Algèbre 1-GROUPES

David Harari

1. Généralités

1.1. Définitions, premières propriétés

Définition 1.1 Un *groupe* $(G, .)$ est la donnée d'un ensemble G et d'une loi interne (notée multiplicativement) $G \times G \to G$, $(x, y) \mapsto xy$ vérifiant :

1. . est associative : pour tous x, y, z de G, on a $(xy)z = x(yz)$.
2. . possède un élément neutre (nécessairement unique), noté e ou 1, i.e. : $xe = ex = x$ pour tout x de G.
3. Tout élément x admet un symétrique (qui est forcément unique), c'est-à-dire un élément x' tel que $xx' = x'x = e$. On note en général $x' = x^{-1}$ et on dit que x' est l'*inverse* de x.

Définition 1.2 On dit que G est *abélien* (ou *commutatif*) si on a de plus $xy = yx$ pour tous x, y de G. Dans ce cas on notera souvent $+$ la loi, 0 le neutre, et $-x$ le symétrique de x qu'on appelle alors l'*opposé* de x.

Remarques :

- Si $(G, +)$ est un groupe abélien, on peut noter $x - y$ pour $x + (-y) = (-x) + y$. On se gardera par contre bien d'utiliser une notation du genre "x/y" si G n'est pas abélien car on ne saurait pas si cela signifie xy^{-1} ou $y^{-1}x$.
- Ne pas oublier de vérifier les deux sens pour le neutre et le symétrique si on veut montrer que $(G, .)$ est un groupe.
- Si G et H sont deux groupes, l'ensemble $G \times H$ est muni ipso facto d'une structure de groupe définie par $(g, h).(g', h') := (gg', hh')$. Ceci se généralise immédiatement à une famille (pas forcément finie) de groupes. On dit que le groupe ainsi obtenu est le *produit direct* des groupes considérés.

Exemples :

1. Le groupe trivial $G = \{0\}$.

2. $(\mathbf{R}, +)$ et $(\mathbf{R}^*, \times)$ sont des groupes (mais pas $(\mathbf{R}, \times)$, car l'élément 0 n'a pas d'inverse).

   Il en va de même en remplaçant $\mathbf{R}$ par $\mathbf{C}$, ou encore par n'importe quel corps. [1]

3. $G = (\mathbf{Z}/n\mathbf{Z}, +)$, où $n \in \mathbf{N}^*$. Il est d'*ordre* (i.e. de cardinal) n.

4. Soient E un ensemble et $\mathcal{S}(E)$ l'ensemble des bijections de E dans E. Alors $\mathcal{S}(E)$, muni de la composition $\circ$ des applications, est un groupe. Quand $E = \{1, ..., n\}$, on note $\mathcal{S}_n$ pour $\mathcal{S}(E)$ et on appelle ce groupe le *groupe symétrique* sur n lettres (ou n éléments). Son ordre est $n!$, et il n'est pas abélien si $n \geq 3$.

5. Soit K un corps. Alors le groupe $\mathrm{GL}_n(K)$ des matrices inversibles (n, n) est un groupe (non abélien si $n \geq 2$) pour la multiplication.

Définition 1.3 Soient G et G' deux groupes. Une application $f : G \to G'$ est un *morphisme de groupes* si $f(xy) = f(x)f(y)$ pour tous x, y de G. Si f est de plus bijective, alors f^{-1} est aussi un morphisme et on dit que f est un *isomorphisme* de G sur G'. Un isomorphisme de G sur lui-même s'appelle un *automorphisme* de G.

Remarques :

- On dit parfois "homomorphisme" au lieu de morphisme.
- Si $f : G \to G'$ est un morphisme, alors $f(e_G) = e_{G'}$, et $f(x^{-1}) = f(x)^{-1}$ pour tout x de G.
- L'ensemble $\mathtt{Aut}\, G$ des automorphismes de G, muni de la composition $\circ$ des applications, est un groupe. Il peut être non commutatif même si G l'est [exercice : montrer que c'est le cas pour $G = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$].
- On notera parfois $G \simeq H$ pour "G est isomorphe à H."

[1] Par convention dans ce cours, un *corps* ("field" en anglais) désignera un anneau **commutatif** dans lequel tout élément non nul possède un inverse, contrairement à la terminologie (qu'on rencontre parfois en français) dans laquelle on parle de corps commutatifs ou non commutatifs.

Exemples.

1. Si $a \in \mathbf{R}$, alors $x \mapsto ax$ est un morphisme de $(\mathbf{R}, +)$ dans lui-même. C'est un isomorphisme si $a \neq 0$, et on a l'analogue en remplaçant $\mathbf{R}$ par n'importe quel corps commutatif.

2. L'application $z \mapsto \exp z$ est un morphisme, surjectif mais non injectif, de $(\mathbf{C}, +)$ dans $(\mathbf{C}^*, \times)$.

3. Si G est un groupe et $a \in G$, l'application $x \mapsto ax$ ("translation à gauche") est une bijection de G dans G, mais (sauf cas triviaux) ce n'est **pas** un morphisme.

4. Si G est abélien et $n \in \mathbf{N}^*$, alors l'application $x \mapsto x^n$ est un morphisme, mais en général cela ne marche pas si G n'est pas abélien. On notera aussi que pour tout groupe G, l'application $x \mapsto x^{-1}$ est un "anti-morphisme" de G dans G, i.e. on a $(xy)^{-1} = y^{-1}x^{-1}$. [2]

5. Si E est fini de cardinal n, on a $\mathcal{S}(E) \simeq \mathcal{S}_n$. Pour $n \geq 2$, il existe un unique morphisme non trivial ε de $\mathcal{S}_n$ vers $\{\pm 1\}$, la *signature*. En particulier la signature de toute transposition est -1.

6. Soit K un corps. Le déterminant est un morphisme de $\mathrm{GL}_n(K)$ dans K^*. Si E est un K-ev de dimension n, alors $\mathrm{GL}_n(K)$ est isomorphe au groupe $(\mathrm{GL}(E), \circ)$ des applications linéaires bijectives de E dans E.

Définition 1.4 Un sous-ensemble H d'un groupe G est un *sous-groupe* si il vérifie :

- $1 \in H$.
- Pour tous x, y de H, on a $xy \in H$.
- Pour tout x de H, on a $x^{-1} \in H$.

Il revient au même de dire que . est une loi de composition interne sur H qui en fait un groupe.

Pour vérifier que H est un sous-groupe, on peut aussi vérifier qu'il est non vide et que xy^{-1} reste dans H pour tous x, y de H, mais ce n'est pas plus simple en pratique.

[Exercice : Soient K un corps et G une partie de $M_n(K)$ telle que G soit un groupe pour la multiplication. G est-il un sous-groupe de $\mathrm{GL}_n(K)$?]

[2] En termes pompeux, c'est un morphisme de G vers G^{opp}, qui est par définition le groupe ayant même ensemble sous-jacent que G mais une loi définie par $x \bullet y = yx$.

Proposition 1.5 *Si $f : G \to H$ est un morphisme de groupes, alors l'image directe $f(G')$ d'un sous-groupe G' de G et l'image réciproque $f^{-1}(H')$ d'un sous-groupe H' de H sont des sous-groupes respectifs de H, G. En particulier le noyau* $\ker f := f^{-1}(\{e\})$ *est un sous-groupe de G et l'image* $\operatorname{Im} f := f(G)$ *est un sous-groupe de H. Le morphisme f est injectif si et seulement si son noyau est réduit à l'élément neutre.*

Exemples.

- Si $a \in \mathbf{R}$, alors $a\mathbf{Z}$ est un sous-groupe de $(\mathbf{R}, +)$ (tous ceux qui ne sont pas denses sont de cette forme).
- Les sous-groupes de $\mathbf{Z}$ sont les $n\mathbf{Z}$ avec $n \in \mathbf{N}$.
- Soit $n \geq 2$. Le noyau de la signature $\varepsilon : \mathcal{S}_n \to \{\pm 1\}$ est un sous-groupe de $\mathcal{S}_n$, le *groupe alterné* $\mathcal{A}_n$.
- Soit K un corps. Le noyau du déterminant $\mathrm{GL}_n(K) \to K^*$ est un sous-groupe de $\mathrm{GL}_n(K)$, appelé *groupe spécial linéaire*. On le note $\mathrm{SL}_n(K)$.
- Si $(G, +)$ est un groupe abélien et $n \in \mathbf{N}^*$, alors l'ensemble $G[n]$ des x de G qui vérifient $nx = 0$ est un sous-groupe de G, appelé *sous-groupe de n-torsion* (ici on a noté $nx := x + x + ... + x$, avec n termes dans la somme). Le groupe $G_{\mathrm{tors}} := \bigcup_{n \in \mathbf{N}^*} G[n]$ est également un sous-groupe [3] de G, appelé *sous-groupe de torsion* de G. Notons qu'il n'y a pas de bon analogue de cette notion si G n'est pas abélien.

  Par exemple le sous-groupe de torsion de $(\mathbf{R}, +)$ est $\{0\}$ (on a l'analogue pour tout corps **de caractéristique zéro**, mais pour un corps K de caractéristique $p > 0$, on a par définition $K[p] = K$). Celui de $(\mathbf{R}^*, \times)$ est $\{\pm 1\}$, celui de $\mathbf{C}^*$ est le groupe multiplicatif de toutes les racines de l'unité. Si G est un groupe abélien fini d'ordre n, on a $G[n] = G$, cas particulier du théorème de Lagrange que nous verrons plus loin.

1.2. Générateurs d'un groupe; groupes cycliques

Proposition 1.6 *Soient G un groupe et A une partie de G. Alors il existe un plus petit sous-groupe H de G contenant A. On l'appelle sous-groupe engendré par A et on le note $\langle A \rangle$.*

[3] Attention en général une réunion de sous-groupes n'est pas un sous-groupe; cela marche ici parce qu'un élément x qui vérifie $mx = 0$ ou $nx = 0$ vérifie $(mn)x = 0$.

Démonstration : Il suffit de prendre pour $\langle A \rangle$ l'intersection de tous les sous-groupes de G contenant A. On peut aussi décrire $\langle A \rangle$ comme l'ensemble des produits $x_1 ... x_n$, où chaque x_i vérifie : $x_i \in A$ ou $x_i^{-1} \in A$ (si A est vide on prend $\langle A \rangle = \{e\}$).

□

Définition 1.7 *Soient G un groupe et $g \in G$. L'ordre de g est le plus petit entier $n > 0$ (s'il existe) tel que $g^n = 1$. Si $g^n \neq 1$ pour tout $n > 0$, on dit que g est d'ordre infini.*

Proposition 1.8 *Soient G un groupe et $g \in G$. Si $\langle g \rangle$ est infini, il est isomorphe à $\mathbf{Z}$. S'il est de cardinal n, il est isomorphe à $\mathbf{Z}/n\mathbf{Z}$. Dans les deux cas, l'ordre de g est le cardinal de $\langle g \rangle$ dans $\mathbf{N}^* \cup \{\infty\}$.*

Démonstration : Supposons d'abord g d'ordre infini. Alors $\mathbf{Z} \to \langle g \rangle$, $m \mapsto g^m$ est un morphisme surjectif. Son noyau est trivial (car g est d'ordre infini, et $g^m = 1$ est équivalent à $g^{-m} = 1$ si m est un entier négatif) donc c'est un isomorphisme. Ainsi $\mathbf{Z}$ est isomorphe à $\langle g \rangle$.

Supposons maintenant g d'ordre $n \in \mathbf{N}^*$. Comme $g^n = 1$, l'application $\varphi : \mathbf{Z}/n\mathbf{Z} \to \langle g \rangle$, $\bar{m} \mapsto g^m$ est bien définie, et par définition de $\langle g \rangle$ c'est un morphisme surjectif. Soit $\bar{m}$ dans le noyau de φ, effectuons la division euclidienne $m = nq + r$ de m par n ($0 \leq r < n$). On obtient $g^r = 1$ d'où $r = 0$ par définition de l'ordre. Ainsi $\bar{m} = 0$ et φ est finalement un isomorphisme de $\mathbf{Z}/n\mathbf{Z}$ sur $\langle g \rangle$.

□

Définition 1.9 Un groupe est dit *monogène* s'il est engendré par un seul élément, *cyclique* s'il est de plus fini.

Ainsi un groupe monogène infini est isomorphe à $\mathbf{Z}$, un groupe cyclique à $\mathbf{Z}/n\mathbf{Z}$, où n est le cardinal du groupe.

[Exercice : si d divise n, $\mathbf{Z}/n\mathbf{Z}$ possède un et un seul sous-groupe d'ordre d.]

Exemples de groupes engendrés.

1. Le groupe $(\mathbf{Z}^n, +)$ est engendré par $(1, 0, ...0), (0, 1, ..., 0), ..., (0, ..., 0, 1)$.
2. Le groupe symétrique $\mathcal{S}_n$ est engendré par les transpositions.

3. Pour $n \geq 2$, le groupe orthogonal $O_n(\mathbf{R})$ est engendré par les *réflexions* (i.e. les symétries orthogonales par rapport à un hyperplan), et pour $n \geq 3$ le groupe spécial orthogonal $SO_n(\mathbf{R}) := O_n(\mathbf{R}) \cap \mathrm{SL}_n(\mathbf{R})$ est engendré par les *retournements* (i.e. les symétries orthogonales par rapport à un sous-espace de codimension 2).

[Exercice : $(\mathbf{Q}, +)$ n'est pas engendré par une partie finie.]

1.3. Sous-groupes distingués, groupes quotients.

Proposition 1.10 *Soient G un groupe et $g \in G$. Alors l'application* $\mathrm{int}\, g : G \to G$, $h \mapsto ghg^{-1}$ *est un automorphisme de G, appelé automorphisme intérieur associé à g. L'application $g \mapsto \mathrm{int}\, g$ est un morphisme de groupes de G dans* $(\mathtt{Aut}\, G, \circ)$.

Définition 1.11 Un sous-groupe H de G est dit *distingué* ou *normal* s'il est laissé stable par tout automorphisme intérieur, i.e. : pour tout g de G et tout h de H, on a $ghg^{-1} \in H$. On note alors $H \lhd G$.

Remarques :

- $H \lhd G$ se traduit aussi par $gHg^{-1} = H$ pour tout g de G (à partir de $gHg^{-1} \subset H$, changer g en g^{-1} et multiplier à gauche par g, à droite par g^{-1}).
- Si G est abélien, tout sous-groupe de G est distingué.
- $\{e\}$ et G sont toujours des sous-groupes distingués de G.
- Attention, la notion de sous-groupe distingué est relative (H est toujours distingué dans lui-même).

Proposition 1.12 *Si $f : G \to G'$ est un morphisme de groupes et si $H' \lhd G'$, alors $f^{-1}(H')$ est distingué dans G. En particulier* $\ker f$ *est distingué dans G. Si $H \lhd G$, alors $f(H)$ est distingué dans $f(G)$ (mais pas dans G' en général). L'intersection de deux sous-groupes distingués dans G est un sous-groupe distingué de G.*

Exemples

1. Soit $n \geq 2$. Alors $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$.
2. Si K est un corps commutatif, alors $\mathrm{SL}_n(K)$ est distingué dans $\mathrm{GL}_n(K)$.

3. Soient $n \geq 3$ et H le sous-groupe de $\mathcal{S}_n$ constitué de l'identité et d'une transposition $\tau = (a, b)$. Alors si $\sigma \in \mathcal{S}_n$, on a $\sigma\tau\sigma^{-1} = (\sigma(a), \sigma(b))$ donc H n'est pas distingué dans $\mathcal{S}_n$.

4. Soient G un groupe et Z le *centre* de G, i.e. l'ensemble des x de G qui vérifient $xy = yx$ pour tout y de G. Alors Z est le noyau du morphisme int : $G \to \mathtt{Aut}\, G$ donc $Z \lhd G$.

Attention, $\lhd$ n'est pas une relation transitive, on peut avoir $K \lhd H \lhd G$ et pas $K \lhd G$.

[Exercice : soit $V_4 \subset \mathcal{S}_4$ l'ensemble constitué de l'identité et des trois double-transpositions $(a, b)(c, d)$ avec $\{a, b, c, d\} = \{1, 2, 3, 4\}$. Alors V_4 est un sous-groupe distingué de $\mathcal{S}_4$, isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, et contenant des sous-groupes d'ordre 2 qui ne sont pas distingués dans $\mathcal{S}_4$.]

Définition 1.13 Un sous-groupe H de G est dit *caractéristique* si pour tout $\varphi \in \mathtt{Aut}\, G$, on a $\varphi(H) \subset H$ (dans ce cas on a en particulier $H \lhd G$).

Par exemple le centre Z de G est caractéristique dans G. D'autre part si K est caractéristique dans H et H dans G, alors K est caractéristique dans G.

Proposition 1.14 *Soit H un sous-groupe de G. Alors la relation $x \sim y$ si et seulement si $x^{-1}y \in H$ (resp. $xy^{-1} \in H$) est une relation d'équivalence sur G. L'ensemble quotient s'appelle ensemble des classes à gauche (resp. classes à droite) selon H, et est noté G/H (resp. $H \setminus G$). Ses éléments sont de la forme aH (resp. Ha) avec $a \in G$ (en particulier H est la classe de e).*

Démonstration : On le fait pour les classes à gauche. $x \sim x$ est clair. Si $x^{-1}y \in H$, alors $(x^{-1}y)^{-1} = y^{-1}x \in H$ d'où la symétrie. Si $x^{-1}y \in H$ et $y^{-1}z \in H$, alors $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$, d'où la transitivité.

Soit $a \in H$. Alors si $x \in aH$, on a $x = ay$ avec $y \in H$ d'où $a^{-1}x = y \in H$ et $x \sim a$. Réciproquement si $x \sim a$, on a $a^{-1}x \in H$ donc $x \in aH$. finalement la classe de a dans G/H est bien aH.

□

Corollaire 1.15 (Th. de Lagrange) *Si G est fini, l'ordre de tout sous-groupe de H de G divise l'ordre de G.*

En effet les classes à gauche constituent une partition de G et le cardinal de aH est le même que celui de H puisque les translations à gauche sont des bijections de G sur G.

Theorème 1.16 *Soient G un groupe et H un sous-groupe distingué de G. Alors :*

1. *Pour tout a de G, on a $aH = Ha$ d'où $G/H = H \setminus G$.*
2. *Il existe une unique structure de groupe sur G/H telle que la surjection canonique $p : G \to G/H$ (qui à tout a associe sa classe $\bar{a} = aH = Ha$) soit un morphisme de groupes. Le groupe G/H ainsi obtenu s'appelle le groupe quotient de G par H.*

Démonstration : 1. Par définition d'un sous-groupe distingué, on a les inclusions $aHa^{-1} \subset H$ et $a^{-1}Ha \subset H$ d'où on tire $aH \subset Ha$ et $Ha \subset aH$.

2. La loi sur G/H doit nécessairement être définie par $\bar{a}\bar{b} = \overline{ab}$. Montrons d'abord que cette loi est bien définie, i.e. que $\bar{a}\bar{b}$ ne dépend pas du choix des représentants a et b. Si $\bar{a} = \bar{a}'$ et $\bar{b} = \bar{b}'$, on peut d'après 1. écrire $a' = h_1 a$ et $b' = bh_2$ avec h_1, h_2 dans H, d'où $a'b' = h_1(ab)h_2$. Ainsi $a'b' \in H(abh_2) = (abh_2)H$ d'après 1., mais ce dernier ensemble n'est autre que $(ab)H$ vu que $h_2 \in H$. Finalement $a'b' \sim ab$, c'est ce qu'on voulait.

Le fait que l'on ait défini une loi de groupe résulte alors immédiatement de la surjectivité de p jointe à la formule $p(xy) = p(x)p(y)$ pour tous x, y de G.

□

Remarques :

- L'élément neutre de G/H est $\bar{e} = H$.
- Si G est abélien, on peut donc quotienter par n'importe quel sous-groupe, mais il est facile de voir que le théorème est toujours faux si H n'est pas distingué dans G ("G/H est juste un ensemble"), vu que la propriété voulue implique que H est le noyau du morphisme de groupes p.
- Le groupe $\mathbf{Z}/n\mathbf{Z}$ est le quotient de $\mathbf{Z}$ par le sous-groupe $n\mathbf{Z}$. [4]

[Exercice : trouver un groupe d'ordre 8 non abélien dont tous les sous-groupes sont distingués, cf. TD...]

Proposition 1.17 *Si G est un groupe fini et H un sous-groupe, alors on a $\#(G/H) = \#(H \setminus G) = \#G/\#H$. En particulier l'ordre du groupe quotient G/H (quand H est distingué) est le quotient des ordres de G et H.*

[4] Définition meilleure que celles qu'on rencontre parfois en classes préparatoires !

Démonstration : Cela résulte de ce que les classes à gauche (resp. à droite) forment une partition de G, et chacune a pour cardinal celui de H.

Remarque : Plus généralement G/H est en bijection avec $H \setminus G$ via $aH \mapsto Ha^{-1}$. Quand leur cardinal est fini, on dit que H est un sous-groupe *d'indice fini* de G, et on note $[G : H]$ ce cardinal.

Theorème 1.18 (Th. de factorisation) *Soit $f : G \to G'$ un morphisme de groupes. Alors il existe un unique morphisme de groupes $\tilde{f} : G/\ker f \to G'$ tel que $f = \tilde{f} \circ p$. De plus $\tilde{f}$ est injectif d'image* $\operatorname{Im} f$*, i.e. $G/\ker f \simeq \operatorname{Im} f$.*

Remarques :

- $G/\ker f$ est bien un groupe car on a vu que $\ker f$ était distingué dans G.
- Quand G est fini, on retrouve la formule $\#G = \#\ker f \#\operatorname{Im} f$.

Démonstration : Nécessairement $\tilde{f}$ doit être définie par $\tilde{f}(\bar{a}) = f(a)$, où $\bar{a}$ est la classe de a dans G/H. Cette définition a bien un sens car si $\bar{a} = \bar{b}$, alors $a = bn$ avec $n \in \ker f$, d'où $f(a) = f(b)f(n) = f(b)$. Si $\bar{a}$, $\bar{b}$ sont dans G/H, on a $\tilde{f}(\bar{a}\bar{b}) = \tilde{f}(\overline{ab}) = f(ab) = f(a)f(b) = \tilde{f}(\bar{a})\tilde{f}(\bar{b})$ donc $\tilde{f}$ est un morphisme. Par définition $f = \tilde{f} \circ p$ d'où $\operatorname{Im} f = \operatorname{Im} \tilde{f}$ par surjectivité de p. Enfin $\bar{a} \in \ker \tilde{f}$ signifie $a \in \ker f$, i.e. $\bar{a} = e_{G/H}$.

□

[Exercice : Soient G un groupe et H un sous-groupe distingué de G. alors les sous-groupes (resp. les sous-groupes distingués) de G/H sont les N/H avec N sous-groupe (resp. sous-groupe distingué) de G contenant H. Dans le cas $N \lhd G$, on a de plus $(G/H)/(N/H) \simeq G/N$. Autrement dit, dans G/H on obtient un sous-groupe si on diminue G et un quotient si on augmente H.]

1.4. Quelques compléments

On va d'abord voir l'importante notion de suite exacte :

Définition 1.19 On dit qu'une suite (finie ou infinie)

$$... \to G_i \to G_{i+1} \to G_{i+2} \to ...$$

est *exacte* (les G_i étant des groupes et les f_i des morphismes) si pour tout i, on a $\operatorname{Im} f_i = \ker f_{i+1}$. En particulier

$$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$

est une suite exacte (dite courte) si et seulement si on a les trois propriétés : i injective, p surjective, $\operatorname{Im} i = \ker p$. Dans ce cas, on a $G/N \simeq H$ via le théorème de factorisation, et on dit que G est une *extension* de H par N. [5]

Remarques :

- De même qu'on ne confondra pas sous-groupe et quotient, on ne confondra pas "sur-groupe" et extension.
- Quand tous les groupes sont abéliens et notés additivement, on écrira 0 au lieu de 1 dans une suite exacte courte.

Exemples.

1. Si K est un corps, alors la suite

   $$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \xrightarrow{\det} K^* \to 1$$

   est exacte.

2. Les suites

   $$1 \to SO_n(\mathbf{R}) \to O_n(\mathbf{R}) \xrightarrow{\det} \{\pm 1\} \to 1$$

   et

   $$1 \to SU_n(\mathbf{C}) \to U_n(\mathbf{C}) \xrightarrow{\det} S^1 \to 1$$

   sont exactes, où S^1 désigne le groupe multiplicatif des complexes de module 1.

3. Si $n \geq 2$, la suite

   $$1 \to \mathcal{A}_n \to \mathcal{S}_n \xrightarrow{\varepsilon} \{\pm 1\} \to 1$$

   est exacte.

4. Soit G un groupe de centre Z. Le groupe $(\operatorname{Int} G, \circ)$ des automorphismes intérieurs de G est isomorphe à G/Z via la suite exacte

   $$1 \to Z \to G \xrightarrow{\mathrm{int}} \mathrm{Int}G \to 1$$

[5] Certains auteurs, par exemple D. Perrin, disent plutôt extension de N par H.

[Exercices : -montrer que $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/4\mathbf{Z}$ sont tous deux des extensions de $\mathbf{Z}/2\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$.

-Si $n \geq 3$, le centre de $\mathcal{S}_n$ est réduit à l'identité. (Utiliser la formule $\sigma\tau\sigma^{-1} = (\sigma(a), \sigma(b))$ pour $\sigma \in \mathcal{S}_n$ et $\tau = (a, b)$ transposition).

-Si K est un corps, le centre de $\mathrm{GL}_n(K)$ est réduit au sous-groupe (isomorphe à K^*) des homothéties.]

Une notion importante est celle de sous-groupe dérivé :

Définition 1.20 Soit G un groupe, et x, y deux éléments de G. On appelle *commutateur* de x et y l'élément $[x, y] := xyx^{-1}y^{-1}$. Le sous-groupe *dérivé* de G est par définition le sous-groupe **engendré** par les commutateurs.[6] On le note $D(G)$.

L'intérêt de $D(G)$ résulte dans la proposition suivante :

Proposition 1.21 *Le sous-groupe $D(G)$ est caractéristique (en particulier distingué) dans G. Le quotient $G/D(G)$ est abélien, et $D(G)$ est le plus petit sous-groupe de G qui a cette propriété. On note $G^{\mathrm{ab}} := G/D(G)$ ("abélianisé" de G).*

L'abélianisé de G est donc le plus "grand quotient abélien" de G, au sens suivant : si G/H est un autre quotient abélien, alors G^{ab} est une extension de G/H.

Démonstration : Si φ est un automorphisme de G, alors on a $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ d'où $\varphi(D(G)) \subset D(G)$ et $D(G)$ est caractéristique. Si H est un sous-groupe tel que G/H soit abélien, alors on a $\overline{xyx^{-1}y^{-1}} = \bar{e}$ dans G/H pour tous x, y de G, donc $[x, y] \in H$; ainsi H contient $D(G)$ puisqu'il contient tous les commutateurs.

□

Par exemple $D(G) = \{e\}$ si et seulement si G est abélien et $D(\mathcal{S}_3) = \mathcal{A}_3$. On verra plus tard que pour $n \geq 3$, on a $D(\mathcal{S}_n) = \mathcal{A}_n$ donc $\mathcal{S}_n^{\mathrm{ab}} \simeq \mathbf{Z}/2\mathbf{Z}$.

Définition 1.22 Un groupe G est dit *simple* si ses seuls sous-groupes distingués sont G et $\{e\}$, *parfait* si $D(G) = G$.

Par exemple un groupe abélien est simple si et seulement s'il est isomorphe à $\mathbf{Z}/p\mathbf{Z}$ avec p premier, et un groupe simple non abélien est parfait. On verra que $\mathcal{A}_n$ est simple si $n \geq 5$, et $\mathrm{SL}_n(K)$ est parfait si $n \geq 3$.

[6] Attention l'ensemble des commutateurs ne forme en général pas un sous-groupe, bien qu'il soit assez difficile de construire un contre-exemple.

2. Groupes opérant sur un ensemble

2.1. Généralités, premiers exemples

Définition 2.1 Soit G un groupe et X un ensemble. On dit que G *opère* (ou agit) sur X si on s'est donné une application $G \times X \to X$, $(g, x) \mapsto g.x$, vérifiant

- Pour tous g, g' de G et tout x de X, on a $g.(g'.x) = (gg').x$
- Pour tout x de X, on a $1.x = x$

Remarques :

- On a en particulier pour tout g que $x \mapsto g.x$ est une bijection de X sur X, de réciproque $x \mapsto g^{-1}.x$. Une définition équivalente consiste à se donner un morphisme $\Phi : G \to (\mathcal{S}(X), \circ)$, en posant $g.x = (\Phi(g))(x)$.
- La définition ci-dessus correspond à celle d'action à gauche. On peut également parler d'action à droite : $(g, x) \mapsto x.g$, satisfaisant $x.(gg') = (x.g).g'$. Cela correspond à se donner un anti-morphisme de G vers $\mathcal{S}(X)$ au lieu d'un morphisme.

Premiers exemples.

1. G opère sur lui-même par *translations à gauche* via $g.x := gx$. De même tout sous-groupe H de G opère sur G par translations à gauche.
2. G opère sur lui-même par conjugaison : $g.x := gxg^{-1}$. Ici l'image de G dans $\mathcal{S}(G)$ est de plus contenue dans $\texttt{Aut}\, G$ (ce qui n'était pas le cas dans l'exemple précédent).
3. $\mathcal{S}_n$ opère sur $\{1, ..., n\}$ par $\sigma.x = \sigma(x)$.
4. Si H est un sous-groupe de G, G opère sur l'ensemble des classes à gauche G/H par $g.(aH) = (ga)H$.

Définition 2.2 Étant donnée une opération d'un groupe G sur un ensemble X, on appelle :

- *orbite* d'un élément x de X l'ensemble des $g.x$, $g \in G$. Les orbites sont les classes d'équivalence sur X pour la relation : $x \sim y$ si et seulement s'il existe $g \in G$ tel que $y = g.x$. S'il n'y a qu'une orbite, on dit que G opère *transitivement* sur X.

- *stabilisateur* d'un élément x de X le sous-groupe H_x des g de G qui vérifient $g.x = x$. Il n'est pas distingué dans G en général. On dit que l'action est *fidèle* si le seul élément de G qui stabilise tous les éléments de X est e, *libre* si tous les stabilisateurs sont réduits à $\{e\}$ (c'est beaucoup plus fort).

Exemples.

1. Si H est un sous-groupe de G, l'action de H sur G par translation à gauche est libre, et les orbites ne sont autre que les classes à **droite** suivant H. Si G est fini d'ordre n, on obtient en particulier qu'il existe un morphisme injectif (l'opération de G sur lui-même) de G dans $\mathcal{S}(G) \simeq \mathcal{S}_n$ (théorème de Cayley).

2. L'action de $\mathcal{S}_n$ sur $\{1, ..., n\}$ est transitive, et tous les stabilisateurs sont isomorphes à $\mathcal{S}_{n-1}$.

3. L'action de G sur G/H vue plus haut est transitive. La proposition ci-dessous va montrer que c'est en quelque sorte le cas "générique" d'une action transitive.

Proposition 2.3 *Étant donnée une opération d'un groupe G sur un ensemble X et $x \in X$, on définit une bijection de l'ensemble des classes à gauche G/H_x sur l'orbite $\omega(x)$ de x via : $\bar{g} \mapsto g.x$. En particulier si G est fini on a $\#\omega(x) = \#G/\#H_x$ (donc le cardinal de $\omega(x)$ divise celui de G). Ainsi si l'action est transitive, l'action de G s'identifie à l'action de G sur G/H_x par translation à gauche.*

Démonstration : Déjà l'application $\varphi : \bar{g} \mapsto g.x$ de G/H_x vers X est bien définie car si $\bar{g} = \bar{g}'$, alors $g' = g.h$ avec $h \in H_x$, donc $g'.x = g.(h.x) = g.x$. Elle est surjective par définition de l'orbite. Enfin si $g.x = g'.x$, alors $(g'^{-1}g).x = x$, i.e. $g'^{-1}g \in H_x$, ou encore $\bar{g}' = \bar{g}$ dans G/H_x.

□

Corollaire 2.4 (Équation aux classes) *Soit G un groupe fini opérant sur un ensemble fini X. Soit Ω l'ensemble des orbites, notons $\#H_\omega$ le cardinal du stabilisateur de x pour x dans l'orbite ω (indépendant du choix de x dans Ω d'après la proposition précédente). Alors*

$$\#X = \sum_{\omega \in \Omega} \frac{\#G}{\#H_\omega}$$

Démonstration : Comme les orbites forment une partition de X, c'est immédiat d'après la proposition précédente. Il y a néanmoins (comme on le verra plus tard) des conséquences tout à fait non triviales !

□

Theorème 2.5 (Formule de Burnside) *Soit G un groupe fini opérant sur un ensemble fini X. Pour tout $g \in G$, notons $\mathrm{Fix}\, g$ le sous-ensemble de X constitué des points fixes de G. Alors*

$$\sum_{x \in X} \frac{1}{\#\,\omega(x)} = \frac{1}{\#G} \sum_{g \in G} \#(\mathrm{Fix}\, g)$$

De plus ce nombre est égal au nombre d'orbites.

Démonstration : Soit E l'ensemble des couples (g, x) de $G \times X$ qui vérifient $g.x = x$. Alors son cardinal est $\sum_{g \in G} \#(\mathrm{Fix}\, g)$, mais ce cardinal est aussi $\sum_{x \in X} \#H_x = \sum_{x \in X} \frac{\#G}{\#\,\omega(x)}$. La formule en résulte. D'autre part, si Ω est l'ensemble des orbites, on a

$$\sum_{x \in X} \frac{1}{\#\,\omega(x)} = \sum_{\omega \in \Omega} \sum_{x \in \omega} \frac{1}{\#\omega} = \sum_{\omega \in \Omega} 1 = \#\Omega$$

□

[Exercices : -Soit $P_n(k)$ le nombre de permutations de $\{1, ..., n\}$ qui ont exactement k points fixes. Alors $\sum_{k=0}^{n} k P_n(k) = n!$.

-Retrouver la décomposition d'une permutation en cycles en utilisant une action de groupe; vérifier que l'ordre d'une permutation dans $\mathcal{S}_n$ est le p.p.c.m. des longueurs des cycles qui apparaissent dans sa décomposition.]

2.2. p-groupes; théorèmes de Sylow

Définition 2.6 Soit p un nombre premier. On appelle *p-groupe* un groupe de cardinal p^n, où n est un entier.

Proposition 2.7 *Soit G un p-groupe non trivial. Alors*

1. *Le centre Z de G n'est pas trivial.*
2. *Si G est de cardinal p ou p^2, alors p est abélien.*

Démonstration : 1. On fait opérer G sur lui-même par conjugaison. Il y a $\#Z$ orbites réduites à un élément, et le cardinal des autres orbites est un diviseur de $p^n := \#G$ autre que 1, donc est divisible par p. Ainsi p^n (avec $n > 0$) est la somme du cardinal de Z et d'un multiple de p, donc p divise $\#Z$.

2. Si G est de cardinal p, alors tout élément non trivial de G est d'ordre divisant p, donc d'ordre p, et G est cyclique. Supposons que G soit de cardinal p^2. Si G n'était pas abélien, le cardinal de Z serait p d'après 1., donc G/Z serait cyclique (car de cardinal p). Mais on obtient une contradiction via le lemme suivant :

Lemme 2.8 *Soit G un groupe de centre Z avec G/Z cyclique. Alors G est abélien.*

Le lemme se démontre en prenant un générateur $\bar{a}$ de G/Z. Alors tout élément g de G s'écrit $g = a^m z$ avec $z \in Z$, et il est alors immédiat que deux éléments de G commutent.

□

Théorèmes de Sylow.

On se pose la question suivante : étant donnés un groupe fini G et un entier n divisant son cardinal, peut-on trouver un sous-groupe d'ordre n ? En général la réponse est non ($\mathcal{A}_4$ est de cardinal 12, mais n'a pas de sous-groupe d'ordre 6, regarder la décomposition d'une permutation en cycles), mais dans le cas particulier des p-sous-groupes, on va voir qu'on a une réponse positive.

Définition 2.9 *Soit p un nombre premier divisant le cardinal n d'un groupe fini. On appelle p-sous-groupe de Sylow un sous-groupe H de cardinal p^α, où $n = p^\alpha m$ avec p ne divisant pas m (i.e. p ne divise pas $[G : H]$).*

Theorème 2.10 (Premier théorème de Sylow) *Soit G un groupe fini et p un diviseur premier de $\#G$. Alors G contient au moins un p-sous-groupe de Sylow.*

La preuve repose sur deux lemmes, qui ont un intérêt propre.

Lemme 2.11 *Soit H un sous-groupe de G. Si G contient un p-Sylow S, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.*

(Ce lemme permet de se ramener à un "sur-groupe" pour prouver le théorème).

Lemme 2.12 *Soit $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ (corps à p éléments) et $G_p := \mathrm{GL}_n(\mathbf{F}_p)$ avec $n \in \mathbf{N}^*$. Alors G_p possède un p-Sylow.*

Le premier théorème de Sylow résulte facilement de ces deux lemmes. En effet, il ne reste plus qu'à prouver que G est isomorphe à un sous-groupe de G_p. Or G est isomorphe à un sous-groupe de $\mathcal{S}_n$ (théorème de Cayley), et $\mathcal{S}_n$ se plonge dans G_p en envoyant la permutation σ sur la matrice M_σ qui envoie le vecteur e_i sur $e_{\sigma(i)}$, où $(e_1, ..., e_n)$ est la base canonique. [7] Il reste à prouver les deux lemmes.

Preuve du lemme 2.11 : On a vu que H opérait sur l'ensemble G/S des classes à gauche via $(h, aS) \mapsto (ha)S$. On voit tout de suite que le stabilisateur $\mathrm{Stab}_H(aS)$ de aS pour cette action est $aSa^{-1} \cap H$. Chacun de ces $\mathrm{Stab}_H(aS)$ est un p-groupe comme sous-groupe de aSa^{-1}, donc il suffit de montrer que l'un d'entre eux a un indice dans H non divisible par p. Or, cet indice $\frac{\#H}{\#\mathrm{Stab}_H(aS)}$ est aussi le cardinal de l'orbite $\omega_H(aS)$. Comme p ne divise pas le cardinal de l'ensemble G/S (puisque S est un p-Sylow de G), le résultat vient de ce que les orbites forment une partition de G/S.

□

Preuve du lemme 2.12 : On calcule d'abord le cardinal de G_p. C'est celui du nombre de bases du $\mathbf{F}_p$-espace vectoriel $\mathbf{F}_p^n$, soit

$$(p^n - 1)(p^n - p)...(p^n - p^{n-1})$$

d'où il ressort qu'un p-Sylow de G_p est de cardinal $p^{1+2+...+n-1} = p^{n(n-1)/2}$. Or l'ensemble des matrices triangulaires supérieures dont la diagonale n'a que des 1 est un sous-groupe de G_p qui possède ce cardinal.

□

[Exercice : Un groupe de cardinal $p^\alpha m$, avec p ne divisant pas m, contient des sous-groupes d'ordre p^i pour tout $i \leq \alpha$ (se ramener à un p-groupe et raisonner par récurrence sur le cardinal en distinguant les cas G abélien et non-abélien).]

Le théorème suivant étudie la conjugaison des p-Sylow.

Theorème 2.13 (Deuxième théorème de Sylow) *Soit G un groupe fini de cardinal $n = p^\alpha m$ avec p ne divisant pas m. Alors*

1. *Si $H \subset G$ est un p-groupe, il existe un p-Sylow de G qui le contient.*

[7] Attention si on permutait les coordonnées au lieu des vecteurs de base, on obtiendrait un anti-morphisme et pas un morphisme.

2. Les p-Sylow de G sont tous conjugués, et leur nombre k divise n.

3. k est congru à 1 mod. p (donc k divise m).

Démonstration : 1. D'après le premier théorème de Sylow, il existe au moins un p-Sylow S de G. Le lemme 2.11 dit alors qu'il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H, i.e. $aSa^{-1} \cap H = H$ puisque H est un p-groupe. Ainsi H est inclus dans aSa^{-1} qui est un p-Sylow de G.

2. Si H est un p-Sylow de G, on a de plus $H = aSa^{-1}$ par cardinalité, donc tout p-Sylow de G est conjugué de S. Faisons alors opérer G par conjugaison sur l'ensemble X des p-Sylow. Comme il n'y a qu'une seule orbite, son cardinal k (qui divise celui de G) est celui de X, i.e. le nombre de p-Sylow.

3. Soit S un p-Sylow de G, on fait opérer S sur X par conjugaison. Soient X^S l'ensemble des points fixes pour cette action (i.e. les orbites réduites à un élément) et Ω' l'ensemble des autres orbites. L'équation aux classes s'écrit

$$k = \#X^S + \sum_{\omega \in \Omega'} \#\omega$$

Le cardinal des orbites qui sont dans Ω' divise celui de S et n'est pas 1, donc est divisible par p. Pour conclure il suffit donc de montrer qu'il n'y a qu'une seule orbite réduite à un point (celle de S). i.e. : si T est un p-Sylow de G tel que $sTs^{-1} = T$ pour tout s de S, alors $S = T$.

Pour cela, on introduit le sous-groupe N de G engendré par S et T. A fortiori S et T sont des p-Sylow de N, donc sont conjugués par un élément de N. Mais T est distingué dans N via le fait que $sTs^{-1} = T$ pour tout s de S, donc finalement $T = S$. [8]

□

Un cas particulier important est celui où m n'a aucun diviseur $\neq 1$ qui est congru à 1 modulo p. Alors G possède un p-Sylow unique, qui est donc distingué. Par exemple un groupe d'ordre 63 ou 255 n'est pas simple.

2.3. Produit semi-direct de deux groupes

Attention à cette notion, qui est en générale la source de nombreuses erreurs, notamment à l'oral de l'agrégation...

Rappelons que quand G_1 et G_2 sont deux groupes, on dispose du produit direct $G_1 \times G_2$ qui correspond à mettre la loi $(g_1, g_2)(h_1, h_2) = (g_1 g_2, h_1 h_2)$ sur l'ensemble produit.

[8] Ce raisonnement s'appelle "l'argument de Frattini".

Le produit semi-direct est une généralisation de cette notion. Soient N et H deux groupes et $\varphi : H \to \mathtt{Aut}\, N$ un morphisme de groupes, qui définit en particulier une action $h.n := \varphi(h)(n)$ de N sur G (mais on demande en plus ici que l'image de φ soit incluse dans $\mathtt{Aut}\, N$, et pas seulement dans $\mathcal{S}(N)$).

Proposition 2.14 *On définit une loi de groupes sur l'ensemble produit $N \times H$ en posant*

$$(n, h).(n', h') := (n(h.n'), hh')$$

Ce groupe s'appelle le produit semi-direct de N par H relativement à l'action φ; on le note $N \rtimes_\varphi H$ (ou simplement $N \rtimes H$ si l'action φ est sous-entendue).

Démonstration : Clairement $(1, 1)$ est élément neutre pour la loi définie (on utilise déjà ici que $h.1 = 1$, qui vient du fait que l'action est à valeurs dans $\mathtt{Aut}\, N$). D'autre part (n, h) a pour inverse $(h^{-1}.n^{-1}, h^{-1})$ (ici on utilise $h^{-1}.(nn^{-1}) = (h^{-1}.n)(h^{-1}.n^{-1})$). Il reste à vérifier l'associativité.

On a

$$[(n_1, h_1)(n_2, h_2)](n_3, h_3) = (n_1(h_1.n_2), h_1h_2)(n_3, h_3) = (n_1(h_1.n_2)[(h_1h_2).n_3], h_1h_2h_3)$$

et

$$(n_1, h_1)[(n_2, h_2)(n_3, h_3)] = (n_1, h_1)(n_2(h_2.n_3), h_2h_3) = (n_1[h_1.(n_2(h_2.n_3))], h_1h_2h_3)$$

Or $(h_1.n_2)[(h_1h_2).n_3] = [h_1.(n_2(h_2.n_3))]$ d'après les axiomes des actions de groupe et le fait que $n \mapsto h_1.n$ soit un automorphisme de N. D'où le résultat. □

Remarques :

- Parler "du" produit semi-direct de N par H n'a de sens que si on précise l'action, il peut exister plusieurs actions de H sur N, donc plusieurs produits semi-directs. On fera aussi attention au fait que H et N ne jouent pas des rôles symétriques.
- L'action triviale correspond au produit direct.

Proposition 2.15 *Avec les notations ci-dessus, soit $G = N \rtimes H$. Alors :*

1. *On a une suite exacte*

   $$1 \to N \xrightarrow{i} G \xrightarrow{p} H \to 1$$

   avec $i(n) = (n, 1)$ et $p(n, h) = h$. En particulier N s'identifie à un sous-groupe distingué (noté encore N) [9] dans G.

[9] N comme "normal"; le symbole $\rtimes$ ressemble à $\lhd$ et permet de se rappeler le "sens" dans lequel on effectue le produit semi-direct.

2. *La suite exacte est scindée, i.e. il existe un morphisme $s : H \to G$ ("section") vérifiant $p \circ s = \mathrm{Id}_H$. Ainsi H s'identifie à un sous-groupe (encore noté H) de G.*

3. *Dans G, on a $N \cap H = \{1\}$ et $NH = G$, où NH est par définition l'ensemble des nh avec $n \in N$ et $h \in H$. De plus l'opération de H sur N est décrite par $h.n = hnh^{-1}$, le produit de droite étant effectué dans G.*

Démonstration : 1. i et n sont des morphismes via $(n,1)(n',1) = (n(1.n'),1) = (nn',1)$ et $(n,h)(n',h') = (n(h.n'),hh')$. Le fait que la suite soit exacte est immédiat.

2. Il suffit de poser $s(h) = (1,h)$.

3. D'après 1., $N \cap H$ est l'ensemble des (n,h) avec $n = h = 1$, donc il est réduit au neutre de G. si $g = (n,h)$ est un élément de G, on a $g = (n,1).(1,h)$, donc $G = NH$. Enfin on a dans G : $hnh^{-1} = (1,h)(n,1)(1,h^{-1}) = (h.n,h)(1,h^{-1}) = (h.n,1) = h.n$.

□

Remarque : Via la proposition précédente, on peut désormais écrire les éléments de $N \rtimes H$ de manière unique sous la forme nh ($n \in N, h \in H$) avec la règle de commutation $hn = (h.n)h$. Notons aussi que $N \rtimes H$ est abélien si et seulement si l'opération est triviale, avec N et H tous deux abéliens.

On a une sorte de réciproque de la proposition précédente pour savoir quand un groupe se décompose en produit semi-direct.

Proposition 2.16 *1. (Caractérisation "interne") Soit G un groupe contenant deux sous-groupes N et H avec*

i) $N \lhd G$.

ii) $N \cap H = \{1\}$.

iii) $G = NH$.

Alors $G \simeq N \rtimes H$ pour l'opération $h.n = hnh^{-1}$.

2. (Caractérisation "externe") Soit

$$1 \to N \to G \to H \to 1$$

une suite exacte admettant une section $s : H \to G$. Alors $G \simeq N \rtimes H$ pour l'opération $h.n = s(h)ns(h)^{-1}$.

Démonstration : 1. Soit φ l'opération de H sur N définie par $\varphi(h)(n) = hnh^{-1}$. Alors l'application $\Phi : N \rtimes_\varphi H \to G$ qui associe à (n, h) le produit nh (dans G) est un morphisme car $\Phi((n,h)(n',h')) = \Phi(n(hn'h^{-1}), hh') = nhn'h'$. L'injectivité de Φ résulte de ii) et sa surjectivité de iii).

2. Posons $H_1 = s(H)$. Comme s est injective vu que $p \circ s = \mathrm{id}_H$, H_1 est un sous-groupe de G isomorphe à H et via 1., il suffit de montrer : $N \cap H_1 = \{1\}$ et $NH_1 = G$ (on a identifié N à son image dans G). Si $h_1 \in N \cap H_1$, alors $p(h_1) = 1$ mais $h_1 = s(h)$ avec $h \in H$, d'où $1 = p(s(h)) = h$ et $h_1 = 1$. Si maintenant $g \in G$, alors g et $s(p(g))$ ont même image par p, donc ils diffèrent d'un élément du noyau N, i.e. $g = nh_1$ avec $h_1 := s(p(g))$, et $g \in NH_1$.

□

C'est en général le deuxième critère qui est le plus utile pour obtenir des décompositions en produit semi-direct, mais on gardera bien à l'esprit la façon de déterminer l'opération de H sur N associée en fonction de la suite exacte et de la section.

[Exercices : -Soit $G = N \rtimes H$, alors l'opération de H sur N est triviale (i.e. le produit est direct) si et seulement si le sous-groupe H de G est distingué.

-Soient N et H deux groupes, φ et ψ deux morphismes $H \to \mathtt{Aut}\, N$. S'il existe $u \in \mathtt{Aut}\, N$ tel que $\psi(h) = u \circ \varphi(h) \circ u^{-1}$ ("actions conjuguées"), alors $N \rtimes_\varphi H \simeq N \rtimes_\psi H$.]

-Soient N et H deux groupes, φ et ψ deux morphismes $H \to \mathtt{Aut}\, N$. S'il existe $\alpha \in \mathtt{Aut}\, H$ tel que $\varphi = \psi \circ \alpha$, alors $N \rtimes_\varphi H \simeq N \rtimes_\psi H$ (envoyer $nh \in N \rtimes_\varphi H$ sur $n\alpha(h) \in N \rtimes_\psi H$).]

Exemples.

1. Pour $n \geq 2$, la suite exacte

$$1 \to \mathcal{A}_n \to \mathcal{S}_n \xrightarrow{\varepsilon} \mathbf{Z}/2\mathbf{Z} \to 1$$

est scindée via la section s qui envoie $\bar{0}$ sur Id et $\bar{1}$ sur une transposition (arbitraire) τ. On en déduit une décomposition $\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbf{Z}/2\mathbf{Z}$.

2. Soient K un corps et $n \in \mathbf{N}^*$. La suite exacte

$$1 \to \mathrm{SL}_n(K) \to \mathrm{GL}_n(K) \xrightarrow{\det} K^* \to 1$$

est scindée (envoyer $\lambda \in K^*$ sur la matrice $\mathrm{Diag}(\lambda, 1, ..., 1)$). Ainsi $\mathrm{GL}_n(K) \simeq \mathrm{SL}_n(K) \rtimes K^*$.

3. Le groupe $\mathbf{Z}/4\mathbf{Z}$ n'est *pas* produit semi-direct de $\mathbf{Z}/2\mathbf{Z}$ par $\mathbf{Z}/2\mathbf{Z}$. En effet le seul automorphisme de $\mathbf{Z}/2\mathbf{Z}$ est l'identité, donc l'action serait triviale; or $\mathbf{Z}/4\mathbf{Z}$ n'est pas isomorphe au produit direct $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (le premier groupe a des éléments d'ordre 4 et pas le deuxième). En particulier la suite exacte

$$0 \to \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0$$

(obtenue en envoyant x (mod. 4) sur x (mod.2), le noyau est $\{\bar{0}, \bar{2}\}$ qui est isomorphe à $\mathbf{Z}/2\mathbf{Z}$) n'est pas scindée.[10]

4. Soit $n \geq 3$, on note D_n le groupe des isométries du plan conservant un polygone régulier convexe à n côtés. Il contient les n rotations de centre O (le centre du polygone) et d'angle $2k\pi/n$ ($0 \leq k \leq n-1$) et les n réflexions par rapport aux droites passant par O et les sommets (si n est impair) ou les milieux des côtés (si n est pair). On a une suite exacte

$$1 \to \mathbf{Z}/n\mathbf{Z} \to D_n \to \mathbf{Z}/2\mathbf{Z} \to 1$$

obtenue en prenant le déterminant d'une isométrie, qui est à valeurs dans $\{\pm 1\}$. Elle est scindée (on envoie l'élément non trivial ε de $\mathbf{Z}/2\mathbf{Z}$ sur une réflexion), d'où une décomposition $D_n \simeq \mathbf{Z}/n\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$. Notons que l'action correspondante de $\mathbf{Z}/2\mathbf{Z}$ sur $\mathbf{Z}/n\mathbf{Z}$ consiste à poser $\varepsilon.x = -x$ pour $x \in \mathbf{Z}/n\mathbf{Z}$.

2.4. Compléments sur $\mathbf{Z}/n\mathbf{Z}$

Pour construire des produits semi-directs non triviaux, on s'intéresse aux automorphismes de $(\mathbf{Z}/n\mathbf{Z}, +)$, ce qui comme on va le voir est étroitement lié à la structure du groupe des inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$.

On commence par la proposition élémentaire suivante, que nous rappelons sans démonstration :

Proposition 2.17 *Soit $n \in \mathbf{N}^*$, $s \in \mathbf{Z}$. Alors les propriétés suivantes sont équivalentes :*

i) $(s, n) = 1$.

ii) $\bar{s}$ *engendre le groupe additif* $\mathbf{Z}/n\mathbf{Z}$.

iii) $\bar{s}$ *appartient au groupe des inversibles* $(\mathbf{Z}/n\mathbf{Z})^*$ *de l'anneau* $\mathbf{Z}/n\mathbf{Z}$.

[10] On voit donc que même dans des cas très élémentaires, on ne peut pas toujours "reconstituer" un groupe à partir de ses sous-groupes. En particulier, la connaissance des groupes finis simples ne suffit absolument pas à connaître tous les groupes finis, contrairement à une croyance populaire assez répandue (notamment chez les agrégatifs !).

On prendra garde de ne pas confondre les structures additives et multiplicatives (par exemple ne pas remplacer iii) par "$\bar{s}$ engendre $(\mathbf{Z}/n\mathbf{Z})^*$", ce qui est trivialement faux par exemple pour $s = 1$; on verra que le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ n'est pas cyclique en général, ex. $n = 8$).

On va préciser maintenant un peu la structure de $(\mathbf{Z}/n\mathbf{Z})^*$ et son lien avec $\mathtt{Aut}\,((\mathbf{Z}/n\mathbf{Z}, +))$; pour tout $n \in \mathbf{N}^*$, on note $\varphi(n)$ l'*indicatrice d'Euler* de n, i.e. le nombre d'entiers x de $[1, n]$ qui sont premiers avec n.

Proposition 2.18 *Soit $n \in \mathbf{N}^*$, on écrit $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts. Alors :*

1. *Le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$ est $\varphi(n)$. Pour p premier, on a $\varphi(p) = p - 1$, et plus généralement $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ si $\alpha \geq 1$.*

2. *Le groupe $\mathtt{Aut}\,(\mathbf{Z}/n\mathbf{Z})$ des automorphismes du groupe additif [11] $\mathbf{Z}/n\mathbf{Z}$ est isomorphe au groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$.*

3. *On a un isomorphisme d'anneaux*

$$\mathbf{Z}/n\mathbf{Z} \simeq \prod_{i=1}^{r} \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$$

et un isomorphisme de groupes

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq \prod_{i=1}^{r} (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^*$$

4. *On a $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r}(1 - \frac{1}{p_i})$.*

Démonstration : 1. résulte de la proposition précédente, et de ce que les entiers de $[1, p^\alpha]$ non premiers avec p sont les multiples de p.

2. Il est immédiat que l'application Φ du groupe $((\mathbf{Z}/n\mathbf{Z})^*, \times)$ dans le groupe $(\mathtt{Aut}\,(\mathbf{Z}/n\mathbf{Z}), \circ)$ qui envoie a sur $x \mapsto ax$ est un morphisme de groupes. Ce morphisme est injectif car si $\Phi(a)$ est l'identité, alors $ax = x$ pour tout x soit $a = 1$ en prenant $x = \bar{1}$. Il est surjectif car si $\varphi \in \mathtt{Aut}\,(\mathbf{Z}/n\mathbf{Z})$, alors en posant $a = \varphi(\bar{1})$, on obtient que pour tout x de $\mathbf{N}$, on a $\varphi(\bar{x}) = \varphi(1 + ... + 1)$ (x termes) soit $\varphi(\bar{x}) = a\bar{x}$; d'autre part $a \in (\mathbf{Z}/n\mathbf{Z})^*$ car $\bar{1}$ doit avoir un antécédent par φ.

[11] et non pas de l'anneau; le seul automorphisme de l'anneau $(\mathbf{Z}/n\mathbf{Z})$ est l'identité, vu que $\bar{1}$ doit être envoyé sur $\bar{1}$.

3. L'application de $\mathbf{Z}/n\mathbf{Z}$ dans $\prod_{i=1}^{r} \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$ qui envoie $\bar{x}$ sur $(x_i)_{1\leq i\leq r}$, où x_i est la classe de x mod. $p_i^{\alpha_i}$ est clairement un morphisme d'anneaux. Il est injectif car si x est divisible par tous les $p_i^{\alpha_i}$, il est divisible par leur produit n vu qu'ils sont deux à deux premiers entre eux. Comme $\mathbf{Z}/n\mathbf{Z}$ et $\prod_{i=1}^{r} \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$ ont même cardinal, il est aussi surjectif [12]. La deuxième assertion est immédiate en écrivant que deux anneaux isomorphes ont des groupes d'inversibles isomorphes.

4. résulte de 1. et 3.

□

Pour aller plus loin, on voudrait maintenant déterminer la structure de $(\mathbf{Z}/p^{\alpha}\mathbf{Z})$ pour p premier et $\alpha \in \mathbf{N}^*$. On commence par le cas $\alpha = 1$.

Proposition 2.19 *Soient K un corps[13] et G un sous-groupe fini du groupe multiplicatif K^*. Alors G est cyclique.*

Démonstration : On utilise le lemme suivant

Lemme 2.20 *Soit $n \in \mathbf{N}^*$, alors*

$$n = \sum_{d|n} \varphi(d)$$

Le lemme se démontre en observant que $\mathbf{Z}/n\mathbf{Z}$ contient un unique sous-groupe C_d de cardinal d, qui est cyclique et est précisément l'ensemble des x de $\mathbf{Z}/n\mathbf{Z}$ tels que $dx = 0$. Comme C_d est isomorphe à $\mathbf{Z}/d\mathbf{Z}$, il contient exactement $\varphi(d)$ éléments d'ordre d. Finalement $\mathbf{Z}/n\mathbf{Z}$ contient exactement $\varphi(d)$ éléments d'ordre d (un tel élément x doit vérifier $dx = 0$, donc appartenir à C_d) et on obtient le lemme en triant les éléments de $\mathbf{Z}/n\mathbf{Z}$ suivant leur ordre.

Revenons à la proposition. Soit n le cardinal de G et supposons que G contienne un élément x d'ordre d. Alors le sous-groupe G_d engendré par x est de cardinal d, et tous ses éléments g vérifient $g^d = 1$. Mais dans le corps K l'équation polynomiale $X^d - 1 = 0$ a au plus d solutions, donc nécessairement G_d est l'ensemble de ces solutions. Comme il est cyclique d'ordre d, il contient $\varphi(d)$ éléments d'ordre d qui sont exactement les éléments d'ordre d de G (un élément d'ordre d de G vérifie l'équation $X^d - 1 = 0$, i.e. appartient à G_d). On a ainsi montré que pour tout d divisant n, G possède 0 ou $\varphi(d)$ éléments

[12] C'est une des formulations du "lemme chinois".

[13] Rappelons qu'on impose que la multiplication de K soit commutative; sinon la proposition est fausse, l'algèbre $\mathbf{H}$ des quaternions sur $\mathbf{C}$ contenant par exemple un sous-groupe non-abélien de $\mathbf{H}^*$ d'ordre 8.

d'ordre d, c'est-à-dire en tout cas au plus $\varphi(d)$ éléments d'ordre d. D'après le lemme, on a $n > \sum_{d|n, d\neq n} \varphi(d)$, donc on obtiendrait une contradiction si G n'avait pas d'éléments d'ordre n. Ceci montre que G est cyclique.

□

Corollaire 2.21 *Pour p premier, le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique (donc isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z}$).*

En effet dans ce cas $\mathbf{Z}/p\mathbf{Z}$ est un corps. Notons que déterminer explicitement un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ est un problème en général difficile.

On passe maintenant au cas général.

Theorème 2.22 *Soient p un nombre premier* **différent de 2** *et $\alpha \in \mathbf{N}^*$. Alors le groupe $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est cyclique (donc isomorphe à $\mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}$).*

Comme on le verra plus loin, ce résultat est faux si $p = 2$ et $\alpha \geq 3$.

Pour montrer le théorème, on commence par exhiber un élément d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ à l'aide du lemme suivant :

Lemme 2.23 *Soient p premier $\neq 2$ et $k \in \mathbf{N}^*$, alors*

$$(1+p)^{p^k} = 1 + \lambda p^{k+1}$$

avec λ entier non divisible par p.

Démonstration : On procède par récurrence sur k. Pour $k = 1$, on écrit

$$(1+p)^p = 1 + pC_p^1 + p^2C_p^2 + ... + p^p = 1 + p^2(1 + C_p^2 + ... + p^{p-2})$$

et on utilise le fait que p divise C_p^k pour $1 \leq k \leq p-1$ (noter que pour $p = 2$ cette étape ne marche pas car p ne divise pas p^{p-2}). Supposons le résultat vrai pour p, alors

$$(1+p)^{p^{k+1}} = (1+\lambda p^{k+1})^p = 1 + \lambda p^{k+2} + p^{k+2}\sum_{i=2}^{p} C_p^i \lambda^i p^{i(k+1)-(k+2)}$$

et comme p divise $\sum_{i=2}^{p} C_p^i \lambda^i p^{i(k+1)-(k+2)}$ (il divise C_p^i pour $2 \leq i \leq p-1$, et $p^{p(k+1)-(k+2)}$), on obtient le résultat.

□

Preuve du théorème : D'après le lemme, l'élément $s = \overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. Cherchons maintenant un élément d'ordre $p-1$. On a un morphisme surjectif $\pi : (\mathbf{Z}/p^\alpha\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$ obtenu en envoyant $\bar{x}$ sur la classe de x modulo p (en effet x est inversible modulo p^α si et seulement s'il est inversible modulo p). Soient u un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ (qui est cyclique d'après le corollaire 2.21) et $v \in (\mathbf{Z}/p^\alpha\mathbf{Z})^*$ tel que $\pi(v) = u$. Soit m l'ordre de v, alors $v^m = \bar{1}$ donc $u^m = \pi(v^m) = \bar{1}$ et $p-1$ (qui est l'ordre de u) divise m. Posons $r = v^{m/(p-1)}$, alors r est d'ordre $p-1$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$.

Maintenant rs est d'ordre $(p-1)p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ car il est immédiat que dans un groupe abélien (noté multiplicativement), l'ordre d'un produit xy est le produit des ordres de x et de y quand ceux-ci sont premiers entre eux. [14]

□

Le cas $p = 2$ est exceptionnel et fait l'objet du théorème suivant :

Theorème 2.24 *Pour tout entier $\alpha \geq 3$, le groupe multiplicatif $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ est isomorphe au groupe additif $\mathbf{Z}/2\mathbf{Z} \times (\mathbf{Z}/2^{\alpha-2}\mathbf{Z})$.*

Ainsi pour $\alpha \geq 3$ le groupe $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ n'est pas cyclique (l'ordre de tout élément divise $2^{\alpha-2}$). Les cas $\alpha = 1$ et $\alpha = 2$ sont triviaux, $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ étant alors respectivement isomorphe à $\{0\}$ et à $\mathbf{Z}/2\mathbf{Z}$.

Démonstration : On montre aisément par récurrence sur $k \geq 1$ qu'on a : $5^{2^k} = 1 + \lambda 2^{k+2}$ avec λ entier impair. Il en résulte que l'ordre de $\bar{5}$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ est exactement $2^{\alpha-2}$. Considérons la surjection $\pi : (\mathbf{Z}/2^\alpha\mathbf{Z})^* \to (\mathbf{Z}/4\mathbf{Z})^*$ qui associe à un élément $\bar{x}$ la classe de x modulo 4. C'est un morphisme surjectif, dont le noyau contient $\bar{5}$, donc aussi le sous-groupe N engendré par $\bar{5}$. Comme le noyau est de cardinal $\frac{\#(\mathbf{Z}/2^\alpha\mathbf{Z})^*}{\#(\mathbf{Z}/4\mathbf{Z})^*} = \frac{2^{\alpha-1}}{2} = 2^{\alpha-2}$, il en résulte que ce noyau est exactement N (dont le cardinal est l'ordre de $\bar{5}$). Maintenant on définit une section de la suite exacte

$$1 \to N \to (\mathbf{Z}/2^\alpha\mathbf{Z})^* \to (\mathbf{Z}/4\mathbf{Z})^* \to 1$$

en envoyant l'élément non trivial de $(\mathbf{Z}/4\mathbf{Z})^*$ sur $-\bar{1}$. De ce fait $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$ est produit semi-direct, donc direct puisqu'il est abélien, de N par $(\mathbf{Z}/4\mathbf{Z})^*$. On conclut en observant que N est isomorphe au groupe additif $\mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ et $(\mathbf{Z}/4\mathbf{Z})^*$ au groupe additif $\mathbf{Z}/2\mathbf{Z}$.

□

[14] Ce n'est pas vrai sans cette dernière hypothèse, prendre par exemple $y = x^{-1}$.

L'étude du groupe d'automorphismes de $\mathbf{Z}/n\mathbf{Z}$ permet de construire des produits semi-directs non triviaux. Voici un exemple simple d'application (on en verra d'autres en T.D.) :

Theorème 2.25 *Soient p et q deux nombres premiers avec $p < q$. Alors :*

- *Si p ne divise pas $q-1$, tout groupe d'ordre pq est cyclique.*
- *Si p divise $q-1$, il y a deux groupes d'ordre pq à isomorphisme près : le groupe cyclique, et un produit semi-direct non commutatif $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$.*

Par exemple, le seul groupe d'ordre 15 est $\mathbf{Z}/15\mathbf{Z}$, et pour $q \geq 3$, les deux groupes d'ordre $2q$ sont le groupe cyclique et le groupe diédral D_q.

Démonstration : Soit G d'ordre pq, alors G possède un q-Sylow Q. D'après le deuxième théorème de Sylow, le nombre de q-Sylow est congru à 1 mod. q, et il divise p donc c'est 1 car $p < q$. Ainsi Q est distingué dans G. On obtient une suite exacte

$$1 \to Q \to G \xrightarrow{f} G/Q \to 1$$

Cette suite est scindée car G contient un p-Sylow P, et la restriction de f à P est alors injective parce que le cardinal de son noyau $P \cap Q$ doit diviser p et q. Ainsi f induit une bijection de P sur G/Q, dont la bijection réciproque fournit la section voulue. Finalement G est un produit semi-direct $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$, associé à un morphisme $\varphi : \mathbf{Z}/p\mathbf{Z} \to \mathtt{Aut}\,(Z/q\mathbf{Z}) \simeq Z/(q-1)\mathbf{Z}$.

Si p ne divise pas $q-1$, le cardinal de l'image de φ divise p et $q-1$, donc vaut 1, i.e. φ est triviale est le produit est direct. Comme p et q sont premiers entre eux, G est isomorphe à $\mathbf{Z}/pq\mathbf{Z}$ via le lemme chinois.

Si p divise $q-1$, on a un morphisme φ non trivial en envoyant $\bar{1}$ sur la classe de $(q-1)/p$, d'où un produit semi-direct non commutatif. Mais si ψ est un autre morphisme non trivial de $\mathbf{Z}/p\mathbf{Z}$ dans $\mathtt{Aut}\,(Z/q\mathbf{Z})$, il existe $\alpha \in \mathtt{Aut}\,(\mathbf{Z}/p\mathbf{Z})$ tel que $\varphi = \psi \circ \alpha$ car $Z/(q-1)\mathbf{Z}$ possède un unique sous-groupe d'ordre p. Alors comme on l'a déjà vu, on a $\mathbf{Z}/q\mathbf{Z} \rtimes_\varphi \mathbf{Z}/p\mathbf{Z} \simeq \mathbf{Z}/q\mathbf{Z} \rtimes_\psi \mathbf{Z}/p\mathbf{Z}$ via l'application $nh \mapsto n\alpha(h)$, $n \in \mathbf{Z}/q\mathbf{Z}$, $h \in \mathbf{Z}/p\mathbf{Z}$.

□

3. Étude plus détaillée de $\mathcal{S}_n$ et $\mathcal{A}_n$

Le théorème principal de cette section est

Theorème 3.1 *Pour $n \geq 5$, le groupe alterné $\mathcal{A}_n$ est simple.*

Notons que le résultat est encore vrai (trivialement) pour $n = 2$ et $n = 3$, mais pas pour $n = 4$, le groupe consitué des doubles transpositions dans $\mathcal{A}_4$ étant un sous-groupe distingué non trivial.

Avant de passer à la démonstration du théorème, donnons tout de suite quelques corollaires.

Corollaire 3.2 *Pour $n \geq 5$, on a $D(\mathcal{A}_n) = \mathcal{A}_n$ et $D(\mathcal{S}_n) = \mathcal{A}_n$.*

On notera que la deuxième assertion est vraie pour tout $n \geq 2$ (seul le cas $n = 4$ est à vérifier séparément).

Démonstration : On a $D(\mathcal{A}_n) \subset \mathcal{A}_n$ vu que tout commutateur est de signature 1, mais $D(\mathcal{A}_n)$ est distingué dans $\mathcal{A}_n$ et n'est pas trivial vu que pour $n \geq 4$, $\mathcal{A}_n$ n'est pas abélien (deux 3-cycles dont les supports ont un ou deux éléments en commun ne commutent pas). D'où $D(\mathcal{A}_n) = \mathcal{A}_n$ par simplicité de $\mathcal{A}_n$. De même, $D(\mathcal{S}_n)$ est un sous-groupe de $\mathcal{A}_n$ non trivial, distingué dans $\mathcal{A}_n$ (il est déjà distingué dans $\mathcal{S}_n$), d'où $D(\mathcal{S}_n) = \mathcal{A}_n$ avec le théorème.

□

Corollaire 3.3 *Si $n \geq 5$, $\mathcal{S}_n$ a trois sous-groupes distingués : $\{\mathrm{Id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$.*

Démonstration : Soit H un sous-groupe distingué de $\mathcal{S}_n$. Alors $H \cap \mathcal{A}_n$ est distingué dans $\mathcal{A}_n$, donc par le théorème $H \cap \mathcal{A}_n$ est égal à $\mathcal{A}_n$ ou bien réduit à $\{\mathrm{Id}\}$. Dans le premier cas, $H \supset \mathcal{A}_n$, donc $H = \mathcal{A}_n$ ou $H = \mathcal{S}_n$ car $\mathcal{A}_n$ est d'indice 2 dans $\mathcal{S}_n$. Supposons donc $H \cap \mathcal{A}_n = \{\mathrm{Id}\}$ et montrons que H est le groupe trivial. Si τ et σ sont deux éléments non triviaux de H, alors $\tau\sigma$ est de signature $(-1)(-1) = 1$, donc $\tau = \sigma^{-1}$. De ce fait $H = \{\mathrm{Id}, \sigma, \sigma^{-1}\}$, mais alors H se surjecte sur $\{\pm 1\}$ par la signature, ce qui n'est pas possible parce qu'il est de cardinal 3, et 2 ne divise pas 3. Finalement H est de cardinal 1 ou 2, mais on a déjà vu que les sous-groupes d'ordre 2 de $\mathcal{S}_n$, qui sont de la forme $\{\mathrm{Id}, \tau\}$ où τ est une transposition, ne sont pas distingués dans $\mathcal{S}_n$ si $n \geq 3$.

□

Corollaire 3.4 *Soit H un sous-groupe d'indice n de $\mathcal{S}_n$ pour $n \geq 2$. Alors $H \simeq \mathcal{S}_{n-1}$.*

Démonstration : Les cas $n = 2$, $n = 3$ sont triviaux. Pour $n = 4$, H est de cardinal 6, mais il ne peut pas être cyclique (il n'y a pas d'éléments d'ordre 6 dans $\mathcal{S}_4$, vu que l'ordre d'un élément est le ppcm des longueurs des cycles de sa décomposition) donc il est isomorphe au groupe diédral D_3, i.e. à $\mathcal{S}_3$. Supposons donc $n \geq 5$. Alors $\mathcal{S}_n$ opère par translation sur l'ensemble $E := \mathcal{S}_n/H$ des classes à gauche, d'où un morphisme $\varphi : \mathcal{S}_n \to \mathcal{S}(E)$. Le noyau est un sous-groupe distingué de $\mathcal{S}_n$, et il ne peut pas contenir $\mathcal{A}_n$ parce qu'il est inclus dans H (le stabilisateur de la classe du neutre est H), qui est de cardinal $(n-1)! < \frac{n!}{2}$. D'après le corollaire précédent, le noyau est donc trivial. Ainsi φ est injective, et comme E est de cardinal n, c'est un isomorphisme. Posons alors $U := \varphi(H)$. Alors un élément u de $\mathcal{S}(E)$ est dans U si et seulement si $u.H = H$, c'est-à-dire que U est le stabilisateur de l'élément H de E. Comme E est de cardinal n, U (qui est isomorphe à H) est isomorphe au stabilisateur d'un point dans $\mathcal{S}_n$, i.e. à $\mathcal{S}_{n-1}$.

□

Remarque : Cela n'implique pas que H soit le stabilisateur d'un point pour l'action naturelle de $\mathcal{S}_n$ sur $\{1, ..., n\}$. En fait c'est quand même vrai si $n \neq 6$, et cela est lié au fait que pour $n \neq 6$, les seuls automorphismes de $\mathcal{S}_n$ sont intérieurs (cf. TD).

Preuve de la simplicité de $\mathcal{A}_n$ pour $n \geq 5$. Toutes les méthodes passent par deux lemmes assez simples :

Lemme 3.5 *Pour $n \geq 3$, les 3-cycles engendrent $\mathcal{A}_n$.*

Démonstration : Comme $\mathcal{S}_n$ est engendré par les transpositions, $\mathcal{A}_n$ est engendré par les produits de deux transpositions. Or, si a, b, c, d sont des éléments deux à deux distincts de $[1, n]$, on a $(a, b)(b, c) = (a, b, c)$, $(a, b)(a, c) = (a, c, b)$, et $(a, b)(c, d) = (a, b)(a, c)(a, c)(c, d) = (a, c, b)(a, c, d)$.

□

Lemme 3.6 *Pour $n \geq 5$, les 3-cycles sont conjugués dans $\mathcal{A}_n$.*

Démonstration : Soient $\tau = (a_1, a_2, a_3)$ et $\tau' = (b_1, b_2, b_3)$ deux 3-cycles. Alors il existe $\sigma \in \mathcal{S}_n$ telle que $\sigma(a_i) = b_i$ pour $i = 1, 2, 3$, d'où $\sigma\tau\sigma^{-1} = \tau'$. Si $\varepsilon(\sigma) = 1$, c'est fini. Sinon on remplace σ par $\sigma' = \sigma(c, d)$,où c et d sont deux éléments de $[1, n]$, distincts, et distincts de a_1, a_2, a_3 (c'est ici que l'hypothèse $n \geq 5$ est utilisée).

□

Il résulte des deux lemmes que tout sous-groupe de $\mathcal{A}_n$ contenant un 3-cycle est égal à $\mathcal{A}_n$ si $n \geq 5$.

On montre maintenant le résultat pour $n = 5$:

Proposition 3.7 *Le groupe $\mathcal{A}_5$ est simple.*

Démonstration : Le cardinal de $\mathcal{A}_5$ est 60. On commence par trier ses éléments par leur ordre, en utilisant leur décomposition en cycles.

Les éléments d'ordre 2 sont les produits de deux transpositions à supports disjoints, il y en a $5 \times 3 = 15$ (5 choix pour le point fixe, et 3 doubles transpositions dans $\mathcal{S}_4$).

Les éléments d'ordre 3 sont les 3-cycles, il y en a $C_5^3 \times 2 = 20$ (C_5^3 choix pour les éléments permutés, et deux 3-cycles dans $\mathcal{S}_3$).

Il n'y a pas d'élément d'ordre 4 (les 4-cycles sont de signature -1).

Les éléments d'ordre 5 sont les 5-cycles, il y en a $4! = 24$.

Soit maintenant H un sous-groupe distingué de $\mathcal{A}_5$. Montrons que si H contient un élément d'ordre ω, avec $\omega \in \{2, 3, 5\}$, alors il contient tous les éléments d'ordre ω. Si $\omega = 3$, cela résulte du lemme 1. Si $\omega = 2$, il suffit de voir que les éléments d'ordre 2 sont conjugués dans $\mathcal{A}_5$; or si $\tau = (a_1, a_2)(a_3, a_4)(a_5)$ et $\tau' = (b_1, b_2)(b_3, b_4)(b_5)$ sont deux tels éléments, il existe un élément σ de $\mathcal{S}_5$ tel que $\sigma(a_i) = b_i$ pour $i = 1, ..., 5$, d'où $\sigma\tau\sigma^{-1} = \tau'$. Si σ est de signature -1, on la remplace par $\sigma(a_2, a_1)$. Enfin, bien que les 5-cycles ne soient pas tous conjugués dans $\mathcal{A}_5$ [15], les sous-groupes d'ordre 5 le sont car ce sont les 5-Sylow de $\mathcal{A}_5$; alors si H contient un élément d'ordre 5, il contient le sous-groupe qu'il engendre, donc tous les sous-groupes d'ordre 5, donc tous les éléments d'ordre 5.

Supposons maintenant $H \neq \{\mathrm{Id}\}$. Alors il ne peut exister $\omega \in \{2, 3, 5\}$ tel que tout élément non trivial de H soit d'ordre ω, sinon d'après ce qui précède H serait de cardinal $15 + 1$, $20 + 1$, ou $24 + 1$, et aucun de ces nombres ne divise 60. Il existe donc au moins deux nombres ω, ω' parmi $2, 3, 5$ tels que H contienne tous les éléments d'ordre ω et ω', mais alors le cardinal de H dépasse strictement $60/2$, et $H = \mathcal{A}_5$ vu que son cardinal doit diviser 60.

□

Remarque : En fait $\mathcal{A}_5$ est le le plus petit groupe simple autre que les $\mathbf{Z}/p\mathbf{Z}$ pour p premier (voir TD).

[15] En fait si c et c' sont deux 5-cycles, c est conjugué de c' ou c'^2, ce qui suffit à faire l'argument.

Preuve du théorème dans le cas général. Soit $E = [1, n]$, H un sous-groupe de $\mathcal{A}_n$ non réduit à l'identité. On choisit σ non trivial dans H. On va se ramener au cas $n = 5$ en fabriquant un élément de H qui agit sur un sous-ensemble de cardinal au plus 5 de E. Pour cela, on va considérer non pas un conjugué de σ (qui aurait le même nombre de points fixes que σ), mais un commutateur $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$ (qui a une chance d'en avoir davantage). On choisit τ de la manière suivante : soit a dans E tel que $b := \sigma(a)$ soit distinct de a, puis c dans E distinct de a, b, et $\sigma(b)$. On pose alors $\tau = (a, c, b)$, ce qui fait que $\rho = (\tau\sigma\tau^{-1})\sigma^{-1}$ est bien dans H. Alors $\tau^{-1} = (a, b, c)$ d'où $\rho = (a, c, b)(\sigma\tau^{-1}\sigma^{-1}) = (a, c, b)(\sigma.a, \sigma.b, \sigma.c)$. Comme $\sigma.a = b$, on voit qu'il existe un sous-ensemble F de E qui a au plus 5 éléments (et on peut le prendre de cardinal exactement 5) tel que ρ opère trivialement en dehors de F, et F contienne $\{a, b, c, \sigma(b), \sigma(c)\}$.

On obtient un morphisme injectif i de $\mathcal{A}(F)$ dans $\mathcal{A}_n$ en prolongeant une permutation de f par l'identité en dehors de F. Posons $H_0 = i^{-1}(H)$, c'est un sous-groupe distingué de $\mathcal{A}(F) \simeq \mathcal{A}_5$. Mais H_0 n'est pas trivial car il contient la restriction de ρ à F, et on a $\rho(b) = \tau\sigma(b) \neq b$ (vu que $\sigma(b) \neq c = \tau^{-1}(b)$). Ainsi $H_0 = \mathcal{A}(F)$ d'après le cas $n = 5$. En particulier H_0 contient un 3-cycle, donc H aussi, donc $H = \mathcal{A}_n$ avec les deux lemmes.

□

4. Groupes résolubles et nilpotents

On se contentera ici des définitions et des premières propriétés. On pourra se reporter au livre de Hall pour plus de détails.

Définition 4.1 Soit G un groupe.[16] On dit que G est *résoluble* s'il existe une suite finie

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

avec pour tout $i \in [1, n]$, $G_{i-1} \lhd G_i$ et G_i/G_{i-1} abélien.

Remarques :

1. Comme la proposition 4.3 le montrera, on peut demander en plus que chaque G_i soit distingué dans G tout entier. Alors G résoluble signifie que G se déduit de $\{1\}$ par une suite finie d'*extensions à noyaux abéliens* (en effet chaque G/G_{i-1} est extension de G/G_i par G_i/G_{i-1}).

[16] La notion est surtout intéressante pour les groupes finis, mais ce n'est pas indispensable de le supposer.

2. Si G est fini et qu'on n'impose pas $G_i \lhd G$, on peut demander G_i/G_{i-1} cyclique d'ordre premier au lieu d'abélien (car tout groupe abélien fini H admet une suite $H \supset ... \supset \{1\}$ avec tous les H_i/H_{i-1} simple, par récurrence sur $\#H$). Par contre demander G_i/G_{i-1} cyclique et $G_i \lhd G$ pour tout i est plus fort (on parle de groupe *hyper-résoluble*).

3. Le terme résoluble vient de la théorie des équations algébriques. Si P est un polynôme irréductible à coefficients dans $\mathbf{Q}$, et $K \subset \mathbf{C}$ son *corps de décomposition* (c'est le plus petit corps contenant toutes ses racines), on définit le *groupe de Galois* G de P comme le groupe des automorphismes du corps K. La théorie de Galois dit qu'une équation est résoluble par radicaux si et seulement si G est résoluble.[17]Le fait que $\mathcal{S}_n$ ne soit pas résoluble pour $n \geq 5$ entraîne l'impossiblité de résoudre par radicaux l'équation générale de degré 5.

Une notion plus forte que résoluble (et même qu'hyper-résoluble pour les groupes finis) est celle de groupe nilpotent :

Définition 4.2 On dit qu'un groupe G est *nilpotent* s'il existe une suite finie

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

avec pour tout $i \in [1, n]$, $G_i \lhd G$ et G_i/G_{i-1} inclus dans le centre de G/G_{i-1}.

Cela signifie donc que G se déduit de $\{1\}$ par une suite finie d'*extensions centrales* (une extension $1 \to N \to G \to H \to 1$ est dite centrale si N est inclus dans le centre de G).

Exemples.

1. Un groupe abélien est nilpotent.

2. Un p-groupe est nilpotent : c'est immédiat par récurrence sur son cardinal, vu que son centre est non trivial, et le quotient par son centre est encore un p-groupe.

3. $\mathcal{S}_n$ et $\mathcal{A}_n$ ne sont pas résolubles pour $n \geq 5$. Cela résulte de ce que $D(\mathcal{S}_n) = D(\mathcal{A}_n) = \mathcal{A}_n$, et de la proposition ci-dessous.

[17]Sans rentrer dans les détails, rajouter une racine n-ième à un corps donne un groupe de Galois cyclique, donc obtenir K en extrayant des racines correspond à une suite d'extensions cycliques.

4. $\mathcal{S}_4$ est résoluble, via la suite

$$\mathcal{S}_4 \supset \mathcal{A}_4 \supset V_4 \supset \{1\}$$

où V_4 est le sous-groupe constitué de l'identité et des doubles transpositions, mais il ne peut pas être nilpotent car son centre est trivial. Les mêmes conclusions valent pour $\mathcal{A}_4$ et $\mathcal{S}_3$

La proposition suivante donne la caractérisation la plus canonique d'un groupe résoluble. En particulier, c'est la plus commode pour montrer qu'un groupe n'est *pas* résoluble.

Proposition 4.3 *Soit G un groupe, on pose $D^0(G) = G$, $D^1(G) = D(G)$, et $D^i(G) = D(D^{i-1}(G))$ pour tout $i \geq 2$. Alors G est résoluble si et seulement s'il existe un entier n tel que $D^n(G) = \{1\}$.*

Démonstration : S'il existe n tel que $D^n(G) = \{1\}$, alors chaque $D^i(G)/D^{i-1}(G)$ est un groupe abélien par définition du sous-groupe dérivé donc G est résoluble via la suite des $D^i(G)$. Notons que chaque $D^i(G)$ est distingué dans G tout entier parce que le sous-groupe dérivé d'un groupe H est caractéristique dans H, et cette propriété est transitive.

En sens inverse si G est résoluble, soit $(G_i)_{1\leq i\leq n}$ une suite comme dans la définition 4.1. Alors G/G_{n-1} est abélien donc $G_{n-1} \supset D(G)$. Par récurrence sur i, on a $G_{n-i} \supset D^i(G)$ (si $G_{n-i+1} \supset D^{i-1}(G)$, alors comme G_{n-i+1}/G_{n-i} est abélien, on a $G_{n-i} \supset D(G_{n-i+1}) \supset D(D^{i-1}(G)) = D^i(G)$). Pour $i = n$ cela donne $D^n(G) = \{1\}$.

□

[Exercices : - $\mathcal{S}_3$ est hyper-résoluble mais pas $\mathcal{A}_4$.

-Un sous-groupe et un quotient d'un groupe résoluble sont résolubles, ainsi qu'une extension d'un groupe résoluble par un groupe résoluble.]