Cours agrégation (2019-2020) : Groupes

David Harari

1. Généralités

1.1. Conventions

Dans ce cours, la loi d'un groupe G (pas forcément commutatif) sera le plus souvent notée multiplicativement, i.e. $(x,y) \mapsto xy$. Le neutre sera noté e ou 1, et le symétrique (ou *inverse*) d'un élément x de G sera noté x^{-1}. Pour $n > 0$, on pose $x^n = x.x...x$ (n termes), avec les conventions $x^0 = 1$ et $x^{-n} = (x^n)^{-1}$. Noter que pour tous $x, y \in G$, on a $(xy)^{-1} = y^{-1}x^{-1}$.

Si G est *abélien* (c'est-à-dire commutatif), 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 1.1 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]

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.

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.

1.2. Morphisme de groupes, sous-groupes

Définition 1.2 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 1.3 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 1.4 Un sous-ensemble H d'un groupe G est un *sous-groupe* si il vérifie :

— $1 \in H$.

— Pour tous x, y de H, on a $xy \in H$.

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

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

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

C'est immédiat à vérifier.

Exemple 1.6 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 $\texttt{Aut}\, G$ 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 1.7 *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 $\langle A \rangle$.*

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 1.8 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 1.9 *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 1.10 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 1.11 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 1.12 *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 1.13 (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 (voir les exercices pour une généralisation quand G n'est pas supposé fini).

Corollaire 1.14 *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 1.9.

Proposition 1.15 *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 1.16 *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 1.17 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 1.18 *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 1.19 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 1.20 Attention, $\lhd$ n'est pas une relation transitive, on peut avoir $K \lhd H \lhd G$ et pas $K \lhd G$ (cf. exercices).

Définition 1.21 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.

Theorème 1.22 *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 $p : G \to G/H$ (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.

□

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 p.

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 1.23 (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* $\operatorname{Im} f$.

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

□

Remarque 1.24 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 $\ker f/N$).

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

Corollaire 1.25 ("Premier théorème d'isomorphisme") *Avec les notations du théorème 1.23, on a $G/\ker f \simeq \operatorname{Im} f$.*

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 1.26 *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 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 $N/H = p(N)$ 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.

□

Theorème 1.27 ("Théorèmes d'isomorphisme, II et III") *Soit G un groupe. Soient H un sous-groupe distingué de G et $p : G \to G/H$ la surjection canonique.*

a) 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").

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 1.26, l'ensemble $KH = HK$ est bien un sous-groupe de G contenant H. 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 $K/K \cap H \simeq KH/H$.

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.

$\square$

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

Corollaire 1.28 *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 1.29 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 1.30 *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).*

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.

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.

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 1.31 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 $n \geq 5$ (cf. leçon "groupe symétrique"). 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 $\#K \leq 3$ (cf. exercices).

Définition 1.32 Un groupe G est dit *simple* si ses seuls sous-groupes distingués sont G et $\{e\}$, *parfait* si $D(G) = G$.

Exemple 1.33 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 $n \geq 5$ (cf. exercices).

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), voir par exemple le cours d'algèbre de D. Perrin.

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.

$\square$

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 (voir exercices).

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. Notions de théorie des représentations

Dans toute la suite, G désignera un groupe fini (noté multiplicativement) et V un espace vectoriel de dimension finie n sur le corps des complexes $\mathbf{C}$. On note $\mathrm{GL}(V)$ le groupe des applications linéaires bijectives de V dans V, muni de la loi $\circ$ (qu'on notera souvent également multiplicativement).

3.1. Généralités

Définition 3.1 Une *représentation linéaire* (ou simplement représentation) ρ de G dans V est un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$. On dit que V est l'*espace* de la représentation ρ et $n = \dim V$ son *degré*.

Si on choisit une base de V, on peut se donner ρ via la matrice M_s de $\rho(s)$ dans cette base pour tout $s \in G$. On notera souvent ρ_s pour $\rho(s)$. On parlera parfois de "la représentation V" si le morphisme ρ est sous-entendu.

Définition 3.2 Deux représentations $\rho : G \to V$ et $\rho' : G \to V'$ de G sont dite *isomorphes* (ou semblables) s'il existe un isomorphisme de $\mathbf{C}$-espaces vectoriels $u : V \to V'$ tel que

$$u \circ \rho(s) = \rho'(s) \circ u$$

pour tout $s \in G$.

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

On notera bien que l'isomorphisme u qui réalise l'égalité $u \circ \rho(s) = \rho'(s) \circ u$ doit être indépendant de s.

Exemple 3.3 a) Une représentation de degré 1 d'un groupe fini G n'est pas autre chose qu'un morphisme $\rho : G \to \mathbf{C}^*$. La *représentation unité* est le morphisme constant égal à 1. Voir les exercices pour une étude du groupe multiplicatif de ces morphismes, notamment quand G est abélien (cas auquel on peut se ramener car un morphisme de G dans le groupe abélien $\mathbf{C}^*$ est trivial sur le sous-groupe dérivé $D(G)$, donc induit un morphisme de l'abélianisé $G^{\mathrm{ab}} = G/D(G)$ dans $\mathbf{C}^*$).

b) La *représentation constante de degré n* envoie tout $s \in G$ sur l'identité d'un espace vectoriel de dimension n.

c) Soit G un groupe fini de cardinal g. Soit V un $\mathbf{C}$-espace vectoriel de dimension g, muni d'une base $(e_t)_{t \in G}$ indexée par les éléments de G. On définit alors une représentation $\rho : G \to V$ par la formule

$$\rho_s(e_t) = e_{st}.$$

On dit que ρ est la *représentation régulière* de G (il est immédiat qu'à isomorphisme près, elle ne dépend pas du choix de V et de la base (e_t)). Elle est de degré g. On peut aussi la définir en prenant pour V l'espace des fonctions de G dans $\mathbf{C}$ et en prenant pour ρ_s l'élément de $\mathrm{GL}(V)$ qui envoie toute fonction f sur la fonction $t \mapsto f(s^{-1}t)$; le lecteur vérifiera qu'on obtient bien des représentations isomorphes avec les deux définitions.

3.2. Sous-représentations

Définition 3.4 Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire. Une *sous-représentation* de ρ est la restriction $\rho^W : G \to \mathrm{GL}(W)$ de ρ à un sous-espace vectoriel W de V stable par tous les ρ_s, $s \in G$. Ainsi ρ^W est définie par :

$$\rho_s^W = (\rho_s)_{|W}, \quad \forall s \in G.$$

Exemple 3.5 Si $\rho : G \to \mathrm{GL}(V)$ est la représentation régulière de G, et si W est le sous-espace de dimension 1 de V engendré par $x := \sum_{t \in G} e_t$, alors tous les ρ_s induisent l'identité sur W, ce qui fait que W est une sous-représentation de V, qui est d'ailleurs isomorphe à la représentation unité.

Définition 3.6 Soit $\rho : G \to \mathrm{GL}(V)$ une représentation. Soit $V = \bigoplus_{i=1}^r V_i$ une décomposition de V en somme directe de sous-espaces stables par ρ. On dit alors que ρ est la *somme directe* des sous-représentations $\rho_i : G \to \mathrm{GL}(V_i)$ associées à ρ, et on note $\rho = \bigoplus_{i=1}^r \rho_i$.

Par exemple, la représentation constante de degré n est la somme directe de n copies de la représentation unité.

Theorème 3.7 *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire d'un groupe fini G. Soit W un sous-espace de V stable par ρ. Alors il existe un sous-espace supplémentaire W^0 de W dans V, qui est stable par ρ.*

Démonstration : On commence à choisir un supplémentaire quelconque W' de W dans V, et on appelle p le projecteur sur W parallèlement à W'. Soit g le cardinal de G, posons

$$p^0 := \frac{1}{g} \sum_{t \in G} \rho_t p \rho_t^{-1}.$$

On observe que $\operatorname{Im} p^0 \subset W$ (car $\operatorname{Im} p \subset W$ et W est stable par ρ), et d'autre part si $x \in W$, on a $p(\rho_t^{-1}(x)) = \rho_t^{-1}(x)$ (puisque $\rho_t^{-1}(x) \in W$, toujours par stabilité de W pour ρ) d'où $p^0(x) = x$. Il en résulte que p^0 est un projecteur d'image W.

Définissons alors $W^0 := \operatorname{Ker} p^0$. On observe qu'on a l'égalité $\rho_s p^0 = p^0 \rho_s$ pour tout $s \in G$. En effet, on a :

$$\rho_s p^0 \rho_s^{-1} = \frac{1}{g} \sum_{t \in G} \rho_{st} p \rho_{t^{-1}s^{-1}} = \frac{1}{g} \sum_{t \in G} \rho_{st} p \rho_{(st)^{-1}} = p^0,$$

vu que l'application $t \mapsto st$ est une bijection de G dans lui-même. Il en résulte immédiatement que W^0 est stable par ρ, et c'est bien un supplémentaire de W dans V.

□

3.3. Représentations irréductibles

La notion suivante est fondamentale :

Définition 3.8 Soit G un groupe fini. Une représentation linéaire $\rho : G \to \mathrm{GL}(V)$ est dite *irréductible* (ou simple) si $V \neq \{0\}$ et V n'admet aucun sous-espace stable par ρ autre que V et $\{0\}$.

Par exemple, toute représentation de degré 1 est de manière évidente irréductible (noter par contre que par convention, la représentation $V = \{0\}$ n'est pas irréductible).

Theorème 3.9 *Soit G un groupe fini. Soit V un $\mathbf{C}$-espace vectoriel de dimension finie. Alors, toute représentation $\rho : G \to \mathrm{GL}(V)$ est somme directe d'un nombre fini de représentations irréductibles.*

Démonstration (esquisse): C'est une conséquence facile, par récurrence sur $\dim V$, du théorème 3.7.

□

Noter qu'en général la décomposition en somme directe de représentations irréductibles n'est pas unique, mais on verra que le *nombre* de représentations iréductibles V_i isomorphes à une représentation irréductible donnée ne dépend pas de la décomposition choisie.

Remarque 3.10 Soit $\mathbf{C}[G]$ l'algèbre du groupe G (c'est l'espace des fonctions de G dans $\mathbf{C}$, muni du produit de convolution). Alors, se donner une représentation de G revient à se donner un module (de type fini) sur l'anneau $\mathbf{C}[G]$. Le théorème précédent assure qu'un tel module est *semi-simple* (il se décompose en somme directe de modules simples).

3.4. Caractère d'une représentation, lemme de Schur

Définition 3.11 Soit $\rho : G \to \mathrm{GL}(V)$ une représentation linéaire d'un groupe fini G. Le *caractère* de ρ est la fonction $\chi : G \to \mathbf{C}$ définie par $\chi(s) = \mathrm{Tr}\,(\rho_s)$ pour tout $s \in G$, où Tr désigne la trace.

Proposition 3.12 *Soit χ le caractère d'une représentation ρ de degré n. Alors, on a :*

a) Si ρ est la représentation constante de degré n, on a $\chi(s) = n$ pour tout $s \in G$.

b) $\chi(s^{-1}) = \overline{\chi(s)}$ pour tout $s \in G$.

c) $\chi(tst^{-1}) = \chi(s)$ pour tous $s, t \in G$ (on dit qu'un caractère est une fonction centrale sur G, i.e. il vérifie $\chi(st) = \chi(ts)$ pour tous $s, t \in G$).

d) Si ρ est somme directe de $\rho_1, ..., \rho_r$, alors son caractère χ est somme des caractères $\chi_1, ..., \chi_r$ des ρ_i.

Démonstration : a) est immédiat. Pour b), on observe qu'en notant g le cardinal de G, on a $s^g = 1$ pour tout s de G par le théorème de Lagrange, et donc $\rho_s^g = \mathrm{Id}$, ce qui implique que les valeurs propres complexes $\lambda_1, ...\lambda_n$ de ρ_s sont des racines de l'unité, et celles de $\rho_{s^{-1}} = \rho_s^{-1}$ sont $\lambda_1^{-1}, ..., \lambda_n^{-1}$. Ainsi

$$\chi(s^{-1}) = \sum_i \lambda_i^{-1} = \sum_i \bar{\lambda}_i = \overline{\chi(s)}.$$

Le c) résulte de la formule $\mathrm{Tr}\,(\rho_s\rho_t) = \mathrm{Tr}\,(\rho_t\rho_s)$, et le d) est immédiat en choisissant une base de l'espace de chaque ρ_i, puis en recollant ces bases en une base de l'espace de $\bigoplus_i \rho_i$.

□

Lemme 3.13 (Lemme de Schur) *Soit G un groupe fini. Soient $\rho^1 : G \to \mathrm{GL}(V_1)$ et $\rho^2 : G \to \mathrm{GL}(V_2)$ deux représentations irréductibles de G. Soit $f : V_1 \to V_2$ une application linéaire vérifiant $\rho^2_s \circ f = f \circ \rho^1_s$ pour tout $s \in G$. Alors :*

a) Si f n'est pas bijective (en particulier si ρ^1 et ρ^2 ne sont pas isomorphes), alors $f = 0$.

b) Supposons $V_1 = V_2$ et $\rho^1 = \rho^2$. Alors f est une homothétie.

Démonstration : a) Supposons $f \neq 0$ et posons $W_1 = \mathrm{Ker}\, f$. Alors on voit tout de suite que $\mathrm{Ker}\, f$ est stable par ρ^1, donc par irréductibilité on obtient $\mathrm{Ker}\, f = \{0\}$ puisqu'on a exclu le cas $\mathrm{Ker}\, f = V_1$. On démontre de même par irréductibilité de ρ^2 que $\mathrm{Im}\, f = V_2$, donc f est bijective.

b) Comme on est sur $\mathbf{C}$, l'endomorphisme f possède au moins une valeur propre λ. Posons alors $f' = f - \lambda \mathrm{id}$, alors $\rho^2_s \circ f' = f' \circ \rho^1_s$ pour tout $s \in G$; comme f' n'est pas bijective, le a) donne que $f' = 0$, i.e. f est une homothétie.

□

Corollaire 3.14 *Soit G un groupe fini de cardinal g. Soient $\rho^1 : G \to \mathrm{GL}(V_1)$ et $\rho^2 : G \to \mathrm{GL}(V_2)$ deux représentations irréductibles de G. Pour toute application linéaire $h : V_1 \to V_2$, on définit une application linéaire $h^0 : V_1 \to V_2$ par la formule :*

$$h^0 = \frac{1}{g} \sum_{t \in G} (\rho^2_t)^{-1} h \rho^1_t.$$

Alors :

a) Si ρ^1 et ρ^2 ne sont pas isomorphes, on a $h^0 = 0$.

b) Si $V_1 = V_2$ et $\rho^1 = \rho^2$, on a $h^0 = \frac{\mathrm{Tr}\, h}{n} \mathrm{id}$, où n est la dimension de V_1 et V_2.

Démonstration : On observe que $\rho^2_s h^0 = h^0 \rho^1_s$ (le calcul est le même que dans la preuve du théorème 3.7). Le lemme 3.13 donne alors : dans le cas a), $h^0 = 0$ et dans le cas b), h^0 est une homothétie. Comme par ailleurs on a, dans le cas b), $\mathrm{Tr}\,(h^0) = \mathrm{Tr}\, h$ via l'invariance de la trace d'une matrice par conjugaison, on en déduit bien alors que $h^0 = \frac{\mathrm{Tr}\, h}{n} \mathrm{id}$ vu que la trace de l'identité est n.

□

Il est intéressant d'avoir maintenant une traduction matricielle du corollaire précédent. Si φ et ψ sont des fonctions $G \to \mathbf{C}$, notons

$$\langle \varphi, \psi \rangle = \frac{1}{g} \sum_{t \in G} \varphi(t^{-1}) \psi(t) = \frac{1}{g} \sum_{t \in G} \varphi(t) \psi(t^{-1}). \tag{1}$$

On obtient ainsi une forme bilinéaire symétrique définie sur l'espace vectoriel $\mathcal{F}(G, \mathbf{C})$ des fonctions de G dans $\mathbf{C}$.

Proposition 3.15 *Pour $t \in G$, soient $(r_{i_1 j_1}(t))$ et $(u_{i_2 j_2}(t))$ les matrices respectives de $\rho^1(t)$ et $\rho^2(t)$ dans des bases $\mathcal{B}_1$, $\mathcal{B}_2$ de V_1, V_2. Alors :*

a) Si ρ^1 et ρ^2 ne sont pas isomorphes, on a $\langle u_{i_2 j_2}, r_{j_1 i_1}\rangle = 0$ pour tous indices i_1, j_1, i_2, j_2.

b) Si $V_1 = V_2$ est de dimension n et $\rho^1 = \rho^2$ (auquel cas on prend $\mathcal{B}_1 = \mathcal{B}_2$ et on a $r_{ij} = u_{ij}$ pour tous indices i, j), alors $\langle r_{i_2 j_2}, r_{j_1 i_1}\rangle = 0$ si $i_1 \neq i_2$ ou $j_1 \neq j_2$, et $\langle r_{ij}, r_{ji}\rangle = 1/n$ pour tous indices i, j.

Démonstration : Soit $h : V_1 \to V_2$ une application linéaire quelconque, de matrice $(x_{i_2 i_1})$ dans les bases $\mathcal{B}_1, \mathcal{B}_2$. On peut lui associer l'application linéaire h^0 comme dans le corollaire 3.14, de matrice $(x^0_{i_2 i_1})$. On a alors, d'après la formule définissant le produit de deux matrices :

$$x^0_{i_2 i_1} = \frac{1}{g} \sum_{t \in G} \sum_{j_1, j_2} u_{i_2 j_2}(t^{-1}) x_{j_2 j_1} r_{j_1 i_1}(t) = \sum_{j_1, j_2} \langle u_{i_2 j_2}, r_{j_1 i_1}\rangle x_{j_2 j_1}.$$

Dans le cas a), ceci indique que la forme linéaire en les $x_{j_2 j_1}$ définie par le deuxième membre est nulle, ce qui implique que tous ses coefficients sont nuls. Ainsi : $\langle u_{i_2 j_2}, r_{j_1 i_1}\rangle = 0$ pour tous indices i_1, j_1, i_2, j_2.

Dans le cas b), on sait que h^0 est une homothétie de rapport

$$\lambda = \frac{\operatorname{Tr} h}{n} = \frac{1}{n} \sum_{j_1 = j_2} x_{j_2 j_1}.$$

ainsi on a $x^0_{i_2 i_1} = 0$ si $i_2 \neq i_1$, ce qui donne $\langle r_{i_2 j_2}, r_{j_1 i_1}\rangle = 0$ si $i_2 \neq i_1$. Si $i_2 = i_1 = i$, on obtient $\langle r_{i j_2}, r_{j_1 i}\rangle = 0$ si $j_1 \neq j_2$ et $\langle r_{ij}, r_{ji}\rangle = 1/n$ pour tous i, j.

□

3.5. Les relations d'orthogonalité des caractères

C'est dans ce paragraphe que se trouvent les résultats fondamentaux sur les *caractères irréductibles* (=caractères des représentations irréductibles), et leurs conséquences sur la décomposition d'une représentation en somme d'irréductibles.

Soit G un groupe fini de cardinal g. On définit un produit scalaire hermitien sur l'espace vectoriel $\mathcal{F}(G, \mathbf{C})$ des fonctions de G dans $\mathbf{C}$, par la formule :

$$(\varphi|\psi) := \frac{1}{g} \sum_{t \in G} \overline{\varphi(t)} \psi(t).$$

Noter que cette formule est légèrement différente de celle de la forme bilinéaire symétrique $\langle \varphi, \psi \rangle$ définie par la formule (1). Néanmoins, si φ et ψ sont des caractères, les deux formules coïncident car dans ce cas $\overline{\varphi(t)} = \varphi(t^{-1})$ par la proposition 3.12, (b). Travailler maintenant avec le produit scalaire hermitien $(.|.)$ est meilleur, afin d'utiliser les propriétés usuelles des espaces hermitiens (alors que l'emploi provisoire de la forme bilinéaire symétrique $\langle ., . \rangle$ était plus commode pour formuler la proposition 3.15).

Theorème 3.16 *a) Soient ρ^1, ρ^2 deux représentations irréductibles non isomorphes de G. Soient χ_1, χ_2 leurs caractères respectifs. Alors $(\chi_1|\chi_2) = 0$.*

b) Soit χ le caractère d'une représentation irréductible ρ de G. Alors $(\chi|\chi) = 1$.

Observons que b) donne aussi la valeur de $(\chi|\chi')$ lorsque χ, χ' sont les caractères respectifs de deux représentations irréductibles isomorphes, puisqu'alors les fonctions χ et χ' coïncident.

Démonstration : a) Écrivons les formes matricielles respectives $r_{ij}(t)$ et $u_{ij}(t)$ de ρ^1, ρ^2. Alors

$$(\chi_1|\chi_2) = \langle \chi_1, \chi_2 \rangle = \sum_{i,j} \langle r_{ii}, u_{jj} \rangle,$$

qui est nul d'après la proposition 3.15, a).

b) Supposons ρ de degré n, donnée sous forme matricielle $\rho_t = (r_{ij}(t))$. Alors $\chi(t) = \sum_i r_{ii}(t)$, d'où

$$(\chi|\chi) = \langle \chi, \chi \rangle = \sum_{i,j} \langle r_{ii}, r_{jj} \rangle.$$

D'après la proposition 3.15 b), on a $\langle r_{ii}, r_{jj} \rangle = 0$ si $i \neq j$ et $\langle r_{ii}, r_{jj} \rangle = 1/n$ si $i = j$, ce qui donne finalement $(\chi|\chi) = 1$.

□

On appellera pour simplifier *caractère irréductible* de G le caractère d'une représentation irréductible de G. Le théorème précédent peut s'interpréter comme l'*orthogonalité* de deux caractères irréductibles distincts de G. En particulier, les caractères irréductibles forment une famille orthonormée de vecteurs de l'espace vectoriel hermitien $\mathcal{F}(G, \mathbf{C})$ des fonctions de G dans $\mathbf{C}$ (qui est de dimension finie $\#G$). On en déduit :

Corollaire 3.17 *Les caractères irréductibles sont en nombre fini.*

Dans toute la suite, on écrira pour simplifier

$$\rho = \bigoplus_{i=1}^{r} \rho_i$$

pour signifier qu'une reprśentation ρ est isomorphe à la somme directe des représentations $\rho_1, ..., \rho_r$.

Theorème 3.18 *Soient ρ_1, ρ_2, ..., ρ_r les représentations irréductibles de G (bien définies à isomorphisme près) avec ρ_i non isomorphe à ρ_j si $i \neq j$. On note χ_i le caractère de ρ_i Soit ρ une représentation de G, de caractère χ, telle que*

$$\rho = \bigoplus_{i=1}^{r} m_i \rho_i,$$

où on a noté $m_i \rho_i$ la somme directe de m_i représentations qui sont toutes isomorphes à ρ_i. Alors on a $m_i = (\chi|\chi_i)$.

La décomposition de ρ en somme directe de représentations irréductibles est donc unique à isomorphisme près des sous-représentations intervenant dans cette décomposition. On dit que m_i est le *nombre de fois que ρ contient ρ_i*.

Démonstration : On a $\chi = \sum_j m_j \chi_j$ par la proposition 3.12 d), et $(\chi_j|\chi_i)$ vaut 1 si $i = j$, 0 sinon d'après le théorème 3.16. On conclut par linéarité du produit scalaire (.|.).

$\square$

Corollaire 3.19 *Soit G un groupe fini. Alors deux représentations de G de même caractère sont isomorphes.*

Cet énoncé et le corollaire 3.17 seront précisés au paragraphe suivant

Démonstration : En effet, leurs décompositions respectives en somme de représentations irréductibles contiennent alors le même nombre de fois toute représentation irréductible donnée.

$\square$

Corollaire 3.20 *Soit φ le caractère d'une représentation $\rho : G \to \mathrm{GL}(V)$. Alors $(\varphi|\varphi)$ est un entier ≥ 0 (et > 0 si $\dim V > 0$), égal à 1 si et seulement si ρ est irréductible.*

Démonstration : Écrivons $V = \oplus m_i\rho_i$ avec les ρ_i irréductibles et deux à deux non isomorphes. Alors $(\varphi|\varphi) = \sum m_i^2$ est un entier, égal à 1 si et seulement s'il y a une seule ρ_i avec de plus $m_i = 1$, ce qui signifie exactement que ρ est irréductible.

□

3.6. Nombre de représentations irréductibles

On commence par un énoncé sur la représentation régulière.

Proposition 3.21 *Soit G un groupe fini de cardinal g.*

a) Le caractère r_G de la représentation régulière τ est donné par $r_G(1) = g$ et $r_G(s) = 0$ si $s \neq 1$.

b) Soit ρ une représentation irréductible. Alors ρ est contenue $\deg\rho$ *fois dans la représentation régulière.*

c) Si $n_1, ..., n_h$ sont les degrés des reprśentations irréductibles (à isomorphisme près) $\rho_1, ...\rho_h$ de G et $\chi_1, ..., \chi_h$ leurs caractères, on a $\sum_{i=1}^h n_i^2 = g$ et $\sum_{i=1}^h n_i\chi_i(s) = 0$ pour $s \neq 1$.

Démonstration : a) La représentation régulière $\tau : G \to \mathrm{GL}(V)$ est donnée par $\rho_s(e_t) = e_{st}$, où $(e_t)_{t\in G}$ est une base de V. On a $r_G(1) = g = \dim V$ car $\tau(1) = \mathrm{id}_V$. Pour $s \neq 1$, la matrice de ρ_s dans la base (e_t) n'a que des zéros sur la diagonale, donc sa trace est nulle.

b) Soit χ le caractère de ρ. D'après le théorème 3.18, le nombre de fois que ρ est contenue dans τ est :

$$(r_G|\chi) = \frac{1}{g}\sum_{s\in G}\overline{r_G(s)}\chi(s) = \frac{1}{g}g\chi(1) = \chi(1)$$

d'après a). Or $\chi(1) = \deg\rho$.

c) D'après b), la représentation régulière τ s'écrit $\tau = \bigoplus_{i=1}^h n_i\rho_i$, d'où $r_G = \sum_{i=1}^h n_i\chi_i$. Il suffit alors d'appliquer a).

□

On va maintenant déterminer le nombre de caractères irréductibles de G via le lien avec les fonctions centrales.

Lemme 3.22 *Soit f une fonction centrale sur G. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G. On définit un endomorphisme ρ_f de V par :*

$$\rho_f = \sum_{t\in G} f(t)\rho(t).$$

Supposons ρ irréductible de degré n et de caractère χ. Alors $\rho_f = \lambda \mathrm{Id}$, avec

$$\lambda = \frac{1}{n} \sum_{t \in G} f(t)\chi(t) = \frac{g}{n} (\bar{\chi}|f).$$

Démonstration : On calcule, pour $s \in G$:

$$\rho(s)^{-1} \rho_f \rho(s) = \sum_{t \in G} f(t)\rho(s^{-1}ts) = \rho_f$$

car $f(s^{-1}ts) = f(t)$ par l'hypothèse que f est centrale et $t \mapsto s^{-1}ts$ est une bijection de G dans G.

D'après le lemme de Schur, on obtient que ρ_f est une homothétie. Son rapport est

$$\mathrm{Tr}\,(\rho_f)/n = \frac{1}{n} \sum_{t \in G} f(t)\chi(t),$$

comme on voulait.

□

Theorème 3.23 *Soit H le $\mathbf{C}$-espace vectoriel des fonctions centrales sur G. Soient χ_1,...,χ_h les caractères irréductibles (deux à deux distincts) de G. Alors $(\chi_1, ..., \chi_h)$ est une base orthonormée de H.*

Démonstration : On sait déjà que la famille $(\chi_1, ..., \chi_h)$ est orthonormée par le théorème 3.16. Pour montrer qu'elle engendre H, il suffit de montrer que son orthogonal est nul, ou encore que l'orthogonal de la famille conjuguée $(\bar{\chi}_1, ..., \bar{\chi}_h)$ est nul. Soit donc $f \in H$ une fonction centrale orthogonale à tous les $\bar{\chi}_i$. Si ρ est une représentation irréductible de G, le lemme 3.22 donne $\rho_f = 0$. Ceci reste vrai pour toute représentation ρ (en la décomposant en somme directe de représentations irréductibles), donc en particulier pour la représentation régulière $\tau : G \to \mathrm{GL}(V)$. Pour celle-ci, on a une base $(e_t)_{t \in G}$ de V telle qu'on ait $\tau(t)e_1 = e_t$ pour tout t de G, d'où :

$$0 = \tau_f.e_1 = \sum_{t \in G} f(t)e_t,$$

ce qui donne $f(t) = 0$ pour tout $t \in G$ puisque (e_t) est une base. Ainsi $f = 0$.

□

Corollaire 3.24 *Le nombre de représentations irréductibles de G à isomorphisme près est le nombre c de classes de conjugaison de G.*

Démonstration : D'après le corollaire 3.19, le nombre de représentations irréductibles de G à isomorphisme près est l'entier h du théorème 3.23. Or, ce théorème dit qu'il s'agit de la dimension du $\mathbf{C}$-espace vectoriel H des fonctions centrales, lequel est de dimension c vu que se donner une fonction centrale revient à donner sa valeur sur chaque classe de conjugaison de G.

□

4. Tables de caractères, exemples

Soit G un groupe fini possédant h classes de conjugaison. D'après le corollaire 3.24, le nombre de caractères irréductibles de G est h. La *table de caractères* de G est le tableau carré possédant h lignes (correspondant aux caractères irréductibles $\chi_1, ..., \chi_h$) et h colonnes (correspondant aux classes de conjugaison $c_1, .., c_h$), l'élément de coordonnées (i, j) du tableau étant $\chi_i(c_j)$ (ceci a un sens puisqu'un caractère est une fonction centrale). Nous allons passer en revue quelques exemples où on peut déterminer la table de caractères et parfois expliciter les différentes représentations irréductibles de G. La table des caractères est une information importante, même si deux groupes peuvent avoir la même table (i.e. le tableau est le même pour un certain choix dans l'ordre des χ_i et des c_i) sans être isomorphes (c'est le cas par exemple pour le groupe diédral d'ordre 8 et le groupe des quaternions d'ordre 8).

La première étape pour trouver la table de caractères d'un groupe G consiste en général à déterminer les morphismes de G dans $\mathbf{C}^*$, qui donnent les représentations de degré 1 ; ils correspondent aussi aux morphismes de $G^{\text{ab}} = G/D(G)$ dans $\mathbf{C}^*$ (puisqu'un morphisme de G dans un groupe abélien est trivial sur tout commutateur, donc sur le sous-groupe dérivé $D(G)$). Il y a donc $\#G^{\text{ab}}$ représentations de degré 1 (on peut le voir par exemple en décomposant G^{ab} en produit de groupes cycliques). On peut ensuite déterminer le nombres de classes de conjugaison c de G soit directement, soit parfois en utilisant le théorème 3.21, c). Les valeurs des caractères de degré 1 sont souvent assez faciles à déterminer, et on s'aide du théorème 3.21 c) pour les autres caractères.

4.1. Le groupe $\mathcal{S}_3$

Soit $\mathcal{S}_3$ le groupe des permutations d'un ensemble à 3 éléments, qui possède le groupe alterné $\mathcal{A}_3$ comme sous-groupe distingué d'indice 2. Le cardinal de G est $g = 6$, et le nombre de classes de conjugaison est $h = 3$: l'élément 1, la classe d'une transposition t, et la classe d'un 3-cycle c.

On a deux représentations irréductibles de degré 1, correspondant au caractère unité χ_1 et à la signature ϵ. On sait qu'il y a un troisième caractère irréductible θ, qui vérifie $(\deg\theta)^2+2=6$ d'après la Prop. 3.21 c). Ainsi θ est de degré 2. On obtient aussi avec la Prop. 3.21 c), que $\theta(s)=1/2(-1-\epsilon(s))$ si $s\neq 1$ et $\theta(1)=\deg\theta=2$, d'où la table de caractères :

$$\begin{pmatrix} & 1 & t & c \\ \chi_1 & 1 & 1 & 1 \\ \epsilon & 1 & -1 & 1 \\ \theta & 2 & 0 & -1 \end{pmatrix}$$

La représentation irréductible de degré 2 peut se réaliser géométriquement en voyant $\mathcal{S}_3$ comme le groupe des isométries d'un triangle équilatéral (qui est un sous-groupe de $O_2(\mathbf{R})\subset \mathrm{GL}_2(\mathbf{C})$). En effet, les transpositions correspondent à des réflexions (de trace nulle) et les 3-cycles à des rotations d'angle $2\pi/3$ (de trace -1).

4.2. Le groupe $\mathcal{A}_4$

Soit $G=\mathcal{A}_4$, c'est un groupe de cardinal 12. Le groupe G possède un sous-groupe distingué $V_4\simeq(\mathbf{Z}/2\mathbf{Z})^2$, constitué de l'identité et des doubles transpositions, et $H=G/V_4$ est de cardinal 3, donc isomorphe à $\mathbf{Z}/3\mathbf{Z}$ (c'est d'ailleurs l'abélianisé de G). On a donc déjà trois caractères irréductibles de degré 1 de G, notés χ_1 (caractère trivial), χ_2, χ_3, correspondant aux trois caractères du groupe cyclique H. Par ailleurs G possède 4 classes de conjugaison : celle de 1, celle d'une double transposition x, celle du 3-cycle $y=(1,2,3)$ et celle du 3-cycle $z=(2,1,3)$ (qui est conjugué du précédent dans $\mathcal{S}_4$ mais pas dans $\mathcal{A}_4$).

Le caractère χ_2 est non trivial, donc envoie y (dont l'image dans H en est un générateur) sur une racine primitive cubique j de l'unité. Le caractère χ_3 envoie alors y sur l'autre élément non trivial d'ordre 3 de $\mathbf{C}^*$, à savoir j^2.

Le dernier caractère irréductible χ' est de degré $\sqrt{12-(1+1+1)}=3$ par la Prop. 3.21 c), et on détermine les valeurs de χ' par cette même proposition, ce qui donne la table de caractères suivante :

$$\begin{pmatrix} & 1 & x & y & z \\ \chi_1 & 1 & 1 & 1 & 1 \\ \chi_2 & 1 & 1 & j & j^2 \\ \chi_3 & 1 & 1 & j^2 & j \\ \chi' & 3 & -1 & 0 & 0 \end{pmatrix}$$

Une autre possibilité, si on ne veut pas au départ chercher les classes de conjugaison de G, est d'utiliser le fait que comme G^{ab} est de cardinal

3, il y a exactement trois représentations de degré 1 ; on voit alors que la seule possiblité pour que la somme des degrés au carré des représentations irréductibles donne 12, est que $h = 4$; pour cela, il faut savoir que V_4 est bien le sous-groupe dérivé de $\mathcal{A}_4$.

Remarque 4.1 Dans l'espace euclidien $\mathbf{R}^3$, soit T le tétraèdre régulier de centre 0, de sommets $(1,1,1), (1,-1,-1), (-1,1,-1), (-1,-1,1)$. Le groupe $\mathcal{S}_4$ peut se réaliser comme le groupe des isométries de $\mathbf{R}^3$ laissant stable T, et son sous-groupe $\mathcal{A}_4$ correspond alors aux isométries positives (les rotations).

On obtient ainsi un morphisme injectif $\mathcal{S}_4 \to \mathrm{GL}_3(\mathbf{R})$, et donc une représentation fidèle $\rho : \mathcal{S}_4 \to \mathrm{GL}_3(\mathbf{C})$, que l'on peut restreindre à $\mathcal{A}_4$. La trace d'une rotation d'angle $\pm\theta$ est $1+2\cos(\theta)$. L'image de $x \in \mathcal{A}_4$ par ρ doit être d'ordre 2, c'est donc un renversement (rotation d'angle π), dont la trace est -1, tandis que les images de y et z sont des rotations d'ordre 3, donc d'angle $\pm 2\pi/3$ et de trace nulle. Ainsi le caractère de $\rho : \mathcal{A}_4 \to \mathrm{GL}_3(\mathbf{C})$ est χ', et cette représentation "géométrique" est bien la représentation irréductible de degré 3 de $\mathcal{A}_4$.

4.3. Le groupe $\mathcal{S}_4$

Ce cas est déjà nettement plus compliqué, et va nécessiter d'utiliser les remarques générales suivantes (valables pour tout groupe fini G) :

Remarque 4.2 a) Si N est un sous-groupe distingué de G et $H := G/N$, alors toute représentation ρ de H donne naissance[6] à une représentation τ de G définie par la formule $\tau(s) = \rho(\pi(s))$ pour tout $s \in G$, où $\pi : G \to H$ est la surjection canonique. On a clairement : ρ irréductible $\Leftrightarrow$ τ irréductible. On va voir une application de ce principe pour $G = \mathcal{S}_4$ et $N = V_4$ (sous-groupe constitué des doubles transpositions).

b) Si la restriction d'une représentation ρ_G de G à un sous-groupe H de G est irréductible, il est immédiat que ρ_G elle-même est irréductible. Là encore, ce sera utile dans le cas $G = \mathcal{S}_4$ (avec $H = \mathcal{A}_4$).

c) Si $\varepsilon : G \to \mathbf{C}^*$ est un caractère de degré 1 de G, et χ est le caractère d'une représentation irréductible ρ, alors $\varepsilon\chi$ est encore le caractère d'une représentation irréductible, à savoir la représentation $s \mapsto \varepsilon(s)\rho(s)$ (vérification immédiate). Cette remarque est souvent utile pour les groupes symétriques (en prenant pour ε la signature).

6. En revanche définir une représentation de G à partir d'une représentation d'un sous-groupe n'est pas évident : c'est la notion importante de *représentation induite*, qui n'est pas au programme de l'agrégation.

Comme on sait que dans un groupe symétrique, les classes de conjugaison sont déterminées par la décomposition en cycles d'une permutation, on obtient que $G = \mathcal{S}_4$ possède 5 classes de conjugaison : celle de 1, celle d'une transposition t, celle d'une double transposition d, celle d'un 3-cycle c, et celle d'un 4-cycle q.

Le groupe G possède encore le sous-groupe V_4 (constitué de l'identité et des doubles transpositions) comme sous-groupe distingué, avec cette fois-ci un quotient $S = \mathcal{S}_4/N$ isomorphe à $\mathcal{S}_3$. Les trois caractères irréductibles χ_1, ϵ et θ de $\mathcal{S}_3$ vus au paragraphe 4.1. sont de degré respectif 1, 1, et 2, et correspondent (cf. remarque 4.2, a) à trois caractères irréductibles de ces mêmes degrés de $\mathcal{S}_4$ (on les notera encore χ_1, ϵ et θ). Noter que si on sait que le sous-groupe dérivé de $\mathcal{S}_4$ est $\mathcal{A}_4$ (qui est d'indice 2), cela donne tout de suite qu'il n'y a que deux représentations de degré 1 (ce qui permet de prévoir via la formule $\sum n_i^2 = \#G = 24$ du théorème 3.21 c) qu'il reste deux autres représentations irréductibles, chacune de degré 3).

On a d'autre part la représentation géométrique fidèle $\rho : G \to \mathrm{GL}_3(\mathbf{R}) \subset \mathrm{GL}_3(\mathbf{C})$ de la remarque 4.1. Pour $s \in G$, le déterminant de $\rho(s)$ est la signature de s (il suffit de le vérifier quand s est une transposition, ce qui est facile puisqu'alors $\rho(s)$ induit l'identité sur un plan et l'opposé de l'identité sur la droite orthogonale à ce plan). Comme on a vu au paragraphe précédent que la restriction de ρ à $\mathcal{A}_4$ était irréductible, on obtient que ρ est irréductible (remarque 4.2, b)), et de degré 3. Enfin, on obtient (cf. remarque 4.2, c)) une autre représentation irréductible ρ_ε de degré 3 de G en posant $\rho_\varepsilon(s) = \varepsilon(s).\rho(s)$, où ε est la signature. Comme $1^2 + 1^2 + 2^2 + 3^2 + 3^2 = 24 = |G|$, on a obtenu toutes les représentations irréductibles de G (ce qui est cohérent avec le fait qu'il y a 5 classes de conjugaison dans G).

Les valeurs des caractères χ_1, ϵ et θ se déduisent de la table de caractères de $S \cong \mathcal{S}_3$, en observant que l'image de t et q (qui sont d'ordre pair) dans S correspond à la classe d'une transposition (car cette image ne peut être que d'ordre 2), l'image de c (d'ordre 3) correspond à la classe d'un 3-cycle de $\mathcal{S}_3$, et l'image de d est le neutre de S.

Les valeurs du caractère ψ de ρ en d et c se déduisent de la table de caractère de $\mathcal{A}_4$. Enfin, l'image de t par ρ est (comme on l'a déjà vu) une réflexion par rapport à un plan (de trace 1) ; l'image de q par ρ est une isométrie négative d'ordre 4, dont la matrice dans une base adaptée est donc

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$$

qui est de trace -1. On en déduit la table de caractères de $\mathcal{S}_4$:

$$\begin{pmatrix} & 1 & t & d & c & q \\ \chi_1 & 1 & 1 & 1 & 1 & 1 \\ \varepsilon & 1 & -1 & 1 & 1 & -1 \\ \theta & 2 & 0 & 2 & -1 & 0 \\ \psi & 3 & 1 & -1 & 0 & -1 \\ \varepsilon\psi & 3 & -1 & -1 & 0 & 1 \end{pmatrix}$$

Pour aller plus loin sur la théorie des représentations, on pourra consulter la partie I de [3].

5. Compléments : Produit semi-direct

Soit N un groupe. L'ensemble $\texttt{Aut}\, N$ 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 $\varphi : H \to \texttt{Aut}\, N$ 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 $\texttt{Aut}\, N$, 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 $\texttt{Aut}\, N$). 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 $(h^{-1}.n^{-1})(h^{-1}.n) = h^{-1}.(nn^{-1}) = h^{-1}.1 = 1$).

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*[7] *H par N* s'il existe une suite exacte courte

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

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)[8] *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.*

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

8. 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 $\Phi((n,h)(n',h')) = \Phi(n(hn'h^{-1}),hh') = nhn'h'$. L'injectivité de Φ résulte de ii) et sa surjectivité de iii).

2. Posons $H_1 = s(H)$. Comme s est injective vu que $p \circ s = \mathrm{id}_H$, H_1 est un sous-groupe de G isomorphe à H et via 1., il suffit de montrer : $N \cap H_1 = \{1\}$ et $NH_1 = G$ (on a identifié N à son image dans G). Si $h_1 \in N \cap H_1$, alors

$p(h_1) = 1$ mais $h_1 = s(h)$ avec $h \in H$, d'où $1 = p(s(h)) = h$ et $h_1 = 1$. Si maintenant $g \in G$, alors g et $s(p(g))$ ont même image par p, donc ils diffèrent d'un élément du noyau N, i.e. $g = nh_1$ avec $h_1 := s(p(g))$, et $g \in NH_1$.

□

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

Exemple 5.7 1. Pour $n \geq 2$, la suite exacte

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

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

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

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

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

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

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

(obtenue en envoyant x (mod. 4) sur x (mod.2), le noyau est $\{\bar{0}, \bar{2}\}$ qui est isomorphe à $\mathbf{Z}/2\mathbf{Z}$) n'est pas scindée. [9]

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 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

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

9. 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 !).

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 $x \in \mathbf{Z}/n\mathbf{Z}$.

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, qui ne se décompose pas en produit semi-direct de groupes plus petits ([2], exercice IE1).

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.