Cours M1 FES (2023-2024) : Groupes

David Harari

Table des matières

1. Généralités

1.1. Conventions

Rappelons pour mémoire la définition :

Définition 1.1 Un *groupe* $(G, .)$ est la donnée d'un ensemble G et d'une loi de composition interne (le plus souvent notée multiplicativement) $(x, y) \mapsto xy$ dans G, vérifiant :

i) La loi est associative : $(xy)z = x(yz)$ pour tous $x, y \in G$.

ii) Elle possède un élément neutre (noté en général 1) : $x.1 = 1.x = x$ pour tout $x \in G$.

iii) Tout élément possède un symétrique : pour tout $x \in G$, il existe $x' \in G$ (nécessairement unique) tel que $xx' = x'x = 1$. On notera x^{-1} le symétrique (appelé aussi *inverse*) de x.

Pour $n > 0$, on pose $x^n = x.x...x$ (n termes), avec les conventions $x^0 = 1$ et $x^{-n} = (x^n)^{-1}$. Noter que pour tous $x, y \in G$, on a $(xy)^{-1} = y^{-1}x^{-1}$.

Définition 1.2 Un groupe G est *abélien* (ou commutatif) si on a de plus $xy = yx$ pour tous $x, y \in G$.

Si G est abélien, on notera souvent $+$ la loi, 0 le neutre, et $-x$ le symétrique de x qu'on appelle alors l'*opposé* de x. On pourra aussi alors noter $x-y$ pour $x+(-y)$, et nx pour $x+x+...x$ (n termes) quand n est un entier > 0, avec les conventions $0.x = 0$ et $(-n)x = n(-x)$. Ainsi, tout groupe abélien est ipso facto muni d'une structure de *module* sur l'anneau commutatif $\mathbf{Z}$.

On se gardera bien d'utiliser la notation "x/y" si G n'est pas abélien car on ne saurait pas si cela signifie xy^{-1} ou $y^{-1}x$.

Exemple 1.3 a) Le groupe trivial, qu'on note $G = \{0\}$ ou $G = \{1\}$ suivant les cas (il est souvent vu comme sous-groupe d'un groupe additif ou multiplicatif).

b) 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.

c) $(\mathbf{R}, +)$ 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]

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

e) 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 $n \geq 3$.

f) 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.

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.

1.2. Morphisme de groupes, sous-groupes

Définition 1.4 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.

On dit aussi "homomorphisme" au lieu de morphisme. Noter que si $f : G \to G'$ est un morphisme, les propriétés $f(1) = 1$ et $f(x^{-1}) = f(x)^{-1}$ pour tout x de G sont automatiques. On notera parfois $G \simeq H$ pour "G est isomorphe à H."

Exemple 1.5 a) 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.

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

c) Si E est un ensemble 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, celle d'un cycle de longueur k est $(-1)^{k+1}$.

d) 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 1.6 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.

Proposition 1.7 *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* $\mathrm{Im}\, f := f(G)$ *est un sous-groupe de H. Le morphisme f est injectif si et seulement si son noyau est réduit à l'élément neutre.*

C'est immédiat à vérifier.

Exemple 1.8 a) 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).

b) Les sous-groupes de $\mathbf{Z}$ sont les $n\mathbf{Z}$ avec $n \in \mathbf{N}$.

c) 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* $\mathcal{A}_n$.

d) 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 $\mathrm{SL}_n(K)$.

e) L'ensemble $\mathtt{Aut}\, G$ des automorphismes d'un groupe G, muni de la composition $\circ$ des applications, est un sous-groupe du groupe des permutations $\mathcal{S}(G)$.

f) Le groupe $O_n(\mathbf{R})$ des matrices orthogonales réelles (ce sont les matrices M qui vérifient ${}^tMM = I$) est un sous-groupe de $\mathrm{GL}_n(\mathbf{R})$; le groupe $U_n(\mathbf{C})$ des matrices unitaires complexes (constitué des matrices M qui vérifient $M^*M = I$, où $M^* = {}^t\,\overline{M}$) est un sous-groupe de $\mathrm{GL}_n(\mathbf{C})$.

1.3. Générateurs d'un groupe ; groupes cycliques

Proposition 1.9 *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 $\langle A \rangle$.*

Il suffit en effet de prendre pour $\langle A \rangle$ l'intersection de tous les sous-groupes de G contenant A. Le sous-groupe engendré par la partie vide est $\{1\}$, et on a $\langle A \rangle = A$ si et seulement si A est un sous-groupe de G.

Pour toute partie A de G, on peut aussi décrire $\langle A \rangle$ comme l'ensemble des produits $x_1 ... x_n$ (avec $n \in \mathbf{N}$ quelconque), où chaque x_i vérifie : $x_i \in A$ ou $x_i^{-1} \in A$ (on convient que si $n = 0$, le produit vide est égal à 1). Si $A = \{a_1, ..., a_m\}$ est un groupe abélien fini, la description de $\langle A \rangle$ est plus simple : c'est l'ensemble des $\sum_{i=1}^m n_i a_i$ avec $a_i \in \mathbf{Z}$ (attention, ceci ne s'étend pas au cas où A n'est pas abélien). Plus généralement, si $(a_i)_{i \in I}$ est une famille d'éléments d'un groupe abélien, le sous-groupe engendré par les a_i est l'ensemble des combinaisons linéaires $\sum_{i \in I} n_i a_i$, où $(n_i)_{i \in I}$ est une famille presque nulle d'éléments de $\mathbf{Z}$.

Définition 1.10 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 1.11 *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 $\mathbf{N}^* \cup \{\infty\}$.*

On a en effet que si g est d'ordre fini n, alors $\langle g\rangle = \{1, g, g^2, ..., g^{n-1}\}$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ (pour le voir, effectuer la division euclidienne d'un entier quelconque m par n) ; si g est d'ordre infini, alors $\langle g\rangle = \{g^m, m \in \mathbf{Z}\}$ avec les g^m distincts deux à deux, ce qui permet de voir immédiatement que $\langle g\rangle$ est isomorphe à $\mathbf{Z}$.

Définition 1.12 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.

Exemple 1.13 a) Le groupe $(\mathbf{Z}^n, +)$ est engendré par la famille

$$(1, 0, ...0), (0, 1, ..., 0), ..., (0, ..., 0, 1).$$

Il n'est pas monogène si $n \geq 2$ (le démontrer !). On a même un résultat plus précis : toute partie génératrice de ce groupe a au moins n éléments (c'est un cas particulier de la théorie des modules sur un anneau principal).

b) Le groupe symétrique $\mathcal{S}_n$ est engendré par les transpositions.

c) 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).

1.4. Théorème de Lagrange

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.

□

Theorème 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 (i.e. les applications $x \mapsto ax$ pour $a \in G$ fixé) sont des bijections de G sur G. Le cardinal de G/H (qui est aussi celui de $H \setminus G$, ou encore $\#G/\#H$) s'appelle l'*indice* de H dans G.

Corollaire 1.16 *Dans un groupe fini G, l'ordre de tout élément est fini et divise l'ordre de G. En particulier si m est l'ordre de G, on a $x^m = 1$ pour tout x de G.*

On applique le théorème précédent et la proposition 1.11.

Proposition 1.17 *Soit $G = \mathbf{Z}/n\mathbf{Z}$. Soit d un entier > 0 divisant n. Alors G possède un et un seul sous-groupe d'ordre d. Ce sous-groupe C_d est lui-même cyclique d'ordre d (donc isomorphe à $\mathbf{Z}/d\mathbf{Z}$).*

Démonstration : On observe d'abord que $C_d := \{\bar{0}, \overline{n/d}, ..., \overline{(d-1)n/d}\}$ est un sous-groupe d'ordre d de G. Si maintenant H est un sous-groupe d'ordre d de G, le théorème de Lagrange dit que tout élément x de H vérifie $dx = 0$, autrement dit $H \subset C_d$. Comme H et C_d sont tous deux de cardinal d, ceci implique que $H = C_d$.

□

1.5. Sous-groupes distingués, groupes quotients.

Proposition 1.18 *Soient G un groupe et $g \in G$. Alors l'application* $\operatorname{int} g : G \to G$, $h \mapsto ghg^{-1}$ *est un automorphisme de G, appelé automorphisme intérieur associé à g. L'application $g \mapsto \operatorname{int} g$ est un morphisme de groupes de G dans* $(\mathtt{Aut}\, G, \circ)$.

C'est immédiat à vérifier.

Définition 1.19 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 $H \lhd G$.

Noter que si G est abélien, tout sous-groupe de G est distingué, et d'autre part $\{1\}$ 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 1.20 *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).*

Vérification facile, laissée au lecteur.

Exemple 1.21 a) Soit $n \geq 2$. Alors $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$.

b) Si K est un corps, alors $\mathrm{SL}_n(K)$ est distingué dans $\mathrm{GL}_n(K)$.

c) 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 $\mathrm{int} : G \to \mathtt{Aut}\, G$ donc $Z \lhd G$.

d) Considérons dans le groupe $G = \mathcal{S}_n$ (avec $n \geq 3$) le sous-groupe $H = \{\mathrm{Id}, \tau\}$ où τ est la transposition échangeant 1 et 2. On vérifie facilement que si $\sigma \in G$, alors $\sigma\tau\sigma^{-1}$ est la transposition échangeant $\sigma(1)$ et $\sigma(2)$. En choisissant par exemple pour σ une permutation qui envoie 1 sur 3, on voit que H n'est pas distingué dans G.

Remarque 1.22 Attention, $\lhd$ n'est pas une relation transitive, on peut avoir $K \lhd H \lhd G$ et pas $K \lhd G$ (cf. exercices).

Définition 1.23 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. Contrairement à être distingué, être caractéristique est une relation transitive (le vérifier...).

Theorème 1.24 *Soient G un groupe et H un sous-groupe distingué de G. Alors :*

a) Pour tout a de G, on a $aH = Ha$ d'où $G/H = H \setminus G$. Ainsi, deux éléments a et b sont dans la même classe selon H (à gauche ou à droite) si et seulement s'il existe $h \in H$ tel que $a = bh$, ou encore tel que $a = hb$.

b) Il existe une unique structure de groupe sur G/H telle que la surjection canonique $\pi : G \to G/H$ (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 : a) 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 $Ha \subset aH$.

b) 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 a) 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 a), 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 π jointe à la formule $p(xy) = \pi(x)\pi(y)$ pour tous x, y de G.

□

En particulier, on voit que l'élément neutre de G/H est $\bar{e} = H$ et quand G est fini, le cardinal du groupe quotient G/H est $\#G/\#H$. Si G est abélien, on peut 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 π.

Noter que le groupe $\mathbf{Z}/n\mathbf{Z}$ peut être défini comme le quotient de $\mathbf{Z}$ par le sous-groupe $n\mathbf{Z}$.[2]

Theorème 1.25 (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 $f = \tilde{f} \circ \pi$, où π est la surjection canonique $G \to G/\ker f$. De plus $\tilde{f}$ est injectif d'image* $\operatorname{Im} f$.

Noter que $G/\ker f$ 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 $f = \tilde{f} \circ \pi$ d'où $\operatorname{Im} f = \operatorname{Im} \tilde{f}$ par surjectivité de π. Enfin $\bar{a} \in \ker \tilde{f}$ signifie $a \in \ker f$, i.e. $\bar{a} = e_{G/H}$.

□

Remarque 1.26 Plus généralement, si N est un sous-groupe distingué de G inclus dans $\ker f$, on peut factoriser f par un morphisme $\tilde{f} : G/N \to G'$, mais le morphisme $\tilde{f}$ n'est plus injectif en général (son noyau est $\ker f/N$).

Corollaire 1.27 ("Théorème d'isomorphisme I") *Avec les notations du théorème 1.25, on a $G/\ker f \simeq \operatorname{Im} f$.*

2. Définition meilleure que celles qu'on rencontre parfois en classes préparatoires !

Cela résulte de ce que $\tilde{f}$ est un morphisme injectif d'ensemble de départ $G/\ker f$ et d'image $\operatorname{Im} f$.

Proposition 1.28 *Soit G un groupe. Soit H un sous-groupe distingué de G, on note $\pi : G \to G/H$ la surjection canonique. Alors :*

a) Les sous-groupes de G/H sont exactement les N/H, où N est un sous-groupe de G contenant H. De plus $N/H \lhd G/H$ si et seulement si $N \lhd G$.

b) Soit K un sous-groupe de G. Posons $KH = \{kh, k \in K, h \in H\}$ (avec une notation similaire pour HK). Alors on a $KH = HK$, et cet ensemble est un sous-groupe de G qui contient H et K.

Démonstration : a) On vérifie immédiatement que si N est un sous-groupe de G contenant H, alors H (qui est distingué dans G) est a fortiori distingué dans N, et qu'alors $N/H = \pi(N)$ est un sous-groupe de G/H. Réciproquement si A est un sous-groupe de G/H, alors $N := \pi^{-1}(A)$ est un sous-groupe de G contenant H (car A contient le neutre de G/H), et on a bien $A = \pi(N) = N/H$ car π est surjective. Si $A \lhd G/H$, son image réciproque N est un sous-groupe distingué de G, et si $N \lhd G$, alors $A = \pi(N)$ est bien distingué dans $\pi(G) = G/H$.

b) L'égalité $KH = HK$ résulte des identités (valables pour $k \in K, h \in H$) : $kh = (khk^{-1})k$ et $hk = k(k^{-1}hk)$ avec $khk^{-1} \in H$, $k^{-1}hk \in H$ vu que $H \lhd G$. On a alors $1 = 1.1 \in HK$; si $u_1, u_2 \in KH$, on peut écrire $u_1 = k_1h_1$ et $u_2 = h_2k_2$ avec $h_1, h_2 \in H$ et $k_1, k_2 \in K$. Alors $u_1u_2 = k_1h_3k_2$ avec $h_3 = h_1h_2 \in H$; comme $h_3k_2 \in HK = KH$, on peut écrire $h_3k_2 = k_3h_4$ avec $k_3 \in K$ et $h_4 \in H$, ce qui donne que $u_1u_2 = (k_1k_3)h_4 \in KH$. Finalement si $u = kh \in KH$, alors $u^{-1} = h^{-1}k^{-1} \in HK = KH$. Ainsi KH est bien un sous-groupe de G.

□

Theorème 1.29 ("Théorèmes d'isomorphisme") *Soit G un groupe. Soit H un sous-groupe distingué de G et $\pi : G \to G/H$ la surjection canonique.*

a) Pour tout sous-groupe K de G, le le sous-groupe $\pi(K)$ de G/H est aussi le sous-groupe KH/H. Ce dernier est isomorphe à $K/(K \cap H)$ ("deuxième théorème d'isomorphisme").

b) Soit N un sous-groupe distingué de G contenant H. Alors le groupe $(G/H)/(N/H)$ est isomorphe au groupe quotient G/N ("troisième théorème d'isomorphisme").

Ainsi, dans G/H "on obtient un sous-groupe si on diminue G et un quotient si on augmente H."

Démonstration : a) On note déjà que d'après la proposition 1.28, l'ensemble $KH = HK$ est bien un sous-groupe de G contenant H. Soit $u = kh \in KH$. Alors on a $\pi(u) = \pi(k) \in \pi(K)$ car $\pi(h)$ est le neutre de G/H, d'où $KH/H \subset \pi(K)$. Réciproquement, tout élément de $\pi(K)$ est de la forme $\bar{k}$ avec $k \in K \subset KH$, il est donc a fortiori dans KH/H. Soit alors $\varphi : K \to KH/H$ le morphisme de groupes défini par $\varphi(k) = \bar{k} = \pi(k)$. Son noyau est clairement $K \cap H$ car $\ker \pi = H$. Comme $\pi(K) = KH/H$, on voit que φ est surjectif, et le théorème de factorisation donne alors $K/K \cap H \simeq KH/H$.

b) Soit $\psi : G/H \to G/N$ le morphisme de groupes défini par $\psi(\bar{g}) = \tilde{g}$, où $\tilde{g}$ désigne l'image de g dans G/N. Cette définition a un sens car si g, g' sont des éléments de G avec $\bar{g} = \bar{g}'$, alors $g^{-1}g' \in H \subset N$ donc $\tilde{g} = \tilde{g}'$. On voit immédiatement que ψ est surjectif de noyau N/H, d'où le résultat avec le théorème de factorisation.

□

Dans le cas abélien, le deuxième théorème d'isomorphisme s'écrit :

Corollaire 1.30 *Soit $(A, +)$ un groupe abélien. Soient B un sous-groupe de A et $\pi : A \to A/B$ la surjection canonique. Alors, pour tout sous-groupe C de A, on a $\pi(C) = (B+C)/B$, et ce dernier groupe est isomorphe à $B/(B \cap C)$.*

1.6. Sous-groupe dérivé

Définition 1.31 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. [3] On le note $D(G)$.

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

Proposition 1.32 *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 distingué 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 de G, alors G/H est un quotient de G^{ab} (cela résulte immédiatement de $D(G) \subset H$ et du troisième théorème d'isomorphisme), ou encore G^{ab} se surjecte sur G/H.

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

Démonstration : Commençons par un lemme utile en soi : si A est une partie d'un groupe G et si $\varphi : G \to G'$ est un morphisme de groupes, alors $\varphi(\langle A\rangle) = \langle\varphi(A)\rangle$. En effet, tout élément de $\langle A\rangle$ peut s'écrire $x = a_1...a_r$ avec $a_i \in A$ ou $a_i^{-1} \in A$ pour tout i ; du coup on a $\varphi(x) = \varphi(a_1)...\varphi(a_r)$, avec $\varphi(a_i) \in \varphi(A)$ ou $\varphi(a_i)^{-1} \in \varphi(A)$ pour chaque i, ce qui montre que $\varphi(x) \in \langle\varphi(A)\rangle$. Ainsi $\varphi(\langle A\rangle) \subset \langle\varphi(A)\rangle$ et l'inclusion dans l'autre sens se montre de façon tout à fait analogue.

Si maintenant φ est un automorphisme de G, alors on a $\varphi([x,y]) = [\varphi(x),\varphi(y)]$ d'où $\varphi(D(G)) \subset D(G)$ avec le lemme, ce qui montre que $D(G)$ est caractéristique. Le groupe $G/D(G)$ est abélien car par définition, on a $xyx^{-1}y^{-1} \in D(G)$ pour tous $x, y \in G$, ce qui montre que dans $G/D(G)$ on a $\bar{x}\bar{y} = \bar{y}\bar{x}$. Si H est un sous-groupe tel que G/H soit abélien, alors on a $\overline{xyx^{-1}y^{-1}} = \bar{1}$ 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.

□

Remarque 1.33 On vérifie facilement que tout sous-groupe N contenant $D(G)$ est automatiquement distingué (et on peut donc parler du groupe quotient G/N, qui est abélien).

Par exemple $D(G) = \{e\}$ si et seulement si G est abélien. Pour $n \geq 2$, on a $D(\mathcal{S}_n) = \mathcal{A}_n$ et $D(\mathcal{A}_n) = \mathcal{A}_n$ pour $n \geq 5$ (voir un peu plus loin). Si K est un corps et $n \geq 2$, on a $D(\mathrm{GL}_n(K)) = \mathrm{SL}_n(K)$ sauf si on a simultanément $n = 2$ et $\#K = 2$; on a aussi $D(\mathrm{SL}_n(K)) = \mathrm{SL}_n(K)$ sauf si on a à la fois $n = 2$ et $\#K \leq 3$ (voir par exemple le cours d'algèbre de D. Perrin [2], chapitre 4).

Définition 1.34 Un groupe G est dit *simple* si ses seuls sous-groupes distingués sont G et $\{e\}$, *parfait* si $D(G) = G$.

Exemple 1.35 a) 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.

b) Le groupe $\mathcal{A}_n$ est simple si $n \geq 5$ (voir plus loin).

c) En général $\mathrm{SL}_n(K)$ n'est pas simple car son centre (constitué des homothéties λI avec $\lambda^n = 1$) est non trivial si K contient des racines n-ièmes de l'unité autre que 1, par exemple si $K = \mathbf{C}$. Par contre $\mathrm{SL}_n(K)$ est parfait si l'on n'est pas dans l'un des deux cas exceptionnels ($n = 2$ et K fini de cardinal 2 ou 3).

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 $1.x = x$

Remarque 2.2 a) 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 $g.x = (\Phi(g))(x)$.

b) 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" (i.e. une application Φ qui vérifie $\Phi(gg') = \Phi(g')\Phi(g)$ pour tous g, g') de G vers $\mathcal{S}(X)$ au lieu d'un morphisme.

Exemple 2.3 a) 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.

b) 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 $\mathtt{Aut}\, G$ (ce qui n'était pas le cas dans l'exemple précédent). On parle dans ce cas d'*action par automorphismes*.

c) $\mathcal{S}_n$ opère sur $\{1, ..., n\}$ par $\sigma.x = \sigma(x)$.

d) Si H est un sous-groupe de G, G opère sur l'ensemble des classes à gauche G/H par $g.(aH) := (ga)H$. Noter qu'il opère aussi à droite sur l'ensemble des classes à droite par $(Ha).g := H(ag)$.

Définition 2.4 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.

Exemple 2.5 a) Si H est un sous-groupe de G, les orbites de l'action de H sur G par translation à gauche ne sont autre que les classes à **droite** suivant H.

b) L'action de $\mathcal{S}_n$ sur $\{1, ..., n\}$ est transitive.

c) L'action de G sur G/H vue plus haut est transitive, ainsi que celle de G sur lui-même par translations.

d) Les orbites pour l'action de G sur lui-même par conjugaison s'appellent les *classes de conjugaison* de G. Noter que si G n'est pas le groupe trivial, l'action n'est jamais transitive vu que 1 est seul dans son orbite.

Définition 2.6 Soit G un groupe opérant sur un ensemble X. On appelle *stabilisateur* d'un élément x de X le sous-groupe Stab_x des g de G qui vérifient $g.x = x$. Il n'est pas distingué dans G en général.

On dit que l'opération est *libre* si tous les stabilisateurs Stab_x (pour $x \in X$) sont réduits à $\{1\}$. On dit que l'action est *fidèle* (ce qui est nettement moins fort) si le morphisme $G \to \mathcal{S}(X)$ associée à l'opération est injectif, autrement dit si $\bigcap_{x\in X} \mathrm{Stab}_x = \{1\}$.

Exemple 2.7 a) L'opération d'un groupe G sur lui-même par translation à gauche est libre (donc a fortiori fidèle). Si G est fini d'ordre n, on obtient en particulier qu'il existe un morphisme injectif (donné par cette opération) de G dans $\mathcal{S}(G) \simeq \mathcal{S}_n$ (théorème de Cayley).

b) Dans l'opération de $\mathcal{S}_n$ sur $\{1, ..., n\}$, tous les stabilisateurs sont isomorphes à $\mathcal{S}_{n-1}$. Ils sont du reste tous conjugués, ce qui est un fait général pour une action transitive : en effet, quand un groupe G opère sur un ensemble X et x, y sont dans la même orbites, alors Stab_x et $\mathrm{Stab}\, y$ sont conjugués vu que si $y = g.x$, alors $\mathrm{Stab}_y = g\mathrm{Stab}_x g^{-1}$.

La proposition ci-dessous va montrer que l'exemple 2.5 c) ci-dessus est en quelque sorte le cas "générique" d'une action transitive.

Proposition 2.8 *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/Stab_x sur l'orbite $\omega(x)$ de x via : $\bar{g} \mapsto g.x$. En particulier si G est fini on a $\#\,\omega(x) = \#G/\#\mathrm{Stab}_x$ (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/Stab_x par translation à gauche.*

Noter que sans supposer G fini, on obtient que le cardinal de l'orbite $\omega(x)$ est celui de l'indice $[G : \mathrm{Stab}_x]$, lequel est donc fini si et seulement si $\omega(x)$ est finie.

Démonstration : Déjà l'application $\varphi : \bar{g} \mapsto g.x$ de G/Stab_x vers X est bien définie car si $\bar{g} = \bar{g}'$, alors $g' = g.h$ avec $h \in \mathrm{Stab}_x$, 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. $g'^{-1}g \in \mathrm{Stab}_x$, ou encore $\bar{g}' = \bar{g}$ dans G/Stab_x, ce qui prouve l'injectivité de φ.

□

Corollaire 2.9 (Équation aux classes) *Soit G un groupe fini opérant sur un ensemble fini X. Soit Ω l'ensemble des orbites, notons $\#\mathrm{Stab}_\omega$ 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*

$$\#X = \sum_{\omega \in \Omega} \frac{\#G}{\#\mathrm{Stab}_\omega}.$$

Démonstration : Comme les orbites forment une partition de X, c'est immédiat d'après la proposition précédente.

□

Remarque 2.10 Malgré la simplicité de la démonstration, l'équation aux classes a des conséquences tout à fait non triviales, comme on va le voir au paragraphe suivant. Noter que cette équation aux classes est valable dès que l'ensemble X est fini (sans supposer forcément G fini), à condition de remplacer $\frac{\#G}{\#\mathrm{Stab}_\omega}$ par l'indice $[G : \mathrm{Stab}_\omega]$ du stabilisateur Stab_ω dans G, lequel est bien fini puisque c'est aussi le cardinal de l'orbite ω.

2.2. p-groupes ; théorèmes de Sylow

Définition 2.11 Soit p un nombre premier. On appelle *p-groupe* un groupe de cardinal p^n, où $n \in \mathbf{N}$.

Notons que nous adoptons ici la convention selon laquelle le groupe trivial est bien un p-groupe.

Proposition 2.12 *Soit G un p-groupe non trivial. Alors :*

a) Si G est de cardinal p, alors G est cyclique.
b) Le centre Z de G n'est pas trivial.
c)Si G est de cardinal p ou p^2, alors p est abélien.

Démonstration : a) Soit $x \in G$ un élément autre que le neutre. Alors son ordre divise p d'après le théorème de Lagrange, donc c'est p puisque ce n'est pas 1. Cela signifie que le groupe engendré par x est de cardinal p, donc c'est G tout entier et G est cyclique.

b) On fait opérer G sur lui-même par conjugaison. Il y a $\#Z$ *points fixes* (:=orbites réduites à un élément), et le cardinal des autres orbites est un diviseur de $p^n := \#G$ (par le théorème de Lagrange) autre que 1, donc est divisible par p. Ainsi, on obtient (via l'équation aux classes) que le nombre

$\#G = p^n$ (avec $n > 0$) est la somme du cardinal de Z et d'un multiple de p, donc p divise $\#Z$.

c) Si G est de cardinal p, le résultat est immédiat avec a) puisqu'alors G est isomorphe à $\mathbf{Z}/p\mathbf{Z}$. Supposons que G soit de cardinal p^2. Si G n'était pas abélien, le cardinal de Z serait p d'après b), donc G/Z serait cyclique (car de cardinal p). Mais on obtient alors une contradiction via le lemme suivant :

Lemme 2.13 *Soit G un groupe de centre Z avec G/Z monogène. 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, voir exercices) mais dans le cas particulier des p-sous-groupes, on va voir qu'on a une réponse positive.

Définition 2.14 *Soit p un nombre premier. Soit G un groupe fini de cardinal n. On appelle p-sous-groupe de Sylow (ou plus simplement p-Sylow de G) 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 l'indice $[G : H]$ de H dans G).*

Si p ne divise pas $\#G$, un p-Sylow de G est simplement le sous-groupe trivial (dans ce cas, la notion n'est pas intéressante). On observera que H est un p-Sylow de G si et seulement s'il vérifie les deux conditions : H est un p-groupe et p ne divise pas l'indice $[G : H]$.

Theorème 2.15 (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 2.16 *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).

Démonstration : On a vu que le sous-groupe H de G 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 l'action de H 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.

□

Lemme 2.17 *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.*

Démonstration : On calcule d'abord le cardinal de G_p. C'est celui du nombre de bases du $\mathbf{F}_p$-espace vectoriel $\mathbf{F}_p^n$: en effet si on fixe une base $\mathcal{B}_0$ de $\mathbf{F}_p^n$ (par exemple la base canonique), il existe pour toute base $\mathcal{B}$ de $\mathbf{F}_p^n$ un et un seul élément de G_p qui envoie $\mathcal{B}_0$ sur $\mathcal{B}$. De ce fait, le cardinal de G_p est

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

car pour le premier vecteur e_1 de $\mathcal{B}$ on a $p^n - 1$ choix (tout vecteur non nul), pour le deuxième e_2 on a $p^n - p$ choix (tout vecteur non multiple de e_1) etc. Il en 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.

□

Preuve du premier théorème de Sylow : 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. [4]

□

Avant d'énoncer et démontrer un théorème sur la conjugaison des p-Sylow, voici une notion souvent utile en théorie des groupes :

Définition 2.18 Soit G un groupe. Soit H un sous-groupe de G. Le *normalisateur* de H dans G est le sous-groupe $N_G(H)$ de G constitué des $g \in G$ vérifiant $gHg^{-1} = H$.

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

Il est facile de vérifier que $N_G(H)$ est bien un sous-groupe de G et qu'il contient H. Par définition on a $N_G(H) = G$ si et seulement si H est distingué dans G. Si H est fini, tout élément de g vérifiant $gHg^{-1} \subset H$ est dans $N_G(H)$ (en effet gHg^{-1} et H ont même cardinal), mais ce n'est plus vrai en général.

Theorème 2.19 (Deuxième théorème de Sylow) *Soit G un groupe fini de cardinal $n = p^\alpha m$ avec p ne divisant pas m. Alors :*

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

b) Les p-Sylow de G sont tous conjugués, et leur nombre k divise n. En particulier, si un p-Sylow est distingué, c'est le seul p-Sylow de G.

c) On a k congru à 1 modulo p (et donc k divise m).

On peut montrer qu'un groupe G comme ci-dessus possède des sous-groupes d'ordre p^β pour tout $\beta \leq \alpha$ et pas seulement pour $\beta = \alpha$ (voir exercices), le premier théorème de Sylow permettant de se ramener au cas où G est lui-même un p-groupe.

Démonstration : a) D'après le premier théorème de Sylow, il existe au moins un p-Sylow S de G. Le lemme 2.16 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.

b) 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, le cardinal k de cette orbite (qui divise celui de G) est celui de X, i.e. le nombre de p-Sylow.

c) 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,

car le normalisateur $N_G(T)$ contient S et T, donc aussi le sous-groupe qi'ils engendrent, ce qui implique $N \subset N_G(T)$. Finalement on a bien $T = S$. [5]

□

Un cas particulier important de c) 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 (prendre $p = 7$) n'est pas simple. Le même type de raisonnement marche pour un groupe d'ordre 255.

Exemple 2.20 Le groupe $\mathcal{A}_4$ est de cardinal 12. Il possède un 2-Sylow distingué d'ordre 4, constitué de l'identité et des doubles transpositions, qui est donc son seul 2-Sylow. Le 3-cycle $(1, 2, 3)$ est un 3-Sylow de G ; les autres s'obtiennent par conjugaison, ce qui fait que les 3-Sylow sont exactement les 3-cycles de G.

3. Groupes simples, exemple du groupe alterné

Un groupe non trivial est *simple* si ses seuls sous-groupes distingués non triviaux sont lui-même et $\{1\}$. Par exemple, les groupes simples abéliens sont les $\mathbf{Z}/p\mathbf{Z}$ avec p premier. Il n'est pas a priori facile de trouver d'autres exemples de groupes simples (voir [2], IV.4 pour l'exemple du groupe $\mathrm{PSL}_n(K)$ quand $n \geq 3$ ou le corps K possède au moins quatre éléments). Le but de ce paragraphe est de démontrer :

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 ; voir TD).

5. Ce raisonnement s'appelle "l'argument de Frattini".

Démonstration : On a $D(\mathcal{S}_n) \subset \mathcal{A}_n$ vu que tout commutateur est de signature 1, et $D(\mathcal{S}_n)$ est 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, vu que $D(\mathcal{S}_n)$ n'est pas réduit au neutre (en effet $\mathcal{S}_n$ n'est pas abélien). On a de même $D(\mathcal{A}_n)$ distingué dans $\mathcal{A}_n$ et non trivial (deux 3-cycles dont les supports ont un ou deux éléments en commun ne commutent pas), d'où $D(\mathcal{A}_n) = \mathcal{A}_n$.

□

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 si $\sigma \neq \sigma^{-1}$ parce qu'alors H est de cardinal 3, et 2 ne divise pas 3. Finalement H est de cardinal 1 ou 2 ; mais un sous-groupe de cardinal 2 de $\mathcal{S}_n$ est de la forme $\{\mathrm{Id}, \tau\}$ où τ est un produit de transpositions dont les supports sont disjoints, donc un tel sous-groupe ne peut pas être distingué si $n \geq 3$ par un calcul facile.

□

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

Lemme 3.4 *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 $(a, b)(b, c) = (a, b, c)$, et $(a, b)(c, d) = (a, b)(a, c)(a, c)(c, d) = (a, c, b)(a, c, d)$, donc un produit de deux transpositions est un 3-cycle ou un produit de deux 3-cycle.

□

Lemme 3.5 *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 distingué 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 3.6 *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 $4! = 24$, car se donner un 5-cycle c revient à se donner $c(1)$ (4 choix), puis $c^2(1)$ (3 choix) etc.

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 $\mathcal{A}_5$ [6], 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

6. 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.

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.

□

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).

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 note aussi que ρ opère non trivialement sur F car $\rho(b) = \tau\sigma(b) \neq b$ (vu que $\sigma(b) \neq c = \tau^{-1}(b)$).

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

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

Proposition 4.1 *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* $\mathbf{Z}/n\mathbf{Z}$.

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. $n = 8$). Attention aussi à ne pas écrire "x est premier avec n" pour un élément x de $\mathbf{Z}/n\mathbf{Z}$ (au lieu d'un représentant entier de x), la notion d'éléments premiers entre eux n'ayant pas de sens dans un anneau non intègre.

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 4.2 *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 :*

a) 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 $\alpha \geq 1$.

b) Le groupe $\mathtt{Aut}\,(\mathbf{Z}/n\mathbf{Z})$ des automorphismes du groupe additif[7] *$\mathbf{Z}/n\mathbf{Z}$ est isomorphe au groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$.*

c) 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

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

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

b) 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.

7. 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 $\bar{1}$.

c) 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 [8]. La deuxième assertion est immédiate en écrivant que deux anneaux isomorphes ont des groupes d'inversibles isomorphes.

d) résulte de a) et c).

□

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 $\alpha = 1$.

Theorème 4.3 *Soient K un corps [9] et G un sous-groupe fini du groupe multiplicatif K^*. Alors G est cyclique.*

Démonstration : On utilise le lemme suivant :

Lemme 4.4 *Soit $n \in \mathbf{N}^*$, alors*

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

Le lemme est une conséquence immédiate du fait que les éléments d'ordre d dans $\mathbf{Z}/n\mathbf{Z}$ sont forcément dans l'unique sous-groupe C_d de $\mathbf{Z}/n\mathbf{Z}$ qui est de cardinal d ; or, comme C_d est isomorphe à $\mathbf{Z}/d\mathbf{Z}$, il contient $\varphi(d)$ éléments d'ordre d, donc finalement $\mathbf{Z}/n\mathbf{Z}$ contient $\varphi(d)$ éléments d'ordre d ; d'où le lemme en triant les éléments de $\mathbf{Z}/n\mathbf{Z}$ suivant leur ordre.

Revenons à la preuve du théorème 4.3. 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 d'ordre d, c'est-à-dire en tout cas au plus $\varphi(d)$ éléments

8. C'est une des formulations du "lemme chinois".

9. 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. 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 4.5 *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 (cas particulier de la proposition 4.1). Notons que déterminer explicitement un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ est un problème algorithmique en général difficile.

On passe maintenant au cas général.

Theorème 4.6 *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 au groupe additif $\mathbf{Z}/p^{\alpha-1}(p-1)\mathbf{Z}$).*

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 4.7 *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}), ce qui implique que

$$1 + C_p^2 + ... + p^{p-2}$$

n'est pas divisible par p.

Supposons le résultat vrai pour k, 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 que

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

n'est pas divisible par p par hypothèse de récurrence, ce qui montre le lemme.

□

On aura besoin aussi d'un lemme classique sur les groupes abéliens :

Lemme 4.8 *Soit G un groupe abélien, noté multiplicativement. Soit $x \in G$ un élément d'ordre a et $y \in G$ un élément d'ordre b. Si a et b sont premiers entre eux, alors l'ordre de xy est ab.*

Noter que le résultat est faux si on ne suppose pas a et b premiers entre eux (prendre $y = x^{-1}$) et il est également faux dans un groupe non abélien si x et y ne commutent pas (prendre une transposition et un 3-cycle dans $\mathcal{S}_3$).

Preuve du lemme 4.8 : Soit $n \in \mathbf{N}^*$ tel que $(xy)^n = 1$, alors $x^n = y^{-n}$, d'où $y^{-na} = 1$ et b divise na. Comme b est premier avec a, on obtient que b divise n et de même a divise n, d'où ab divise n (toujours parce que $(a, b) = 1$). Comme par ailleurs $(xy)^{ab} = 1$, on voit que l'ordre de xy est bien ab.

□

Preuve du théorème 4.6 : D'après le lemme 4.7, 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 4.5) 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 $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ par le lemme 4.8.

□

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

Theorème 4.9 *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 $2^{\alpha-2}$, autrement dit le sous-groupe N engendré par $\bar{5}$ est de cardinal $2^{\alpha-2}$. Son intersection avec le sous-groupe $C = \{\pm\bar{1}\}$ est $\bar{1}$, car toute puissance de 5 (contrairement à -1) est congrue à 1 modulo 4. Il en résulte que $(n, c) \mapsto nc$ est un morphisme injectif de $N \times C$ dans $(\mathbf{Z}/2^\alpha\mathbf{Z})^*$, et c'est donc un isomorphisme par cardinalité. On conclut en observant que N est isomorphe au groupe additif $\mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ et C au groupe additif $\mathbf{Z}/2\mathbf{Z}$.

□

5. Produit semi-direct

Soit N un groupe. L'ensemble $\mathtt{Aut}\, N$ des automorphismes de groupe de N est lui-même un groupe pour la loi $\circ$. Par exemple si n est un entier ≥ 2, le groupe des automorphismes du groupe additif $\mathbf{Z}/n\mathbf{Z}$ est isomorphe au groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^*$ des éléments inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$. Si p est un nombre premier, le groupe des automorphismes du groupe abélien $(\mathbf{Z}/p\mathbf{Z})^r$ est le groupe multiplicatif $\mathrm{GL}_r(\mathbf{Z}/p\mathbf{Z})$.

Soient N et H deux groupes. Le produit semi-direct est une généralisation de la notion de produit direct $N \times H$. Soit $\varphi : H \to \mathtt{Aut}\, N$ 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 5.1 *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 $(h^{-1}.n^{-1}, h^{-1})$ (pour voir que c'est un inverse aussi à gauche, on utilise $(h^{-1}.n^{-1})(h^{-1}.n) = h^{-1}.(n^{-1}n) = h^{-1}.1 = 1$).

Il reste à vérifier l'associativité. Or 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. □

Remarque 5.2 a) 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.

b) L'action triviale correspond au produit direct.

Définition 5.3 Si H et N sont deux groupes, on dit qu'un groupe G est une *extension de*[10] H *par* N s'il existe une suite exacte courte

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

ce qui signifie qu'on a un morphisme surjectif de G dans H dont le noyau est $i(N)$ (lequel est isomorphe à N).

Proposition 5.4 *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)[11] *dans G. Ainsi un produit semi-direct de N par H est une extension de H par N.*

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.*

10. Certains auteurs, par exemple D. Perrin, disent plutôt extension de N par H.

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

Démonstration : 1. Les applications i et p 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 5.5 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 5.6 *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 $\Phi((n,h)(n',h')) = \Phi(n(hn'h^{-1}),hh') = (nh)(n'h')$. 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.

Exemple 5.7

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 $\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbf{Z}/2\mathbf{Z}$. Noter que $\mathcal{S}_n$ n'est pas isomorphe au produit direct $\mathcal{A}_n \times \mathbf{Z}/2\mathbf{Z}$, car $\mathcal{S}_n$ ne possède pas de sous-groupe distingué d'ordre 2.

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 $\mathrm{GL}_n(K) \simeq \mathrm{SL}_n(K) \rtimes K^*$. Ici, encore, ce n'est pas isomorphe au produit direct en général (exercice, pas évident...).

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. [12]

4. Soit $n \geq 3$, on note D_n le *groupe diédral* des isométries du plan conservant un polygone régulier convexe à n côtés. Il est de cardinal $2n$; plus

12. 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 !).

précisément D_n contient les n rotations de centre O (le centre du polygone) et d'angle $2k\pi/n$ ($0 \leq k \leq n-1$) et n réflexions par rapport aux droites passant : par O et chaque sommet (si n est impair), par O et chaque sommet ou milieu d'un côté (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 $D_n \simeq \mathbf{Z}/n\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$ (non isomorphe au produit direct car D_n n'est pas abélien). Notons que l'action correspondante de $\mathbf{Z}/2\mathbf{Z}$ sur $\mathbf{Z}/n\mathbf{Z}$ consiste à poser $\varepsilon.x = -x$ pour $x \in \mathbf{Z}/n\mathbf{Z}$.

5. Si p et q sont des nombres premiers avec $p < q$, les groupes d'ordre pq sont tous cycliques si p ne divise pas $q-1$ (c'est une application classique des théorèmes de Sylow, cf. [2], Th. I.7.13, 1)). Si par contre p divise $q-1$, on a de plus un produit semi-direct non commutatif $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$, via le fait qu'il y a des morphismes non triviaux $\mathbf{Z}/p\mathbf{Z} \to \mathtt{Aut}\,(\mathbf{Z}/q\mathbf{Z}) \simeq \mathbf{Z}/(q-1)\mathbf{Z}$ (il faut un peu plus d'efforts pour montrer qu'il n'y a qu'un tel produit semi-direct non commutatif à isomorphisme près, voir [2], Lemme 8.12 et Th. I.7.13, 2)).

6. Si p est un nombre premier impair, il y a deux groupes non commutatifs d'ordre p^3, qui sont des produits semi-directs de groupes plus petits ([2], exercice IE8). Le cas $p = 2$ est exceptionnel : le groupe diédral est le seul produit semi-direct non trivial d'ordre 8, et on a de plus le groupe des quaternions H_8, qui ne se décompose pas en produit semi-direct de groupes plus petits ([2], exercice IE1). En effet, si on avait H_8 isomorphe à $N \rtimes H$ avec N et H de cardinal < 8, alors N et H seraient abéliens (car de cardinal ≤ 4) ; mais alors, pour ne pas avoir le produit direct (qui donnerait un groupe abélien), il faudrait N de cardinal 4 (pour que $\mathtt{Aut}\,N$ soit non trivial), soit en l'occurrence isomorphe à $\mathbf{Z}/4\mathbf{Z}$, mais le seul produit semi-direct non trivial avec $H \simeq \mathbf{Z}/2\mathbf{Z}$ donne alors le groupe diédral et non H_8.

Références

[1] M. Hall Jr : *The theory of groups*, The Macmillan Co., New York, N.Y. 1959.

[2] D. Perrin : *Cours d'algèbre*, Ellipses 1996.

[3] J-P. Serre : *Représentations linéaires des groupes finis*, Hermann, Paris, 1967.