dernière édition : 30 novembre 2019

Notes prises par Téofil Adamski

THÉORIE DES GROUPES

(THGR)

Frédéric Touzet

1A maths 2019, ENS de Rennes

Chapitre 1

Théorie des groupes

1.1 Notions de bases

Définition 1.1 *(groupe).* Un groupe est un couple $(G, *)$ où G est un ensemble non vide et $*$ une loi de composition interne sur G, *i. e.* une application de $G \times G$ dans G, vérifiant

- pour tous $x, y, z \in G$, on a $x * (y * z) = (x * y) * z$;
- il existe $e \in G$ tel que, pour tout $x \in E$, on ait $x * e = e * x = e$;
- pour tout $x \in G$, il existe $x' \in G$ tel que $x * x' = e$.

De plus, on dira que G est abélien (ou commutatif) si, pour tous $x, y \in G$, on a $x * y = y * x$.

◇ Remarques. – L'élément neutre e est unique.

– Si $x \in G$, alors l'élément x admet un unique symétrique. En effet, si x' et x'' sont deux symétriques de x, alors $x'' * x = e$, donc $(x'' * x) * x' = x'$, donc $x'' * (x * x') = x'$ par associativité, donc $x'' = x$. D'où l'unicité.

– On peut supprimer le parenthésage du fait de l'associativité.

Notations. Soit $(G, *)$ un groupe. Dans une notation multiplication, on notera simplement $xy \coloneqq x * y$, x^{-1} le symétrique de x et $1 \coloneqq e$. Si $n \geqslant 0$, on notera $x^n \coloneqq x * \cdots * x$ où le terme x apparaît n fois avec la convention $x^0 = 1$. Si $n \leqslant 0$, on notera $x^n \coloneqq (x^{-1})^{-n}$.

Quand G est abélien, on pourra adopter la notation additive où l'on note $x + y \coloneqq x * y$, $-x$ le symétrique de x et $0 \coloneqq e$. Si $n \geqslant 0$, on notera $nx \coloneqq x * \cdots * x$ où le terme x apparaît n fois.

Propriété 1.2. – Pour tous $x \in G$ et $n, m \in \mathbb{Z}$, on a $(x^n)^m = x^{nm}$. En particulier, on a $(x^{-1})^{-1} = x$.
– Pour tous $x, y \in G$, on a $(xy)^{-1} = y^{-1}x^{-1}$.

▷ Exemples. – Les couples $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{C}^*, \times)$ sont des groupes.

– Si E est un ensemble, on note $\mathfrak{S}_E$ le groupe symétrique de E, *i. e.* l'ensemble des bijections de E dans E. Alors $(\mathfrak{S}_E, \circ)$ est un groupe de neutre Id_E, mais il n'est pas abélien si $|E| \geqslant 3$. Dans le cas où $E = [\![1, n]\!]$, on note $\mathfrak{S}_n \coloneqq \mathfrak{S}_E$ et on a $|\mathfrak{S}_n| = n!$.

– Si K est un corps, alors $\mathrm{GL}_n(K)$ est un groupe pour le produit matriciel et il n'est pas abélien si $n \geqslant 2$.

– Le couple $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe pour tout $n \geqslant 1$.

– Si $(G_1, *_1)$ et $(G_2, *_2)$ sont des groupes, alors on peut former leur produit $(G_1 \times G_2, *)$ où la loi $*$ est définie par $(x, y) * (x', y') = (x *_1 x', y *_2, y')$ pour tout $x, y \in G_1$ et $x', y' \in G_2$.

Définition 1.3 *(table d'un groupe fini).* Soit $(G, *)$ un groupe fini. On le note $G = \{a_1, \ldots, a_n\}$. On peut dresser la table de l'opération $*$ qui est la table dont le coefficient en (i, j) en $a_i * a_j$.

▷ Exemple. La table du groupe $(\mathbb{Z}/3\mathbb{Z}, +)$ est

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Définition 1.4 *(sous-groupe).* Soit $(G,*)$ un groupe. Une partie non vide H de G est un sous-groupe de $(G,*)$ si, pour tous $x,y\in H$, on a $x*y\in H$ et $x^{-1}\in H$. Alors $(H,*)$ est un groupe et on note $H<G$.

◇ Remarques. 1. Le couple $(H,*)$ est un sous-groupe de G si et seulement si, pour tous $x,y\in H$, on a $xy^{-1}\in H$.
2. Si $(H_i)_{i\in I}$ est une famille de sous-groupes de G, alors $\bigcap_{i\in I}H_i<G$.
3. Si A est une partie finie et non vide de G, alors A est un sous-groupe de G si et seulement si, pour tous $x,y\in A$, on a $xy\in A$.

▷ Exemples. On a $\mathbb{Z}<\mathbb{Q}<\mathbb{R}<\mathbb{C}$ et $\mathrm{GL}_n(\mathbb{Q})<\mathrm{GL}_n(\mathbb{R})<\mathrm{GL}_n(\mathbb{C})$. Si $n\in\mathbb{N}$, alors $n\mathbb{Z}<\mathbb{Z}$. Pour $n\geqslant 1$, en notant $\mathrm{GL}_n(\mathbb{Z})=\{M\in\mathrm{GL}_n(\mathbb{Q})\mid M\in\mathscr{M}_n(\mathbb{Z}),\det M=\pm1\}$, on a $\mathrm{GL}_n(\mathbb{Z})<\mathrm{GL}_n(\mathbb{Q})$.

Exercice 1.1. Montrer que $Q_8\coloneqq\{\pm\mathrm{Id},\pm I,\pm J,\pm K\}$ est un groupe non abélien, appelé groupe des quaternions, où

$$\mathrm{Id}=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad I=\begin{pmatrix}i&0\\0&i\end{pmatrix},\quad J=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\quad\text{et}\quad K=\begin{pmatrix}0&i\\i&0\end{pmatrix}.$$

Définition 1.5 *(groupe engendré).* Soient G un groupe et $A\subset G$. On note

$$\langle A\rangle=\bigcap_{\substack{H<G\\H\supset A}}H.$$

C'est le plus petit sous-groupe de G contenant A.

▷ Exemple. On a $\langle G\rangle=G$ et $\langle\emptyset\rangle=\{e\}$. Si $x\in G$, alors $\langle x\rangle\coloneqq\langle\{x\}\rangle=\{x^n\mid n\in\mathbb{Z}\}$.

Définition 1.6. On dira que G est de type fini s'il existe $A\subset G$ finie telle que $\langle A\rangle=G$.

◇ Remarque. Si G est fini, alors G est de type fini. La réciproque est fausse en considérant $\mathbb{Z}=\langle1\rangle$.

Définition 1.7. L'ordre d'un groupe G est son cardinal noté $|G|$. L'ordre de $x\in G$ est l'ordre de $\langle x\rangle$ noté $\mathrm{o}(x)$.

Proposition 1.8. Soit $x\in G$. On a $\mathrm{o}(x)<+\infty$ si et seulement s'il existe $n\in\mathbb{N}^*$ tel que $x^n=1$. Dans ce cas, l'ordre $m=\mathrm{o}(x)$ divise n et $\langle x\rangle=\{1,x,\dots,x^{m-1}\}$.

Preuve On suppose qu'il existe $n\in\mathbb{N}^*$ tel que $x^n=1$. On pose alors $m=\min\{x\in\mathbb{N}^*\mid x^n=1\}$. On a $m'\leqslant n$. Une division euclidienne donne l'existence de $q,r\in\mathbb{N}$ tels que $n=qm+r$ et $r<m$. On a alors $x^n=x^r$, donc $x^r=1$, donc $r=0$ par minimalité de m', donc $m\mid n$. On note $A=\{1,x,\dots,x^{m-1}\}$. On a $A\subset\langle x\rangle$. De plus, on a $|A|=m$ sinon il existerai $a,b\in[\![0,m-1]\!]$ tels que $a<b$ et $x^a=x^b$, donc $x^{b-a}=1$ avec $b-a<m$ ce qui impossible. Montrons que A est stable par multiplication. Si $a,b\in[\![0,m-1]\!]$, alors $x^ax^b=x^r$ où r est le reste de la division euclidienne de $a+b$ par m. Montrons que A est stable par inverse. Si $a\in[\![0,m-1]\!]$, alors $(x^a)^{-1}=x^{m'-a}\in A$. Donc $A=\langle x\rangle$ et $\mathrm{o}(x)=m$. □

Théorème 1.9 *(Lagrange).* Soient G un groupe fini et H un sous-groupe de G. Alors $|H|\mid|G|$. En particulier, si $x\in G$, alors $\mathrm{o}(x)\mid|G|$.

Notation. On pose alors $[G:H]=|G|/|H|$, appelé indice de H dans H.

◇ Remarque. Si $|G|=4$, alors on est dans un des deux cas :
- soit il existe $x\in G$ tel que $\mathrm{o}(x)=4$ et $G=\langle x\rangle$,
- soit $x^2=1$ pour tout $x\in G$.

Définition 1.10 *(morphisme de groupes).* Une application $f\colon(G,\cdot)\to(H,*)$ entre deux groupes est un morphisme si, pour tous $x,y\in G$, on a $f(x\cdot y)=f(x)*f(y)$. On dira que f est un isomorphisme si f est bijective. On dira que f est un automorphisme de G si $f\colon G\to G$ est un isomorphisme et on note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G

◇ Remarque. On a $f(e_G)=e_H$ car $f(e_G)=f(e_G*e_G)=f(e_G)*f(e_G)$ et, en multipliant par $f(e_G)^{-1}$, on a $f(e_G)=e_H$. Par conséquent, si $x\in G$, alors $f(x)^{-1}=f(x^{-1})$.

PRINCIPE GÉNÉRAL. Si $\varphi\colon G \to H$ est un isomorphisme, alors tout ce qui vaut pour G vaut pour H.

▷ EXEMPLES. – L'application $f\colon (\{\pm 1\}, \times) \to (\mathbb{Z}/2\mathbb{Z}, +)$ telle que $f(1) = \overline{0}$ et $f(-1) = \overline{1}$ est un morphisme.
– Si $H < G$, alors $h \in H \longmapsto h \in H$ est un morphisme.
– Si $n \in \mathbb{Z}^*$, alors $n \in \mathbb{Z} \longmapsto \overline{n} \in \mathbb{Z}/n\mathbb{Z}$ est un morphisme surjectif.
– Si $G = \langle x \rangle$ et $|G| = n$, alors $\overline{a} \in \mathbb{Z}/n\mathbb{Z} \longmapsto x^a \in G$ est un morphisme.
– La fonction exp$\colon (\mathbb{R}, +) \longmapsto (\mathbb{R}^*, \times)$ est un morphisme.
– Si K est un corps commutatif, alors det$\colon \mathrm{GL}_n(K) \to K^*$ est un morphisme surjectif.
– Si G est abélien, alors $g \in G \longmapsto g^{-1} \in G$ est un morphisme.

PROPOSITION 1.11. Soit $f\colon G \to H$ un morphisme. Si $G' < G$, alors $f(G') < H$. Si $H' < H$, alors $f^{-1}(H') < G$. En particulier, on a $\operatorname{Ker} f < G$.

DÉFINITION 1.12. Deux groupes G et H sont dits isomorphes s'il existe un isomorphisme de G dans H. Dans ce cas, on note $G \simeq H$.

PROPOSITION 1.13. Un morphisme $f\colon G \to H$ est injectif si et seulement si $\operatorname{Ker} f = \{1_H\}$.

EXERCICE 1.2. Soient G un groupe et H et K deux sous-groupes de G. On pose

$$\varphi\colon \left| \begin{array}{l} H \times K \longrightarrow G, \\ (h,k) \longmapsto h + k \end{array} \right. .$$

Montrer que
– l'application φ est surjective si et seulement si $\langle H \cap K \rangle = G$;
– l'application φ est injective si et seulement si $H \cap K = \{0\}$.

THÉORÈME 1.14 *(chinois).* Soient $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. Alors l'application

$$\varphi\colon \left| \begin{array}{l} \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \\ \overline{a}^{mn} \longmapsto (\overline{a}^m, \overline{a}^n) \end{array} \right.$$

est un isomorphisme.

1.2 Groupes abéliens de type fini

1.2.1 Groupes monogènes, cycliques

DÉFINITION 1.15. Un groupe G est monogène s'il existe $x \in G$ tel que $G = \langle x \rangle$. De plus, si G est fini, alors il est dit cyclique.

◇ REMARQUE. Dans l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, on peut considérer le groupe des éléments inversibles pour $\times$, noté $(\mathbb{Z}/n\mathbb{Z})^\times$. Si a et b sont inversibles pour $\times$, alors $ab \equiv 1 \mod n$, donc le théorème de BÉZOUT donne alors $a \wedge n = 1$. Alors ce groupe est fini, abélien mais pas forcément cyclique. Par exemple, le groupe $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ n'est pas cyclique

PROPOSITION 1.16. Si G est un groupe monogène et $H < G$, alors H est monogène.

Preuve Il suffit de prendre $G = \mathbb{Z}$ ou $G = \mathbb{Z}/n\mathbb{Z}$. On suppose que $G = \mathbb{Z}$. Soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, c'est bon. Sinon on suppose que $H \neq \{0\}$ et alors $H \cap \mathbb{N}^* \neq \emptyset$. Soit $m \coloneqq \min\{n \in \mathbb{N}^* \mid n \in H\} > 0$. Par suite, on a $n\mathbb{Z} < H$. De plus, si $b \in H$, alors il existe $q \in \mathbb{N}$ et $r \in [\![0, m-1]\!]$ tels que $b = nq + r$, donc $r \in H$, donc $r = 0$ par minimalité de m, donc $b \in n\mathbb{Z}$. Même argument dans le cas où $G = \mathbb{Z}/n\mathbb{Z}$. □

PROPOSITION 1.17. Soit G un groupe cyclique. On note $G = \langle x \rangle$ et $m = |G|$. Soit $d \in \mathbb{N}^*$ et $d_1 \coloneqq d \wedge n$. Alors l'équation $X^d = 1$ admet d_1 solutions et l'ensemble solution de $X^d = 1$ est l'ensemble des solutions de $X^{d_1} = 1$, *i. e.* $S \coloneqq \{x_k \mid 0 \leqslant k \leqslant d_1 - 1\}$ où $x_k \coloneqq x^{km/d_1}$.

Preuve Montrons que les deux ensembles sont égaux. Soit $y \in G$. Alors $y^d = 1 \Leftrightarrow y^{d_1} = 1$. En effet, le sens réciproque est évident car $d_1 \mid d$. Le théorème de BÉZOUT donne l'existence de $u, v \in \mathbb{Z}$ tels que $um + vd = d_1$. Si $y^d = 1$, alors $y^{d_1} = y^{um} y^{vd} = (y^m)^u (u^d)^v = 1$.

Par ailleurs, pour tout $k \in [\![0, d_1 - 1]\!]$, on a $x_k^{d_1} = 1$. Si $z \in G - S$, alors on peut écrire $z = x^{km/d_1 + i}$ avec $1 < i < m/d_1$, donc $z^{d_1} = x^{d_1 i} \neq 1$ car $d_1 i < m$. □

LEMME 1.18. Soient G un groupe abélien et $x, y \in G$ d'ordres finis respectifs n et m. On suppose que $n \wedge m = 1$. Alors l'ordre de xy est nm.

Preuve On a $(xy)^{nm} = 1$, donc $\mathrm{o}(xy) \mid nm$. Par ailleurs, le groupe $\langle x\rangle \cap \langle y\rangle$ est un sous-groupe de $\langle x\rangle$ et de $\langle y\rangle$, donc le théorème de LAGRANGE donne que $|\langle x\rangle \cap \langle y\rangle|$ divise à la fois n et m, donc $\langle x\rangle \cap \langle y\rangle = \{1_G\}$ car $n \wedge m = 1$. On note $p = \mathrm{o}(xy)$. Par commutativité et comme $(xy)^p = 1$, on a $x^p = y^{-p}$, donc $x^p = y^{-p} = 1$, donc $x^p = 1$ et $y^p = 1$, donc $n \mid p$ et $m \mid p$, donc $nm \mid p$ car $n \wedge m = 1$. D'où $p = nm$. □

PROPOSITION 1.19. Soit G un groupe abélien fini tel que, pour tout $d \in \mathbb{N}^*$, l'équation $X^d = 1$ admette au plus d solutions dans G. Alors G est cyclique.

Preuve On note $n \coloneqq |G|$. La proposition est évidente pour $n = 1$. On suppose que $n \geqslant 2$. Il existe $p_1, \dots, p_\ell$ premiers et $d_1, \dots, d_\ell > 0$ tels que $n = \prod_{i=1}^{\ell} p_i^{\alpha_i}$. Soit $i \in [\![1, \ell]\!]$. Par hypothèse, il existe $b_i \in G$ tel que $b_i^{n/p_i} \neq 1$, donc $b_i^{n/p_i^{\gamma_i}} \neq 1$ $(*)$ pour tout $\gamma_i \in [\![1, \alpha_i]\!]$. On note $a_i \coloneqq b_i^{n/p_i^{\alpha_i}}$. Alors $a_i^{p_i^{\alpha_i}} = b_i^n = 1$, donc $\mathrm{o}(a_i) \mid p_i^{\alpha_i}$ et donc il existe $\beta_i \in [\![0, \alpha_i]\!]$ tel que $\mathrm{o}(a_i) = p_i^{\beta_i}$. Par $(*)$, on conclut que $\mathrm{o}(a_i) = p_i^{\alpha_i}$. Par application successives du lemmes, on en déduit que

$$\mathrm{o}\Big(\prod_{i=1}^{\ell} a_i\Big) = \prod_{i=1}^{\ell} p_i^{\alpha_i} = n.$$

Donc le groupe G est cyclique et engendré par $\prod_{i=1}^{\ell} a_i$. □

COROLLAIRE 1.20. Si K est un corps commutatif, alors tout sous-groupe fini de $(K^*, \times)$ est cyclique. En particulier, le groupe $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ est cyclique pour p premier.

Preuve Si $d \in \mathbb{N}^*$, alors le polynôme $X^d - 1$ de $K[X]$ a au plus d racines dans K. Donc K^* est cyclique. □

1.2.2 Groupes abéliens de type fini

DÉFINITION 1.21. Soient $(G, +)$ un groupe abélien de type fini. On dit qu'une famille génératrice $(x_1, \dots, x_n)$ est une pseudo-base si

$$\forall (m_1, \dots, m_n) \in \mathbb{Z}^n, \quad \sum_{i=1}^{n} m_i x_i = 0 \quad \Longrightarrow \quad m_1 x_1 = \cdots = m_n x_n = 0.$$

On dit que c'est une base si

$$\forall (m_1, \dots, m_n) \in \mathbb{Z}^n, \quad \sum_{i=1}^{n} m_i x_i = 0 \quad \Longrightarrow \quad m_1 = \cdots = m_n = 0.$$

On note $\mathrm{Tor}(G) \coloneqq \{x \in G \mid \mathrm{o}(x) < +\infty\}$. Alors $\mathrm{Tor}(G)$ est un sous-groupe de G, appelé sous-groupe de torsion de G. Si $\mathrm{Tor}(G) = G$, on dira que G est de torsion.

▷ EXEMPLES. – Soit $r \in \mathbb{N}^*$. Pour $i \in [\![1, r]\!]$, on note x_i l'élément de $\mathbb{Z}^r$ dont toutes les composantes sont nulles sauf la i-ième qui vaut 1. Alors $(x_1, \dots, x_r)$ est une base de $\mathbb{Z}^r$, appelée base canonique.
– Soit $n \in \mathbb{N}^*$. On note $G \coloneqq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}$. Alors (x_1, x_2) est une pseudo-base de G où $x_1 \coloneqq (\overline{1}, 0)$ et $x_2 \coloneqq (\overline{0}, 1)$. On a $\mathrm{Tor}(G) = \mathbb{Z}/n\mathbb{Z} \times \{0\} \simeq \mathbb{Z}/n\mathbb{Z}$.

◇ REMARQUES. – Si G admet une pseudo-base $(x_1, \dots, x_n)$, alors $G \simeq \langle x_1\rangle \times \cdots \times \langle x_n\rangle$. En effet, il suffit de considérer le morphisme

$$\phi\colon \left| \begin{array}{c} \langle x_1\rangle \times \cdots \times \langle x_n\rangle \longrightarrow G, \\ (m_1 x_1, \dots, m_n x_n) \longmapsto m_1 x_1 + \cdots + m_n x_n. \end{array} \right.$$

– Si G admet une base $(x_1, \dots, x_r)$, alors $G \simeq \mathbb{Z}^r$. En effet, il suffit de considérer le morphisme

$$\psi\colon \left| \begin{array}{c} \mathbb{Z}^r \longrightarrow G, \\ (m_1, \dots, m_r) \longmapsto m_1 x_1 + \cdots + m_r x_r. \end{array} \right.$$

THÉORÈME 1.22. Si G est un groupe abélien de type fini, alors il admet une pseudo-base. En particulier, il existe $m_1, \dots, m_s \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z} \times \mathbb{Z}^r$.

◇ REMARQUES. Par un isomorphisme, le groupe $\mathrm{Tor}(G)$ s'identifie à $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z}$. Alors G est d'ordre fini si et seulement si $\mathrm{Tor}(G) = G$. De plus, on a $\mathrm{Tor}(G) = \{0\}$ si et seulement si $G \simeq \mathbb{Z}^r$. Dans ce dernier cas, on dira que G est un groupe abélien libre.

LEMME 1.23 *(RADO).* Soient G un groupe abélien de type fini, $(x_1, \dots, x_k)$ une famille génératrice de G et $c \coloneqq (c_1, \dots, c_k) \in \mathbb{N}^k$ telle que $c_1 \wedge \cdots \wedge c_k = 1$. Alors il existe une famille génératrice $(y_1, \dots, y_k)$ de G telle que

$$y_1 = \sum_{i=1}^{k} c_i x_i.$$

Preuve On procède par récurrence sur $\sum_{i=1}^k c_i$. Si $\sum_{i=1}^k c_i = 1$, alors quitte à permuter les indices, on peut supposer que $c_1 = 1$ et donc $c_i = 0$ pour $i \in [\![2, k]\!]$, donc la famille $(x_1, \dots, x_n)$ convient.

On suppose que $\sum_{i=1}^k c_i > 1$. Alors il existe au moins deux éléments non nuls parmi c. Quitte à permuter les indices, on suppose que c_1 et c_2 sont non nuls et que $c_1 \geqslant c_2$. On considère la famille $c' \coloneqq (c_1 - c_2, c_2, \dots, c_k)$. On a bien $(c_1 - c_2) \wedge c_2 \wedge \cdots \wedge c_k = 1$. On considère la famille génératrice $(x_1, x_1 + x_2, x_3, \dots, x_k)$. On a alors $(c_1 - c_2) + c_2 + \cdots + c_k \leqslant \sum_{i=1}^k c_i$. D'après l'hypothèse de récurrence, il existe une famille génératrice $(y_1, \dots, y_k)$ de G telle que

$$y_i = (c_1 - c_2)x_1 + c_2(x_1 + x_2) + c_3 x_3 + \cdots + c_k x_k = \sum_{i=1}^{k} c_i x_i$$

ce qui termine la récurrence. □

Preuve du théorème On montre le résultat sur le nombre minimal k de générateurs. C'est vrai si $k = 1$ car alors $G \simeq \mathbb{Z}$. Soit $k \geqslant 2$. On suppose que la propriété est vraie au rang $k - 1$. Parmi les famille génératrice à k éléments, on en prend une $(x_1, \dots, x_k)$ où l'ordre de x_1 est minimal. Montrons que $G \simeq \langle x_1 \rangle \times \langle x_2, \dots, x_k \rangle$ ce qui permettra de conclure par l'hypothèse de récurrence. Il suffit de montrer que $\langle x_1 \rangle \cap \langle x_2, \dots, x_k \rangle = \{0\}$. Par l'absurde, supposons que $\langle x_1 \rangle \cap \langle x_2, \dots, x_k \rangle \neq \{0\}$. Dans ce cas, il existe $(m_1, \dots, m_r) \in \mathbb{Z}^r$ telle que $\sum_{i=1}^k m_i x_i = 0$. Quitte à remplacer les x_i par $-x_i$, on peut supposer que $m_i \geqslant 0$ pour tout $i \in [\![1, r]\!]$ et que $0 \neq m_1 < \mathrm{o}(x_1)$. Pour $i \in [\![1, r]\!]$, on note $c_i = m_i/d$ avec $d \coloneqq m_1 \wedge \cdots \wedge m_k$. Alors la famille $c \coloneqq (c_1, \dots, c_k)$ satisfait les hypothèses du lemme, donc il existe une famille génératrice $(y_1, \dots, y_k)$ telle que

$$y_1 = \sum_{i=1}^{k} c_i x_i.$$

En multipliant cette relation par d, on a $dy_1 = \sum_{i=1}^k m_i x_i = 0$, donc $\mathrm{o}(y_1) \mid d \leqslant m_1 < \mathrm{o}(x_1)$ avec $\mathrm{o}(x_1)$ minimal ce qui est impossible. D'où $G \simeq \langle x_1 \rangle \times \langle x_2, \dots, x_k \rangle$. L'hypothèse de récurrence permet alors de conclure. □

PROPOSITION 1.24. Soit G un groupe abélien de type fini. De la décomposition $G \simeq \mathrm{Tor}(G) \times \mathbb{Z}^r$, l'entier r est défini de façon unique et s'appelle le rang de G.

Preuve On traite le cas où $\mathrm{Tor}(G) = \{0\}$. Alors $G \simeq \mathbb{Z}^r$. Il suffit de montrer que, si $\varphi \colon \mathbb{Z}^r \to \mathbb{Z}^{r'}$ est un isomorphisme, alors $r = r'$. Soit $(e_1, \dots, e_r)$ la base canonique de $\mathbb{Z}^r$. Comme φ est un isomorphisme, la famille $(\varphi(e_1), \dots, \varphi(e_r))$ est une base de $\mathbb{Z}^{r'}$, donc elle engendre sur $\mathbb{Q}$ un $\mathbb{Q}$-espace vectoriel de dimension r, donc $r' \geqslant r$. En utilisant φ^{-1}, on obtient également que $r' \leqslant r$. D'où $r = r'$ et donc l'unicité. □

THÉORÈME 1.25. Soit G un groupe abélien de type fini. On note r son rang. Soit H un sous-groupe de G. Alors H est de type fini et son rang est inférieur à r.

Preuve On suppose que G est libre. Alors $G \simeq \mathbb{Z}^r$. On procède alors par récurrence sur r. Si $r = 1$, alors $H = n\mathbb{Z}$ avec $n \in \mathbb{N}$, donc le rang de H vaut 0 ou 1. Soit $r > 1$. On suppose que la propriété est vraie au rang $r - 1$. On considère la projection

$$\varphi \colon \left| \begin{array}{c} \mathbb{Z}^r \longrightarrow \mathbb{Z}, \\ (m_1, \dots, m_r) \longmapsto m_r. \end{array} \right.$$

Alors l'application φ est un morphisme. Soit H un sous-groupe de $\mathbb{Z}^r$. Alors $\varphi(H)$ est un sous-groupe de $\mathbb{Z}$, donc il s'écrit sous la forme $\varphi(H) = \varphi(h_0)\mathbb{Z}$ avec $h_0 \in H$. Si $\varphi(H) = \{0\}$, alors $H < \mathrm{Ker}\,\varphi \simeq \mathbb{Z}^{r-1}$ et on applique la récurrence. On suppose désormais que $\varphi(H) \neq \{0\}$. Alors $H \cap \mathrm{Ker}\,\varphi$ est un sous-groupe de $\mathbb{Z}^{r-1}$, donc il admet une base $(h_1, \dots, h_s)$ avec $s \leqslant r - 1$ par l'hypothèse de récurrence. Soit $h \in H$. Alors il existe $n_0 \in \mathbb{Z}$ tels que $\varphi(h) = n_0\varphi(h_0)$, donc $h - n_0 h_0 \in \mathrm{Ker}\,\varphi$. De même, on montre qu'il existe $(m_0, \dots, m_s) \in \mathbb{Z}^{s+1}$ telle que $h = \sum_{i=0}^s m_i h_i$. Donc la famille $(h_0, \dots, h_s)$ est génératrice de H et on vérifie qu'elle est libre, donc le rang s de H est inférieur à r.

On revient au cas général. On peut supposer que $G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z} \times \mathbb{Z}^r$. Soit H un sous-groupe de G. Alors $\mathrm{Tor}(H)$ est un sous-groupe de $\mathrm{Tor}(G)$, donc $H = \mathrm{Tor}(G) \times p(H)$ où $p \colon G \to \mathbb{Z}^r$ est la projection sur $\mathbb{Z}^r$. On se ramène alors au cas précédent. □

◇ REMARQUE. Il n'y a pas unicité des entiers m_i. Par exemple, le théorème chinois donne $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Par contre, il y a unicité dans le cas suivant.

THÉORÈME 1.26. Un groupe abélien G de type fini s'écrit sous l'une des formes suivantes :
1. il existe $m_1, \dots, m_s \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_s\mathbb{Z} \times \mathbb{Z}^r$ et $m_i \mid m_{i+1}$ pour tout $i \in [\![1, s-1]\!]$;
2. il existe $p_1, \dots, p_s \in \mathbb{N}$ premiers, $\alpha_1, \dots, \alpha_s \in \mathbb{N}^*$ et $r \in \mathbb{N}$ tels que $G \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z} \times \mathbb{Z}^r$.

Ces décompositions sont uniques à l'ordre près des facteurs.

EXERCICE 1.3. Donner les décompositions 1 et 2 du groupe

$$G \coloneqq \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/45\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}.$$

▷ On a $60 = 2^2 \times 3 \times 5$, $45 = 3^2 \times 5$ et $36 = 2^2 \times 3^2$, donc le théorème chinois donne

$$G \simeq (\mathbb{Z}/2^2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/3^2\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2 = (\mathbb{Z}/4)^2 \times \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/9\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2.$$

Pour avoir la décomposition 1 à partir de la décomposition 2, on la casse et on la recompose avec le théorème chinois.

1.3 Le groupe diédral

1.3.1 Définition

DÉFINITION 1.27. Soit $n \geqslant 3$. On identifie $\mathbb{C}$ à $\mathbb{R}^2$. On considère le polygone régulier

$$\mathscr{P}_n = \{e^{2i\pi k/n} \mid k \in [\![0, n-1]\!]\}$$

qui possède n sommets. Le groupe D_n est le sous-groupe des isométries du plan affine qui fixent globalement $\mathscr{P}_n$.

THÉORÈME 1.28. Le groupe D_n est d'ordre $2n$, il est engendré par la symétrie axiale $s \in \mathscr{L}(\mathbb{R}^2)$ telle que

$$\mathrm{Mat}_{\mathscr{B}}(s) \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

et par la rotation r d'angle $\theta \coloneqq 2\pi/n$ telle que

$$\mathrm{Mat}_{\mathscr{B}}(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

où $\mathscr{B}$ est la base canonique de $\mathbb{R}^2$. Les isométries r et r sont respectivement d'ordre 2 et n. On a $srs = r^{-1}$. Enfin, on a

$$D_n = \{\mathrm{Id}, r, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}.$$

Preuve Il est clair que $\langle r, s\rangle$ est un sous-groupe de D_n. Réciproquement, soit $f \in D_n$. Comme f est une isométrie affine préservant $\mathscr{P}_n$, elle préserve les barycentres et l'origine en particulier, donc $f(0) = 0$, donc f est une rotation ou une symétrie axiale. Soit $A \in \mathscr{P}_n$. Alors $f(A) \in \mathscr{P}_n$, donc il existe $k \in [\![0, n-1]\!]$ tel que $r^k(A) = f(A)$, donc $r^{-k} \circ f(A) = A$. Si f est une rotation, alors $r^{-k} \circ f$ est aussi une rotation fixant A et 0, donc $r^{-k} \circ f = \mathrm{Id}$ et $f = r^k$. Si f est une symétrie, alors $f \circ s$ est une rotation, donc on se ramène au cas précédent et il existe $k \in [\![0, n-1]\!]$ tel que $f = r^k \circ s$. D'où le théorème. □

◇ REMARQUES. 1. On remarque que $D_n = \langle r\rangle \sqcup \langle r\rangle s$.
2. On peut définir D_1 et D_2 comme $D_i = \langle r_\theta, s\rangle$ avec $\theta = 2\pi/i$. On vérifie que $D_1 \simeq \mathbb{Z}/2\mathbb{Z}$ et $D_2 \simeq (\mathbb{Z}/Z\mathbb{Z})^2$.
3. Si $n \geqslant 3$, alors le groupe D_n n'est pas abélien car, si $rs = sr$, alors $srs = s^2r = r = r^{-1}$, donc $r^2 = \mathrm{Id}$ ce qui est impossible.

1.3.2 Caractérisation abstraite

LEMME 1.29. Soient G un groupe et H et K deux sous-groupes de G. On note $HK \coloneqq \{hk \mid h \in H, k \in K\}$. On suppose que $H \cap K = \{1\}$. Alors l'application

$$\left|\begin{array}{l} H \times K \longrightarrow HK, \\ (h, k) \longmapsto hk \end{array}\right.$$

est bijective. En particulier, on a $\sharp HK = |H|\,|K|$ si H et K sont finis.

Preuve Il suffit de montrer que cette application est injective. Soient $h, h' \in H$ et $k, k' \in K$ tels que $hk = h'k'$. Alors $k' = h'^{-1}hk \in K$ avec $k \in K$, donc $h'^{-1}h \in K \cap H$, donc $h' = h$ puis $k' = k$. D'où l'injectivité. □

THÉORÈME 1.30. Soit G un groupe. On suppose que
(i) le groupe G est engendré par deux éléments r et s ;
(ii) $\mathrm{o}(s) = 2$ et $\mathrm{o}(r) = n \geqslant 3$;
(iii) $srs = r^{-1}$.
Alors $G \simeq D_n$.

Preuve On a $\langle s\rangle \cap \langle r\rangle = \{1\}$ car sinon, comme $\langle s\rangle = \langle 1, s\rangle$, il existerait $k \in \mathbb{N}$ tel que $s = r^k$, donc $sr = rs$ ce qui est impossible. D'après le lemme précédent, la partie

$$A \coloneqq \{r^i s^j \mid i \in [\![0, n-1]\!], j \in \{0, 1\}\}$$

possède $2n$ éléments dont r et s. Montrons que $A = G$. On a déjà $A \subset G$. Puisque A est finie, il suffit de montrer qu'elle est stable par multiplication. Pour cela, remarquons que $srs = srs^{-1} = r^{-1}$, donc $sr^i s = r^{-i}$ pour tout $i \in [\![0, n-1]\!]$. Puis pour tout $i, i' \in [\![0, n-1]\!]$ et $j, j' \in \{0, 1\}$,
– si $j = 0$, alors $r^i s^j r^{i'} s^{j'} = r^I s^{j'}$ avec $I \coloneqq i + i'$ $[n] \in [\![0, n-1]\!]$;
– si $j = 1$, alors $r^i s^j r^{i'} s^{j'} = r^I s^J$ avec $I \coloneqq i - i'$ $[n] \in [\![0, n-1]\!]$ et $J \coloneqq 1 + j^2$ $[2] \in \{0, 1\}$.
Dans tous les cas, on a $r^i s^j r^{i'} s^{j'} \in A$ ce qui permet de conclure que $A = G$. On a ainsi calculé la table : elle est entièrement déterminée par les hypothèses (i), (ii) et (iii), conditions vérifiées par D_n. D'où $G \simeq D_n$. □

1.4 Sous-groupes normaux

1.4.1 Définition

DÉFINITION 1.31. Soient G un groupe et H un sous-groupe de G. On dit que H est normal (ou distingué) dans G si, pour tous $g \in G$ et $h \in H$, on a $ghg^{-1} \in H$. Dans ce cas, on note $H \triangleleft G$.

◇ REMARQUE. On peut également reformuler cette définition par l'équivalence

$$H \triangleleft G \quad \Longleftrightarrow \quad (\forall g \in G, \quad \mathrm{int}_g(H) = H)$$

où, pour tout $g \in G$, on pose l'automorphisme de G

$$\mathrm{int}_g : \begin{vmatrix} G \longrightarrow G, \\ x \longmapsto gxg^{-1}, \end{vmatrix}$$

appelé automorphisme intérieur de G associé à g. On a également

$$H \triangleleft G \quad \Longleftrightarrow \quad (\forall h \in G, \quad gH = Hg).$$

▷ EXEMPLES. 1. Si G est abélien, alors tout sous-groupe de G est normal.
2. Les groupes G et $\{1\}$ sont des sous-groupes normaux dans G.
3. Soit $\varphi : G \to G'$ un morphisme. Alors $\ker \varphi$ est un sous-groupe normal dans G'.
4. Comme $\det : \mathrm{GL}_n(K) \to K^\times$ est un morphisme, son noyau, noté $\mathrm{SL}_n(K)$, est normal dans $\mathrm{GL}_n(K)$.
5. Dans D_n avec $n \geqslant 3$, le groupe $\langle s\rangle$ n'est pas normal. En effet, on a $rsr^{-1} = r^2 s \neq s$

PROPOSITION 1.32. Soient G un sous-groupe et H un sous-groupe de G. Si $[G : H] = 2$, alors $H \triangleleft G$.

Preuve On suppose que $[G : H] = 2$. Soit $g \in G \setminus H$. La partition par les classes à droites donne $G = H \sqcup Hg$ et celle par les classes à gauches donne $G = H \sqcup gH$, donc $Hg = gH$. Ceci est également vrai pour $g \in H$. □

◇ REMARQUE. Soit G un groupe de type fini, noté $G = \langle A\rangle$, et H un sous-groupe de G. Alors

$$H \triangleleft G \quad \Longleftrightarrow \quad (\forall g \in A, \quad \mathrm{int}_a(H) = H)$$

car le groupe $\{a \in G \mid \mathrm{int}_a(H) = H\}$ est un sous-groupe de G.

PROPOSITION 1.33. Soient G un groupe et $A \subset G$ telle que $xAx^{-1} = A$ pour tout $x \in G$. Alors $\langle A\rangle \triangleleft G$.

LEMME 1.34. Soient G_1 et G_2 deux groupes, $\varphi : G_1 \to G_2$ un morphisme et $A \subset G_1$. Alors $\varphi(\langle A\rangle) = \langle \varphi(A)\rangle$.

Preuve de la proposition Il suffit de prendre $G = G_1 = G_2$ et $\varphi = \mathrm{int}_x$ pour $x \in G$. □

▷ EXEMPLE. Soit G un groupe. Pour tous $x, y \in G$, on note $[x, y] = xyx^{-1}y^{-1}$ le commutateur de x et y. On pose

$$\mathrm{D}(G) \coloneqq \langle \mathscr{C}\rangle \quad \text{avec} \quad \mathscr{C} \coloneqq \{[x, y] \mid x, y \in G\}$$

le groupe dérivé de G. Montrons qu'il est normal dans G. Il suffit de montrer que $\varphi(\mathrm{D}(G)) = \mathrm{D}(G)$ pour tout $\varphi \in \mathrm{Aut}(G)$ et il suffira de prendre $\varphi = \mathrm{int}_x$ ensuite. Soient $\varphi \in \mathrm{Aut}(G)$ et $x, y \in G$. On a $[x,y] = xyx^{-1}y^{-1}$, donc $\varphi([x,y]) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = [\varphi(x), \varphi(y)] \in \mathrm{D}(G)$ et $[x,y] = \varphi([\varphi^{-1}(x), \varphi^{-1}(y)]) \in \varphi(\mathrm{D}(G))$. Ainsi $\varphi(\mathscr{C}) = \mathscr{C}$, donc le lemme donne $\varphi(\mathrm{D}(G)) = \mathrm{D}(G)$.

Définition 1.35. Soient G un groupe et H un sous-groupe de G. On dit que H est caractéristique si, pour tout $\varphi \in \mathrm{Aut}(G)$, on a $\varphi(H) = H$.

▷ Exemple. On vient de démontrer que $\mathrm{D}(G)$ est caractéristique.

1.4.2 Groupes quotient

Définition 1.36. Soient G un groupe et H un sous-groupe de G. On pose

$$G/H \coloneqq \{gH \mid g \in G\}$$

l'ensemble des classes d'équivalences par la relation d'équivalence $\sim$ sur G définie par

$$x \sim y \quad \Longleftrightarrow \quad y^{-1}x \in H.$$

But. On considère la projection canonique

$$\pi : \left| \begin{array}{l} G \longrightarrow G/H, \\ g \longmapsto g \mod H. \end{array} \right.$$

On veut munir l'ensemble G/H d'une structure de groupe pour une loi $*$ telle que l'application φ sois un morphisme, *i. e.* $\overline{x} * \overline{y} = \overline{x * y}$. Dans ce cas, le loi $*$ est unique.

Théorème 1.37. Soit H un sous-groupe normal de G. Il existe une unique loi $*$ de groupe sur G/H telle que l'application π soit un morphisme.

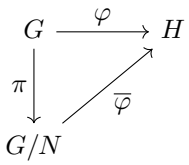
Preuve Il s'agit de montrer que $*$ est bien définie. Soient $x, x' \in G$ et $y, y' \in G$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$. Il faut et il suffit que $\overline{xy} = \overline{x'y'}$. On a $(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' \in H$ car $x^{-1}x' \in H$ et le sous-groupe H est normal. Donc la loi $*$ a un sens : elle ne dépend pas des représentants choisis.

On remarque que G/H admet bien un élément neutre qui est $\overline{1_G}$. Par ailleurs, pour tout $x \in G$, le symétrique de $\overline{x}$ est $\overline{x^{-1}}$. On montre également l'associativité. En particulier, l'application φ est bien un morphisme. □

Corollaire 1.38. Alors H est un sous-groupe normal dans G si et seulement s'il existe un groupe G_1 et un morphisme $\varphi : G \to G_1$ tel que $H = \mathrm{Ker}\,\varphi$.

Preuve Le sens réciproquement a déjà été montré. Si H est normal dans G, alors on prend $\varphi : G \to G/H$ la projection canonique de G sur G/H. □

Théorème 1.39 *(de factorisation).* Soient $\varphi : G \to H$ un morphisme et N un sous-groupe normal de G qui soit un sous-groupe de $\mathrm{Ker}\,\varphi$. Alors il existe un unique morphisme $\overline{\varphi} : G/N \to H$ qui fait commuter le diagramme



i. e. tel que $\overline{\varphi} \circ \pi = \varphi$. De plus, si $N = \mathrm{Ker}\,\varphi$, alors l'application $\overline{\varphi}$ est injective et l'application

$$\left| \begin{array}{l} G/N \longrightarrow \mathrm{Im}\,\overline{\varphi} = \mathrm{Im}\,\varphi, \\ x \longmapsto \overline{\varphi}(x) \end{array} \right.$$

est un isomorphisme.

Preuve Si un telle application $\overline{\varphi}$ existe, alors $\overline{\varphi}(\overline{x}) = \varphi(x)$ pour tout $x \in G$, donc φ est unique. Par ailleurs, si $\overline{y} = \overline{x}$, alors $x^{-1}y \in N < \mathrm{Ker}\,\varphi$, donc $\varphi(x^{-1}y) = 1$, donc $\varphi(x) = \varphi(y)$. Donc $\overline{\varphi}$ est bien définie. Le reste se vérifient facilement. □

Proposition 1.40. Soit $N \triangleleft G$. On note $\overline{G} \coloneqq G/N$, puis $\mathfrak{G}$ l'ensemble des sous-groupes H de G tel que $N < H$

et $\overline{\mathfrak{G}}$ l'ensemble des sous-groupes de $\overline{G}$. Alors les applications

$$\begin{vmatrix} \mathfrak{G} \longrightarrow \overline{\mathfrak{G}}, \\ H \longmapsto \pi(H) = \overline{H}, \end{vmatrix} \quad \text{et} \quad \begin{vmatrix} \overline{\mathfrak{G}} \longrightarrow \mathfrak{G}, \\ \overline{H} \longmapsto \pi^{-1}(\overline{H}) \end{vmatrix}$$

sont des bijections, réciproque l'une de l'autre. De plus, on a $N < H \triangleleft H \Leftrightarrow \overline{H} \triangleleft \overline{G}$

1.4.3 Exemples fondamentaux

(i) Centre d'un groupe

Définition 1.41. Soit G un groupe. On pose

$$\mathrm{Z}(G) \coloneqq \{x \in G \mid \forall g \in G, xg = gx\}$$

le centre de G.

Proposition 1.42. Alors $Z(G) \triangleleft G$ comme noyau du morphisme

$$\mathrm{Int}: \begin{vmatrix} G \longrightarrow \mathrm{Aut}(G), \\ g \longmapsto \mathrm{int}_g\,. \end{vmatrix}$$

Par le théorème d'isomorphisme, on a $\mathrm{Im}(\mathrm{Int}) \simeq G/\mathrm{Z}(G)$.

▷ Exemple. Comme $\mathrm{Z}(D_3) = \{\mathrm{Id}\}$, on a $\mathrm{Int}(D_3) \simeq D_3$, donc $\mathrm{Aut}(D_3) = D_3$.

◇ Remarques. 1. Un groupe coïncide avec son centre si et seulement s'il est abélien.

2. Pour tout $n \in \mathbb{N}$, on a $|\mathrm{Aut}(D_n)| = n\varphi(n)$.

3. On peut montrer que $\mathrm{Int}(G) \triangleleft \mathrm{Aut}(G)$. Le quotient $\mathrm{Out}(G) \coloneqq \mathrm{Aut}(G)/\mathrm{Int}(G)$ est appelé groupe des automorphismes extérieurs de G.

(ii) Groupe dérivé

Définition 1.43. Soit G un groupe. On pose

$$\mathrm{D}(G) \coloneqq \langle \mathscr{C} \rangle \quad \text{avec} \quad \mathscr{C} \coloneqq \{[x,y] \coloneqq xyx^{-1}y^{-1} \mid x, y \in G\}$$

le groupe dérivé de G.

◇ Remarque. On a $\mathrm{D}(G) = \{1\}$ si et seulement si G est abélien.

Proposition 1.44. 1. On a $\mathrm{D}(G) \triangleleft G$. On note alors

$$G^{\mathrm{ab}} \coloneqq G/\mathrm{D}(G)$$

l'abélianisé de G. C'est un groupe abélien.

2. Soient G_1 un groupe abélien et $\varphi\colon G \to G_1$ un morphisme. Alors $\mathrm{D}(G) < \mathrm{Ker}\,\varphi$ et il existe un unique morphisme $\overline{\varphi}\colon G^{\mathrm{ab}} \to G_1$ tel que $\overline{\varphi} \circ \pi = \varphi$ où l'application π est la projection de G sur G^{ab}

Preuve 1. Cela résulte du fait que $\mathrm{D}(G)$ est caractéristique dans G (cf. exemple page 8). Montrons que G^{ab} est abélien. Soient $\overline{x}, \overline{y} \in G^{\mathrm{ab}}$. On a $[\overline{x}, \overline{y}] = \overline{[x,y]}$ car l'application π est un morphisme.

2. Soient $x, y \in G$. On a $\varphi([x,y]) = [\varphi(x), \varphi(y)] = 1$, donc $[x,y) \in \mathrm{Ker}\,\varphi$. D'où $\mathrm{D}(G) < \mathrm{Ker}\,\varphi$. On conclut par factorisation des morphismes. □

Corollaire 1.45. Soit $H \triangleleft G$ tel que G/H soit abélien. Alors $\mathrm{D}(G) < H$.

Preuve C'est la conséquence du point 3 de la proposition précédente avec $\varphi = \pi$. □

▷ Exemples. – On a $\mathrm{D}(D_3) = \langle r \rangle$ et, puisque $[D_3, \langle r \rangle] = 2$, on a $D_3^{\mathrm{ab}} = D_3/\langle r \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. En effet, on a $[s,r] = srs^{-1}r^{-1} = srsr^{-1} = r^{-2} = r$, donc $\mathrm{D}(D_3) > \langle r \rangle$. Par ailleurs, on a $\langle y \rangle \triangleleft D_3$ car $[D_3, \langle r \rangle] = 2$, donc le groupe $D_3/\langle r \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ est abélien, donc $\mathrm{D}(D_3) < \langle r \rangle$ par le corollaire.

– On a $\mathrm{D}(D_4) = \langle r^2 \rangle = \langle \pm\mathrm{Id} \rangle$. En effet, on a $r^{-2} = [s,r]$, donc $\mathrm{D}(D_4) > \langle r^{-2} \rangle = \{\pm\mathrm{Id}\}$. Par ailleurs, on a $\{\pm\mathrm{Id}\} \triangleleft D_4$, donc le groupe quotient $D_4/\{\pm\mathrm{Id}\}$ est d'ordre 4 et donc il est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$ qui sont abéliens. Comme précédent, on conclut que $\mathrm{D}(D_4) = \{\pm\mathrm{Id}\}$. Finalement, on a $D_4^{\mathrm{ab}} \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

POUR CONCLURE. Soit G un groupe abélien de type fini. Alors il existe $m_1, \dots, m_s \in \mathbb{Z}$ et $r \in \mathbb{N}$ tels que

$$G \simeq \underbrace{\mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_s^{n_s}}_{\simeq \mathrm{Tor}(G)} \times \mathbb{Z}^r \quad \text{et} \quad m_1 \mid \cdots \mid m_s.$$

On a donc $G/\mathrm{Tor}(G) \simeq \mathbb{Z}^r$. Ceci montre en toute généralité la proposition 1.24, *i. e.* le rang r de G est unique.

1.5 Actions de groupes

1.5.1 Définitions et premières propriétés

NOTATION. Soit X un ensemble. On note $\mathfrak{S}_X$ son groupe symétrique, *i. e.* l'ensemble des bijections $X \to X$.

DÉFINITION 1.46 *(action de groupe).* Soient G un groupe et X un ensemble. On appelle action de G sur X tout morphisme $\rho\colon G \to \mathfrak{S}_X$ telle que l'application

$$\left|\begin{array}{l} G \times X \longrightarrow X, \\ (g,x) \longmapsto g \cdot x \coloneqq \rho(g)(x) \end{array}\right.$$

vérifie les conditions suivantes :

(i) pour tout $x \in X$, on a $1 \cdot x = x$;

(ii) pour tous $g, h \in G$ et $x \in X$, on a $g \cdot (h \cdot x) = (gh) \cdot x$.

◇ REMARQUE. Beaucoup de groupes viennent naturellement avec des actions. Par exemple, l'ensemble $[\![1, n]\!]$ agit sur les groupes $\mathfrak{S}_n$ et D_n, l'ensemble $\mathbb{R}^n$ agit sur le groupe $\mathrm{GL}_n(\mathbb{R})$.

DÉFINITION 1.47 *(terminologie de base).* Pour tout $x \in X$, on appelle orbite de x l'ensemble

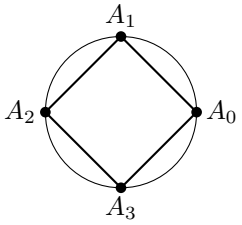
$$G \cdot x \coloneqq \{g \cdot x \mid g \in G\}$$

et on appelle stabilisateur de x l'ensemble

$$G_x \coloneqq \{g \in G \mid g \cdot x = x\}.$$

On a alors $G \cdot x \subset X$ et $G_x < G$.

▷ EXEMPLE. On fait agir l'ensemble des sommets $\{A_0, \dots, A_3\}$ du carré sur le groupe D_4.



Alors $(D_4)_{A_0} = \{\mathrm{Id}, s\}$ et $D_4 \cdot A_0 = \mathscr{P}_4$.

PROPOSITION 1.48. Soit X un ensemble agissant sur G. Alors

1. pour tout $g \in G$ et $x \in X$, on a $G_{g\cdot x} = gG_xg^{-1}$;
2. pour tout $x \in X$, l'application

$$\alpha\colon \left|\begin{array}{l} G/G_x \longrightarrow G \cdot x, \\ gG_x \longmapsto g \cdot x \end{array}\right.$$

est bien définie et bijective.

3. Soit $\mathscr{R}$ la relation sur X telle que $x \mathscr{R} y \Leftrightarrow x \in G \cdot y$ pour tout $x, y \in X$. Alors $\mathscr{R}$ est une relation d'équivalence. En particulier, ses classes forment une partition de X.

Preuve 1. Soient $g \in G$, $x \in X$ et $h \in G$. On a

$$h \in G_{g\cdot x} \;\Leftrightarrow\; h \cdot (g \cdot x) = g \cdot x \;\Leftrightarrow\; (hg) \cdot x = g \cdot x \;\Leftrightarrow\; (g^{-1}hg) \cdot x = x \;\Leftrightarrow\; h \in gG_xg^{-1}.$$

2. Soit $x \in X$. L'application α est bien définie car, pour $h \in gG_x$, on a $g^{-1}h \in G_x$, donc $g^{-1}h \cdot x = x$, donc $h \cdot x = g \cdot x$. Elle est clairement surjective. Montrons qu'elle est injective. Soient $g, h \in G$ tels que $\alpha(g) = \alpha(h)$. Alors $h \cdot x = g \cdot x$, donc $(g^{-1}h) \cdot = x$, donc $g^{-1}h \in G_x$, donc $h \in gG_x$. On en déduit que $gG_x = hG_x$.

3. La relation $\mathscr{R}$ est réflexive car, pour tout $x \in X$, le premier axiome donne $x = 1 \cdot x$, donc $x \mathscr{R} x$. Pour tous $x, y \in X$, si $x \mathscr{R} y$, alors il existe $g \in G$ tel que $x = g \cdot y$, donc $y = g^{-1} \cdot x$, donc $y \mathscr{R} x$. On montre également que $\mathscr{R}$ est transitive ce qui en fait une relation d'équivalence avec ce qui précède. □

◇ Remarque. Ainsi, si G est fini, alors $|G \cdot x| = [G : G_x]$ pour tout $x \in X$ et, en particulier, $|G \cdot x| \mid |G|$. Si G possède une unique orbite, on dit que l'action est transitive.

▷ Exemples. – L'ensemble $\mathbb{R}^n$ agit sur le groupe $G \coloneqq \mathrm{GL}_n(\mathbb{R})$ par l'action $(A, x) \longmapsto Ax$. On a $G \cdot 0 = \{0\}$ et, si $x \in \mathbb{R}^n - \{0\}$, on a $G \cdot x = \mathbb{R}^n$. Ainsi, la partition de $\mathbb{R}^n$ par les orbites donne $\mathbb{R}^n = (\mathbb{R}^n - \{0\}) \sqcup \{0\}$. De plus, on a $G_0 = G$ et, si e_1 désigne le premier vecteur de la base canonique de $\mathbb{R}^n$, alors

$$G_{e_1} = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & M & \\ 0 & & & \end{pmatrix} \;\middle|\; M \in \mathrm{GL}_{n-1}(\mathbb{R}) \right\}.$$

– • *Translation à gauche.* On fait agir G sur lui-même *via* l'action $(g, x) \longmapsto gx$. Cette action est transitive car toutes les orbites coïncident avec G. De plus, pour tout $x \in G$, on a $G_x = \{1\}$. En particulier, l'application

$$\varphi \colon \left| \begin{array}{l} G \longrightarrow \mathfrak{S}_G \\ g \longmapsto \{x \longmapsto gx\} \end{array} \right.$$

est injective, donc $G \simeq \varphi(G) < \mathfrak{S}_G$. Ainsi, on en déduit le théorème de Cayley qui affirme que, si G est d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

1.5.2 Exemples fondamentaux

(i) Action par conjugaison

L'application $\mathrm{Int} \colon G \to \mathrm{Aut}(G) < \mathfrak{S}_G$ induit une action de groupe $(g, x) \longmapsto g \cdot x \coloneqq gxg^{-1}$ de G sur lui-même. Pour $x \in G$, on appelle alors $G \cdot x$ la classe de conjugaison de x dans G et on note

$$\mathrm{C}_G(x) \coloneqq G_x = \{g \in G \mid gx = xg\},$$

appelé centralisateur de x dans G.

▷ Exemple. On prend $G = D_3$. La partition suivant les classes de conjugaison donne

$$|D_3 \cdot x| = \frac{6}{|\mathrm{C}_{D_3}(x)|}, \quad \forall x \in D_3.$$

On a $D_3 \cdot \mathrm{Id} = \{\mathrm{Id}\}$. Que vaut $D_3 \cdot r$? On a $\mathrm{C}_{D_3}(r) = \langle r \rangle$, donc $|D_3 \cdot r| = 2$. Par ailleurs, on a $r^{-1} = srs = srs^{-1}$, donc $D_3 \cdot r = \{r, r^{-1}\}$. De même, on a $\mathrm{C}_{D_3}(s) = \langle s \rangle$, donc $|D_3 \cdot s| = 3$. Puis $1 + 2 + 3 = 6 = |D_3|$, donc on a nécessairement $D_3 \cdot s = \{s, rs, r^2 s\}$.

(ii) Action sur un groupe quotient

Soit $H < G$. On considère une action de G sur G. Alors G agit sur G/H par $g \cdot (xH) \coloneqq (gx) \cdot H$. Alors c'est une action transitive, *i. e.* $G_H = H$. On montre alors que $G_{xH} = xHx^{-1}$ pour tout $x \in G$.

(iii) Action sur les sous-groupes

Un groupe G agit sur l'ensemble des sous-groupes de G par conjugaison $g \cdot H \coloneqq gHg^{-1} = \mathrm{int}_g(H)$. Pour un sous-groupe H de G, on note

$$\mathrm{N}_G(H) \coloneqq G_H = \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\},$$

appelé normalisateur de H dans G. On remarque que $H \lhd \mathrm{N}_G(H)$ et que, si $H \lhd K < G$, alors $K < \mathrm{N}_G(H)$.

1.5.3 Équation aux classe

Soit X un ensemble fini. On considère une action de groupe de X sur G. On rappelle que les orbites partitionnent X et que, pour tout $x \in X$, on a $\sharp(G \cdot x) = [G : G_x]$. On prend un système de représentants des orbites $\{x_1, \ldots, x_n\} \subset X$. On a donc

$$\sharp X = \sum_{i=1}^{n} [G : G_x].$$

En distinguant les orbites formées d'un seul élément (les classes de x_i telles que $g \cdot x_i = x_i$ pour tout $g \in G$), on obtient la proposition suivante.

PROPOSITION 1.49 *(équation aux classes).* Alors en notant $X^G \coloneqq \{x \in X \mid \forall g \in G, g \cdot x = x\}$, on a

$$|X| = |X^G| + \sum_{\substack{i \in [\![1,n]\!] \\ G_{x_i} \neq G}} [G : G_{x_i}].$$

Application

DÉFINITION 1.50. Un p-groupe est un groupe G tel qu'il existe $n \in \mathbb{N}^*$ vérifiant $|G| = p^n$.

COROLLAIRE 1.51. Soit une action de X sur un p-groupe G avec $\sharp X < +\infty$. Alors $\sharp X = |X^G| \mod p$.

PROPOSITION 1.52. Soit G un p-groupe. Alors $\mathrm{Z}(G) \neq \{1\}$

Preuve On considère l'action par conjugaison de G sur lui-même. Alors $\mathrm{Z}(G) = G^G \neq \{1\}$. □

THÉORÈME 1.53 *(CAUCHY).* Soient G un groupe fini et $p \in \mathbb{N}$ un diviseur premier de $|G|$. Alors G contient au moins un élément d'ordre p.

Preuve On suppose d'abord que G est abélien. Dans ce cas, il est isomorphe à un groupe de la forme

$$\prod_{i=1}^{\ell} \mathbb{Z}/m_i\mathbb{Z}.$$

En particulier, on a $|G| = \prod_{i=1}^{\ell} m_i$. Ainsi il existe $i \in [\![1, \ell]\!]$ tel que $p \mid m_i$. Alors l'élément

$$\left(0, \ldots, 0, \overline{\frac{m_i}{p}}, 0, \ldots, 0\right)$$

est d'ordre p. On ne suppose plus que G est abélien. On procède par récurrence sur $|G|$. Si $|G| = p$, alors $G \simeq \mathbb{Z}/p\mathbb{Z}$ et le résultat devient évident. On suppose que $|G|$ est quelconque. Alors on considère l'action de G sur lui-même par conjugaison. En notant $\{x_1, \ldots, x_n\}$ l'ensemble des représentants des classes, l'équation aux classes donne

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{n} [G : \mathrm{C}_G(x_i)].$$

S'il existe $i \in [\![1, n]\!]$ tel que $p \nmid [G : \mathrm{C}_G(x_i)]$, alors $p \mid |\mathrm{C}_G(x_i)|$ puisque $p \mid |G|$ et on conclut par récurrence. Sinon on a $p \mid |\mathrm{Z}(G)|$ et on peut se ramener au cas précédent. Ce qui montre le résultat dans tous les cas. □

APPLICATION. Si $|G| = 2p$ avec $p \geqslant 3$ premier, alors $G \simeq \mathbb{Z}/2p\mathbb{Z}$ ou $G \simeq D_p$. En effet, le théorème de CAUCHY affirme l'existence de $x, y \in G$ d'ordre respectifs 2 et p. Alors $\langle x \rangle \cap \langle y \rangle = \{e\}$ car l'ordre de $\langle x \rangle \cap \langle y \rangle$ divise à la fois 2 et p. Par conséquent, on a $x \notin \langle y \rangle$ et $[G : \langle y \rangle] = 2$, donc la partition suivant les orbites donne

$$G = \langle x \rangle \sqcup \langle y \rangle x.$$

Puisque $\langle y \rangle \triangleleft G$, on a $xyx^{-1} = y^j$ avec $j \in [\![1, p-1]\!]$. En particulier, si $j = 1$, on trouve que G est abélien et, par suite, que $G \simeq \mathbb{Z}/2\pi\mathbb{Z}$ par la structure des groupes abéliens de types finis et le théorème chinois. Si $j = p - 1$, alors $G \simeq D_p$ par la caractérisation de D_p.

1.6 GROUPES SYMÉTRIQUES

DÉFINITION 1.54. Soit $n \in \mathbb{N}^*$. On appelle groupe symétrique d'ordre n l'ensemble des bijections de $[\![1, n]\!]$ dans lui-même. On le note $\mathfrak{S}_n$.

NOTATION. Une permutation $\sigma \in \mathfrak{S}_n$ sera notée

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}.$$

1.6.1 Signature

DÉFINITION 1.55. La signature d'une permutation $\sigma \in \mathfrak{S}_n$ est l'entier

$$\epsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Définition-proposition 1.56. La signature définit une morphisme $\epsilon\colon \mathfrak{S}_n \to (\{\pm 1\}, \times)$. On note $\mathfrak{A}_n$ son noyau, appelé groupe alterné.

Preuve Comme $\epsilon(\mathfrak{S}_n) < \mathbb{Q}^\times$, il suffit de montrer que $\epsilon\colon \mathfrak{S}_n \to \mathbb{Q}^\times$ est bien un morphisme. Soient $\sigma, \tau \in \mathfrak{S}_n$. On a

$$\begin{aligned}\epsilon(\sigma\tau) &= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j-i} \\ &= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)} \frac{\tau(j)-\tau(i)}{j-i} \\ &= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j)-\tau(i)} \epsilon(\tau) \\ &= \prod_{1\leqslant i<j\leqslant n} \frac{\sigma(j) - \sigma(i)}{j-i} \epsilon(\tau) = \epsilon(\sigma)\epsilon(\tau)\end{aligned}$$

car l'application τ est une bijection. □

1.6.2 Décomposition en produit de cycles

Définition 1.57. Soit $\sigma \in \mathfrak{S}_n$. On note

$$\operatorname{supp}(\sigma) \coloneqq \{i \in [\![1,n]\!] \mid \sigma(i) \neq i\},$$

appelé support de σ.

Définition 1.58. Soit $k \in [\![1,n]\!]$. On appelle k-cycle toute permutation $\sigma \in \mathfrak{S}_n$ telle que, en notant

$$\operatorname{supp}(\sigma) = \{a_1, \dots, a_k\},$$

on ait

$$\sigma(a_k) = a_1 \quad \text{et} \quad \forall i \in [\![1, k-1]\!], \quad \sigma(a_i) = a_{i+1}.$$

On le note alors $\sigma = (a_1\ a_2\ \cdots\ a_k)$. Une transposition est un 2-cycle.

◇ Remarques. – Pour toute $\sigma \in \mathfrak{S}_n$, on a $\sigma \circ (a_1\ \cdots\ a_k) \circ \sigma^{-1} = (\sigma(a_1)\ \cdots\ \sigma(a_k))$. Par suite, tous les k-cycles sont conjugués.

– Un k-cycle est d'ordre k.

– On a $(a_1\ \cdots\ a_k) = (a_1\ a_k) \circ \cdots \circ (a_2\ a_3) \circ (a_1\ a_2)$.

– Soit τ une transposition. Alors $\epsilon(\tau) = -1$. Si $n \geqslant 2$, l'application $\varepsilon\colon \mathfrak{S}_n \to \{\pm 1\}$ est surjective et $|\mathfrak{A}_n| = n!/2$. En effet, on a $\epsilon(1\ 2) = -1$ et on exploite la première remarque.

– Comme ε est un morphisme et par la deuxième remarque, on a $\varepsilon(a_1\ \cdots\ a_k) = (-1)^{k-1}$.

– Si $n \geqslant 3$, alors le groupe D_n s'injecte dans $\mathfrak{S}_n$ en numérotant les sommets du polygone de 1 à n. Cette application $\rho\colon D_n \to \mathfrak{S}_n$ injective définit une action de D_n dans $[\![1,n]\!]$.

Proposition 1.59. Soient $\sigma, \tau \in \mathfrak{S}_n$ telles que $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \emptyset$. Alors $\sigma\tau = \tau\sigma$.

Lemme 1.60. Soit $\sigma \in \mathfrak{S}_n$. Alors $\sigma(\operatorname{supp}(\sigma)) = \operatorname{supp}(\sigma)$. S'il existe $\sigma_1, \dots, \sigma_\ell \in \mathfrak{S}_n$ dont les supports sont deux à deux disjoints telles que $\sigma = \sigma_1 \cdots \sigma_\ell$, alors

$$\operatorname{supp}(\sigma) = \bigsqcup_{i=1}^{\ell} \operatorname{supp}(\sigma_i).$$

En particulier, on a $\sigma = \mathrm{Id}$ si et seulement si $\sigma_i = \mathrm{Id}$ pour tout $i \in [\![1, \ell]\!]$

Preuve de la proposition Soit $i \in [\![1,n]\!]$. Si $i \notin \operatorname{supp}(\tau) \cup \operatorname{supp}(\sigma)$, alors $\sigma(i) = \tau(i) = i$, donc $\sigma\tau(i) = \tau\sigma(i) = i$. Si $i \in \operatorname{supp}(\sigma)$, alors $\tau(i) = i$ et le lemme donne $\sigma(i) \in \operatorname{supp}(\sigma)$, donc $\tau\sigma(i) = \tau(i) = \sigma(\tau(i))$. De même pour $i \in \operatorname{supp}(\tau)$. □

Théorème 1.61. Toute permutation $\sigma \in \mathfrak{S}_n \setminus \{\mathrm{Id}\}$ s'écrit sous la forme $\sigma = c_1 \cdots c_k$ où les c_i sont des cycles à supports disjoints. De plus, cette décomposition est unique à l'ordre près des facteurs et

$$\mathrm{o}(\sigma) = \operatorname{ppcm}(\ell(c_1), \dots, \ell(c_k))$$

où $\ell(c)$ désigne la longueur d'un cycle c.

Preuve On regarde l'action du groupe $\langle\sigma\rangle$ sur $X \coloneqq [\![1,n]\!]$. On peut alors décomposer G en orbites

$$X = \bigsqcup_{i=1}^{r} O_i.$$

Pour $i \in [\![1,r]\!]$, on note $a_i \coloneqq \sharp O_i$ et $\sigma_i \in \mathfrak{S}_n$ telle que

$$\forall x \in X, \quad \sigma_i(x) = \begin{cases} x & \text{si } x \notin O_i, \\ \sigma(x) & \text{sinon.} \end{cases}.$$

En particulier, on a $\sigma = \mathrm{Id} \Leftrightarrow \sharp O_i = 1$. Si $\sigma_i \neq \mathrm{Id}$, alors on peut l'écrire sous la forme $(\alpha_i\ \sigma(\alpha_i)\ \cdots\ \sigma^{a_i-1}(\alpha_i))$ où $\alpha_i \in O_i$. D'après la partition en orbites, on obtient que $\sigma = \sigma_1 \cdots \sigma_r = \sigma_{i_1} \cdots \sigma_{i_k}$ où les entiers i_j sont tels que les orbites O_{i_j} soient de cardinaux supérieurs ou égaux à 2. Pour $j \in [\![1,k]\!]$, on pose alors $c_j \coloneqq \sigma_{i_k}$.

Montrons l'unicité. On se donne une décomposition $\sigma = c_1 \cdots c_N$. Soient $i \in [\![1,n]\!]$ et $j \in [\![1,N]\!]$ tel que $i \in \operatorname{supp} c_j$. Puisque $c_j(\operatorname{supp} c_j) = \operatorname{supp} c_j$, on a $\sigma(i) = c_j(i)$. Finalement, on a $\sigma(\operatorname{supp} c_j) = \operatorname{supp} c_j$. Ainsi les supports $\operatorname{supp} c_j$ sont les orbites de cardinaux supérieur à 2 sous l'action de $\langle\sigma\rangle$ et ils sont déterminés de façon unique.

Déterminons son ordre. Soit $\ell \in \mathbb{N}^*$. On a $\sigma^\ell = c_1^\ell \cdots c_k^\ell$, donc $\sigma^\ell = \mathrm{Id}$ si et seulement si $c_i^\ell = \mathrm{Id}$ pour tout $i \in [\![1,k]\!]$ par le lemme et le fait que $\operatorname{supp} c_i^\ell \subset \operatorname{supp} c_i$. Comme $\mathrm{o}(c_i) = \ell(c_i)$ pour tout $i \in [\![1,k]\!]$, le plus petit entier ℓ qui vérifie cela est bien $\operatorname{ppcm}(\ell(c_1), \ldots, \ell(c_k))$. □

▷ Exemple. La permutation

$$\sigma \coloneqq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix}$$

se décompose en produit de transpositions

$$\sigma = (1\ 3\ 4\ 5) \circ (2\ 6\ 8).$$

Corollaire 1.62. Le groupe $\mathfrak{S}_n$ est engendré par les cycles ou par les transpositions.

Corollaire 1.63. Le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles.

Preuve On pose H le sous-groupe engendré par les 3-cycles. Il suffit de montrer que $H \ni \tau_1\tau_2$ où τ_1 et τ_2 sont deux transpositions. Si $\operatorname{supp}\tau_1 = \operatorname{supp}\tau_2$, alors $\tau_1 = \tau_2$, donc $\tau_1\tau_2 = \mathrm{Id} \in H$. Si $|\operatorname{supp}\tau_1 \cap \operatorname{supp}\tau_2| = 1$, alors on note $\tau_1 = (a\ b)$ et $\tau_2 = (a\ c)$, donc $\tau_1\tau_2 = (a\ c\ b) \in H$. Si $\operatorname{supp}\tau_1 \cap \operatorname{supp}\tau_2 = \emptyset$, alors on note $\tau_1 = (a\ b)$ et $\tau_2 = (c\ d)$, donc $\tau_1\tau_2 = (a\ b)(c\ d)$ et on se ramène au cas précédent. □

Théorème 1.64. Deux permutations de $\mathfrak{S}_n$ différentes de l'identité sont conjugués si et seulement si, pour tout $k \in [\![2,n]\!]$, elles ont le même nombre de k-cycle dans leur décomposition.

Preuve On rappel les faits suivants. Soient $c \coloneqq (a_1\ \cdots\ a_p)$ et c' deux permutations conjugués. Alors il existe $\sigma \in \mathfrak{S}_n$ tel que $c' = \sigma c \sigma^{-1} = (\sigma(a_1)\ \cdots\ \sigma(a_p))$. Alors σ' est un p-cycle vérifiant $\operatorname{supp} c' = \sigma(\operatorname{supp} c)$ et c'est seulement déterminé par $\sigma_{|\operatorname{supp} c}$.

Soit $\tau \in \mathfrak{S}_n$. On la décompose en cycles $\tau = c_1 \cdots c_k$. Alors la décomposition d'une permutation conjuguées $\sigma \in \mathfrak{S}_n$ s'écrit $\sigma\tau\sigma^{-1} = (\sigma c_1 \sigma^{-1}) \cdots (\sigma c_k \sigma^{-1})$. Réciproquement, soient $\tau = c_1 \cdots c_k$ et $\tau' = c_1' \cdots c_k'$ avec $\ell(c_i) = \ell(c_i')$ pour tout $i \in [\![1,k]\!]$. On considère $\sigma \in \mathfrak{S}_n$ tel que $\sigma c_i \sigma^{-1} = c_i'$ pour tout $i \in [\![1,k]\!]$. Une telle permutation σ existe sachant que les supports des c_i sont disjoints, donc τ et τ' sont conjuguées. □

Proposition 1.65. Le nombre de classes de conjugaisons dans $\mathfrak{S}_n$ est

$$p(n) \coloneqq \sharp\Big\{(n_1, \ldots, n_\ell) \in \mathbb{N}^\ell \;\Big|\; \ell \in \mathbb{N},\ 1 \leqslant n_1 \leqslant \cdots \leqslant n_\ell \leqslant n,\ \sum_{i=1}^{\ell} n_i = n\Big\}.$$

▷ Exemple. On vérifie que $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$ et $p(5) = 7$.

1.6.3 Le groupe alterné

Proposition 1.66. Si $n \geqslant 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Preuve Soient $c \coloneqq (a\ b\ c)$ et c' deux 3-cycles. On sait qu'il existe $\sigma \in \mathfrak{S}_n$ tel que $\sigma c \sigma^{-1} = c' = (\sigma(a)\ \sigma(b)\ \sigma(c))$. Si $\sigma \in \mathfrak{A}_n$, la preuve est terminée. Sinon on considère $\tau = (e\ f)$ avec $e, f \notin \{a,b,c\}$ (c'est possible car $n \geqslant 5$). Alors $\sigma\tau \in \mathfrak{A}_n$ et $(\sigma\tau)c(\sigma\tau)^{-1} = (\sigma\tau(a)\ \sigma\tau(b)\ \sigma\tau(c)) = (\sigma(a)\ \sigma(b)\ \sigma(c)) = c'$, donc c et c' sont conjugués. □

La proposition suivante donne des propriétés sur le centre et le groupe dérivée de $\mathfrak{A}_n$ et de $\mathfrak{S}_n$.

Proposition 1.67. 1. Si $n \geqslant 3$, on a $\mathrm{Z}(\mathfrak{S}_n) = \{\mathrm{Id}\}$ et, si $n \geqslant 4$, on a $\mathrm{Z}(\mathfrak{A}_n) = \{\mathrm{Id}\}$.
2. Si $n \geqslant 1$, on a $\mathrm{D}(\mathfrak{S}_n) = \mathfrak{A}_n$.
3. Si $n \geqslant 5$, on a $\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$.

◇ Remarques. Pour $n = 2$, on a $\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$, donc $\mathrm{Z}(\mathfrak{S}_2) = \mathfrak{S}_2$. Pour $n \geqslant 4$ ou $n \in \{1, 2\}$, on a $\mathrm{Z}(\mathfrak{A}_n) = \{\mathrm{Id}\}$. Pour $n = 3$, on a $\mathfrak{A}_3 = \langle (1\ 2\ 3) \rangle$, donc $\mathrm{Z}(\mathfrak{A}_3) = \mathfrak{A}_3$. Calculons $\mathrm{D}(\mathfrak{A}_4)$. On remarque que

$$V_4 \coloneqq \{\mathrm{Id}, (1\ 2)(3\ 4), (2\ 3)(1\ 4), (1\ 3)(2\ 4)\}$$

est un sous-groupe de $\mathfrak{S}_4$. De plus, celui-ci est formé de deux classes de conjugaison dans $\mathfrak{S}_4$, donc $V_4 \triangleleft \mathfrak{S}_4$. En remarquant que $V_4 < \mathfrak{A}_4$, on a $V_4 \triangleleft \mathfrak{A}_4$. On a $V_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2$, donc $\mathfrak{A}_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$ est abélien. On en déduit que $\mathrm{D}(\mathfrak{A}_4) < V_4$. Montrons qu'il y en fait égalité. Il suffit de remarquer que $(1\ 2)(3\ 4) = [(1\ 2\ 3), (1\ 2\ 4)]$ et de même pour les autres, donc $V_4 = \mathrm{D}(\mathfrak{A}_4)$.

Preuve 1. Soit $n \geqslant 3$. Soit $\sigma \in \mathfrak{S}_n - \{\mathrm{Id}\}$. Il existe $i, j \in [\![1, n]\!]$ tels que $i \neq j$ et $\sigma(i) = j$. Comme $n \geqslant 3$, soit $k \in [\![1, n]\!] - \{i, j\}$. On considère $\tau \coloneqq (j\ k)$. On a alors $\sigma\tau(i) = j$ et $\tau\sigma(i) = k$.

Soit $n \geqslant 4$. On considère $\tau \coloneqq (j\ k\ \ell)$ avec $k, \ell \notin \{i, j\}$ et on montre de même que $\sigma\tau \neq \tau\sigma$ pour $\sigma \in \mathfrak{A}_n$.

2 et 3. Remarquons que $\mathrm{D}(\mathfrak{S}_n) < \mathfrak{A}_n$ car, pour tous $\sigma, \tau \in \mathfrak{S}_n$, on a $\epsilon([\sigma, \tau]) = [\epsilon(\sigma), \epsilon(\tau)] = 1$. On peut supposer que $n \geqslant 3$. Soit $c \coloneqq (a\ b\ c)$ un 3-cycle. Alors $c^2 = (a\ c\ b)$, donc il existe $_sigma \in \mathfrak{S}_n$ tel que $c^2 = \sigma c \sigma^{-1}$, *i. e.* $c = [\sigma, c]$. De plus, on peut choisir $\sigma \in \mathfrak{A}_n$ si $n \geqslant 5$ et donc $c \in \mathrm{D}(\mathfrak{A}_n)$. On conclut en utilisant le fait que les 3-cycles engendrent $\mathfrak{A}_n$. □

Définition 1.68. On dira qu'un groupe non nul G est *simple* si $\{e\}$ et G sont les seuls sous-groupes distingués dans G.

Exercice 1.4. Soit G un groupe abélien. Montrer que G est simple si et seulement si $G \simeq \mathbb{Z}/p\mathbb{Z}$ avec p premiers.

Théorème 1.69 *(Galois).* Pour $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est simple.

◇ Remarque. Il n'existe pas de groupes simples non abélien de cardinal strictement inférieur à $60 = |\mathfrak{A}_5|$. Le groupe $\mathfrak{A}_5$ est le seul groupe simple abélien d'ordre 60. Le suivant sur la liste est $\mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ qui est d'ordre 168.

Preuve Soit $n \geqslant 5$. Soit N un sus-groupe distingué non nul dans $\mathfrak{A}_n$. Montrons que $N = \mathfrak{A}_n$. C'est vrai si N contient un 3-cycles car les 3-cycles engendrent $\mathfrak{A}_n$ et ils sont conjugués dans $\mathfrak{A}_n$. On choisit $\sigma \in N - \{\mathrm{Id}\}$ tel que $L \coloneqq |\mathrm{supp}\,\sigma|$ soit minimal. Comme σ n'est ni l'identité ni une transposition, on a $L \geqslant 3$. Si σ_0 est un 3-cycle, c'est fini. Sinon on suppose que ce n'est pas un 3-cycle. On va exhiber $\sigma_2 \in N - \{\mathrm{Id}\}$ avec $\mathrm{supp}\,\sigma_2 \subsetneq \mathrm{supp}\,\sigma_0$. On décompose $\sigma_0 = c_1 \cdots c_k$ en cycles à supports disjoints. On peut supposer que $\ell(c_1)$ est maximale parmi les $\ell(c_i)$. On a alors deux cas :

– On suppose que $c_1 = (a_1\ \cdots\ a_\ell)$ avec $\ell \geqslant 3$. Si $k \geqslant \ell$, alors $|\mathrm{supp}\,\sigma_0| \geqslant 5$. Si $k = 1$, alors le cas $\ell = 3$ est clair et, si $\ell > 3$, on a $\ell \geqslant 5$ car $\sigma_0 \in \mathfrak{A}_n$. En conclusion, si σ_0 n'est pas un 3-cycle, alors $L \geqslant 5$. Alors il existe $\gamma \coloneqq (a_3\ a\ b)$ un 3-cycle tel que $a, b \notin \mathrm{supp}\,\sigma_0 - \{a_2, a_3\}$. On pose alors $\sigma_1 \coloneqq \gamma\sigma_0\gamma^{-1} \in N$. Alors $\sigma_1 \neq \sigma_0$ car $\sigma_1(a_2) = a$ et $\sigma_0(a_2) = a_3 \neq a$. On remarque que les points fixes de σ_0 sont fixes pour σ_1 et $\sigma_2 \coloneqq \sigma_1\sigma_0^{-1} \in N - \{\mathrm{Id}\}$, donc $\mathrm{supp}\,\sigma_2 \subset \mathrm{supp}\,\sigma_0$. Cette inclusion est stricte puisque $\sigma_2(a_2) = a_2$ avec $a_2 \in \mathrm{supp}\,\sigma_0$. Ceci est impossible.

– On suppose que chaque c_i est une transposition et donc $k \geqslant 2$. On note alors $\sigma_0 = (a_1\ a_2)(a_3\ a_4)\cdots$. On prend ici un 3-cycle $\gamma \coloneqq (a_3\ a_4\ f)$ avec $f \notin \{a_1, a_2, a_3, a_4\}$. On vérifie que $\sigma_1 = \gamma\sigma_0\gamma^{-1} \neq \sigma_0$ et, en considérant $\sigma_2 \coloneqq \sigma_1\sigma_0^{-1}$, on obtient que $\mathrm{supp}\,\sigma_2 - \{f\} \subset \mathrm{supp}\,\sigma_0$, mais on a $\sigma_2(a_1) = a_1$ et $\sigma_2(a_2) = a_2$ avec $a_1, a_2 \in \mathrm{supp}\,\sigma_0$, donc $\sharp\,\mathrm{supp}\,\sigma_2 \leqslant \sharp\,\mathrm{supp}\,\sigma_0 - 1$ ce qui est également impossible. □

Corollaire 1.70. Soient $n \geqslant 5$ et $N \triangleleft \mathfrak{S}_n$. Alors $N \in \{\{1\}, \mathfrak{A}_n, \mathfrak{S}_n\}$.

Preuve On note $G \coloneqq N \cap \mathfrak{A}_n \triangleleft \mathfrak{A}_n$. Par la simplicité de $\mathfrak{A}_n$, on a $G = \{1\}$ ou $G = \mathfrak{A}_n$. Si $G = \mathfrak{A}_n$, alors $N = \mathfrak{A}_n$ ou $N = \mathfrak{S}_n$ car $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$. Si $G = \{1\}$, alors $|N| = 1$ ou $|N| = 2$ car $\epsilon\colon N \to \{\pm 1\}$ est injectif. Si $|N| = 1$, alors $N = \{1\}$. Si $|N| = 2$, alors $N < \mathrm{Z}(\mathfrak{S}_n) = 1$ car $G \triangleleft \mathfrak{S}_n$ ce qui est impossible. □

1.7 Produit semi-direct

1.7.1 Produit direct

Définition-proposition 1.71. Soient N et Q deux groupes. La loi

$$\left|\begin{array}{l}(N\times Q)\times(N\times Q)\longrightarrow N\times Q,\\ \quad((n_1,q_1),(n_2,q_2))\longmapsto(n_1n_2,q_1,q_2)\end{array}\right.$$

définit une structure de groupe sur $N\times Q$. Avec les injections canoniques

$$\left|\begin{array}{l}N\longrightarrow N\times Q,\\ n\longmapsto(n,1_Q)\end{array}\right. \quad\text{et}\quad \left|\begin{array}{l}Q\longrightarrow N\times Q,\\ q\longmapsto(1_N,Q),\end{array}\right.$$

on vérifie que $N,Q\triangleleft N\times Q$ et que

$$\frac{N\times Q}{N}\simeq Q \quad\text{et}\quad \frac{N\times Q}{Q}\simeq N.$$

Proposition 1.72. Soient G un groupe et $N,Q\triangleleft G$. On suppose que $N\cap Q=\{1\}$ et $NQ=G$. Alors l'application

$$f\colon \left|\begin{array}{l}N\times Q\longrightarrow G,\\ (n,q)\longmapsto nq\end{array}\right.$$

est un isomorphisme.

Preuve Comme $N\cap Q=\{1\}$, l'application f est injective et, comme $\operatorname{Im} f=NQ=G$, elle est surjective.

Pour $n\in N$ et $q\in Q$. Comme $nqn^{-1}\in Q$ et $qn^{-1}q^{-1}\in Q$, on a $[n,q]=nqn^{-1}q^{-1}\in N\cap Q$, donc $[n,q]=1$. Montrons que c'est un morphisme. Pour $(n_1,q_1),(n_2,q_2)\in N\times Q$, on a

$$\begin{aligned}f((n_1,q_1)(n_2,q_2))&=f(n_1n_2,q_1q_2)\\&=n_1n_2q_1q_2\\&=n_1q_1n_2q_2\\&=f(n_1,q_1)f(n_2,q_2).\end{aligned}$$

□

1.7.2 Produit semi-direct

On veut étendre la notion de produit direct.

Définition 1.73. Soient N et Q deux groupes et α une action de Q sur N par automorphisme, *i. e.* un morphisme $\alpha\colon Q\to\operatorname{Aut}(N)$. Ceci permet de définir la loi $*_\alpha$ sur $N\times Q$ par

$$(n_1,q_1)*_\alpha(n_2,q_1)=(n_1(q_1\cdot n_2),q_1q_2)\quad\text{avec}\quad q\cdot n=\alpha(q)(n).$$

Le couple $(N\times Q,*_\alpha)$ est noté $N\rtimes_\alpha Q$, appelé produit semi direct de N et Q.

▷ Exemples. 1. Soient $N,Q<G$ tels que $N\triangleleft G$. Alors une action de Q sur N par automorphisme est donnée par $q\cdot n:=qnq^{-1}$ et on peut considérer $N\rtimes Q$.

2. Soient N et Q deux sous-groupes. Soit $\alpha\colon\mathbb{Q}\to\operatorname{Aut}(N)$ le morphisme triviale. On a un produit semi-direct.

3. On a un produit semi-direct $N\rtimes\operatorname{Aut}(N)$ en prenant $Q=\operatorname{Aut}(N)$ et $\alpha=\mathrm{Id}_N$ muni de la loi

$$(n,\varphi)*(n,\varphi')=(n\varphi(n'),\varphi\circ\varphi').$$

Proposition 1.74. L'ensemble $N\rtimes_\alpha Q$ est un groupe.

Preuve Montrons l'associativité. Pour $(n_1,q_1),(n_2,q_2),(n_3,q_3)\in N\times Q$, on a

$$\begin{aligned}[(n_1,q_1)*_\alpha(n_2,q_2)]*_\alpha(n_3,q_3)&=(n_1(q_1\cdot n_2),q_1q_2)*_\alpha(n_3,q_3)\\&=(n_1(q_1\cdot n_2)(q_1q_2\cdot n_3),q_1q_2q_3)\\&=(n_1q_1\cdot(n_2(q_2\cdot n_3)),q_1q_2q_3)\\&=(n_1,q_1)*_\alpha[(n_2,q_2)*_\alpha(n_3,q_3)].\end{aligned}$$

On vérifie que l'élément neutre est $(1_N,1_Q)$ et que le symétrique de (n,q) est $(q^{-1}\cdot n^{-1},q^{-1})$. □

◇ Remarque. Les applications

$$\left|\begin{array}{l}N\longrightarrow N\rtimes_\alpha Q,\\ n\longmapsto(n,1_Q)\end{array}\right. \quad\text{et}\quad \left|\begin{array}{l}Q\longrightarrow N\rtimes_\alpha Q,\\ q\longmapsto(1_N,Q)\end{array}\right.$$

sont des morphismes injectifs avec les identifications $N\triangleleft N\rtimes_\alpha Q$ et $(N\rtimes_\alpha Q)/N\simeq Q$. Dans la suite, on omettra le morphisme α en indice, mais il sera sous-entendue.

PROPOSITION 1.75. Soient G un groupe et $N, Q < G$ avec $N \triangleleft G$. On pose

$$\alpha\colon \left|\begin{array}{l} Q \longrightarrow \mathrm{Aut}(N), \\ q \longmapsto \alpha(q) \coloneqq \mathrm{int}_{q|N}\,. \end{array}\right.$$

On suppose que $N \cap Q = \{1\}$ et $NQ = G$. Alors l'application

$$f\colon \left|\begin{array}{l} N \rtimes_\alpha Q \longrightarrow G, \\ \quad (n,q) \longmapsto nq \end{array}\right.$$

est un isomorphisme.

Preuve Comme précédemment, c'est une bijection. Pour tous $(n_1,q_1),(n_2,q_2) \in N \times Q$, on a

$$\begin{aligned} f((n_1,q_1)(n_2,q_2)) &= f(n_1(q_1 \cdot n_2), q_1q_2) \\ &= f(n_1q_1n_2q_2^{-1}, q_1q_2) \\ &= n_1q_1n_2q_2^{-1}q_1q_2 \\ &= n_2q_1n_2q_2 = f(n_1,q_1)f(n_2,q_2). \end{aligned}$$

□

◇ REMARQUE. Si $N, Q < G$ et $N \triangleleft G$, alors $NQ < G$.

▷ EXEMPLES. – Soit $n \geqslant 2$. Dans $G \coloneqq \mathfrak{S}_n$, on pose $N \coloneqq \mathfrak{A}_n$ et $Q \coloneqq \langle\tau\rangle \simeq \mathbb{Z}/2\mathbb{Z}$ où τ est une transposition de $\mathfrak{S}_n$. On a $N \triangleleft \mathfrak{S}_n$ et $\mathfrak{S}_n = N \sqcup \tau N$. De plus, on a $\mathfrak{S}_n = NQ$ et $N \cap Q = \{\mathrm{Id}\}$. On a donc $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes \langle\tau\rangle \simeq \mathfrak{A}_n \times \mathbb{Z}/2\mathbb{Z}$ par l'action définie par $\overline{1} \cdot \sigma = \tau\sigma\tau^{-1}$ et $\overline{0} \cdot \sigma = \sigma$.
– Soit k un corps. On pose $G \coloneqq \mathrm{GL}_n(k)$. On a $G \simeq G \simeq N \rtimes Q \simeq \mathrm{SL}_n(k) \rtimes k^*$ avec $N \coloneqq \mathrm{SL}_n(k)$ et

$$Q \coloneqq \left\{ \begin{pmatrix} \ell & 0 \\ 0 & I_{n-1} \end{pmatrix} \;\middle|\; \ell \in k^* \right\}.$$

En effet, on a $N \triangleleft G$ et $N \cap Q = \{I_n\}$. Par ailleurs, si $g \in G$, on a

$$g \begin{pmatrix} (\det g)^{-1} & 0 \\ 0 & I_{n-1} \end{pmatrix} \in N,$$

donc $NQ = G$. L'ensemble k^* agit sur N par l'action définie par

$$\ell \cdot g = \begin{pmatrix} \ell & 0 \\ 0 & I_{n-1} \end{pmatrix} g \begin{pmatrix} \ell^{-1} & 0 \\ 0 & I_{n-1} \end{pmatrix}.$$

1.7.3 Le groupe $\mathfrak{S}_4$ comme produit semi-direct

RAPPEL. On a $V_4 \triangleleft \mathfrak{S}_4$ avec

$$V_4 \coloneqq \{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

On considère $\Sigma \coloneqq \{\sigma \in \mathfrak{S}_n \mid \sigma(4) = 4\}$. Alors $\Sigma \simeq \mathfrak{S}_3$. On a $\Sigma \cap V_4 = \{\mathrm{Id}\}$. Comme $|\Sigma| = 6$ et $|V_4| = 4$, du fait de l'intersection vide, on a $|\Sigma V_4| = 24$. On en déduit que $\Sigma V_4 = 24$. On a alors le produit semi-direct $\mathfrak{S}_4 \simeq V_4 \rtimes \Sigma$ où on considère l'action α de Σ sur V_4 par conjugaison. On remarque que

$$\alpha\colon \Sigma \to \mathrm{Aut}(V_4) \hookrightarrow \mathfrak{S}_4$$

est injectif (à vérifier). Réciproquement, si $\varphi \in \mathrm{Aut}(V_4)$, on a $\varphi(\mathrm{Id}) = \mathrm{Id}$. Donc l'action de $\mathrm{Aut}(V_4)$ sur V_4 induit une action de $\mathrm{Aut}(V_4)$ sur $\{a,b,c\}$. On a donc une morphisme injectif de $\mathrm{Aut}(V_4)$ dans $\mathfrak{S}_{\{a,b,c\}} \simeq \mathfrak{S}_3$, donc $\mathrm{Aut}(V_4) \simeq \mathfrak{S}_3$. Finalement, on a $\mathfrak{S}_4 \simeq V_4 \rtimes \mathrm{Aut}(V_4)$;

1.7.4 Critère d'isomorphisme du produit semi-direct

PROPOSITION 1.76. Soient N et Q deux groupes et $\alpha, \beta\colon Q \to \mathrm{Aut}(N)$. Alors $N \rtimes_\alpha Q \simeq N \rtimes_\beta Q$ si l'un des deux critères est vérifié :

(i) il existe $\varphi \in \mathrm{Aut}(Q)$ tel que $\alpha = \beta \circ \varphi$;

(ii) il existe $u \in \mathrm{Aut}(N)$ tel que, pour tout $q \in Q$, on ait $\alpha(q) = u \circ \beta(q) \circ u^{-1}$.

Preuve On suppose (i). Alors l'application

$$f\colon \left|\begin{array}{l} N \rtimes_\alpha Q \longrightarrow N \rtimes_\beta Q, \\ \quad (n,q) \longmapsto (n, \varphi(q)). \end{array}\right.$$

est une bijection et un morphisme. En effet, pour tous $(n_1,q_1),(n_2,q_2) \in N \times Q$, on a

$$f((n_1,q_1)(n_2,q_2)) = f(n_1\alpha(q_1)(n_2), q_1q_2)$$

$$\begin{aligned}&= (n_1\alpha(q_1)(n_2), \varphi(q_1q_2))\\ &= (n_1\beta\circ\varphi(q_1)(n_2), \varphi(q_1)\varphi(q_2))\\ &= (n_1, \varphi(q_1))(n_2, \varphi(q_2))\end{aligned}$$

ce qui montre que f est un morphisme. On montre ensuite que c'est une bijection ce qui montre l'isomorphie. Pour le point (ii), on considère l'application

$$f\colon \left|\begin{array}{l} N\rtimes_\alpha Q \longrightarrow N\rtimes_\beta Q,\\ \quad (n,q)\longmapsto (u(n),q).\end{array}\right.$$

□

Application. Soient $\alpha,\beta\colon Q\to \mathrm{Aut}(N)$ injectif de même image. Alors $N\rtimes_\alpha Q\simeq N\rtimes_\beta Q$.

Preuve Il suffit de remplir la condition (i) de la proposition précédente en posant $\varphi=\beta^{-1}\circ\alpha$ où β^{-1} est le morphisme réciproque de $\beta\colon Q\to \mathrm{Im}\,\beta=\mathrm{Im}\,\alpha$. □

1.7.5 Remarques finales

Si $G=N\rtimes Q$ avec $N\triangleleft G$, alors $G/N\simeq Q$. Réciproquement, si $N\triangleleft G$, alors on n'a pas nécessairement $G\simeq N\rtimes G/N$. En effet, il suffit de prendre $G=Q_8$ et $N=\mathrm{Z}(Q_8)\triangleleft Q_8$. Alors pour tout $H<Q_8$ tel que $|H|\neq 1$, on a $1\in H$, donc $H\cap N\neq\{1\}$, donc on n'aura jamais $Q_8\simeq \mathrm{Z}(Q_8)\rtimes H$ et, en particulier, avec $H=Q_8/\mathrm{Z}(Q_8)$. En revanche, le critère suivant est vraie.

Proposition 1.77. Soit $N\triangleleft G$. On note $\pi\colon G\to G/N$ la projection canonique. S'il existe $Q<G$ tel que $\pi\colon Q\to G/N$ soit un isomorphisme, alors $G\simeq N\rtimes Q$ où Q agit par conjugaison sur N.

Preuve Comme $\pi_{|Q}$ est injective, on a $N\cap Q=\{1\}$ et, comme elle est surjective, on a $G=NQ$. D'où le produit semi-direct. □

1.8 Théorème de Sylow

1.8.1 Préliminaires

On va décrire les groupes d'ordre inférieur ou égal à 11. Si G est un groupe finie, ce qu'on sait :

- si $p\coloneqq|G|$ est premier, alors $G\simeq\mathbb{Z}/p\mathbb{Z}$;
- si $|G|=2p$ est pair avec p premier, alors $G\simeq D_p$ ou $G\simeq\mathbb{Z}/2p\mathbb{Z}$;
- Si G est abélien, on peut écrire $G\simeq\prod_{i=1}^{\ell}\mathbb{Z}/m_i\mathbb{Z}$;
- si G est non abélien et $|G|=8$, alors soit $G\simeq D_4$ soit $G\simeq Q_8$;

Preuve Montrons ce dernier point. Comme $|G|=8$, il existe un élément y de G d'ordre 4. Soit $x\in G-\langle y\rangle$. Alors $\mathrm{o}(x)=2$ ou $\mathrm{o}(x)=4$. En notant $H\coloneqq\langle y\rangle$, on a $[G:H]=2$, donc $H\triangleleft G$. De plus, comme $G=H\sqcup Hx$, on a $G=\langle x,y\rangle$. L'élément y ou y^{-1} est un générateur de H et y^2 est l'unique élément d'ordre 2 dans H. Comme G est abélien, on a $xyx^{-1}=y^{-1}=y^3$. Si $\mathrm{o}(x)=2$, alors $G\simeq D_4$. Sinon on suppose que $\mathrm{o}(x)=4$. En posant $K\coloneqq\langle x\rangle$, on a $K\cap H\neq\{1\}$ car sinon on aurait $|KH|=|K|\,|H|=16$ ce qui est impossible. Donc $|H\cap K|=2$ et $x^2=y^2$. Finalement, on a $G=\langle x,y\rangle$ où $\mathrm{o}(x)=\mathrm{o}(y)=4$, $xyx^{-1}=y^3$ et $x^2=y^2$. Cela suffit pour dresser la table de

$$G\coloneqq\left\{1,y,y^2,y^2,x,yx,y^2x,y^2x\right\}$$

et, en identifiant x à I et y à J, on a $G\simeq Q_8$. □

On peut compléter ces résultats par la proposition suivant.

Propriété 1.78. Soit G un groupe tel que $G/\mathrm{Z}(G)$ soit monogène. Alors G est abélien.

Preuve On note $\pi\colon G\to G/\mathrm{Z}(G)$ la projection. Soit $a\in G$. Alors $\langle\pi(a)\rangle=G/\mathrm{Z}(G)$. Soient $x,y\in G$. Il existe $m,n\in\mathbb{Z}$ et $c,d\in\mathrm{Z}(G)$ tels que $x=a^nc$ et $y=a^md$, donc $[x,y]=[a^n,a^m]=1$. Donc le groupe G est abélien. □

Corollaire 1.79. Soient G un groupe tel que $|G|=p^2$ avec p premier. Alors G est abélien.

Preuve On sait que $\mathrm{Z}(G)\neq\{1\}$. Il existe $r\in\{1,2\}$ tel que $|\mathrm{Z}(G)|=p^r$. Si $r=2$, on a terminé. Si $r=1$, alors $G/\mathrm{Z}(G)\simeq\mathbb{Z}/p\mathbb{Z}$ et on peut appliquer la proposition. □

On obtient la classification suivant pour les groupes d'ordre inférieur à 11.

$\lvert G\rvert$	G à isomorphisme près
2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, D_3
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$, D_4, Q_8, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$
9	$\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^2$
10	$\mathbb{Z}/10\mathbb{Z}$, D_5
11	$\mathbb{Z}/11\mathbb{Z}$

1.8.2 Structure des p-groupes

PROPOSITION 1.80. Soit G un p-groupe. On note $|G| = p^n$. Alors

1. pour tout $r \in [\![0, n]\!]$, il existe un sous-groupe de G d'ordre p^r ;
2. pour tout $H < G$ tel que $[G : H] = p$, alors $H \triangleleft G$;
3. pour tout $K < G$ tel que $K \neq G$, il existe $H < G$ tel que $[G : H] = p$ et $K < H$.

Preuve Procédons par récurrence sur n. C'est vrai pour $n = 1$. Soit $n > 1$. Pour $N \triangleleft G$, on note $\pi_N : G \to G/N$ la projection canonique. Si $K < G/N$ et $H \coloneqq \pi_N^{-1}(K)$, alors $[G/N : K] = [G : H]$ où $K = H/N$ et, si $K \triangleleft G/N$, alors $H \triangleleft H$.

On suppose que les résultats vrais pour des groupes d'ordre inférieur ou égal à $n-1$. Montrons le point 1. Soit G un p-groupe tel que $|G| = p^n$. Alors il existe $m \in [\![1, n]\!]$ tel que $|\mathrm{Z}(G)| = p^m$. Par le théorème de CAUCHY, il existe $x \in \mathrm{Z}(G)$ tel que $\mathrm{o}(x) = p$. Comme $x \in \mathrm{Z}(G)$, on a $\langle x\rangle \triangleleft G$, donc le groupe $G/\langle x\rangle$ est d'ordre p^{n-1}. Par hypothèse de récurrence, pour tout $r \in [\![0, n-1]\!]$, il existe $K < G/\langle x\rangle$ tel que $|K| = p^r$ et donc $H = \pi_{\langle x\rangle}^{-1}(K)$ est d'ordre p^{r+1}.

Montrons le point 2. Soit $H < G$ d'indice p. On pose $K \coloneqq \mathrm{Z}(G)H < G$. On a $H < K < \mathrm{N}_G(H)$. Si $\mathrm{Z}(G) \not< H$, alors $H \not< K = G = \mathrm{N}_g(H)$ car $[G : H] = p$, donc $H \triangleleft G$. On suppose que $\mathrm{Z}(G) < h$. Le groupe $G/\mathrm{Z}(G)$ est un p-groupe d'ordre p^m avec $m < n$. Comme $\pi_{\mathrm{Z}(G)}^{-1}(\pi_{\mathrm{Z}(G)}(H)) = H$, on a $[G/\mathrm{Z}(G) : \pi_{\mathrm{Z}(G)}(H)] = p$ et on conclut par récurrence.

Montrons le point 3. Soit $K < G$ tel que $K \neq G$ et $K \neq \{1\}$. Si $K \triangleleft G$, on applique l'hypothèse de récurrence à G/K. Si $K > \mathrm{Z}(G)$, on applique l'hypothèse de récurrence au couple $(G/\mathrm{Z}(G), \pi_{\mathrm{Z}(G)}(K))$. Dans le cas général, on considère $K' \coloneqq \mathrm{Z}(G)K < \mathrm{N}_G(H)$. Si $K' = G$, alors $K \triangleleft G$. Sinon $K' > \mathrm{Z}(G)$ et on se ramène au cas précédent. □

1.8.3 Énonce des deux théorèmes de SYLOW

DÉFINITION 1.81. Soit G un groupe fini. On suppose que $|G| = p^r m$ où p est un nombre premier, $r > 0$ et $p \nmid m$. Un p-sous-groupe de SYLOW de G est un sous-groupe H de G d'ordre p^r. On note $\mathrm{Syl}_p(G)$ l'ensemble des p-groupes de SYLOW de G et $\mathrm{s}_p(G)$ son cardinal.

THÉORÈME 1.82 *(SYLOW).* Avec les notations précédentes, on a $\mathrm{s}_p(G) \geqslant 1$.

▷ EXEMPLE. On note $G \coloneqq \mathrm{GL}_n(\mathbb{F}_p)$ avec $\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$. Le cardinal de $|G|$ est le nombre de base du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p^n$ qui est

$$(p^n-1)(p^n-p)\cdots(p^n-p) = p^{n(n-1)/2}m \quad \text{avec} \quad m \coloneqq \prod_{i=1}^{d}(p^i-1)$$

avec $m \wedge p = 1$. On note

$$\mathrm{U}_n(\mathbb{F}_p) \coloneqq \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix} \right\} < G.$$

Alors $|\mathrm{U}_n(\mathbb{F}_p)| = p^{n(n-1)/2}$, donc $\mathrm{U}_n(\mathbb{F}_p) \in \mathrm{Syl}_p(G)$.

THÉORÈME 1.83 *(SYLOW).* Avec les notations précédentes,

1. deux p-sous-groupe de SYLOW de G sont conjugués dans G, *i. e.* pour tous $P_1, P_2 \in \mathrm{Syl}_p(G)$, il existe $g \in G$

tel que $P_1 = gP_2g^{-1}$;
2. on a $\mathrm{s}_p(G) \mid m$ et $\mathrm{s}_p(G) \equiv 1 \ \ [p]$;
3. tout p-sous-groupes de G est contenu dans un p-sous-groupe de Sylow de G.

On admet provisoirement ces deux théorèmes.

Corollaire 1.84. Soit G un groupe telle que $|G| = p^r m$ avec p premiers, $r > 0$ et $p \nmid m$. Alors
1. pour tout $r' \in [\![0, r]\!]$, il existe $H < G$ tel que $|H| = p^{r'}$;
2. pour tout $P \in \mathrm{Syl}_p(G)$, on a $P \triangleleft G$ si et seulement si $\mathrm{s}_p(G) = 1$.

◇ Remarque. Une action naturelle existe de G sur $\mathrm{Syl}_p(G)$ par conjugaison, définie par $g \cdot H \coloneqq gHg^{-1}$. D'après le point 1 du théorème 1.83, cette action est transitive. Soient $P, P' \in \mathrm{Syl}_p(G)$. On note $\mathrm{N}_G(P)$ le stabilisateur de P. Alors $\mathrm{s}_p(G) = |\mathrm{N}_G(P)| = |G|$. De plus, le groupe $\mathrm{N}_G(P)$ est conjugués à $\mathrm{N}_G(P')$.

1.8.4 Exemples et applications

(i) Critère de non simplicité

Ces théorèmes donnent un critère de non simplicité. Par exemple, un groupe d'ordre $99 = 3^2 \times 11$ n'est pas simple. En effet, on a $\mathrm{s}_3(G) \mid 11$ et $\mathrm{s}_3(G) \equiv 1 \ \ [3]$, donc $\mathrm{s}_3(G) = \{1\}$. Donc il existe un seul sous-groupe d'ordre 9 dans G et donc normal.

(ii) Description des p-Sylow

On considère les groupes $\mathfrak{S}_n$ avec $n \in \{3, 4, 5\}$. On suppose que $n = 3$. Alors $\mathfrak{A}_3$ est l'unique 3-Sylow. De plus, on a $\mathrm{s}_2(\mathfrak{S}_3) = 3$ car les sous-groupes $\langle \tau_i \rangle$ sont des 2-Sylow avec $\tau_1 = (1\ 2)$, $\tau_2 = (1\ 3)$ et $\tau_3 = (2\ 3)$.

On suppose que $n = 4$. Comme $|\mathfrak{S}_4| = 2^3 \times 3$, on a $\mathrm{s}_2(\mathfrak{S}_4) \mid 4$ et $\mathrm{s}_2(\mathfrak{S}_4) \equiv 1 \ \ [2]$, donc $\mathrm{s}_2(\mathfrak{S}_4) \in \{1, 3\}$. Par ailleurs, pour $P \in \mathrm{Syl}_2(\mathfrak{S}_4)$, on a $|P| = 8$ et $P \not\triangleleft \mathfrak{S}_4$ car sinon $\mathfrak{S}_4 / P \simeq \mathbb{Z}/3\mathbb{Z}$ est abélien et donc $\mathfrak{A}_4 = \mathrm{D}(\mathfrak{S}_4) < P$ ce qui est absurde. On en déduit que $\mathrm{s}_2(\mathfrak{S}_4) = 3$ et, par exemple, le groupe D_4 est un isomorphe à un groupe de $\mathrm{Syl}_2(\mathfrak{S}_4)$. Alors $|\mathrm{N}_{D_4}(\mathfrak{S}_4)|\, \mathrm{s}_2(\mathfrak{S}_4) = 24$, donc $|\mathrm{N}_{D_4}(\mathfrak{S}_4)| = 8$ et, puisque $D_4 < \mathrm{N}_{D_4}(\mathfrak{S}_4)$, on a $D_4 = \mathrm{N}_{D_4}(\mathfrak{S}_4)$. Par ailleurs, on a vu que $\mathrm{s}_3(\mathfrak{S}_4) = 4$.

On suppose que $n = 5$, On a $|\mathfrak{S}_5| = 2^3 \times 3 \times 5$. On a $\mathfrak{S}_5 > S_4 \coloneqq \{\sigma \in \mathfrak{S}_5 \mid \sigma(5) = 5\}$. Donc les 2 et 3-Sylows sont, à conjugaisons près, D_4 et $\langle (1\ 2\ 3) \rangle$. De plus, pour $\sigma \in \mathrm{N}_{D_4}(\mathfrak{S}_5)$, on a $\sigma(5) = 5$. On en déduit que $\mathrm{N}_{D_4}(\mathfrak{S}_4) = \mathrm{N}_{D_4}(\mathfrak{S}_5)$, donc $\mathrm{s}_2(\mathfrak{S}_5) = |\mathfrak{S}_5| / 8 = 15$. Il reste le cas des 5-Sylows. Les 5-Sylows sont les sous-groupes $\langle \sigma \rangle$ où σ est un 5-cycle. Il faut donc dénombrer le nombre de 5-cycles. On a donc $\mathrm{s}_5(\mathfrak{S}_6) = 4!/4 = 6$. En conséquence, pour tout $P \in \mathrm{Syl}_5(\mathfrak{S}_5)$, on a $|\mathrm{N}_P(\mathfrak{S}_5)| = 20$.

(iii) Classification des groupes d'ordre pq

Soit G un groupe d'ordre pq où p et q sont deux nombres premiers distincts tels que $p < q$. Les théorèmes donnent $\mathrm{s}_q(G) \mid p$ et $\mathrm{s}_q(G) \equiv 1 \mod q$, donc $\mathrm{s}_p(G) = 1$. Par suite, on a $G = N \rtimes H$ où $N \coloneqq \mathbb{Z}/q\mathbb{Z}$ et $H \coloneqq \mathbb{Z}/p\mathbb{Z}$ sont les uniques q et p-Sylow. Par ailleurs, on a $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) = \mathbb{Z}/(q-1)\mathbb{Z}$. Alors si $p \nmid q - 1$, on a

$$G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$$

et, si $p \mid q - 1$, on a

$$G \simeq \mathbb{Z}/pq\mathbb{Z} \quad \text{ou} \quad G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$$

où $\alpha \colon \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$ est le morphisme naturel.

1.8.5 Classification des groupes d'ordre 12

Soit G un groupe d'ordre $12 = 2^2 \times 3$. Distinguons deux cas.

1. On suppose que $\mathrm{s}_2(G) = 1$. Alors G peut s'écrire sous la forme $N \rtimes H$ où N est un 2-Sylow et H est un 3-Sylow. On peut avoir avoir (i) $N = \mathbb{Z}/4\mathbb{Z}$ ou (ii) $N = (\mathbb{Z}/2\mathbb{Z})^2$. Dans le premier cas (i), on aura

$$G \simeq \mathbb{Z}/4\mathbb{Z} \rtimes_\alpha \mathbb{Z}/3\mathbb{Z}$$

avec un morphisme $\alpha \colon \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \simeq (\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$ qui est nécessairement le morphisme trivial. Le théorème chinois donne alors

$$G \simeq \mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Dans le second cas (ii), on a

$$G \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\alpha \mathbb{Z}/3\mathbb{Z}.$$

Or $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})\simeq\mathfrak{S}_3$. Alors un morphisme $\alpha\colon\mathbb{Z}/3\mathbb{Z}\longrightarrow\mathfrak{S}_3$ est (ii.a) soit trivial (ii.b) soit $\operatorname{Ker}\alpha=\{0\}$ et $\operatorname{Im}\alpha=\langle(1\ 2\ 3)\rangle$. Dans cette première situation (ii.a), on a

$$G\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}.$$

Dans cette seconde situation (ii.b), on a

$$G\simeq(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})\rtimes_\alpha\mathbb{Z}/3\mathbb{Z}\simeq\mathfrak{A}_4$$

pour un morphisme non trivial α.

2. On suppose que $\mathrm{s}_3(G)=1$. Alors G peut s'écrire sous la forme $N\rtimes H$ où N est un 3-Sylow et H est un 2-Sylow. On a $N=\mathbb{Z}/3\mathbb{Z}$. Alors (i) soit $H=\mathbb{Z}/4\mathbb{Z}$ (ii) soit $H=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Dans ce premier cas (i), on a

$$G\simeq\mathbb{Z}/3\mathbb{Z}\rtimes_\alpha\mathbb{Z}/4\mathbb{Z}$$

avec un morphisme $\alpha\colon\mathbb{Z}/4\mathbb{Z}\longrightarrow\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})\simeq\mathbb{Z}/2\mathbb{Z}$. Soit α est trivial (voir précédemment), soit $\alpha(1)=1$. Dans le second cas (ii), on a

$$G\simeq\mathbb{Z}/3\mathbb{Z}\rtimes_\alpha(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})$$

avec un morphisme $\alpha\colon\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\longrightarrow\mathbb{Z}/2\mathbb{Z}$. Si α est non trivial, alors

$$G\simeq\mathfrak{S}_3\times\mathbb{Z}/2\mathbb{Z}.$$

En effet, dans $G'\coloneqq\mathbb{Z}/2\mathbb{Z}$, on a $\mathrm{s}_3(G')=1$, donc $\langle(1\ 2)\rangle\times\mathbb{Z}/2\mathbb{Z}\simeq(\mathbb{Z}/2\mathbb{Z})^2$ est un 2-Sylow et G' est non abélien.

Bilan. Pour les 5 premiers cas, on a au plus 5 classes d'isomorphisme deux à deux non isomorphes. À isomorphisme près, il y a donc 5 groupes d'ordre 12.

1.8.6 Preuve des deux théorèmes de Sylow

On considère un groupe G d'ordre p^rm où p est un nombre premier, $r>0$ et $p\nmid m$. Il faut montrer l'existence d'un p-Sylow. Pour cela, on admet provisoirement le lemme suivant.

Lemme 1.85. On a

$$p\nmid\binom{mp^r}{p^r}.$$

Preuve du premier théorème On note

$$\mathscr{X}\coloneqq\{X\subset G\mid|X|=p^r\}.$$

Remarquons que $|\mathscr{X}|=\binom{mp^r}{p^r}$. On considère l'action de G sur X par l'action $(g,X)\longmapsto g\cdot X\coloneqq gX$. Pour $X\in\mathscr{X}$, le groupe G_X agit alors sur X par l'action $(h,x)\longmapsto k\cdot x\coloneqq hx$. Pour $x\in X$, l'application

$$\varphi_x\colon\left|\begin{array}{l}G_X\longrightarrow X,\\ h\longmapsto hx\end{array}\right.$$

est injective, donc $|G_X|\leqslant p^r$. Choisissons un bon ensemble $X\in\mathscr{X}$ de sorte que $|G_X|=p^r$. Soit $(X_1,\dots,X_n)$ un famille de $\mathscr{X}$ de représentants des orbites de l'action de G sur X. L'équation aux classes donne

$$|\mathscr{X}|=\sum_{i=1}^n|G\cdot X_i|.$$

Le lemme affirme l'existence d'un indice $i_0\in[\![1,n]\!]$ tel que $p\nmid|G\cdot X_{i_0}|$. Puisque $|G\cdot X_{i_0}|=|G|/|G_{X_{i_0}}|$, on a $|G_{X_{i_0}}|\geqslant p^r$. Finalement, on a $|G_{X_{i_0}}|=p^r$ et le groupe $G_{X_{i_0}}$ est bien un p-Sylow. □

Preuve du lemme On a

$$\binom{mp^r}{p^r}=\frac{(mp^r)!}{(p^r)([m-1]p^r)!}=\prod_{j=1}^{p^r-1}\frac{mp^r-j}{p^r-j}.$$

Pour tout $j\in[\![1,p^r-1]\!]$, les entiers mp^r-j et p^r-j sont divisibles par la même puissance de p, donc le quotient $(mp^r-j)/(p^r-j)$ n'est pas divisible par p ce qui donne le lemme. □

Montrons maintenant le second théorème de Sylow. La preuve repose sur une application du second théorème d'isomorphisme.

THÉORÈME 1.86. Soient G un groupe et N et H deux sous-groupes de G tels que $N \triangleleft G$. Alors
1. NH est un sous-groupe de G ;
2. $H/(H \cap N) \simeq (NH)/N$

Preuve Montrons le point 1. On a bien $e \in NH$. Soient $x \coloneqq nk \in NH$ et $y \coloneqq n'h' \in NH$. On a

$$xy^{-1} = nhh'^{-1}n'^{-1} = nhh'^{-1}n'^{-1}(hh'^{-1})^{-1}hh'^{-1} \in NH$$

puisque, comme N est distingué, on a $hh'^{-1}n'^{-1}(hh'^{-1})^{-1} \in N$.

Il existe un morphisme naturel

$$\varphi\colon H \xhookrightarrow{i} NH \xrightarrow{\pi} NH/N.$$

Il est surjectif puisque, pour tous $n \in N$ et $h \in H$, on a $\pi(h) = \pi(nh)$. De plus, on a $\operatorname{Ker}\varphi = H \cap N$. On conclut alors par le premier théorème d'isomorphisme. □

COROLLAIRE 1.87. Soit $P \in \mathrm{Syl}_p(G)$ et $H < G$ un p-sous-groupe tel que $H < \mathrm{N}_G(P)$. Alors $H < P$

Preuve Comme P et H sont des sous-groupes de $\mathrm{N}_G(P)$ et $P \triangleleft \mathrm{N}_G(P)$, le second théorème d'isomorphisme donne

$$H/(P \cap H) \simeq (PH)/P.$$

Le groupe $H/(P \cap H)$ est un p-groupe. Comme P est un p-Sylow, on en déduit que PH est un p-sous-groupe et $P < PH$, donc $P = PH$ et donc $H < P$. □

Preuve du second théorème Le groupe G agit sur $\mathrm{Syl}_p(G)$ par conjugaison par l'action $(g, P) \longmapsto g \cdot P \coloneqq gPg^{-1}$. Soit $P_0 \in \mathrm{Syl}_p(G)$. On considère $\mathscr{O} \coloneqq G \cdot P_0$. Alors on a une action induit de $H < G$ sur $\mathscr{O}$ par conjugaison. Si H est un p-sous-groupe, alors l'équation aux classes s'écrit

$$|\mathscr{O}| \equiv |\mathscr{O}^H| \quad [p]\,.$$

Si on prend $H = P_0$ et $P \in \mathscr{O}$, alors $P \in \mathscr{O}^{P_0} \Leftrightarrow P_0 < \mathrm{N}_G(P) \Leftrightarrow P = P_0$ par le corollaire. On en déduit que $\mathscr{O}^{P_0} = \{P_0\}$. Ainsi par l'équation aux classes, on a donc $|\mathscr{O}| \equiv 1 \ [p]$. On en déduit que, pour tout p-sous-groupe H, on a $|\mathscr{O}^H| \equiv 1 \ [p]$ et, en particulier, on a $\mathscr{O}^H \neq \emptyset$, donc il existe $P \in \mathscr{O}$ tel que $H < \mathrm{N}_G(P)$. On en déduit les points 1 et 3 du second théorème. Par suite, on a $\mathscr{O} = \mathrm{Syl}_p(G)$ ce qui entraîne le point 2. □