Groupes Finis et leurs représentations

Jean-François Dat

2009-2010

Table des matières

1 Généralités

1.1 Groupes. Sous-groupes. Morphismes. Quotients

1.1.1 Définition.– *Un* groupe *est un ensemble muni d'une* loi de composition interne*, c-à-d une application*

$$\begin{array}{rcl} G \times G & \to & G \\ (x,y) & \mapsto & xy \end{array},$$

satisfaisant de plus les propriétés suivantes :

- *associativité : pour tous $x, y, z \in G$, on a $(xy)z = x(yz)$ qu'on peut donc noter xyz.*
- *existence d'un élément neutre e tel que $\forall x \in G, ex = xe = x$.*
- *existence d'inverses : $\forall x \in G, \exists y \in G, xy = yx = e$. On vérifie immédiatement qu'un tel y est unique, on l'appelle "inverse de x" et on le note x^{-1}.*

La loi peut être notée par différents symboles comme $(x, y) \mapsto x \circ y$ ou $x * y$ ou $x \cdot y$. Lorsque le groupe est commutatif, on la note volontiers $x + y$ (et l'inverse de x est alors noté $-x$ et appelé aussi "opposé de x"). À ce sujet, rappelons que :

- deux éléments x, y de G *commutent* si $xy = yx$
- le groupe G est *abélien* (ou *commutatif*) si c'est le cas pour tout $x, y \in G$.

Lorsque G est un ensemble fini, son cardinal (*i.e.* le nombre d'éléments de G) est appelé l'*ordre* de G, et est noté $|G|$.

1.1.2 Définition.– *Un* sous-groupe *H de G (notation : $H < G$) est une partie H contenant e , stable sous la loi de groupe de G et sous l'inversion, ou, de façon équivalente, telle que $xy^{-1} \in H$ pour tout $x, y \in H$.*

On vérifie facilement qu'une intersection de sous-groupes est encore un sous-groupe. Soit alors $S \subset G$ un sous-ensemble quelconque de G. L'intersection $\langle S \rangle$ des sous-groupes de G contenant S est appelé *sous-groupe engendré par S*. C'est le "plus petit" sous-groupe de G contenant S. Lorsque $S = \{x\}$ est un singleton, on note simplement $\langle x \rangle := \langle \{x\} \rangle$ le sous-groupe engendré par x. L'ordre $|\langle x \rangle|$ s'appelle l'ordre de x, et est parfois noté $\mathrm{ord}(x)$.

On dit que G est *monogène* s'il est engendré par un seul élément, et que G est *cyclique* s'il est monogène et d'ordre fini.

1.1.3 Définition.– *Un homomorphisme d'un groupe G vers un groupe G' est une application $f : G \to G'$ telle que $f(xy) = f(x)f(y)$ pour tout $(x, y) \in G \times G$.*

On a alors $f(e) = e'$ et $f(x^{-1}) = f(x)^{-1}$ pour tout x. On dit aussi *morphisme* au lieu de homomorphisme. On parle d'*endomorphisme* si $G = G'$, d'*isomorphisme* s'il existe un homomorphisme g de G' dans G tel que $f \circ g = id_{G'}, g \circ f = id_G$, d'*automorphisme* si f est à la fois un endomorphisme et un isomorphisme.

On vérifie immédiatement que l'image $f(H)$ d'un sous-groupe de G est un sous-groupe de G'. C'est en particulier le cas pour $f(G)$ que l'on note aussi $\mathrm{Im}(f)$.

De même l'image inverse (ou pré-image) $f^{-1}(H')$ d'un sous-groupe H' de G' est un sous-groupe de G. C'est en particulier le cas pour $f^{-1}(\{e'\})$ que l'on note aussi $\mathrm{Ker}(f)$ et que l'on appelle le *noyau* de f.

1.1.4 Soient A et B deux parties de G. On note AB (resp. A^{-1}) la *partie* de G formée des éléments de la forme $ab, a \in A, b \in B$ (resp. $a^{-1}, a \in A$). En d'autres termes, on a :

$$AB = \{x \in G,\ \exists (a,b) \in A \times B,\ x = ab\} \quad \text{et} \quad A^{-1} = \{a^{-1}, a \in A\}.$$

Par exemple, A est un sous-groupe de G si et seulement si A est non vide et $A.A^{-1} = A$. Si A et B sont des sous-groupes de G, AB est un sous-groupe de G si et seulement si $AB = BA$.

1.1.5 On appelle *classe à gauche modulo* H tout sous-ensemble C de G de la forme

$$C = xH = \{xh; h \in H\}$$

pour un élément x de G. Dans ce cas on a aussi $C = yH$ pour tout élément $y \in C$. Les éléments de C sont aussi appelés "représentants" de C dans G. L'ensemble des classes à gauche modulo H est noté G/H. C'est un sous-ensemble de l'ensemble $\mathcal{P}(G)$ des sous-ensembles de G, et on a une application "canonique" surjective

$$G \xrightarrow{\pi} G/H, \quad x \mapsto xH$$

dont les fibres sont justement les classes à gauche modulo H.

Supposons G fini. Le cardinal de G/H est noté $[G : H]$ et est appelé l'*indice* de H dans G. On définit de même l'ensemble $H \setminus G$ des classes à droite Hx ; il a encore $[G : H]$ éléments (considérer l'application $g \mapsto g^{-1}$).

Lorsque G est fini, toutes les classes à gauche modulo H ont le même nombre d'éléments, à savoir $|H|$. Comme deux classes distinctes sont disjointes, on obtient la relation :

1.1.6 Proposition.– $|G| = |H| \times [G : H]$.

Ainsi, si G est fini, $|H|$ divise $|G|$ (théorème de Lagrange) ; en particulier, *l'ordre de tout élément de G divise l'ordre de G.*

1.1.7 Définition.– *On dit que H est distingué dans G (ou normal) si pour tout $x \in G$ on a $xH = Hx$. Ceci équivaut à $\forall x \in G, xHx^{-1} = H$, ou encore plus explicite :*

$$\forall x \in X,\ \forall h \in H, xhx^{-1} \in H.$$

On note souvent $H \triangleleft G$ pour souligner qu'un sous-groupe $H < G$ est distingué.

1.1.8 Proposition.– *Supposons H distingué. Il existe alors une unique structure de groupe sur l'ensemble G/H telle que la surjection canonique $\pi : G \to G/H : x \mapsto xH$ soit un homomorphisme de groupes.*

Le groupe G/H obtenu dans la proposition est appelé *quotient* de G par H. Il est aussi caractérisé par la propriété suivante :

1.1.9 PROPOSITION.– *Pour tout morphisme $G \xrightarrow{f} G'$, si $f(H) = \{e'\}$ alors il existe un unique morphisme $\overline{f} : G/H \longrightarrow G'$ tel que f se factorise en :*

$$f : G \xrightarrow{\pi} G/H \xrightarrow{\overline{f}} G'.$$

Appliquant ceci au noyau de f, on obtient la décomposition canonique d'un homomorphisme :

1.1.10 PROPOSITION.– *Soit $f : G \to G'$ un homomorphisme de groupes. Alors $\mathrm{Ker}(f)$ est un sous groupe distingué de G et le morphisme $\overline{f}$ de la proposition précédente appliquée à $H = \mathrm{Ker}(f)$ induit un isomorphisme*

$$\overline{f} : G/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f)$$

qui s'insère dans la factorisation suivante de f :

$$f : G \xrightarrow{\pi} G/\mathrm{Ker}(f) \xrightarrow{\overline{f}} \mathrm{Im}(f) \xrightarrow{i} G'$$

où π est la projection canonique et i l'inclusion de $\mathrm{Im}(f)$ dans G.

En particulier, pour des groupes finis on a l'égalité $|G| = |\mathrm{Ker}(f)|.|\mathrm{Im}(f)|$. Enfin, les deux énoncés suivant seront démontrés en TD.

1.1.11 PROPOSITION.– *Soient G un groupe, H un sous-groupe distingué de G, et K un sous-groupe de G. Alors, $KH = HK$ est un sous-groupe de G, H est un sous-groupe distingué de KH, $H \cap K$ est un sous-groupe distingué de K, et l'application $x \mapsto \pi(x) = xH$ induit un isomorphisme $K/K \cap H \simeq KH/H$.*

1.1.12 PROPOSITION.– *Soient G un groupe, H un sous-groupe distingué de G. L'application $\pi : G \to G/H$ établit une bijection entre l'ensemble des sous groupes A de G contenant H et l'ensemble des sous-groupes A/H de G/H, pour laquelle on a $A \triangleleft G \Leftrightarrow A/H \triangleleft G/H$; dans ce cas, l'application $xH \mapsto xA$ induit un isomorphisme $(G/H)/(A/H) \simeq G/A$.*

1.1.13 *Produits directs. Somme directes.* Soient G, G' deux groupes. On définit une structure de groupes sur $G \times G'$ en posant $(x, x')(y, y') := (xy, x'y')$. Plus généralement, soit I un ensemble, et $\{G_i; i \in I\}$ une collection de groupes. On définit une structure de groupe, appelée *produit (direct)* et notée $\prod_{i\in I} G_i)$ sur le produit des ensembles G_i, en posant $(x_i)_{i\in I}.(y_i)_{i\in I} = (x_i y_i)_{i\in I}$. Si tous les G_i sont égaux à un G , ce groupe, noté G^I (ou G^n si $card(I) = n$ est fini), s'identifie au groupe des applications de I dans G. La notion duale de coproduit fournit, lorsque les G_i sont abéliens, celle de *somme directe* : c'est le sous-groupe $\oplus_{i\in I} G_i$ de, $\prod_{i\in I} G_i$ formé par les $(x_i)_{i\in I}$ tels que $x_i = e_i$ sauf pour un nombre fini d'indices $i \in I$.

1.1.14 *Automorphismes intérieurs et extérieurs.* Soit G un groupe. L'ensemble des automorphismes de G, muni de la loi de composition des applications, forme un groupe, noté $\mathrm{Aut}(G)$. Pour tout $h \in G$, l'application

$$\mathrm{Int}(h) : G \to G; g \mapsto \mathrm{Int}(h)(g) := hgh^{-1}$$

est un automorphisme de G, dit *intérieur*. On l'appelle aussi *conjugaison par* h. L'application $\mathrm{Int} : G \to \mathrm{Aut}(G) : h \mapsto \mathrm{Int}(h)$ est un homomorphisme de groupes, dont le noyau

$$Z(G) := \{h \in G,\ \forall g \in G, hg = gh\}$$

s'appelle le *centre* de G. L'image $\mathrm{Int}(G) \simeq G/Z(G)$ de Int est un sous-groupe distingué de $\mathrm{Aut}(G)$, puisque $\forall h \in G, f \in \mathrm{Aut}(G), f \circ \mathrm{Int}(h) \circ f^{-1} = \mathrm{Int}(f(h))$. Les éléments du groupe quotient $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Int}(G)$ s'appellent les automorphismes extérieurs de G.

Un sous-groupe H de G est ainsi distingué si $f(H) = H$ pout tout $f \in \mathrm{Int}(G)$. On dit que H est *caractéristique* si $f(H) = H$ pour tout $f \in \mathrm{Aut}(G)$. Par exemple, le centre de G est un sous-groupe caractéristique.

1.1.15 Définition.– *On dit qu'un groupe G est simple s'il n'admet pas de sous-groupe distingué propre (i.e. distinct de $\{1\}$ et de G).*

1.2 Premiers exemples

1.2.1 *Groupes monogènes et cycliques.* L'ensemble $\mathbb{Z}$ des entiers rationnels, muni de la loi d'addition, est un groupe monogène (engendré par 1), donc en particulier abélien. En fait, *tout groupe monogène est quotient de* $\mathbb{Z}$. En effet, si $G = \langle x \rangle$, l'application $m \in \mathbb{Z} \mapsto x^m \in G$ est un homomorphisme surjectif de $\mathbb{Z}$ dans G. Rappelons le fait suivant, classique :

Lemme. – *Tout sous-groupe non nul de $\mathbb{Z}$ est monogène, donc de la forme $n\mathbb{Z}$ pour un unique entier $n > 0$.*

Démonstration. Soit Γ un sous-groupe non nul de $\mathbb{Z}$ et soit n le plus petit élément strictement positif de Γ. On veut montrer que $\Gamma = n\mathbb{Z}$. Soit $m \in \Gamma$ non nul. Quitte à prendre son opposé, on peut le supposer positif. Par division euclidienne, il existe un unique couple (q, r) d'entiers positifs avec $r < n$ tel que $m = qn + r$. Ainsi $r = m - qn \in \Gamma$ est positif et $< n$, donc par définition de n, doit être nul. On a donc bien $m = qn \in n\mathbb{Z}$. □

Il s'ensuit que *tout groupe cyclique est isomorphe à un groupe quotient* $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence d'entiers modulo n. Si $G = \langle x \rangle$, un tel isomorphisme est donné par le morphisme précédent $m \in \mathbb{Z} \mapsto x^m \in G$ qui se factorise par $\mathbb{Z}/n\mathbb{Z}$ avec n l'ordre de x. On remarque ainsi que l'ensemble des isomorphismes $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} G$ est en bijection avec l'ensemble des générateurs de G. Ceci nous amène au rappel suivant :

Lemme. – *L'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$ est le sous-ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ des classes modulo n d'entiers premiers à n. C'est aussi le* sous-groupe des unités de l'anneau *$\mathbb{Z}/n\mathbb{Z}$ (i.e. le groupe des inversibles pour la multiplication, cf plus bas).*

Démonstration. Pour $x \in \mathbb{Z}$, notons $\overline{x}$ son image dans $\mathbb{Z}/n\mathbb{Z}$. Supposons x premier à n. Par Bezout, il existe deux entiers a, b tels que $ax+bn = 1$. On a donc $a\overline{x} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$, ce qui montre d'une part que $\overline{x}$ est inversible d'inverse $\overline{a}$, et d'autre part que $\langle\overline{x}\rangle \supseteq \langle\overline{1}\rangle = \mathbb{Z}/n\mathbb{Z}$. Réciproquement, supposons que $\overline{x}$ engendre $\mathbb{Z}/n\mathbb{Z}$. Alors il existe un entier a tel que $a\overline{x} = \overline{1}$ dans $\mathbb{Z}/n\mathbb{Z}$. Autrement dit, $ax \equiv 1$ modulo n, donc x est premier à n, et $\overline{x}$ est inversible d'inverse $\overline{a}$. □

Par ce qui précède, l'application $\alpha \mapsto \alpha(\overline{1})$ induit un isomorphisme $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$. L'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$ est traditionnellement noté $\phi(n)$, et la fonction $n \mapsto \phi(n)$ est appelée "fonction indicatrice d'Euler" (on pose $\phi(1) = 1$).

C'est le moment de rappeler le non moins classique *lemme chinois*. Auparavant, lorsque deux entiers n, m avec n divisant m seront donnés, on conviendra d'appeler *morphisme canonique* $\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ l'unique morphisme envoyant $\overline{1}$ sur $\overline{1}$, c'est-à-dire envoyant un entier x modulo m sur x modulo n.

LEMME. (Lemme chinois) – *Soient m_1 et m_2 deux entiers > 0 premiers entre eux. Alors, le morphisme canonique d'anneaux $\mathbb{Z}/m_1m_2\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z})\times(\mathbb{Z}/m_2\mathbb{Z})$ est un isomorphisme. En particulier, les groupes d'unités de ces anneaux sont isomorphes, et $\phi(m_1m_2) = \phi(m_1)\phi(m_2)$.*

Démonstration. Vu que source et but ont même cardinal, il suffit de prouver l'injectivité. Or, puisque m_1 et m_2 sont supposés premiers entre eux, un entier x est divisible par m_1m_2 si et seulement si il est divisible par m_1 et par m_2. □

Exercice. – À l'aide de Bézout, expliciter l'isomorphisme réciproque.

Exercice. – Pour tout nombre premier p et tout entier $k > 0$, montrer que $\phi(p^k) = p^{k-1}(p-1)$. En déduire que pour tout entier $n > 0$:

$$\phi(n) = n \prod_{p \text{ premier}, p|n} (1 - \frac{1}{p}).$$

Puisque l'ordre d'un élément divise l'ordre du groupe, on a pour tout entier x premier à n, $x^{\phi(n)} \equiv 1 \pmod{n}$, et en particulier (petit théorème de Fermat) :

$$\forall\ p \text{ premier}, \forall\ x \text{ t.q. } p \not| x\ :\ x^{p-1} \equiv 1 \bmod p.$$

Soient G un groupe cyclique, et n son ordre. Le premier lemme ci-dessus montre que tout sous-groupe de G est cyclique (et son ordre divise n).

Exercice. – Inversement, montrer que pour tout diviseur d de n, G admet un unique sous-groupe (forcément cyclique) d'ordre d.

En particulier, un groupe cyclique (ou, plus généralement, un groupe fini et abélien) est simple si et seulement son ordre est un nombre premier.

1.2.2 *Groupes d'unités.* Bien que l'on ait déjà utilisé cette notion, on rappelle qu'un *anneau* (unitaire) A est un groupe abélien (de loi notée additivement), muni d'une loi de composition interne $A\times A \to A : (x, y) \mapsto xy$ associative, distributive par rapport à la loi $+$ et admettant un élément neutre noté 1 . On appelle *unité* de A tout élément x de A tel qu'il existe $y \in A$ vérifiant $xy = yx = 1$ (y est alors unique, et noté x^{-1}). L'ensemble des unités d'un anneau non nul A forme un groupe (pour la loi multiplicative), noté $A^\times$. Si A_1 et A_2 sont deux anneaux, on munit (en calculant coordonnée par coordonnée comme pour les groupes) le produit $A_1 \times A_2$ d'une structure d'anneau. On a : $(A_1 \times A_2)^\times = (A_1)^\times \times (A_2)^\times$.

Nous avons déjà rencontré le groupe des unités $(\mathbb{Z}/n\mathbb{Z})^\times$ de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Le groupe $\mathbb{Z}^\times$ des unités de l'anneau $\mathbb{Z}$ est réduit à $\{\pm 1\}$. C'est un groupe cyclique, d'ordre 2. Le groupe des unités de l'anneau $\mathbb{Z}[i]$ est cyclique d'ordre 4. En revanche, le groupe des unités de l'anneau $\mathbb{Z}[\sqrt{2}]$ est infini.

Remarque. – On montre en théorie des nombres que le groupe des unités de l'anneau des entiers d'un extension finie de $\mathbb{Q}$ est un groupe abélien *de type fini*. Un tel groupe est (non canoniquement) isomorphe au produit de son sous-groupe fini maximal et d'un groupe $\mathbb{Z}^r$. La proposition suivante montre que le sous-groupe fini maximal est toujours *cyclique*.

Rappelons qu'un *corps* est un anneau non nul K tel que $K^\times = K \setminus \{0\}$. Il est dit *algébriquement clos* si tout polynôme $P(X) \in K[X]$ est *scindé*, i.e. de la forme $P(X) = c\prod_i (X - \alpha_i)$ pour des éléments α_i dans K. On rappelle qu'une *clôture algébrique* d'un corps K est un corps algébriquement clos $\overline{K}$ contenant K, et dont tous les éléments sont *algébriques* sur K (i.e. satisfont une équation polynômiale à coefficients dans K). On admet ici que *tout corps admet une clôture algébrique*, et on rappelle que celle-ci n'est unique qu'à isomorphisme près.

Le résultat suivant est bien connu des agrégatifs.

PROPOSITION. – *Soit K un corps. Tout sous-groupe fini G du groupe multiplicatif $K^\times$ est cyclique.*

Démonstration. Condidérons le polynôme $X^{|G|} - 1 \in K[X]$. Il a au plus $|G|$ racines distinctes. Or, tout élément de G en est une racine. Donc G est exactement l'ensemble de ses racines. En d'autre termes, G est le groupe des racines $|G|$-èmes de l'unité. On est donc ramené à prouver que ce groupe est cyclique, *i.e.* qu'il existe une racine *primitive* (d'ordre exactement $|G|$). Notons d'abord que $|G|$ est premier à la caractéristique de K (sinon le polynôme ci-dessus ne serait pas séparable et on n'aurait pas autant de racines).

On prouve l'existence d'une racine primitive d-ème de l'unité par récurrence "divisorielle" sur le diviseur d de $|G|$. Si d est premier, comme il est différent de $car(K)$, on sait que le polynôme $X^d - 1$ a d racines distinctes dans une clôture algébrique de K, et ces racines étant racines de $X^{|G|} - 1$, elles appartiennent à K. Toute racine d-ème différente de 1 est alors primitive. Maintenant, soit p un diviseur premier de $|G|$ et soit $d := |G|/p$. Supposons qu'on ait une racine d-ème primitive de l'unité x. Alors toute racine de $X^p - x$ dans une clôture algébrique de K est une racine primitive $|G|$-ème de l'unité (et appartient nécessairement à G). □

Si l'on applique ce résultat à un corps fini K, on constate que $K^\times$ est un groupe cyclique. Cependant, il n'est pas facile d'exhiber un générateur. Rappelons à ce propos le résultat suivant de théorie des corps.

1.2.3 THÉORÈME.– *Si K est un corps fini, son cardinal est une puissance d'un nombre premier p. Réciproquement, pour tout premier p et tout entier n, il existe un corps de cardinal p^n, unique à isomorphisme près. On le note $\mathbb{F}_{p^n}$.*

Démonstration. On pourrait admettre ce résultat dans le présent cours. Voici un résumé des arguments, en admettant l'existence des clôtures algébriques.

Soit K un corps fini ; l'image du morphisme d'anneaux canonique $\mathbb{Z} \longrightarrow K$ est un anneau intègre et fini, donc de la forme $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ pour un premier p. Ainsi, K est canoniquement un $\mathbb{F}_p$-espace vectoriel, nécessairement de dimension finie d, donc son cardinal est p^d. Choisissons un plongement de K dans une clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$. Par la proposition précédente, l'image de K est exactement l'ensemble des racines du polynôme $X^{p^d} - X$. En particulier, tout autre corps de cardinal p^d est isomorphe à K.

Réciproquement, fixons p et n comme dans l'énoncé. Considérons l'ensemble K des racines du polynômes $X^{p^n} - X$ dans $\overline{\mathbb{F}}_p$. Il est de cardinal p^n. Montrons que c'est un corps. Il contient 0 et 1. Pour $x, y \in K$, on a $(x-y)^{p^n} = x^{p^n} - y^{p^n} = x - y$ donc K est un sous-groupe additif. Pour $x, y \in K^\times$, on a $(xy^{-1})^{p^n} = xy^{-1}$ donc K est bien un sous-corps. □

Exemple. – $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$.

Soient K un corps commutatif, n un entier > 0 et $\mathrm{M}_n(K)$ l'anneau des matrices carrées d'ordre n à coefficients dans K. Son groupe des unités $(\mathrm{M}_n(K))^\times := \mathrm{GL}_n(K)$ est formé des matrices de déterminant non nul. Plus généralement, pour tout anneau commutatif A, le groupe $\mathrm{GL}_n(A)$ des unités de l'anneau $\mathrm{M}_n(A)$ des matrices carrées d'ordre n à coefficients dans A est formé des matrices x de déterminant $\det(x) \in A^\times$. Le quotient de $\mathrm{GL}_n(A)$ par le sous-groupe $A^\times \mathbf{I}_n$ des matrices scalaires (qui en forme le centre) est noté $\mathrm{PGL}_n(A)$. L'application $\det : \mathrm{GL}_n(A) \to A^\times$ est un homomorphisme de groupes, dont on note $\mathrm{SL}_n(A) = \{x \in \mathrm{M}_n(A), \det(x) = 1\}$ le noyau. Par exemple, $\mathrm{SL}_n(\mathbb{Z})$ est un sous-groupe (normal) d'indice 2 de $\mathrm{GL}_n(\mathbb{Z})$. On note $\mathrm{PSL}_n(A)$ l'image de $\mathrm{SL}_n(A)$ dans $\mathrm{PGL}_n(A)$.

Remarque. – Pour toute puissance q d'un nombre premier, le groupe $L_n(q) := \mathrm{PSL}_n(\mathbb{F}_q)$ est simple (sauf pour $n = 2, q = 2, 3$). On ne prouvera pas ce résultat ici.

1.2.4 *Groupe symétrique.* Soit X un ensemble. L'ensemble des bijections de X sur lui-même (appelées aussi *permutations* de X) forme un groupe pour la composition des applications : c'est le *groupe symétrique* S_X de X. Si, comme nous le supposons maintenant, X est de cardinal fini n, ou, de façon équivalente, $X = \{1, 2, ..., n\}$, on le note simplement S_n. Il a pour ordre $n!$. Ses éléments généraux se notent $\sigma : \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$.

Le *support* d'une permutation σ est le complémentaire de l'ensemble des éléments de X laissés fixes par σ. On vérifie facilement que *deux permutations de supports disjoints commutent.*

Un *cycle* est une permutation σ qui induit une permutation circulaire de son support. On peut donc numéroter ce support $\{i_1, \cdots, i_k\}$ de sorte que $\sigma(i_1) = i_2, \sigma(i_2) = i_3, ..., \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$. On note alors $\sigma = (i_1, ..., i_k)$. Notons qu'une telle numérotation n'est pas unique ; deux cycles $(i_1, ..., i_k)$ et $(j_1, ..., j_k)$ coïncident si et seulement s'il existe $t \in \mathbf{N}$ tel que $\forall s, j_s = i_{s+t}$, où les indices s sont lus dans $\mathbb{Z}/k\mathbb{Z}$. Le cardinal k du support est appelé *longueur du cycle.* On parle aussi de k-cycle. Un 2-cycle est plutôt appelé une *transposition.*

Rappelons le résultat classique suivant :

PROPOSITION. – *Tout élément $\sigma \in S_n$ peut s'écrire*

i) comme produit de cycles à supports disjoints, ces cycles étant déterminés de manière unique,

ii) comme produit de transpositions,

iii) comme produit de transpositions du type $(1, j)$, $j = 2, \cdots, n$,

iv) comme produit de transpositions du type $(i, i+1)$, $i = 1, \cdots, n-1$.

Démonstration. i) Par récurrence sur n. Soit k_1 le cardinal de l'orbite de $1 \in \{1, \cdots, n\}$ sous l'action des itérés de σ, et soit $c_1 := (1, \sigma(1), \cdots, \sigma^{k_1-1}(1))$, un cycle de longueur k_1. Alors le support de $\sigma' := c_1^{-1}\sigma$ est disjoint de celui de c_1. On peut donc appliquer l'hypothèse de récurrence.

ii) On vérifie que le cycle $(i_1, \cdots, i_k)$ est égal au produit $(i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$, puis on applique i). [Attention à l'ordre : on compose des applications, donc on commence par faire (i_{k-1}, i_k).]

iii) En effet, $(i, j) = (1, i)(1, j)(1, i)$.

iv) En effet, supposons $i < j$. On vérifie que

$$(j-1, j)(j-2, j-1) \cdots (i+1, i+2)(i, i+1)(i+1, i+2) \cdots (j-2, j-1)(j-1, j) = (i, j).$$

□

Exercice. – Montrer que S_n est engendré par $(1, 2)$ et $(1, 2, \cdots, n)$.

On appelle *signature* $sgn(\sigma)$ d'un élément σ de S_n le nombre $\Pi_{1 \leqslant i < j \leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j} = \pm 1$. On dit que σ est paire (resp. impaire) si sa signature vaut 1 (resp. -1). Par exemple, une transposition est une permutation impaire, un cycle de longueur k a pour signature $(-1)^{k+1}$. L'application $sgn : S_n \to \{\pm 1\}$ est un homomorphisme de groupes. Son noyau, dont les éléments sont donc les permutations paires, s'appelle le *groupe alterné* A_n. Pour $n \geqslant 2$, c'est un sous-groupe (normal) d'indice 2 de S_n.

Remarque. – Les groupes A_n sont simples dès que $n \geqslant 5$. C'est un résultat classique qui sera prouvé en TD.

1.3 Groupes abéliens finis

Un produit (direct) de groupes cycliques, ou plus généralement abéliens, est évidemment abélien. La réciproque est vraie : tout groupe abélien fini est isomorphe à un produit de groupes cycliques. Plus précisément :

1.3.1 THÉORÈME.– *Soit G un groupe abélien fini $\neq \{0\}$. Il existe une unique famille d'entiers $a_1, ..., a_s \geqslant 2$, vérifiant les propriétés suivantes :*
i) pour tout $i = 1, ..., s-1$, a_i divise a_{i+1} ;
ii) G est isomorphe au produit $(\mathbb{Z}/a_1\mathbb{Z}) \times ... \times (\mathbb{Z}/a_s\mathbb{Z})$.
On appelle ces entiers a_i les facteurs invariants *de G.*

Démonstration. La preuve directe qui suit repose sur le lemme suivant, où l'*exposant* du groupe fini G désigne le ppcm des ordres de ses éléments ; de façon équivalente, le pgcd des entiers n (ou encore : le plus petit des entiers $n \geqslant 1$) tels que $\forall x \in G, nx = 0$.

1.3.2 LEMME.– *Soient G un groupe abélien fini, et r l'exposant de G. Alors, G possède un élément d'ordre r.*

Démonstration. Il suffit par induction de montrer que si x et y sont deux éléments de G d'ordres respectifs n et m, il existe un élément de G d'ordre $r = ppcm(n, m)$. En décomposant n et m en produits de puissances de nombres premiers, on voit qu'il existe des diviseurs n' de n, m' de m, premiers entre eux, tels que $r = n'm'$. Alors, $x' = \frac{n}{n'}x$ est d'ordre n', $y' = \frac{m}{m'}y$ est d'ordre m', et $x'y'$ est d'ordre $ppcm(n', m') = r$. □

Existence des a_i (par récurrence sur $|G|$). Soient a_s l'exposant de G, x_s un élément de G d'ordre a_s, et G' le groupe quotient $G/ < x_s >$. D'après l'hypothèse de récurrence, il existe des entiers $a_1, ..., a_{s-1}$ se divisant successivement, et des éléments $x'_1, ..., x'_{s-1}$ de G' d'ordres respectifs $a_1, ..., a_{s-1}$, tels que $G' =< x'_1 > \times ... \times < x'_{s-1} >$; noter que a_{s-1} est l'exposant de G', qui divise l'exposant a_s de G. Montrons que pour tout $i = 1, ..., s-1$, il existe un élément x_i de G d'ordre a_i dont l'image dans G' soit x'_i. Soit y_i un représentant de x'_i dans G. Alors, $a_i y_i \in < x_s >$, et il existe un entier k_i tel que $a_i y_i = k_i x_s$. Je dis que a_i divise k_i, et que $x_i := y_i - \frac{k_i}{a_i}x_s$ répond à la question. En effet, $0 = a_s y_i = \frac{a_s}{a_i}a_i y_i = (\frac{a_s}{a_i}k_i)x_s$, donc a_s divise $\frac{a_s}{a_i}k_i$ et $a_i | k_i$. Alors, $a_i(y_i - \frac{k_i}{a_i}x_s) = 0$, donc l'ordre de x_i divise a_i, et lui est égal puisque l'image x'_i de x_i dans G' est déjà d'ordre a_i.

Dans ces conditions, le sous-groupe $H =< x_1 > \times ... \times < x_{s-1} >$ de G ne rencontre $K =< x_s >$ qu'en 0 ($n_1x_1 + ... + n_{s-1}x_{s-1} = n_s x_s \Rightarrow n_1x'_1 + ... + n_{s-1}x'_{s-1} = 0 \Rightarrow a_1 | n_1, ..., a_{s-1} | n_{s-1} \Rightarrow n_1x_1 = ... = n_{s-1}x_{s-1} = 0$), et $|G| = |G'|.|K| = |H|.|K|$. Le groupe abélien G est donc produit direct de H et K, d'où la décomposition recherchée.

Unicité des a_i. Le plus grand facteur invariant étant l'exposant de G, son unicité est claire, mais c'est par celle de a_1 (et de s) qu'on va débuter. Pour tout entier d, posons $\Phi(d) = card\{x \in G, dx = 0\}) = \prod_{i=1,...,s}(pgcd(d, a_i)) \leqslant d^s$. Alors, s est le plus petit des entiers k tels que $\Phi(d) \leqslant d^k$ pour tout $d \geqslant 1$, et ne dépend donc que de G. De plus, a_1 est le plus grand des entiers d tels que $\Phi(d) \geqslant d^s$, et ne dépend donc que de G.

On conclut par une récurrence sur $|G|$: soit $G[a_1]$ le sous-groupe de G formé des éléments d'ordre divisant a_1. Pour tout $i \geqslant 1$, $(\mathbb{Z}/a_i\mathbb{Z})[a_1] = \frac{a_i}{a_1}\mathbb{Z}/a_i\mathbb{Z}$, donc $G/G[a_1]$ admet pour facteurs invariants $(\frac{a_2}{a_1}, ..., \frac{a_s}{a_1})$. L'hypothèse de récurrence entraîne qu'ils ne dépendent que de G. Il en est donc de même des facteurs invariants $(a_1, ..., a_s)$ de G. □

2 Actions. Produits semi-directs. Groupes classiques

2.1 Action d'un groupe sur un ensemble

2.1.1 Définition.– *Soient G un groupe, et X un ensemble. Une* action *(à gauche) de G sur X est une application*

$$\begin{array}{rcl} G \times X & \to & X \\ (g,x) & \mapsto & g.x \end{array}$$

vérifiant les propriétés suivantes :

- *Pour tout $x \in X$, on a $e.x = x$.*
- *Pour tout $x \in X$ et tout $(g,h) \in G \times G$, on a $g.(h.x) = (gh).x$.*

Ici aussi, l'action peut être notée de plusieurs manières : $g \cdot x$, $g * x$, ou simplement gx et parfois ${}^g x$. La donnée d'une action de G sur X équivaut à celle d'un homomorphisme τ de G dans le groupe S_X des permutations de X : poser $\tau(g)(x) = g.x$ et noter que $\tau(g^{-1}) = (\tau(g))^{-1}$. On dit aussi que G *opère* (à gauche) sur X (par τ). On définit de même ce qu'est une action à droite de G sur X : $(g,x) \mapsto xg$, avec la condition $x(gh) = (xg)h$.

2.1.2 *Orbites.* Soit G un groupe agissant sur un ensemble X (quand on ne précise pas, cela veut dire "à gauche"). Si A (resp. Y) est une partie de G (resp. X), on note AY l'ensemble des éléments de X de la forme $ay, a \in A, y \in Y$.

$$AY = \{x \in X, \exists (a,y) \in A \times Y,\ x = a.y\}.$$

Pour tout $x \in X$, la partie $G\,x := G\{x\} = \{gx, g \in G\}$ de X s'appelle l'*orbite* sous G (ou G-orbite) de x. Alors, $G\,x = G\,y$ si et seulement si $y \in G\,x$, et l'ensemble $G \setminus X$ des G-orbites forme une partition de X. Si l'action de G sur X est à droite, on le note X/G.

On dit que G agit *transitivement* sur un ensemble X si $G \setminus X$ n'a qu'un élément. Par exemple, G agit transitivement sur chaque orbite.

2.1.3 *Points fixes. Stabilisateurs.* Soient x un point de X, et H un sous-groupe de G. On dit que x est fixé par H si $\forall h \in H, hx = x$. On note X^H l'ensemble des points de X fixés par H. Inversement, pour tout $x \in X$, on appelle *stabilisateur* (ou fixateur) de x le sous-groupe $G_x := \{g \in G, gx = x\}$. On dit que G agit *fidèlement* sur X si $\cap_{x \in X} G_x = \{1\}$, c'est-à-dire si l'homomorphisme τ est injectif. Plus généralement, pour toute partie Y de X, le fixateur $Fix_G(Y)$ de Y est le sous-groupe $\cap_{x \in Y} G_x$ de G formé des éléments qui fixent Y point par point. En général, l'ensemble $\{g \in G, gY \subset Y\}$ des éléments de G qui laissent stable Y globalement est seulement un sous-monoïde de G (partie stable par la loi de groupe et contenant 1). Néanmoins, il coïncide souvent (par exemple si Y est fini) avec le sous-groupe $G_Y := \{g \in G, gY = Y\}$ de G, qu'on appelle alors le *stabilisateur* de Y.

2.1.4 *Exemples.* (i) soit H un sous-groupe de G. Alors, H agit à gauche sur G par translation : $(h,g) \mapsto hg$, et une orbite Hg n'est autre qu'une classe à droite modulo H.

Les deux notations $H \setminus G$ (1.1.5 et 2.1.2) sont donc compatibles. Idem avec G/H, pour l'action de H sur G par translation à droite. Pour chacune de ces actions, le fixateur de tout élément est réduit à $\{1\}$.

(ii) l'action (à gauche) $(g, x) \mapsto gxg^{-1}$ de G sur $X = G$ donnée par l'homomorphisme $\tau = \mathrm{Int}$ s'appelle *l'action par conjugaison* de G sur G. Deux éléments de G sont dit *conjugués* s'ils sont dans une même orbite. Les orbites $C_x := \{gxg^{-1}, g \in G\}$ s'appellent les *classes de conjugaison* (des éléments) de G. L'ensemble des classes de conjugaison de G sera noté $C\ell(G)$, ou encore G/adG ; son cardinal $c\ell(G)$ s'appelle le nombre de classes de G. Pour toute partie Y de G, le fixateur $Z_G(Y) = \{g \in G, \forall\ y \in Y, gy = yg\}$ de Y s'appelle le *centralisateur* (ou commutant) de Y (dans G). Le sous-groupe $N_G(Y) = \{g \in G, gY = Yg\}$ s'appelle le *normalisateur* de Y (dans G). Le centralisateur de G lui-même est le centre $Z(G) = Z_G(G)$ de G.

(iii) soit $S(G)$ l'ensemble des sous-groupes de G. Pour tout $g \in G, H \in S(G)$, $H' = gHg^{-1}$ est encore un sous-groupe de G, et cela munit $S(G)$ d'une action de G. Deux sous-groupes de G sont dit conjugués s'ils sont dans une même orbite. Les orbites s'appellent les classes de conjugaison de sous-groupes de G. Pour $H \in S(G)$, le fixateur de H n'est autre que son normalisateur $N_H(G)$; c'est le plus grand sous-groupe de G dans lequel H est normal. Par exemple, $H \lhd G \Leftrightarrow N_H(G) = G$..

2.1.5 Soit G un groupe agissant sur un ensemble X. Pour tout $x \in X$, l'application $g \mapsto gx$ induit une bijection de G/G_x sur $G.x$ (dans laquelle la classe de 1 s'envoie sur x). En particulier,

$$|G.x| = [G : G_x].$$

Si on remplace x par $x' = gx \in G.x$, alors G_x est remplacé par le sous-groupe $G_{x'} = gG_xg^{-1}$, et inversément. Donc la donnée de X où G agit transitivement équivaut à celle de la classe de conjugaison d'un stabilisateur dans G. Par exemple, pour tout corps K, le groupe $G = Aff^1(K)$ des similitudes $x \mapsto ax + b, a \in K^\times, b \in K$ de la droite affine $X = \mathbf{A}^1(K)$ agit transitivement sur X ; pour tout $x \in X$, le stabilisateur de x est le sous-groupe des homothéties centrées en x, et on peut identifier X à la classe de conjugaison du sous-groupe $\mathrm{GL}_1(K) = K^\times$ de G.

2.1.6 Soient G un groupe fini agissant sur un ensemble fini X, et $x_1, ..., x_m$ un système de représentants des orbites de X sous G. Autrement dit, m est le cardinal de $G \setminus X$, et $X = \cup_{i=1,...m} Gx_i$ (réunion disjointe). Donc $|X| = \Sigma_{i=1,...,m}[G : G_{x_i}] = \Sigma_{i=1,...,m} \frac{|G|}{|G_{x_i}|}$ et

$$\frac{|X|}{|G|} = \sum_{i=1}^{m} \frac{1}{|G_{x_i}|}.$$

Appliquons cette "*formule des classes*" à l'action de G sur lui-même par conjugaison. Dans ce cas, $m = c\ell(G)$ est le nombre de classes de conjugaison de G, chaque G_{x_i} est le centralisateur $Z_G(x_i)$ de x_i dans G (par exemple, la classe de $x_1 = 1$, qui est réduite à un

élément, vérifie $Z_G(1) = G$), et on obtient

$$1 = \sum_{i=1}^{c\ell(G)} \frac{1}{|Z_G(x_i)|}.$$

2.2 Produits semi-directs et extensions

2.2.1 Soient A et C deux groupes. On dit qu'une action (à gauche) de C sur A est compatible avec la structure de groupe de A si l'homomorphisme correspondant $\tau : C \to S_A$ est à valeurs dans $\mathrm{Aut}(A)$. Autrement dit, en notant ${}^c a = \tau(c)(a)$ cette action, on veut que ${}^c(a_1 a_2) = {}^c a_1 . {}^c a_2$ pour tous c, a_1, a_2.

2.2.2 PROPOSITION.– *Avec les notations ci-dessus, l'ensemble $A \times C$, muni de la loi de composition interne*

$$(a, c), (a', c') \to (a.{}^c a', c.c'),$$

est un groupe, d'élement neutre $(1, 1)$ (avec $(a, c)^{-1} = ({}^{c^{-1}} a^{-1}, c^{-1})$).

Le groupe défini dans la proposition est appelé *produit semi-direct de C par A relativement à $\tau : C \to \mathrm{Aut}(A)$*, et noté $A \times_\tau C$.

2.2.3 *Injections.* Les applications $i : A \to A \times_\tau C : i(a) = (a, 1)$ et $s : C \to A \times_\tau C : s(c) = (1, c)$ sont alors des homomorphismes de groupes injectifs, qui permettent d'identifier A et C à des sous-groupes de $A \times_\tau C$. Avec cette identification, A est normal dans G, et l'action de G sur A par conjugaison induit précisément τ sur C : ${}^c a = cac^{-1}$. En revanche, C n'est en général pas normal dans G : il l'est si et seulement si l'action est triviale ($\tau = id_A$), auquel cas le produit semi-direct n'est autre que le produit direct $A \times C$ des groupes A et C. L'application $\phi : A \times C \to A \times_\tau C : (a, c) \mapsto ac$ (c-à-d. $i(a)s(c)$) est toujours une bijection *ensembliste*, mais n'est un isomorphisme de groupes que si τ est triviale.

2.2.4 *Projections.* La projection $p : A \times_\tau C \longrightarrow C$, $(a, c) \mapsto c$ est un homomorphisme surjectif de groupes. Son noyau est A, identifié à un sous-groupe de $A \times_\tau C$ via l'injection i définie ci-dessus. En revanche, la projection $A \times_\tau C \longrightarrow A$, $(a, c) \mapsto a$ n'est généralement *pas un morphisme de groupes*. Elle l'est si et seulement si τ est l'action triviale, auquel cas son noyau est C identifié à un sous-groupe de $A \times_\tau C$ via l'injection s ci-dessus.

2.2.5 *Exemple : groupes diédraux.* soit n un entier $\geqslant 2$. Le groupe diédral D_n est le stabilisateur dans $O_2(\mathbf{R})$ d'un polygone régulier à n sommets (un segment si $n = 2$), centré à l'origine. Son intersection avec $SO_2(\mathbf{R})$ est le groupe cyclique C_n d'ordre n engendré par la rotation r d'angle $2\pi/n$. L'indice de ce sous-groupe divise $[O_2(\mathbf{R}) : SO_2(\mathbf{R})] = 2$, et vaut 2 puisque D_n contient l'une quelconque, soit s, des symétries par rapport aux droites joignant l'origine à un sommet. On a

$$r^n = 1, s^2 = 1, srs = srs^{-1} = r^{-1},$$

d'où $sr^{-k}s = r^k$ pour tout entier k. Ainsi, D_n est un groupe d'ordre $2n$, isomorphe au produit semi-direct $C_n \times_\tau \{\pm 1\}$, pour l'action de $\{\pm 1\}$ sur C_n donnée par $\tau(-1)(a) := a^{-1}$. Les éléments d'ordre 2 de D_n sont les n symétries sr^k, ainsi que, pour n pair, la rotation $r^{n/2}$. Pour $n = 2$, le produit est direct, et le groupe D_2, isomorphe à $C_2 \times C_2$, est souvent noté $\mathbf{V}$ (Vierergruppe ; il apparaît comme sous-groupe distingué d'indice 3 de A_4, qui est donc résoluble). Le groupe D_3 est isomorphe au groupe symétrique S_3.

2.2.6 *Extensions.* Une suite de morphismes de groupes

$$A \overset{i}{\hookrightarrow} E \overset{p}{\twoheadrightarrow} C$$

avec i injective, p surjective, et $\mathrm{Im}(i) = \mathrm{Ker}(p)$ est appelée *suite exacte courte*. On dit aussi que (E, i, p) *est une extension de C par A*. Un produit semi-direct de C par A est donc en particulier une extension de C par A. On aimerait savoir à quelle condition une extension est un produit-semidirect pour une action τ convenable, et à quel point cette action τ est bien déterminée. Pour cela appelons *morphisme d'extension* $(E, i, p) \overset{\varphi}{\longrightarrow} (E', i', p')$ tout morphisme de groupe $\varphi : E \longrightarrow E'$ tel que $\varphi \circ i = i'$ et $p' \circ \varphi = p$.

2.2.7 Proposition.– *Soit (E, i, p) une extension de C par A. Alors (E, i, p) est isomorphe à un produit semi-direct $(A \times_\tau C, i, p)$ si et seulement si il existe une section s de p,* i.e. *un morphisme de groupes $s : C \longrightarrow E$ tel que $p \circ s = \mathrm{Id}_E$. On dit alors que l'extension (E, i, p) est* scindée.

2.2.8 *Exemple : groupe quaternionien.* considérons le corps des quaternions de Hamilton $\mathbf{H} = \mathbf{R} \oplus \mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k$, dont la loi de multiplication est définie par $\mathbf{R}$-bilinéarité à partir des relations $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$ (on vérifie qu'elle est bien associative). Le groupe quaternionien H_8 est le sous groupe

$$H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

du groupe multiplicatif $\mathbf{H}^\times$. Il est d'ordre 8, admet exatement trois sous-groupes cycliques $< i >, < j >, < k >$ d'ordre 4 (contrairement au groupe diédral D_4, qui n'en admet qu'un) et un seul élément d'ordre 2 (alors que D_4 en a 5). L'injection de C_4 dans H_8 définie par l'élément i munit H_8 d'une structure d'extension de C_2 par C_4. Cette extension n'est pas scindée, puisque le seul élément de H_8 d'ordre 2 est -1. L'injection de ± 1 dans H_8 munit également H_8 d'une structure d'extension (centrale, et non scindée) de $\mathbf{V}$ par C_2.

2.2.9 1-*cocycles.* Soit C un groupe agissant par τ sur un autre groupe A. Un 1-cocycle pour l'action τ est une application $C \overset{\alpha}{\longrightarrow} A$ telle que

$$\forall c_1, c_2 \in C,\ \alpha(c_1 c_2) = \alpha(c_1)^{c_1} \alpha(c_2).$$

2.2.10 Proposition.– *Soient τ et τ' deux actions de C sur A. Alors les produits semi-directs associés sont isomorphes en tant qu'extensions de C par A si et seulement si*

il existe un 1*-cocycle* α *pour l'action de* τ *tel que*

$$\forall c \in C,\ \tau'(c) = \tau(c) \circ \mathrm{Int}(\alpha(c)).$$

2.2.11 *Reconnaitre un produit semi-direct.* Inversement, soient G un groupe, et H, K deux sous-groupes de G tels que l'application $\phi : H \times K \to G : (h,k) \mapsto hk$ soit une bijection ensembliste. Cela entraîne en particulier que $H \cap K = \{1\}$, et pour G fini, cela équivaut à la conjonction de cette condition et de la relation $|G| = |H|.|K|$. Si H et K commutent, c'est-à-dire si $kh = hk$ pour tout $(h,k) \in H \times K$, l'application ϕ est un isomorphisme de groupes (pour la loi de produit sur $H \times K$), et G est le produit direct de H et K.

Les sous-groupes H et K commutent si et seulement si K est contenu dans le centralisateur $Z_G(H)$ de H. Supposons maintenant seulement que K soit contenu dans le normalisateur $N_G(H)$ de H (comme $HK = G$, cela équivaut à demander que H soit normal dans G). Alors, K agit sur H par conjugaison : $(k,h) \mapsto \tau(k)(h) := khk^{-1}$, et G est isomorphe au produit semi-direct $H \times_\tau K$ de K par H relativement à $\tau = (\mathrm{Int}_{|K})_{|H}$.

2.2.12 *Exemples.* Soit k un corps commutatif. Le sous-groupe triangulaire supérieur B_n de $\mathrm{GL}_n(k)$ est produit semi-direct du sous-groupe $T_n \simeq (k^\times)^n$ formé des matrices diagonales par le sous-groupe triangulaire supérieur strict U_n (l'action de T_n sur U_n est donnée par la conjugaison dans $\mathrm{GL}_n(k)$).

Le groupe des affinités $\mathrm{Aff}^1(k)$ de la droite affine sur k est produit semi-direct du sous-groupe multiplicatif $\simeq k^\times$ formé des homothéties centrées en 0, par le sous-groupe additif $\simeq k$ formé des translations (l'action de $k^\times$ sur k par conjugaison dans $\mathrm{Aff}^1(k)$ est simplement donnée par la multiplication).

2.3 Groupes libres et présentations

2.3.1 *Groupes libres.* Soit X un ensemble non vide. Si $k \in \mathbb{N}$, un *mot de longueur* k *sur l'alphabet* X est une application $\{1, \cdots, k\} \longrightarrow X$. Si $k = 0$, il y a une unique telle application (car la source est alors l'ensemble vide) que l'on appelle le *mot vide* et que l'on note e. Si $k > 0$, un mot est une séquence $m = (x_1 x_2 \cdots x_k)$ d'éléments de X. On note $M(X)$ l'ensemble des mots sur l'alphabet X. On le munit d'une loi de composition comme suit. Pour tout m on pose $em = me = m$ (donc e est élément neutre). Pour m, m' de longueurs k, k', on pose mm' le mot de longueur $k+k'$ obtenu par concaténation. En d'autres termes, $(x_1 x_2 \cdots x_k)(x'_1 x'_2 \cdots x'_{k'}) := (x_1 x_2 \cdots x_k x'_1 x'_2 \cdots x'_{k'})$. Cette loi est visiblement associative, et fait donc de $M(X)$ un *monoïde associatif*. Notons que X s'identifie naturellement au sous-ensemble des mots de longueur 1 de $M(X)$. On vérifie facilement que ce monoïde a la propriété universelle suivante : *toute application de* X *dans un monoïde associatif se prolonge* de manière unique *en un homomorphisme de monoïdes* $M(X) \longrightarrow M$. On dit que $M(X)$ est un monoïde *libre* sur l'ensemble X.

Remarquons qu'aucun élément non neutre de $M(X)$ ne possède d'inverse ; $M(X)$ est donc loin d'être un groupe. Mais on aimerait maintenant fabriquer un groupe $F(X)$ ayant

une propriété universelle analogue à la précédente. Pour cela, introduisons formellement un ensemble X^{-1} muni d'une bijection de X dans X^{-1}, que nous noterons $x \mapsto x^{-1}$. On s'intéresse alors au monoïde $M(X \sqcup X^{-1})$ des mots sur l'alphabet $X \sqcup X^{-1}$ (réunion disjointe). On définit une relation d'ordre sur $M(X \sqcup X^{-1})$ en déclarant $m \leqslant m'$ si l'on peut obtenir m à partir de m' en effaçant successivement des sous-mots de la forme xx^{-1} ou $x^{-1}x$ pour $x \in X$. Un mot est dit *réduit* s'il est minimal pour cette relation d'ordre, *i.e.* s'il ne contient pas de sous-mot du type xx^{-1} ou $x^{-1}x$ pour un $x \in X$. On montre par récurrence sur la longueur que tout mot majore un *unique* mot réduit. On en déduit une application de "réduction" de $M(X \sqcup X^{-1})$ vers le sous-ensemble $F(X)$ des mots réduits. On munit alors $F(X)$ de la loi de composition définie par concaténation des mots puis réduction $(m, m') \mapsto \mathrm{red}(mm')$. Les propriétés de l'ordre et de l'application de réduction font que cette loi est encore associative, et que le mot vide en est élément neutre. De plus, tout élément admet un inverse. L'inverse de $x \in X$ (resp. x^{-1}) est x^{-1} (resp. x), l'inverse d'un mot quelconque $y_1 ... y_n$ (avec $y_i \in X \cup X^{-1}$ pour tout i) est $y_n^{-1} ... y_1^{-1}$. Ainsi $F(X)$ est un groupe, visiblement engendré par son sous-ensemble X.

PROPOSITION. – *Pour tout groupe G, l'application*

$$\mathrm{Hom}_{\mathrm{gpes}}(F(X), G) \longrightarrow G^X = \mathrm{Hom}_{\mathrm{ens}}(X, G)$$

qui à $\varphi : F(X) \longrightarrow G$ associe $\varphi_{|X}$ est une bijection.

En d'autres termes, toute application de X dans un groupe G se prolonge de manière unique en un homomorphisme de $F(X)$ dans G. Le groupe $F(X)$ est appelé *groupe libre sur X*.

Démonstration. Comme $F(X)$ est engendré par X, un homomorphisme φ comme ci-dessus est déterminé par sa restriction à X. Donc l'application de l'énoncé est injective. Pour la surjectivité, partons de $\alpha : X \longrightarrow G$ et prolongeons-là à $X \cup X^{-1}$ en posant $\alpha(x^{-1}) := \alpha(x)^{-1}$. L'application obtenue se prolonge encore en une application $M(X \sqcup X^{-1}) \longrightarrow G$ qui envoie un mot $y_1 \cdots y_n$ sur le produit $\alpha(y_1) \cdots \alpha(y_n)$. Cette application est compatible à la concaténation. De plus, l'image d'un mot coincide avec celle du mot réduit associé. Elle induit donc le morphisme de groupes $F(X) \longrightarrow G$ cherché. □

2.3.2 *Exemples.* Si $X = \emptyset$, on obtient le groupe trivial. Si X a n éléments, on note aussi $F(n)$ et on l'appelle le groupe libre à n éléments ou "de rang n". Le groupe $F(1)$ est isomorphe à $\mathbb{Z}$. Le groupe $F(2)$ est déjà "énorme". C'est un théorème non trivial que tout sous-groupe d'un groupe libre est libre. De plus, pour $n > 1$, $F(n)$ contient des groupes libres de rang arbitrairement grand !

2.3.3 *Présentations.* Soit S un ensemble, et $R \subset F(S)$ un ensemble de mots réduits sur S. On note $\langle S|R\rangle$ le groupe quotient du groupe $F(S)$ par le sous-groupe *distingué* engendré par R (*i.e.* le plus petit sous-groupe distingué de $F(S)$ contenant R). On dit que $\langle S|R\rangle$ est un groupe *présenté*.

DÉFINITION. – *Soit G un groupe. Une* présentation[1] *de G est la donnée d'un couple (S, R) comme ci-dessus et d'une application $S \longrightarrow G$, telle que l'homomorphisme canonique $F(S) \longrightarrow G$ qui s'en déduit (cf prop. précédente) induise un isomorphisme $\langle S|R\rangle \xrightarrow{\sim} G$.*

Tout groupe admet une présentation. Concrètement, soit S une partie génératrice de G, *i.e.* telle que $\langle S\rangle = G$. L'homomorphisme $\pi : F(S) \to G$ (induisant l'identité sur S) qui s'en déduit par propriété universelle de $F(S)$ est alors surjectif, et π induit un isomorphisme $F(S)/\operatorname{Ker}(\pi) \xrightarrow{\sim} G$. Il suffit alors de prendre pour R toute partie de $\operatorname{Ker}(\pi)$ telle que le plus petit sous-groupe *distingué* de $F(X)$ contenant R soit $\operatorname{Ker}(\pi)$.

On notera qu'une telle présentation n'est aucunement unique. En fait cette notion, relativement simple à définir, est très subtile. Par exemple, les questions (vagues) suivantes sont toujours l'objet de recherches actuelles.

– Étant donné G trouver une présentation "aussi simple que possible" de G.

– Étant donné (S, R), calculer le groupe $\langle S|R\rangle$ (estimer son ordre, son exposant, etc.).

Pour illustrer la seconde, le lecteur pourra vérifier que le groupe présenté sur deux générateurs $\langle\{a, b\}|\{a^4, b^3, a^{-2}bab^{-1}\}\rangle$ est cyclique d'ordre 3 et que le groupe présenté sur trois générateurs $\langle\{a, b, c\}|\{a^{-1}bab^{-2}, b^{-1}cbc^{-2}, c^{-1}aca^{-2}\}\rangle$ est... trivial.

2.3.4 *Exemples.* $(\{a\} \mid \{a^n\})$ est une présentation de C_n ; $(\{a, b\} \mid \{a^n, b^2, abab\})$ est une présentation de D_n ; $(\{a, b\} \mid \{a^4, a^2b^2, ab^{-1}ab\})$ est une présentation de H_8. Notons qu'à chaque fois il est facile de trouver un morphisme surjectif du groupe présenté annoncé sur le groupe dont on prétend donner une présentation. Montrer que le noyau est nul est plus difficile. Néanmoins, pour les petits groupes comme ci-dessus, un simple argument de comptage fait l'affaire.

2.3.5 *Exemple : groupe symétrique.* Dans S_n notons s_i la permutation $(i, i+1)$ pour $i = 1, \cdots, n-1$. On sait que les s_i engendrent S_n. On a les relations suivantes :

– $s_i^2 = e$ (relations quadratiques)

– $(s_is_j)^2 = e$ pour $|i-j| > 1$ et $(s_is_{i+1})^3 = e$ (relations de tresse).

Posant $S = \{s_i, i = 1, \cdots n-1\}$ et $R_0 = \{s_i^2, i = 1, \cdots n-1\}$ et $R_1 = \{(s_is_{i+1})^3, (s_is_j)^2\}$ comme ci-dessus, on montre que la paire $(S|R_0 \cup R_1)$ est une présentation du groupe S_n. On pourrait aussi présenter S_n à partir du n-cycle et d'une permutation. Mais ce n'est pas la présentation la plus intéressante. En effet, en modifiant un peu les relations ci-dessus, on obtient deux familles de groupes très intéressantes et très étudiées : les groupes de tresses et les groupes de Coxeter.

2.3.6 *Groupes de tresses.* Avec les notations ci-dessus, on définit B_n comme le groupe présenté $\langle S|R_1\rangle$. C'est un groupe infini, appelé "groupe de tresses" qui a une grande importance en physique théorique. Ses éléments peuvent être représentés par des "tresses", c'est-à-dire des manières de relier bijectivement, à l'aide de n ficelles, deux ensembles de n-points-alignés mis en regard (des points physiques et des vraies ficelles, *cf* article wikipe-

[1] On dit aussi "présentation par générateurs et relations"

dia "braid groups"). Il y a aussi une interprétation topologique rigoureuse, comme "groupe fondamental" de l'espace de configurations de n points distincts dans le plan complexe.

2.3.7 *Groupes de Coxeter.* Un groupe de Coxeter est un groupe présenté $\langle S, R\rangle$ pour lequel l'ensemble de relations R est de la forme $R = \{(st)^{m_{st}}, s, t \in S\}$, où les $(m_{st})_{s,t\in S}$ sont des entiers (éventuellement infinis) tels que pour tout s on ait $m_{ss} = 1$, et pour tous $s \neq t$, on ait $m_{st} = m_{ts} \geqslant 2$. On a donc en particulier $s^2 = e$ pour tout s ; le groupe W est donc engendré par des éléments d'ordre 2. La condition $m_{st} = \infty$ signifie simplement qu'on n'impose pas de relation entre s et t. La condition $m_{st} = 2$ équivaut à demander que s et t commutent.

Ces présentations ont la particularité d'être "irredondantes" : on montre en effet que l'application $S \longrightarrow \langle S, R\rangle$ est injective et que les éléments st sont d'ordre m_{st} dans $\langle S, R\rangle$ (ce qui n'est pas évident *a priori*, cf exemples plus haut).

Les groupes symétriques en sont des cas particuliers (prendre $S = \{1, \cdots, n-1\}$, $m_{i,i+1} = m_{i+1,i} = 3$ et $m_{ij} = 2$ pour $|j - i| > 1$). Les groupes diédraux aussi : D_m est obtenu pour $S = \{s, t\}$ et $m_{st} = m_{ts} = m$. En général un groupe de Coxeter n'est pas nécessairement fini, même lorsque S et les m_{st} sont tous finis.

Coxeter lui-même a déterminé lesquels de ses groupes sont finis. Pour cela, il associe à la donnée $(S|R)$ un graphe dont l'ensemble des sommets est S et dont deux sommets s, t sont reliés par $m_{st} - 2$ arêtes. Il a alors fait la liste de tous les graphes finis tels que le groupe associé soit fini. Dès que $|S| \geqslant 3$, il n'y a qu'un nombre fini de tels graphes ayant pour ensemble de sommets S.

On a vu que les groupes diédraux sont les groupes de symétrie des polygones réguliers du plan euclidien. Plus généralement, les groupes de Coxeter finis avec $|S| = n$ sont les groupes de symétrie de certains "polytopes" (semi)-réguliers d'un espace euclidien de dimension n. Par exemple, pour $|S| = 3$, ces polytopes sont les "solides de Platon" (tétraèdre, cube, octahèdre, dodécaèdre, icosaèdre). Le groupe d'isométrie du premier est isomorphe à S_4, celui des deux suivants est isomorphe au produit semi-direct $\{\pm 1\}^4 \rtimes S_4$, et celui des deux derniers est A_5.

2.3.8 *Groupes de réflexions.* Soit K un corps. Un automorphisme $P \in \mathrm{GL}_n(K)$ est appelé *réflexion* s'il est diagonalisable, d'ordre fini, et si 1 est valeur propre avec multiplicité $n-1$ (l'unique autre valeur propre est alors une racine de l'unité). L'hyperplan $\mathrm{Ker}(P - I_n)$ est l'axe de la réflexion, et la droite $\mathrm{Im}(P - I_n)$ en est la direction. On dit qu'un sous-groupe $G \subset \mathrm{GL}_n(K)$ est un *groupe de réflexions* s'il est engendré par des réflexions.

Lorsque $K = \mathbb{R}$, une réflexion est une symétrie hyperplane, et donc d'ordre 2. On montre alors que tout sous-groupe de réflexions dans $\mathrm{GL}_n(\mathbb{R})$ admet une présentation de Coxeter. Inversement, tout groupe de Coxeter $\langle S, R\rangle$ peut être vu comme sous-groupe de réflexions de $\mathrm{GL}_{|S|}(\mathbb{R})$. Si on se restreint aux groupes finis, on peut même remplacer dans ces deux assertions $\mathrm{GL}_n(\mathbb{R})$ par $\mathrm{O}_n(\mathbb{R})$ (groupe orthogonal, voir plus bas). En d'autres termes, on peut imposer que les réflexions soient "orthogonales" (*i.e.* l'axe est orthogonal à la direction) pour un produit scalaire euclidien.

2.4 Quelques groupes classiques.

Outre les exemples déjà rencontrés au chapitre I, comme les groupes cycliques $C_n = \mathbb{Z}/n\mathbb{Z}$, les groupes symétriques et alternés S_n, A_n, et quelques sous-quotients du groupe de matrices $\mathrm{GL}_n(k)$, on peut citer :

2.4.1 *Le groupe modulaire.* c'est le sous-groupe d'ordre infini $\mathrm{PSL}_2(\mathbf{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm\mathbf{1}_2\}$ de $\mathrm{PSL}_2(\mathbf{R})$. Le groupe $\mathrm{SL}_2(\mathbb{Z})$ est engendré par les matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (d'ordre 4) et $U = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ (d'ordre 6). Le groupe $\mathrm{PSL}_2(\mathbf{Z})$ admet pour présentation $(\{a, b\} \mid \{a^2, b^3\})$.

2.4.2 *Groupes n-transitifs.* soient E un ensemble, n un entier $\leqslant card(E)$, et G un sous-groupe du groupe symétrique S_E. On dit que G est n-transitif (ou mieux : agit n fois transitivement sur E) si pour tout couple de parties $\{x_1, ..., x_n\}, \{y_1, ..., y_n\}$ de E à n éléments, il existe un élément g de G tel que $g.x_i = y_i$ pour tout $i = 1, ..., n$. Par définition, G est $1-$transitif si l'action de G sur E est transitive. Le groupe S_n est n-transitif, donc A_n est $(n-2)$-transitif (si $n \geqslant 3$). Pour tout corps k, le groupe $\mathrm{PGL}_2(k)$ (resp. $\mathrm{PSL}_2(k)$) agit 3 fois (resp. 2 fois) transitivement sur $\mathbf{P}_1(k)$. Et $\mathrm{PGL}_2(k)$ n'est pas 4-transitif (si $k \neq \mathbb{F}_3$), puisque le *birapport* $(x_1 : x_2 : x_3 : x_4) := \frac{x_3-x_1}{x_3-x_2} : \frac{x_4-x_1}{x_4-x_2}$ d'un quadruplet est invariant sous son action, et que $(\infty : 0 : 1 : x) = x$. Hors de A_n, S_n eux-mêmes, on connait peu de groupes 4 ou 5 -transitifs (groupes de Mathieu), et on conjecture qu'aucun n'est 6-transitif.

Passons à quelques nouveaux groupes de type matriciel.

2.4.3 *Groupes symplectiques et orthogonaux.* soient k un corps commutatif, n un entier > 0, et $J = \begin{pmatrix} 0_n & \mathbf{1}_n \\ -\mathbf{1}_n & 0_n \end{pmatrix}$ la matrice carrée d'ordre $2n$ représentant la forme bilinéaire alternée sur l'espace vectoriel k^{2n} : $(\underline{x}, \underline{y}) \mapsto \Sigma_{i=1,..,n} x_i y_{n+i} - x_{n+i} y_i$. Le groupe symplectique est le groupe $Sp_{2n}(k) = \{P \in \mathrm{GL}_{2n}(k), {}^t PJP = J\}$. Ainsi, $Sp_2(k) = \mathrm{SL}_2(k)$. Plus généralement, on démontre que le déterminant d'une matrice symplectique vaut toujours 1, de sorte que pour tout n, $Sp_{2n}(k)$ est un sous-groupe de $\mathrm{SL}_{2n}(k)$.

Le groupe orthogonal est le groupe $O_n(k) = \{P \in \mathrm{GL}_n(k), {}^t P.P = \mathbf{1}_n\}$. Ses éléments représentent les "transformations orthogonales" de l'espace k^n, muni de la forme bilinéaire symétrique $(\underline{x}, \underline{y}) \mapsto \Sigma_{i=1,..,n} x_i y_i)$. Son intersection avec $\mathrm{SL}_n(k)$ est notée $SO_n(k)$.

Remarque : les groupes $PSp_{2n}(\mathbb{F}_q)$ sont simples et les groupes $SO_{2n+1}(\mathbb{F}_q)$ sont "presque" simples.

2.4.4 *Groupes unitaires.* soit k un corps commutatif muni d'une involution non triviale $x \mapsto \overline{x}$ (exemple : $k = \mathbf{C}, {}^- =$ la conjugaison complexe ; ou encore : $k = \mathbb{F}_{p^2}, {}^- =$ le Frobenius $x \mapsto x^p$). Pour tout entier $n > 0$, le groupe unitaire $U_n(k)$ est le sous-groupe de $\mathrm{GL}_n(k)$ formé des matrices P telles que ${}^t\overline{P}.P = \mathbf{1}_n$. Son intersection avec $\mathrm{SL}_n(k)$ est notée $SU_n(k)$.

Remarque les groupes $PSU_n(\mathbb{F}_q)$ sont simples.

3 Structure des groupes finis

3.1 Les théorèmes de Sylow.

Dans tout ce paragraphe, p désigne un nombre premier, et G un groupe fini. On dit que G est un p-groupe si son ordre est une puissance p^n de p (avec $n \geqslant 0$).

3.1.1 DÉFINITION.– *On dit qu'un sous-groupe S de G est* un p-sous-groupe de Sylow *de G (ou plus simplement : un p-Sylow de G) si S est un p-groupe d'indice $[G : S]$ premier à p.*

Autrement dit, si on écrit $|G| = p^n m$ avec m premier à p, un p-Sylow de G est un sous-groupe d'ordre p^n. Il est alors clair que tout sous-groupe conjugué à S est encore un p-Sylow de G. Ce qui est moins clair, c'est de savoir s'il existe un p-Sylow !

3.1.2 *Exemple.* Soit k un corps fini, de cardinal $q = p^f$. Le groupe $G = \mathrm{GL}_n(k)$ est d'ordre $p^{fn(n-1)/2}m$, où $m = \Pi_{i=1,..,n}(q^i - 1)$, qui est premier à p. Le sous-groupe S de G formé par les matrices triangulaires supérieures strictes (i.e. n'ayant que des 1 sur la diagonale) est un p-Sylow de G.

3.1.3 THÉORÈME.– *Soient G un groupe fini, et p un nombre premier. Alors,*

i) G possède des p-Sylow ;

ii) deux p-Sylow de G sont conjugués l'un de l'autre ;

iii) tout p-sous-groupe de G est contenu dans un p-Sylow de G.

La démonstration de l'existence (point i)) consiste à se ramener à un cas explicite grâce au lemme suivant :

3.1.4 LEMME.– *Soient G un groupe fini, H un sous-groupe de G et S un p-Sylow de G. Alors il existe $g \in G$ tel que $H \cap gSg^{-1}$ soit un p-Sylow de H.*

Démonstration. soit $X = G/S$ l'ensemble des classes à gauche de G modulo S, sur lequel le groupe H agit par translation à gauche. Le fixateur de tout point gS de X sous l'action de H est l'intersection de H avec le conjugué gSg^{-1} de S ; c'est donc un p-groupe. Comme p ne divise pas $card(X) = [G : S]$, l'une au moins des orbites, soit $H.gS$, de X sous H a un cardinal $[H : (H \cap gSg^{-1})]$ premier à p. Donc $H \cap gSg^{-1}$ est un p-sous-groupe de H d'ordre premier à son indice dans H, i.e. un p-Sylow de H. □

Démonstration du théorème. i) D'après le Lemme 1, il suffit de plonger G (c'est-à-dire de construire un homomorphisme injectif de G) dans un groupe $\mathbf{G}$ admettant un p-Sylow. Or si $n = |G|$, G se plonge dans le groupe symétrique S_n, et ce dernier se plonge dans $\mathbf{G} = \mathrm{GL}_n(\mathbb{F}_p)$ par l'homomorphisme ρ qui attache à $\sigma \in S_n$ l'automorphisme $\rho(\sigma)$ du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_p^n$ défini par $\rho(\sigma)(x_1, ..., x_n) = (x_{\sigma^{-1}(1)}, ..., x_{\sigma^{-1}(n)})$. D'après l'exemple au-dessus du théorème, $\mathbf{G}$ admet un p-Sylow, donc G aussi.

ii) (resp. iii) Appliquer le lemme au cas où H est un p-Sylow (resp. un p-sous-groupe) de G. □

3.1.5 COROLLAIRE.– *G est toujours un groupe fini.*

i) Pour tout nombre premier p divisant $|G|$, G admet des éléments d'ordre p.

ii) G est un p-groupe si et seulement si tous ses éléments sont d'ordre une puissance de p.

3.1.6 PROPOSITION.– *Si $|G| = p^n m$ avec $(p, m) = 1$, le nombre $s = card(\mathcal{S})$ de p-sous-groupes de Sylow de G divise m, et vérifie $s \equiv 1$ mod p.*

Démonstration. D'après le Théorème, G agit par conjugaison sur $\mathcal{S}$, et ce de façon transitive. Or le fixateur dans G d'un élément S de $\mathcal{S}$ est $N_G(S)$, qui contient S. Par conséquent, $s = [G : N_G(S)]$, qui divise $[G : S] = m$. Faisons maintenant agir S sur $\mathcal{S}$ par conjugaison, et montrons que la seule orbite à un élément est celle de S lui-même : si $sS's^{-1} = S'$ pour tout $s \in S$, alors SS' est un sous-groupe de G, dont tous les éléments sont d'ordre une puissance de p ; d'après le corollaire 1.ii, c'est donc un p-groupe, d'où par maximalité des p-Sylow : $SS' = S = S'$. Les autres orbites ont un cardinal distinct de 1 et diviseur de $|S|$, donc divisible par p. Ainsi, $s \equiv 1 \bmod p$. □

3.2 Groupes résolubles et groupes nilpotents

3.2.1 *Commutateurs.* Dans un groupe G, on appelle commutateur de deux éléments x, y l'élément $[x, y] := x^{-1}y^{-1}xy$ de G. Pour deux sous-groupes A, B de G, l'ensemble des commutateurs $[a, b]$ pour $a \in A$ et $b \in B$ *n'est généralement pas un sous-groupe de G*, même lorsqu'on prend $A = B = G$.

3.2.2 DÉFINITION.– *On note $[A, B]$ le sous-groupe de G engendré par les commutateurs $[a, b], a \in A, b \in B$.*

Quelques propriétés faciles :
- B distingué dans $G \Rightarrow [A, B] \subset B$.
- A et B distingués dans $G \Rightarrow [A, B]$ distingué dans G
- A et B caractéristiques dans $G \Rightarrow [A, B]$ caractéristique dans G.

3.2.3 *Sous-groupe dérivé.* Le sous-groupe $DG := [G, G]$ est appelé *sous-groupe dérivé* de G. C'est un sous-groupe caractéristique. Par sa définition même, DG est le plus petit sous-groupe distingué N de G tel que G/N soit abélien, et on peut interpréter G/DG (souvent noté G^{ab}) comme "le plus grand quotient" abélien de G : tout homomorphisme de G vers un groupe abélien se factorise de manière unique à travers G/DG.

3.2.4 *Suite dérivée.* Posons $D^0G = G$ et pour tout entier $i \geqslant 0, D^{i+1}G = [D^iG, D^iG]$. Les D^iG forment une suite décroissante de sous-groupes caractéristiques de G, dont les

quotients successifs $D^iG/D^{i+1}G$ sont abéliens, et qu'on appelle la *suite dérivée* de G. Elle vérifie clairement la propriété de minimalité suivante : *soit* $\{G_i, i = 0, 1, ...\}$ *une suite décroissante de sous-groupes tels que* $G_0 = G, G_{i+1} \triangleleft G_i$ *et que* G_i/G_{i+1} *soit abélien pour tout* i. *Alors,* D^iG *est contenu dans* G_i *pour tout* i.

3.2.5 *Groupes résolubles.* On dit que G est *résoluble* s'il existe un entier n tel que $D^nG = \{1\}$. Ceci équivaut à l'existence d'une suite décroissante $G_0 = G \supset G_1 \supset \cdots \supset G_n = \{1\}$ de sous-groupes tels que $G_{i+1} \triangleleft G_i$ et que G_i/G_{i+1} soit abélien pour tout i.

Pour un groupe résoluble, le plus petit des entiers n tels que $D^nG = \{1\}$ s'appelle la *classe de résolubilité de* G. C'est aussi le plus petit des entiers n tels qu'il existe une suite $G_0 = G \supset G_1 \supset \cdots \supset G_n = \{1\}$ décroissante de sous-groupes tels que $G_{i+1} \triangleleft G_i$ et que G_i/G_{i+1} soit abélien pour tout i.

Par exemple, un groupe abélien est résoluble de classe 1. Le groupe diédral D_n (stabilisateur dans $O_2(\mathbf{R})$ d'un polygone régulier à n côtés) est résoluble de classe 2. Plus généralement, il résulte des propositions 1.1.11 et 1.1.12 que

3.2.6 Proposition.– *i) tout sous-groupe (resp. tout quotient) d'un groupe résoluble est résoluble ;*

ii) soit H *un sous-groupe distingué d'un groupe* G *; si* H *et* G/H *sont résolubles (de classes de résolubilité* n_1, n_2*), G est résoluble (de classe de résolubilité* $\leqslant n_1 + n_2$*).*

Un peu d'histoire : pour $n \geqslant 5$, le groupe alterné A_n est simple et non abélien, de sorte que le groupe S_n n'est pas résoluble ; en revanche, S_2, S_3, S_4 sont résolubles. On montre en théorie de Galois qu'une équation algébrique est résoluble par radicaux si et seulement si son groupe de Galois est résoluble ; on en déduit que pour $n \geqslant 5$, l'équation générale de degré n n'est pas résoluble par radicaux, tandis qu'elle l'est pour $n = 2$ (formule du trinôme), $n = 3$ (formules de Cardan), $n = 4$ (formules de Ferrari).

3.2.7 *Suite centrale descendante.* Posons $C^0G = G$ et pour tout entier $i \geqslant 0, C^{i+1}G = [G, C^iG]$. Les C^iG forment une suite décroissante de sous-groupes caractéristiques de G, qu'on appelle la *suite centrale descendante* de G. Pour tout $i > 0$, on a $C^i(G) \supset D^i(G)$, et $C^{i+1}(G)$ est le plus petit sous-groupe distingué N de G contenu dans $C^i(G)$ et tel que $C^i(G)/N$ soit contenu dans le centre $Z(G/N)$ de G/N.

3.2.8 *Groupes nilpotents.* On dit que G est *nilpotent* s'il existe un entier n tel que $C^n(G) = \{1\}$. Le plus petit de ces entiers n s'appelle la classe de nilpotence de G. Un groupe G est nilpotent si et seulement s'il admet une suite de sous-groupes $G_0 = G \supset G_1 \supset ... \supset G_m = \{1\}$ telle que $[G, G_i] \subset G_{i+1}$ pour tout i (puisqu'alors, $C^i(G) \subset G_i$ pour tout i). Cette condition équivaut à demander que $G_i/G_{i+1} \subset Z(G/G_{i+1})$ pour tout i.

On en déduit que tout sous-groupe et tout quotient d'un groupe nilpotent est nilpotent. Inversement, si$H$ est un sous-groupe de G *contenu dans le centre* $Z(G)$ de G et si G/H est nilpotent, alors G est nilpotent.

Le centre d'un groupe nilpotent est toujours non trivial. D'ailleurs, pour savoir si un

groupe fini est nilpotent, on peut calculer son centre, puis le centre du quotient de G par son centre, etc. Si à un moment on tombe sur un groupe de centre trivial, alors G n'est pas nilpotent.

3.2.9 *Exemples.* Un groupe abélien est nilpotent. Un groupe nilpotent est résoluble. Mais S_3 est résoluble sans être nilpotent (son centre est trivial). De même, pour tout corps commutatif k, le sous-groupe B de $G = \mathrm{GL}_n(k)$ formé par les matrices triangulaires supérieures (à coefficients diagonaux quelconques) est résoluble, mais (si $k \neq \mathbb{F}_2$) pas nilpotent. Le sous-groupe S de B formé par les matrices triangulaires supérieures strictes est, lui, nilpotent.

3.2.10 PROPOSITION.– *i) tout p-groupe G est nilpotent.*

ii) Soit G un groupe nilpotent. Tout sous-groupe propre H de G est strictement inclus dans son normalisateur $N_G(H)$; en particulier, tout sous-groupe de G d'indice premier est distingué dans G.

iii) Soient G un groupe fini, et S un p-Sylow de G. Pour tout sous-groupe H de G contenant $N_G(S)$, on a $H = N_G(H)$.

Démonstration. i) d'après la formule des classes pour l'action de G par conjugaison sur lui-même, le centre Z de G est non trivial (si $|G| > 1$). On conclut par une récurrence sur $|G|$. On peut aussi montrer cet énoncé en plongeant, pour n assez grand, G dans $\mathrm{GL}_n(\mathbb{F}_p)$, puis en notant que les p-Sylow de G sont conjugués au groupe triangulaire strict S, qui est nilpotent.

ii) Récurrence sur la classe de nilpotence n de G. L'énoncé est clair si $n = 1$. Si $n > 1$, le sous-groupe $A = C^{n-1}(G)$ de G est contenu dans le centre de G, et G/A est nilpotent de classe $n - 1$. Alors, $N_G(H)$ contient A, et on a gagné si H ne contient pas A. Sinon, l'hypothèse de récurrence entraîne que H/A est strictement inclus dans $N_{G/A}(H/A)$, donc $H \neq N_G(H)$.

iii) Soit n un élément de $N_G(H)$. Alors, S et $nSn^{-1} \subset nHn^{-1} = H$ sont des p-Sylow de H, donc sont conjugués dans H : il existe $h \in H$ tel que $hSh^{-1} = nSn^{-1}$. Donc $h^{-1}n \in N_G(S) \subset H$, et $n \in H$. □

3.2.11 THÉORÈME.– *Soit G un groupe fini. Les conditions suivantes sont équivalentes :*

i) G est nilpotent ;

ii) pour tout sous-groupe propre H de G, $H \neq N_G(H)$;

iii) pour tout nombre premier p, G admet un unique p-Sylow ;

iv) G est isomorphe au produit direct de ses sous-groupes de Sylow.

v) deux éléments de G d'ordres premiers entre eux commutent ;

Démonstration. On a déjà vu *i)* ⇒ *ii)*. Montrons *ii)* ⇒ *iii)*. Soit S un p-Sylow de G. D'après l'hypothèse ii) et le iii) de la proposition précédente, $N_G(S) = G$, i.e. S est distingué dans G. Comme on sait que les p-Sylows sont tous conjugués (théorème 3.1.3 ii)),

on en déduit que S est l'unique p-Sylow de G. Passons à *iii)* $\Rightarrow$ *iv)*. L'unique p-Sylow S_p est nécessairement distingué. Il s'ensuit que pour tout autre premier $\ell \neq p$, on aura $[S_p, S_\ell] \subset S_p \cap S_\ell = \{1\}$, d'où un morphisme injectif du produit des S_p vers G, qui pour des raisons d'ordre est aussi bijectif. L'implication *iv)* $\Rightarrow$ *v)* est claire, et sa réciproque aussi. L'implication *iv)* $\Rightarrow$ *i)* découle du point i) de la proposition précédente et du fait que $C^i(G_1 \times G_2) = C^i(G_1) \times C^i(G_2)$. □

Si G est abélien, son unique p-Sylow s'appelle la composante p-primaire $G^{(p)}$ de G. On peut énoncer :

3.2.12 Corollaire.– *Tout groupe abélien fini G est isomorphe au produit direct $\Pi_p\, G^{(p)}$ de ses composantes p-primaires, où p parcourt l'ensemble des diviseurs premiers de $|G|$.*

Il est d'ailleurs facile de déduire cet énoncé de la décomposition de G donnée par ses facteurs invariants (voir chap. II, S2).

4 Représentations linéaires

4.1 Définitions et exemples

Soient G un groupe, et K un corps commutatif.

4.1.1 Définition.– *Une représentation linéaire de G à coefficients dans K est une paire (ρ, V) formée d'un K-espace vectoriel V et d'un morphisme de groupes $\rho : G \longrightarrow \mathrm{GL}_K(V)$.*

On dit aussi que ρ est une représentation d'espace sous-jacent V. On remarquera que se donner ρ équivaut à se donner une action à gauche de G sur V compatible avec la structure de K-espace vectoriel sur V.

On commet souvent l'abus raisonnable de désigner une représentation (ρ, V) simplement par ρ, et parfois celui moins défendable de la désigner par V... On note alors simplement $g.v$ pour ce qu'on devrait noter $\rho(g)(v)$, *i.e.* l'image d'un vecteur v de V sous l'action (via ρ) d'un élément g de G. On a donc $g(\lambda v + v') = \lambda gv + gv', (gg')v = g(g'v), 1_G v = v$ pour tout $g, g' \in G, v, v' \in V, \lambda \in K$.

4.1.2 *Exemples.*

i) *Représentation triviale.* Pour tout K-ev V, la représentation triviale $\mathbf{1}_V$ sur V est définie par $\mathbf{1}_V(g) = id_V$ pour tout $g \in G$. Pour $V = K$, la représentation triviale $\mathbf{1}_K$ s'appelle la *représentation unité* de G (relativement au corps K).

ii) *Représentations standard.* Quand G est déjà défini comme un sous-groupe de $\mathrm{GL}(V)$ (par exemple le groupe diédral D_n dans $\mathrm{GL}(2, \mathbb{C})$), V est une représentation de G, dite souvent représentation naturelle, ou représentation standard.

iii) *Représentations de permutation.* Soit X un ensemble muni d'une action à gauche de G. La représentation de permutation associée est le K-espace vectoriel $V = KX$ de base $\{e_x, x \in X\}$, muni de l'action définie par K-linéarité à partir des conditions $g.e_x = e_{g.x}$. Ainsi un élément e dans KX s'écrit de manière unique $\sum_x \lambda_x e_x$ pour une famille "presque nulle" $(\lambda_x)_{x \in X}$ d'éléments de K (ce qui signifie que tous les λ_x sont nuls sauf un nombre fini d'entre eux), et on a

$$g.e = g.(\sum_x \lambda_x e_x) = \sum_x \lambda_x e_{gx}.$$

Exemple : Prenant $G = \mathfrak{S}_n$ et $X = \{1, \cdots, n\}$, on obtient une représentation de $\mathfrak{S}_n$ sur K^n. Le morphisme $\mathfrak{S}_n \longrightarrow \mathrm{GL}_n(K)$ envoie une permutation sur la matrice-permutation associée.

Plus généralement, dans la base $(e_x)_{x \in X}$ on voit que la matrice donnant l'action de g est une matrice-permutation (une seule entrée non nulle et égale à 1 par ligne et par colonne). D'où le nom de représentation de permutation.

iv) *Espaces de fonctions.* Partant de X comme ci-dessus, l'espace $\mathcal{F}(X,K) := K^X$ des fonctions $X \xrightarrow{f} K$ est muni de l'action définie par

$$\forall x \in X,\ (g.f)(x) := f(g^{-1}x).$$

On notera que le passage à l'inverse est nécessaire pour avoir l'égalité $g.(h.f) = (gh).f$ (ie une action à gauche). Sans cela on aurait une action à droite).

Remarquons que l'espace KX ci-dessus peut se voir comme le sous-espace vectoriel $\mathcal{F}_0(X,K)$ de K^X formé des fonctions dont le support est fini (i.e. nulles hors d'une partie finie de X). En effet un isomorphisme est donné par

$$\begin{array}{ccc} KX & \to & \mathcal{F}_0(X,K) \\ e_x & \mapsto & \delta_x \end{array}$$

où δ_x désigne la fonction de Dirac centrée en x définie par $\delta_x(y) = 0$ si $x \neq y, \delta_x(x) = 1$. Or, la formule plus haut montre que $g.\delta_x = \delta_{gx}$. Ainsi l'isomorphisme ci-dessus est compatible avec les représentations de G sur KX et $\mathcal{F}_0(X,K)$.

v) *Représentation régulière.* Pour $X = G$, muni de l'action par translation à gauche de G, la représentation de permutation $V = KG \simeq \mathcal{F}_0(G,K)$ s'appelle la *représentation régulière (à gauche)* R de G. Elle est donc définie par

$$R(g)\left(\sum_{h\in G} \lambda_h e_h\right) = \sum_{h\in G} \lambda_h e_{gh} = \sum_{h\in G} \lambda_{g^{-1}h} e_h,$$

où pour tout $h \in G$, λ_h est un élément de K, avec $\lambda_h = 0$ pour tout h en dehors d'une partie finie de G.

4.1.3 *Petit lexique.*

Degré d'une représentation. C'est la dimension sur K de l'espace vectoriel sous-jacent.

Vecteur fixe. C'est un point fixe de l'action de G sur V, *i.e.* un élément v de V tel que $gv = v$. Le vecteur nul $0 \in V$ est toujours fixe par G. On note souvent V^G l'ensemble des vecteurs fixes sous G. C'est un sous-K-espace vectoriel de V.

Exemples

i) Dans une représentation de permutation KX, le vecteur $\sum_{x\in X} e_x$ est fixe sous G.

ii) *Si G est un p-groupe fini et K est de caractéristique p, alors toute représentation admet des vecteurs fixes* non nuls. En effet, partons de $v \in V$ non nul et regardons le $\mathbb{F}_p$-espace vectoriel W engendré par les vecteurs gv, $g \in G$. C'est une $\mathbb{F}_p$-représentation de G de dimension finie. Son nombre d'éléments est p^n pour un certain n. Il y a au moins un vecteur fixe, le vecteur nul, et la formule des classes pour l'action de G sur W nous dit que le nombre de vecteurs fixes est divisibles par p.

Représentation fidèle. C'est une représentation (ρ, V) telle que l'homomorphisme ρ est injectif.

Sous-représentation. C'est un K-ss-ev W de V qui est stable (on dit aussi : invariant) sous l'action de G. Ceci signifie que pour tout $v \in W$ et tout $g \in G$, on a $gv \in W$. Pour bien faire, on devait la noter $(\rho, W) \subset (\rho, V)$.

Représentation quotient. Si W est un sous-espace stable de V, l'espace vectoriel quotient V/W est naturellement muni d'une structure de représentation de G, appelée *représentation quotient* de V par W. Pour toute classe $v + W$, on pose simplement $g(v + W) := gv + W$, qui ne dépend pas du choix de v puisque W est supposé stable.

4.1.4 Définition.– *Un morphisme $(\rho, V) \longrightarrow (\pi, W)$ entre deux représentations de G est un homomorphisme K-linéaire $\phi : V \to W$ tel que $\phi(g.v) = g.\phi(v)$ pour tout $(g, v) \in G \times V$.*

On parle aussi de G-morphisme, ou encore d'application linéaire G-équivariante. Comme d'habitude on a les variantes *monomorphisme* = G-morphisme injectif, *épimorphisme* = G-morphisme surjectif, *isomorphisme* = G-morphisme bijectif (on dit alors que les représentations V et W sont *isomorphes*, ou encore *équivalentes*), *endomorphisme* si $V = W$ et *automorphisme*=endomorphisme bijectif.

Par ailleurs, l'image d'un G-morphisme $\varphi : V \longrightarrow W$ est une sous-représentation de W, et le noyau est une sous-représentation de V. Comme pour les espaces vectoriels, φ induit alors un G-isomorphisme $V/\operatorname{Ker}(\varphi) \xrightarrow{\sim} \operatorname{Im}(\varphi)$.

4.1.5 *Exemples.*

i) la sous-représentation $W = K.v$ de V engendrée par un vecteur fixe v de V est isomorphe à la représentation unité $\mathbf{1}_K$ de G.

ii) Pour un G-ensemble X, l'application linéaire $KX \longrightarrow K^X$ définie plus haut est un G-monomorphisme, et induit un G-isomorphisme $KX \xrightarrow{\sim} \mathcal{F}_0(X, K)$.

iii) Pour deux G-ensembles X et Y, toute application G-équivariante $X \longrightarrow Y$ se prolonge par linéarité en un G-morphisme $KX \longrightarrow KY$, et induit un G-morphisme $K^Y \longrightarrow K^X$.

4.1.6 Définition.– *On dit qu'une représentation (ρ, V) est* irréductible *si elle n'admet pas de sous-représentation propre (i.e. distincte de $\{0\}$ et de V).*

4.1.7 *Exemples.*

i) *Si G est abélien fini, une représentation irréductible de G sur $\mathbb{C}$ est de dimension* 1. En effet pour tout élement g d'ordre $o(g)$, le polynôme minimal de l'endomorphisme $\rho(g)$ de V divise $X^{o(g)} - 1$. Donc la famille des $\rho(g)$ est une famille d'endomorphismes diagonalisables commutant deux à deux, et on sait qu'une telle famille est "simultanément diagonalisable", *i.e.* qu'il existe une base formée de vecteurs propres pour tous les $\rho(g)$. Chaque vecteur propre engendre une droite vectorielle stable sous G.

ii) La représentation standard du groupe dihédral D_n sur $\mathbb{C}^2$ est irréductible.

iii) La représentation de permutation de $\mathfrak{S}_n$ sur K^n n'est pas irréductible puisque la droite engendrée par $e_1 + \cdots + e_n$ est stable sous $\mathfrak{S}_n$. Plus généralement, une représentation de permutation de dimension finie $\neq 1$ n'est jamais irréductible.

iv) *Si G est un p-groupe et K est de caractéristique p, alors la seule représentation irréductible est (à isomorphisme près) la représentation triviale $\mathbf{1}_K$.* Cela découle en effet du fait, vu plus haut, que toute représentation admet des vecteurs fixes non nuls.

v) Marions les exemples i) et iv). Soit $G = \mathbb{Z}/p\mathbb{Z}$, et supposons que K soit algébriquement clos. Alors les représentations irréductibles de G sont toutes de dimension 1 et de la forme $\rho_\zeta : n \in G \mapsto \zeta^n \in \mathrm{GL}_1(K) = K^\times$ pour ζ une racine p-ème de l'unité. Mais il y a une grosse différence selon la caractéristique de K. Si celle-ci est $\neq p$, il y a donc p représentations irréductibles non-isomorphes 2 à 2 (p racines p-ème de l'unité). Si la caractéristique vaut p, il y en a une seule (la triviale), puisque la seule racine p-ème de l'unité est 1.

4.1.8 Proposition. (Lemme de Schur)– *Soient V et W deux représentations irréductibles d'un groupe G , et $\varphi : V \longrightarrow W$ un G-morphisme non identiquement nul. Alors,*

i) φ est un isomorphisme

ii) si de plus $V = W$ est de dimension finie, et si K est algébriquement, il existe un scalaire non nul λ tel que $\varphi = \lambda.id_V$.

Démonstration. Le noyau (resp. l'image) de φ est un sous-espace invariant de V (resp. W). L'irréductibilité de ces représentations entraîne la première assertion. Sous les hypothèses de la seconde, φ admet au moins une valeur propre $\lambda \in K$, et il suffit d'appliquer la première assertion au G-morphisme $\varphi - \lambda id_V$. □

Remarque. Pour une représentation V, l'ensemble des G-endomorphismes de V est une K-algèbre. Si V est de dimension finie, cette K-algèbre l'est aussi. Si V est irréductible, cette K-algèbre est un corps (éventuellement non commutatif, encore appelé "algèbre à division"). Toute algèbre à division de dimension finie sur un corps algébriquement clos est isomorphe à ce corps.

Somme directe. Si V et W sont deux représentations de G, leur somme directe est la représentation $V \oplus W$ définie par $g.(v \oplus w) = gv \oplus gw$.

4.1.9 Définition.– *On dit qu'une représentation (ρ, V) est* indécomposable *si elle n'est pas somme directe de deux sous-représentations propres. Sinon elle est dite décomposable.*

Noter qu'une représentation indécomposable n'est pas forcément irréductible. Voici un contre-exemple typique.

4.1.10 Proposition.– *La représentation régulière KG d'un p-groupe fini G à coefficients dans un corps K de caractéristique p est indécomposable mais pas irréductible.*

Démonstration. On a déjà vu qu'elle n'est pas irréductible puisqu'elle a des vecteurs fixes non nuls, par exemple le vecteur $v_0 := \sum_g e_g$. En fait on voit facilement que *tout vecteur fixe de KG* est multiple de v_0. En effet, soit $v = \sum_g \lambda_g e_g$ un tel vecteur. Pour tout h, on $hv = v$ si et seulement si pour tout g on a $\lambda_g = \lambda_{hg}$. En particulier pour tout h on a $\lambda_h = \lambda_e$ et $v = \lambda_e v_0$. Il s'ensuit que toute sous-représentation de W contient un multiple non nul de v_0 et donc v_0. Ainsi deux sous-représentations non nulles auront toujours une intersection non nulle et ne pourront a fortiori pas être en somme directe. □

Ce phénomène est vraiment dû au fait que la caractéristique de K divise l'ordre du groupe, comme le montre le lemme suivant. Rappelons à cette occasion qu'on a équivalence entre "la caractéristique de K ne divise pas l'ordre de G" et "l'ordre de G est inversible dans K".

4.1.11 Proposition. (Lemme de Maschke)– *Soit G un groupe fini et K un corps de caractéristique ne divisant pas $|G|$. Soit V une représentation et W une sous-représentation non nulle. Alors il existe une sous-représentation W' de V telle que $V = W \oplus W'$.*

Démonstration. Soit $\tilde{W}$ un supplémentaire (au sens des espaces vectoriels) de W dans V, et $\tilde{p}$ la projection linéaire de V sur W le long de W'. C'est un élément de $\mathrm{Hom}(V, W)$, mais, en général, pas un G-morphisme. Posons alors :

$$p = |G|^{-1} \left(\sum_{g \in G} \rho(g) \circ \tilde{p} \circ \rho(g)^{-1} \right).$$

On vérifie que p est toujours un projecteur de V sur W, et cette fois, qu'il est invariant sous G. Donc son noyau $W' = \mathrm{Ker}(p)$ est un supplémentaire de W dans V, stable sous G. □

4.1.12 Corollaire.– *Soit G un groupe fini d'ordre inversible dans K.*

i) toute représentation indécomposable est irréductible.

ii) toute représentation ρ se décompose en une somme directe $\rho = \rho_1 \oplus \cdots \oplus \rho_k$ de représentations irréductibles.

En regroupant dans le ii) les représentations irréductibles isomorphes entre elles, on obtient une décomposition

$$\rho = \rho_1^{a_1} \oplus \cdots \oplus \rho_l^{a_l},$$

où a_i est un entier non nul, $\rho_i^{a_i}$ désigne la somme directe $\rho_i \oplus \rho_i \oplus \cdots \oplus \rho_i$ de a_i copies de ρ_i, et les ρ_i sont deux-à-deux non isomorphes. Une telle décomposition est appelée *décomposition isotypique*. Le lemme suivant dit que les facteurs directs ρ_i et les entiers a_i d'une décomposition isotypique ne dépendent que de ρ (et pas du procédé inductif utilisé pour obtenir la décomposition).

4.1.13 Lemme.– *Si $\rho = {\rho'}_1^{a'_1} \oplus \cdots \oplus {\rho'}_{l'}^{a'_{l'}}$ est une autre décomposition comme ci-dessus, alors $l = l'$ et il existe une permutation $\sigma \in \mathfrak{S}_l$ telle que $\rho_i \simeq \rho'_{\sigma(i)}$ pour tout $i = 1, \cdots, l$.*

4.1.14 DÉFINITION.– *Les représentations irréductibles apparaissant dans une décomposition comme ci-dessus sont appelés* facteurs de Jordan-Hölder *ou* sous-quotients irréductibles. *L'entier a_i associé est appelé* multiplicité.

On voit donc que la théorie des représentations d'un groupe fini G à coefficients dans un corps algébriquement clos de caractéristique étrangère à $|G|$ revient essentiellement à classifier les représentations irréductibles. Si la caractéristique divise $|G|$, la théorie est beaucoup plus compliquée car il faut aussi comprendre les extensions "non-scindées" entre irréductibles, et plus généralement les représentations indécomposables. Il s'avère (hors programme !) que pour un groupe aussi simple que $(\mathbb{Z}/p\mathbb{Z})^2$ il n'y a aucun espoir d'arriver à une classification raisonnable des représentations indécomposables...

4.1.15 *Exemple.* Regardons la représentation régulière du groupe $G = \mathbb{Z}/2\mathbb{Z}$. Elle a une base (e_0, e_1) sur laquelle le générateur γ de G agit par $\gamma.e_0 = e_1$ et $\gamma.e_1 = e_0$. Si K n'est pas de caractéristique 2, on voit que les vecteurs $e_+ = e_0 + e_1$ et $e_- = e_0 - e_1$ sont propres pour γ (de valeurs propres 1 et -1) donc engendrent des droites L_+ et L_- stables sous G. On vérifie alors immédiatement que $KG = L_- \oplus L_+$. Si par contre K est de caractéristique 2, alors $e_+ = e_-$, et $L_+ = L_-$ est la seule droite stable sous G dans KG.

4.1.16 *Contragrédiente (ou représentation duale).* Soient (V, ρ) une représentation de G, et $V^* = Hom(V, K)$ le dual du K-espace vectoriel V. On munit V^* d'une structure de représentation de G en posant, pour toute forme linéaire f sur V et tout g dans G : $\rho^*(g)(f) = f \circ \rho(g^{-1})$ (en abrégé : $g.f = f \circ g^{-1}$), de sorte que pour tout $(g, f, v) \in G \times V^* \times V$, on a : $\langle g.f | g.v \rangle := \langle \rho^*(g)(f) | \rho(g)(v) \rangle = \langle f | v \rangle$; autrement dit, $\rho^*(g) \in End_K(V^*)$ est la transposée de $\rho(g^{-1}) \in End_K(V)$. On dit que ρ^* est la représentation duale , ou *contragrédiente*, de ρ.

4.1.17 Hom *internes.* Plus généralement, soient (ρ, V) et (π, W) deux représentations de G. L'espace $\mathrm{Hom}_K(V, W)$ des homomorphismes K-linéaires de V dans W est naturellement muni d'une structure de représentation de G : pour tout g dans G et tout K-homom. $\varphi : V \longrightarrow W$, on pose

$$g.\varphi := \pi(g) \circ \varphi \circ \rho(g^{-1}).$$

Une application linéaire φ fixe sous cette action n'est autre qu'un G-morphisme. L'ensemble $\mathrm{Hom}_K(V, W)^G$ des G-morphismes est donc un K-sev, traditionnellement noté $\mathrm{Hom}_{KG}(V, W)$. Si $V = W$, $\mathrm{End}_{KG}(V)$ est une sous-K-algèbre de $\mathrm{End}_K(V)$, parfois appelée "algèbre commutante de G" dans V.

Voici deux cas particuliers : la représentation V^* s'identifie à $\mathrm{Hom}_K(V, \mathbf{1}_K)$ tandis que la représentation W s'identifie à $\mathrm{Hom}_K(\mathbf{1}_K, W)$.

4.1.18 *Produits tensoriels.* Nous rappelons (ou expliquons) une construction qui fait le lien entre l'algèbre *bilinéaire* et l'algèbre *linéaire*. Fixons deux K-espaces vectoriels V, W. On a une notion d'application K-bilinéaire $V \times W \xrightarrow{\theta} E$ pour E un K-ev. Il s'agit d'une application telle que pour tout $v \in V$, l'application $w \in W \mapsto \theta(v, w) \in E$ soit K-linéaire,

et de même pour tout $w \in W$, l'application $v \in V \mapsto \theta(v,w) \in E$ soit K-linéaire. Il est important de garder à l'esprit que θ n'est pas linéaire : par exemple $\theta(2x,2y) = 4\theta(x,y)$. Cependant, on peut ramener la théorie des applications bilinéaires à celle des applications linéaires en utilisant la notion de *produit tensoriel.*

Pour cela, remarquons d'abord que si $E \xrightarrow{\varphi} E'$ est une application K-linéaire, alors $\varphi \circ \theta : V \times W \longrightarrow E'$ est encore K-bilinéaire.

4.1.19 PROPOSITION.– *Il existe un espace vectoriel, unique à isomorphisme près, noté $V \otimes_K W$ et appelé* produit tensoriel *de V et W sur K, muni d'une application K-bilinéaire $\otimes : V \times W \longrightarrow V \otimes_K W, (v,w) \mapsto x \otimes w$ et qui satisfait la propriété universelle suivante : pour toute application K-bilinéaire $\theta : V \times W \longrightarrow E$, il existe une unique application K-linéaire $\varphi_\theta : V \otimes_K W \longrightarrow E$ telle que $\theta(v,w) = \varphi_\theta(v \otimes w)$ pour tous $(v,w) \in V \times W$.*

Ainsi une application bilinéaire $\theta : V \times W \longrightarrow E$ comme ci-dessus détermine et est déterminée par *une unique application K-linéaire $\varphi_\theta : V \otimes_K W \longrightarrow E$.*

La structure de K-ev de $V \otimes_K W$ peut être source d'erreurs. C'est pourquoi il est bon de remarquer explicitement les propriétés suivantes, imposées par l'hypothèse de bilinéarité de $(v,w) \mapsto v \otimes w$:

– $(v+v')\otimes w = v\otimes w + v'\otimes w$ et $v\otimes(w+w') = v\otimes w + v\otimes w'$ pour tous $v, v' \in V, w, w' \in W$.
– $(\lambda v) \otimes w = v \otimes (\lambda w) = \lambda(v \otimes w)$ pour tout $\lambda \in K$.

En tout état de cause on gardera à l'esprit que $(v+v') \otimes (w+w') \neq v \otimes w + v' \otimes w'$.

Démonstration. Une fois l'existence prouvée, on en déduit l'unicité comme pour toute "solution d'un problème universel". Pour l'existence, on peut procéder comme suit : soit $\{e_i; i \in I\}, \{\epsilon_j; j \in J\}$ des bases respectives de V, W. Considérons l'espace vectoriel $\mathcal{E}$ ayant pour base les symboles $e_i \otimes \varepsilon_j$, pour $i \in I, j \in J$. On définit une application K-bilinéaire

$$\begin{array}{rccc} \theta_{\mathcal{E}} & V \times W & \to & \mathcal{E} \\ & (v,w) & \mapsto & \sum_{i,j}(v_i w_j) e_i \otimes \varepsilon_j \end{array}$$

où $v = \sum_i v_i e_i$ et $w = \sum_j w_j \varepsilon_j$ sont les décompositions de v, resp. w, dans la base $(e_i)_i$, resp $(\varepsilon_j)_j$. Pour toute application K-bilinéaire θ comme dans l'énoncé, on définit $\varphi_\theta : \mathcal{E} \longrightarrow E$ en posant $\varphi_\theta(e_i \otimes \varepsilon_j) = \theta(e_i, \varepsilon_j)$. Il est clair que $\theta = \varphi_\theta \circ \theta_{\mathcal{E}}$. Il est aussi clair que φ_θ est l'unique application K-linéaire $\mathcal{E} \longrightarrow E$ vérifiant cette propriété, puisqu'une forme bilinéaire de source $V \times W$ est uniquement déterminée par ses valeurs sur les couples (e_i, ε_j) pour $i \in I$, $j \in J$ □

De la preuve on déduit comment fabriquer des bases de $V \otimes_K W$, et en particulier que si V et W sont de dimension finie, alors $V \otimes_K W$ aussi, et on a $\dim(V \otimes W) = \dim(V)\dim(W)$.

Supposons maintenant que V, W soient les espaces de représentations ρ, σ du groupe G. Alors, $V \otimes_K W$ est l'espace d'une représentation de G, notée $\rho \otimes \sigma$ et définie par la condition $(\rho\otimes\sigma)(g)(v\otimes w) := \rho(g)(v)\otimes\sigma(g)(w) = gv\otimes gw$ pour tout $(g,v,w) \in G\times V\times W$. On l'appelle *produit tensoriel* des représentations ρ et σ.

4.1.20 *Exemple.* Si ρ et σ sont irréductible, cela n'est souvent plus vrai pour $\rho \otimes \sigma$. Par exemple pour $G = D_n$ et ρ la représentation standard sur $\mathbb{C}^2$, on montre que $\rho \otimes \rho$ contient encore ρ.

4.1.21 *Produits tensoriels et* Hom *internes..* Soit V^* le dual de V. Par la proposition précédente, l'application bilinéaire $W \times V^* \to \mathrm{Hom}_K(V, W) : (w, f) \mapsto \{\varphi : v \mapsto \varphi(v) := f(v)w\}$ définit un homomorphisme canonique

$$\iota : W \otimes_K V^* \longrightarrow \mathrm{Hom}_K(V, W).$$

4.1.22 Lemme.– *L'homomorphisme ι est injectif. De plus,*

i) il est bijectif si V et W sont de dimension finie.

ii) il est G-équivariant, si V et W sont des représentations, et si $W \otimes_K V^*$ et $\mathrm{Hom}_K(V, W)$ sont munis des représentations "produit tensoriel" et "Hom internes".

Remarque : de manière générale, l'image de ι est formée des homomorphismes $\varphi : V \to W$ de rang fini, i.e. tels que $\varphi(V)$ soit un sous-espace de dimension finie de W.

Si (ρ, V) et (π, W) sont des représentations de dimension finie, la représentation sur $\mathrm{Hom}_K(V, W)$ est donc isomorphe à $\pi \otimes \rho^*$.

Voici un cas particulier utile : $V = W$ avec $\dim_K(V)$ finie. Alors ι est un isomorphisme $V \otimes V^* \xrightarrow{\sim} End_K(V)$. L'image inverse de Id_V est donnée par le tenseur $\sum_{i \in I} e_i \otimes e_i^*$, où $\{e_i\}$ désigne une base quelconque de V, et $\{e_i^*\}$ sa base duale dans V^*.

4.1.23 Lemme.– *Soit φ un endomorphisme de V correspondant au tenseur $\sum_\ell v_\ell \otimes f_\ell \in V \otimes V^*$. Alors sa trace est donnée par la formule*

$$\mathrm{Tr}(\varphi) = \sum_\ell f_\ell(v_\ell) \in K.$$

4.2 Caractères des représentations complexes

On suppose dorénavant le groupe G *fini* et on ne considère plus que des représentations de dimension *finie*.

4.2.1 Définition.– *Soit (V, ρ) une représentation de degré fini de G sur un corps K. On appelle caractère de ρ la fonction*

$$\begin{array}{rccc} \chi_\rho = \chi_V : & G & \to & K \\ & g & \mapsto & \chi_V(g) = \mathrm{Tr}(\rho(g)) \end{array}$$

qui associe à tout élément g de G la trace de l'automorphisme $\rho(g)$ de V.

La formule classique $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ en algèbre matricielle montre que le caractère χ_V vérifie les égalités

$$\forall g \in G, \forall h \in G,\ \chi_V(ghg^{-1}) = \chi_V(h).$$

Les fonctions $G \longrightarrow K$ vérifiant ces égalités sont appelées *fonctions centrales*, ou encore *fonctions invariantes par conjugaison.*

Pour la même raison, deux représentations isomorphes ont des caractères égaux. Évidemment, de même qu'un endomorphisme est loin d'être déterminé par sa trace, on peut s'attendre à ce que le caractère d'une représentation en soit une invariant assez grossier. Cependant, nous allons voir que sur le corps $K = \mathbb{C}$, deux représentations ayant même caractère sont isomorphes ! En attendant, on remarque que le caractère connait la dimension de la représentation, puisque $\chi_V(e) = \dim_K(V)$.

4.2.2 *Remarque.* Dans la littérature, on trouve souvent le nom de "caractères de G" pour désigner les homomorphismes de G dans le groupe multiplicatif $K^\times$. Un caractère en ce sens est le caractère en le sens ci-dessus d'une représentation de degré 1. Mais le caractère χ_V d'une représentation V de degré > 1 n'est jamais multiplicatif (puisque en e il prend la valeur $\dim(V)$). Il y a donc là un conflit de terminologie.

4.2.3 Théorème.– *Soient V et W deux représentations de degré fini de G. Alors :*

i) le caractère de la repr. contragrédiente V^* est donné par $\chi_{V^*}(g) = \chi_V(g^{-1})$.

ii) le caractère de la représentation $V \oplus W$ est donné par : $\chi_{V\oplus W}(g) = \chi_V(g) + \chi_W(g)$.

iii) le caractère de la représentation $V \otimes W$ est donné par : $\chi_{V\otimes W}(g) = \chi_V(g)\chi_W(g)$.

iv) le caractère de la repr. $H = Hom(V, W)$ est donné par : $\chi_H(g) = \chi_W(g)\chi_V(g^{-1})$.

Démonstration. Soit $B_V = \{e_i, i \in I\}$ une base du K-ev V, et $B_{V^*} = \{e_i^*, i \in I\}$ sa base duale dans V^*. Par définition de la trace, on a

$$\chi_V(g) = \sum_{i\in I} \langle ge_i, e_i^* \rangle.$$

On en déduit donc

$$\chi_V(g) = \sum_{i\in I} \langle ge_i, e_i^* \rangle = \sum_{i\in I} \langle e_i, g^{-1}e_i^* \rangle = \chi_{V^*}(g^{-1}),$$

l'égalité du milieu provenant de la définition de la représentation contragrédiente. D'où i).

Fixons aussi une base $B_W = \{\varepsilon_j, j \in J\}$ de W. La réunion $B_V \cup B_W$ est une base de $V \oplus W$ et la réunion des bases duales $B_{V^*} \cup B_{W^*}$ est sa base duale dans $(V \oplus W)^* = V^* \oplus W^*$. Ainsi, par définition de la représentation somme directe, on a

$$\chi_{V\oplus W}(g) = \sum_{i\in I} \langle ge_i, e_i^* \rangle + \sum_{j\in J} \langle g\varepsilon_j, \varepsilon_j^* \rangle = \chi_V(g) + \chi_W(g).$$

On a vu que l'ensemble $B_{V\otimes W} := \{e_i \otimes \varepsilon_j, i \in I, j \in J\}$ est une base de $V \otimes W$. On a un isomorphisme évident de K-ev $V^* \otimes W^* \xrightarrow{\sim} (V \otimes W)^*$ qui envoie le tenseur $v^* \otimes w^*$ sur la forme linéaire sur $V \otimes_K W$ associée à la forme bilinéaire $(v, w) \mapsto \langle v, v^*\rangle\langle w, w^*\rangle$. Cela permet d'identifier l'ensemble $\{e_i^* \otimes \varepsilon_j^*, i \in I, j \in J\}$ à la base duale de $B_{V\otimes W}$. Ainsi on a

$$\begin{aligned}\chi_{V\otimes W}(g) &= \sum_{i,j}\langle ge_i \otimes g\varepsilon_j, e_i^* \otimes \varepsilon_j^*\rangle = \sum_{i,j}\langle ge_i, e_i^*\rangle\langle g\varepsilon_j, \varepsilon_j^*\rangle \\ &= \left(\sum_i \langle ge_i, e_i^*\rangle\right)\left(\sum_j \langle g\varepsilon_j, \varepsilon_j^*\rangle\right) = \chi_V(g)\chi_W(g).\end{aligned}$$

Enfin, on a vu que $\mathrm{Hom}(V, W) \simeq V^\times \otimes W$ donc iv) se déduit de i) et iii). □

4.2.4 *Exemple.* Soit X un G-ensemble et KX la représentation de permutation associée. Son caractère est donné par

$$\chi_{KX}(g) = \text{ nombre de points fixes de } g \text{ dans } X.$$

4.2.5 *Exemple.* Soit $G = D_n$ et $V = \mathbb{C}^2$ la représentation standard. Alors $\chi_V(g) = 0$ si g n'appartient pas au sous-groupe cyclique distingué C_n de D_n engendré par la rotation r_n d'angle $\frac{2\pi}{n}$, et $\chi_V(r_n^k) = 2\cos(2k\pi/n)$ pour $k = 0, \cdots, n-1$.

4.2.6 *Le cas complexe.* Nous supposerons dorénavant que $K = \mathbb{C}$. Nous noterons z^* le conjugué d'un nombre complexe z.

La première particularité de $\mathbb{C}$ est d'être algébriquement clos. Ainsi la trace de l'automorphisme $\rho(g)$ est la *somme de ses valeurs propres*. Comme on a $\rho(g)^{|G|} = \mathrm{Id}_V$, les valeurs propres de $\rho(g)$ sont des racines de l'unité, et on a donc $\chi_V(g^{-1}) = \chi_V(g)^*$.

La deuxième particularité de $\mathbb{C}$ vient de la positivité de zz^* pour tout z. Cela permet de munir l'espace $\mathbb{C}G = \mathbb{C}[G] = \mathcal{F}(G, \mathbb{C})$ des fonctions complexes sur G de sa norme L^2, i.e. du produit scalaire hermitien :

$$(f, f') = |G|^{-1}\sum_{g\in G} f(g)f'(g)^*.$$

On considérera aussi son sous-espace

$$\mathcal{F}^{cent}(G, \mathbb{C}) = \{f \in \mathcal{F}(G, \mathbb{C}), \forall g, h \in G, f(hgh^{-1}) = f(g)\}$$

des fonctions centrales, qu'on munit de la norme induite. (Comme G est ici fini, on a supprimé l'indice 0 de la notation $\mathcal{F}_0$.) Les *relations d'orthogonalité* suivantes sont la clef de la théorie des caractères.

4.2.7 Théorème.– *Soient V et W deux représentations irréductibles de G . Alors,*

i) si W n'est pas isomorphe à V : $(\chi_V, \chi_W) = 0$,

ii) si W est isomorphe à V : $(\chi_V, \chi_V) = 1$.

Démonstration. Considérons d'abord une représentation quelconque (ρ, V) et regardons le sous-espace V^G des vecteurs fixes de V sous G. L'endomorphisme $p = |G|^{-1} \sum_{g\in G} \rho(g)$ de V est un projecteur de V sur V^G. Sa trace vaut donc :

$$\mathrm{Tr}(p) = \dim(V^G) = |G|^{-1} \sum_{g\in G} \mathrm{Tr}(\rho(g)) = |G|^{-1} \sum_{g\in G} \chi_V(g) = (\chi_V, \mathbf{1})$$

en notant $\mathbf{1}$ la fonction constante de valeur 1 sur G.

Reprenons les notations de l'énoncé et appliquons ce résultat à la représentation $H = \mathrm{Hom}(V, W)$. On a $(\chi_H, \mathbf{1}) = (\chi_W \chi_V^*, \mathbf{1}) = (\chi_W, \chi_V)$. D'après le lemme de Schur, le K-ev $\mathrm{Hom}(V, W)^G$ est de dimension 0 (resp. 1) si V et W ne sont pas (resp. sont) isomorphes. Ainsi $(\chi_H, \mathbf{1}) = 0$ ou 1 suivant qu'on est dans le cas i) ou le cas ii), comme annoncé. □

4.2.8 Corollaire.– *Soit V une représentation de G, et $V_1^{\oplus a_1} \oplus ... \oplus V_k^{\oplus a_k}$ sa décomposition isotypique.*

i) Pour tout $i = 1, ..., k$, la multiplicité a_i de V_i dans V est donnée par $a_i = (\chi_V, \chi_{V_i})$. En particulier, deux représentations sont isomorphes si et seulement si elles ont le même caractère.

ii) On a $(\chi_V, \chi_V) = \sum_{i=1}^k a_i^2$. En particulier, V est irréductible si et seulement si $(\chi_V, \chi_V) = 1$.

iii) Toute représentation irréductible W de G apparaît dans la représentation régulière de G avec une multiplicité égale à son degré $\dim(W)$. En particulier, $|G| = \sum_W \dim(W)^2$, où W parcourt l'ensemble des classes d'isomorphisme de représentations irréductibles de G.

Démonstration. i) + ii) découle des relations d'orthogonalité et du fait que $\chi_{V_i^{\oplus a_i}} = a_i \chi_{V_i}$. iii) Le caractère r de la représentation régulière R vérifie $r(1) = |G|$, et $r(g) = 0$ pour tout $g \neq 1$. Pour toute repr. W de G, on a donc

$$(r, \chi_W) = |G|^{-1}(r(1)\chi_W(1)^* + 0) = \dim(W).$$

Si W est irréductible, et si R est isomorphe à $W_1^{\oplus a_1} \oplus ... \oplus W_k^{\oplus a_k}$, on déduit alors des relations d'orthogonalité que W est isomorphe à l'un des W_i , avec $a_i = \dim(W)$. □

Cette dernière conclusion montre que G n'a qu'un nombre fini de classes d'isomorphisme de représentations irréductibles. En fait, il y en a exactement $cl(G)$ (qui est la dimension de $\mathcal{F}^{cent}(G, \mathbb{C})$). En effet :

4.2.9 Théorème.– *les caractères des différentes classes d'isomorphismes de représentations irréductibles de G forment une base de l'espace des fonctions centrales sur G. Il y en a donc autant que de classes de conjugaison du groupe G.*

Démonstration. il s'agit de voir que la seule fonction centrale f telle que $(f, \chi_V) = 0$ pour toute repr. irréd. V, est la fonction nulle. Pour une telle V, posons $\varphi_V = \sum_{g\in G} f(g)\rho_V(g)$. Comme f est centrale, on voit que φ est un G-morphisme de V dans V, donc par Schur, une homothétie, et puisque sa trace $|G|(f, \chi_V^*)$ est nulle , $\varphi_V = 0$. Donc l'endomorphisme $\sum_{g\in G} f(g)R(g)$ de l'espace $\mathcal{F}(G, \mathbb{C})$ de la représentation régulière est identiquement nul. Ses vecteurs $R(g)(e_1) = e_g$ étant $\mathbf{C}$-linéairement indépendantes, $f(g)$ est bien nul pour tout g dans G . □

4.2.10 *Remarque.* Le fait que les caractères des irréductibles forment une base de l'espace des fonctions centrales est encore vrai sur un corps de coefficients K, pourvu que $|G|$ soit inversible dans K et que K contienne une racine primitive $|G|$-ème de l'unité. Sinon, il y a des contre-exemples. Le plus spectaculaire est quand K est de caractéristique p et G est un p-groupe. Dans ce cas le caractère de toute représentation est constant !

Le fait qu'une représentation est déterminée par son caractère (à isomorphisme près) est encore vrai sur un corps de caractéristique nulle. Mais il est toujours faux si K est de caractéristique positive ℓ. Par exemple la représentation triviale de dimension ℓ a un caractère nul ! Aussi les caractères ne voient pas la différence entre $\rho \oplus \sigma$ et une extension non scindée de ρ par σ.

4.2.11 *Table des caractères.* Par ce qui précède, on peut associer à un groupe fini G un tableau de nombres complexes dont les lignes sont indexées par les classes de représentations irréductibles ρ de G, et les colonnes sont indexées par les classes de conjugaison c dans G. À la ligne ρ et la colonne c on associe $\chi_\rho(x)$ où x est un élément quelconque de c. Voici quelques exemples.

Le groupe cyclique $G = \mathbb{Z}/n\mathbb{Z}$. Ce groupe étant commutatif, ses classes de conjugaison sont des singletons, *i.e.* simplement $\{\overline{0}\}, \cdots, \{\overline{n-1}\}$. Par ailleurs on a déjà vu que les représentations irréductibles de G sont de dimension 1, et donnés par les homomorphisme $\rho_{\bar{i}} : \bar{j} \in G \mapsto \omega^{\overline{ji}}$ où ω est une racine n-ème primitive de l'unité fixée, et $\bar{i}$ décrit les entiers modulo n. La table est alors simplement donnée par les formules $\chi_{\rho_{\bar{i}}}(\bar{j}) = \omega^{\overline{ij}}$. Remarquons tout de même que la manière dont on a écrit cette table dépend du choix de ω. Changer ω induira une permutation des lignes de la table.

Le groupe S_3. Les classes de conjugaison sont $\{e\}$, $c_2 = \{(1,2),(2,3),(1,3)\}$, et $c_3 = \{(1,2,3),(2,1,3)\}$. Il nous faut trouver 3 représentations irréductibles. On connait déjà la triviale $\mathbf{1}$, et le caractère signature $\mathrm{Sgn} : \mathrm{S}_3 \longrightarrow \{\pm 1\}$. Pour trouver la troisième, on peut penser au fait que $S_3 = D_3$ est le groupe des isométries préservant un triangle équilatéral, d'où une représentation standard de dimension 2 $\mathrm{Std} : \mathrm{S}_3 = \mathrm{D}_3 \subset \mathrm{O}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{R}) \subset \mathrm{GL}_2(\mathbb{C})$. On peut maintenant dresser la table :

	$\{e\}$	c_2	c_3
$\mathbf{1}$	1	1	1
Sgn	1	-1	1
Std	2	0	-1

Le groupe D_4. Il est de la forme $\langle r\rangle \rtimes \langle s\rangle$ où r est la rotation d'angle $\pi/2$ (donc engendrant un sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z}$), et s la réflexion orthogonale d'axe (Ox), chacune préservant le carré de sommets $(\pm 1, \pm 1)$ dans $\mathbb{R}^2$. A partir de la relation $srs = r^2$, on trouve les classes de conjugaison $\{e\}$, $\{r^2\}$, $\{r, r^3s\}$, $\{s, r^2s\}$, et $\{rs, r^3s\}$. Pour trouver les représentations irréductibles, on remarque que $D_4/\langle r^2\rangle$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. D'où 4 caractères de dimension 1 : $\mathbf{1}$, χ, ψ, et $\chi\psi$, définis par $\chi(r) = -1$, $\chi(s) = 1$, et $\psi(r) = 1$, $\psi(s) = -1$. Il ne manque qu'une représentation à trouver, et c'est la standard, de dimension 2. On peut maintenant écrire la table :

	$\{e\}$	$\{r^2\}$	$\{r, r^3s\}$	$\{s, r^2s\}$	$\{rs, r^3s\}$
$\mathbf{1}$	1	1	1	1	1
χ	1	1	-1	1	-1
ψ	1	1	1	-1	-1
$\chi\psi$	1	1	-1	-1	1
Std	2	-2	0	0	0

Le groupe H_8. On vérifie facilement que les classes de conjugaison sont $\{1\}, \{-1\}, \{\pm i\}$, $\{\pm j\}$ et $\{\pm k\}$. Par ailleurs $H_8/\{\pm 1\}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ avec pour générateurs les images de i et de j (par exemple). On en déduit 4 caractères de dimension 1 : $\mathbf{1}$, χ, ψ, et $\chi\psi$, définis par $\chi(i) = -1$, $\chi(j) = 1$, et $\psi(i) = 1$, $\psi(j) = -1$. Reste à trouver la dernière représentation irréductible. Considérons $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j$ comme un $\mathbb{C}$-espace vectoriel de dimension 2, de base $1, j$, et faisons agir H_8 sur $\mathbb{H}$ par multiplication à gauche : $\rho(g)(x) := xg^{-1}$. On obtient ainsi une représentation $\mathbb{C}$-linéaire (noter que la multiplication à droite ne serait pas $\mathbb{C}$-linéaire mais seulement $\mathbb{R}$-linéaire). On peut alors dresser la table.

	$\{1\}$	$\{-1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
$\mathbf{1}$	1	1	1	1	1
χ	1	1	-1	1	-1
ψ	1	1	1	-1	-1
$\chi\psi$	1	1	-1	-1	1
$\mathbb{H}$	2	-2	0	0	0

Remarque 1 : si on ne trouve pas la dernière représentation irréductible, on peut toujours déduire la dernière ligne de la table de caractère à partir du corollaire 4.2.8 iii). Celui-ci dit en effet que le carré de la norme euclidienne de la première colonne est le cardinal de G, tandis que les autres colonnes sont orthogonales à la première. Inversement, cette relation permet de détecter d'éventuelles erreurs dans une table.

Remarque 2 : les deux exemples précédents montrent que deux groupes non-isomorphes G, G' peuvent avoir des tables de caractères "isomorphes" au sens où il existe une bijection des classes de conjugaison de G sur celles de G', resp. des classes d'irréductibles de G sur celles de G', telles que les tables obtenues soient les mêmes. Il existe néanmoins deux manières de distinguer deux groupes ayant la même table, à partir de la table, *à condition de se rappeler de quelques structures.*

Exemple 1 : L'application $g \mapsto g^2$ est compatible à la conjugaison, donc induit une application $c \mapsto c^2$ de l'ensemble des classes de conjugaison de G dans lui-même. Pour D_4, on constate que $\{s, r^2 s\}^2 = \{e\}$, tandis que pour H_8, on a $\{\pm j\}^2 = \{-1\}$. Ceci montre que la bijection entre les classes de conjugaison qui rend les tables de caractères identiques n'est pas compatible à l'opération "carré des classes de conjugaison", ce qui permet de distinguer les deux groupes.

Exemple 2 : Plutôt qu'une opération sur les classes de conjugaison (comme ci-dessus l'application "carré"), on peut utiliser une opération sur les représentations. Si (V, ρ) est une représentation de G, on note

$$\mathrm{Sym}^2 V := (V \otimes V)/\mathrm{Vect}\{(v_1 \otimes v_2 - v_2 \otimes v_1),\, v_1, v_2 \in V\}$$

Exercice : vérifier que c'est une représentation quotient de $\rho \otimes \rho$, notée $\mathrm{Sym}^2(\rho)$ et que son caractère est donné par $\chi_{\mathrm{Sym}^2(\rho)}(g) = \frac{1}{2}\left(\chi_\rho(g)^2 + \chi_\rho(g^2)\right)$. En déduire que $\mathrm{Sym}^2(\mathrm{Std}) = \mathbf{1} + \chi + \chi\psi$ tandis que $\mathrm{Sym}^2(\mathbb{H}) = \chi + \psi + \chi\psi$. Ceci montre que la bijection entre les caractères de D_4 et ceux de H_8 n'est pas compatible à l'opération "carré symétrique", ce qui permet de distinguer les deux groupes.

4.3 Représentations induites et caractères induits

Nous étudions maintenant un procédé pour construire une représentation d'un groupe G à partir d'une représentation d'un sous-groupe H de G.

4.3.1 *Point de vue des caractères.* Soit (V, ρ) une représentation de G. Par restriction de ρ à H, on obtient une représentation $(V, \rho_{|H})$ de H. Son caractère aussi est donné par restriction :

$$\chi_{\rho_{|H}} = (\chi_\rho)_{|H}.$$

Notons que si ρ est irréductible, $\rho_{|H}$ ne l'est généralement pas (penser au cas extême $H = \{e\}$).

Inversement, partons d'une représentation (W, τ) de H. Notons χ_τ^0 l'extension par 0 de son caractère. On a donc

$$\chi_\tau^0(g) \quad = \quad \begin{cases} \chi_\tau(g) & \text{si} \quad g \in H \\ 0 & \text{si} \quad g \notin H \end{cases} .$$

En général cette fonction est invariante par H-conjugaison, mais pas par G-conjugaison. Une manière "minimale" de la rendre invariante par G-conjugaison est de poser

$$\chi_\tau^G(g) := \sum_{x \in H\backslash G} \chi_\tau^0(xgx^{-1}) = \frac{1}{|H|} \sum_{x \in G} \chi_\tau^0(xgx^{-1}).$$

Ainsi, χ_τ^G est une fonction centrale sur G et $\chi_\tau^G(g) = 0$ si g n'est pas conjugué à un élément de H. Dans le théorème suivant, on note $\langle ., . \rangle_G$ le produit scalaire sur $\mathcal{F}(G, \mathbb{C})$, et $\langle ., . \rangle_H$ celui sur $\mathcal{F}(H, \mathbb{C})$.

THÉORÈME. – *Soient $H < G$ et (W, τ) comme ci-dessus.*

i) Pour toute fonction centrale f sur G, on a $\langle \chi_\tau^G, f\rangle_G = \langle \chi_\tau, f_{|H}\rangle_H$.

ii) La fonction centrale χ_τ^G est le caractère d'une représentation de G.

Démonstration. Pour i), on calcule

$$\begin{aligned}\langle \chi_\tau^G, f\rangle_G &= \frac{1}{|G||H|}\sum_{g\in G}\sum_{x\in G}\chi_\tau^0(xgx^{-1})\overline{f(g)} = \frac{1}{|G||H|}\sum_{x\in G}\sum_{g\in G}\chi_\tau^0(xgx^{-1})\overline{f(xgx^{-1})}\\ &= \frac{1}{|G||H|}\sum_{x\in G}\sum_{g\in x^{-1}Hx}\chi_\tau(xgx^{-1})\overline{f(xgx^{-1})} = \frac{1}{|G||H|}\sum_{x\in G}\sum_{h\in H}\chi_\tau(h)\overline{f(h)}\\ &= \frac{1}{|G|}\sum_{x\in G}\langle \chi_\tau, f_{|H}\rangle_H = \langle \chi_\tau, f_{|H}\rangle_H.\end{aligned}$$

En particulier, pour toute représentation ρ irréductible de G, on a

$$a_{\tau\rho} := \langle \chi_\tau^G, \chi_\rho\rangle_G = \langle \chi_\tau, \chi_{\rho_{|H}}\rangle_H \in \mathbb{N}.$$

Par l'égalité $\chi_\tau^G = \sum_\rho a_{\tau\rho}\chi_\rho$, on en déduit que χ_τ^G est le caractère de la représentation $\bigoplus_\rho \rho^{\oplus a_{\tau\rho}}$. □

Le caractère χ_τ^G s'appelle *caractère induit* de χ_τ à G.

Exemples :

i) Le caractère de la représentation régulière $\mathbb{C}G$ est le caractère induit de la représentation triviale $\mathbf{1}$ du sous-groupe trivial $H = \{e\}$. Ce que l'on peut écrire $\chi_{\mathbb{C}G} = \chi^G_{\mathbf{1}_{\{e\}}}$.

ii) Plus généralement, le caractère de la représentation de permutation $\mathbb{C}X$ où X est un G-ensemble transitif de la forme G/H est le caractère induit de la représentation triviale $\mathbf{1}_H$ de H. C'est-à-dire $\chi_{\mathbb{C}X} = \chi^G_{\mathbf{1}_H}$.

iii) Soit $G = D_n = \langle r\rangle \rtimes \langle s\rangle$. On a vu que le caractère standard χ_{std} de G est nul en dehors du sous-groupe cyclique $\langle r\rangle$ et donné par

$$\chi_{\mathrm{std}}(r^k) = 2\cos(2\pi k/n) = e^{2i\pi k/n} + e^{-2i\pi k/n}$$

pour tout k. Soit alors ψ le caractère (irréductible de dimension 1) du groupe $\langle r\rangle$ donné par $\psi(r^k) := e^{2i\pi k/n}$. Comme $sr^ks^{-1} = r^{-k}$, on voit que χ_{std} est le caractère induit de ψ, *i.e.* $\chi_{\mathrm{std}} = \psi^G$.

Le troisième exemple invite à chercher un critère pour que le caractère induit d'un caractère irréductible soit encore irréductible. On disposerait alors d'un outil pratique pour fabriquer des caractères irréductibles.

Supposons pour simplifier que *H est distingué dans G*, et soit $\chi = \chi_\tau$ un caractère irréductible de H. Pour tout $x \in G$, la fonction $\chi^x : h \mapsto \chi(xhx^{-1})$ est une fonction centrale sur H. C'est le caractère de la représentation (W, τ^x) définie par $\tau^x(h) := \tau(xhx^{-1})$, laquelle est irréductible, comme (W, τ). Le caractère χ^x est appelé "caractère conjugué" de χ par x.

PROPOSITION. – *Suppposons que $\chi \neq \chi^x$ pour tout $x \in G \setminus H$. Alors le caractère induit χ^G est irréductible.*

Démonstration. Il suffit de vérifier que $\langle \chi^G, \chi^G \rangle_G = 1$. D'après le théorème précédent on a $\langle \chi^G, \chi^G \rangle_G = \langle \chi, (\chi^G)_{|H} \rangle_H$. Or par définition, $(\chi^G)_{|H} = \sum_{x \in G/H} \chi^x$. Ainsi $\langle \chi^G, \chi^G \rangle_G = \sum_{x \in G/H} \langle \chi, \chi^x \rangle$ vaut 1 d'après notre hypothèse et l'orthogonalité des caractères.

□

4.3.2 *Point de vue des représentations.* Comme précédemment, partons d'une représentation (W, τ) d'un sous-groupe H de G. On pose

$$Ind_H^G(W) := \{ f : G \longrightarrow W, \, \forall h \in H, \forall x \in G, \; f(hx) = \tau(h) f(x) \} .$$

On munit cet espace vectoriel de l'action par translations à droite $(gf)(x) := f(xg)$. On obtient ainsi une représentation notée $Ind_H^G(\tau)$.

Exercice : montrer que le caractère de $Ind_H^G(\tau)$ est égal au caractère induit χ_τ^G.

L'avantage du point de vue des représentations sur celui des caractères est qu'il fonctionne pour tout corps de coefficients K, même de caractéristique positive.