M1 2021-2022 : GROUPES

David Harari

Table des matières

1. Quelques rappels

Il s'agit principalement ici de rappels de L3, on ira donc assez vite et sans détailler la plupart des démonstrations. On suppose déjà connues les notions de groupe, de sous-groupe, et de morphisme de groupes.

1.1. Notations, premières propriétés

Les lois de groupes seront en général notées multiplicativement. En particulier, l'élément neutre d'un groupe G sera le plus souvent noté 1 et le symétrique d'un élément x sera noté x^{-1}. Pour $n > 0$, on pose $x^n = x.x...x$

(n termes), avec les conventions $x^0 = 1$ et $x^{-n} = (x^n)^{-1}$. Si le groupe G est abélien (c'est-à-dire commutatif), on notera parfois $+$ 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 $(-n)x = n(-x)$.

Remarque 1.1 On se gardera 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 $y^{-1}x$.

Exemple 1.2 a) Le groupe trivial $G = \{0\}$.

b) $(\mathbf{R}, +)$ 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].

c) $G = (\mathbf{Z}/n\mathbf{Z}, +)$, où $n \in \mathbf{N}^*$. Il est d'*ordre* (i.e. de cardinal) n. On abrégera parfois $\mathbf{Z}/n\mathbf{Z}$ en $\mathbf{Z}/n$. Le groupe additif $\mathbf{Z}$ est quant à lui infini.

d) 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.

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.

Définition 1.3 Soit $f : G \to G'$ un morphisme de groupes. Si f est bijectif, 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.

Remarque 1.4 a) On dit parfois "homomorphisme" au lieu de morphisme.

b) L'ensemble $\mathtt{Aut}\, G$ des automorphismes de G, muni de la composition $\circ$ des applications, est un sous-groupe de $\mathcal{S}(G)$. Il peut être non commutatif

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.

même si G l'est (ex. $G = \mathbf{Z}/2 \times \mathbf{Z}/2$, le vérifier en observant que $\mathtt{Aut}\, G$ est isomorphe à $GL_2(\mathbf{Z}/2)$).

c) On notera parfois $G \simeq H$ pour "G est isomorphe à H."

On rappelle :

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 $\ker f := f^{-1}(\{1\})$ 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.*

Exemple 1.6 Voici quelques exemples de sous-groupes et de morphismes de groupes :

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

b) 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.

c) 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]

d) 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. Le noyau de la signature est un sous-groupe de $\mathcal{S}_n$, le *groupe alterné* $\mathcal{A}_n$

e) 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. Le noyau du déterminant est un sous-groupe de $\mathrm{GL}_n(K)$, appelé *groupe spécial linéaire*. On le note $\mathrm{SL}_n(K)$.

f) 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).

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

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 $x \bullet y = yx$.

h) Si $(A,+)$ est un groupe abélien et $n \in \mathbf{N}^*$, alors l'ensemble $A[n]$ des x de A qui vérifient $nx = 0$ est un sous-groupe de A, appelé *sous-groupe de n-torsion*. Le groupe $A_{\text{tors}} := \bigcup_{n\in\mathbf{N}^*} A[n]$ est également un sous-groupe[3] de A, appelé *sous-groupe de torsion* de A. 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 $\{0\}$. Celui de $(\mathbf{R}^*,\times)$ est $\{\pm 1\}$, celui de $\mathbf{C}^*$ est le groupe multiplicatif de toutes les racines de l'unité.

1.2. Générateurs d'un groupe, théorème de Lagrange

Proposition 1.7 *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 $\langle A\rangle$.*

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 $\langle A\rangle = \{1\}$).

□

Remarque 1.8 Si G est un groupe abélien (noté additivement), la description de $\langle A\rangle$ est plus simple : c'est l'ensemble des $\sum_{i=1}^m n_i a_i$ avec $n_i \in \mathbf{Z}$ et $a_i \in A$ (l'entier m pouvant être quelconque), autrement dit l'ensemble des $\sum_{a\in A} n_a a$, où $(n_a)_{a\in A}$ est une famille presque nulle d'entiers. Attention, ceci ne s'étend pas au cas où A n'est pas abélien (par exemple on ne peut pas simplifier une expression du genre xyx dans un groupe non abélien).

Définition 1.9 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. L'ordre de g est aussi le cardinal du sous-groupe $\langle g\rangle$ engendré par g.

Rappelons en particulier :

Proposition 1.10 *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 $\mathbf{Z}/n\mathbf{Z}$.*

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 $(mn)x = 0$.

Définition 1.11 Un groupe est dit *monogène*[4] s'il est engendré par un seul élément, *cyclique* s'il est de plus fini. En particulier, 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.

On a le très important résultat suivant :

Theorème 1.12 (Th. de Lagrange) *Soit G un groupe fini. Alors l'ordre de tout sous-groupe de H de G divise l'ordre de G. En particulier, l'ordre de tout élément de G est fini et divise l'ordre de G.*

(Le théorème se démontre en regardant l'ensemble des classes à gauche aH pour $a \in G$, qui constituent une partition de G ; or le cardinal de chaque classe aH est le même que celui de H puisque les translations à gauche sont des bijections de G sur G).

Proposition 1.13 *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 $H = C_d$.

□

Exemple 1.14 a) Le groupe $(\mathbf{Z}^n, +)$ est engendré par la famille

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

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 *renversements* (i.e. les symétries orthogonales par rapport à un sous-espace de codimension 2). Voir par exemple [2], chapitre VI, pour des démonstrations de ces énoncés.

d) Le groupe $(\mathbf{Q}, +)$ n'est pas engendré par une partie finie (exercice !).

4. En anglais, on appelle parfois cyclique un groupe engendré par un seul élément, même s'il est infini.

1.3. Sous-groupes distingués, groupes quotients.

Rappelons d'abord une proposition dont la vérification est immédiate :

Proposition 1.15 *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 $(\mathtt{Aut}\, G, \circ)$. Si on fixe $x \in G$, les éléments de G de la forme gxg^{-1} (avec $g \in G$) sont appelés conjugués de x.*

Définition 1.16 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 $H \lhd G$.

Remarque 1.17 a) $H \lhd G$ 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}).

b) Si G est abélien, tout sous-groupe de G est distingué.

c) $\{1\}$ et G sont toujours des sous-groupes distingués de G.

d) Attention, la notion de sous-groupe distingué est relative (H est toujours distingué dans lui-même).

Exemple 1.18 a) 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.

b) Soit $n \geq 2$. Alors $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ en tant que noyau de la signature.

c) Si K est un corps commutatif, alors $\mathrm{SL}_n(K)$ est distingué dans $\mathrm{GL}_n(K)$ en tant que noyau du déterminant.

d) 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 $\mathcal{S}_n$ (choisir σ tel que $\sigma(a) = c$ avec c distinct de a et b).

Remarque 1.19 Attention, $\lhd$ n'est pas une relation transitive, on peut avoir $K \lhd H \lhd G$ et pas $K \lhd G$. Soit par exemple $V_4 \subset \mathcal{S}_4$ 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 $\mathcal{S}_4$, abélien car isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, et contenant des sous-groupes d'ordre 2 (les sous-groupes engendrés par l'une des double-transpositions) qui ne sont pas distingués dans $\mathcal{S}_4$ mais sont bien sûr distingués dans le groupe abélien V_4.

Définition 1.20 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 groupe $\mathcal{A}_3$ est caractéristique dans $\mathcal{S}_3$ car tout automorphisme de $\mathcal{S}_3$ doit envoyer un 3-cycle sur un élément d'ordre 3, donc sur un autre 3-cycle. On verra un peu plus loin deux exemples généraux de sous-groupes caractéristiques d'un groupe G, son centre et son sous-groupe dérivé (on verra aussi que $\mathcal{A}_n$ est le sous-groupe dérivé de $\mathcal{S}_n$).

Remarque 1.21 Si K est caractéristique dans H et H est caractéristique dans G, on vérifie facilement (exercice !) que K est caractéristique dans G.

Voici une notion souvent utile en théorie des groupes, étroitement liée à celle de sous-groupe distingué.

Définition 1.22 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 $gHg^{-1} = H$.

Il est facile de vérifier que $N_G(H)$ est bien un sous-groupe de G et qu'il contient H. C'est le plus grand sous-groupe de G dans lequel H est distingué, et 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.

On passe maintenant aux groupes quotients. Rappelons que si H est un sous-groupe d'un groupe G, alors l'ensemble des classes à gauche G/H (resp. des classes à droite $H \setminus G$) est l'ensemble des aH (resp. des Ha) pour $a \in G$; c'est aussi l'ensemble quotient de G pour la relation d'équivalence $x \sim y$ si $x^{-1}y \in H$ (resp. $xy^{-1} \in H$).

Theorème 1.23 *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 $G/H = H \setminus G$.

b) 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 : 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 p jointe à la formule $p(xy) = p(x)p(y)$ pour tous x, y de G.

□

Remarque 1.24 a) L'élément neutre de G/H est $\bar{1} = H$.

b) 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.

c) Le groupe $\mathbf{Z}/n\mathbf{Z}$ est le quotient de $\mathbf{Z}$ par le sous-groupe $n\mathbf{Z}$.

d) Si H est un sous-groupe d'un groupe G, l'ensemble G/H est en bijection avec $H \backslash G$ 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, qu'on appelle *l'indice* de H dans G ; c'est simplement $\#G/\#H$ si G est fini.

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 $f = \tilde{f} \circ p$. De plus $\tilde{f}$ est injectif d'image* $\operatorname{Im} f$*, i.e. $G/\ker f \simeq \operatorname{Im} f$ ("premier théorème d'isomorphisme"). En particulier, quand G est fini, on a*

$$\#G = \#\ker f \#\operatorname{Im} f.$$

Démonstration (esquisse): Nécessairement, l'application $\tilde{f}$ 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 $f(a) = f(b)f(n) = f(b)$. Les autres propriétés se vérifient alors immédiatement.

□

Remarque 1.26 Si N est un sous-groupe distingué de G inclus dans $\ker f$, alors f se factorise encore par un morphisme $\tilde{f} : G/N \to G'$ d'image $\operatorname{Im} f$, mais on perd alors l'injectivité de $\tilde{f}$.

Theorème 1.27 ("Théorèmes d'isomorphisme, II et III")

Soit G un groupe. Soit H un sous-groupe distingué de G, on note $p : G \to G/H$ 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.

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

d) 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 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 est un sous-groupe de G/H. Réciproquement si A est un sous-groupe de G/H, alors $N := p^{-1}(A)$ est un sous-groupe de G contenant H (car A contient le neutre de G/H), et on a bien $A = p(N) = N/H$ car p est surjective. Si $A \lhd G/H$, son image réciproque N est un sous-groupe distingué de G, et si $N \lhd G$, alors $A = p(N)$ est bien distingué dans $p(G) = G/H$.

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.

c) Soit $u = kh \in KH$. Alors on a $p(u) = p(k) \in p(K)$ car $p(h)$ est le neutre de G/H, d'où $KH/H \subset p(K)$. Réciproquement, tout élément de $p(K)$ 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 $\varphi(k) = \bar{k} = p(k)$. Son noyau est clairement $K \cap H$ car $\ker p = H$. Comme

$p(K) = KH/H$, on voit que φ est surjectif, et le théorème de factorisation donne alors $K/K \cap H \simeq KH/H$.

d) 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.

□

Remarque 1.28 Le cas particulier d'un groupe abélien $(A, +)$ est déjà intéressant : si B est un sous-groupe de A, alors les sous-groupes de A/B sont les C/B, où C est un sous-groupe de A contenant B. Plus généralement, l'image dans A/B d'un sous-groupe D de A est $(D + B)/B \simeq D/(B \cap D)$.

1.4. Centre et sous-groupe dérivé

Définition 1.29 Soient G un groupe. Le *centre* Z de G est l'ensemble des x de G qui vérifient $xy = yx$ pour tout y de G.

Exemple 1.30 a) Si K est un corps, le centre de $GL_n(K)$ est le sous groupe des $\lambda I_n, \lambda \in K^*$.

b) Pour $n \geq 3$, le centre de $\mathcal{S}_n$ est réduit à l'élément neutre, comme il résulte facilement du fait que si $\tau = (a, b)$ est une transposition et $\sigma \in \mathcal{S}_n$, alors $\sigma\tau\sigma^{-1} = (\sigma(a), \sigma(b))$, donc σ ne commute pas avec τ dès qu'on choisit a avec $\sigma(a) := c$ distinct de a, puis b distinct de a et c (ce qui est possible pour tout σ distinct de l'identité, dès que $n \geq 3$).

Par définition Z est le noyau du morphisme int : $G \to \mathtt{Aut}\, G$ donc $Z \lhd G$. On vérifie même immédiatement que Z est caractéristique dans G.

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.[5] On le note $D(G)$.

L'intérêt de $D(G)$ réside 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 de G qui a cette propriété. On note $G^{\mathrm{ab}} := G/D(G)$ ("abélianisé" de G).*

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

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/H est un quotient de G^{ab} (via le troisième théorème d'isomorphisme).

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. Par définition du quotient, tout commutateur de $G/D(G)$ est trivial, donc $G/D(G)$ est abélien. Enfin, si $H \lhd G$ 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. [6]

□

Par exemple $D(G) = \{1\}$ si et seulement si G est abélien et $D(\mathcal{S}_3) = \mathcal{A}_3$: en effet on voit tout de suite que la signature d'un commutateur est 1, donc $D(\mathcal{S}_3) \subset \mathcal{A}_3$; mais $\mathcal{S}_3$ n'est pas commutatif donc $D(\mathcal{S}_3)$ n'est pas trivial, donc $D(\mathcal{S}_3) = \mathcal{A}_3$ est la seule possibilité via le théorème de Lagrange, vu que $\mathcal{A}_3$ est de cardinal 3.

On verra plus tard que pour $n \geq 2$, on a $D(\mathcal{S}_n) = \mathcal{A}_n$ donc $\mathcal{S}_n^{\text{ab}} \simeq \mathbf{Z}/2\mathbf{Z}$.

2. Groupes finis

2.1. Opérations de groupes, formule des classes

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 de G vers $\mathcal{S}(X)$ au lieu d'un morphisme.

6. Réciproquement, si H est un sous-groupe qui contient $D(G)$, alors H est automatiquement distingué car si $h \in H$ et $g \in G$, alors $(ghg^{-1})h^{-1} \in D(G) \subset H$, d'où $ghg^{-1} \in H$; il est immédiat que G/H est alors abélien.

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 dit alors que G *opère 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 $g.(aH) = (ga)H$.

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.
- *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'action est *fidèle* si le seul élément de G qui stabilise tous les éléments de X est 1, *libre* si tous les stabilisateurs sont réduits à $\{1\}$ (c'est beaucoup plus fort).

Exemple 2.5 a) 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).

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

c) 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 2.6 *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.*

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.

□

Corollaire 2.7 (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. Il y a néanmoins (comme on le verra plus tard) des conséquences tout à fait non triviales !

□

Remarque 2.8 La formule est encore valable si G est infini, en remplaçant $\frac{\#G}{\#\mathrm{Stab}_\omega}$ par l'indice $[G : \mathrm{Stab}_x]$ avec $x \in \omega$ (cet indice est fini dès que X est fini via la proposition 2.6).

Theorème 2.9 (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 $\sum_{g \in G} \#(\mathrm{Fix}\, g)$, car pour chaque g de G on a $\mathrm{Fix}\, g$ éléments x de X tels que $(g, x) \in E$. Mais ce cardinal est aussi $\sum_{x \in X} \#\mathrm{Stab}_x = \sum_{x \in X} \frac{\#G}{\#\,\omega(x)}$ puisque pour chaque $x \in X$, on a $\#\mathrm{Stab}_x = \frac{\#G}{\#\,\omega(x)}$ éléments g de G tels que $(g, x) \in E$. La formule en résulte. D'autre part, si Ω est l'ensemble des orbites, on a

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

□

2.2. p-groupes ; théorèmes de Sylow

Définition 2.10 Soit p un nombre premier. On appelle *p-groupe* un groupe de cardinal p^n, où n est un entier [7].

Proposition 2.11 *Soit G un p-groupe non trivial. Alors :*

a) Le centre Z de G n'est pas trivial.

b) Si G est de cardinal p, il est cyclique. Si G est de cardinal p^2, il est abélien.

Démonstration : a) 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 $\#Z$.

b) 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 a), donc G/Z serait cyclique (car de cardinal p). Mais on obtient une contradiction via le lemme suivant :

Lemme 2.12 *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.

□

On passe maintenant aux théorèmes de Sylow, qui proviennent de 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, exercice...), mais dans le cas particulier des p-sous-groupes, on va voir qu'on a une réponse positive.

Définition 2.13 *Soit p un nombre premier. Soit G un groupe de cardinal $n = p^\alpha m$ avec $\alpha \in \mathbf{N}, m \in \mathbf{N}^*$ et p ne divisant pas m. On appelle p-sous-groupe de Sylow (ou p-Sylow en abrégé) un sous-groupe H de cardinal p^α.*

7. Certains auteurs considèrent que le groupe trivial n'est pas un p-groupe, nous préférons la convention contraire qui permet en particulier de dire qu'un sous-groupe d'un p-groupe est toujours un p-groupe.

Autrement dit, un p-Sylow est un p-sous groupe de G dont l'indice est premier à p (la notion est intéressante si p divise l'ordre de G, sinon un p-Sylow est juste le groupe trivial).

Theorème 2.14 (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 2.15 *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 2.16 *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 $\mathcal{S}_n$ par le 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 de $\mathbf{F}_p^n$.[8] Il reste à prouver les deux lemmes.

Preuve du lemme 2.15 : Le groupe H opère 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.

□

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

Preuve du lemme 2.16 : 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 $\mathcal{B}$ est une telle base, il y a un et un seul élément de G_p qui envoie la base canonique sur $\mathcal{B}$), soit

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

On a en effet p^n-1 choix pour le premier vecteur de la base (tout vecteur e_1 non nul), puis p^n-p choix pour le deuxième (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.

□

Remarque 2.17 En exercice, on peut voir qu'un groupe de cardinal $p^\alpha m$, avec p ne divisant pas m, contient des sous-groupes d'ordre p^i pour tout $i \leq \alpha$ (indication : 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 2.18 (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.

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

Démonstration : a) D'après le premier théorème de Sylow, il existe au moins un p-Sylow S de G. Le lemme 2.15 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, son cardinal k (qui divise celui de G via la proposition 2.6) 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 (qui est une puissance de p) 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 via b). Mais T est distingué dans N via le fait que $sTs^{-1} = T$ pour tout s de S : en effet, le normalisateur $N_G(T)$ contient T et S, donc aussi le sous-groupe N qu'ils engendrent. Finalement $T = S$.[9]

□

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 n'est pas *simple*, i.e. il possède un sous-groupe distingué autre que lui-même et le groupe trivial : en effet son nombre k de 7-Sylow doit diviser 9 et être congru à 1 modulo 7, donc $k = 1$, ce qui implique que l'unique 7-Sylow est distingué. Le même argument fonctionne pour un groupe d'ordre 255.

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

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

Proposition 2.19 *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.

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

Proposition 2.20 *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[10] *$\mathbf{Z}/n\mathbf{Z}$ 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.

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[11]. 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 $\alpha = 1$.

10. 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 $\bar{1}$.

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

Theorème 2.21 *Soient K un corps*[12] *et G un sous-groupe fini du groupe multiplicatif K^*. Alors G est cyclique.*

Démonstration : On utilise le lemme suivant :

Lemme 2.22 *Soit $n \in \mathbf{N}^*$, alors*

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

Le lemme est une conséquence immédiate de la proposition 1.13 : 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 2.21. 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 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 2.23 *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 2.19). 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.

12. 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.

Theorème 2.24 *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 2.25 *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 2.26 *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 2.26 : 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 2.24 : D'après le lemme 2.25, 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 2.23) 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 2.26.

□

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

Theorème 2.27 *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 $\mathbf{Z}/2\mathbf{Z}$.

□

Concluons cette section en énonçant le théorème de structure des groupes abéliens de type fini, dont la démonstration sera donnée dans le chapitre sur les modules (un groupe abélien n'étant rien d'autre qu'un module sur l'anneau $\mathbf{Z}$) :

Theorème 2.28 *Soit A un groupe abélien admettant une partie génératrice finie. Alors il existe un entier $r \in \mathbf{N}$ et des entiers $d_1, ..., d_m$ au moins égaux à 2 vérifiant :*

a) Le groupe A est isomorphe au produit direct $\mathbf{Z}^r \times \mathbf{Z}/d_1 \times ... \times \mathbf{Z}/d_m$.

b) On a $d_1|d_2|...|d_m$.

De plus, cette décomposition est unique.

3. Quelques notions supplémentaires liées aux sous-groupes distingués

3.1. Suites exactes

On commence par la très utile notion de suite exacte, qu'on peut d'ailleurs étendre aux espaces vectoriels (et, comme on le verra plus tard, aux modules).

Définition 3.1 On dit qu'une suite (finie ou infinie)

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

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

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

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 $G/N \simeq H$ (en identifiant N à $i(N)$) via le théorème de factorisation, et on dit que G est une *extension* de H par N.[13]

Remarque 3.2 a) De même qu'on ne confondra pas sous-groupe et quotient, on ne confondra pas "sur-groupe" et extension.

b) Quand tous les groupes sont abéliens et notés additivement, on écrira souvent 0 au lieu de 1 dans une suite exacte courte.

Exemple 3.3 a) Si K est un corps, alors la suite

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

est exacte.

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

b) Les suites

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

et

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

sont exactes, où S^1 désigne le groupe multiplicatif des complexes de module 1. Ici $O_n(\mathbf{R})$ (resp $U_n(\mathbf{C})$) est le groupe orthogonal (resp. le groupe unitaire) constitué des matrices A réelles (resp. complexes) (n, n) telles que $A^*A = I_n$.

c) Si $n \geq 2$, la suite

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

est exacte.

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

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

e) Le groupe $\mathbf{Z}/4$ peut se voir comme une extension de $\mathbf{Z}/2$ par $\mathbf{Z}/2$, via la suite exacte

$$0 \to \mathbf{Z}/2 \to \mathbf{Z}/4 \to \mathbf{Z}/2 \to 0, \tag{1}$$

où la flèche $\mathbf{Z}/4 \to \mathbf{Z}/2$ envoie chaque $\bar{x} \in \mathbf{Z}/4$ sur la classe de x dans $\mathbf{Z}/2$, et la flèche $\mathbf{Z}/2 \to \mathbf{Z}/4$ envoie chaque $\bar{y} \in \mathbf{Z}/2$ sur la classe de $2y$ dans $\mathbf{Z}/4$. Noter que $\mathbf{Z}/4$ n'est pas pour autant isomorphe au produit de $\mathbf{Z}/2$ par $\mathbf{Z}/2$.

3.2. Produit semi-direct de deux groupes

Attention à cette notion, qui est en général 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.

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 H sur N (mais on demande en plus ici que l'action soit par automorphismes, i.e. l'image de φ doit être incluse dans $\mathtt{Aut}N$, et pas seulement dans $\mathcal{S}(N)$).

Theorème 3.4 *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 $h^{-1}.(n^{-1}n) = (h^{-1}.n^{-1})(h^{-1}.n)$). 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. □

Remarque 3.5 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.

Proposition 3.6 *Avec les notations ci-dessus, soit $G = N \rtimes H$. Alors :*

a) 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)[14] *dans G.*

b) 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.

c) 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.

14. 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 : a) 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.

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

c) D'après a), $N \cap H$ 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 :

$$hnh^{-1} = (1,h)(n,1)(1,h^{-1}) = (h.n,h)(1,h^{-1}) = (h.n,1) = h.n.$$

□

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 $hn = (h.n)h$.

Remarque 3.7 Soit $G := N \rtimes_\varphi H$. Si $H \lhd G$, on a $n^{-1}(h.n)h \in H$ (pour tous $n \in N$, $h \in H$) car $n^{-1}(h.n)h = n^{-1}hn \in H$. Ceci implique que $n^{-1}(h.n) \in H$ et comme $N \cap H = \{1\}$, ceci entraîne que $n^{-1}(h.n) = 1$, autrement dit l'action est triviale. Le produit semi-direct est abélien ssi cette condition est vérifiée et N et H sont de plus abéliens.

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

Proposition 3.8 *a) (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 $h.n = hnh^{-1}$.

b) (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 : a) 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).

b) 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 a), 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.

Remarque 3.9 On verra en TD deux conditions suffisantes pour obtenir des produits semi-directs isomorphes pour des actions différentes :

a) 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 $N \rtimes_\varphi H \simeq N \rtimes_\psi H$.

b) 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 $N \rtimes_\varphi H \simeq N \rtimes_\psi H$.

Exemple 3.10 a) 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 $\mathcal{S}_n \simeq \mathcal{A}_n \rtimes \mathbf{Z}/2\mathbf{Z}$.

b) 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 $\mathrm{GL}_n(K) \simeq \mathrm{SL}_n(K) \rtimes K^*$.

c) 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, ce serait alors un produit direct vu que $\mathbf{Z}/4\mathbf{Z}$ est abélien. 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 (1) de l'exemple 3.3 n'est pas scindée. [15]

d) Soit $n \geq 3$, on note D_n le *groupe diédral* 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 $x \in \mathbf{Z}/n\mathbf{Z}$.

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 :

Theorème 3.11 *Soient p et q deux nombres premiers avec $p < q$. Alors G est un produit semi-direct $\mathbf{Z}/q\mathbf{Z} \rtimes \mathbf{Z}/p\mathbf{Z}$, et G est même isomorphe au produit direct $\mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \simeq \mathbf{Z}/pq\mathbf{Z}$ si p ne divise pas $q-1$. Si p divise $q-1$, ce produit semi-direct peut ne pas être abélien.*

(En fait si p ne divise pas $q-1$, il y a exactement un produit semi-direct non abélien comme ci-dessus à isomorphisme près, par exemple le groupe diédral si $p = 2$ et $q \geq 3$; cela résulte de la remarque 3.9).

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

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

Montrons que cette suite est scindée : le groupe 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

15. 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 !).

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 $\varphi : \mathbf{Z}/p\mathbf{Z} \to \mathtt{Aut}(\mathbf{Z}/q\mathbf{Z}) \simeq \mathbf{Z}/(q-1)\mathbf{Z}$.

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 et le produit est direct.

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.

□

3.3. 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 3.12 *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 3.13 *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).

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 3.14 *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 analogue à celui de l'exemple 1.18, d).

□

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

Lemme 3.15 *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 3.16 *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 3.17 *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 $\mathcal{A}_5$ [16], 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.

□

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

16. 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.

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.

□

3.4. Groupes résolubles et nilpotents

On se contentera ici des définitions et des premières propriétés. On pourra se reporter au livre de Hall [1] pour plus de détails.

Définition 3.18 Soit G un groupe.[17] 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.

Il est commode d'avoir la caractérisation suivante :

Proposition 3.19 *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 quotient $D^{i-1}(G)/D^i(G)$ 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.

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

En sens inverse si G est résoluble, soit $(G_i)_{1\leq i\leq n}$ une suite comme dans la définition 3.18. 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 $D^n(G) = \{1\}$.

□

Remarque 3.20 a) La proposition 3.19 donne qu'on peut demander en plus que chaque G_i soit distingué dans G tout entier (en utilisant la suite $D^i(G)$ des sous-groupes dérivés successifs). Ainsi G résoluble signifie que G se déduit de $\{1\}$ par une suite finie d'*extensions à noyaux abéliens* :

$$1 \to G_i/G_{i-1} \to G/G_{i-1} \to G/G_i \to 1.$$

b) 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 : en effet tout groupe abélien fini H admet une suite $H \supset ... \supset \{1\}$ avec tous les H_i/H_{i-1} simples (donc cycliques d'ordre premier car abéliens), 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 alors de groupe *hyper-résoluble*).

c) Le terme résoluble vient de la théorie de Galois. 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 que l'équation $P(x) = 0$ est résoluble par radicaux si et seulement si G est résoluble. 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. On verra tout cela plus en détails dans le chapitre consacré à la théorie de Galois.

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

Définition 3.21 On dit qu'un groupe G est *nilpotent* s'il existe une suite finie

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

tel que pour tout $i \in [1, n]$: $G_i \lhd G$ et l'extension

$$1 \to G_i/G_{i-1} \to G/G_{i-1} \to G/G_i \to 1$$

est *centrale*, i.e. G_i/G_{i-1} est 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.

Exemple 3.22 a) Un groupe abélien est nilpotent.

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

c) $\mathcal{S}_n$ 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 3.19.

d) $\mathcal{S}_4$ 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 $\mathcal{S}_3$

e) $\mathcal{S}_3$ est hyper-résoluble mais pas $\mathcal{A}_4$.

f) Un sous-groupe et un quotient d'un groupe résoluble sont résolubles, ainsi qu'une extension d'un groupe résoluble par un groupe résoluble (voir TD).

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.