour $N_7 = 1$ ou $N_7 = 8$. Si $N_7 = 1$, l'unique 7-sous-groupe de Sylow est normal donc G n'est pas simple. Supposons maintenant que $N_7 = 8$. Notons $S_1, \ldots, S_8$ les 7-sous-groupes de Sylow de G. Chaque S_i comprend 6 éléments d'ordre 7 plus le neutre d'ordre 1. Comme $S_i \cap S_j = \{e\}$ si $i \neq j$, le groupe G contient donc $8 \times 6 = 48$ éléments d'ordre 7. Il reste alors $56 - 48 = 8$ éléments disponibles et, comme les 2-sous-groupes de Sylow de G sont d'ordre 8, il ne peut exister qu'un seul 2-sous-groupe de Sylow. Il est donc normal, et G n'est pas simple.

Si $|G| = 36 = 3^2 \times 2^2$, on a N_3 qui divise 2^2, donc vaut $1, 2$ ou 4. La condition $N_3 \equiv 1 \bmod 3$ n'est vérifiée que pour $N_3 = 1$ ou $N_3 = 4$. Si $N_3 = 1$, l'unique 3-sous-groupe de Sylow est normal donc G n'est pas simple. Supposons maintenant que $N_3 = 4$. Notons $S_1, \ldots, S_4$ les 3-sous-groupes de Sylow de G. On sait qu'ils sont tous conjugués ; notons $\Omega_{S_1} = \{S_1, S_2, S_3, S_4\}$ la classe de conjugaison qu'ils forment. Son cardinal est $|\Omega_{S_1}| = [G : N_1]$ où le stabilisateur N_1 est ici le normalisateur $N_1 = N_G(S_1)$. Ainsi, $[G : N_1] = 4$ et $|G| = 36$ ne divise pas $4! = 24$; on conclut avec le corollaire 3.3.2 que G n'est pas simple. □

THÉORÈME DE SYNTHÈSE. *Il n'existe pas de groupes simples non abéliens d'ordre* < 60.

Preuve. Soit G un groupe fini d'ordre $n < 60$.

Si $n = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53$ ou 59, G est d'ordre premier, donc cyclique d'ordre premier, donc abélien simple d'après la proposition 5.

Si $n = 4, 8, 9, 16, 25, 27, 32$ ou 49, le corollaire 6 montre que G n'est pas simple.

Si $n = 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57$ ou 58, la proposition 1 montre que G n'est pas simple.

Si $n = 12, 18, 20, 28, 44, 45, 50$ ou 52, la proposition 2 montre que G n'est pas simple.

Si $n = 24$ ou 48, le second cas du lemme 4 montre que G n'est pas simple. Si $n = 54$, le premier cas du lemme 4 montre que G n'est pas simple. Si $n = 30$ ou 42, la proposition 3 montre que G n'est pas simple. Les seuls cas restants sont $n = 36, 40$ ou 56, qui font l'objet de l'exercice 8. □

REMARQUE. Le groupe alterné A_5 est non-abélien, d'ordre 60, et on verra dans le chapitre suivant qu'il est simple.

4.2.3 Quelques résultats de classification

PROPOSITION. *Tout groupe d'ordre pq avec p et q premiers distincts tels $q \not\equiv 1 \bmod p$ et $p \not\equiv 1 \bmod q$ est cyclique.*

Preuve. On a : N_p divise q, donc $N_p = q$ ou $N_p = 1$, et $N_p \equiv 1 \bmod p$. L'hypothèse $q \not\equiv 1 \bmod p$ implique alors $N_p = 1$; notons S l'unique p-sous-groupe de Sylow de G, qui est donc normal dans G. De même G admet un unique q-sous-groupe de Sylow T, et il est normal dans G. Comme $|S| = p$ et $|T| = q$, il est clair par le théorème de Lagrange que $S \cap T = \{e\}$, donc $|ST| = pq$, et donc $G = ST$ est produit direct de $S \simeq C_p$ et $T \simeq C_q$. On conclut par le théorème des restes chinois que $G \simeq C_{pq}$. □

PROPOSITION. *Tout groupe d'ordre $2p$ avec p premier impair est cyclique ou diédral.*

Preuve. Comme $p > 2$, la preuve de la proposition 1 de 4.2.2 avec $q = 2$ montre que G admet un unique p-sous-groupe de Sylow. Notons-le S ; il est normal dans G et d'ordre p.

Par ailleurs, le nombre N_2 de 2-sous-groupes de Sylow de G divisant p, il ne peut valoir que 1 ou p. Si $N_2 = 1$, l'unique 2-sous-groupe de Sylow T de G est normal dans G, d'ordre 2, et en reprenant la preuve de la proposition précédente, on conclut que $G \simeq C_{2p}$.

Supposons donc maintenant $N_2 = p$. Soit $y \in G$ tel que $y \notin S$. L'ordre de y divise $2p$, ne peut pas valoir 1 (car sinon $y = e \in S$), ne peut pas valoir p (car sinon $\langle y \rangle$ est un sous-groupe d'ordre p, donc égal à S par unicité de S, d'où $y \in S$), et ne peut pas valoir $2p$ (car sinon $\langle y \rangle$ est un sous-groupe d'ordre $2p$, donc égal à G, d'où $G \simeq C_{2p}$, ce qui contredit $N_2 = p$ puisque C_{2p} admet un unique sous-groupe d'ordre 2). On conclut donc que les p éléments de G qui ne sont pas dans S sont tous d'ordre 2. On conclut que $G \simeq \mathbb{D}_{2p}$. □

THÉORÈME DE SYNTHÈSE. *Tous les groupes d'ordre ≤ 15 sont, à isomorphisme près, donnés dans le tableau suivant :*

ordre du groupe	*groupes abéliens*	*groupes non abéliens*
$n = 1$	groupe trivial $C_1 = \{e\}$	
$n = 2$	groupe cyclique C_2	
$n = 3$	groupe cyclique C_3	
$n = 4$	groupe cyclique C_4 groupe de Klein $C_2 \times C_2$ = groupe diédral $\mathbb{D}_4$	
$n = 5$	groupe cyclique C_5	
$n = 6$	groupe cyclique C_6	groupe symétrique S_3 = groupe diédral $\mathbb{D}_6$
$n = 7$	groupe cyclique C_7	
$n = 8$	groupe cyclique C_8 produit direct $C_2 \times C_4$ produit direct $C_2 \times C_2 \times C_2$	groupe diédral $\mathbb{D}_8$ groupe quaternionique Q_8
$n = 9$	groupe cyclique C_9 produit direct $C_3 \times C_3$	
$n = 10$	groupe cyclique C_{10}	groupe diédral $\mathbb{D}_{10}$
$n = 11$	groupe cyclique C_{11}	
$n = 12$	groupe cyclique C_{12} produit direct $C_2 \times C_6$	groupe diédral $\mathbb{D}_{12}$ groupe quaternionique Q_{12} groupe alterné A_4
$n = 13$	groupe cyclique C_{13}	
$n = 14$	groupe cyclique C_{14}	groupe diédral $\mathbb{D}_{14}$
$n = 15$	groupe cyclique C_{15}	

Preuve. Les deux propositions précédentes, ainsi que le fait que tout groupe d'ordre premier soit cyclique (voir 1.1.3) et que tout groupe d'ordre p^2 avec p premier soit abélien (voir 3.2.4), permettent de conclure immédiatement dans tous les cas sauf $n = 8$ et $n = 12$. Ces derniers doivent faire l'objet d'une étude technique détaillée, basée sur l'utilisation fine des théorèmes de Sylow, qui pourra être menée en travaux dirigés. □

Chapitre 5

Groupe symétrique, groupe alterné

5.1 Décomposition en cycles disjoints

Fixons un entier $n \geq 1$. On note S_n le groupe symétrique des permutations sur un ensemble fini à n éléments, c'est-à-dire à isomorphisme près le groupe des permutations de $\mathbb{N}_n := \{1, 2, \ldots, n\}$. S_n est un groupe fini, d'ordre $n!$, non abélien dès lors que $n \geq 3$.
On a vu que les transpositions engendrent le groupe S_n, mais d'une part la décomposition d'une permutation en produit de transpositions n'est pas unique, et d'autre part les transpositions ne commutent pas entre elles dans une telle décomposition.
On va donner dans ce qui suit une décomposition canonique de toute permutation en éléments de type particulier (appelés cycles), qui est unique, avec commutation des facteurs.

5.1.1 Support et orbites

Définition. Pour tout $\sigma \in S_n$, on appelle *support* de σ l'ensemble des éléments de $\mathbb{N}_n$ qui ne sont pas fixés par σ :

$$\operatorname{Supp}\sigma = \{i \in \mathbb{N}_n \,;\, \sigma(i) \neq i\}.$$

En particulier, $\operatorname{Supp}\sigma = \emptyset$ si et seulement si $\sigma = e$.

Lemme. *Pour toute $\sigma \in S_n$ non triviale, la restriction de σ à $\operatorname{Supp}\sigma$ est une permutation de $\operatorname{Supp}\sigma$.*

> *Preuve.* Soit $i \in \operatorname{Supp}\sigma$; notons $j = \sigma(i)$. Si on avait $j \notin \operatorname{Supp}\sigma$, on aurait $\sigma(j) = j$, donc $\sigma(j) = \sigma(i)$, donc $i = j$, c'est-à-dire $i = \sigma(i)$, ce qui contredirait $i \in \operatorname{Supp}\sigma$. C'est donc que $\operatorname{Supp}\sigma$ est stable par σ. La restriction σ' de σ à $\operatorname{Supp}\sigma$ est une application de $\operatorname{Supp}\sigma$ dans lui-même, injective car σ l'est, et donc bijective. □

Proposition. *Deux permutations de S_n dont les supports sont disjoints commutent.*

> *Preuve.* On peut supposer $n \geq 2$. Soient $\sigma, \eta \in S_n$ tels que $\operatorname{Supp}\sigma \cap \operatorname{Supp}\eta = \emptyset$. Soit $i \in \mathbb{N}_n$ quelconque. Si $i \notin \operatorname{Supp}\sigma \cup \operatorname{Supp}\eta$; alors $\sigma(i) = i = \eta(i)$; donc $\sigma\eta(i) = \eta\sigma(i)$. Supposons maintenant $i \in \operatorname{Supp}\sigma$. D'une part, $i \notin \operatorname{Supp}\eta$, donc $\eta(i) = i$, donc $\sigma\eta(i) = \sigma(i)$. D'autre part, $i \in \operatorname{Supp}\sigma$ implique $\sigma(i) \in \operatorname{Supp}\sigma$ d'après le lemme précédent, donc $\sigma(i) \notin \operatorname{Supp}\eta$, donc $\eta\sigma(i) = \sigma(i)$. On conclut que $\sigma\eta(i) = \eta\sigma(i)$. Le dernier cas est celui où $i \in \operatorname{Supp}\eta$, que l'on traite de façon analogue en échangeant les rôles de σ et η. □

DÉFINITION. Pour toute $\sigma \in S_n$, le sous-groupe cyclique $\langle\sigma\rangle$ de S_n opère sur $\mathbb{N}_n$ par :

$$\begin{array}{ccc} \langle\sigma\rangle \times \mathbb{N}_n & \longrightarrow & \mathbb{N}_n \\ (\sigma^k, i) & \longmapsto & \sigma^k(i) \end{array}.$$

On appelle *σ-orbite* toute orbite d'un élément de $\mathbb{N}_n$ pour cette action. On note :

$$\Omega_\sigma(i) = \{\sigma^k(i)\,;\, k \in \mathbb{Z}\}, \quad \text{pour tout } 1 \leq i \leq n.$$

Remarque. Soit p l'ordre de l'élément σ dans S_n, c'est-à-dire l'ordre du sous-groupe $\langle\sigma\rangle$. Comme on l'a vu en 3.2.1, Le cardinal d'une orbite divise l'ordre du groupe ; donc ici $|\Omega_\sigma(i)|$ divise p, et en particulier $1 \leq |\Omega_\sigma(i)| \leq p$. En outre :

$$\begin{cases} i \notin \operatorname{Supp}\sigma & \Leftrightarrow \quad \Omega_\sigma(i) = \{i\} \ \text{ (orbite ponctuelle)}, \\ i \in \operatorname{Supp}\sigma & \Leftrightarrow \quad 2 \leq |\Omega_\sigma(i)| \leq p. \end{cases}$$

5.1.2 Cycles

DÉFINITION. Une permutation $\sigma \in S_n$ est appelée un *cycle* lorsqu'il existe une σ-orbite et une seule qui n'est pas ponctuelle.

Exemple : soit $\sigma = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 5&2&3&6&4&1 \end{smallmatrix}\right) \in S_6$; $\Omega_2 = \{2\}$, $\Omega_3 = \{3\}$, $\Omega_1 = \{1,5,4,6\} = \Omega_5 = \Omega_4 = \Omega_6$.

PROPOSITION ET DÉFINITION. *Soit $\sigma \in S_n$ un cycle. On note r l'ordre de σ dans S_n.*

(i) *L'unique σ-orbite non ponctuelle est égale au support de σ.*

(ii) *Le cardinal du support de σ est égal à r.*

(iii) *Il existe $j_1, j_2, \ldots, j_r$ distincts dans $\mathbb{N}_n$ tels que :*

$$\sigma(j_1) = j_2,\ \sigma(j_2) = j_3,\ \ldots,\ \sigma(j_r) = j_1 \quad \text{et} \quad \sigma(i) = i \ \text{ si } \ i \notin \{j_1, \ldots, j_r\}.$$

On dit que σ est un r-cycle, ou un cycle de longueur r, et l'on note : $\sigma = [j_1, j_2, \ldots, j_r]$.
On a alors aussi : $\sigma = [j_k, j_{k+1}, \ldots, j_r, j_1, \ldots, j_{k-1}]$ pour tout $1 < k \leq r$.

Preuve. Notons Ω l'unique σ-orbite non ponctuelle. Soit j_1 un représentant quelconque de Ω. Donc : $\Omega = \Omega_\sigma(j_1) = \{i \in \mathbb{N}_n\,;\, \Omega_\sigma(i) \neq \{i\}\}$ c'est-à-dire $\Omega = \operatorname{Supp}\sigma$. Soit $p = |\Omega| = |\operatorname{Supp}\sigma|$. Donc :

$$\Omega = \operatorname{Supp}\sigma = \{j_1, \sigma(j_1), \sigma^2(j_1), \ldots, \sigma^{p-1}(j_1)\},$$

les éléments étant deux à deux distincts. On a alors $\sigma^p(j_1) = j_1$, et ceci étant vrai pour tout représentant j_1 choisi dans $\Omega = \operatorname{Supp}\sigma$, on a $\sigma^p(i) = i$ pour tout $i \in \operatorname{Supp}\sigma$. Mais l'égalité $\sigma^p(i) = i$ est claire si $i \notin \operatorname{Supp}\sigma$ puisqu'alors $\sigma(i) = i$. Ainsi $\sigma^p = e$ dans S_n. L'ordre r de σ dans S_n est donc un diviseur de p. Par ailleurs, dans l'action de $G = \langle\sigma\rangle$ sur $\mathbb{N}_n$, le cardinal de l'orbite $\Omega = \Omega_\sigma(j_1)$ divise l'ordre de G ; donc p divise $|G| = r$. On conclut que $p = r$. □

REMARQUES.

1. Le seul 1-cycle est e. Les 2-cycles sont les transpositions $[i, j]$.
2. Le n-cycle $[1, 2, \ldots, n] = \left(\begin{smallmatrix} 1&2&3&\ldots&n-1&n \\ 2&3&4&\ldots&n&1 \end{smallmatrix}\right)$ s'appelle la *permutation circulaire* de S_n. Il existe des n-cycles qui ne sont pas la permutation circulaire, par exemple $[1, 3, 4, 2] \in S_4$.
3. L'inverse d'un r-cycle est un r-cycle : $[j_1, j_2, \ldots, j_r]^{-1} = [j_r, j_{r-1}, \ldots, j_1]$.
4. Attention : si $\gamma \in S_n$ est un r-cycle, et si $2 \leq k \leq r-2$, alors γ^k n'est pas nécessairement un cycle. Par exemple, si γ est la permutation circulaire $[1, 2, 3, 4] \in S_4$, alors $\gamma^2 = [1, 3][2, 4]$ n'est pas un cycle.

Le lemme suivant, bien qu'évident, est d'une utilisation fréquente et précieuse.

LEMME (conjugué d'un cycle). *Pour tout r-cycle $\gamma = [j_1, j_2, \ldots, j_r]$ de S_n et tout $\sigma \in S_n$, le conjugué $\sigma\gamma\sigma^{-1}$ est égal au r-cycle $[\sigma(j_1), \sigma(j_2), \ldots, \sigma(j_r)]$.*

Preuve. Soit $i \in \mathbb{N}_n$. Si $\sigma^{-1}(i) \in \operatorname{Supp}\gamma$, il existe $1 \leq k \leq r$ tel que $i = \sigma(j_k)$. On a $\sigma\gamma\sigma^{-1}(i) = \sigma\gamma(j_k) = \sigma(j_{k+1})$ si $1 \leq k < r$, et $\sigma\gamma\sigma^{-1}(i) = \sigma\gamma(j_r) = \sigma(j_1)$ si $k = r$. Si maintenant $\sigma^{-1}(i) \notin \operatorname{Supp}\gamma$, alors $\gamma\sigma^{-1}(i) = \sigma^{-1}(i)$ et donc $\sigma\gamma\sigma^{-1}(i) = i$. Ceci prouve par définition même que $\sigma\gamma\sigma^{-1}$ est le r-cycle $[\sigma(j_1), \sigma(j_2), \ldots, \sigma(j_r)]$. □

Exercice. Montrer que l'action par conjugaison de S_n sur l'ensemble des r-cycles est transitive.

THÉORÈME (décomposition en produit de cycles disjoints). *Soit $\sigma \in S_n$ non triviale. Alors :*

(i) *σ se décompose en un produit de cycles non triviaux à supports disjoints,*

(ii) *les cycles dans une telle décomposition commutent deux à deux,*

(iii) *cette décomposition est unique à l'ordre près des facteurs,*

(iv) *l'ordre de σ est égal au* P.P.C.M. *des longueurs des cycles disjoints de cette décomposition.*

Preuve. Soit $\sigma \in S_n$ non triviale. Il existe donc au moins une σ-orbite non ponctuelle. Désignons par $\Omega_1, \ldots, \Omega_q$ les σ-orbites non ponctuelles deux à deux distinctes (et donc deux à deux disjointes). Pour tout $1 \leq k \leq q$, définissons $\gamma_k : \mathbb{N}_n \longrightarrow \mathbb{N}_n$ par : $\gamma_k(i) = \sigma(i)$ si $i \in \Omega_k$ et $\gamma_k(i) = i$ sinon. Alors γ_k est un cycle dans S_n, de support égal à Ω_k ; en effet si l'on note $r_k = |\Omega_k|$, on a $\Omega_k = \{j, \sigma(j), \sigma^2(j), \ldots, \sigma^{r_k-1}(j)\}$ quel que soit $j \in \Omega_k$. Il en résulte que les supports des γ_i sont deux à deux disjoints, donc (d'après la proposition de 5.1.1), que les γ_i commutent deux à deux dans S_n. Posons $\sigma' = \gamma_1\gamma_2 \ldots \gamma_q$; on montre que $\sigma' = \sigma$.

En effet, soit $j \in \mathbb{N}_n$; distinguons deux cas. Si $j \in \Omega_1 \cup \ldots \cup \Omega_q$, alors j appartient à une seule de ces orbites : il existe $1 \leq k \leq q$ tel que $j \in \Omega_k$ et $j \notin \Omega_i$ si $i \neq k$. Puisque les γ_i commutent deux à deux, on peut écrire $\sigma' = \gamma_k\gamma_1 \ldots \gamma_{k-1}\gamma_{k+1} \ldots \gamma_q$. Pour tout indice $i \neq k$, on $\gamma_i(j) = j$ car $j \notin \Omega_i = \operatorname{Supp}\gamma_i$; donc $\gamma_1 \ldots \gamma_{k-1}\gamma_{k+1} \ldots \gamma_q(j) = j$, d'où $\sigma'(j) = \gamma_k(j)$. Or $\gamma_k(j) = \sigma(j)$ puisque $j \in \Omega_k$. On conclut finalement que $\sigma'(j) = \sigma(j)$. Si maintenant $j \notin \Omega_1 \cup \ldots \cup \Omega_q$, alors, pour tout $1 \leq k \leq q$, on a $j \notin \operatorname{Supp}\gamma_k$ donc $\gamma_k(j) = j$, de sorte que $\sigma'(j) = j$. Mais $j \notin \Omega_1 \cup \ldots \cup \Omega_q$ signifie que la σ-orbite de j est ponctuelle, c'est-à-dire que $\sigma(j) = j$. Dans ce cas aussi, on a vérifié que $\sigma'(j) = \sigma(j)$.

On a ainsi prouvé les points (i) et (ii). Pour (iii), supposons que $\sigma = \gamma'_1\gamma'_2 \ldots \gamma'_p$ est une autre décomposition en produit de cycles à supports deux à deux disjoints. Pour tout $1 \leq i \leq p$, notons $\Omega'_i = \operatorname{Supp}\gamma'_i$. Chaque Ω'_i est une σ-orbite non ponctuelle, plus précisément on a :

$$\text{pour tout } 1 \leq k \leq p \text{ et pour tout } j \in \Omega'_k, \text{ on a } \Omega'_k = \Omega_\sigma(j). \qquad (1)$$

En effet. Fixons $1 \leq k \leq p$ et $j \in \Omega'_k$. Il en résulte que $j \notin \Omega'_i$ si $1 \leq i \neq k \leq p$ (puisque les supports des γ'_i sont deux à deux disjoints). En d'autres termes, $\gamma'_i(j) = j$ pour tout $1 \leq i \neq k \leq p$. Donc en écrivant $\sigma = \gamma'_k\gamma'_1 \ldots \gamma'_{k-1}\gamma'_{k+1} \ldots \gamma'_p$, suivant la méthode déjà employée ci-dessus, on calcule $\sigma(j) = \gamma'_k(j)$. Comme $\gamma'_k(j)$ appartient à Ω'_k et n'appartient pas à Ω'_i pour $1 \leq i \neq k \leq p$, on réitère pour obtenir $\sigma^2(j) = (\gamma'_k)^2(j)$. Et finalement $\sigma^m(j) = (\gamma'_k)^m(j)$ pour tout entier $m \geq 1$. On conclut que : $\Omega'_k = \Omega_\sigma(j)$.

Réciproquement, on obtient ainsi toutes les σ-orbites non ponctuelles ; plus précisément :

$$\text{pour tout } j \in \mathbb{N}_n \text{ telle que } \Omega_\sigma(j) \neq \{j\}, \text{ il existe } 1 \leq k \leq p \text{ tel que } \Omega'_k = \Omega_\sigma(j). \qquad (2)$$

En effet. Par contraposée, si l'on suppose que quel que soit $1 \leq k \leq p$, on a $j \notin \Omega'_k$, alors $\gamma'_k(j) = j$ pour tout $1 \leq k \leq p$, de sorte que $\sigma(j) = j$, c'est-à-dire $\Omega_\sigma(j) = \{j\}$.

Il résulte de (1) et (2) que la décomposition $\sigma = \gamma'_1\gamma'_2 \ldots \gamma'_p$ est, à l'ordre près, celle que l'on a construite dans la preuve du point (i), c'est-à-dire que $p = q$ et $\{\gamma_1, \ldots, \gamma_p\} = \{\gamma'_1, \ldots, \gamma'_p\}$, de qui montre (iii). Le point (iv) est évident et laissé en exercice. □

Exemple. Dans S_{12}, la permutation $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 5 & 10 & 11 & 3 & 6 & 9 & 4 & 7 & 12 & 8 & 2 \end{smallmatrix}\right)$ se décompose sous la forme $\sigma = [2,5,3,10,12][4,11,8][7,9]$. Les orbites sont $\Omega_1 = \{1\}$, $\Omega_2 = \{2,5,3,10,12\}$, $\Omega_4 = \{4,11,8\}$, $\Omega_6 = \{6\}$, $\Omega_7 = \{7,9\}$. Le support est $\Omega_2 \cup \Omega_4 \cup \Omega_7$. L'ordre de σ est 30.

5.2 Simplicité de A_n pour $n \geq 5$

5.2.1 Générateurs du groupe alterné.

Rappels. On a défini la signature d'une permutation $\sigma \in S_n$ comme le signe $\varepsilon(\sigma) = (-1)^m$, où m désigne le nombre de transpositions d'une décomposition quelconque de σ en produit de transpositions. Rappelons que cette définition équivaut à une définition de ε par le nombre d'inversions :

$$\varepsilon(\sigma) = \prod_{1 \leq i < k \leq n} \frac{\sigma(k) - \sigma(i)}{k - i}.$$

L'ensemble des permutations de signature 1 (c'est-à-dire des permutations qui se décomposent en un nombre pair de transpositions) est un sous-groupe du groupe S_n appelé *groupe alterné*, noté A_n. Ce n'est autre que le noyau du morphisme signature $\varepsilon : S_n \to \{-1, 1\}$. En particulier :

$$A_n \lhd S_n \quad \text{et} \quad |A_n| = \tfrac{n!}{2}.$$

La décomposition en cycles permet de donner une autre définition équivalente de la signature.

Lemme.

(i) *Si γ est un r-cycle, alors $\varepsilon(\gamma) = (-1)^{r-1}$.*

(ii) *Plus généralement, pour toute $\sigma \in S_n$, on a $\varepsilon(\sigma) = (-1)^{n-t}$ où t désigne le nombre de σ-orbites distinctes dans S_n.*

Preuve. si $\gamma = [j_1, j_2, \ldots, j_r]$, alors $\gamma = [j_1, j_r][j_1, j_{r-1}] \cdots [j_1, j_2]$, ce qui montre (i). Le point (ii) en découle immédiatement en utilisant le théorème 5.1.2. □

Proposition. *Pour $n \geq 3$, le groupe alterné A_n est engendré par les 3-cycles de S_n.*

Preuve. On a vu ci-dessus que tout 3-cycle est de signature $(-1)^{3-1} = 1$, donc appartient à A_n. Réciproquement, tout élément de A_n est un produit d'un nombre pair de transpositions, donc A_n est engendré par les produits de deux transpositions. Or un produit de deux transpositions est nécessairement de l'un des deux types suivants (où i, j, k, l sont distincts deux à deux) : $[i,j][i,k] = [i,k,j]$, ou bien $[i,j][k,l] = [i,l,k][i,j,k]$. Donc tout élément de A_n est un produit de 3-cycles. □

Exercice. On peut montrer que A_n est engendré par des famillles plus restreintes, par exemple par l'ensemble des 3-cycles de la forme $[1,i,j]$, où $2 \leq i \neq j \leq n$, ou encore par l'ensemble des 3-cycles de la forme $[1,2,j]$, où $3 \leq j \leq n$.

5.2.2 Simplicité du groupe alterné

On a $A_1 = A_2 = \{e\}$. Le groupe A_3 est d'ordre 3, donc est cyclique d'ordre premier, donc simple. Le groupe A_4 n'est pas simple car il contient le sous-groupe normal V isomorphe au groupe de Klein. Le théorème suivant est fondamental pour la théorie des corps, en raison d'une de ses conséquences que l'on démontrera dans la dernière partie de ce chapitre.

THÉORÈME. *Le groupe alterné A_n est simple pour $n \geq 5$.*

Preuve. On divise la démonstration en plusieurs étapes.

(1) Remarque préliminaire : quel que soit un 3-cycle $[i,j,k] \in A_n$, il existe $\sigma \in A_n$ tel que $\sigma[1,2,3]\sigma^{-1} = [i,j,k]$. Par conséquent, deux 3-cycles quelconques sont toujours conjugués dans A_n.

En effet : donnons-nous dans $\mathbb{N}_n$ cinq éléments deux à deux distincts i,j,k,ℓ,m et considérons dans S_n les permutations :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ i & j & k & l & m & \dots & ? \end{pmatrix} \quad \text{et} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ i & j & k & m & l & \dots & ? \end{pmatrix} = [l,m]\sigma_1.$$

On a : $\sigma_1[1,2,3]\sigma_1^{-1} = [i,j,k] = \sigma_2[1,2,3]\sigma_2^{-1}$, et comme $\sigma_2 = [\ell,m]\sigma_1$, l'une des deux permutations σ_1 et σ_2 est dans A_n.

(2) Soit H un sous-groupe non trivial de A_n, normal dans A_n. Si H contient un 3-cycle, alors $H = A_n$.

En effet : si γ_0 est un 3-cycle de H, tout 3-cycle de A_n est d'après (1) de la forme $\sigma\gamma_0\sigma^{-1}$ pour un $\sigma \in A_n$. Comme H est normal dans A_n, on déduit que H contient tous les 3-cycles, d'où $H = A_n$ d'après la proposition de 5.2.1.

(3) Fixons un sous-groupe non trivial H de A_n, normal dans A_n, et montrons que H contient un 3-cycle.

Partons de $\mu \in H, \mu \neq e$. Il existe $i \in \mathbb{N}_n$ tel que $\mu(i) \neq i$. Notons $j = \mu(i)$. Comme $n \geq 5$, il est clair qu'on peut choisir $k \in \mathbb{N}_n$ distinct de i et de j tel que $\mu(k) \neq i$. Notons $\ell = \mu(k)$. En résumé i,j,k sont deux à deux distincts, et donc $\mu(i) = j, \mu(j), \mu(k) = \ell$ sont deux à deux distincts (mais rien n'empêche a priori que $\mu(j) = i$ ou $\mu(j) = k$).

On peut donc considérer le 3-cycle $\gamma = [i,j,k] \in A_n$. D'après le lemme de conjugaison de 5.1.2, on a : $\mu\gamma\mu^{-1} = [\mu(i),\mu(j),\mu(k)] = [j,\mu(j),\ell]$. Rappelons aussi que $\gamma^{-1} = [i,k,j]$.

Notons $\sigma = \gamma^{-1}\mu\gamma\mu^{-1} = [i,k,j][j,\mu(j),\ell]$. Cette écriture n'est pas la décomposition canonique de σ, car les deux 3-cycles qui interviennent ne sont pas disjoints.

On a $\sigma \in H$ (car d'une part $\gamma^{-1}\mu\gamma \in H$ puisque $\mu \in H$ et H normal dans A_n, et d'autre part $\mu^{-1} \in H$). On a aussi $\sigma \neq e$ (car sinon $[j,\mu(j),\ell] = \gamma = [i,j,k] = [j,k,i]$, d'où $i = \ell$, ce qui est contraire aux données).

Par définition de σ, σ permute au plus 5 éléments (en d'autres termes, $|\operatorname{Supp}\sigma| \leq 5$). La décomposition canonique de σ en produit de cycles disjoints ne peut donc être que de l'une des formes suivantes : un 5-cycle, un 4-cycle, un 3-cycle, une transposition, le produit d'un 3-cycle par une transposition disjointe, le produit de deux transpositions disjointes. Mais comme σ doit être paire, seuls les trois cas suivants sont à retenir :

• si σ est un 3-cycle, c'est fini, on a montré que H contient un 3-cycle.

• si σ est un 5-cycle, notons $\sigma = [x,y,z,s,t]$; introduisons $\nu = [x,y,z]$; on calcule en utilisant le lemme de conjugaison de 1.4 : $\nu^{-1}\sigma\nu\sigma^{-1} = [x,y,z]^{-1}[\sigma(x),\sigma(y),\sigma(z)] = [x,z,y][y,z,s] = [x,z,s]$. Comme H normal dans A_n, $\nu \in A_n$ et $\sigma \in H$, on a $\nu^{-1}\sigma\nu \in H$ et finalement $\nu^{-1}\sigma\nu\sigma^{-1} \in H$. Donc H contient un 3-cycle.

• si σ est le produit de deux transpositions disjointes, notons $\sigma = [x,y][z,s]$; posons $\nu = [x,y,t]$ où t est un élément quelconque de $\mathbb{N}_n$ choisi distinct de x,y,z,s (ce qui est possible parce que $n \geq 5$). Alors $\nu^{-1}\sigma\nu\sigma^{-1} = [x,y,t]^{-1}[\sigma(x),\sigma(y),\sigma(t)] = [x,t,y][y,x,t] = [x,y,t]$. On conclut comme dans le cas précédent que H contient un 3-cycle.

Bilan : si H est un sous-groupe non trivial de A_n normal dans A_n, il contient un 3-cycle d'après (3), donc $H = A_n$ d'après (2). On conclut que A_n est un groupe simple. □

5.3 Une approche directe des questions de résolubilité

5.3.1 Sous-groupes normaux de S_n

Pour tout $n \in \mathbb{N}$, on connaît comme sous-groupe normal de S_n, distinct de $\{e\}$ et S_n, le groupe alterné A_n. De plus, dans le cas particulier où $n = 4$, le groupe A_4 contient le sous-groupe $V = \{e, a, b, c\}$ avec : $a = [1,2][3,4]$, $b = [1,3][2,4]$ et $c = [1,4][2,3]$. Il vérifie :

$$V \lhd S_4, \text{ et le groupe quotient } S_4/V \text{ n'est pas abélien.}$$

En effet. D'après le lemme de conjugaison de 5.1.2, on a pour tout $\sigma \in S_4$:

$$\sigma a \sigma^{-1} = \sigma[1,2][3,4]\sigma^{-1} = \sigma[1,2]\sigma^{-1}\sigma[3,4]\sigma^{-1} = [\sigma(1),\sigma(2)][\sigma(3),\sigma(4)] \in V.$$

On montre de même que $\sigma b \sigma^{-1} \in V$ et $\sigma c \sigma^{-1} \in V$ pour tout $\sigma \in S_4$, et l'on conclut que $V \lhd S_4$. De plus, si l'on prend par exemple $\tau = [1,2]$ et $\sigma = [1,3]$, on a $\tau\sigma\tau^{-1}\sigma^{-1} = [1,2,3] \notin V$, de sorte que $\overline{\tau}\,\overline{\sigma} \neq \overline{\sigma}\,\overline{\tau}$ dans S_4/V, ce qui prouve que S_4/V n'est pas abélien. Puisque S_4/V est d'ordre 6, on a donc $S_4/V \simeq S_3$. □

Le but du théorème suivant est de montrer qu'il s'agit des seuls sous-groupes normaux de S_n.

THÉORÈME. *Soit n un entier ≥ 2.*

(i) *Si $n \neq 4$, les seuls sous-groupes normaux de S_n sont $\{e\}$, A_n et S_n.*

(ii) *Si $n = 4$, les seuls sous-groupes normaux de S_4 sont $\{e\}$, V, A_4 et S_4.*

Preuve. Soit G un sous-groupe normal de S_n. On divise la démonstration en plusieurs étapes.

(1) Si G contient une transposition, alors $G = S_n$.

En effet. Soit $[i,j]$ une transposition appartenant à G. Soit $[k,\ell]$ une transposition quelconque. On peut toujours trouver $\varphi \in S_n$ telle que $\varphi(i) = k$ et $\varphi(j) = \ell$. Avec le lemme de conjugaison de 5.1.2, on calcule $\varphi[i,j]\varphi^{-1} = [\varphi(i),\varphi(j)] = [k,\ell]$. Comme $[i,j] \in G$ et $G \lhd S_n$, en on déduit que $[k,\ell] \in G$. Ceci prouve que G contient toutes les transpositions, donc que $G = S_n$.

(2) Si G contient un 3-cycle, alors $G = S_n$ ou $G = A_n$.

En effet. Soit $[i,j,k]$ un 3-cycle appartenant à G. Soit $\gamma = [i',j',k']$ un 3-cycle quelconque. On peut toujours trouver $\varphi \in S_n$ telle que $\varphi(i) = i'$, $\varphi(j) = j'$ et $\varphi(k) = k'$. Avec le lemme de conjugaison de 5.1.2, on calcule $\varphi[i,j,k]\varphi^{-1} = [\varphi(i),\varphi(j),\varphi(k)] = \gamma$. Comme $[i,j,k] \in G$ et $G \lhd S_n$, on en déduit que $\gamma \in G$. Ceci prouve que G contient tous les 3-cycles, donc que $A_n \subseteq G \subseteq S_n$. Ainsi $|S_n|/|G| \leq |S_n|/|A_n| = 2$, d'où $G = S_n$ ou $G = A_n$.

(3) Si G contient un cycle, alors $G = S_n$ ou $G = A_n$.

En effet. Soit $\gamma = [j_1, j_2, \ldots, j_r]$ un r-cycle appartenant à G. Si $r = 2$, alors $G = S_n$ d'après (1). Si $r = 3$, alors $G = S_n$ ou $G = A_n$ d'après (2). On suppose donc maintenant que $r \geq 4$. Considérons le 3-cycle $\omega = [j_1, j_2, j_3]$ et formons le commutateur $\beta := \omega\gamma\omega^{-1}\gamma^{-1}$. Parce que $\gamma \in G$ et $G \lhd S_n$, on a $\alpha := \omega\gamma\omega^{-1} \in G$, et donc $\beta = \alpha\gamma^{-1} \in G$ comme produit de deux éléments de G. Par ailleurs, on calcule avec le lemme de conjugaison de 5.1.2 : $\gamma\omega^{-1}\gamma^{-1} = \gamma[j_3,j_2,j_1]\gamma^{-1} = [\gamma(j_3),\gamma(j_2),\gamma(j_1)] = [j_4,j_3,j_2]$, d'où l'on tire que $\beta = [j_1,j_2,j_3][j_4,j_3,j_2] = [j_1,j_2,j_4]$, qui est donc un 3-cycle. Ainsi G contient un 3-cycle, et on applique (2) pour conclure.

(4) Si G contient le produit de deux transpositions à supports disjoints, alors $G = S_n$ ou $G = A_n$ lorsque $n \geq 5$, et $G = S_4$, $G = A_4$ ou $G = V$ lorsque $n = 4$.

En effet. Soit $\sigma = [i,j][k,\ell]$ un produit de transpositions appartenant à G tel que i,j,k,ℓ sont deux à deux distincts. Supposons $n \geq 5$. On peut alors considérer un entier $m \in \mathbb{N}_n$ distincts de i,j,k,ℓ. Notons $\nu = [i,j,m]$. En utilisant le lemme de conjugaison de 5.1.2, on calcule :

$$\nu^{-1}\sigma\nu\sigma^{-1} = [i,j,m]^{-1}[\sigma(i),\sigma(j),\sigma(m)] = [m,j,i][j,i,m] = [i,j,m] = \nu.$$

Or $\lambda := \nu^{-1}\sigma\nu \in G$ car $\sigma \in G$ et $G \lhd S_n$, d'où $\nu = \lambda\sigma^{-1} \in G$. On applique alors (2) pour conclure que $G = S_n$ ou A_n.

Supposons maintenant que $n = 4$. Quels que soient $x, y, z, t \in \mathbb{N}_4$ deux à deux distincts, il existe $\varphi \in S_4$ tel que $\varphi(i) = x$, $\varphi(j) = y$, $\varphi(k) = z$ et $\varphi(\ell) = t$. On calcule :

$$\varphi\sigma\varphi{-}1 = \varphi[i,j]\varphi^{-1}\varphi[k,\ell]\varphi^{-1} = [\varphi(i),\varphi(j)][\varphi(k),\varphi(\ell)] = [x,y][z,t].$$

Or $\varphi\sigma\varphi^{-1} \in G$ puisque $\sigma \in G$ et $G \lhd S_4$. On a ainsi prouvé que G contient tous les produits de deux transpositions à supports disjoints ; mais dans S_4 il n'y en a que trois, que l'on a noté a, b, c, et qui avec e forment le sous-groupe V. Donc $V \subseteq G$. Si $G \not\subset V$, alors G contient nécessairement un cycle (car tous les éléments de S_4 sont des cycles à part a, b, c), et l'on applique (3) pour conclure que $G = S_4$ ou A_4. Si $G \subseteq V$, alors $G = V$.

On achève alors la preuve de la façon suivante. Supposons $G \neq \{e\}$. Soit $\varphi \in G$ tel que $\varphi \neq e$. Si φ est un cycle, c'est fini d'après l'étape (3). Sinon, la décomposition canonique de φ en produit de cycles disjoints contient au moins deux cycles disjoints σ_1 et σ_2. Fixons $i \in \operatorname{Supp}\sigma_1$ et $j \in \operatorname{Supp}\sigma_2$. Ils vérifient $i \neq j$ puisque σ_1 et σ_2 sont disjoints. On a $\varphi(i) = \sigma_1(i)$, et donc $\varphi(i) \neq i$ (car $\sigma_1(i) \neq i$). On a aussi $\varphi(i) \neq j$ (car on aurait sinon $\sigma_1(i) = \varphi(i) = j = \sigma_1(j)$, ce qui contredirait $i \neq j$). Ainsi les trois éléments $i, j, \varphi(i)$ sont deux à deux distincts, ce qui permet de considérer le 3-cycle $\gamma = [i, \varphi(i), j]$. Formons le commutateur $\theta = \gamma\varphi\gamma^{-1}\varphi^{-1}$. Il appartient à G comme produit de $\gamma\varphi\gamma^{-1} \in G$ (car $\varphi \in G$ et $G \lhd S_n$) par $\varphi^{-1} \in G$. En utilisant le lemme de conjugaison de 5.1.2, on peut préciser le calcul de θ :

$$\theta = [i,\varphi(i),j]\varphi[i,\varphi(i),j]^{-1}\varphi^{-1} = [i,\varphi(i),j]\varphi[j,\varphi(i),i]\varphi^{-1} = [i,\varphi(i),j][\varphi(j),\varphi^2(i),\varphi(i)].$$

Si $\varphi^2(i) \neq i$, alors les cinq éléments $i, \varphi(i), \varphi^2(i), j, \varphi(j)$ sont deux à deux distincts, et on calcule $\theta = [i,\varphi(i),j][\varphi(j),\varphi^2(i),\varphi(i)] = [i,\varphi(i),\varphi(j),\varphi^2(i),j]$ qui est un 5-cycle. Ainsi G contient un cycle ; on applique (3) pour conclure.

Si $\varphi^2(i) = i$, on calcule $\theta = [i,\varphi(i),j][\varphi(j),i,\varphi(i)] = [i,j][\varphi(i),\varphi(j)]$. Ainsi G contient un produit de deux transpositions à supports disjoints ; on applique (4) pour conclure. □

5.3.2 Suites normales de S_n

Grâce au théorème 5.3.1, on peut expliciter toutes les suites normales de S_n, c'est-à-dire par définition les suites strictement décroissantes de sous-groupes normaux de S_n commençant à S_n et finissant à $\{e\}$.

	suites normales	*groupes quotients*
$n = 1$	$S_1 = \{e\}$	
$n = 2$	$S_2 \supset \{e\} = A_2$	$S_2/\{e\} \simeq C_2$ abélien
$n = 3$	$S_3 \supset \{e\}$	$S_3/\{e\} \simeq S_3$ non abélien
	$S_3 \supset A_3 \supset \{e\}$	$S_3/A_3 \simeq C_2$ abélien, et $A_3/\{e\} \simeq C_3$ abélien
$n = 4$	$S_4 \supset \{e\}$	$S_4/\{e\} \simeq S_4$ non abélien
	$S_4 \supset A_4 \supset \{e\}$	$S_4/A_4 \simeq C_2$ abélien, et $A_4/\{e\} \simeq A_4$ non abélien
	$S_4 \supset V \supset \{e\}$	$S_4/V \simeq S_3$ non abélien, et $V/\{e\} \simeq V$ abélien
	$S_4 \supset A_4 \supset V \supset \{e\}$	$S_4/A_4 \simeq C_2$ abélien, et $A_4/V \simeq C_3$ abélien, et $V/\{e\} \simeq V$ abélien
$n \geq 5$	$S_n \supset \{e\}$	$S_n/\{e\} \simeq S_n$ non abélien
	$S_n \supset A_n \supset \{e\}$	$S_n/A_n \simeq C_2$ abélien, et $A_n/\{e\} \simeq A_n$ non abélien

En résumé :

(i) si $n \leq 4$, il existe une suite normale de S_n telles que tous les quotients de deux termes successifs soient abéliens,

(ii) si $n \geq 5$, il n'existe pas de telles suites.

On traduit cette propriété en disant que S_n est résoluble si $n \leq 4$, et non résoluble si $n \geq 5$. Cette propriété importante, liée à la résolubilité des équations par radicaux (voir cours ultérieur de théorie des corps) sera étudiée en détail au chapitre suivant.

Exercice. Le centre et le sous-groupe dérivé sont toujours de sous-groupes normaux d'un groupe (voir 2.2.4). Au vu des théorèmes 5.2.2 et 5.3.1, c'est donc une question naturelle de savoir à quoi ils sont égaux dans le cas des groupes symétriques et alternés. On pourra montrer en exercice que :

(i) Pour tout $n \geq 3$, le centre de S_n est $\{e\}$ et le groupe dérivé de S_n est A_n.

(ii) Pour tout $n \geq 5$, le centre de A_n est $\{e\}$ et le groupe dérivé de A_n est A_n.

(iii) Pour $n = 4$, le centre de A_4 est $\{e\}$ et le groupe dérivé de A_4 est V.

Exercice. Un autre résultat classique sur le groupe symétrique, que l'on cite ici pour mémoire et qui poura faire l'objet d'une étude personnelle ou de travaux dirigés, concerne le groupe de ses automorphismes (voir 2.2.4).

(i) Pour tout $n \neq 6$, tout automorphisme de S_n est intérieur.

(ii) Pour tout $n = 6$, le sous-groupe $\operatorname{Inn} S_6$ est d'indice 2 dans $\operatorname{Aut} S_6$.

Chapitre 6

Groupes résolubles

6.1 Suites normales et groupes résolubles

6.1.1 Groupes dérivés successifs

Rappel. Soient G un groupe et $D(G)$ son groupe dérivé. On a : $D(G) \lhd G$ et $G/D(G)$ abélien, et pour tout $N \lhd G$: $(G/N \text{ abélien } \Leftrightarrow D(G) \subseteq N)$.

NOTATION. Soit G un groupe ; on pose : $D_0(G) = G$, $D_1(G) = D(G)$ le groupe dérivé de G, $D_2(G) = D(D_1(G)$ le groupe dérivé de $D_1(G)$, et par récurrence :

$$D_{i+1}(G) = D(D_i(G)) \text{ le groupe dérivé de } D_i(G), \text{ pour tout } i \in \mathbb{N}.$$

D'après le rappel ci-dessus :

$$D_{i+1}(G) \lhd D_i(G), \text{ et } D_i(G)/D_{i+1}(G) \text{ est abélien, pour tout } i \in \mathbb{N}.$$

On considère la *suite des groupes dérivés successifs* $(D_i(G))_{i\in\mathbb{N}}$, que l'on note aussi :

$$D_0(G) = G \rhd D_1(G) = D(G) \rhd D_2(G) \rhd D_3(G) \rhd \cdots \rhd D_i(G) \rhd D_{i+1}(G) \rhd \cdots.$$

THÉORÈME. *Pour tout $i \in \mathbb{N}$, on a : $D_i(G) \lhd G$.*

Preuve. Montrons d'abord que l'image de $D(G)$ par tout automorphisme de G est égal à $D(G)$. Soit $\alpha \in \operatorname{Aut} G$. Pour tous $x, y \in G$, on a $\alpha(xyx^{-1}y^{-1}) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1} \in D(G)$. Comme $D(G)$ est engendré par les commutateurs, on déduit que $\alpha(D(G)) \subseteq D(G)$. En considérant l'automorphisme α^{-1}, on obtient de même $\alpha^{-1}(D(G)) \subseteq D(G)$, donc $D(G) \subseteq \alpha(D(G))$, et finalement $\alpha(D(G)) = D(G)$.

Montrons maintenant que $\alpha(D_i(G)) = D_i(G)$ pour tout $\alpha \in \operatorname{Aut} G$ et tout $i \in \mathbb{N}$. La propriété est vraie pour $i = 1$ d'après la première étape. Par récurrence, supposons-la vraie jusqu'à un rang $i \geq 1$. Soit $\alpha \in \operatorname{Aut} G$. Par hypothèse de récurrence, $\alpha(D_i(G)) = D_i(G)$, donc la restriction de α à $D_i(G)$ détermine un automorphisme α' de $D_i(G)$. En appliquant la première étape au groupe $D_i(G)$ et à $\alpha' \in \operatorname{Aut} D_i(G)$, on a : $\alpha'(D(D_i(G)) = D(D_i(G))$. Mais $D_{i+1}(G) = D(D_i(G))$, de sorte que cette dernière égalité s'écrit encore $\alpha(D_{i+1}(G)) = D_{i+1}(G)$. Ce qui montre la propriété voulue au rang $i + 1$.

Dès lors, soient $x \in G$ quelconque et $i \in \mathbb{N}$. D'après la seconde étape ci-dessus, l'automorphisme intérieur $\alpha : g \mapsto xgx^{-1}$ vérifie $\alpha(D_i(G)) = D_i(G)$, donc $xD_i(G)x^{-1} = D_i(G)$, ce qui prouve que $D_i(G) \lhd G$. □

6.1.2 Notion de groupe résoluble.

DÉFINITION. Un groupe G est dit *résoluble* s'il existe un rang $n \in \mathbb{N}$ à partir duquel on a $D_n(G) = \{e\}$.

Cela signifie donc que la suite des groupes dérivés successifs est stationnaire :

$$G = D_0(G) \rhd D_1(G) \rhd D_2(G) \rhd D_3(G) \rhd \cdots \rhd D_n(G) = \{e\}.$$

PROPOSITION (facile mais importante). *Si G est un groupe résoluble, tout sous-groupe de G et tout quotient de G est résoluble.*

Preuve. Soit G un groupe résoluble. Soit $n \in \mathbb{N}$ tel que $D_n(G) = \{e\}$. Considérons un sous-groupe H de G ; il est clair que $D(H)$ est un sous-groupe de $D(G)$ et donc, par une récurrence évidente, que $D_i(H)$ est un sous-groupe de $D_i(G)$ pour tout $i \in \mathbb{N}$. En particulier on a $D_n(H)$ sous-groupe de $D_n(G) = \{e\}$, donc $D_n(H) = \{e\}$, ce qui prouve que H est résoluble.

Considérons $N \lhd G$ et le groupe quotient G/N. Notons π la surjection canonique $G \to G/N$. Pour tout sous-groupe H de G, un commutateur quelconque du groupe $\pi(H)$ est de la forme :

$$\pi(x)\pi(y)\pi(x)^{-1}\pi(y)^{-1} = \pi(xyx^{-1}y^{-1}), \text{ avec } x, y \in H,$$

d'où il résulte que $D(\pi(H)) = \pi(D(H))$. On en déduit que $D(\pi(G)) = D(G/N) = \pi(D(G))$, puis $D_2(G/N) = D(\pi(D(G))) = \pi(D_2(G))$, et par une récurrence évidente, $D_i(G/N) = \pi(D_i(G))$ pour tout $i \in \mathbb{N}$. En particulier pour $i = n$, on a $D_n(G/N) = \pi(D_n(G)) = \pi(\{e\}) = \{\pi(e)\}$, ce qui prouve que G/N est résoluble. □

6.1.3 Caractérisation de la résolubilité par les suites de compositions et les suites normales.

DÉFINITIONS. Soit G un groupe.

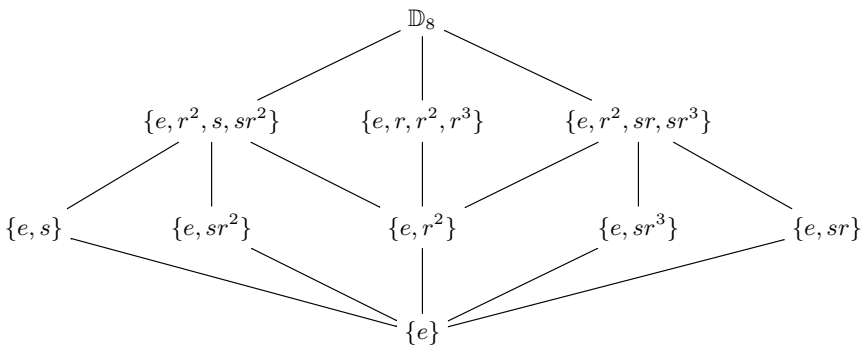
1. On appelle *suite de composition* de G toute chaîne finie de sous-groupes
$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_n = \{e\},$$
où $G_i \rhd G_{i+1}$ signifie que G_{i+1} est un sous-groupe de G_i normal dans G_i. Les groupes G_i/G_{i+1} sont appelés les *quotients* de la suite, et le nombre n de quotients est appelé la *longueur* de la suite.
2. On dit que la suite est strictement décroissante lorsque $G_i \neq G_{i+1}$ pour tout $0 \leq i \leq n-1$.
3. On dit que cette suite est une *suite normale* lorsque $G_i \lhd G$ pour tout $0 \leq i \leq n-1$.

Attention ! Certains auteurs appellent suite normale ce que nous appelons suite de composition, suite de composition ce que nous appelerons suite de Jordan-Hölder, ou encore suite de composition ce que nous appelons suite de composition strictement décroissante.

EXEMPLE 1. Considérons le groupe symétrique S_4, le sous-groupe alterné A_4, leur sous-groupe $V = \{e, a, b, c\}$ où $a = [1,2][3,4]$, $b = [1,3][2,4]$, $c = [1,4][2,3]$, et le sous-groupe $H = \{e, a\}$. D'après les résultats vus au chapitre 1 :

- $S_4 \rhd A_4 \rhd V \rhd \{e\}$ est une suite normale,
- $S_4 \rhd A_4 \rhd V \rhd H \rhd \{e\}$ est une suite de composition, mais pas une suite normale, car H n'est pas normal dans S_4.

EXEMPLE 2. Considérons le groupe diédral $\mathbb{D}_8 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$, avec $r^4 = s^2 = e$ et $rs = sr^3$. Les sous-groupes de $\mathbb{D}_8$ sont :



Tout chemin à 4 sommets de $\mathbb{D}_8$ à $\{e\}$ dans ce diagramme est une suite de composition.

- $\mathbb{D}_8 \rhd \{e, r^2, s, sr^2\} \rhd \{e, r^2\} \rhd \{e\}$ est une suite normale, (car de plus $\{e, r^2\} \lhd \mathbb{D}_8$),
- $\mathbb{D}_8 \rhd \{e, r^2, sr, sr^3\} \rhd \{e, sr^3\} \rhd \{e\}$ n'est pas une suite normale, (car $s(sr^3)s^{-1} = r^3 s = sr \notin \{e, sr^3\}$, de sorte que $\{e, sr^3\}$ n'est pas normal dans $\mathbb{D}_8$).

THÉORÈME. *Soit G un groupe. Les propriétés suivantes sont équivalentes :*

(i) *G est résoluble ;*

(ii) *G admet une suite normale dont tous les quotients sont abéliens ;*

(iii) *G admet une suite de composition dont tous les quotients sont abéliens.*

Preuve. Supposons G résoluble, et considérons la suite (finie) des groupes dérivés successifs :

$$G = D_0(G) \rhd D_1(G) \rhd D_2(G) \rhd D_3(G) \rhd \cdots \rhd D_n(G) = \{e\}.$$

Elle est normale d'après le théorème de 6.1.1 et tous ses quotients sont abéliens d'après la proposition de 6.1.1. Ceci prouve que (i) implique (ii). Il est trivial que (ii) implique (iii). Supposons maintenant que G vérifie (iii). On considère donc une suite de composition :

$$G = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_i \rhd H_{i+1} \rhd \cdots \rhd H_m = \{e\},$$

telle que H_i/H_{i+1} abélien pour tout $0 \leq i \leq m-1$. Quitte à supprimer certains H_i, on peut sans restriction supposer que les H_i sont deux à deux distincts, c'est-à-dire que la suite de composition est strictement décroissante. Pour $i = 0$, l'abélianité de $H_0/H_1 = G/H_1$ implique que $D(G) \subset H_1$ (voir le rappel au début de ce chapitre). De plus, $D(G) \subset H_1$ implique $D(D(G)) = D_2(G) \subset D(H_1)$, et comme l'abélianité de H_1/H_2 implique que $D(H_1) \subseteq H_2$, on déduit que $D_2(G) \subseteq H_2$. Une récurrence évidente permet ainsi de vérifier que $D_{i+1}(G) \subseteq H_{i+1}$ pour tout $0 \leq i \leq m-1$. En particulier $D_m(G) \subseteq H_m = \{e\}$, donc G est résoluble. □

6.1.4 Exemples de groupes résolubles

PROPOSITION 1. *Tout groupe abélien est résoluble.*

Preuve. Evident puisqu'alors $D(G) = \{e\}$. □

PROPOSITION 2. *Les seuls groupes simples résolubles sont les groupes cycliques d'ordre premier.*

Preuve. Si G est simple, sa seule suite de composition est $G \rhd \{e\}$. Si de plus G est résoluble, le théorème de 6.1.3 implique que l'unique quotient $G/\{e\}$ de cette suite est abélien, c'est-à-dire que G est abélien. D'où le résultat d'après la proposition 5 du 4.2.2. □

PROPOSITION 3. *Pour tout $n \geq 2$, le groupe diédral $\mathbb{D}_{2n}$ est résoluble.*

Preuve. Considérons dans $\mathbb{D}_{2n} = \{e, r, r^2, r^3, \ldots, r^{n-1}, s, sr, sr^2, sr^3, \ldots, sr^{n-1}\}$ le sous-groupe $C_n = \{e, r, r^2, r^3, \ldots, r^{n-1}\}$. On a la suite normale $\mathbb{D}_{2n} \rhd C_n \rhd \{e\}$ avec $\mathbb{D}_{2n}/C_n \simeq C_2$ abélien, et $C_n/\{e\} \simeq C_n$ abélien, donc $\mathbb{D}_{2n}$ est résoluble d'après le théorème 6.1.3. □

PROPOSITION 4. *Pour $n \geq 5$, le groupe symétrique S_n et le groupe alterné A_n ne sont pas résolubles.*

Preuve. Soit $n \geq 5$. Si S_n était résoluble, A_n le serait d'après la proposition 6.1.2. Or on a vu au théorème 5.2.2 que A_n est simple. D'après la proposition 2 ci-dessus, A_n serait cyclique d'ordre premier, ce qui est évidemment faux. □

Remarque. La non résolubilité des S_n pour $n \geq 5$ a des conséquences fondamentales en théorie des corps. On l'avait déjà montrée par une preuve directe en 5.3.2. Rappelons que S_2, S_3 et S_4 sont quant à eux résolubles.

THÉORÈME. *Pour tout nombre premier p, tout p-groupe est résoluble.*

Preuve. Soit G fini d'ordre p^n, avec $n \in \mathbb{N}^*$. Si G est abélien, il est résoluble. Supposons donc G non abélien. Notons $C_1 = Z(G)$ son centre. On sait qu'il est normal dans G, strictement inclus dans G (puisque G non abélien), et distinct de $\{e\}$ (d'après la proposition 3.2.4). On a donc une suite normale strictement décroissante : $G \rhd C_1 \rhd \{e\}$.

Le groupe quotient G/C_1 est un p-groupe (évident) ; son centre $Z(G/C_1)$ est normal dans G/C_1, donc de la forme C_2/C_1 pour un certain sous-groupe C_2 de G contenant C_1 (voir 2.2.6) qui vérifie $C_1 \lhd C_2$ (puisque plus généralement $C_1 \lhd G$), et tel que $C_2 \lhd G$ (car $C_2/C_1 \lhd G/C_1$). On a $C_1 \neq C_2$, car sinon $Z(G/C_1) = C_2/C_1$ serait trivial, ce qui est exclu puisque G/C_1 est un p-groupe.

- OU $G = C_2$. Alors $G/C_1 = Z(G/C_1)$, donc G/C_1 est abélien. On a donc construit une suite normale $G \rhd C_1 \rhd \{e\}$ dont tous les quotients sont abéliens. On conclut que G est résoluble.
- OU $G \neq C_2$. On a donc une suite normale strictement décroissante : $G \rhd C_2 \rhd C_1 \rhd \{e\}$. Le groupe G/C_2 est un p-groupe non trivial. Son centre $Z(G/C_2)$ est normal dans G/C_2, donc de la forme C_3/C_2 pour un certain sous-groupe C_3 de G contenant C_2 (d'après le troisième théorème d'isomorphisme, voir 2.2.6). Ce sous-groupe C_3 vérifie $C_2 \lhd C_3$ (puisque plus généralement $C_2 \lhd G$) et $C_3 \lhd G$ (car $C_3/C_2 \lhd G/C_2$). On a $C_2 \neq C_3$, car sinon $Z(G/C_2) = C_3/C_2$ serait trivial, ce qui est exclu puisque G/C_2 est un p-groupe.
  - OU $G = C_3$. Alors $G/C_2 = Z(G/C_2)$, donc G/C_2 est abélien. On a donc construit une suite normale $G \rhd C_2 \rhd C_1 \rhd \{e\}$ dont tous les quotients sont abéliens. On conclut que G est résoluble.
  - OU $G \neq C_3$. On réitère le raisonnement en considérant $Z(G/C_3) = C_4/C_3$.

On construit ainsi de proche en proche une suite croissante (C_i) de sous-groupes normaux de G telle que $C_1 = Z(G)$ et $C_{i+1}/C_i = Z(G/C_i)$ pour tout $i \geq 1$. Comme G est fini, le processus s'arrête, c'est-à-dire qu'il existe un plus petit entier k tel que $C_k = G$. On a alors obtenu la suite normale strictement décroissante : $G = C_k \rhd C_{k-1} \rhd \cdots \rhd C_2 \rhd C_1 \rhd \{e\}$, dont tous les quotients sont abéliens, et on conclut que G est résoluble. □

EXERCICE. *Tout groupe fini d'ordre pq ou p^2q, avec p, q premiers distincts, est résoluble.*

Indication pour la preuve : utiliser le fait, vu en 4.2.2 qu'il n'y a pour un tel groupe qu'un seul p-sous-groupe de Sylow ou qu'un seul q-sous-groupe de Sylow.

Ce résultat facile est un cas particulier d'un théorème beaucoup plus profond de W. Burnside, selon lequel tout groupe fini dont l'ordre n'admet que deux diviseurs premiers est résoluble.

6.1.5 Quelques compléments sur la notion de groupe résoluble

THÉORÈME. *Un groupe G est résoluble si et seulement s'il admet un sous-groupe normal propre N tel que N et G/N soient résolubles.*

Preuve. Supposons G résoluble. Le groupe dérivé $N = D(G)$ est normal dans G et distinct de G (car sinon $D_i(G) = G$ pour tout $i \in \mathbb{N}^*$, ce qui contredirait la résolubilité). D'après la proposition 6.1.2, N et G/N sont résolubles.

Supposons réciproquement qu'il existe un sous-groupe normal propre N de G tel que N et G/N soient résolubles. D'après le théorème 6.1.3, il existe deux suites de composition :

$$N = K_0 \rhd K_1 \rhd \cdots \rhd K_r = \{e\} \qquad \text{et} \qquad G/N = T_0 \rhd T_1 \rhd \cdots \rhd T_s = \{\overline{e}\},$$

avec K_i/K_{i+1} abélien pour tout $0 \leq i \leq r-1$, et T_i/T_{i+1} abélien pour tout $0 \leq i \leq s-1$.

Chaque T_i étant un sous-groupe de G/N, il est de la forme $T_i = G_i/N$ pour un certain sous-groupe G_i de G contenant N (voir 2.2.6). Comme $T_{i+1} \lhd T_i$, on a $G_{i+1} \lhd G_i$, et par application du troisième théorème d'isomorphisme : G_i/G_{i+1} est isomorphe à T_i/T_{i+1}, donc abélien. En outre, pour $i = s$, le fait que $T_s = \{\overline{e}\}$ implique $G_s = N$. On peut alors considérer la suite de composition :

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{s-1} \rhd G_s = N = K_0 \rhd K_1 \rhd \cdots \rhd K_r = \{e\},$$

dont tous les quotients sont abéliens. Donc G est résoluble. □

COROLLAIRE. *Soient G un groupe, H et K deux sous-groupes normaux et résolubles de G. Alors HK est un sous-groupe normal et résoluble de G.*

Preuve. Il est clair que HK est un sous-groupe normal de G. Par application du deuxième théorème d'isomorphisme (voir 2.2.5), on a : $H \cap K \lhd K$ et $H \lhd HK$, et l'isomorphisme $HK/H \simeq K/(H \cap K)$. Comme K est résoluble, $K/(H \cap K)$ est résoluble par application de la proposition 6.1.2, et donc HK/H est résoluble. Puisque H est un sous-groupe normal et résoluble dans HK, on déduit avec le théorème précédent que HK est résoluble. □

COROLLAIRE. *Le produit direct de deux groupes résolubles est résoluble.*

Preuve. Soient G_1 et G_2 deux groupes résolubles, et $G = G_1 \times G_2$ leur produit direct. Les sous-groupes $H = G_1 \times \{e_2\}$ et $K = \{e_1\} \times G_2$ vérifient : $H \simeq G_1,\ K \simeq G_2,\ H \lhd G,\ K \lhd G$, et $G = HK$. On applique le corollaire ci-dessus pour conclure que G est résoluble. □

6.2 Suites de Jordan-Hölder et groupes résolubles

6.2.1 Notion de suite de Jordan-Hölder

DÉFINITION. Soient G un groupe, et (Σ) une suite de composition de G strictement décroissante :

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}.$$

On dit que (Σ) admet un *raffinement propre* lorsqu'il existe $1 \leq i \leq n-1$ et un sous-groupe K tel que $G_{i+1} \lhd K \lhd G_i$ avec $G_{i+1} \neq K \neq G_i$.

Remarque. Comme $G_{i+1} \lhd G_i$, tout sous-groupe K tel que $G_{i+1} \subset K \subset G_i$ vérifie $G_{i+1} \lhd K$. En conséquence, dire que (Σ) n'admet pas de raffinement propre signifie que, quel que soit $1 \leq i \leq n-1$, on ne peut pas trouver de sous-groupe K tel que $G_{i+1} \subset K \lhd G_i$ avec $G_{i+1} \neq K \neq G_i$, c'est-à-dire que G_{i+1} est normal maximal dans G_i.

LEMME. *Soient G un groupe, et (Σ) une suite de composition de G strictement décroissante :*

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\}.$$

Les assertions suivantes sont équivalentes :

(i) (Σ) *est sans raffinement propre ;*

(ii) G_{i+1} *est normal maximal dans* G_i*, pour tout* $0 \leq i \leq n-1$ *;*

(iii) G_i/G_{i+1} *est un groupe simple, pour tout* $0 \leq i \leq n-1$.

Preuve. L'équivalence de (i) et (ii) résulte de la remarque précédente. Pour (iii), rappelons d'abord que tout sous-groupe normal H de G_i/G_{i+1} est de la forme $H = K/G_{i+1}$ avec K un sous-groupe normal de G_i contenant G_{i+1}. Dès lors :

$$\begin{aligned}(G_i/G_{i+1} \text{ simple}) \quad &\Leftrightarrow \quad G_i/G_{i+1} \neq \{\overline{e}\} \text{ et, si } H \lhd G_i/G_{i+1}, \text{ alors } H = \{\overline{e}\} \text{ ou } H = G_i/G_{i+1} \\ &\Leftrightarrow \quad G_i \neq G_{i+1} \text{ et, si } G_{i+1} \subseteq K \lhd G_i, \text{ alors } K = G_{i+1} \text{ ou } K = G_i,\end{aligned}$$

d'où l'équivalence de (ii) et (iii). □

DÉFINITION. Une suite de composition satisfaisant l'une des conditions équivalentes du lemme ci-dessus s'appelle une *suite de Jordan-Hölder* de G.

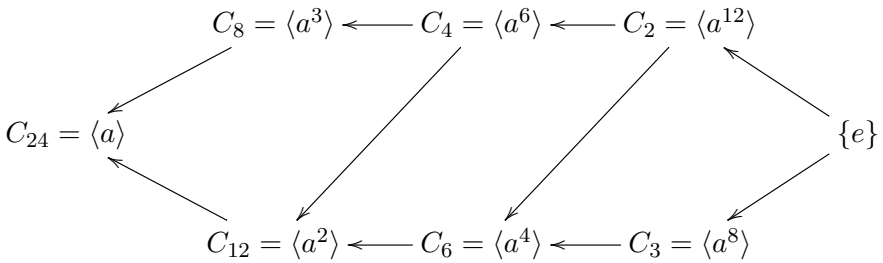
6.2.2 Exemples de suites de Jordan-Hölder.

EXEMPLE 1. La suite $S_5 \rhd A_5 \rhd \{e\}$ est de Jordan-Hölder car $S_5/A_5 \simeq C_2$ qui est simple, et $A_5/\{e\} \simeq A_5$ qui est simple.

EXEMPLE 2. La suite $S_4 \rhd A_4 \rhd \{e\}$ n'est pas de Jordan-Hölder car $A_4/\{e\} \simeq A_4$ n'est pas simple.

- Elle admet le raffinement propre $S_4 \rhd A_4 \rhd V \rhd \{e\}$, qui n'est pas de Jordan-Hölder car $V/\{e\} \simeq V$ n'est pas simple.
- Elle admet le raffinement propre $S_4 \rhd A_4 \rhd V \rhd H \rhd \{e\}$, qui est de Jordan-Hölder car tous les quotients $S_4/A_4 \simeq C_2$, $A_4/V \simeq C_3$, $V/H \simeq C_2$ et $H/\{e\} \simeq C_2$ sont simples. On ne peut pas raffiner davantage.

EXEMPLE 3. Considérons le groupe cyclique $C_{24} = \{e, a, a^2, \ldots, a^{23}\}$ d'ordre 24. Ses sous-groupes sont :



On obtient quatre suites de Jordan-Hölder :

$$\begin{aligned}&C_{24} \rhd C_{12} \rhd C_6 \rhd C_3 \rhd \{e\}, \qquad && C_{24} \rhd C_8 \rhd C_4 \rhd C_2 \rhd \{e\}, \\ &C_{24} \rhd C_{12} \rhd C_4 \rhd C_2 \rhd \{e\}, && C_{24} \rhd C_{12} \rhd C_6 \rhd C_2 \rhd \{e\}.\end{aligned}$$

EXEMPLE 4. Le groupe additif $\mathbb{Z}$ n'admet aucune suite de Jordan-Hölder.

En effet, considérons une suite de composition $G_0 = \mathbb{Z} \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd G_n = \{0\}$ strictement décroissante. Rappelons que tout sous-groupe de $\mathbb{Z}$ est de la forme $k\mathbb{Z}$ avec $k \in \mathbb{N}$. Il existe donc ici $k \in \mathbb{N}^*$ tels que $G_{n-1} = k\mathbb{Z} \rhd G_n = \{0\}$. Soit alors le sous-groupe $H = 2k\mathbb{Z}$ de $\mathbb{Z}$. C'est un sous-groupe de $G_{n-1} = k\mathbb{Z}$, distinct de $k\mathbb{Z}$ et de $\{0\}$, de sorte que la suite de composition $G_0 = \mathbb{Z} \rhd G_1 \rhd \cdots \rhd G_{n-1} \rhd H \rhd G_n = \{0\}$ est un raffinement propre de la suite (quelconque) donnée au départ. Cette dernière n'est donc pas une suite de Jordan-Hölder.

PROPOSITION 1. *Tout groupe fini non-trivial admet au moins une suite de Jordan-Hölder.*

Preuve. Si G est simple, alors $G = G_0 \rhd G_1 = \{e\}$ est une suite de Jordan-Hölder (et c'est la seule suite de composition strictement décroissante). On suppose donc maintenant que G n'est pas simple. L'ensemble $\mathscr{H}$ des sous-groupes normaux dans G distincts de G et $\{e\}$ est alors non-vide. Il est fini (puisque G est fini). Il admet donc (au moins) un élément maximal H_1. Ce sous-groupe H_1 étant normal maximal dans G, il résulte du lemme 6.2.1 que G/H_1 est simple. Si H_1 est simple, c'est fini car $G \rhd H_1 \rhd \{e\}$ est alors une suite de Jordan-Hölder. Sinon, l'ensemble $\mathscr{H}_1$ des sous-groupes normaux dans H_1 distincts de H_1 et $\{e\}$ est fini non-vide, donc admet (au moins) un élément maximal H_2, et il résulte du lemme 6.2.1 que H_1/H_2 est simple. Si H_2 est simple, c'est fini car $G \rhd H_1 \rhd H_2 \rhd \{e\}$ est alors une suite de Jordan-Hölder. Sinon, on réitère. Comme G n'a qu'un nombre fini de sous-groupes, le processus s'arrête : il existe un rang k à partir duquel on obtient nécessairement un sous-groupe H_k simple, et la suite strictement décroissante $G \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_k \rhd \{e\}$ est alors de Jordan-Hölder. □

PROPOSITION 2. *Un groupe abélien admet au moins une suite de Jordan-Hölder si et seulement s'il est fini non trivial.*

Preuve. Un sens est clair d'après la proposition précédente. Pour la réciproque, donnons-nous un groupe abélien G admettant une suite de Jordan-Hölder $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$. Pour tout $0 \leq i \leq n-1$, le groupe G_i/G_{i+1} est simple (par définition d'une suite de Jordan-Hölder) et abélien (car G l'est), et donc (d'après la proposition 5 du 4.2.2) cyclique d'ordre premier. Notons $p_{i+1} = |G_i/G_{i+1}| = [G_i : G_{i+1}]$.

D'après la formule des indices (voir 2.2.6), les égalités $[G : G_1] = p_1$ et $[G_1 : G_2] = p_2$ impliquent que G_2 est d'indice fini dans G, et $[G : G_2] = [G : G_1][G_1 : G_2] = p_1p_2$. De même, $[G : G_2] = p_1p_2$ et $[G_2 : G_3] = p_3$ impliquent $[G : G_3] = p_1p_2p_3$. En itérant, on obtient ainsi $[G : G_n] = p_1p_2 \cdots p_n$, ce qui, comme $G_n = \{e\}$, montre que G est fini d'ordre $p_1p_2 \cdots p_n$. □

6.2.3 Caractérisation de la résolubilité d'un groupe fini par les suites de Jordan-Hölder.

On a défini la notion de groupe résoluble par le caractère stationnaire de la suite des groupes dérivés. Nous avons donné au théorème 6.1.3 une définition équivalente en termes de suite de composition ou en terme de suites normales. Le théorème suivant donne une autre définition équivalente, dans le cas des groupes finis, en termes cette fois de suites de Jordan-Hölder.

THÉORÈME. *Soit G un groupe fini non trivial. Le groupe G est résoluble si et seulement s'il existe une suite de Jordan-Hölder de G dont tous les quotients sont (cycliques) d'ordre premier.*

Preuve. Supposons qu'il existe une suite de Jordan-Hölder de G dont tous les quotients sont d'ordre premier. Chaque quotient est alors cyclique, donc abélien, de sorte que la résolubilité de G découle directement du théorème 6.1.3. Réciproquement, supposons que G est résoluble. Comme G est supposé fini, il résulte de la proposition 1 de 6.2.2 qu'il existe une suite de

Jordan-Hölder $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$. Donc, pour tout $0 \leq i \leq n-1$, le quotient G_i/G_{i+1} est simple. Puisque G est résoluble, il en est de même de chaque sous-groupe G_i et de chaque quotient G_i/G_{i+1}, par application de la proposition 6.1.2. Ainsi, tous les quotients G_i/G_{i+1} sont simples et résolubles, donc cycliques d'ordre premier d'après la proposition 2 de 6.1.4 □

6.2.4 A propos du théorème de Jordan-Hölder.

DÉFINITION. Deux suites de composition $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{e\}$ et $G = K_0 \triangleright K_1 \triangleright \cdots \triangleright K_p = \{e\}$ d'un groupe G sont dites *équivalentes* lorsque $n = p$ et qu'il existe une permutation $\sigma \in S_n$ telle que $G_i/G_{i+1} \simeq K_{\sigma(i)}/K_{\sigma(i)+1}$ pour tout $0 \leq i \leq n-1$.

Exemple. Reprenons l'exemple 3 de 6.2.2. Les quatre suites de Jordan-Hölder de C_{24} sont équivalentes, car les quotients correspondants sont respectivement isomorphes à :

suites	quotients
$C_{24} \triangleright C_{12} \triangleright C_6 \triangleright C_3 \triangleright \{e\}$	$C_2,\ C_2,\ C_2,\ C_3$
$C_{24} \triangleright C_8 \triangleright C_4 \triangleright C_2 \triangleright \{e\}$	$C_3,\ C_2,\ C_2,\ C_2$
$C_{24} \triangleright C_{12} \triangleright C_4 \triangleright C_2 \triangleright \{e\}$	$C_2,\ C_3,\ C_2,\ C_2$
$C_{24} \triangleright C_{12} \triangleright C_6 \triangleright C_2 \triangleright \{e\}$	$C_2,\ C_2,\ C_3,\ C_2$

Cette propriété est un cas d'application du théorème général suivant (que nous citons pour mémoire, mais ne démontrerons pas ici).

THÉORÈME (dit de Jordan-Hölder). *Si G est un groupe admettant une suite de Jordan-Hölder (en particulier si G est un groupe fini), alors toutes les suites de Jordan-Hölder de G sont équivalentes.*

Preuve. Voir ouvrage de référence. □

En particulier, toutes les suites de Jordan-Hölder d'un groupe G admettant des suites de Jordan-Hölder sont de même longueur. On appelle cette longueur commune la longueur de G.
Par exemple, il résulte de l'exemple précédent que C_{24} est de longueur 4.
En reprenant la preuve du théorème de 6.1.4, on vérifie aisément que tout groupe d'ordre p^n (avec p premier et $n \geq 1$) est de longueur n.