Représentations linéaires des groupes finis, application au théorème de Burnside
Rapport de stage

Perrine Jouteur

mai-juin 2020

Table des matières

Depuis les découvertes de Galois, on sait exactement dans quel cas une équation polynomiale est résoluble par radicaux : c'est lorsque son groupe de Galois est résoluble. Encore faut-il pouvoir déterminer facilement si un groupe est résoluble... L'objectif principal de ce stage a été de démontrer un théorème dû à Burnside, qui donne un critère de résolubilité pour les groupes finis. La preuve initiale de ce théorème utilise la théorie des représentations de groupes. L'étude de cette théorie a fourni l'occasion d'aborder la notion de module sur un anneau [1], qui fait l'objet de la première partie du rapport, et qui est intimement liée à la notion de représentation, comme nous le verrons dans la deuxième partie sur les représentations de groupes finis [5], [3], [6]. La troisième partie illustre ce qui précède avec l'exemple du groupe général linéaire $GL_2(\mathbb{F}_q)$ [4]. Enfin, le théorème de Burnside et sa preuve sont présentés dans

la quatrième partie, qui donne également un autre critère de résolubilité plus intrinsèquement lié aux représentations de groupes.

1 Notions générales sur les modules

Dans cette partie, on met en place des outils généraux qui serviront pour la théorie des représentations. On désigne par A une algèbre sur un corps $\mathbb{K}$.

1.1 Premières définitions

Définition 1 A-module à gauche
Un A-module à gauche M est un $\mathbb{K}$-espace vectoriel compatible avec A, c'est-à-dire muni d'une application $(a, m) \longmapsto a \cdot m$ qui vérifie, pour tout $a, a' \in A$, pour tout $m, m' \in M$:
(i) $(a + a') \cdot m = a \cdot m + a' \cdot m$ et $a \cdot (m + m') = a \cdot m + a \cdot m'$
(ii) $a \cdot (b \cdot m) = (ab) \cdot m$
(iii) $1 \cdot m = m$
Un sous-module de M est un sous-espace vectoriel de M stable par A.

Remarque 1 On peut définir de même la notion de A-module à droite.

Définition 2 Morphisme de modules
Soient M, N deux A-modules à gauche, et $f : M \to N$ une application $\mathbb{K}$-linéaire. On dit que f est un morphisme de A-modules lorsque pour tout $a \in A$, pour tout $m \in M$,

$$f(a \cdot m) = a \cdot f(m)$$

On note $\mathrm{Hom}_A(M, N)$ l'ensemble des morphismes de A-modules de M dans N, qui peut lui-même être muni d'une structure de A-module à gauche.

La plupart des notions d'algèbre linéaire peuvent ainsi se généraliser aux modules : somme directe, produit tensoriel, famille libre, famille génératrice (s'il existe une famille génératrice finie, on dit que le module est de type fini), base... La suite de la partie a pour but de démontrer un isomorphisme qui servira dans une démonstration importante de la théorie des représentations.

Définition 3 Suite exacte, courte, décomposée
• Une suite de A-modules $M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} ... \xrightarrow{f_{n-1}} M_n$ est dite exacte lorsque pour tout $i \in [\![1, n-1]\!]$, on a $\mathrm{Ker}(f_{i+1}) = \mathrm{Im}(f_i)$.
• Une suite exacte courte est une suite exacte de la forme $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$, ce qui implique que f soit injective et g soit surjective.
• On dit qu'une suite exacte courte est décomposée lorsque M est une somme directe dont $\mathrm{Im}(f)$ est l'un des facteurs.

Propriété 1 Soit la suite exacte courte suivante : $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$. Il y a équivalence entre :
(i) La suite est décomposée ;
(ii) Il existe $h \in \mathrm{Hom}_A(M, L)$ tel que $h \circ f$ soit un automorphisme de L ;
(iii) Il existe $h' \in \mathrm{Hom}_A(N, M)$ tel que $g \circ h'$ soit un automorphisme de N.

Démonstration
• $(i) \Rightarrow (ii)$ Supposons que la suite soit décomposée. On peut écrire $M = \mathrm{Im}(f) \oplus M'$, pour un certain A-module M'. Comme f est injective, la corestriction à son image est un isomorphisme, que l'on note $\tilde{f}$. On définit alors le A-morphisme $h : M \to L$ par :

$$h(m) = \begin{cases} \tilde{f}^{-1}(m) \text{ si } m \in \mathrm{Im}(f) \\ 0 \text{ si } m \in M' \end{cases}$$

Par définition de la somme directe, h est bien défini sur M tout entier, et on a $h \circ f = \mathrm{id}_L \in \mathrm{Aut}_A(L)$.

• $(ii) \Rightarrow (i)$. Soit $m \in M$. En écrivant $m = \big(m - f(h(m))\big) + f(h(m))$, on remarque que tout élément de M est dans $\mathrm{Im}(f) + \mathrm{Ker}(h)$.

D'autre part, si $m \in \mathrm{Im}(f) \cap \mathrm{Ker}(h)$, alors il existe $l \in L$ tel que $m = f(l)$, et on a $h(f(l)) = 0$. Or par hypothèse $h \circ f$ est bijectif, donc $l = 0$, puis $m = 0$. Ainsi $\mathrm{Im}(f)$ et $\mathrm{Ker}(h)$ sont en somme directe, et

$$M = \mathrm{Im}(f) \oplus \mathrm{Ker}(h)$$

• L'équivalence entre (i) et (iii) se montre avec le même type d'arguments. ■

Définition 4 Foncteurs exacts
On note Mod la catégorie des A-modules (à gauche ou à droite).
• Soit $F : \mathrm{Mod} \to \mathrm{Mod}$ un foncteur covariant. On dit que F est exact à gauche lorsque pour toute suite exacte : $0 \to L \xrightarrow{f} M \xrightarrow{g} N$, la suite "image" est aussi exacte :

$$0 \to F_L \xrightarrow{Ff} F_M \xrightarrow{Fg} F_N$$

On définit de même l'exactitude à droite d'un foncteur covariant.

• Soit $G : \mathrm{Mod} \to \mathrm{Mod}$ un foncteur contravariant. On dit que G est exact à gauche lorsque pour toute suite exacte : $L \xrightarrow{f} M \xrightarrow{g} N \to 0$, la suite "image" est aussi exacte :

$$0 \to G_N \xrightarrow{Gg} G_M \xrightarrow{Gf} G_L$$

On définit de même l'exactitude à droite d'un foncteur contravariant.

• Enfin, on dit qu'un foncteur est exact lorsqu'il est exact à gauche et à droite.

Propriété 2 Soient X un A-module à gauche et Y un A-module à droite. Alors les foncteurs covariants $- \otimes_A X$ et $Y \otimes_A -$ sont exacts à droite.

Démonstration
• Soit $L \xrightarrow{f} M \xrightarrow{g} N \to 0$ une suite exacte de A-modules à droite. On va montrer que la suite "tensorielle" associée est exacte :

$$L \otimes X \xrightarrow{f\otimes 1} M \otimes X \xrightarrow{g\otimes 1} N \otimes X \to 0$$

Par définition, $\mathrm{Im}(f) = \mathrm{Ker}(g)$, ce qui implique immédiatement que $\mathrm{Im}(f \otimes 1) \subset \mathrm{Ker}(g \otimes 1)$. Montrons l'inclusion réciproque. On note $I := \mathrm{Im}(f \otimes 1)$, et comme $I \subset \mathrm{Ker}(g \otimes 1)$, l'application

$$\phi := \overline{(g \otimes 1)} : (M \otimes X)/I \longrightarrow N \otimes X$$

est encore un morphisme. Pour montrer que $I = \mathrm{Ker}(g \otimes 1)$, il suffit de montrer que ϕ est injective. On va pour cela construire une application ψ telle que $\psi \circ \phi = \mathrm{id}_{(M\otimes X)/I}$.
Pour $n \in N$, il existe $m \in M$ tel que $g(m) = n$. On pose ainsi, pour tout $x \in X$, $\psi(n \otimes x) = \pi(m \otimes x)$ (où on a noté $\pi : M \otimes X \to (M \otimes X)/I$ le morphisme canonique). Vérifions que ψ est bien définie :
Soient $m_1, m_2 \in M$ tels que $g(m_1) = g(m_2) = n$. Alors $m_1 - m_2 \in \mathrm{Ker}(g) = \mathrm{Im}(f)$ par hypothèse, donc $m_1 \otimes x - m_2 \otimes x \in I$, donc $\pi(m_1 \otimes x) = \pi(m_2 \otimes x)$, et ψ est bien définie, ce qui donne le résultat voulu : $I = \mathrm{Ker}(g \otimes 1)$.

Il ne reste plus qu'à montrer que $g \otimes 1$ est surjective. Soient $n \in N$ et $x \in X$. Comme g est surjective, il existe $m \in M$ tel que $g(m) = n$. D'où $(g \otimes 1)(m \otimes x) = n \otimes x$, et par linéarité, $(g \otimes 1)(M \otimes X) = N \otimes X$, donc $g \otimes 1$ est surjective.

• La preuve est analogue pour l'exactitude à droite de $Y \otimes_A -$. ■

Notation 1 Soit X un A-module à gauche. Pour tout morphisme de modules $f \in \mathrm{Hom}_A(M_1, M_2)$, on note $f_* := \mathrm{Hom}(X, f)$ le morphisme image de f par le foncteur $\mathrm{Hom}_A(X, -)$.
De même, on note f^* le morphisme image de f par le foncteur $\mathrm{Hom}_A(-, X)$. (voir annexe)

Propriété 3 Soit X un A-module à gauche. Alors le foncteur covariant (resp. contravariant) $\mathrm{Hom}_A(X, -)$ (resp. $\mathrm{Hom}_A(-, X)$) est exact à gauche.

Démonstration
Soit $0 \to L \xrightarrow{f} M \xrightarrow{g} N$ une suite exacte de A-modules à gauche. Montrons que la suite suivante est encore exacte :

$$0 \to \mathrm{Hom}(X, L) \xrightarrow{f_*} \mathrm{Hom}(X, M) \xrightarrow{g_*} \mathrm{Hom}(X, N)$$

Soit $\beta \in \mathrm{Im}(f_*)$: il existe $\alpha \in \mathrm{Hom}(X, L)$ tel que $\beta = f \circ \alpha$. Alors :

$$g_*(\beta) = g_*(f \circ \alpha) = g \circ f \circ \alpha$$

Or $\mathrm{Im}(f) = \mathrm{Ker}(g)$ donc $g_*(\beta) = 0$, et ainsi $\mathrm{Im}(f_*) \subset \mathrm{Ker}(g_*)$.
Inversement, soit $\beta \in \mathrm{Ker}(g_*)$. Pour tout $x \in X$, $\beta(x) \in \mathrm{Ker}(g) = \mathrm{Im}(f)$, donc pour tout $x \in X$, il existe $l_x \in L$ tel que $\beta(x) = f(l_x)$. On définit de la sorte une application : $\alpha : x \longmapsto l_x$
Comme β et f sont des morphismes, et que f est injectif, α est un morphisme de A-modules, et on a $f_*(\alpha) = \beta$. Donc $\beta \in \mathrm{Im}(f_*)$, et on a l'égalité recherchée $\mathrm{Ker}(g_*) = \mathrm{Im}(f_*)$.
De plus, si $\alpha \in \mathrm{Hom}(X, L)$ est tel que $f_*(\alpha) = 0$, alors pour tout $x \in X$, $f(\alpha(x)) = 0$ et par injectivité de f, pour tout $x \in X$, $\alpha(x) = 0$ donc $\alpha = 0$ et f_* est injectif.

La démonstration dans le cas contravariant $\mathrm{Hom}_A(-, X)$ est similaire. ■

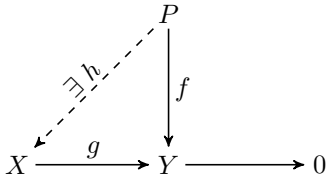
1.2 Module libre, module projectif

Définition 5 Soit M un A-module à gauche.
• On dit que M est libre lorsqu'il possède une A-base, c'est-à-dire une famille $(m_i)_{i \in I}$ telle que tout élément de M puisse s'écrire de manière unique comme une somme finie de termes de la forme $a_i m_i$, pour $a_i \in A$.
• On dit que M est projectif s'il est un facteur direct d'un module libre.

Propriété 4 Soit P un A-module à gauche. Il y a équivalence entre :

(*i*) P est projectif ;

(*ii*) Pour tout $g \in \mathrm{Hom}_A(X, Y)$ surjectif, pour tout $f \in \mathrm{Hom}_A(P, Y)$, il existe un morphisme $h \in \mathrm{Hom}_A(P, X)$ tel que le diagramme exact suivant commute :



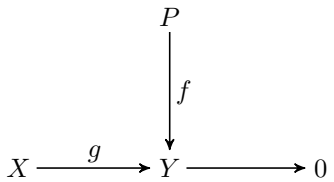
(*iii*) Pour tout $g \in \mathrm{Hom}_A(X, Y)$ surjectif, le morphisme $g_* : \mathrm{Hom}_A(P, X) \to \mathrm{Hom}_A(P, Y)$ est surjectif ;

(*iv*) Le foncteur $\mathrm{Hom}_A(P, -)$ est exact ;

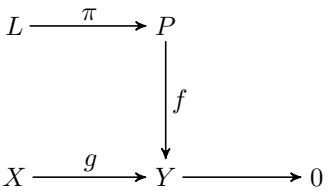
(*v*) Toute suite exacte courte $0 \to X \to Y \to P \to 0$ est décomposée.

Démonstration
• $(i) \Rightarrow (ii)$ Commençons par le cas où P est libre, et montrons qu'il existe un morphisme $h : P \to X$ tel que $f = g \circ h$.
Soit $(l_i)_{i \in I}$ une base de P en tant que module libre. Comme g est surjectif, pour tout $i \in I$, il existe $x_i \in X$ tel que $g(x_i) = f(l_i)$. On construit alors un morphisme h en posant $h(l_i) = x_i$ pour tout $i \in I$, ce qui est bien défini car (l_i) est une base de P. On constate que h convient.

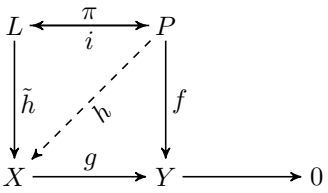
À présent, traitons le cas général, où P est seulement projectif. Il existe P' un A-module, tel que $L := P \oplus P'$ soit libre. Si on se donne un diagramme



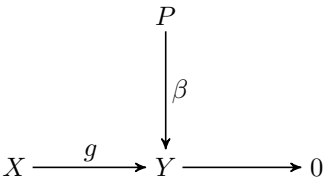
on peut le compléter en rajoutant la projection $\pi : L \to P$ associée à la décomposition en somme directe :



D'après le cas précédent, il existe un morphisme $\tilde{h} : L \to X$, qui fait commuter ce diagramme. En composant $\tilde{h}$ et l'inclusion $i : P \to L$, on obtient un nouveau morphisme $h : P \to X$ et qui fait commuter le diagramme.



• $(ii) \Rightarrow (iii)$ Supposons (ii), et prenons $g \in \mathrm{Hom}_A(X, Y)$, surjectif. Montrons que g_* l'est encore : soit $\beta \in \mathrm{Hom}_A(P, Y)$. On a le diagramme suivant :



D'après l'hypothèse (ii), il existe $\alpha \in \mathrm{Hom}_A(X, P)$ tel que ce diagramme commute, c'est-à-dire tel que $g_*(\alpha) = \beta$.

• $(iii) \Rightarrow (iv)$ On sait déjà que le foncteur covariant $\mathrm{Hom}_A(P, -)$ est exact à gauche. Pour montrer qu'il est exact à droite, on reproduit la même preuve que pour l'exactitude à gauche, rendue possible grâce à l'hypothèse de conservation de la surjectivité.

• $(iv) \Rightarrow (v)$ Supposons (iv), et considérons une suite exacte courte : $0 \to X \xrightarrow{f} Y \xrightarrow{g} P \to 0$.
Par hypothèse, en appliquant le foncteur $\mathrm{Hom}_A(P, -)$, on obtient encore une suite exacte :

$$0 \to \mathrm{Hom}(P, X) \xrightarrow{f_*} \mathrm{Hom}(P, Y) \xrightarrow{g_*} \mathrm{Hom}(P, P) \to 0$$

En particulier, g_* est surjectif, donc il existe $h \in \mathrm{Hom}_A(P, Y)$ tel que $g_*(h) = \mathrm{id}_P$, c'est-à-dire $g \circ h = \mathrm{id}_P$, ce qui équivaut au fait que la suite exacte soit décomposée d'après la propriété 12.

• $(v) \Rightarrow (i)$ Supposons (v). On peut plonger P dans un module libre, en prenant par exemple le A-module libre $N := A^{(P)}$ engendré par tous les éléments de P. Il existe donc une projection $\pi : N \to P$. La suite $0 \to \mathrm{Ker}(\pi) \to N \to P \to 0$ est alors exacte, et par l'hypothèse (v), elle est décomposée. Donc $N = \mathrm{Ker}(\pi) \oplus P$, et P est bien facteur direct d'un module libre. ■

Définition 6 Soit X un A-module à gauche. On dit que X est plat lorsque le foncteur $- \otimes_A X$ est exact.

Propriété 5 Tout module projectif est plat.

Démonstration
• On commence par remarquer que tout module libre est plat. En effet, un module libre est isomorphe à une somme directe de copies de A en tant que A-module. Or A est un module plat, et le produit tensoriel est distributif par rapport à la somme directe, donc toute somme directe de copies de A est plate.

• Considérons à présent P, un module projectif. On sait déjà que le foncteur $- \otimes_A P$ est exact à droite. Soit la suite exacte suivante :

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N$$

Comme P est projectif, il existe un module P' tel que $F = P \oplus P'$ soit un module libre. D'après ce qui précède, F est plat, donc la suite suivante est exacte :

$$0 \to L \otimes F \xrightarrow{f\otimes 1_F} M \otimes F \xrightarrow{g\otimes 1_F} N \otimes F$$

Mais comme $F = P \oplus P'$, pour tout module X on a $X \otimes F \simeq (X \otimes P) \oplus (X \otimes P')$, et pour tout morphisme $h : X \to Y$, on a $h \otimes 1_F = (h \otimes 1_P) \oplus (h \otimes 1_{P'})$. Donc la suite suivante est exacte :

$$0 \to (L \otimes P) \oplus (L \otimes P') \xrightarrow{f\otimes 1_P \oplus f\otimes 1_{P'}} (M \otimes P) \oplus (M \otimes P') \xrightarrow{g\otimes 1_P \oplus g\otimes 1_{P'}} (N \otimes P) \oplus (N \otimes P')$$

Et nécessairement, on a l'exactitude de la suite $0 \to L\otimes P \xrightarrow{f\otimes 1_P} M \otimes P \xrightarrow{g\otimes 1_P} N \otimes P$, donc P est plat.■

1.3 Un isomorphisme naturel

Théorème 1
• Soient L et M deux A-modules à droite. On suppose que L est projectif et de type fini. Alors il y a un isomorphisme naturel :

$$L \otimes_A \mathrm{Hom}_A(M, A) \simeq \mathrm{Hom}_A(M, L)$$

• Soient L et M deux A-modules à gauche. On suppose que M est projectif et de type fini. Alors il y a un isomorphisme naturel :

$$\mathrm{Hom}_A(M, A) \otimes_A L \simeq \mathrm{Hom}_A(M, L)$$

Démonstration
• Considérons l'application bilinéaire suivante :

$$\begin{array}{rccc} \tilde{\psi}_{M,L} : & L \times \mathrm{Hom}_A(M, A) & \longrightarrow & \mathrm{Hom}_A(M, L) \\ & (l, \alpha) & \longmapsto & (m \mapsto \alpha(m)l) \end{array}$$

Par propriété universelle du produit tensoriel, il existe un unique morphisme de A-modules $\psi_{M,L}$ tel que pour tout $l \in L$, pour tout $\alpha \in \mathrm{Hom}_A(M, A)$, on ait $\psi_{M,L}(l \otimes \alpha) = \tilde{\psi}_{M,L}((l, \alpha))$.
Supposons dans un premier temps que L soit libre et de type fini. Alors il existe une famille libre $(l_1, ..., l_k)$ qui engendre L, donc tout morphisme $\beta : M \to L$ se décompose de manière unique en somme de morphismes $\beta_i : M \to \mathrm{Vect}(l_i)$. Ceci fournit une application réciproque à $\psi_{M,L}$, qui est donc un isomorphisme.
Traitons à présent le cas où L est seulement projectif de type fini : il existe un module L' tel que $L \oplus L'$ soit libre. D'après ce qui précède, $(L \oplus L') \otimes \mathrm{Hom}_A(M, A)$ est isomorphe à $\mathrm{Hom}_A(M, L \oplus L')$. Mais $(L \oplus L') \otimes \mathrm{Hom}_A(M, A)$ est isomorphe à $L \otimes \mathrm{Hom}_A(M, A) \oplus L' \otimes \mathrm{Hom}_A(M, A)$ et $\mathrm{Hom}_A(M, L \oplus L')$ est isomorphe à $\mathrm{Hom}_A(M, L) \oplus \mathrm{Hom}_A(M, L')$. Donc l'application suivante est un isomorphisme :

$$\Psi_M : L \otimes \mathrm{Hom}_A(M, A) \oplus L' \otimes \mathrm{Hom}_A(M, A) \longrightarrow \mathrm{Hom}_A(M, L) \oplus \mathrm{Hom}_A(M, L')$$

Or pour tout $l \in L$, pour tout $\alpha \in \mathrm{Hom}_A(M, A)$, $\Psi_M(l \otimes \alpha)$ appartient à $\mathrm{Hom}_A(M, L)$, donc $\Psi_M = \psi_{M,L} \oplus \psi_{M,L'}$, et le morphisme $\psi_{M,L}$ est bijectif.
Montrons que cet isomorphisme est naturel. Soient M et N deux A-modules à droite, et $f \in \mathrm{Hom}_A(M, N)$. On note $f_A^* : \mathrm{Hom}_A(N, A) \to \mathrm{Hom}_A(M, A)$ et $f_L^* : \mathrm{Hom}_A(N, L) \to \mathrm{Hom}_A(M, L)$ les morphismes images de f par les foncteurs $\mathrm{Hom}_A(-, A)$ et $\mathrm{Hom}_A(-, L)$ respectivement. Il s'agit de montrer que le diagramme suivant commute :

$$\begin{array}{ccc} L \otimes_A \mathrm{Hom}_A(M, A) & \xrightarrow{\psi_{M,L}} & \mathrm{Hom}_A(M, L) \\ \uparrow{\scriptstyle 1_L \otimes f_A^*} & & \uparrow{\scriptstyle f_L^*} \\ L \otimes_A \mathrm{Hom}_A(N, A) & \xrightarrow{\psi_{N,L}} & \mathrm{Hom}_A(N, L) \end{array}$$

Soit donc $(l, \alpha) \in L \otimes_A \mathrm{Hom}_A(N, A)$. On a d'une part :

$$\psi_{M,L} \circ 1_L \otimes f_A^*(l \otimes \alpha) = m \mapsto \alpha(f(m))l$$

Et d'autre part :

$$f_L^* \circ \psi_{N,L}(l \otimes \alpha) = f_L^*(n \mapsto \alpha(n)l) = m \mapsto \alpha(f(m))l$$

Les deux morphismes $\psi_{M,L} \circ (1_L \otimes f_A^*)$ et $f_L^* \circ \psi_{N,L}$ coïncident sur la famille génératrice des $l \otimes \alpha$, donc ils sont égaux. Ainsi le diagramme commute, et on a bien une transformation naturelle.

• Le deuxième point se montre de manière identique. ■

Remarque 2 On peut en fait aller plus loin, en démontrant que le produit tensoriel est adjoint à gauche du foncteur Hom :

Soit L un (A, A)-bimodule (c'est-à-dire un A-module à droite et à gauche). Soient M et N deux A-modules à gauche. Il y a un isomorphisme ϕ entre $\mathrm{Hom}_A(L \otimes M, N)$ et $\mathrm{Hom}_A(M, \mathrm{Hom}_A(L, N))$, tel que pour tout $\alpha \in \mathrm{Hom}_A(L \otimes M, N)$, $\phi(\alpha)$ soit défini par :

$$\begin{array}{rccc} \phi(\alpha) : & M & \longrightarrow & \mathrm{Hom}_A(L, N) \\ & m & \longmapsto & \big(l \mapsto \alpha(l \otimes m)\big) \end{array}$$

De plus, si $f : M' \to M$ et $g : N \to N'$ sont des morphismes de A-modules à gauche, alors le diagramme suivant commute :

$$\begin{array}{ccc} \mathrm{Hom}_A(L \otimes M, N) & \xrightarrow{\mathrm{Hom}(L \otimes f, g)} & \mathrm{Hom}_A(L \otimes M', N') \\ \Big\downarrow{\scriptstyle \phi} & & \Big\downarrow{\scriptstyle \mathrm{Hom}(f, \mathrm{Hom}(L, g))} \\ \mathrm{Hom}_A(M, \mathrm{Hom}_A(L, N)) & \xrightarrow[\phi]{} & \mathrm{Hom}_A(M', \mathrm{Hom}_A(L, N')) \end{array}$$

2 Théorie des représentations

Dans toute la partie, G est un groupe fini et $\mathbb{K}$ est un corps dont la caractéristique ne divise pas l'ordre de G.

2.1 Fondamentaux

Définition 7 Représentation linéaire de groupe
Soit V un $\mathbb{K}$-espace vectoriel de dimension finie. On appelle représentation de G sur V tout morphisme de groupes $\rho : G \longrightarrow GL(V)$.

Remarque 3 Lien avec les modules
Modules et représentations sont en fait deux points de vue pour un même objet : en effet, toute représentation définit une structure de $\mathbb{K}[G]$-module pour V, en posant $a \cdot v = \rho_a(v)$ pour tout $a \in G$, tout $v \in V$, et en étendant par linéarité à $\mathbb{K}[G]$. Inversement, tout $\mathbb{K}[G]$-module définit une représentation de G, en prenant pour ρ_a l'application linéaire qui envoie v sur $a \cdot v$.

Définition 8 Catégorie Rep(G)
La catégorie des représentations du groupe G est la catégorie dont les objets sont les représentations de G, et où les morphismes sont les applications définies comme suit : un morphisme de représentations de (V_1, ρ^1) vers (V_2, ρ^2) est une application $f \in \mathcal{L}(V_1, V_2)$, telle que pour tout $s \in G$, $\rho_s^2 \circ f = f \circ \rho_s^1$.
Si on assimile représentations et $\mathbb{K}[G]$-modules, un morphisme de représentations est simplement un morphisme de modules.

Définition 9 Soit V_1 et V_2 deux représentations de G. On dit que V_1 et V_2 sont équivalentes lorsqu'il existe un isomorphisme de représentations entre V_1 et V_2.

Remarque 4 Considérons l'action de G sur l'ensemble des applications $\mathbb{K}$-linéaires de V_1 dans V_2, définie par :

$$s \cdot f = \rho_s^2 \circ f \circ (\rho_s^1)^{-1}$$

Cette action dote $\mathcal{L}(V_1, V_2)$ d'une structure de $\mathbb{K}[G]$-module à gauche, et un morphisme de représentations entre V_1 et V_2 est un point fixe pour cette action.

Définition 10 Sous-représentation
Soit V une représentation de G. Une sous-représentation de V est un sous espace vectoriel W de V, stable par G, c'est-à-dire tel que :

$$\forall s \in G,\ \rho_s(W) \subset W$$

Cela correspond à la notion de sous-module.

Remarque 5 Si on fixe une base $\mathcal{B}_W$ de la sous-représentation W, et qu'on la complète en une base $\mathcal{B}$ de V, alors pour tout $s \in G$, on a :

$$\mathrm{mat}_{\mathcal{B}}(\rho_s) = \left(\begin{array}{c|c} \mathrm{mat}_{\mathcal{B}_W}(\rho_s^W) & (*) \\ \hline (0) & (**) \end{array}\right)$$

La matrice $(**)$ décrit la sous-représentation de G sur le quotient V/W.

Théorème 2 (Maschke)
Soit V une représentation de G, et W une sous-représentation de V.
Alors il existe une sous-représentation W^o de V telle que $V = W \oplus W^o$.

Démonstration
• Commençons par le cas où $\mathbb{K} = \mathbb{C}$, de telle sorte qu'on puisse munir V d'un produit scalaire hermitien, $\langle , \rangle_0$.
On définit, pour $x, y \in V$,

$$\langle x, y \rangle = \sum_{s \in G} \langle \rho_s(x), \rho_s(y) \rangle_0$$

$\langle , \rangle$ est une forme sesquilinéaire, hermitienne, définie positive car on est ici en caractéristique 0, donc il s'agit d'un produit scalaire hermitien. De plus, $\langle , \rangle$ est stable par G. Ainsi l'orthogonal de W par ce produit scalaire est également stable par G.

• Dans le cas général :
Soit $\tilde{W}$ un supplémentaire de W dans V, et p le projecteur sur $\tilde{W}$ parallèlement à W. On définit :

$$p^o = \frac{1}{|G|} \sum_{s \in G} \rho_s^{-1} \circ p \circ \rho_s$$

On remarque que c'est ici que prend son intérêt l'hypothèse que la caractéristique de $\mathbb{K}$ ne divise pas $|G|$.
On a : $p^o \circ p^o = p^o$, donc p^o est un projecteur. De plus, comme W est stable par G, $W \subset \mathrm{Ker}(p^o)$. Or $\mathrm{rg}(p^o) = \mathrm{Tr}(p^o) = \mathrm{Tr}(p) = \mathrm{rg}(p)$, et V est de dimension finie, donc $W = \mathrm{Ker}(p^o)$.
Notons $W^o = \mathrm{Im}(p^o)$. Soit $y = p^o(x) \in \mathrm{Im}(p^o)$. Alors pour tout $s \in G$,

$$\begin{aligned} \rho_s(y) &= \frac{1}{|G|} \sum_{t \in G} \rho_{st^{-1}}(p(\rho_t(x))) \\ &= \frac{1}{|G|} \sum_{t \in G} \rho_{t^{-1}}(p(\rho_{ts}(x))) \text{ par décalage d'indices} \\ &= \left(\frac{1}{|G|} \sum_{t \in G} \rho_{t^{-1}} \circ p \circ \rho_t \right) \circ \rho_s\ (x) = p^o(\rho_s(x)) \end{aligned}$$

Ainsi W^o est stable par G, et on a bien $W \oplus W^o = V$. ■

Définition 11 Représentation irréductible
On dit qu'une représentation V de G est irréductible lorsqu'elle est non nulle et que ses seules sous-représentations sont $\{0\}$ et V.

Propriété 6 Toute représentation est somme directe de représentations irréductibles.

Démonstration Cela provient d'une récurrence immédiate sur la dimension, en utilisant le théorème de Maschke. ■

Notation 2 Soit U un $\mathbb{K}[G]$-module à gauche. On notera U^G l'espace des invariants par l'action de G sur U, c'est-à-dire l'ensemble des vecteurs $x \in U$ tels que pour tout $s \in G$, $s \cdot x = x$

Théorème 3 Lemme de Schur
Soient deux représentations de G irréductibles, V et W, sur $\mathbb{K}$. Alors :

- Si elles ne sont pas isomorphes, $(\mathrm{Hom}(V,W))^G = \{0\}$;
- Si elles sont égales, $(\mathrm{Hom}(V,V))^G$ est un corps, non nécessairement commutatif, qui est une extension de $\mathbb{K}$. De plus, si $\mathbb{K}$ est algébriquement clos, alors $(\mathrm{Hom}(V,V))^G = \mathbb{K} \cdot \mathrm{id}_V$.

Démonstration
• Supposons que V et W ne soient pas isomorphes. Soit $f \in (\mathrm{Hom}(V,W))^G$. f est un morphisme de représentations, donc $\mathrm{Ker}(f)$ (resp. $\mathrm{Im}(f)$) est une sous-représentation de V (resp. de W). Par irréductibilité de V et de W :

$$\mathrm{Ker}(f) = \{0\} \text{ ou } V \text{ et } \mathrm{Im}(f) = \{0\} \text{ ou } W$$

Mais V et W ne sont pas isomorphes, donc f ne peut pas être bijectif : soit $\mathrm{Ker}(f) \neq \{0\}$ (défaut d'injectivité), soit $\mathrm{Im}(f) \neq W$ (défaut de surjectivité). Nécessairement, $f = 0$.

• Supposons à présent que $V = W$. On note $E_G(V) := (\mathrm{Hom}(V,V))^G$. Pour montrer que $E_G(V)$ est un corps, il suffit de montrer que tous ses éléments non nuls sont inversibles, car $E_G(V)$ possède déjà une structure d'anneau.
Soit $f \in E_G(V)$, non nul. Par le même raisonnement qu'au point précédent, on montre que $\mathrm{Ker}(f) = \{0\}$ et $\mathrm{Im}(f) = V$. Ainsi f est bijectif, et son inverse est encore un point fixe de l'action de G sur V.
On pose :

$$\begin{array}{rccc} \phi : & \mathbb{K} & \longrightarrow & E_G(V) \\ & k & \longmapsto & k \cdot \mathrm{id}_V \end{array}$$

ϕ est un morphisme de corps, ce qui fait bien de $E_G(V)$ une extension de $\mathbb{K}$.
De plus, si $\mathbb{K}$ est algébriquement clos, toute extension finie est l'extension triviale, donc $E_G(V) = \mathbb{K} \cdot \mathrm{id}_V$.■

2.2 Caractères

Dans toute la suite, on prend $\mathbb{K} = \mathbb{C}$.

Définition 12 Caractère d'une représentation
Soit $\rho : G \longrightarrow GL(V)$ une représentation. On appelle caractère de ρ l'application suivante :

$$\begin{array}{rccc} \chi : & G & \longrightarrow & \mathbb{C} \\ & s & \longmapsto & \mathrm{Tr}(\rho(s)) \end{array}$$

Remarque 6 Toute représentation de degré 1 coïncide avec son caractère : on parle de caractère linéaire.

Propriété 7 Soit χ le caractère d'une représentation de G. On a :

(*i*) $\chi(1) = \dim(V)$
(*ii*) $\forall s \in G$, $\chi(s^{-1}) = \overline{\chi(s)}$
(*iii*) χ est une fonction de classe, c'est-à-dire qu'il est constant sur chaque classe de conjugaison de G.
(*iv*) $\forall s \in G$, $|\chi(s)| \leqslant \chi(1)$

Démonstration
(*i*) Comme ρ est un morphisme de groupes, $\rho(1) = \mathrm{id}_V$ donc $\mathrm{Tr}(\rho(1)) = \dim(V)$.

(*ii*) Soit $s \in G$. Par propriété de morphisme, et comme G est d'ordre fini, les valeurs propres de $\rho(s)$ sont des racines de l'unité, donc leur inverse est égal à leur conjugué. Ainsi les valeurs propres de $\rho(s^{-1})$ sont les conjugués des valeurs propres de $\rho(s)$. Or la trace est la somme des valeurs propres d'une application linéaire, d'où le résultat.

(*iii*) Ceci provient immédiatement du fait que $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ pour n'importe quelles matrices carrées A, B.

(*iv*) Comme les racines de $\rho(s)$ sont de module 1, il suffit d'appliquer l'inégalité triangulaire pour avoir le résultat. ■

Propriété 8 Soient $\rho^1 : G \longrightarrow GL(V_1)$ et $\rho^2 : G \longrightarrow GL(V_2)$ deux représentations de G, de caractères χ_1 et χ_2 respectivement. Alors :
(*i*) Le caractère de $V_1 \oplus V_2$ vaut $\chi_1 + \chi_2$
(*ii*) Le caractère de $V_1 \otimes V_2$ vaut $\chi_1 \cdot \chi_2$

Démonstration Soit $s \in G$.
(*i*) Dans une base B adaptée à la décomposition $V := V_1 \oplus V_2$, on a :

$$\mathrm{mat}_B(\rho_s^1 + \rho_s^2) = \left(\begin{array}{c|c} \mathrm{mat}_{B_{V_1}}(\rho_s^1) & (0) \\ \hline (0) & \mathrm{mat}_{B_{V_2}}(\rho_s^2) \end{array}\right)$$

Ainsi, $\mathrm{Tr}(\rho_s^1 + \rho_s^2) = \mathrm{Tr}(\rho_s^1) + \mathrm{Tr}(\rho_s^2)$.

(*ii*) Les valeurs propres de $\rho_s^1 \otimes \rho_s^2$ sont les produits $\lambda \cdot \mu$ pour λ (resp. μ) valeur propre de ρ_s^1 (resp. ρ_s^2). Ainsi :

$$\mathrm{Tr}(\rho_s^1 \otimes \rho_s^2) = \sum_{i=1}^{n}\sum_{j=1}^{m} \lambda_i \cdot \mu_j = \mathrm{Tr}(\rho_s^1) \cdot \mathrm{Tr}(\rho_s^2)$$

D'où le résultat. ■

Définition 13 Soit (V, ρ) une représentation de G, de caractère χ. On peut construire la représentation duale V^* par : $\forall s \in G, \rho_s^* = {}^t\rho_{s^{-1}}$.

Propriété 9 Le caractère dual associé à V sera alors : $\chi^* = \overline{\chi}$.

Démonstration En effet, pour $s \in G$, les valeurs propres de $\rho^*(s)$ sont les inverses des valeurs propres de $\rho(s)$. Comme ce sont des racines de l'unité, leur inverse est égal à leur conjugué, donc la somme des valeurs propres de $\rho(s)^*$ est le conjugué de la somme des valeurs propres de $\rho(s)$. ■

2.3 Orthonormalité des caractères irréductibles

Lemme 1 Soit $\rho : G \longrightarrow GL(U)$ une représentation de G, de caractère χ.
Alors $\dim(U^G) = \dfrac{1}{|G|}\displaystyle\sum_{s\in G} \chi(s)$

Démonstration
On remarque que $f := \dfrac{1}{|G|}\displaystyle\sum_{s\in G} \rho_s$ est un projecteur sur U^G. En effet, $f \circ f = f$, et $\mathrm{Im}(f) = U^G$.
Ainsi $\dim(U^G) = \mathrm{Tr}(f) = \dfrac{1}{|G|}\sum_{s\in G} \chi(s)$. ■

Propriété 10 Première relation d'orthogonalité
Soient V, W deux représentations irréductibles de G, de caractères χ_V et χ_W respectivement. Alors :

$$\frac{1}{|G|}\sum_{s\in G} \overline{\chi_V(s)}\chi_W(s) = \begin{cases} 1 \text{ si } V \simeq W \\ 0 \text{ sinon} \end{cases}$$

Remarque 7 Dans le cas d'un corps quelconque $\mathbb{K}$, cette formule se réécrit :

$$\frac{1}{|G|}\sum_{s\in G} \overline{\chi_V(s)}\chi_W(s) = \begin{cases} \dim_{\mathbb{K}}(E_G(V)) \text{ si } V \simeq W \\ 0 \text{ sinon} \end{cases}$$

Et la démonstration est identique au cas complexe.

Démonstration
Appliquons le lemme à $U = \mathrm{Hom}(V, W)$: dans la première partie, on a vu que $\mathrm{Hom}_{\mathbb{C}}(V, W) \simeq \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C}) \otimes W$ donc $U \simeq V^* \otimes W$, et on peut écrire, grâce au lemme 1 :

$$\dim(U^G) = \dim((V^* \otimes W)^G) = \frac{1}{|G|} \sum_{s \in G} \chi_{V^* \otimes W}(s) = \frac{1}{|G|} \sum_{s \in G} \overline{\chi_V(s)} \chi_W(s)$$

Le lemme de Schur permet de conclure. ■

Remarque 8 La formule ci-dessus amène à définir, pour ϕ, ψ deux fonctions de G dans $\mathbb{C}$, la quantité suivante :

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{s \in G} \overline{\phi(s)} \psi(s)$$

Il s'agit d'un produit scalaire hermitien. La propriété précédente montre ainsi que sur un corps algébriquement clos dont la caractéristique ne divise pas $|G|$, les caractères irréductibles de G forment une famille orthonormée pour ce produit scalaire.

Corollaire 1 Soit V une représentation de G, de caractère ϕ, décomposée en somme directe de sous-représentations irréductibles : $V = W_1 \oplus ... \oplus W_h$.
Soit W une représentation irréductible de G, de caractère χ. Le nombre de W_i isomorphes à W dans la décomposition de V vaut alors $\langle \phi, \chi \rangle$, et est indépendant du choix de la décomposition de V en sous-représentations irréductibles.

Démonstration On a $\phi = \sum_{i=1}^{h} \chi_i$, où χ_i désigne le caractère de W_i. Donc, par semi-linéarité à gauche du produit scalaire, $\langle \phi, \chi \rangle = \sum_{i=1}^{h} \langle \chi_i, \chi \rangle$.
On simplifie en utilisant la propriété d'orthonormalité : $\langle \phi, \chi \rangle = \sum_{i \text{ tq } \chi_i = \chi} 1$, ce qui donne le résultat. ■

Corollaire 2 Deux représentations de G sont isomorphes si et seulement si elles sont le même caractère.

Démonstration Si deux représentations sont isomorphes, il est facile de voir qu'elles ont le même caractère, puisque la trace est invariante sur les classes de similitudes.
Inversement, si deux représentations ont le même caractère, d'après le corollaire précédent, leurs décompositions en sous-représentations irréductibles seront isomorphes, donc elles seront elles-mêmes isomorphes. ■

Propriété 11 Soit V une représentation de G, de caractère ϕ. Alors la quantité $\langle \phi, \phi \rangle$ est un entier positif, qui vaut 1 si et seulement si V est irréductible.

Démonstration Décomposons V en somme directe de sous-représentations irréductibles W_i, de caractères χ_i : $V = m_1 W_1 \oplus ... \oplus m_h W_h$.

$$\langle \phi, \phi \rangle = \sum_{i=1}^{h} \sum_{j=1}^{h} m_i m_j \langle \chi_i, \chi_j \rangle = \sum_{i=1}^{h} m_i^2$$

Donc $\langle \phi, \phi \rangle \in \mathbb{N}$, et si $\langle \phi, \phi \rangle = 1$, alors V ne contient qu'une représentation irréductible, avec une multiplicité 1, donc V est irréductible. ■

Définition 14 La représentation régulière R de G est la représentation associée à l'action de G sur lui-même : on pose $V = \mathbb{C}^{|G|}$, muni d'une base $(e_s)_{s \in G}$ indexée par les éléments de G, et pour tout $s, t \in G$, $R_s(e_t) = e_{st}$.
En terme de $\mathbb{K}[G]$-modules, la représentation régulière consiste à voir $\mathbb{K}[G]$ comme un module sur lui-même.

Propriété 12 Soit R la représentation régulière de G, et r_G son caractère. Alors $\chi(s) = 0$ pour tout $s \neq 1$ et $\chi(1) = |G|$.

Démonstration Soit $s \in G$. Pour tout $t \in G$, $st = s$ si et seulement si $s = 1$, donc la matrice dans la base $(e_s)_{s \in G}$ de R_t n'a que des zéros sur la diagonale sauf si $t = 1$ et dans ce cas, il s'agit de la matrice identité de taille $|G| \times |G|$. ■

Propriété 13 La représentation régulière de G contient toutes les représentations irréductibles de G avec une multiplicité égale à leur degré.

Démonstration Soit χ le caractère d'une représentation irréductible de G. Le nombre de fois que cette représentation apparaît dans une décomposition de R vaut $\langle \chi, r_G \rangle = \frac{1}{|G|} \sum_{t \in G} \chi(t)\overline{r_G(t)} = \chi(1)$
D'où le résultat. ■

Corollaire 3 Soient $\chi_1, ...\chi_h$ les caractères irréductibles de G. Alors $\sum_{i=1}^{h} \chi_i(1)^2 = |G|$

Démonstration On note n_i le degré du caractère χ_i pour $i \in [\![1, h]\!]$
Calculons $\langle r_G, r_G \rangle$. D'une part :

$$\langle r_G, r_G \rangle = \sum_{i=1}^{h} \sum_{j=1}^{h} n_i n_j \chi_i \chi_j = \sum_{i=1}^{h} n_i^2 = \sum_{i=1}^{h} \chi_i(1)^2$$

D'autre part,

$$\langle r_G, r_G \rangle = \frac{1}{|G|} \sum_{t \in G} |r_G(t)|^2 = |G|$$

On obtient finalement le résultat. ■

Théorème 4 Les caractères irréductibles de G forment une base orthonormée de l'espace des fonctions de classe sur G, que l'on notera F_G.

Lemme 2 Soit $f \in F_G$ et $\rho : G \longrightarrow GL(V)$ une représentation irréductible de caractère χ et de degré n. On pose

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

Alors ρ_f est une homothétie de rapport $\frac{|G|}{n}\langle f, \bar{\chi} \rangle$.

Démonstration (du lemme)
Soit $s \in G$. On a

$$\begin{aligned} \rho_s \circ \rho_f &= \sum_{t \in G} f(s^{-1}t)\rho_t \text{ par décalage d'indice} \\ &= \sum_{t \in G} f(ts^{-1})\rho_t \text{ car } f \in F_G \\ &= \rho_f \circ \rho_s \text{ par décalage d'indice} \end{aligned}$$

D'après le lemme de Schur, ρ_f est une homothétie, de rapport $\frac{\mathrm{Tr}(\rho_f)}{n} = \frac{|G|}{n}\langle f, \bar{\chi} \rangle$. ■

Démonstration (du théorème)
On a déjà montré que les caractères irréductibles de G forment une famille orthonormée de F_G. Il ne reste plus qu'à montrer le caractère générateur de cette famille.
Comme $\mathbb{C}$ est complet, il suffit de montrer que l'orthogonal de l'espace engendré par les caractères de G est nul. Soit donc $f \in F_G$, orthogonale à tous les caractères irréductibles de G.
D'après le lemme précédent, pour toute représentation irréductible ρ, l'application ρ_f est nulle. Par linéarité, l'application $R_f = \sum_{t \in G} f(t)R_t$, où R désigne la représentation régulière, est également nulle.
Soit $(e_t)_{t \in G}$ une base de la représentation régulière. On a : $R_f(e_1) = \sum_{t \in G} f(t)e_t = 0$. Comme la famille $(e_t)_t$ est libre, on obtient que $f(t) = 0$ pour tout $t \in G$. Ainsi f est nulle. ■

Corollaire 4 G possède autant de caractères irréductibles que de classes de conjugaison.

Démonstration En effet, la dimension de F_G est égale au nombre de classes de conjugaison dans G. ■

Propriété 14 Seconde relation d'orthogonalité
Soient $g, h \in G$. Alors

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \begin{cases} 0 \text{ si } g \text{ et } h \text{ ne sont pas conjugués} \\ \dfrac{|G|}{|Cl(g)|} \text{ sinon} \end{cases}$$

Démonstration
Soient $C_1, ..., C_r$ les classes de conjugaison de G et $g_1, ..., g_r$ des représentants de ses classes. On note X la matrice de coefficients $(\chi_i(g_j))$ et D la matrice diagonale de coefficients $(\delta_{ij}|C_i|)_{ij}$. D'après la première relation d'orthogonalité, on a $|G|I = XD\overline{X}^t$. Ainsi l'inverse à droite de X vaut $\dfrac{1}{|G|}D\overline{X}^t$. Il s'agit donc aussi de son inverse à gauche, ce qui s'écrit $D\overline{X}^t X = |G|I$, et pour le coefficient i, j, on a :

$$\sum_{k=1}^{r} |C_i|\overline{\chi_k(g_i)}\chi_k(g_j) = |G|\delta_{ij}$$

Comme les caractères sont des fonction de classe, on a le résultat. ■

Exemple 1 Déterminons tous les caractères irréductibles de $\mathfrak{S}_3$.

Ce groupe possède trois classes de conjugaison : l'identité, les 2-cycles et les 3-cycles. $\mathfrak{S}_3$ possède donc trois caractères irréductibles, χ_1, χ_2 et χ_3. On connaît déjà deux caractères de degré 1 qui sont les deux morphismes de groupes de $\mathfrak{S}_3$ dans $\mathbb{C}^*$: le morphisme trivial et la signature.

D'autre part, on doit avoir $\chi_1(1)^2+\chi_2(1)^2+\chi_3(1)^2 = 6$, donc le degré du troisième caractère est 2. Afin de déterminer ses valeurs, on considère l'action de $\mathfrak{S}_3$ sur $\mathbb{C}^3$ qui consiste à permuter les coordonnées des vecteurs dans la base canonique. Cette action définit une représentation de $\mathfrak{S}_3$, de degré 3, qui contient une sous-représentation de degré 1 et une sous-représentation de degré 2.

Le sous-espace engendré par $(1, 1, 1)$ est invariant par cette action, et correspond à la représentation triviale. De plus, le produit scalaire usuel sur $\mathbb{C}^3$ vérifie :

$$< \sigma \cdot x, \sigma \cdot y > = < x, y > \quad \forall x, y \in \mathbb{C}^3, \ \forall \sigma \in \mathfrak{S}_3$$

Donc l'orthogonal de $\mathrm{Vect}((1, 1, 1))$ est également une sous-représentation de $\mathbb{C}^3$. Il s'agit de l'espace des vecteurs dont la somme des coordonnées est nulle. Fixons une base B de cet espace, par exemple $B = ((1, -1, 0) \ , \ (1, 0, -1))$. On peut alors déterminer χ_3 :

$$\chi_3((1\ 2)) = \mathrm{Tr}\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} = 0 \text{ et } \chi_3((1\ 2\ 3)) = \mathrm{Tr}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = -1$$

La table de caractère de $\mathfrak{S}_3$ est donc la suivante :

$\mathfrak{S}_3$	$\{id\}$	2-cycles	3-cycles
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

2.4 Représentations induites

Définition 15 Soit H un sous-groupe de G et S un système de représentants des classes de G/H. On dit qu'une représentation V de G est induite par une représentation W de H lorsque $V = \bigoplus_{s \in S} s \cdot W$.

On note alors $V = \mathrm{Ind}_H^G(W)$ ou $V = W^G$ lorsqu'il n'y a pas de confusion possible.

Propriété 15 Soient H un sous-groupe de G et (V, ρ^G) une représentation de G induite par une représentation (W, ρ) de H. On note θ le caractère de W et θ^G le caractère de V. Alors pour tout $g \in G$, on a :

$$\theta^G(g) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \theta(x^{-1}gx)$$

Démonstration
Soit $(w_1, ..., w_k)$ une base de W, de telle sorte que $B := (s \cdot w_1, ..., s \cdot w_k,\ s \in S)$ soit une base de V (avec S un système de représentants des classes de G/H).
Pour $g \in G$ et $s \in S$, on ne peut avoir $\rho_g^G(s \cdot w_i) = s \cdot w_i$ que si $s^{-1}gs \in H$. Dans ce cas, il y a exactement $\theta(s^{-1}gs)$ indices i tels que $\rho_g^G(s \cdot w_i) = s \cdot w_i$, donc s contribue à hauteur de $\theta(s^{-1}gs)$ à $\theta^G(g)$. D'où :

$$\theta^G(g) = \sum_{\substack{s \in S \\ s^{-1}gs \in H}} \theta(s^{-1}gs) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \theta(x^{-1}gx)$$

Propriété 16 Soient H un sous-groupe de G et W une représentation de H. Alors il existe une unique représentation V de G induite par W, à isomorphisme près.

Démonstration
• Montrons l'existence de V, en construisant un $\mathbb{C}[G]$-module à partir de W. Soit S un système de représentants des classes de G/H. Posons $V = \bigoplus_{s \in S} W \otimes s$, où $s \otimes W := \{s \otimes w \mid w \in W\}$. On fait agir G sur V en définissant $g \otimes w$ pour tout $g \in G$ comme suit : on écrit $g = sh$ avec $h \in H$ et $s \in S$, et on pose $g \otimes w = s \otimes hw \in V$. Ainsi, pour $w \in W$, $s \in S$ et $g \in G$, on a $g \cdot (s \otimes w) = sg \otimes w$, ce qui confère à V une structure de $\mathbb{C}[G]$-module. De plus, pour chaque représentant $s \in S$, le sous-espace $s \otimes W$ est isomorphe à sW. V est bien une représentation induite par W.

• L'unicité de V à isomorphisme près provient de la propriété 14 : en effet, toutes les représentations induites par W auront le même caractère, donc seront isomorphes. ■

Propriété 17 (Formule de réciprocité de Frobenius)
Soit H un sous-groupe de G, θ un caractère de H et χ un caractère de G. Alors $\langle \theta, \mathrm{Res}_H(\chi) \rangle_H = \langle \theta^G, \chi \rangle_G$.

Remarque 9 En fait, cette formule traduit le fait que l'induction est le foncteur adjoint de la restriction. De manière plus formelle, si on note $\mathrm{Ind}_H^G : \mathrm{Rep}(H) \to \mathrm{Rep}(G)$ le foncteur d'induction et $\mathrm{Res}_H^G : \mathrm{Rep}(G) \to \mathrm{Rep}(H)$ le foncteur de restriction, alors pour tout $\rho \in \mathrm{Rep}(G)$ et tout $\theta \in \mathrm{Rep}(H)$, on a un isomorphisme entre $\mathrm{Hom}_G(\mathrm{Ind}_H^G(\theta), \rho)$ et $\mathrm{Hom}_H(\theta, \mathrm{Res}_H^G(\rho))$.

Démonstration D'après la propriété 14 :

$$\langle \theta^G, \chi \rangle_G = \frac{1}{|G|} \sum_{g \in G} \theta^G(g)\chi(g^{-1}) = \frac{1}{|G||H|} \sum_{g \in G} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \theta(x^{-1}gx)\chi(g^{-1})$$

Pour $g \in G$, on note $\mathrm{Stab}(g)$ le stabilisateur de g et $\mathrm{Orb}(g)$ l'orbite de g pour l'action de conjugaison.

$$\sum_{\substack{x \in G \\ x^{-1}gx \in H}} \theta(x^{-1}gx)\chi(g^{-1}) = \sum_{\substack{h \text{ conjugué à } g \\ h \in H}} \theta(h)\chi(g^{-1})|\,\mathrm{Stab}(g)| = \frac{|G|}{|\,\mathrm{Orb}(g)|} \sum_{\substack{h \text{ conjugué à } g \\ h \in H}} \theta(h)\chi(h^{-1}) \quad (*)$$

On note $(C_i)_{1 \le i \le k}$ les classes de conjugaisons de G. En reportant dans $(*)$ et en utilisant le fait que les classes de conjugaisons partitionnent G :

$$\langle \theta^G, \chi \rangle_G = \frac{1}{|H|} \sum_{i=1}^{k} \sum_{h \in H \cap C_i} \theta(h)\chi(h^{-1}) = \frac{1}{|H|} \sum_{h \in H} \theta(h)\chi(h^{-1}) = \langle \theta, \mathrm{Res}_H(\chi) \rangle_H$$

D'où le résultat. ■

3 Exemple : les caractères de $GL(2, q)$

On illustre ce qui précède avec le groupe général linéaire sur $\mathbb{F}_q$ en dimension 2. Dans toute la partie 3, q désigne une puissance de nombre premier impair et $G := GL(2, q)$.

3.1 Structure de G

Cardinal, centre, groupe dérivé

Pour calculer le cardinal de G, il suffit de remarquer qu'une matrice dans G a toutes ses colonnes indépendantes entre elles. Donc pour construire une telle matrice, on commence par choisir la première colonne, avec pour seule contrainte qu'elle soit non nulle. Il y a $q^n - 1$ possibilités. Ensuite, on choisit la deuxième colonne, qui ne doit pas être multiple de la première : il y a $q^n - q$ possibilités. Et on continue ainsi de suite. Au total :

$$|G| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$$

Le centre de G se compose des matrices d'homothéties, donc de $q-1$ éléments. Le groupe dérivé $D(G)$ est le groupe spécial linéaire : $D(G) = SL(2, q)$.

Classes de conjugaisons

Soit $\alpha \in G$. Si le polynôme caractéristique de α est scindé sur $\mathbb{F}_q$, deux cas se présentent :

- Cas 1 : α possède deux valeurs propres distinctes. Alors α est diagonalisable, et semblable à

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

- Cas 2 : α possède une valeur propre de multiplicité algébrique 2. Alors, selon la multiplicité géométrique de cette valeur propre (1 ou 2), α est semblable à

$$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \text{ ou } \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

Si le polynôme caractéristique de α n'est pas scindé sur $\mathbb{F}_q$, c'est qu'il est irréductible car on est en dimension 2, donc il est de la forme $P_\alpha := X^2 - \mathrm{Tr}(\alpha)X + \det(\alpha)$. Ainsi α est semblable à sa matrice compagnon $\left(\begin{smallmatrix} \mathrm{Tr}(\alpha) & 1 \\ -\det(\alpha) & 0 \end{smallmatrix}\right)$. Tout élément de G dont le polynôme minimal vaut P_α sera donc semblable à α. On a déterminé toutes les classes de conjugaison de G. On calcule le nombre d'éléments dans chaque classe (cela servira dans la suite) en utilisant la formule

$$|\,\mathrm{Orb}(\alpha)| = |G : N(\alpha)|$$

où $N(\alpha)$ désigne le centralisateur de α. Par exemple, pour le premier type de classes de conjugaison, le normalisateur d'une matrice de la forme $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ est le sous-groupe composé des matrices diagonales et des matrices de la forme $\left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$, qui est d'indice $q(q+1)$ dans G. On résume toutes les informations dans le tableau suivant :

Type de classe	$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ avec $\lambda \neq \mu$	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} t & 1 \\ -d & 0 \end{pmatrix}$
Nombre de classes de ce type	$(q-1)(q-2)/2$	$q-1$	$q-1$	$q(q-1)/2$
Nombre d'éléments de chaque classe	$q(q+1)$	1	$(q-1)(q+2)$	$q(q-1)$

FIGURE 1 – Classes de conjugaisons de G

Il y a en tout $(q-1)(q+1)$ classes de conjugaisons différentes, donc autant de caractères irréductibles.

3.2 Caractères de degré 1

Le nombre de caractères de degré 1 est égal à l'indice de $D(G)$ dans G. Or le groupe dérivé de G est le groupe spécial linéaire $SL(2, q)$, donc il y a $q-1$ caractères de degré 1 dans G. Le déterminant fournit un morphisme de G dans $\mathbb{F}_q^*$. En composant avec un morphisme de $\mathbb{F}_q^*$ dans $\mathbb{C}^*$, on obtiendrait un caractère de degré 1. Or il existe $q-1$ morphismes de $\mathbb{F}_q^*$ vers $\mathbb{C}^*$, correspondant aux $q-1$ racines $(q-1)$-ièmes

de l'unité. Ainsi, on a construit $q-1$ caractères de degré 1, qui sont tous distincts. On a trouvé tous les caractères de degré 1, qu'on rassemble dans le tableau ci-dessous, où on a noté ϕ un morphisme de $\mathbb{F}_q^*$ dans $\mathbb{C}^*$.

Type de classe	$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ avec $\lambda \neq \mu$	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} t & 1 \\ -d & 0 \end{pmatrix}$
$\phi \circ \det$	$\phi(\lambda\mu)$	$\phi(\lambda)^2$	$\phi(\lambda)^2$	$\phi(d)$

FIGURE 2 – Caractères de degré 1

Pour trouver les autres caractères de G, on va procéder par induction en étudiant d'abord les caractères de sous-groupes de G.

3.3 Caractères induits par B

On s'intéresse au groupe $B = UD$, où U désigne le sous-groupe des matrices de la forme $\left(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix}\right)$, et où D désigne le sous-groupe des matrices diagonales. Le groupe B est ainsi le sous-groupe des matrices triangulaires supérieures de G. On remarque que $U \cap D = \{\mathrm{id}\}$, et que U est distingué dans B, donc il y a un isomorphisme $B/U \simeq D$. Un caractère irréductible de D pourra être vu comme un caractère irréductible de B/U, et donc de B.

Commençons par prendre un caractère de degré 1 de D, soit ψ. Définissons deux morphismes auxiliaires à partir de ψ :

$$\psi_1 : \begin{array}{ccc} \mathbb{F}_q^* & \longrightarrow & \mathbb{C}^* \\ a & \longmapsto & \psi\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \end{array} \quad \text{et} \quad \psi_2 : \begin{array}{ccc} \mathbb{F}_q^* & \longrightarrow & \mathbb{C}^* \\ d & \longmapsto & \psi\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \end{array}$$

En tant que caractère de B, ψ vérifie $\psi\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = \psi_1(a)\psi_2(d)$.

Cas 1 : $\psi_1 = \psi_2$

Si $\psi_1 = \psi_2$, alors $\psi\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) = \psi_1(ad) = \psi_1\left(\det\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)\right)$ donc ψ est la restriction à B d'un caractère du type $\phi \circ \det$ que l'on avait construit précédemment. D'après la relation de Frobenius, le caractère induit $\psi^G = \mathrm{Ind}_B^G(\psi)$ n'est pas irréductible car il contient $\phi \circ \det$:

$$\langle \psi^G, \phi \circ \det \rangle = \langle\ \psi\ ,\ \mathrm{Res}_B(\phi \circ \det)\ \rangle_B = 1 > 0$$

Ainsi l'application $\chi = \psi^G - \phi \circ \det$ est encore un caractère de G, et on va montrer qu'il est irréductible. On calcule les valeurs de ψ^G grâce à la formule :

$$\psi^G(\alpha) = \frac{1}{|B|} \sum_{\substack{\beta \in G \\ \beta^{-1}\alpha\beta \in B}} \phi(\det(\beta^{-1}\alpha\beta))$$

• Si $\alpha = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$, avec $\lambda \neq \mu$: pour tout $\beta \in G$, $\beta^{-1}\alpha\beta \in B$ ssi $\beta \in B$ ou β est de la forme $\left(\begin{smallmatrix} 0 & b \\ c & d \end{smallmatrix}\right)$, et dans les deux cas, $\phi \circ \det(\beta^{-1}\alpha\beta) = \phi(\lambda\mu)$. Finalement, $\psi^G(\alpha) = 2\phi(\lambda\mu)$.

• Si $\alpha = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$: α est dans le centre de G, donc pour tout $\beta \in G$, $\beta^{-1}\alpha\beta = \alpha \in B$, et donc $\psi^G(\alpha) = (q+1)\phi(\lambda)^2$.

• Si $\alpha = \left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$: pour tout $\beta \in G$, $\beta^{-1}\alpha\beta \in B$ ssi $\beta \in B$, et dans ce cas $\phi \circ \det(\beta^{-1}\alpha\beta) = \phi(\lambda)^2$, donc $\psi^G(\alpha) = \phi(\lambda)^2$.

• Enfin, si $\alpha = \left(\begin{smallmatrix} t & 1 \\ -d & 0 \end{smallmatrix}\right)$: α n'est semblable à aucune matrice triangulaire, donc $\psi^G(\alpha) = 0$.

Type de classe	$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ avec $\lambda \neq \mu$	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} t & 1 \\ -d & 0 \end{pmatrix}$
ψ^G	$2\phi(\lambda\mu)$	$(q+1)\phi(\lambda)^2$	$\phi(\lambda)^2$	0
$\chi = \psi^G - \phi \circ \det$	$\phi(\lambda\mu)$	$q\phi(\lambda)^2$	0	$-\phi(d)$

FIGURE 3 – Caractères induits par B (cas 1)

Vérifions que χ est irréductible, en montrant que $\langle \chi, \chi \rangle = 1$. On utilise le fait que les classes de conjugaisons partitionnent G :

$$\sum_{\beta \in G} |\chi(\beta)|^2 = \sum_{\lambda=1}^{q-1} \sum_{\mu=1}^{\lambda-1} |\phi(\lambda\mu)|^2 (q^2+q) + \sum_{\lambda=1}^{q-1} q^2 |\phi(\lambda)^2|^2 + \frac{q}{2} \sum_{d=1}^{q-1} |\phi(d)|^2 (q^2-q)$$

Or pour tout $\lambda \in \mathbb{F}_q^*$, $|\phi(\lambda)| = 1$, par définition de ϕ. Donc on peut simplifier :

$$|G|\langle \chi, \chi \rangle = \frac{1}{2}(q-1)(q-2)(q^2+q) + (q-1)q^2 + \frac{q}{2}(q^2-q)(q-1) = q(q+1)(q-1)^2 = |G|$$

Ainsi $\langle \chi, \chi \rangle = 1$, et donc χ est irréductible. On a trouvé $q-1$ caractères de G de degré $|G:B| - 1 = q$.

Cas 2 : $\psi_1 \neq \psi_2$

Si $\psi_1 \neq \psi_2$, on va montrer que ψ^G est irréductible, en calculant sa table de valeurs (les calculs sont identiques à ceux menés dans le cas précédent).

Type de classe	$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ avec $\lambda \neq \mu$	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} t & 1 \\ -d & 0 \end{pmatrix}$
ψ^G	$\psi_1(\lambda)\psi_2(\mu) + \psi_1(\mu)\psi_2(\lambda)$	$(q+1)\psi_1(\lambda)\psi_2(\lambda)$	$\psi_1(\lambda)\psi_2(\lambda)$	0

FIGURE 4 – Caractères induits par B (cas 2)

On a, d'après cette table :

$$\begin{aligned} |G|\langle \psi^G, \psi^G \rangle &= \sum_{\beta \in G} |\psi^G(\beta)|^2 \\ &= \sum_{\lambda=1}^{q-1} \sum_{\mu=1}^{\lambda-1} |\psi_1(\lambda)\psi_2(\mu) + \psi_1(\mu)\psi_2(\lambda)|^2 (q^2+q) + \sum_{\lambda=1}^{q-1} |(q+1)\psi_1(\lambda)\psi_2(\lambda)|^2 + \sum_{\lambda=1}^{q-1} |\psi_1(\lambda)\psi_2(\lambda)|^2 (q^2-1) \\ &= (q^2+q)S + (q+1)^2(q-1) + (q-1)(q^2-1) \end{aligned}$$

Calculons à part la somme S.

$$\begin{aligned} S &= \frac{1}{2} \sum_{\lambda=1}^{q-1} \sum_{\substack{\mu=1 \\ \mu \neq \lambda}}^{q-1} |\psi_1(\lambda)\psi_2(\mu) + \psi_1(\mu)\psi_2(\lambda)|^2 \\ &= \frac{1}{2} \sum_{\lambda=1}^{q-1} \sum_{\substack{\mu=1 \\ \mu \neq \lambda}}^{q-1} \big(\psi_1(\lambda)\psi_2(\mu) + \psi_1(\mu)\psi_2(\lambda)\big) \cdot \big(\psi_1(\lambda^{-1})\psi_2(\mu^{-1}) + \psi_1(\mu^{-1})\psi_2(\lambda^{-1})\big) \end{aligned}$$

$$= \frac{1}{2}\sum_{\lambda=1}^{q-1}\sum_{\substack{\mu=1\\ \mu\neq\lambda}}^{q-1}\big(1+1+\psi_1(\mu\lambda^{-1})\psi_2(\lambda\mu^{-1})+\psi_1(\lambda\mu^{-1})\psi_2(\mu\lambda^{-1})\big)$$

$$= (q-1)(q-2)+\frac{1}{2}\sum_{\lambda=1}^{q-1}\sum_{\mu=1}^{q-1}\big(\psi_1(\mu\lambda^{-1})\psi_2(\lambda\mu^{-1})+\psi_1(\lambda\mu^{-1})\psi_2(\mu\lambda^{-1})\big)-\frac{1}{2}\sum_{\lambda=1}^{q-1}(1+1)$$

Reformulons la somme centrale qui reste à calculer, en notant $w = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$:

$$\sum_{\lambda=1}^{q-1}\sum_{\mu=1}^{q-1}\big(\psi_1(\mu\lambda^{-1})\psi_2(\lambda\mu^{-1})+\psi_1(\lambda\mu^{-1})\psi_2(\mu\lambda^{-1})\big)=\sum_{\alpha\in D}\big(\psi(\alpha w\alpha^{-1}w)+\psi(w\alpha w\alpha^{-1})\big)$$

Or comme $\psi_1 \neq \psi_2$, le caractère irréductible (sur D) $\chi : \alpha \mapsto \psi(\alpha w\alpha^{-1}w)$ est non trivial, donc par orthogonalité, $\langle\chi, 1\rangle_D = 0$, ce qui se développe en :

$$\sum_{\alpha\in D}\psi(\alpha w\alpha^{-1}w)=0$$

De même,

$$\sum_{\alpha\in D}\psi(w\alpha w\alpha^{-1})=0$$

Donc la somme centrale était nulle, et $S = (q-1)(q-2)-(q-1) = (q-1)(q-3)$. Finalement,

$$|G|\langle\psi^G,\psi^G\rangle = (q^2+q)(q-1)(q-3)+(q+1)^2(q-1)+(q-1)(q^2-1) = |G|$$

ψ^G est bien irréductible. On a trouvé $(q-1)(q-2)/2$ caractères de G, de degré $|G:B| = q+1$.

3.4 Les derniers caractères

On s'intéresse à présent au sous-groupe $H = ZU$, où $Z = Z(G)$. Comme $Z \cap U = \{\mathrm{id}\}$, le cardinal de H vaut $|Z|\times|U| = (q-1)q$. Soient ϕ et ψ deux morphismes de groupes entre $\mathbb{F}_q^*$ et $\mathbb{C}^*$. On prend comme convention $\psi(0) = 1$ de manière à étendre ψ à $\mathbb{F}_q$. On peut construire est un caractère de H de degré 1 :

$$\begin{array}{rccc}(\phi,\psi): & H & \longrightarrow & \mathbb{C}^*\\ & \left(\begin{smallmatrix}a&ac\\0&a\end{smallmatrix}\right) & \longmapsto & \phi(a)\psi(c)\end{array}$$

On dresse la table de valeurs du caractère induit $(\phi,\psi)^G$, toujours grâce à la formule

$$(\phi,\psi)^G(\alpha)=\frac{1}{|H|}\sum_{\substack{\beta\in G\\ \beta^{-1}\alpha\beta\in H}}(\phi,\psi)(\beta^{-1}\alpha\beta)$$

• Si $\alpha = \left(\begin{smallmatrix}\lambda&0\\0&\mu\end{smallmatrix}\right)$, avec $\lambda\neq\mu$, alors α n'est semblable à aucune matrice de H car contrairement à celles-ci, α possède deux valeurs propres distinctes. Donc $(\phi,\psi)^G(\alpha) = 0$.

• Si $\alpha = \left(\begin{smallmatrix}\lambda&0\\0&\lambda\end{smallmatrix}\right)$: α commute avec tous les éléments de G, donc $(\phi,\psi)^G = (q^2-1)\phi(\lambda)$.

• Si $\alpha = \left(\begin{smallmatrix}\lambda&1\\0&\lambda\end{smallmatrix}\right)$: pour tout $\beta\in G$, $\beta^{-1}\alpha\beta\in H$ ssi $\beta\in H$, et dans ce cas $(\phi,\psi)(\beta^{-1}\alpha\beta) = \phi(\lambda)$ donc $(\phi,\psi)^G(\alpha) = \phi(\lambda)$.

• Enfin, si $\alpha = \left(\begin{smallmatrix}t&1\\-d&0\end{smallmatrix}\right)$, alors α n'est semblable à aucune matrice de H, donc $(\phi,\psi)^G(\alpha) = 0$.

Type de classe	$\begin{pmatrix}\lambda&0\\0&\mu\end{pmatrix}$ avec $\lambda\neq\mu$	$\begin{pmatrix}\lambda&0\\0&\lambda\end{pmatrix}$	$\begin{pmatrix}\lambda&1\\0&\lambda\end{pmatrix}$	$\begin{pmatrix}t&1\\-d&0\end{pmatrix}$
$(\phi,\psi)^G$	0	$(q^2-1)\phi(\lambda)$	$\phi(\lambda)$	0

FIGURE 5 – Caractères induits par H

Cette table permet de déduire que le caractère $(\phi,\psi)^G$ n'est pas irréductible. On va chercher à lui retrancher un autre caractère pour obtenir un caractère irréductible. Pour cela, considérons le sous-groupe

$$C = \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} \mid a^2 - b^2\epsilon \neq 0 \right\}$$

où ϵ désigne un élément fixé de $\mathbb{F}_q^*$ qui n'est pas un carré. Un tel sous-groupe est appelé un sous-groupe non décomposé de Cartan.

Soit $\theta : C \to \mathbb{C}^*$ un caractère de degré 1 de C. Calculons la table de valeurs du caractère induit θ^G, de la même façon que d'habitude :

$$\theta^G(\alpha) = \frac{1}{|C|} \sum_{\substack{\beta\in G \\ \beta^{-1}\alpha\beta\in C}} \theta(\beta^{-1}\alpha\beta)$$

• Si $\alpha = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$, avec $\mu \neq \lambda$: pour $\beta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, on a

$$\beta^{-1}\alpha\beta = \frac{1}{\det(\alpha)} \begin{pmatrix} \lambda ad - \mu bc & bd(\lambda-\mu) \\ ac(\mu-\lambda) & ad\mu - bc\lambda \end{pmatrix}$$

Si $\beta^{-1}\alpha\beta \in C$, alors $ad\lambda - bc\mu = ad\mu - bc\lambda$ donc $ad = -bc$ et $\det(\alpha) = 2ad = -2bc$ donc a, b, c, d sont non nuls. D'autre part, on doit avoir :

$$\epsilon = \frac{bd(\lambda-\mu)}{ac(\mu-\lambda)} = \left(\frac{b}{a}\right)^2$$

ce qui est absurde car ϵ n'est pas un carré. α n'est semblable à aucune matrice dans C, donc $\theta^G(\alpha) = 0$.

• Si $\alpha = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$, on a $\theta^G(\alpha) = (q^2 - q)$

• Si $\alpha = \left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$: comme pour le premier cas, on montre que α n'est semblable à aucune matrice de C, donc que $\theta^G(\alpha) = 0$.

• Si $\alpha = \left(\begin{smallmatrix} t & 1 \\ -d & 0 \end{smallmatrix}\right)$: on procède à une étude plus complète des classes de conjugaison du dernier type.
Remarquons d'abord que pour un élément de C, soit $\left(\begin{smallmatrix} a & b\epsilon \\ b & a \end{smallmatrix}\right)$, qui n'est pas scalaire, son polynôme caractéristique est irréductible sur $\mathbb{F}_q$, donc il est semblable à $\left(\begin{smallmatrix} 2a & 1 \\ b^2\epsilon - a^2 & 0 \end{smallmatrix}\right)$. Ainsi les classes de conjugaison des éléments de C non scalaires sont parmi les classes de représentants du type $\left(\begin{smallmatrix} t & 1 \\ -d & 0 \end{smallmatrix}\right)$.
De plus, deux éléments non scalaires de C $\left(\begin{smallmatrix} a & b\epsilon \\ b & a \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} a' & b'\epsilon \\ b' & a' \end{smallmatrix}\right)$ sont conjugués si et seulement si $a = a'$ et $b = \pm b'$. Il y a donc $q(q-1)/2$ classes de conjugaisons qui sont représentées dans $C - Z$. Or il y a exactement $q(q-1)/2$ classes dont un représentant est de la forme $\left(\begin{smallmatrix} t & 1 \\ -d & 0 \end{smallmatrix}\right)$. Ainsi, pour représenter la classe d'un élément de la forme $\left(\begin{smallmatrix} t & 1 \\ -d & 0 \end{smallmatrix}\right)$ on peut prendre un élément de C.
On est à présent en mesure de calculer $\theta^G(\alpha)$. En effet, d'après la discussion précédente, il existe $\alpha' \in C - Z$ semblable à α. Et pour tout $\beta \in G$, on a $\beta^{-1}\alpha'\beta \in C$ ssi $\beta \in C$ ou $w\beta \in C$, et dans le premier cas, $\theta(\beta^{-1}\alpha'\beta) = \theta(\alpha')$ tandis que dans le deuxième cas, $\theta(\beta^{-1}\alpha'\beta) = \theta(w\alpha'w)$. Au total, $\theta^G(\alpha) = \theta^G(\alpha') = \theta(\alpha') + \theta(w\alpha'w)$.

Type de classe	$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ avec $\lambda \neq \mu$	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\alpha = \begin{pmatrix} t & 1 \\ -d & 0 \end{pmatrix}$
θ^G	0	$(q^2-q)\theta(\lambda)$	0	$\theta(\alpha') + \theta(w\alpha'w)$

FIGURE 6 – Caractère induit par C

Utilisons la formule de Frobenius pour montrer que θ^G est contenu dans le caractère $(\mathrm{Res}_Z(\theta),\psi)^G$:

$$\langle \theta^G, (\mathrm{Res}_Z(\theta),\psi)^G\rangle_G = \langle \mathrm{Res}_{ZU}(\theta^G), (\mathrm{Res}_Z(\theta),\psi)\rangle_{ZU} = \frac{1}{|ZU|} \sum_{\alpha\in ZU} \theta^G(\alpha)(\mathrm{Res}_Z(\theta),\psi)(\alpha)$$

Or pour $\alpha = \left(\begin{smallmatrix} a & ac \\ 0 & a \end{smallmatrix}\right)$, on a vu dans la table que $\theta^G(\alpha) \neq 0$ si et seulement si $c = 0$, donc l'expression précédente peut se simplifier :

$$\langle \theta^G, (\mathrm{Res}_Z(\theta), \psi)^G \rangle_G = \frac{1}{|ZU|} \sum_{a=1}^{q-1} (q^2 - q) \theta\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \overline{\theta(a)} = \frac{1}{|ZU|} \sum_{a=1}^{q-1} (q^2 - q) = q - 1 \neq 0$$

Ainsi l'application $\theta' = (\mathrm{Res}_Z(\theta), \psi)^G - \theta^G$ est encore un caractère.

Type de classe	$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ avec $\lambda \neq \mu$	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\alpha = \begin{pmatrix} t & 1 \\ -d & 0 \end{pmatrix}$
θ'	0	$(q-1)\theta(\lambda)$	$\theta(\lambda)$	$-\theta(\alpha') - \theta(w\alpha' w)$

FIGURE 7 – Derniers caractères irréductibles

Montrons que θ' est irréductible :

$$\begin{aligned}
\sum_{\beta \in G} |\theta'(\beta)|^2 &= \sum_{\lambda=1}^{q-1} |(q-1)\theta(\lambda)|^2 + \sum_{\lambda=1}^{q-1} |\theta(\lambda)|^2 (q^2-1) + \frac{q^2-q}{2} \sum_{\alpha \in C-Z} |\theta(\alpha) + \theta(w\alpha w)|^2 \\
&= (q-1)^3 + (q^2-1)(q-1) + \frac{q^2-q}{2} \sum_{\alpha \in C-Z} (1 + 1 + \theta(\alpha w \alpha^{-1} w) + \theta(w \alpha w \alpha^{-1})) \\
&= (q-1)^3 + (q^2-1)(q-1) + (q^2-q)(q^2-q) \\
&+ \frac{q^2-q}{2} \sum_{\alpha \in C} (\theta(\alpha w \alpha^{-1} w) + \theta(w \alpha w \alpha^{-1})) - \frac{q^2-q}{2} \sum_{\alpha \in Z} (1+1) \\
&= 2q(q-1)^2 + q^2(q-1)^2 - (q^2-q)(q-1) \text{ par relation d'orthogonalité} \\
&= 2q(q+1)(q-1)^2 = |G|
\end{aligned}$$

Ainsi θ' est irréductible, et on a trouvé $(q-1)q/2$ caractères de degré $q-1$.

Au total, on a exhibé $q-1$ caractères de degré 1, $q-1$ caractères de degré q, $(q-1)(q-2)/2$ caractères de degré $q+1$ et $(q-1)q/2$ caractères de degré $q-1$: en tout, on a $(q-1)(q+1)$ caractères irréductibles distincts, ce qui correspond au nombre de classes de conjugaison de G. On a donc tous les caractères irréductibles de G, et on est en mesure de dresser sa table de caractères :

Type de classe	$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ avec $\lambda \neq \mu$	$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$	$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$	$\alpha = \begin{pmatrix} t & 1 \\ -d & 0 \end{pmatrix}$
$\phi \circ \det$	$\phi(\lambda\mu)$	$\phi(\lambda)^2$	$\phi(\lambda)^2$	$\phi(d)$
$\psi^G - \phi \circ \det$	$\phi(\lambda\mu)$	$q\phi(\lambda)^2$	0	$-\phi(d)$
ψ^G	$\psi_1(\lambda)\psi_2(\mu) + \psi_1(\mu)\psi_2(\lambda)$	$(q+1)\psi_1(\lambda)\psi_2(\lambda)$	$\psi_1(\lambda)\psi_2(\lambda)$	0
θ'	0	$(q-1)\theta(\lambda)$	$\theta(\lambda)$	$-\theta(\alpha') - \theta(w\alpha' w)$

FIGURE 8 – Table de caractères de G

4 Groupes résolubles

On va à présent utiliser la théorie des représentations pour l'étude des groupes résolubles, et notamment de démontrer le théorème de Burnside.

4.1 Le théorème de Burnside

Définition 16 Suite normale
Soit G un groupe, et $G = G_0 \supset G_1 \supset ... \supset G_s$ une suite de sous-groupes emboîtés. On dit que cette suite est normale lorsque que pour tout $i \in [\![0, s-1]\!]$, G_{i+1} est distingué dans G_i.
On appelle facteurs de la suite les groupes quotients G_i/G_{i+1}.

Définition 17 Suite dérivée
Soit G un groupe. On définit sa suite dérivée $(D^n(G))_{n\geqslant 0}$ par récurrence :

$$\begin{cases} D^0(G) = G \\ D^{n+1}(G) = D(D^n(G)) \end{cases}$$

Où $D(H)$ désigne le groupe dérivé d'un groupe H.

Remarque 10 La suite dérivée d'un groupe est normale.

Définition 18 Soit G un groupe. On dit que G est résoluble lorsque sa suite dérivée est stationnaire, égale à $\{1\}$ à partir d'un certain rang.
La classe de résolubilité de G est alors l'indice minimum pour lequel $D^n(G) = \{1\}$.

Remarque 11 De façon équivalente, un groupe est résoluble lorsqu'il possède une suite normale dont les facteurs sont abéliens et qui atteint $\{1\}$ à partir d'un certain rang.

Propriété 18 Soit G un groupe, N un sous-groupe distingué de G. Si N et G/N sont résolubles, de classe p et q respectivement, alors G l'est aussi, de classe inférieure à $p+q$.

Démonstration
Soit π le morphisme quotient de G dans G/N. On a : $\pi(D^q(G)) = D^q(\pi(G)) = D^q(G/N) = \{1\}$. Donc $D^q(G)$ est un sous groupe de N. Or N est résoluble, donc $D^q(G)$ l'est aussi, de classe inférieure à la classe de N (soit p). Ainsi $D^p(D^q(G)) = \{1_G\}$. Mais $D^p(D^q(G)) = D^{p+q}(G)$, d'où le résultat. ■

4.1.1 Deux lemmes

Notation 3 Pour G un groupe fini et $\chi \in \mathrm{Irr}(G)$, on pose $Z(\chi) = \{g \in G \mid |\chi(g)| = \chi(1)\}$, et $\mathrm{Ker}(\chi) = \{g \in G \mid \chi(g) = \chi(1)\}$.

Propriété 19 Soient G un groupe fini et $\chi \in \mathrm{Irr}(G)$. Alors $Z(\chi)$ et $\mathrm{Ker}(\chi)$ sont des sous-groupes de G et $Z(\chi)/\mathrm{Ker}(\chi) = Z(G/\mathrm{Ker}(\chi))$.

Démonstration
Soit ρ une représentation de G de caractère χ. Alors $\mathrm{Ker}(\chi) = \mathrm{Ker}(\rho)$ et $Z(\chi) = \{g \in G \mid \rho(g) = \epsilon\,\mathrm{id} \text{ pour } \epsilon \in \mathbb{C}\}$ donc $\mathrm{Ker}(\chi)$ et $Z(\chi)$ sont des sous-groupes de G.
De plus, par propriété universelle du quotient, $Z(\chi)/\mathrm{Ker}(\chi) \simeq \rho(Z(\chi)) \subset Z(\rho(G)) \simeq Z(G/\mathrm{Ker}(\chi))$ donc $Z(\chi)/\mathrm{Ker}(\chi) \subset Z(G/\mathrm{Ker}(\chi))$.
Enfin, comme χ est irréductible, tout élément de $\rho(G)$ qui commute avec tous les $\rho(h)$, $h \in G$, est une homothétie. Donc si $\bar{g} \in Z(G/\mathrm{Ker}(\chi))$, alors $\rho(g)$ est une homothétie, donc $|\chi(g)| = \chi(1)$ et $\bar{g} \in Z(\chi)/\mathrm{Ker}(\chi)$. ■

Lemme 3 Soit G un groupe fini. Soient χ un caractère irréductible de G et C une classe de conjugaison. On suppose que $\mathrm{pgcd}(\chi(1), |C|) = 1$.
Alors pour tout $g \in C$, on a $g \in Z(\chi)$ ou $\chi(g) = 0$.

Démonstration
On écrit la relation de Bézout entre $\chi(1)$ et $|C|$: il existe u et v, deux entiers, tels que $u\chi(1) + v|C| = 1$. On reformule cette égalité en :

$$\frac{\chi(g)}{\chi(1)} = u\chi(g) + v\frac{|C|\chi(g)}{\chi(1)}$$

Or (voir l'annexe sur les entiers algébriques) $\dfrac{|C|\chi(g)}{\chi(1)}$ et $u\chi(g)$ sont des entiers algébriques, donc $\alpha := \dfrac{\chi(g)}{\chi(1)}$ en est aussi un. Supposons que $|\alpha| < 1$.
On note n l'ordre de g dans G, et on introduit E, le corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$, de telle sorte que $\alpha \in E$ (car $\chi(g)$ est une somme de racines de $X^n - 1$). Soit $\mathcal{G}$ le groupe de Galois de E sur $\mathbb{Q}$. Tout morphisme $\sigma \in \mathcal{G}$ envoie une racine nième de l'unité sur une racine nième de l'unité, donc pour tout $\sigma \in \mathcal{G}$, $|\sigma(\alpha)| \leqslant 1$. D'où :

$$\left|\beta := \prod_{\sigma\in\mathcal{G}} \sigma(\alpha)\right| < 1$$

Or β est laissé fixe par tous les morphismes de $\mathcal{G}$, et l'extension $E/\mathbb{Q}$ est galoisienne (car $X^n - 1$ est un polynôme irréductible sur $\mathbb{Q}$, à racines simples dans $\mathbb{C}$), donc $\beta \in \mathbb{Q}$ (voir l'annexe sur les extensions de Galois).
β est un entier algébrique rationnel, c'est-à-dire un entier. Et $|\beta| < 1$ donc $\beta = 0$. Par suite, il existe $\sigma \in \mathcal{G}$ tel que $\sigma(\alpha) = 0$, c'est-à-dire que $\alpha = 0$, puis $\chi(g) = 0$. ■

Lemme 4 Soit G un groupe simple non abélien. Alors la seule classe de conjugaison de cardinal une puissance d'un nombre premier est $\{1\}$.

Démonstration
Procédons par l'absurde, en supposant qu'il existe $g \in G$, $g \neq 1$, dont le cardinal de la classe de conjugaison est la puissance d'un nombre premier p : $|Cl(g)| = p^a$.
La seconde relation d'orthogonalité s'écrit dans G :

$$\sum_{\chi\in\mathrm{Irr}(G)} \chi(1)\chi(g) = 0 \quad (*)$$

Soit $\chi \in \mathrm{Irr}(G)$, non trivial. Si p ne divise pas $\chi(1)$, le lemme 3 montre que $g \in Z(\chi)$ ou $\chi(g) = 0$. Or G est simple et non abélien, donc $\mathrm{Ker}(\chi) = \{1\}$ (χ est non trivial), puis $Z(\chi) = Z(G) = \{1\}$ (d'après la propriété 18). Ainsi $\chi(g) = 0$, et on peut simplifier la relation $(*)$:

$$\sum_{\chi\in\mathrm{Irr}(G),\ p|\chi(1)} \chi(1)\chi(g) + 1 = 0$$

Comme $\chi(g)$ est un entier algébrique, on déduit de cette égalité que $-\dfrac{1}{p}$ est un entier algébrique, ce qui est absurde. ■

4.1.2 Preuve du théorème

Théorème 5 (Burnside)
Soit G un groupe de cardinal $p^a q^b$, avec p, q des nombres premiers et a, b des entiers naturels. Alors G est résoluble.

Démonstration
On raisonne par récurrence sur l'ordre de $|G|$. Si $G = \{1\}$, G est évidemment résoluble.
Supposons que $|G| = p^a q^b$, avec p, q des nombres premiers et a, b des entiers naturels, dont l'un au moins est non nul, et que tout groupe d'ordre $p^c q^d$, avec $p^c q^d < p^a q^b$, est résoluble. Soit N un sous-groupe propre maximal distingué de G.

• si $N = \{1\}$, alors G est simple. Soit P un Sylow de G non trivial, et $g \in Z(P)$, $g \neq 1$. Un tel g existe car le centre d'un p-groupe n'est jamais réduit à $\{1\}$.
Comme g commute avec tous les éléments de P, le cardinal de la classe de g dans G divise $|G : P|$, donc c'est une puissance de q. Or G est simple, donc le lemme 4 impose que G soit abélien. G est bien résoluble.

• si $N \neq \{1\}$, alors on peut appliquer l'hypothèse de récurrence à N et G/N, qui sont donc résolubles. Par la propriété 14, G est résoluble. ■

Exemple 2 Grâce au résultat de Burnside, on peut facilement montrer que le plus petit groupe non résoluble est $\mathcal{A}_5$. En effet, un groupe non résoluble d'ordre inférieur à 60 doit contenir au moins trois facteurs premiers, ce qui limite les candidats à $30 = 2 \times 3 \times 5$, $42 = 2 \times 3 \times 7$ et $60 = 2^2 \times 3 \times 5$. Or un groupe G d'ordre 30 ou 42 n'est pas simple (conséquence des théorèmes de Sylow), donc possède un sous-groupe propre N distingué, et dont l'ordre est un produit d'au plus deux nombres premiers. D'après le théorème de Burnside, N et G/N sont résolubles, donc G l'est aussi. En revanche, $\mathcal{A}_5$ est un groupe d'ordre 60 qui est simple et non commutatif, donc non résoluble.
C'est à cause de la non résolubilité de $\mathcal{A}_5$ que les équations polynomiales de degré supérieur à 5 ne sont pas résolubles par radicaux.

4.2 Un autre critère de résolubilité

Dans cette sous-partie, on explore un autre critère de résolubilité qui donne un lien direct entre les caractères d'un groupe et sa résolubilité.

4.2.1 Quelques compléments sur les représentations induites

Propriété 20 Soit H un sous-groupe de G et θ un caractère de H. Alors :

$$\mathrm{Ker}(\theta^G) = \bigcap_{x \in G} \mathrm{Ker}(\theta)^x$$

où on a noté $\mathrm{Ker}(\theta)^x := \{g \in G \mid xgx^{-1} \in H,\ \theta(xgx^{-1}) = \theta(1)\}$

Démonstration
Pour tout $g \in G$, $\theta^G(g) = \sum_{\substack{x \in G \\ xgx^{-1} \in H}} \theta(xgx^{-1})$.
Et $|\theta(xgx^{-1})| \leqslant \theta(1)$, donc $\theta^G(g) = \theta^G(1)$ si et seulement si pour tout $x \in G$ tel que $xgx^{-1} \in H$, on a $\theta(xgx^{-1}) = \theta(1)$, c'est-à-dire si et seulement si $g \in \bigcap_{x \in G} \mathrm{Ker}(\theta)^x$. ■

Définition 19 Soit G un groupe. Une représentation V de G est dite isotypique lorsqu'elle est la somme directe de représentations irréductibles isomorphes : $V \simeq \bigoplus W$.

Propriété 21 Soient A un sous-groupe distingué de G et $\rho : G \to GL(V)$ une représentation irréductible de G. Alors :

- Ou il existe un sous-groupe propre H de G contenant A, et une représentation irréductible σ de H qui induit ρ ;
- Ou bien la restriction de ρ à A est isotypique.

Démonstration
Considérons la décomposition canonique de la restriction de ρ à A (partant d'une décomposition en sous-représentations irréductibles, on regroupe toutes les sous-représentations isomorphes ; on peut montrer que cette décomposition est unique à l'ordre près des facteurs) : $V = \bigoplus_{i=1}^{r} V_i$, où chaque V_i est une représentation isotypique de A. Si $r = 1$, alors on est dans le deuxième cas de la propriété.
Sinon, on remarque que G agit sur cette décomposition en permutant les V_i, et cette action est transitive car V est irréductible. Soit V_{i_0} l'un des V_i. On note H le sous-groupe de G composé des éléments s qui laissent stable V_{i_0} : $\rho_s(V_{i_0}) = V_{i_0}$. Alors H contient A, $H \neq G$ et

$$V = \bigoplus_{t \in G/H} \rho_t(V_{i_0})$$

ce qui signifie que la représentation $\sigma : H \to GL(V_{i_0})$ induit ρ sur G. ■

4.2.2 Théorème de Taketa

Définition 20 Soit G un groupe fini. On dit que G est monomial lorsque chacun de ses caractères est induit par un caractère linéaire sur un sous-groupe de G.

Lemme 5 Soit G un groupe monomial, et $1 = n_1 < n_2 < ... < n_k$ les degrés de ses caractères irréductibles. Alors pour tout $i \in [\![1, k]\!]$, pour tout $\chi \in \mathrm{Irr}(G)$ tel que $\chi(1) = n_i$, on a $D^i(G) \subset \mathrm{Ker}(\chi)$.

Démonstration
On procède par récurrence finie sur i, en montrant la propriété $\mathcal{P}(i)$: "Le noyau de tout caractère irréductible de degré n_i contient $D^i(G)$".
• Pour $i = 1$, le résultat est immédiat car $D(G) = \bigcap_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1)=1}} \mathrm{Ker}(\chi)$.

• Soit $i \in [\![2, k]\!]$, tel que pour tout $j < i$, on ait $\mathcal{P}(j)$. Soit $\chi \in \mathrm{Irr}(G)$, de degré n_i. Comme G est monomial, il existe un sous-groupe H de G et un caractère linéaire $\lambda \in \mathrm{Irr}(H)$ tels que $\lambda^G = \chi$.
Par formule de réciprocité de Frobenius, $\langle 1_H^G, 1\rangle_G = \langle 1_H, 1_H\rangle_H = 1$ donc le caractère induit par 1_H sur G n'est pas irréductible. Considérons ψ, l'un des caractères irréductibles qui le composent. On a :

$$\psi(1) < 1_H^G(1) = |G : H| = \lambda^G(1) = \chi(1)$$

On peut appliquer l'hypothèse de récurrence à ψ, de degré n_j pour $j < i$: $D^j(G) \subset \mathrm{Ker}(\psi)$. Par suite, $D^{i-1}(G) \subset \mathrm{Ker}(\psi)$. Ceci étant valable pour n'importe quel caractère irréductible composant 1_H^G, on a finalement que $D^{i-1}(G) \subset \mathrm{Ker}(1_H^G) = H$ par la propriété 19. Par croissance de la dérivation d'un groupe, $D^i(G) \subset D(H)$, puis $D^i(G) \subset \mathrm{Ker}(\lambda)$. Or $D^i(G)$ est distingué dans G, donc on a aussi $D^i(G) \subset \mathrm{Ker}(\lambda)^x$ pour tout $x \in G$. On en conclut que $D^i(G) \subset \bigcap_{x\in G} \mathrm{Ker}(\lambda)^x = \mathrm{Ker}(\chi)$. ■

Théorème 6 (Taketa)
Tout groupe monomial est résoluble.

Démonstration
D'après le lemme 5 (et avec les mêmes notations), on a $D^k(G) \subset \mathrm{Ker}(\chi)$ pour tout caractère $\chi \in \mathrm{Irr}(G)$, donc $D^k(G) \subset \bigcap_{\chi\in\mathrm{Irr}(G)} \mathrm{Ker}(\chi) = \{1\}$. G est bien résoluble. ■

4.2.3 Une réciproque ?

Un groupe résoluble n'est pas forcément monomial, comme le montre la propriété suivante :

Propriété 22 Le groupe spécial $SL(2, 3)$ est résoluble, mais pas monomial.

Lemme 6 Il y a 7 classes de conjugaison dans $SL(2, 3)$.

Démonstration (du lemme)
On adopte la stratégie brutale qui consiste à calculer à la main les classes de conjugaison :
- Élément neutre : $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$
- Élément d'ordre 2 : $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$
- Éléments d'ordre 3 (a) : $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$
- Éléments d'ordre 3 (b) : $\left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$
- Éléments d'ordre 4 : $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 1 & -1 \\ -1 & -1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} -1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} -1 & -1 \\ -1 & 1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$
- Éléments d'ordre 6 (a) : $\left(\begin{smallmatrix} -1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} -1 & 0 \\ -1 & -1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$
- Éléments d'ordre 6 (b) : $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} -1 & 0 \\ 1 & -1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} -1 & -1 \\ 0 & -1 \end{smallmatrix}\right)$; $\left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ ■

Lemme 7 $SL(2, 3)$ ne contient pas de sous-groupe d'ordre 12.

Démonstration (du lemme)
On procède par l'absurde. Soit H un tel groupe. Comme $12 = 2^2 \times 3$, H contient un ou quatre 3-Sylow et un ou trois 2-Sylow. Et $-\mathrm{id} := \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ appartient à H en tant que générateur d'un sous-groupe d'ordre 2.

• Si H ne contient qu'un seul 3-Sylow, alors H doit contenir huit éléments d'ordre 4 ou 6. Notons m l'un des deux éléments d'ordre 3 appartenant à H (l'autre est m^2). Comme $-\mathrm{id}$ et m commutent et que leurs ordres sont premiers entre eux, $-m$ et $-m^2$ sont d'ordre 6. S'il y a dans H un autre élément d'ordre 6, mettons a, alors a^2 est un élément de H d'ordre 3, donc $a^2 = m$ (ou m^2, mais cela revient au même), et donc $a = -m^2$. Ainsi $-m$ et $-m^2$ sont les seuls éléments d'ordre 6 de H.
Il reste donc à compléter H par les six éléments d'ordre 4 de $SL(2, 3)$. Cependant, les éléments d'ordre 4 et m engendrent $SL(2, 3)$, donc $H = SL(2, 3)$, ce qui est absurde.

• Si H contient quatre 3-Sylow, il contient tous les éléments d'ordre 3 de $SL(2, 3)$, et en les multipliant par $-\mathrm{id}$, il contient également tous les éléments d'ordre 6 de $SL(2, 3)$. Il y a donc au moins 18 éléments dans H, ce qui est absurde. ■

Démonstration (de la propriété)
• Résolubilité : $SL(2,3)$ est d'ordre $24 = 2^3 \times 3$, donc il est résoluble par le théorème de Burnside.

• D'après le lemme, il y a 7 classes de conjugaison dans $SL(2,3)$, donc 7 caractères irréductibles. D'autre part, le groupe dérivé de $SL(2,3)$ est isomorphe à $\mathbb{Q}_8$, donc le quotient $SL(2,3)/D(SL(2,3))$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, ce qui fournit trois caractères irréductibles de degré 1 : χ_1, χ_2 et χ_3. De plus, on doit avoir

$$24 = 1 + 1 + 1 + \chi_4(1)^2 + \chi_5(1)^2 + \chi_6(1)^2 + \chi_7(1)^2$$

En étudiant les différentes possibilités, on conclut qu'il y a nécessairement un caractère de degré 2 parmi les χ_i. Notons χ ce caractère de degré 2 et ρ une représentation de caractère χ. Si ρ était induite par une représentation de degré 1 sur un sous-groupe H de $SL(2,3)$, on devrait avoir $\chi(1) = |SL(2,3) : H|$, donc $|H| = 12$. Or il n'y a pas de sous-groupe d'ordre 12 dans $SL(2,3)$. Ainsi $SL(2,3)$ n'est pas monomial. ■

Cependant, en renforçant un peu l'hypothèse de résolubilité, on obtient une condition suffisante pour qu'un groupe soit monomial.

Définition 21 Groupe super-résoluble
Un groupe G est qualifié de super-résoluble lorsqu'il existe une suite normale $G = G_0 \supset G_1 \supset ... \supset G_k = \{1\}$, telle que :
- $\forall i \in [\![1,k]\!]$, $G_i \triangleleft G$
- $\forall i \in [\![1,k]\!]$, G_{i-1}/G_i est cyclique

Remarque 12 La super-résolubilité entraîne la résolubilité.

Théorème 7 Tout groupe super-résoluble est monomial.

Lemme 8 Soit G un groupe non abélien super-résoluble. Alors il existe un sous-groupe distingué de G, abélien, non contenu dans le centre de G.

Démonstration (du lemme)
Le quotient $G/Z(G)$ est encore super-résoluble et il est non trivial car G est non abélien. Donc le dernier terme non trivial H_k d'une suite normale de $G/Z(G)$ est un sous-groupe cyclique distingué de $G/Z(G)$. L'image réciproque de H_k par le morphisme quotient canonique est donc un sous-groupe distingué de G, abélien, non contenu dans $Z(G)$. ■

Démonstration (du théorème)
On procède par récurrence sur l'ordre du groupe G, ce qui permet de ne considérer que les représentations irréductibles dont le noyau est trivial (en effet, il suffit de se ramener à $G/\operatorname{Ker}(\chi)$).
• Si $|G| = 1$, le résultat est immédiat.

• Soit G un groupe d'ordre $n > 1$ tel que tout groupe super-résoluble d'ordre strictement inférieur à n soit monomial. Si G est abélien, alors tous les caractères irréductibles de G sont de degré 1, et il n'y a rien à prouver. Supposons donc que G ne soit pas abélien.
Soit ρ une représentation irréductible de G, dont le noyau est trivial. Grâce au lemme 8, considérons A, un sous-groupe distingué de G, abélien, non contenu dans le centre de G. Comme A n'est pas inclus dans $Z(G)$, il existe $a \in A$ et $g \in G$ tels que $ag \neq ga$, c'est-à-dire, comme $\operatorname{Ker}(\rho) = \{1\}$, $\rho(ag) \neq \rho(ga)$, donc $\rho(A)$ n'est pas inclus dans le centre de $\rho(G)$. Il existe alors $a' \in A$ tel que $\rho(a')$ ne soit pas une homothétie. La restriction de ρ à A n'est donc pas isotypique, et d'après la propriété 20, il existe un sous-groupe propre H de G, contenant A, et une représentation irréductible σ de H qui induit ρ. Par hypothèse de récurrence, σ est induite par une représentation de degré 1, et par transitivité, ρ également. ■

5 Annexes

5.1 Compléments sur le langage des catégories

Définition 22 Une catégorie $\mathcal{C}$ contient une collection d'objets $\operatorname{Ob}(\mathcal{C})$ et une collection de morphismes $\operatorname{Hom}_{\mathcal{C}}$ entre ses objets. Les morphismes se composent de manière associative, et il existe pour chaque objet un morphisme particulier, l'identité.

Remarque 13 Une fois qu'on a défini ce qu'est un morphisme, la notion d'isomorphisme en découle : en effet, un morphisme $f : A \to B$ est un isomorphisme lorsqu'il existe un morphisme $g : B \to A$ vérifiant : $f \circ g = \mathrm{id}_B$ et $g \circ f = \mathrm{id}_A$.

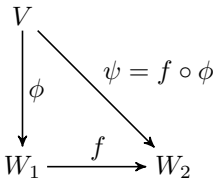
Définition 23 Un foncteur covariant $F : \mathcal{C} \longrightarrow \mathcal{D}$ relie deux catégories $\mathcal{C}$ et $\mathcal{D}$ de telle sorte que pour tous objets $c, c', c'' \in \mathrm{Ob}(\mathcal{C})$, pour tous morphismes $f \in \mathrm{Hom}_{\mathcal{C}}(c, c')$, $g \in \mathrm{Hom}_{\mathcal{C}}(c', c'')$, on ait :

- $F(c) = F_c \in \mathrm{Ob}(\mathcal{D})$
- $F(f) = F_f \in \mathrm{Hom}_{\mathcal{D}}(F_c, F_{c'})$
- $F_{g \circ f} = F_g \circ F_f$
- $F_{\mathrm{id}_c} = \mathrm{id}_{F_c}$

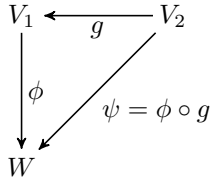
Un foncteur contravariant de $\mathcal{C}$ vers $\mathcal{D}$ est un foncteur covariant de la catégorie opposée $\mathcal{C}^{op}$ dans $\mathcal{D}$.

Exemple 3 Quelques foncteurs classiques
On note Vect la catégorie des $\mathbb{K}-$espaces vectoriels de dimension finie, où $\mathbb{K}$ est un corps arbitraire.

- $\mathrm{Hom}(V, -) : \mathrm{Vect} \longrightarrow \mathrm{Vect}$, qui à tout espace vectoriel W associe $\mathrm{Hom}(V, W)$, et à tout morphisme $f : W_1 \to W_2$ associe le morphisme $\mathrm{Hom}(V, f) : \mathrm{Hom}(V, W_1) \longrightarrow \mathrm{Hom}(V, W_2)$, défini par $\mathrm{Hom}(V, f)(\phi) = f \circ \phi$.



- $\mathrm{Hom}(-, W) : \mathrm{Vect}^{op} \longrightarrow \mathrm{Vect}$, illustré par le diagramme suivant :



- Ces deux foncteurs sont des spécialisations du bifoncteur $\mathrm{Hom} : \mathrm{Vect}^{op} \times \mathrm{Vect} \longrightarrow \mathrm{Vect}$.
- Foncteur dual : $^* : \mathrm{Vect}^{op} \longrightarrow \mathrm{Vect}$, qui correspond à un cas particulier de $\mathrm{Hom}(-, W)$ avec $W = \mathbb{K}$, et qui envoie les morphismes de Vect^{op} sur leur transposée.
- Foncteur produit tensoriel :
  Soient V et W deux espaces vectoriels. Considérons la catégorie des applications bilinéaires depuis $V \times W$, où un morphisme entre $b_1 : V \times W \to U_1$ et $b_2 : V \times W \to U_2$ est une application linéaire $f : U_1 \to U_2$ telle que $f \circ b_1 = b_2$. On admet qu'il existe un objet initial dans cette catégorie, que l'on va noter $b_{V,W}$ (voir la construction explicite du produit tensoriel pour une preuve de l'existence de cet objet). Comme cet objet est unique à unique isomorphisme près, on peut définir le foncteur qui à un couple d'espaces vectoriels (V, W) associe le codomaine de $b_{V,W}$, et à un morphisme $(f, g) : V_1 \times W_1 \to V_2 \times W_2$ associe l'application linéaire $f \otimes g : V_1 \otimes W_1 \to V_2 \otimes W_2$. Ce foncteur est le produit tensoriel $\otimes : \mathrm{Vect} \times \mathrm{Vect} \longrightarrow \mathrm{Vect}$.

5.2 Compléments sur la théorie de Galois

Cette sous-partie est en grande partie tirée de [2].

Définition 24 Extension de corps, extension algébrique
Soit $\mathbb{K}$ un corps. Un extension de $\mathbb{K}$ est la donnée d'un corps $\mathbb{L}$ et d'un morphisme de corps $\iota : \mathbb{K} \to \mathbb{L}$. On note alors l'extension $\mathbb{L}/\mathbb{K}$.
L'extension $\mathbb{L}/\mathbb{K}$ est dite algébrique lorsque tous les éléments de $\mathbb{L}$ sont algébriques sur $\mathbb{K}$ (racine d'un polynôme à coefficients dans $\mathbb{K}$).

Définition 25 On dit que l'extension algébrique $\mathbb{L}/\mathbb{K}$ est

- séparable lorsque tous les éléments de $\mathbb{L}$ ont un polynôme minimal à racines simples dans la clôture algébrique de $\mathbb{K}$;
- normale lorsque tous les éléments $\mathbb{L}$ ont leurs conjugués dans $\mathbb{L}$;
- galoisienne lorsqu'elle est séparable et normale.

Notation 4 Soit $\mathbb{L}/\mathbb{K}$ une extension de corps. On notera $\overline{\mathbb{K}}$ la clôture algébrique de $\mathbb{K}$, et $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$ l'ensemble des morphismes de corps de $\mathbb{L}$ dans $\overline{\mathbb{K}}$ qui fixent les éléments de $\mathbb{K}$.

Propriété 23 Soient $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ deux extensions algébriques. Alors $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{K}}) \times \mathrm{Hom}_{\mathbb{L}}(\mathbb{M},\overline{\mathbb{K}})$ et $\mathrm{Hom}_{\mathbb{K}}(\mathbb{M},\overline{\mathbb{K}})$ sont en bijection.

Démonstration
Soit $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{M},\overline{\mathbb{K}})$. On admet qu'il existe un relèvement $\overline{\sigma}$ de σ à $\overline{\mathbb{K}}$ (théorème de Steiniz). On note $\sigma_{\mathbb{L}}$ la restriction de σ à $\mathbb{L}$, et $\sigma^{\mathbb{L}} := (\overline{\sigma_{\mathbb{L}}})^{-1} \circ \sigma$. Alors l'application Ψ définie ci-dessous est une bijection :

$$\begin{array}{rccc} \Psi : & \mathrm{Hom}_{\mathbb{K}}(\mathbb{M},\overline{\mathbb{K}}) & \longrightarrow & \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{K}}) \times \mathrm{Hom}_{\mathbb{L}}(\mathbb{M},\overline{\mathbb{K}}) \\ & \sigma & \longmapsto & (\sigma^{\mathbb{L}}, \sigma_{\mathbb{L}}) \end{array}$$

En effet, elle est injective car $\sigma = \overline{\sigma_{\mathbb{L}}} \circ \sigma^{\mathbb{L}}$, et surjective car pour tout couple $(\rho,\tau) \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{K}}) \times \mathrm{Hom}_{\mathbb{L}}(\mathbb{M},\overline{\mathbb{K}})$, $\Psi(\overline{\rho} \circ \tau) = (\rho,\tau)$. ■

Propriété 24 Soit $\mathbb{K}(\alpha)/\mathbb{K}$ une extension monogène finie. Il existe une correspondance bijective entre les conjugués de α et les éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(\alpha),\overline{\mathbb{K}})$.

Démonstration
On note P_α le polynôme minimal de α, et n son degré (cela existe car l'extension est finie, donc algébrique). Soit $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(\alpha),\overline{\mathbb{K}})$. Alors $\sigma(\alpha)$ est encore une racine de P_α.
Inversement, soit β une racine de P_α. Montrons qu'il existe un unique morphisme $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(\alpha),\overline{\mathbb{K}})$ tel que $\sigma(\alpha) = \beta$.
On définit une application $\mathbb{K}$-linéaire de $\mathbb{K}(\alpha)$ dans $\mathbb{K}(\beta)$, par $\sigma(x_0 + \alpha x_1 + ... + \alpha^{n-1}x_{n-1}) = x_0 + \beta x_1 + ... + \beta^{n-1}x_{n-1}$, pour tout $(x_0,...,x_{n-1}) \in \mathbb{K}^{n-1}$. Il reste à vérifier que cette application est un morphisme de corps, et il suffit pour cela de montrer que pour tout entier naturel d, $\sigma(\alpha^d) = \beta^d$. Cela est immédiat pour $d \leqslant n-1$, et une récurrence donne le résultat pour $d \geq n-1$.
On a donc associé à β un morphisme de corps, de $\mathbb{K}(\alpha)$ dans $\mathbb{K}(\beta)$. Par linéarité, un tel morphisme est unique.
D'après le premier point de la démonstration, tout morphisme de corps sur $\mathbb{K}(\alpha)$ a son image dans un corps de la forme $\mathbb{K}(\beta)$, pour β un élément conjugué de α. Cela achève de montrer l'unicité de l'élément de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(\alpha),\overline{\mathbb{K}})$ associé à β. ■

Corollaire 5 Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Alors $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{K}})| \leqslant [\mathbb{L}:\mathbb{K}]$.

Démonstration
• Si $\mathbb{L}$ est monogène ($\mathbb{L} = \mathbb{K}(\alpha)$) : d'après la propriété précédente, il y a autant d'éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{K}})$ que de conjugués de α. Donc $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{K}})|$ est inférieur au degré du polynôme minimal de α, qui vaut justement $[\mathbb{L}:\mathbb{K}]$.

• Si $\mathbb{L} = \mathbb{K}(\alpha_1,...,\alpha_m)$: posons $\mathbb{K}_0 = \mathbb{K}$, et, pour $i \in [\![1,m]\!]$, $\mathbb{K}_i = \mathbb{K}(\alpha_1,...,\alpha_i)$.
D'après le cas monogène, on a :

$$|\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}_1,\overline{\mathbb{K}})| \leqslant [\mathbb{K}_1:\mathbb{K}]$$
$$...$$
$$|\mathrm{Hom}_{\mathbb{K}_{n-1}}(\mathbb{K}_n,\overline{\mathbb{K}})| \leqslant [\mathbb{K}_n:\mathbb{K}_{n-1}]$$

Ainsi $\left|\prod_{i=1}^{n} \mathrm{Hom}_{\mathbb{K}_{i-1}}(\mathbb{K}_i,\overline{\mathbb{K}})\right| \leqslant [\mathbb{L}:\mathbb{K}]$.

Or , d'après la propriété 22 (itérée), $\left|\prod_{i=1}^{n} \mathrm{Hom}_{\mathbb{K}_{i-1}}(\mathbb{K}_i,\overline{\mathbb{K}})\right| = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{K}})|$, ce qui achève la preuve. ■

Définition 26 Soit $\mathbb{L}/\mathbb{K}$ une extension de corps.
• On appelle groupe de Galois de $\mathbb{L}/\mathbb{K}$ le groupe des automorphismes de $\mathbb{L}$ qui fixent les éléments de $\mathbb{K}$.
• On appelle groupe de Galois du polynôme P sur $\mathbb{K}$ le groupe de Galois d'un corps de décomposition de P sur $\mathbb{K}$: il est unique à isomorphisme près.

Propriété 25 Une extension finie $\mathbb{L}/\mathbb{K}$ est séparable si et seulement si $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L},\overline{\mathbb{K}})| = [\mathbb{L}:\mathbb{K}]$.

Démonstration
• On commence par le cas où $\mathbb{L}$ est monogène ($\mathbb{L} = \mathbb{K}(\alpha)$). Comme l'extension est finie, elle est algébrique. Si elle est séparable, le degré du polynôme minimal de α est égal à $[\mathbb{L} : \mathbb{K}]$. Or on a vu (propriété 22) que les racines de ce polynôme sont en bijection avec les éléments de $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$, d'où l'égalité. Inversement, s'il y a égalité, tout élément x de $\mathbb{L} - \mathbb{K}$ a son polynôme minimal de degré $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})|$, donc son degré est égal au nombre de conjugués de x (par la propriété 22). Par suite, les racines du polynôme minimal de x sont simples.

• Dans le cas général, soit $(\alpha_1, ..., \alpha_m)$ une base de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel.
Si $\mathbb{L}/\mathbb{K}$ est séparable, alors d'après le cas monogène, il y a égalité dans chaque inégalité de la démonstration du corollaire 4, donc $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = [\mathbb{L} : \mathbb{K}]$. Inversement, supposons que $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = [\mathbb{L} : \mathbb{K}]$. Soit $x \in \mathbb{L}$. On a :

$$[\mathbb{L} : \mathbb{K}] = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})| = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(x), \overline{\mathbb{K}})| \times |\mathrm{Hom}_{\mathbb{K}(x)}(\mathbb{L}, \overline{\mathbb{K}})|$$

$$\begin{cases} |\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(x), \overline{\mathbb{K}}) \leqslant |[\mathbb{K}(x) : \mathbb{K}] \\ |\mathrm{Hom}_{\mathbb{K}(x)}(\mathbb{L}, \overline{\mathbb{K}})| \leqslant [\mathbb{L} : \mathbb{K}(x)] \end{cases}$$

D'où $|\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(x), \overline{\mathbb{K}})| = [\mathbb{K}(x) : \mathbb{K}]$ ce qui équivaut à la séparabilité de x d'après le cas monogène. ■

Propriété 26 Une extension finie $\mathbb{L}/\mathbb{K}$ est normale si et seulement si pour tout $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$, $\sigma(\mathbb{L}) \subset \mathbb{L}$.

Démonstration
Supposons que $\mathbb{L}/\mathbb{K}$ soit normale. Soit $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$, et $x \in \mathbb{L}$. Comme l'extension est finie, elle est algébrique, donc x possède un polynôme minimal P. D'après la propriété 22, $\sigma(x)$ est racine de P. Mais comme $\mathbb{L}/\mathbb{K}$ est normale, les racines de P sont dans $\mathbb{L}$, donc $\sigma(x) \in \mathbb{L}$.

Inversement, supposons que pour tout $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$, $\sigma(\mathbb{L}) \subset \mathbb{L}$. Soit $x \in \mathbb{L}$, et y un conjugué de x. D'après la propriété 22, il existe un unique morphisme $\sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{K}})$ tel que $\sigma(x) = y$. Par hypothèse, $y = \sigma(x) \in \mathbb{L}$, donc $\mathbb{L}/\mathbb{K}$ est normale. ■

Définition 27 Soit $\mathbb{K}$ un corps, et $\mathcal{G}$ un groupe d'automorphismes de $\mathbb{K}$. Le corps des invariants de $\mathbb{K}$ par $\mathcal{G}$, noté $\mathbb{K}^{\mathcal{G}}$, est le sous-corps constitué des éléments laissés fixes par $\mathcal{G}$.

$$\mathbb{K}^{\mathcal{G}} = \{x \in \mathbb{K} \mid \forall \sigma \in \mathcal{G}, \sigma(x) = x\}$$

Théorème 8 (Artin)
Soit $\mathbb{L}$ un corps, $\mathcal{G}$ un groupe fini d'automorphismes de $\mathbb{L}$. Alors l'extension $\mathbb{L}/\mathbb{L}^{\mathcal{G}}$ est galoisienne, de groupe de Galois $\mathcal{G}$.

Démonstration On note $\mathbb{K} = \mathbb{L}^{\mathcal{G}}$ et $\mathcal{G} = \{\sigma_1, ..., \sigma_n\}$.
Montrons que $|\mathcal{G}| = |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})| = [\mathbb{L} : \mathbb{K}]$.
On a déjà les inégalités $|\mathcal{G}| \leqslant |\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})| \leqslant [\mathbb{L} : \mathbb{K}]$. On procède par l'absurde, en supposant que $[\mathbb{L} : \mathbb{K}] > |\mathcal{G}|$.
Il existe alors une famille $(x_1, ..., x_m)$ d'éléments de $\mathbb{L}$, linéairement indépendants par rapport à $\mathbb{K}$, avec $m > n$. On considère le système suivant, d'inconnues $(y_1, ..., y_m)$:

$$(S_1) = \begin{cases} \sigma_1(x_1)y_1 + ... + \sigma_1(x_m)y_m = 0 \\ ... \\ \sigma_n(x_1)y_1 + ... + \sigma_n(x_m)y_m = 0 \end{cases}$$

Comme il y a plus d'inconnues que d'équations, il existe une solution non triviale $Y = (y_1, ..., y_m)$, qui n'est pas dans $\mathbb{K}^m$, sinon la famille (x_i) serait liée. On peut supposer que $Y = (y_1, ..., y_r, 0, ..., 0)$, avec les $y_i \neq 0$ pour $i \in [\![1, r]\!]$ et r minimal. Soit $\sigma_j \in \mathcal{G}$. On applique σ_j au système précédent, et on réordonne les équations pour obtenir :

$$(S_2) = \begin{cases} \sigma_1(x_1)\sigma_j(y_1) + ... + \sigma_1(x_r)\sigma_j(y_r) = 0 \\ ... \\ \sigma_n(x_1)\sigma_j(y_1) + ... + \sigma_n(x_r)\sigma_j(y_r) = 0 \end{cases}$$

En effectuant $(S_1)\sigma_j(y_r) - (S_2)y_r$, on obtient enfin :

$$(S_3) = \begin{cases} \sigma_1(x_1)(y_1\sigma_j(y_r) - y_r\sigma_j(y_1)) + ... + \sigma_1(x_{r-1})(y_{r-1}\sigma_j(y_r) - y_r\sigma_j(y_{r-1})) = 0 \\ ... \\ \sigma_n(x_1)(y_1\sigma_j(y_r) - y_r\sigma_j(y_1)) + ... + \sigma_n(x_{r-1})(y_{r-1}\sigma_j(y_r) - y_r\sigma_j(y_{r-1})) = 0 \end{cases}$$

Par minimalité de r, la solution que l'on vient de construire est nulle : $y_k\sigma_j(y_r) - y_r\sigma_j(y_k) = 0$ pour tout $k \in [\![1, r]\!]$, c'est-à-dire que $\sigma_j(y_k y_r^{-1}) = y_k y_r^{-1}$, donc que $y_k y_r^{-1} \in \mathbb{K}$, pour tout $k \in [\![1, r]\!]$. Donc la famille $(y_k y_r^{-1})_k$ est une solution de (S_1) dans $\mathbb{K}^m$, ce qui contredit la liberté de la famille (x_i).

On a finalement $|\mathcal{G}| = |\operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})| = [\mathbb{L} : \mathbb{K}]$, ce qui montre que l'extension $\mathbb{L}/\mathbb{K}$ est finie, donc algébrique. De plus, si on note k le cardinal du groupe de Galois de $\mathbb{L}/\mathbb{K}$, on a toujours $|\mathcal{G}| \leqslant k \leqslant |\mathbb{L} : \mathbb{K}|$. Ici, on a montré qu'il y a égalité, donc que $\mathcal{G}$ est bien le groupe de Galois de $\mathbb{L}/\mathbb{K}$.
Enfin, le fait que $|\operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})| = [\mathbb{L} : \mathbb{K}]$ équivaut à la séparabilité de $\mathbb{L}$, et le fait que $|\mathcal{G}| = |\operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})|$ montre que $\operatorname{Aut}_{\mathbb{K}}(\mathbb{L}) = \operatorname{Hom}_{\mathbb{K}}(\mathbb{L}, \overline{\mathbb{L}})$, donc que l'extension $\mathbb{L}$ est normale. ■

Corollaire 6 Soit $\mathbb{K}$ un corps et $\mathbb{L}$ une extension galoisienne de $\mathbb{K}$, de degré fini. Soit $\mathcal{G}$ le groupe de Galois de $\mathbb{L}$ sur $\mathbb{K}$.
Alors $\mathbb{L}^{\mathcal{G}} = \mathbb{K}$.

Démonstration Comme l'extension $\mathbb{L}/\mathbb{K}$ est galoisienne, on a $|\mathcal{G}| = [\mathbb{L} : \mathbb{K}]$. Or d'après le théorème d'Artin, le groupe de Galois de l'extension $\mathbb{L}/\mathbb{L}^{\mathcal{G}}$ est $\mathcal{G}$.
D'où : $[\mathbb{L} : \mathbb{K}] = |\mathcal{G}| \leqslant [\mathbb{L} : \mathbb{L}^{\mathcal{G}}]$, donc $[\mathbb{L}^{\mathcal{G}} : \mathbb{K}] \leqslant 1$, ce qui signifie que $\mathbb{L}^{\mathcal{G}} = \mathbb{K}$. ■

5.3 Compléments sur les entiers algébriques

Définition 28 Entier algébrique
Un nombre complexe z est un entier algébrique lorsqu'il existe un polynôme unitaire $P \in \mathbb{Z}[X]$ tel que $P(z) = 0$.

Propriété 27 Les seuls entiers algébriques rationnels sont les entiers.

Démonstration
Soit $x \in \mathbb{Q}$ un entier algébrique. Il existe un polynôme unitaire $P = X^n + \sum_{i=1}^{n-1} a_i X^i \in \mathbb{Z}[X]$ tel que $P(x) = 0$. On écrit x sous forme de fraction irréductible : $x = \dfrac{p}{q}$. En reportant dans l'expression de P et en multipliant par q^n, on obtient

$$p^n = -q \cdot \sum_{i=1}^{n-1} a_i p^i q^{n-i-1}$$

Ainsi q divise p^n, puis, par lemme de Gauss, q divise 1, donc x est entier. ■

Propriété 28 Soit z un nombre complexe. Les propriétés suivantes sont équivalentes :

- (i) z est un entier algébrique
- (ii) L'anneau $\mathbb{Z}[z]$ est un engendré par un nombre fini d'éléments en tant que $\mathbb{Z}$-module.
- (iii) Il existe un sous-anneau de $\mathbb{C}$, contenant z, engendré par un nombre fini d'éléments en tant que $\mathbb{Z}$-module.

Démonstration
• Supposons que z soit un entier algébrique : il existe donc un polynôme unitaire à coefficients entiers $P := \sum_{k=0}^{n} a_k X^k$ qui annule z, soit :

$$z^n = -\sum_{k=0}^{n-1} a_k z^k$$

La famille $(1, z, ..., z^{n-1})$ est donc génératrice du $\mathbb{Z}$-module $\mathbb{Z}[z]$.

• L'implication $(ii) \Rightarrow (iii)$ est immédiate.

• Supposons qu'il existe M, un sous-anneau de $\mathbb{C}$ contenant z, engendré par un nombre fini d'éléments

$(x_1, ..., x_n)$ en tant que $\mathbb{Z}$-module.
Pour tout $i \in [\![1, n]\!]$, il existe donc une famille $(a_{ij})_{1 \leq j \leq n}$ d'entiers telle que

$$zx_i = \sum_{j=1}^{n} a_{ij} x_j$$

On pose $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{Z})$, de telle sorte que $Ax = zx$, où $x = {}^t(x_1 \ ... \ x_n)$. Ainsi z est une racine du polynôme $P(x) = \det(xI_n - A)$, qui est unitaire à coefficients entiers. z est bien un entier algébrique. ■

Corollaire 7 L'ensemble des entiers algébriques forme un anneau dans $\mathbb{C}$.

Démonstration Il suffit de montrer la stabilité par addition et multiplication. Soient z, z' deux entiers algébriques. D'après la propriété précédente, les anneaux $\mathbb{Z}[z]$ et $\mathbb{Z}[z']$ sont de type finis en tant que $\mathbb{Z}$-modules, donc l'anneau $\mathbb{Z}[z, z']$ est également de type fini, et il contient $z + z'$ et zz', qui sont alors des entiers algébriques toujours en vertu de la propriété précédente. ■

Propriété 29 Soient G un groupe fini, χ un caractère irréductible de G et C une classe de conjugaison de G. Alors pour tout g dans C, la quantité $\dfrac{|C|\chi(g)}{\chi(1)}$ est un entier algébrique.

Lemme 9 Soit G un groupe fini. On note $C_1, ..., C_r$ ses classes de conjugaisons et pour tout $i \in [\![1, r]\!]$, $K_i = \sum_{g \in C_i} g$. Alors la famille $(K_1, ..., K_r)$ est une base de l'algèbre $Z(\mathbb{C}[G])$, et les coefficients de la décomposition de $K_i K_j$ (pour $i, j \in [\![1, r]\!]$) sur cette base sont des entiers positifs.

Démonstration (du lemme)
On vérifie simplement que les K_i sont dans le centre de $\mathbb{C}[G]$. Comme chaque K_i se décompose sur G avec des éléments de G qui lui sont propres, la famille $(K_1, ..., K_r)$ est libre. Soit $z \in Z(\mathbb{C}[G])$. Décomposons z sur G : $z = \sum_{g \in G} a_g g$. Or pour tout $h \in G$, $hzh^{-1} = z$ donc :

$$\sum_{g \in G} a_{h^{-1}gh} g = \sum_{g \in G} a_g g$$

Et par identification des coefficients, on obtient que tous les éléments d'une même classe de conjugaison C_i dans G ont le même coefficient a_i. Ainsi en regroupant par classe :

$$z = \sum_{i=1}^{r} a_i K_i$$

La famille $(K_1, ..., K_r)$ est bien une base de $Z(\mathbb{C}[G])$.
Soient $i, j \in [\![1, r]\!]$. On décompose $K_i K_j$ sur G :

$$K_i K_j = \sum_{g \in C_i} \sum_{h \in C_j} gh = \sum_{x \in G} |\{(g, h) \in C_i \times C_j \mid gh = x\}| x$$

D'où le fait que les coefficients de la décomposition de $K_i K_j$ sur la base $(K_1, ..., K_r)$ soient des entiers positifs. ■

Démonstration (de la propriété)
Soit ρ une représentation de G de caractère χ, que l'on étend par linéarité à l'algèbre $\mathbb{C}[G]$. Avec les notations du lemme : pour tout $i \in [\![, r]\!]$, K_i est dans le centre de $\mathbb{C}[G]$, donc $\rho(K_i)$ est une homothétie, de rapport w_i. De plus, par linéarité, $\rho(K_i K_j)$ est encore une homothétie, de rapport $\sum_{v=1}^{r} a_{ijk} w_k$, où on a décomposé $K_i K_j = \sum_{k=1}^{r} a_{ijk} K_k$. Or d'après le lemme, les coefficients a_{ijk} sont entiers. Donc l'ensemble des combinaisons entières de w_i forme un sous-anneau de $\mathbb{C}$ engendré par un nombre fini d'éléments en tant que $\mathbb{Z}$-module. D'après la propriété 26, les w_i sont des entiers algébriques.

Mais pour $i \in [\![1, r]\!]$, on a d'une part $\chi(K_i) = \chi(1) w_i$ car $\rho(K_i) = w_i \, \mathrm{id}$, et d'autre part $\chi(K_i) = \chi(\sum_{h \in C_i} h) = |C_i| \chi(g)$ pour un certain $g \in C_i$. Donc $w_i = \dfrac{|C_i|\chi(g)}{\chi(1)}$, et on a le résultat voulu. ■

Références

[1] Irving Reiner Charles W. Curtis. *Methods of representation theory.* John Wiley and Sons, 1981.

[2] Bruno Deschamps. Théorie de galois, cours de maîtrise, 2002.

[3] Martin Isaacs. *Character theory of finite groups.* Academic Press, 1976.

[4] Serge Lang. *Algebra.* Springer, 2002.

[5] Jean-Pierre Serre. *Linear Representations of Finite Groups.* Springer, 1971.

[6] Joe Harris William Fulton. *Representation theory.* Springer, 1991.