Représentations des groupes finis

Table des matières

Introduction

La théorie des représentations des groupes finis est l'une des rares dont la naissance est datée de façon précise. En avril 1896, en répondant à une question de Dedekind [1], Frobenius [2] pose les bases de la théorie, qu'il va développer dans une série d'une vingtaine d'articles. La théorie sera ensuite consolidée par Burnside [3], Schur [4] puis par l'école de l'université de Chicago au début du XX^{e} siècle avec les travaux de Dickson [5], Maschke [6] ou Wedderburn [7]. Cette théorie a joué un rôle majeur dans la classification des groupes finis simples, achevée dans les années 1980.

Notations 0.1.
1. $\mathbb{K}$ désigne un corps commutatif.
2. Les groupes seront notés multiplicativement. Si G est un groupe, son élément neutre est noté e_G.

1 Définitions et premières propriétés

1.1 Représentation d'un groupe

Lorque l'on considère l'action d'un groupe fini sur un $\mathbb{K}$-espace vectoriel E, il est naturel de considérer les actions linéaires, c'est-à-dire telles que l'image du morphisme de groupes associé à l'action a son image incluse dans le sous groupe $\mathrm{GL}(E)$ du groupe $\mathscr{S}(E)$ des bijections de E. C'est ce qu'on appelle une représentation de G.

Définition 1.1. *Soit G un groupe et E un $\mathbb{K}$-espace vectoriel. Une représentation de G d'espace E est un morphisme de groupes θ de G dans le groupe $\mathrm{GL}(E)$ des automorphismes linéaires de E. La dimension de E est appelée degré de la représentation θ.*

Autrement dit, une représentation d'un groupe G d'espace E peut aussi être considérée comme une application

$$\left\{\begin{array}{ccc} G\times E & \longrightarrow & E \\ (g,x) & \longmapsto & g\cdot x \end{array}\right.$$

telle que pour tous $g,h\in G$, tous $x,y\in E$, tout $\lambda\in\mathbb{K}$,

$$g\cdot(h\cdot x)=(gh)\cdot x, \qquad e_G\cdot x=x,$$
$$g\cdot(x+y)=g\cdot x+g\cdot y, \qquad g\cdot(\lambda x)=\lambda(g\cdot x).$$

On se limitera ici au cas où le degré de la représentation est fini.

Remarque 1.1. Soit θ une représentation de G d'espace E et de degré n. En choisissant une base $\mathscr{B}$ de E, on obtient un isomorphisme de groupes de $\mathrm{GL}(E)$ sur $\mathrm{GL}_n(\mathbb{K})$, groupe des matrices inversibles de taille n à coefficients dans $\mathbb{K}$, envoyant $f\in\mathrm{GL}(E)$ sur $M_{\mathscr{B}}(f)$. Une représentation de G sur E associe à tout élément g de G une matrice M_g (dépendant du choix de la base), de sorte que :
- $M_e=I_n$.
- Si $g,h\in G$, $M_{gh}=M_gM_h$.

Remarque 1.2. Si un groupe G possède une représentation fidèle d'espace E, alors il est isomorphe à un sous-groupe de $\mathrm{GL}(E)$.

Le lemme suivant servira souvent :

Lemme 1.2. *Soit G un groupe, E un espace vectoriel et $\theta : G\longrightarrow\mathscr{L}(E)$ une application telle que $\theta(e_G)=\mathrm{Id}_E$ et pour tous $g,h\in G$, $\theta(gh)=\theta(g)\circ\theta(h)$. Alors θ est une représentation de G.*

1. Richard Dedekind (1831–1916), Mathématicien allemand.
2. Ferdinand Georg Frobenius (1849–1917), mathématicien allemand.
3. William Burnside (1852–1927), mathématicien anglais.
4. Issaï Schur(1875–1941), mathématicien d'origine russe actif en Allemagne.
5. Leonard Eugene Dickson (1874–1954), mathématicien américain.
6. Heinrich Maschke (1853–1908), mathématicien prussien.
7. Joseph Henry Maclagen Wedderburn (1882–1948), mathématicien écossais.

Démonstration. Il reste à montrer que pour tout $g \in G$, $\theta(g)$ est une bijection.

$$\mathrm{Id}_E = \theta(e_G) = \theta(gg^{-1}) = \theta(g) \circ \theta(g^{-1}).$$

De même, $\theta(g^{-1}) \circ \theta(g) = \mathrm{Id}_E$. Donc $\theta(g)$ est bijective, d'inverse $\theta(g^{-1})$. □

1.2 Opérations sur les représentations

Proposition 1.3. *Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation d'un groupe G et soit F un sous-espace de E. On dit que F est un sous-espace invariant de θ si pour tout $g \in G$, $\theta(g)(F) \subseteq F$. Dans ce cas, on obtient une représentation $\theta_{|F} : G \longrightarrow \mathrm{GL}(F)$ de G :*

$$\theta_{|F} : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(F) \\ g & \longmapsto & \left\{ \begin{array}{ccc} F & \longrightarrow & F \\ x & \longmapsto & \theta(g)(x). \end{array} \right. \end{array} \right.$$

Cette représentation est appelée sous-représentation de θ restreinte à F.

Démonstration. Par restriction, on obtient une application $\theta' : G \longrightarrow \mathscr{L}(F)$ telle que $\theta'(e_G) = \mathrm{Id}_F$ et pour tous $g, h \in G$, $\theta'(gh) = \theta'(g) \circ \theta'(h)$. D'après le lemme 1.2, θ' est une représentation de G. □

Proposition 1.4. *Soit θ une représentation de G d'espace E et F un sous-espace invariant de θ. L'espace quotient E/F est également une représentation de G :*

$$\forall x \in G,\ \forall \overline{x} \in E/F, \qquad \overline{\theta}(g)(\overline{x}) = \overline{\theta(g)(x)}.$$

Démonstration. Pour tout $g \in G$, on définit une application

$$\overline{\theta}(g) : \left\{ \begin{array}{ccc} E/F & \longrightarrow & E/F \\ \overline{x} & \longmapsto & \overline{\theta(g)(x)}. \end{array} \right.$$

Montrons qu'elle est bien définie. Soient $x, y \in E$ tels que $\overline{x} = \overline{y}$. Alors $x - y \in F$. Par hypothèse, comme F est invariant,

$$\theta(g)(x - y) = \theta(g)(x) - \theta(g)(y) \in F,$$

donc $\overline{\theta(g)(x)} = \overline{\theta(g)(y)}$: $\overline{\theta}(g)$ est bien définie. Comme $\theta(g)$ est linéaire, $\overline{\theta}(g)$ est linéaire. De plus, pour tout $\overline{x} \in E/F$,

$$\overline{\theta}(e_G)(\overline{x}) = \overline{\theta(e_G)(x)} = \overline{x},$$

donc $\overline{\theta}(e_G) = \mathrm{Id}_{E/F}$. Soient $g, h \in G$. Pour tout $\overline{x} \in E/F$,

$$\begin{aligned} \overline{\theta}(gh)(\overline{x}) &= \overline{\theta(gh)(x)} = \overline{\theta(g)(\theta(h)(x))} \\ &= \overline{\theta}(g)(\overline{\theta(h)(x)}) = \overline{\theta}(g)(\overline{\theta}(h)(\overline{x})) = \overline{\theta}(g) \circ \overline{\theta}(h)(\overline{x}). \end{aligned}$$

Donc $\overline{\theta}(gh) = \overline{\theta}(g) \circ \overline{\theta}(h)$. D'après le lemme 1.2, $\overline{\theta}$ est une représentation du groupe G. □

Proposition 1.5. *Soient θ et θ' deux représentations d'un groupe G, d'espaces respectifs E et E'. On définit une représentation $\theta \oplus \theta'$ d'espace $E \times E'$ par*

$$\forall g \in G,\ \forall (x, x') \in E \times E', \qquad (\theta \oplus \theta')(g)(x, x') = (\theta(g)(x), \theta'(g)(x')).$$

Elle est appelée représentation somme directe de θ et θ'.

Démonstration. Pour tout $g \in G$, $(\theta \oplus \theta')(g)$ est bien un endomorphisme de $E \times E'$. De plus, pour tout $(x, x') \in E \times E'$,

$$(\theta \oplus \theta')(e_G)(x, x') = (\theta(e_G)(x), \theta'(e_G)(x')) = (x, x').$$

Pour tous $g, h \in G$, pour tout $(x, x') \in E \times E'$,

$$\begin{aligned} (\theta \oplus \theta')(g) \circ (\theta \oplus \theta')(h)(x, x') &= (\theta(g) \circ \theta(h)(x), \theta'(g) \circ \theta'(h)(x')) \\ &= (\theta(gh)(x), \theta'(gh)(x')) \\ &= (\theta \oplus \theta')(gh)(x, x'). \end{aligned}$$

D'après le lemme 1.2, $\theta \oplus \theta'$ est bien une représentation de G. □

Proposition 1.6. *Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation d'un groupe G d'espace E. On définit une représentation θ^* d'espace le dual E^* de E (c'est-à-dire l'espace des applications linéaires de E dans $\mathbb{K}$) par*

$$\forall g \in G,\ \forall f \in E^*, \qquad \theta^*(g)(f) = f \circ \theta(g^{-1}).$$

Elle est appelée représentation duale de θ.

Démonstration. Pour tout $f \in E^*$,

$$\theta^*(e_G)(f) = f \circ \theta(e_G^{-1}) = f \circ \theta(e_G) = f \circ \mathrm{Id}_E = f,$$

donc $\theta^*(e_G) = \mathrm{Id}_{E^*}$. Soient $g, h \in G$. Pour tout $f \in E^*$,

$$\begin{aligned}\theta^*(gh)(f) &= f \circ \theta((gh)^{-1}) = f \circ \theta(h^{-1}g^{-1}) \\ &= f \circ \theta(h^{-1}) \circ \theta(g^{-1}) = \theta^*(g)(f \circ \theta(h^{-1})) = \theta^*(g) \circ \theta^*(h)(f).\end{aligned}$$

Donc $\theta^*(gh) = \theta^*(g) \circ \theta^*(h)$. Par le lemme 1.2, θ^* est une représentation du groupe G. □

1.3 Morphismes de représentations

Définition 1.7. *Soient θ et θ' deux représentations d'un même groupe G, d'espaces respectifs E et E'. Soit $\phi : E \longrightarrow E'$ une application linéaire. On dit que ϕ est un morphisme de représentations de G de θ vers θ' si*

$$\forall g \in G, \qquad \phi \circ \theta(g) = \theta'(g) \circ \phi.$$

Lorsque de plus ϕ est bijective, on dira que ϕ est un isomorphisme de représentations de G et que les représentations θ et θ' sont isomorphes. Si $\theta = \theta'$, on dira que ϕ est un endomorphisme de la représentation θ et si de plus ϕ est bijective, on dira que ϕ est un automorphisme de la représentation θ.

Exemple 1.1.

1. Si F est un sous-espace invariant d'une représentation θ d'espace E, l'injection canonique de F dans E et la projection canonique de E dans E/F sont des morphismes de représentations.
2. Soient F et F' deux sous-espaces invariants d'une représentation θ d'espace E. L'application suivante est un morphisme de représentations de G de $\theta_{|F} \oplus \theta_{|F'}$ vers θ :

$$\left\{\begin{array}{ccc} F \times F' & \longrightarrow & E \\ (x, x') & \longmapsto & x + x'. \end{array}\right.$$

   Si de plus $E = F \oplus F'$, alors il s'agit d'un isomorphisme.
3. L'application suivante est un isomorphisme de représentations de G de θ vers $(\theta^*)^*$:

$$\left\{\begin{array}{ccc} E & \longrightarrow & (E^*)^* \\ x & \longmapsto & \left\{\begin{array}{ccc} E^* & \longrightarrow & \mathbb{K} \\ f & \longmapsto & f(x). \end{array}\right. \end{array}\right.$$

Proposition 1.8. *Soient $\theta : G \longrightarrow \mathrm{GL}(E)$ et $\theta' : G \longrightarrow \mathrm{GL}(E')$ deux représentations d'un même groupe G et soit $\phi : E \longrightarrow E'$ un morphisme de représentations de θ vers θ'. Alors $\mathrm{Ker}(\phi)$ est un sous-espace invariant de θ et $\mathrm{Im}(\phi)$ est un sous-espace invariant de θ'. Si $\theta = \theta'$, les espaces propres de ϕ sont des sous-espaces invariants de θ.*

Démonstration. Soit $x \in \mathrm{Ker}(\phi)$. Pour tout $g \in G$,

$$\phi(\theta(g)(x)) = \phi \circ \theta(g)(x) = \theta'(g) \circ \phi(x) = \theta'(g)(0_E) = 0_{E'},$$

donc $\theta(g)(x) \in \mathrm{Ker}(\phi)$: $\mathrm{Ker}(\phi)$ est un sous-espace invariant de θ.

Soit $y \in \mathrm{Im}(\phi)$. Alors il existe $x \in E$ tel que $\phi(x) = y$. Pour tout $g \in G$,

$$\theta'(g)(y) = \theta'(g)(\phi(x)) = \theta'(g) \circ \phi(x) = \phi \circ \theta(g)(x) \in \mathrm{Im}(\phi),$$

donc $\mathrm{Im}(\phi)$ est un sous-espace invariant de θ'.

Supposons $\theta = \theta'$ et soit F un espace propre de ϕ. La valeur propre associée est notée λ. Soit $x \in F$. Pour tout $g \in G$,

$$\phi(\theta(g)(x)) = \phi \circ \theta(g)(x) = \theta(g) \circ \phi(x) = \theta(g)(\lambda x) = \lambda\theta(g)(x),$$

donc $\theta(g)(x) \in F$: F est un sous-espace invariant de θ. □

2 Représentations irréductibles

2.1 Définition

Définition 2.1. *Soit θ une représentation d'un groupe G, d'espace E. On dira qu'elle est simple ou irréductible si elle est non nulle et si ses seuls sous-espaces invariants sont E et $\{0_E\}$.*

Exemple 2.1.

1. Si E est de dimension 1, alors elle est irréductible de façon évidente.
2. On se place sur le corps $\mathbb{K} = \mathbb{R}$. On considère la représentation

$$\begin{cases} \theta : \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathrm{GL}_2(\mathbb{R}) \\ \qquad \overline{n} & \longmapsto & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^n, \end{cases}$$

   en identifiant $\mathrm{GL}(\mathbb{R}^2)$ et $\mathrm{GL}_2(\mathbb{R})$ de façon canonique. Comme

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

   cette représentation est bien définie. La matrice $\theta(1) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ne possède aucun vecteur propre dans $\mathbb{R}^2$, donc elle ne possède aucune droite stable dans $\mathbb{R}^2$. Par suite, les sous-espaces stables par cette matrice sont E et $\{0_E\}$: θ est donc irréductible.
3. On considère de façon similaire la représentation de $\mathbb{Z}/4\mathbb{Z}$ en se plaçant sur le corps $\mathbb{C}$:

$$\begin{cases} \theta : \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathrm{GL}_2(\mathbb{C}) \\ \qquad \overline{n} & \longmapsto & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^n, \end{cases}$$

   La matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ possède deux droites propres, engendrées par les vecteurs $\begin{pmatrix} i \\ 1 \end{pmatrix}$ et $\begin{pmatrix} -i \\ 1 \end{pmatrix}$. Chacune de ces droites est un sous-espace invariant de θ : θ n'est pas irréductible.

2.2 Semi-simplicité des représentations

Proposition 2.2. *On suppose $\mathbb{K}$ de caractéristique ne divisant pas le cardinal de G. Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation d'un groupe fini G et F un sous-espace invariant de θ. Alors il existe un sous-espace invariant F' de θ telle que $E = F \oplus F'$.*

Démonstration. Par le théorème de la base incomplète, il existe un sous-espace V de E tel que $E = F \oplus V$. En général, il n'y a aucune raison pour que V soit un sous-espace invariant. Soit $p : E \longrightarrow E$ le projecteur canonique sur F dans cette somme directe. On considère l'application

$$q = \frac{1}{|G|} \sum_{g \in G} \theta(g) \circ p \circ \theta(g^{-1}).$$

Comme G est fini et que la caractéristique du corps $\mathbb{K}$ ne divise pas $|G|$, cette application existe et c'est un endomorphisme de E. Pour tout $x \in E$, pour tout $g \in G$, $p \circ \theta(g^{-1})(x) \in F$ car p est un projecteur sur F. Comme F est un sous-espace invariant $\theta(g) \circ p \circ \theta(g^{-1})(x) \in F$ et donc $q(x) \in F$: $q(E) \subseteq F$.

Si $x \in F$, pour tout $g \in G$, $\theta(g^{-1})(x) \in F$ et comme p est un projecteur sur F, $p \circ \theta(g^{-1})(x) = \theta(g^{-1})(x)$. En conséquence,

$$\begin{aligned} q(x) &= \frac{1}{|G|} \sum_{g \in G} \theta(g) \circ \theta(g^{-1})(x) = \frac{1}{|G|} \sum_{g \in G} \theta(gg^{-1})(x) \\ &= \frac{1}{|G|} \sum_{g \in G} \theta(e_G)(x) = \frac{1}{|G|} \sum_{g \in G} x = x, \end{aligned}$$

donc q est un autre projecteur sur F. Soit F' le noyau de q ; alors $E = F \oplus F'$. Il reste à montrer que F' est un sous-espace invariant de E. Pour cela, d'après la proposition 1.8, il suffit de montrer que q est un morphisme de représentations de G. Soit $h \in G$.

$$\begin{aligned} q \circ \theta(h) &= \frac{1}{|G|} \sum_{g \in G} \theta(g) \circ p \circ \theta(g^{-1}) \circ \theta(h) \\ &= \frac{1}{|G|} \sum_{g \in G} \theta(g) \circ p \circ \theta(g^{-1}h) \\ &= \frac{1}{|G|} \sum_{k \in G} \theta(hk) \circ p \circ \theta(k^{-1}) \\ &= \frac{1}{|G|} \sum_{k \in G} \theta(h) \circ \theta(k) \circ p \circ \theta(k^{-1}) \\ &= \theta(h) \circ \left(\frac{1}{|G|} \sum_{k \in G} \theta(k) \circ p \circ \theta(k^{-1}) \right) \\ &= \theta(h) \circ q. \end{aligned}$$

On a fait le changement de variable $k = h^{-1}g$: quand g parcourt G, k parcourt G ; de plus, $g^{-1}h = k^{-1}$ et $g = hk$. Donc q est bien un morphisme de représentations de G. □

Remarque 2.1. On peut appliquer ce théorème pour tout groupe fini lorsque la caractéristique de $\mathbb{K}$ est nulle.

Remarque 2.2. Ce théorème est faux si G n'est pas fini ou si la caractéristique de $\mathbb{K}$ divise le cardinal de G. Voici des contre-exemples.

1. On considère la représentation du groupe $\mathbb{Z}$ définie par

$$\theta : \begin{cases} \mathbb{Z} & \longrightarrow & \mathrm{GL}_2(\mathbb{C}) \\ n & \longmapsto & \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}. \end{cases}$$

La matrice $\theta(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, non diagonalisable, possède une seule droite propre D, engendrée par le vecteur $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Cette droite D est donc le seul sous-espace invariant de dimension 1 de θ : elle ne possède pas de supplémentaire invariant.

2. Soit p un nombre premier. On considère la représentation du groupe $\mathbb{Z}/p\mathbb{Z}$ définie par

$$\theta : \begin{cases} \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \\ \overline{k} & \longmapsto & \begin{pmatrix} \overline{1} & \overline{k} \\ \overline{0} & \overline{1} \end{pmatrix}. \end{cases}$$

Un raisonnement semblable à celui effectué sur l'exemple précédent montre que cette représentation possède un seul sous-espace invariant de dimension 1, qui ne possède donc pas de supplémentaire invariant.

Théorème 2.3. ***(Théorème de Maschke)*** *On suppose $\mathbb{K}$ de caractéristique ne divisant pas le cardinal de G. Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation non nulle d'un groupe fini G. Alors il existe des sous-espaces invariants irréductibles $E_1, \ldots, E_k$ de θ telles que $E = E_1 \oplus \ldots \oplus E_k$.*

Démonstration. On procède par récurrence forte sur $n = \dim(E)$. Si $\dim(E) = 1$, alors E est irréductible et on prend $k = 1$, $E_1 = E$. Supposons le résultat vrai pour toutes les représentations θ' de G de dimension $< n$. Si θ est irréductible, on prend $k = 1$ et $E_1 = E$. Sinon, il existe un sous-espace invariant F de θ, non trivial. Par la proposition 2.2, il existe un sous-espace invariant F' de θ, telle que $E = F \oplus F'$. Comme $F \neq \{0_E\}$ et $F \neq E$, $\dim(F) < n$ et $\dim(F') < n$. Par l'hypothèse de récurrence, il existe des sous-espaces invariants $E_1, \ldots, E_k$ et $E_{k+1}, \ldots E_{k+l}$ de $\theta_{|F}$ et $\theta_{|F'}$ (et donc de θ) telles que

$$F = E_1 \oplus \ldots \oplus E_k, \qquad\qquad F' = E_{k+1} \oplus \ldots \oplus E_{k+l}.$$

Comme $E = F \oplus F'$, $E = E_1 \oplus \ldots \oplus E_{k+l}$. □

Remarque 2.3.

1. En conséquence, θ est isomorphe à la représentation $\theta_1 \oplus \ldots \oplus \theta_k$, où $\theta_i = \theta_{|F_i}$.

2. La décomposition de θ en somme directe de représentations irréductibles n'est pas unique : par exemple, si G agit trivialement sur E, toute décomposition de E en somme directe de sous-espaces de dimension 1 est une décomposition de θ.

3. Ce résultat est faux si la caractéristique de $\mathbb{K}$ divise $|G|$ ou si G n'est pas fini, comme le montrent les exemples de la remarque 2.2.

3 Caractères d'un groupe abélien fini

À partir de maintenant, le corps de base est $\mathbb{C}$ et tous les espaces vectoriels considérés sont sur $\mathbb{C}$.

3.1 Représentations d'un groupe abélien fini

On souhaite maintenant trouver toutes les représentations d'un groupe fini G. Il suffit de trouver toutes les représentations irréductibles de G , d'après le théorème 2.3. On débute avec les groupes abéliens.

Lemme 3.1. *Soit G un groupe fini d'ordre n, non nécessairement abélien, et soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation de G. Alors pour tout $g \in G$, $\theta(g)$ est diagonalisable et ses valeurs propres sont des racines n-ièmes de l'unité.*

Démonstration. D'après le théorème de Lagrange, $g^n = e_G$, donc $\theta(g)^n = \theta(g^n) = \theta(e_G) = \mathrm{Id}_E$. Par suite, le polynôme $X^n - 1$ annule l'application linéaire $\theta(g)$. Comme ce polynôme est scindé à racines simples, $\theta(g)$ est diagonalisable et ses valeurs propres sont certaines racines de ce polynôme, donc des racines n-ièmes de l'unité. □

Proposition 3.2. *Soit G un groupe abélien fini. Les représentations irréductibles de G sont ses représentations de dimension* 1.

Démonstration. On a déjà observé que les représentations de dimension 1 sont irréductibles. Il faut maintenant montrer la réciproque lorsque G est abélien.

Première étape. Soit E un espace vectoriel et soient $f_1, \ldots, f_k$ des endomorphismes de E tous diagonalisables. On suppose que pour tous i, j, $f_i \circ f_j = f_j \circ f_i$. Montrons qu'alors $f_1, \ldots, f_k$ possèdent une base commune de vecteurs propres. On procède par récurrence sur k. Si $k = 1$, il n'y a rien à démontrer. Supposons $k > 1$. Comme f_k est diagonalisable, E se décompose en somme d'espaces propres de f_k :

$$E = \bigoplus_{\lambda \in \mathrm{Sp}(f_k)} E_\lambda,$$

où $E_\lambda = \{x \in E,\ f_k(x) = \lambda x\}$. Soit $i < k$. Si $x \in E_\lambda$,

$$f_k(f_i(x)) = f_k \circ f_i(x) = f_i \circ f_k(x) = f_i(\lambda x) = \lambda f_i(x),$$

donc E_λ est stable par f_i pour tout $i < k$. Comme f_i est diagonalisable, il existe un polynôme P scindé à racines simples tel que $P(f_i) = 0$, donc par restriction, $P((f_i)_{|E_\lambda}) = 0$ et $(f_i)_{|E_\lambda}$ est diagonalisable. Par l'hypothèse de récurrence appliquée à $(f_1)_{|E_\lambda}, \ldots, (f_{k-1})_{|E_\lambda}$, il existe une base $\mathscr{B}_\lambda$ de E_λ, formée de vecteurs propres communs à $f_1, \ldots, f_{k-1}$. Comme ce sont des éléments de E_λ, ce sont aussi des vecteurs propres de f_k. On considère alors

$$\mathscr{B} = \bigcup_{\lambda \in \mathrm{Sp}(f_k)} \mathscr{B}_\lambda.$$

Comme les E_λ sont en somme directe, on obtient une base de E, formée de vecteurs propres communs à tous les f_i.

Seconde étape. Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation irréductible de G. On pose $G = \{g_1, \ldots, g_k\}$ et pour tout i, $f_i = \theta(g_i)$. Pour tous i, j, $g_i g_j = g_j g_i$ car G est abélien, donc $f_i \circ f_j = f_j \circ f_i$. Par le lemme 3.1, les f_i sont diagonalisables, donc il existe une base $(e_1, \ldots, e_n)$ de vecteurs propres communs aux f_i. En particulier, $\mathrm{Vect}(e_1)$ est un sous-espace invariant de E. Comme θ est irréductible, $E = \mathrm{Vect}(e_1)$. □

Remarque 3.1. La première étape de cette preuve est le théorème de diagonalisation simultanée.

3.2 Groupe dual

Lorsque E est dimension 1, le groupe $\mathrm{GL}(E)$ est isomorphe à $\mathbb{K}^*$, par le morphisme

$$\left\{\begin{array}{ccc}\mathbb{K}^* & \longrightarrow & \mathrm{GL}(E) \\ \lambda & \longmapsto & \left\{\begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & \lambda x. \end{array}\right.\end{array}\right.$$

Définition 3.3. *Soit G un groupe. Les caractères de G sont les morphismes de groupes de G dans $\mathbb{C}^*$. L'ensemble des caractères de G est noté $\widehat{G}$.*

Lorsque $\mathbb{K} = \mathbb{C}$ et G est abélien, il s'agit donc des représentations irréductibles de G.

Proposition 3.4. *Soit G un groupe. Alors $\widehat{G}$ est un groupe abélien, avec le produit défini par*

$$\forall \lambda, \mu \in \widehat{G},\ \forall g \in G, \qquad \lambda\mu(g) = \lambda(g)\mu(g).$$

Ce groupe est appelé groupe dual de G.

Démonstration. Montrons d'abord qu'il s'agit bien d'une loi interne. Soient λ, $\mu \in \widehat{G}$. Alors $\lambda\mu$ prend bien ses valeurs dans $\mathbb{C}^*$. Pour tous $g, h \in G$,

$$\lambda\mu(gh) = \lambda(gh)\mu(gh) = \lambda(g)\lambda(h)\mu(g)\mu(h) = \lambda(g)\mu(g)\lambda(h)\mu(h) = \lambda\mu(g)\lambda\mu(h),$$

donc $\lambda\mu \in \widehat{G}$. Cette loi est clairement associative et commutative, avec pour élément neutre le caractère constant 1, qui est bien un morphisme de groupes de G dans $\mathbb{C}^*$. Si $\lambda \in \widehat{G}$, on définit $\mu : G \longrightarrow \mathbb{K}^*$ par

$$\mu(g) = \frac{1}{\lambda(g)}.$$

Comme $x \longmapsto \dfrac{1}{x}$ est un endomorphisme du groupe $\mathbb{C}^*$, par composition $\mu \in \widehat{G}$ et de manière évidente, $\lambda\mu = 1$. □

Théorème 3.5. *Soit G un groupe cyclique d'ordre n, engendré par un élément g. Alors $\widehat{G}$ est également un groupe cyclique d'ordre n, engendré par le caractère λ défini par*

$$\lambda(g^k) = \mathrm{e}^{\frac{2\mathrm{i}\pi k}{n}}.$$

Démonstration. Pour alléger l'écriture, on pose $\omega = \mathrm{e}^{\frac{2\mathrm{i}\pi}{n}}$. Soit $\mu \in \widehat{G}$. Alors pour tout $k \in \mathbb{Z}$, $\mu(g^k) = \mu(g)^k$: comme G est cyclique, μ est caractérisé par $\mu(g)$. De plus $g^n = e_G$, donc $\mu(g)^n = \mu(e_G) = 1$ et $\mu(g)$ est une racine n-ième de l'unité. Par suite, il existe un unique $k \in \{0, \ldots, n-1\}$ tel que $\mu(g) = \omega^k$. Alors

$$\mu(g) = \lambda(g)^k = \lambda^k(g),$$

donc $\mu = \lambda^k$. Les éléments de $\widehat{G}$ sont donc $\lambda^0, \ldots, \lambda^{n-1}$, ce qui démontre que $\widehat{G}$ est cyclique d'ordre n, engendré par λ. □

En conséquence, si G est cyclique d'ordre n, engendré par g, on connaît toutes ses représentations irréductibles : il y en a n, données par

$$\theta_k : \left\{\begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(\mathbb{C}) \\ g^l & \longmapsto & \left\{\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \mathrm{e}^{\frac{2\mathrm{i}\pi kl}{n}} x, \end{array}\right. \end{array}\right.$$

pour $0 \leqslant k < n$. En particulier, θ_0 est une représentation triviale.

Remarque 3.2. Si G est un groupe cyclique, alors $\widehat{G}$ est isomorphe à G. Ceci se généralise au cas de tous les groupes abéliens finis, par le théorème de Kronecker, que nous allons montrer dans le paragraphe suivant.

3.3 Théorème de Kronecker

Nous allons utiliser le groupe dual d'un groupe abélien fini pour démontrer le théorème de structure des groupes abéliens finis de Kronecker.

Définition 3.6. *Soit G un groupe fini. L'exposant de G est le maximum des ordres de ses éléments.*

Lemme 3.7. *Soit G un groupe abélien fini d'exposant n. Alors G possède un élément d'ordre n et tout élément de G est d'ordre divisant n.*

Démonstration. Première étape. Montrons que si g et h sont deux éléments de G d'ordre respectifs k et l premiers entre eux, alors xy est d'ordre kl. Soit $p \in \mathbb{Z}$ tel que $(xy)^p = e_G$, alors $x^p = y^{-p} \in \langle x \rangle \cap \langle y \rangle$. De plus, $H = \langle x \rangle \cap \langle y \rangle$, sous-groupe de $\langle x \rangle$ et de $\langle y \rangle$, est d'ordre divisant k et l par le théorème de Lagrange, donc d'ordre divisant le PGCD de k et l qui vaut 1 : $H = \{e_G\}$, donc $x^p = y^{-p} = e_G$. Par suite, k et l divisent p et, comme k et l sont premiers entre eux, kl divise p. Donc l'ordre de xy est divisible par kl. De plus,

$$(xy)^{kl} = x^{kl}y^{kl} = (x^k)^l(y^l)^k = e_G,$$

donc l'ordre de xy est kl.

Par une récurrence simple, on montre que si $x_1, \dots, x_p$ sont des éléments de G d'ordre respectifs $k_1, \dots, k_p$ deux-à-deux premiers entre eux, alors $x_1 \dots x_p$ est d'ordre $k_1 \dots k_p$.

Deuxième étape. Soit N le PPCM des ordres des éléments de G, qu'on décompose en produit de nombres premiers :

$$N = p_1^{\alpha_1} \dots p_m^{\alpha_m},$$

où les p_i sont des nombres premiers deux-à-deux distincts. Si $g \in G$, son ordre divise N, donc est de la forme

$$o(g) = p_1^{\alpha_1(g)} \dots p_m^{\alpha_m(g)}.$$

Il reste à montrer que N est l'exposant de G. Comme N est le PPCM des ordres des éléments de G, pour tout $i \in \{1, \dots, m\}$,

$$\alpha_i = \max\{\alpha_i(g) \mid g \in G\}.$$

Donc pour tout i, il existe un élément $g_i \in G$ tel que $\alpha_i(g) = \alpha_i$: $p_i^{\alpha_i}$ divise l'ordre de g_i. Alors l'élément $y_i = g_i^{\frac{o(g_i)}{p_i^{\alpha_i}}}$ est d'ordre $p_i^{\alpha_i}$. D'après la première étape, $y_1 \dots y_m$ est d'ordre N, qui est donc l'exposant de G. □

Lemme 3.8. *Soit G un groupe abélien fini, H un sous-groupe de G et $\chi \in \widehat{H}$. Il existe $\overline{\chi} \in \widehat{G}$ tel que $\overline{\chi}_{|H} = \chi$.*

Démonstration. On procède par récurrence sur $[G : H]$. Si $[G : H] = 1$, alors $G = H$ et on prend $\overline{\chi} = \chi$. Supposons maintenant $[G : H] > 1$ et le résultat vrai pour tout sous-groupe K de G tel que $[G : K] < [G : H]$ et tout caractère ξ' de K. Comme $H \neq G$, on choisit un élément $x \in G \setminus H$ et on considère le sous-groupe K de G engendré par H et par x. Alors $H \subsetneq K$, donc $[G : K] < [G : H]$. De plus, comme K est engendré par H et x, K/H est engendré par $\overline{x}$, donc est un groupe cyclique d'ordre noté r.

Montrons que tout élément de K s'écrit de façon unique hx^i, avec $h \in H$ et $i \in \{0, \dots, r-1\}$.

Existence. Soit $y \in K$. Comme K/H est cyclique d'ordre r, engendré par $\overline{x}$, il existe $i \in \{0, \dots, r-1\}$ tel que $\overline{y} = \overline{x}^r$. Alors $h = yx^{-r}$ est un élément de H et on obtient $y = hx^r$.

Unicité. Supposons $hx^i = kx^j$, avec $h, k \in H$ et $0 \leqslant i, j \leqslant r-1$. Dans K/H, $\overline{x}^i = \overline{x}^j$, donc $i = j$. Par suite, $h = k$.

Notons que $\overline{x}^r = \overline{e_G}$, donc $x^r \in H$: $\chi(x^r)$ est bien défini. On choisit $\zeta \in \mathbb{C}$ tel que $\zeta^r = \chi(x^r)$. On définit alors une application $\chi' : K \longrightarrow \mathbb{C}$ par $\chi'(hx^i) = \chi(h)\zeta^i$ pour tout $h \in H$ et tout $i \in \{0, \dots, r-1\}$. Par l'existence et l'unicité de l'écriture prouvées précédemment, ceci est une

application bien définie. Montrons qu'il s'agit d'un caractère de K. Soit $y = hx^i$ et $z = kx^j$ dans K. Soit $i + j = pr + s$ la division euclidienne de $i + j$ par r, avec $0 \leqslant s \leqslant r - 1$. Alors l'écriture unique de yz est

$$yz = hx^i kx^j = \underbrace{(hkx^{pr})}_{\in H} x^s,$$

donc

$$\begin{aligned}\chi'(yz) &= \chi(hkx^{pr})\zeta^s = \chi(h)\chi(k)\chi(x^r)^p\zeta^s = \chi(h)\chi(k)\zeta^{rp+s} = \chi(h)\zeta^i\chi(k)\zeta^j \\ &= \chi'(y)\chi'(z),\end{aligned}$$

car h, k et x^r sont dans H. Donc χ' est un caractère de K. Par l'hypothèse de récurrence, il existe un caractère $\overline{\chi}$ de G tel que $\overline{\chi}_{|K} = \chi'$. Alors $\overline{\chi}_{|H} = \chi'_{|H} = \chi$. □

Théorème 3.9. ***(Théorème de Kronecker***[8]***)*** *Soit G un groupe abélien fini non nul. Il existe des entiers $n_1, \ldots, n_k$ tous supérieurs ou égaux à 2 tels que $n_k \mid n_{k-1} \mid \ldots \mid n_1$ et*

$$G \approx \frac{\mathbb{Z}}{n_1\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}}.$$

Démonstration. On procède par récurrence sur $|G|$. Si $|G| = 2$, c'est évident, G est cyclique d'ordre 2. On suppose $|G| > 2$ et le résultat vrai pour tout groupe abélien H d'ordre $< |G|$. Soit n_1 l'exposant de G. Par le lemme 3.7, il existe un élément x de G d'ordre n_1. On considère le sous-groupe $H = \langle x \rangle$ de G. Si $G = H$, alors G est cyclique : on prend $k = 1$ et c'est terminé. Sinon, soient $\zeta = \mathrm{e}^{\frac{2i\pi}{n_1}}$ et $\chi : \langle x \rangle \longrightarrow \mathbb{C}^*$ le caractère du groupe cyclique H envoyant x sur ζ : c'est un isomorphisme de groupes de H dans le groupe $\mathbb{U}_{n_1}$ des racines n_1-ièmes de l'unité. Par le lemme 3.8, soit $\overline{\chi}$ un caractère de G prolongeant χ. Comme n_1 est l'exposant de G, pour tout $y \in G$, $y^{n_1} = e_G$, donc $\overline{\chi}(y)^{n_1} = 1$: $\overline{\chi}$ prend ses valeurs dans $\mathbb{U}_{n_1}$. On pose

$$\alpha : \left\{ \begin{array}{rcl} H \times \mathrm{Ker}(\overline{\chi}) & \longrightarrow & G \\ (h, k) & \longmapsto & hk. \end{array} \right.$$

Montrons que α est un homomorphisme de groupes. Soient (h, k) et $(h', k') \in H \times \mathrm{Ker}(\overline{\chi})$. Comme G est abélien,

$$\alpha((h, k)(h', k')) = \alpha(hh', kk') = hh'kk' = hkh'k' = \alpha(h, k)\alpha(h', k').$$

Montrons que α est injectif. Soit $(h, k) \in \mathrm{Ker}(\alpha)$. Alors $hk = e_G$, donc $h = k^{-1} \in \mathrm{Ker}(\overline{\chi})$. Par suite, comme $h \in H$, $\chi(h) = \overline{\chi}(h) = e_G$. Comme χ est injectif, $h = e_G$ et, en conséquence, $k = e_G$. Par suite, $\mathrm{Ker}(\alpha) = \{(e_G, e_G)\}$ et donc α est injectif.

Montrons que α est surjectif. Soit $g \in G$. Alors $\overline{\chi}(g) \in \mathbb{U}_{n_1} = \chi(H)$, donc il existe $h \in H$ tel que $\overline{\chi}(g) = \chi(h)$. Posons $k = h^{-1}g$. Alors

$$\overline{\chi}(k) = \overline{\chi}(h)^{-1}\overline{\chi}(g) = \chi(h)^{-1}\overline{\chi}(g) = e_G,$$

donc $k \in \mathrm{Ker}(\overline{\chi})$ et $g = hk = \alpha(h, k)$.

En conséquence, G est isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times \mathrm{Ker}(\overline{\chi})$. On peut appliquer le résultat à $\mathrm{Ker}(\overline{\chi})$, d'ordre $|G|/n_1 < |G|$: il existe des entiers $n_2, \ldots, n_k$ tels que $n_k \mid n_{k-1} \mid \ldots \mid n_2$ et

$$\mathrm{Ker}(\overline{\chi}) \approx \frac{\mathbb{Z}}{n_2\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{n_k\mathbb{Z}}.$$

Il ne reste plus qu'à montrer que n_2 divise n_1. Via l'isomorphisme précédent, $\mathrm{Ker}(\overline{\chi})$ contient un élément y d'ordre n_2. Comme n_1 est l'exposant de G, $y^{n_1} = e_G$ et par suite, $n_2 \mid n_1$. □

4 Caractères d'une représentation

Dans cette section, $\mathbb{K} = \mathbb{C}$.

8. Leopold Kronecker (1823–1891), mathématicien et logicien allemand.

4.1 Définition

Définition 4.1. *Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation d'un groupe fini G. Le caractère de cette représentation est l'application*

$$\chi : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \mathrm{Tr}(\theta(g)), \end{array} \right.$$

où Tr *désigne la trace.*

Proposition 4.2. *Soit χ le caractère d'une représentation $\theta : G \longrightarrow \mathrm{GL}(E)$ d'un groupe fini G.*

1. *$\chi(e_G) = \dim(E)$.*
2. *Si g, $h \in G$, alors $\chi(gh) = \chi(hg)$: on dit que χ est une fonction centrale.*
3. *Si $g \in G$, alors $\chi(g)$ est une somme de racines de l'unité.*
4. *Si $g \in G$, $\chi(g^{-1}) = \overline{\chi(g)}$.*

Démonstration.

1. $\theta(e_G) = \mathrm{Id}_E$, donc $\chi(e) = \mathrm{Tr}(\mathrm{Id}_E) = \dim(E)$.
2. $\chi(gh) = \mathrm{Tr}(\theta(gh)) = \mathrm{Tr}(\theta(g) \circ \theta(h)) = \mathrm{Tr}(\theta(h) \circ \theta(g)) = \chi(hg)$.
3. D'après le lemme 3.1, $\theta(g)$ est diagonalisable et ses valeurs propres sont des racines de l'unité. La trace de $\theta(g)$ étant la somme des valeurs propres de g, on obtient le résultat.
4. Comme $\theta(g^{-1}) = \theta(g)^{-1}$, $\chi(g^{-1})$ est la somme des valeurs propres de g^{-1}, c'est-à-dire la somme des inverses des valeurs propres de G. Ces nombres complexes étant des racines de l'unité, leurs inverses sont leurs conjugués et donc $\chi(g^{-1}) = \overline{\chi(g)}$. □

Définition 4.3. *Soit G un groupe fini. L'ensemble $\mathscr{C}(G)$ des fonctions centrales sur G est l'ensemble des applications $\psi : G \longrightarrow \mathbb{C}$ telles que pour tous $g, h \in G$, $\psi(gh) = \psi(hg)$. Il s'agit d'un espace vectoriel, pour la somme et la multiplication externe usuelle des applications de G dans $\mathbb{C}$. C'est également une algèbre, pour le produit usuel des applications de G dans $\mathbb{C}$.*

En particulier, les caractères des représentations de G sont dans $\mathscr{C}(G)$.

Proposition 4.4. *Soit G un groupe fini. Alors $\mathscr{C}(G)$ est de dimension le nombre de classes de conjugaison de G.*

Démonstration. Soit $f : G \longrightarrow \mathbb{C}$ une application quelconque. Montrons que $f \in \mathscr{C}(G)$ si, et seulement si, f est constante sur chacune des classes de conjugaison de G.

$\Longrightarrow$. Si ψ est centrale, alors pour tout $g, h \in G$,

$$\psi(ghg^{-1}) = \psi((gh)g^{-1}) = \psi(g^{-1}(gh)) = \psi(h),$$

donc ψ est constante sur les classes de conjugaison de G.

$\Longleftarrow$. Si ψ est constante sur les classes de conjugaison de G, pour tout $g, h \in G$,

$$\psi(gh) = \psi(ghgg^{-1}) = \psi(g(hg)g^{-1}) = \psi(hg).$$

Donc ψ est centrale.

Soient $C_1, \ldots, C_k$ les classes de conjugaison de G. Pour tout i, on pose

$$\delta_i : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \begin{cases} 1 \text{ si } x \in C_i, \\ 0 \text{ sinon.} \end{cases} \end{array} \right.$$

δ_i est constante sur chaque classe de conjugaison, donc appartient à $\mathscr{C}(G)$. Si $\psi \in \mathscr{C}(G)$, alors ψ s'écrit de façon unique

$$\psi = \sum_{i=1}^{k} a_i \delta_i,$$

où a_i est la valeur prise par ψ sur chacun des éléments de C_i. Donc $(\delta_i)_{1 \leqslant i \leqslant k}$ est une base de $\mathscr{C}(G)$, qui est donc de dimension k. □

Proposition 4.5. *Soient θ_1 et θ_2 deux représentations d'un même groupe G, de caractères respectifs χ_1 et χ_2. Le caractère de $\theta_1 \oplus \theta_2$ est $\chi_1 + \chi_2$.*

Démonstration. Soit $\mathscr{B}_1 = (e_1, \ldots, e_m)$ une base de l'espace E_1 de θ_1 et $\mathscr{B}_2 = (f_1, \ldots, f_n)$ une base de l'espace E_2 de θ_2. Alors

$$\mathscr{B} = ((e_1, 0), \ldots, (e_m, 0), (0, f_1), \ldots, (0, f_n))$$

est une base de $E_1 \times E_2$. Pour tout $g \in G$,

$$M_{\mathscr{B}}(\theta_1 \oplus \theta_2(g)) = \begin{pmatrix} M_{\mathscr{B}_1}(\theta_1(g)) & 0 \\ 0 & M_{\mathscr{B}_1}(\theta_2(g)) \end{pmatrix}.$$

En prenant la trace de cette matrice par blocs, en notant χ le caractère de $\theta_1 \oplus \theta_2$,

$$\chi(g) = \chi_1(g) + \chi_2(g). \qquad \square$$

Par la suite, on sera amené à chercher les caractères des représentations irréductibles d'un groupe G donné, ce qu'on appellera caractères irréductibles de G. La fin de ce paragraphe est consacrée à des résultats qui seront utiles pour effectuer cette recherche.

Proposition 4.6. *Soit $\theta :\longrightarrow \mathrm{GL}(E)$ une représentation d'un groupe fini, de caractère χ. Le caractère de la représentation duale θ^* est $\overline{\chi}$. De plus, si θ est irréductible, alors θ^* est irréductible.*

Démonstration. Soit $(e_1, \ldots, e_n)$ une base de E et $(e_1^*, \ldots, e_n^*)$ la base duale. Pour tout g, on note M_g la matrice de $\theta(g)$ dans la base $(e_1, \ldots, e_n)$. Comme $\theta^*(g) = \theta(g^{-1})^T$, la matrice de $\theta^*(g)$ dans la base $(e_1^*, \ldots, e_n^*)$ est $M_{g^{-1}}^T$. En prenant la trace de cette matrice,

$$\mathrm{Tr}(\theta^*(g)) = \mathrm{Tr}(M_{g^{-1}}^T) = \mathrm{Tr}(M_{g^{-1}}) = \chi(g^{-1}) = \overline{\chi(g)}.$$

Supposons θ irréductible. Soit $F' \subseteq E^*$ un sous-espace invariant de θ^*. On suppose que $F' \neq E^*$. On considère $F = \{x \in E \mid \forall f \in F', f(x) = 0\}$. Il s'agit d'un sous-espace de E (orthogonal de F'). Soit $(f_1, \ldots, f_k)$ une base de F', avec $k < n$. On obtient alors que pour tout $x \in E$,

$$x \in F \iff f_1(x) = \ldots = f_k(x) = 0.$$

En choisissant une base de E, ceci donne un système homogène de k équations à n inconnues. Comme $k < n$, il possède des solutions non nulles : autrement dit, $F \neq \{0_E\}$. Soient $x \in F$ et $g \in G$. Pour tout $f \in F'$,

$$f(\theta(g)(x)) = f \circ \theta(g)(x) = (\theta^*(g^{-1})(f))(x) = 0,$$

car $\theta^*(g^{-1})(f) \in F'$ et $x \in F$. Donc F est un sous-espace stable de θ. Comme θ est irréductible et que $F \neq \{0_E\}$, $F = E$. On obtient que pour tout $f \in F'$, pour tout $x \in E$, $f(x) = 0$, donc $f = 0_{E^*}$ et $F' = \{0_{E^*}\}$. Les seuls sous-espaces stables de θ^* sont $\{0_{E^*}\}$ et E^* : θ^* est irréductible. $\square$

En conséquence, si χ est un caractère irréductible d'un groupe G, son conjugué $\overline{\chi}$ également.

Proposition 4.7. *Soit G un groupe fini.*

1. *Soit $\lambda \in \widehat{G}$ un caractère de G. Alors λ est le caractère d'une représentation irréductible de G.*
2. *Soit χ le caractère d'une représentation $\theta : G \longrightarrow \mathrm{GL}(E)$ de G et soit $\lambda \in \widehat{G}$ un caractère de G. Alors $\lambda\chi$ est aussi le caractère d'une représentation de G. De plus, si θ est irréductible, alors $\lambda\chi$ est aussi le caractère d'une représentation irréductible de G.*

Démonstration. 1. On obtient une représentation de G de dimension 1 :

$$\begin{cases} G & \longrightarrow & \mathrm{GL}(\mathbb{C}) \\ g & \longmapsto & \begin{cases} \mathbb{C} & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \lambda(g)x. \end{cases} \end{cases}$$

Comme elle est de dimension 1, elle est irréductible et son caractère est λ.

2. On considère l'application

$$\theta' : \begin{cases} G & \longrightarrow & \mathrm{GL}(E) \\ g & \longmapsto & \begin{cases} E & \longrightarrow & E \\ x & \longmapsto & \lambda(g)\theta(g)(x). \end{cases} \end{cases}$$

Il s'agit d'une représentation de G, de caractère $\lambda\chi$. De plus, si F est un sous-espace de E, c'est un sous-espace invariant de θ si, et seulement si, c'est un sous-espace invariant de θ', car λ ne prend pas la valeur 0. Par suite, si θ est irréductible, alors θ' aussi (et réciproquement). □

Remarque 4.1. On obtient ainsi une action du groupe des caractères $\widehat{G}$ sur l'ensemble des caractères des représentations irréductibles de G par multiplication.

Proposition 4.8. *Soient G un groupe fini, H un sous-groupe distingué de G et $\theta : G/H \longrightarrow \mathrm{GL}(E)$ une représentation irréductible de G/H, de caractère χ. On note $\pi : G \longrightarrow G/H$ la surjection canonique. Alors $\theta \circ \pi$ est une représentation irréductible de G. En notant son caractère $\tilde{\chi}$, pour tout $g \in G$,*

$$\tilde{\chi}(g) = \chi(\pi(g)).$$

Démonstration. Par composition, $\theta \circ \pi : G \longrightarrow \mathrm{GL}(E)$ est un morphisme de groupes, donc une représentation de G. En appliquant la trace, on obtient la formule pour $\tilde{\chi}$. Soit F un sous-espace invariant de $\theta \circ \pi$. Pour tout $g \in G$, $\theta(\pi(g))(F) \subseteq F$, donc F est un sous-espace invariant de θ. Comme θ est irréductible, $F = \{0_E\}$ ou E, donc $\theta \circ \pi$ est irréductible. □

Ainsi, les caractères irréductibles des quotients de G permettent de trouver certains caractères irréductibles de G.

4.2 Lemme de Schur et applications

Théorème 4.9. ***(Lemme de Schur)*** *Soient $\theta : G \longrightarrow \mathrm{GL}(E)$ et $\theta' : G \longrightarrow \mathrm{GL}(E')$ deux représentations irréductibles d'un groupe fini G. Soit $\psi : E \longrightarrow E'$ un morphisme de représentations de θ vers θ'.*

1. *Soit $\psi = 0$, soit ψ est un isomorphisme.*
2. *Si $\theta = \theta'$, alors $\psi = \lambda \mathrm{Id}_E$ pour un certain nombre complexe λ.*

Démonstration. 1. Comme ψ est un morphisme de représentations, $\mathrm{Ker}(\psi)$ est un sous-espace invariant de E. Comme θ est irréductible, $\mathrm{Ker}(\psi) = \{0_E\}$ ou E. Si $\mathrm{Ker}(\psi) = E$, alors $\psi = 0$. Sinon, ψ est injectif. Comme E est non nul, $\mathrm{Im}(\psi)$ est un sous-espace invariant non nul de E'. Comme θ' est irréductible, $\mathrm{Im}(\psi) = F$ et ψ est un isomorphisme.

2. Supposons $\theta = \theta'$. Comme $\mathbb{K} = \mathbb{C}$, ψ possède une valeur propre λ. Alors E_λ est un sous-espace invariant de θ, d'après la proposition 1.8. Par définition de λ, $E_\lambda \neq \{0_E\}$. Comme θ est irréductible, $E_\lambda = E$ et donc $\psi = \lambda \mathrm{Id}_E$. □

Corollaire 4.10. *Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ et $\theta' : G \longrightarrow \mathrm{GL}(E')$ deux représentations irréductibles d'un même groupe fini G et soit $\psi : E \longrightarrow E'$ une application linéaire quelconque. On définit une application linéaire $\psi_0 : E \longrightarrow E'$ par*

$$\psi_0 = \frac{1}{|G|} \sum_{g \in G} \theta'(g^{-1}) \circ \psi \circ \theta(g).$$

1. *Si θ et θ' ne sont pas isomorphes, alors $\psi_0 = 0$.*

2. *Si $\theta = \theta'$, alors* $\psi_0 = \dfrac{\mathrm{Tr}(\psi)}{\dim(E)}\mathrm{Id}_E$.

Démonstration. Montrons que ψ_0 est un morphisme de représentations. Soit $h \in G$.

$$\begin{aligned}
\psi_0 \circ \theta(h) &= \frac{1}{|G|}\sum_{g\in G} \theta'(g^{-1}) \circ \psi \circ \theta(g) \circ \theta(h) \\
&= \frac{1}{|G|}\sum_{g\in G} \theta'(g^{-1}) \circ \psi \circ \theta(gh) \\
&= \frac{1}{|G|}\sum_{k\in G} \theta'(hk^{-1}) \circ \psi \circ \theta(k) \\
&= \frac{1}{|G|}\sum_{k\in G} \theta'(h) \circ \theta'(k^{-1}) \circ \psi \circ \theta(k) \\
&= \theta'(h) \circ \left(\frac{1}{|G|}\sum_{k\in G} \theta'(k^{-1}) \circ \psi \circ \theta(k)\right) \\
&= \theta'(h) \circ \psi_0.
\end{aligned}$$

On a effectué le changement d'indice $k = gh$, de sorte que $g^{-1} = hk^{-1}$. Par le lemme de Schur, ψ_0 est nul ou est un isomorphisme. En particulier, si θ et θ' ne sont pas isomorphes, $\psi_0 = 0$.

Supposons maintenant $\theta = \theta'$. Par le lemme de Schur, $\psi_0 = \lambda \mathrm{Id}_E$, pour un certain $\lambda \in \mathbb{C}$. Calculons la trace de ψ_0. D'une part,

$$\mathrm{Tr}(\psi_0) = \mathrm{Tr}(\lambda \mathrm{Id}_E) = \lambda \dim(E).$$

D'autre part, pour tout $g \in G$, l'application $\theta(g^{-1}) \circ \psi \circ \theta(g) = \theta(g)^{-1} \circ \psi \circ \theta(g)$ est conjuguée à ψ, et par suite possède la même trace. En conséquence,

$$\mathrm{Tr}(\psi_0) = \frac{1}{|G|}\sum_{g\in G} \mathrm{Tr}(\psi) = \mathrm{Tr}(\psi),$$

ce qui implique le résultat annoncé. □

4.3 Orthonormalité des caractères irréductibles

Définition 4.11. *Soit G un groupe fini. L'espace $\mathscr{C}(G)$ est muni d'une forme hermitienne définie positive donnée par*

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

Démonstration. Il est immédiat que $\langle -, - \rangle$ est hermitienne. Pour tout $\phi \in \mathscr{C}(G)$,

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

donc $\langle -, - \rangle$ est définie positive. □

Proposition 4.12. *Soient $\theta : G \longrightarrow \mathrm{GL}(E)$ et $\theta' : G \longrightarrow \mathrm{GL}(E')$ deux représentations irréductibles de G, de caractères respectifs χ et χ'.*

1. *Si θ et θ' ne sont pas isomorphes, $\langle \chi', \chi \rangle = 0$.*
2. *Si θ et θ' sont isomorphes, alors $\chi = \chi'$ et $\langle \chi', \chi \rangle = 1$.*

Démonstration. On choisit des bases $\mathscr{B}$ et $\mathscr{B}'$ de E et E' et on écrit les matrices de $\theta(g)$ et $\theta'(g)$ dans ces bases :

$$M_{\mathscr{B}}(\theta(g)) = (a_{i,j}(g))_{1\leqslant i,j\leqslant n}, \qquad M_{\mathscr{B}'}(\theta'(g)) = (a'_{i,j}(g))_{1\leqslant i,j\leqslant n'}.$$

Les coefficients $a_{i,j}$ et $a'_{i,j}$ sont des applications de G dans $\mathbb{C}$. Soit $\psi : E \longrightarrow E'$ une application linéaire quelconque. On pose $M_{\mathscr{B},\mathscr{B}'}(\psi) = (x_{i,j})_{\substack{1\leqslant i\leqslant n' \\ 1\leqslant j\leqslant n}}$. On pose

$$\psi_0 = \frac{1}{|G|}\sum_{g\in G} \theta'(g^{-1}) \circ \psi \circ \theta(g).$$

Le coefficient i,j de la matrice de ψ_0 dans ces bases est

$$y_{i,j} = \frac{1}{|G|}\sum_{g\in G}\sum_{k=1}^{n'}\sum_{l=1}^{n} a'_{i,k}(g^{-1})x_{k,l}a_{l,j}(g).$$

1. Supposons θ et θ' non isomorphes. D'après le corollaire 4.10, pour tout i,j, $y_{i,j} = 0$. On choisit ψ de sorte que seul le coefficient $x_{k,l}$ soit non nul et égal à 1 et ce, successivement pour tout couple (k,l). On obtient

$$\forall i,k \in \{1,\dots,n'\},\ \forall j,l \in \{1,\dots,n\}, \qquad \frac{1}{|G|}\sum_{g\in G} a'_{i,k}(g^{-1})a_{l,j}(g) = 0.$$

En sommant pour $i = k$ et $l = j$,

$$\begin{aligned} 0 &= \frac{1}{|G|}\sum_{g\in G}\sum_{i=1}^{n'}\sum_{j=1}^{n} a'_{i,i}(g^{-1})a_{j,j}(g) = \frac{1}{|G|}\sum_{g\in G}\chi'(g^{-1})\chi(g) \\ &= \frac{1}{|G|}\sum_{g\in G}\overline{\chi'(g)}\chi(g) = \langle\chi',\chi\rangle. \end{aligned}$$

2. Supposons θ et θ' isomorphes. Soit $\xi : E \longrightarrow E'$ un isomorphisme. Pour tout $g \in G$, $\theta'(g)\circ\xi = \xi\circ\theta(g)$, donc $\theta(g) = \xi^{-1}\circ\theta'(g)\circ\xi$. Comme $\theta(g)$ et $\theta'(g)$ sont conjugués, ils ont la même trace, donc $\chi(g) = \chi'(g)$.

Par suite, $\langle\chi',\chi\rangle = \langle\chi,\chi\rangle$. On est ramené à $\theta = \theta'$ et on choisit alors $\mathscr{B} = \mathscr{B}'$. On choisit ψ de sorte que seul le coefficient $x_{k,l}$ soit non nul et égal à 1 et ce, successivement pour tout couple (k,l). On obtient, en utilisant le corollaire 4.10 :

$$\begin{aligned} \forall i,j,k,l \in \{1,\dots,n\}, \qquad \frac{1}{|G|}\sum_{g\in G} a_{i,k}(g^{-1})a_{l,j}(g) &= \begin{cases} \dfrac{\mathrm{Tr}(\psi)}{n} \text{ si } i = j, \\ 0 \text{ sinon,} \end{cases} \\ &= \begin{cases} \dfrac{1}{n} \text{ si } i = j \text{ et } k = l, \\ 0 \text{ sinon.} \end{cases} \end{aligned}$$

En sommant sur $i = k$ et $j = l$, on obtient

$$\langle\chi,\chi\rangle = \frac{1}{|G|}\sum_{g\in G}\sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,i}(g^{-1})a_{j,j}(g) = \sum_{i=1}^{n}\frac{1}{n} = 1. \qquad \square$$

Autrement dit, la famille des caractères des représentations irréductibles de G forment une famille orthonormale de $\mathscr{C}(G)$. Elle est donc libre et il y en a donc au plus $\dim(\mathscr{C}(G))$, c'est-à-dire le nombre de classes de conjugaison de G.

Théorème 4.13. *1. Soit $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation d'un groupe fini G, de caractère χ. On la décompose en sous-représentations irréductibles par le théorème de Maschke :*

$$E = E_1 \oplus \ldots \oplus E_k.$$

Pour tout i, posons $\theta_i = \theta_{|E_i}$. Soit θ' une représentation irréductible de G, de caractère χ'. Le nombre de θ_i isomorphe à θ' est $\langle\chi',\chi\rangle$. En particulier, il ne dépend pas de la décomposition choisie.

2. *Soient θ et θ' deux représentations d'un même groupe fini. Alors θ et θ' sont isomorphes si, et seulement si, leurs caractères sont égaux.*

Démonstration. 1. Alors θ est isomorphe à $\theta_1 \oplus \ldots \oplus \theta_k$. En notant χ_i le caractère de θ_i, le caractère de θ est $\chi = \chi_1 + \ldots + \chi_k$. Donc

$$\langle \chi', \chi \rangle = \langle \chi', \chi_1 \rangle + \ldots + \langle \chi', \chi_k \rangle.$$

D'autre part, $\langle \chi', \chi_i \rangle$ vaut 1 si θ' est isomorphe à θ_i et 0 sinon, d'où le résultat.

2. Si θ et θ' sont isomorphes, alors elles ont le même caractère. Réciproquement, si θ et θ' ont le même caractère $\chi = \chi'$, décomposons θ et θ' en représentations irréductibles. En notant $\theta_1, \ldots, \theta_k$ les différentes représentations irréductibles qui apparaissent dans ces décompositions, il existe des entiers $a_1, \ldots, a_k$ et $b_1, \ldots, b_k$, éventuellement nuls, tels que

$$\theta \approx \theta_1^{a_1} \oplus \ldots \oplus \theta_k^{a_k}, \qquad \theta' \approx \theta_1^{b_1} \oplus \ldots \oplus \theta_k^{b_k}.$$

D'après le premier point, en notant χ_i le caractère de θ_i, on obtient

$$a_i = \langle \chi_i, \chi \rangle = \langle \chi_i, \chi' \rangle = b_i.$$

Donc θ et θ' sont isomorphes. □

La connaissance des représentations irréductibles d'un groupe fini G permet donc de connaître toutes les représentations de G à isomorphisme près. De plus, ces représentations irréductibles sont en nombre fini, inférieur ou égal au nombre de classes de conjugaison de G. On montrera dans le théorème 4.17 qu'il s'agit en fait toujours d'une égalité.

Corollaire 4.14. *Soit θ une représentation d'un groupe fini G, de caractère χ. Alors θ est irréductible si, et seulement si $\langle \chi, \chi \rangle = 1$.*

Démonstration. Soient $\theta_1, \ldots, \theta_k$ les différentes représentations irréductibles de G, à isomorphisme près. Leurs caractères sont notés $\chi_1, \ldots, \chi_k$. Il existe des entiers $a_1, \ldots, a_k$, uniques tels que

$$\theta \approx \theta_1^{a_1} \oplus \ldots \oplus \theta_k^{a_k}.$$

Alors $\chi = a_1\chi_1 + \ldots + a_k\chi_k$. Comme la famille $(\chi_i)_{1 \leqslant i \leqslant k}$ est orthonormale, $\langle \chi, \chi \rangle = a_1^2 + \ldots + a_k^2$. Donc $\langle \chi, \chi \rangle = 1$ si, et seulement si, tous les a_i sont nuls à l'exception d'un seul valant 1, autrement dit si et seulement si θ est irréductible. □

4.4 Représentation régulière

Lemme 4.15. *Soient G un groupe fini, λ une fonction centrale sur G et $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation irréductible de G, de caractère χ. On considère $\psi : E \longrightarrow E$, définie par*

$$\psi = \sum_{g \in G} \lambda(g)\theta(g).$$

Alors

$$\psi = \frac{|G|}{\dim(E)} \langle \overline{\chi}, \lambda \rangle \mathrm{Id}_E.$$

Démonstration. Soit $h \in G$.

$$\begin{aligned}
\psi \circ \theta(h) &= \sum_{g \in G} \lambda(g)\theta(g) \circ \theta(h) = \sum_{g \in G} \lambda(g)\theta(gh) = \sum_{k \in G} \lambda(kh^{-1})\theta(k) \\
&= \sum_{k \in G} \lambda(h^{-1}k)\theta(k) = \sum_{l \in G} \lambda(l)\theta(hl) = \sum_{l \in G} \lambda(l)\theta(h) \circ \theta(l) \\
&= \theta(h) \circ \left(\sum_{l \in G} \lambda(g)\theta(l) \right) \\
&= \theta(h) \circ \psi,
\end{aligned}$$

avec les changements d'indice $gh = k$ puis $l = h^{-1}k$. Donc ψ est un morphisme de représentations. Par le lemme de Schur, comme θ est irréductible, $\psi = a\mathrm{Id}_E$ pour un certain scalaire a. Calculons la trace de ψ :

$$a\dim(E) = \mathrm{Tr}(\psi) = \sum_{g\in G} \lambda(g)\chi(g) = \sum_{g\in G} \overline{\overline{\chi}}(g)\lambda(g) = |G|\langle\overline{\chi}, \lambda\rangle. \qquad \square$$

Définition 4.16. *Soit G un groupe fini et E_{reg} un espace vectoriel ayant une base $(x_h)_{h\in G}$ indexée par les éléments de G. On définit une représentation de G en posant*

$$\forall g, h \in G, \qquad \theta_{\mathrm{reg}}(g)(x_h) = x_{gh}.$$

Cette représentation s'appelle représentation régulière de G et son caractère est noté χ_{reg}.

Démonstration. Notons que θ_{reg} est bien définie par linéarité. Soit $h \in G$.

$$\theta_{\mathrm{reg}}(e_G)(x_h) = x_{e_G h} = x_h,$$

donc $\theta_{\mathrm{reg}}(e_G) = \mathrm{Id}_E$.

Soient $g, h \in G$. Pour tout $k \in G$,

$$\theta_{\mathrm{reg}}(gh)(x_k) = x_{(gh)k} = x_{g(hk)} = \theta_{\mathrm{reg}}(g) \circ \theta_{\mathrm{reg}}(h)(x_k),$$

donc $\theta_{\mathrm{reg}}(gh) = \theta_{\mathrm{reg}}(g) \circ \theta_{\mathrm{reg}}(h)$. En conséquence, θ_{reg} est une représentation de G. $\square$

Théorème 4.17. *Soit G un groupe fini. Les caractères des représentations irréductibles de G forment une base orthonormale de G. Il y en a donc exactement autant que de classes de conjugaison de G.*

Démonstration. On sait déjà que les caractères irréductibles, que l'on note $\chi_1, \ldots, \chi_k$, forment une famille orthonormale. Il reste à montrer que c'est une famille génératrice de $\mathscr{C}(G)$. Pour cela, il suffit de montrer que l'orthogonal du sous-espace $\mathrm{Vect}(\chi_1, \ldots, \chi_k)$ est nul. Soit donc une fonction centrale λ, orthogonale à $\chi_1, \ldots, \chi_k$. Si χ est un caractère irréductible, alors $\overline{\chi}$ également (proposition 4.6). Par le lemme 4.15, l'application ψ associée à λ est nulle pour toute représentation irréductible θ, car par hypothèse $\langle\overline{\chi}, \lambda\rangle = 0$ si χ est le caractère de θ. En sommant, cette application est aussi nulle pour la représentation régulière. On trouve, pour $x = x_{e_G}$,

$$0 = \psi(x) = \sum_{g\in G} \lambda(g)\theta_{\mathrm{reg}}(g)(x_{e_G}) = \sum_{g\in G} \lambda(g)x_g.$$

Comme $(x_g)_{g\in G}$ est une base de E, pour tout $g \in G$, $\lambda(g) = 0$. Donc λ est nul. $\square$

Remarque 4.2. Les représentations irréductibles de G sont donc en bijection avec les classes de conjugaison de G. À l'heure actuelle, aucune bijection « naturelle » n'est connue, hormis des cas très particuliers (groupes symétriques).

Proposition 4.18. *Soit G un groupe fini.*

1. *Le caractère χ_{reg} de la représentation régulière de G est donné par*

$$\chi_{\mathrm{reg}}(g) = \begin{cases} |G| \text{ si } g = e_G, \\ 0 \text{ sinon.} \end{cases}$$

2. *Soit θ une représentation irréductible de G. Alors θ apparaît dans la décomposition de la représentation régulière de G exactement $\deg(\theta)$ fois.*
3. *Soient $\theta_1, \ldots \theta_k$ les représentations irréductibles de G, $n_1, \ldots, n_k$ leurs degrés et $\chi_1, \ldots, \chi_k$ leurs caractères. Alors*

$$\forall g \in G \setminus \{e_G\}, \qquad \sum_{i=1}^{k} n_i\chi_i(g) = 0 \qquad \text{et} \qquad \sum_{i=1}^{n} n_i^2 = |G|.$$

Démonstration. 1. $\chi_{\text{reg}}(e_G) = \dim(E_{\text{reg}}) = |G|$. Si $g \neq e_G$, la matrice de $\theta(g)$ dans la base $(x_h)_{h\in G}$ est une matrice de permutation dont la diagonale est entièrement nulle, donc $\text{Tr}(\theta(g)) = \chi_{\text{reg}}(g) = 0$.

2. Le nombre de fois où θ apparaît dans la décomposition de la représentation régulière est

$$\langle \chi, \chi_{\text{reg}} \rangle = \frac{1}{|G|} \sum_{g\in G} \overline{\chi(g)}\chi_{\text{reg}}(g) = \overline{\chi(e_G)} = \deg(\theta).$$

3. En conséquence, la décomposition de la représentation régulière est

$$\theta_1^{n_1} \oplus \ldots \oplus \theta_k^{n_k},$$

donc $\chi_{\text{reg}} = n_1\chi_1 + \ldots + n_k\chi_k$. On trouve directement les résultats annoncés en évaluant en $g \neq e_G$ et en e_G. □

4.5 Noyaux des représentations

Lemme 4.19. *Soient G un groupe fini et $\theta : G \longrightarrow \text{GL}(E)$ une représentation irréductible de G de caractère χ. Alors*

$$\text{Ker}(\theta) = \{g \in G \mid \chi(g) = \dim(E)\}.$$

Démonstration. Soit $g \in \text{Ker}(\theta)$. Alors $\chi(g) = \text{Tr}(\theta(g)) = \text{Tr}(\text{Id}_E) = \dim(E)$.

Soit $g \in G$ tel que $\chi(g) = \dim(E)$. On note $n = \dim(E)$ et $\lambda_1, \ldots, \lambda_n$ les valeurs propres de $\theta(g)$. Par le lemme 3.1, $\theta(g)$ est diagonalisable et $\lambda_1, \ldots, \lambda_n$ sont des racines n-ièmes de l'unité. De plus, par hypothèse,

$$|\lambda_1| + \ldots + |\lambda_n| = n = \text{Tr}(\theta(g)) = \lambda_1 + \ldots + \lambda_n = |\lambda_1 + \ldots + \lambda_n|.$$

Par le cas d'égalité dans l'inégalité triangulaire, $\lambda_1, \ldots, \lambda_n$ sont positivement colinéaires. Comme elles sont toute de module 1, $\lambda_1 = \ldots = \lambda_n$. Comme leur somme vaut n,

$$\lambda_1 = \ldots = \lambda_n = 1.$$

Comme $\theta(g)$ est diagonalisable, $\theta(g) = \text{Id}_E$ et donc $g \in \text{Ker}(\theta)$. □

Lemme 4.20. *Soient $\theta_1, \ldots, \theta_k$ des représentations d'un groupe fini G. Alors*

$$\text{Ker}(\theta_1 \oplus \ldots \oplus \theta_k) = \bigcap_{i=1}^{k} \text{Ker}(\theta_i).$$

Démonstration. On note E_i l'espace de θ_i. Soit $g \in G$. Alors

$$\begin{aligned}
&g \in \text{Ker}(\theta_1 \oplus \ldots \oplus \theta_k) \\
&\iff \forall (x_1 \ldots, x_k) \in E_1 \times \ldots \times E_k,\ (\theta_1(g)(x_1), \ldots, \theta_k(g)(x_k)) = (x_1, \ldots, x_k) \\
&\iff \forall i \in \{1, \ldots, k\},\ \theta_i(g) = \text{Id}_{E_i} \\
&\iff \forall i \in \{1, \ldots, k\},\ g \in \text{Ker}(\theta_i) \\
&\iff g \in \bigcap_{i=1}^{k} \text{Ker}(\theta_i).
\end{aligned}$$

□

Proposition 4.21. *Soient G un groupe et H un sous-groupe distingué de G. Il existe des représentations irréductibles $\theta_1, \ldots, \theta_k$ de G telles que*

$$H = \bigcap_{i=1}^{k} \text{Ker}(\theta_i).$$

Démonstration. Soit E un espace vectoriel possédant une base $(e_{\overline{g}})_{\overline{g}\in G/H}$ indexée par les éléments de G/H. On définit alors une représentation $\theta : G \longrightarrow \mathrm{GL}(E)$ par

$$\forall g \in G,\ \forall \overline{h} \in G/H, \qquad \theta(g)(e_{\overline{h}}) = e_{\overline{gh}}.$$

Si $g \in H$, alors pour tout $\overline{h} \in G/H$,

$$\theta(g)(e_{\overline{h}}) = e_{\overline{gh}} = e_{\overline{h}},$$

donc $H \subseteq \mathrm{Ker}(\theta)$. Si $g \in \mathrm{Ker}(\theta)$, alors

$$e_{\overline{g}} = \theta(g)(e_{\overline{e_G}}) = e_{\overline{e_G}},$$

d'où $\overline{g} = \overline{e_G}$ et $g \in H$: nous avons montré que $\mathrm{Ker}(\theta) = H$. D'après le théorème de Maschke, il existe des représentations irréductibles $\theta_1, \ldots, \theta_k$ de G telles que θ est isomorphe à $\theta_1 \oplus \ldots \oplus \theta_k$. Alors, par le lemme 4.20,

$$\mathrm{Ker}(\theta_1 \oplus \ldots \oplus \theta_k) = \bigcap_{i=1}^{k} \mathrm{Ker}(\theta_i) = \mathrm{Ker}(\theta) = H. \qquad \square$$

Corollaire 4.22. *Soit G un groupe fini non nul.*

1. *Soit θ une représentation de G, de caractère χ. Alors cette représentation est fidèle si, et seulement si, $\chi(g) \neq \chi(e_G)$ pour tout $g \in G \setminus \{e_G\}$.*
2. *G est un groupe simple si, et seulement si, pour tout caractère irréductible χ de G distinct du caractère trivial et pour tout $g \in G \setminus \{e_G\}$, $\chi(g) \neq \chi(e_G)$.*

Démonstration. 1. C'est une conséquence directe du lemme 4.19.

2. Supposons G simple. Soit θ une représentation irréductible de G, non triviale. Alors $\mathrm{Ker}(\theta)$ est un sous-groupe distingué de G, différent de G. Comme G est simple, $\mathrm{Ker}(\theta) = \{e_G\}$, donc θ est fidèle. On conclut avec le premier point.

Supposons G non simple. Soit alors H un sous-groupe distingué non trivial de G. D'après la proposition 4.21, il existe des représentations irréducibles $\theta_1, \ldots, \theta_k$ de G telles que

$$H = \bigcap_{i=1}^{k} \mathrm{Ker}(\theta_i).$$

Comme H est non trivial, au moins l'une de ces représentations irréductibles possède un noyau non trivial. Cette représentation θ_i n'est donc pas triviale et pour tout $h \in H$, en notant χ_i son caractère, $\chi_i(h) = \chi_i(e_G)$. $\square$

5 Exemples de tables de caractères

On cherche maintenant tous les caractères irréductibles d'un groupe fini G donné. Leurs valeurs sont données dans une table, appelée table des caractères de G.

Remarque 5.1. Chaque groupe possède une représentation triviale de degré 1, qui est donc irréductible. Chaque groupe a donc un caractère irréductible χ_T valant 1 sur tous les éléments du groupe.

5.1 Les groupes cycliques

Soit G un groupe cyclique d'ordre n. D'après la proposition 3.2, ses représentations irréductibles sont de dimension 1 et ses caractères irréductibles sont les éléments de $\widehat{G}$. D'après le

théorème 3.5, ce groupe $\widehat{G}$ est cyclique, ce qui détermine la table des caractères. En notant x un générateur de G, on obtient la table de caractères suivante, où $\omega = \mathrm{e}^{\frac{2i\pi}{n}}$:

	e_G	x	x^2	$\dots$	x^{n-1}
T	1	1	1	$\dots$	1
χ	1	ω	ω^2	$\dots$	ω^{n-1}
χ^2	1	ω^2	ω^4	$\dots$	$\omega^{2(n-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
χ^{n-1}	1	ω^{n-1}	$\omega^{2(n-1)}$	$\dots$	$\omega^{(n-1)^2}$

On peut noter que la matrice sous-jacente à cette table est une matrice de Vandermonde [9].

5.2 Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Ce groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ étant abélien, toutes ses représentation irréductibles sont de dimension 1 et ses caractères irréductibles sont les éléments du groupe $\widehat{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$, au nombre de 4. Si χ_1 et χ_2 sont deux éléments de $\widehat{\mathbb{Z}/2\mathbb{Z}}$, on obtient un élément de $\widehat{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$ par multiplication :

$$\forall (x_1, x_2) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad \chi_1 \cdot \chi_2(x_1, x_2) = \chi_1(x_1)\chi_2(x_2).$$

Ceci permet de définir quatre éléments de $\widehat{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$ et donc de trouver les quatre caractères de G à partir des deux caractères de $\mathbb{Z}/2\mathbb{Z}$. Les caractères de $\mathbb{Z}/2\mathbb{Z}$ sont donnés dans la table suivante :

	$\overline{0}$	$\overline{1}$
T	1	1
χ	1	-1

On obtient la table des caractères de G :

	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$
$T \cdot T$	1	1	1	1
$T \cdot \chi$	1	-1	1	-1
$\chi \cdot T$	1	1	-1	-1
$\chi \cdot \chi$	1	-1	-1	1

On peut remarquer que ce groupe n'a aucune représentation irréductible fidèle.

Cette méthode se généralise à tous les produits cartésiens de groupes cycliques et donc à tous les groupes abéliens par le théorème de Kronecker et le théorème 3.2.

5.3 Le groupe symétrique $\mathfrak{S}_3$

Il y a trois classes de conjugaison dans $\mathfrak{S}_3$:
— La classe de conjugaison de Id_3, réduite à un singleton.
— Une classe de conjugaison formée des trois transpositions (12), (13) et (23).
— La classe de conjugaison formée des deux 3-cycles (123) et (132).

Il y a donc trois représentations irréductibles. La représentation triviale en est une, ainsi que la représentation signature, de dimension 1, correspondant au caractère signature de $\mathfrak{S}_3$. La table des caractères a donc la forme suivante :

	Id_1	$(12)_3$	$(123)_2$
T	1	1	1
ε	1	-1	1
χ	a	b	c

9. Alexandre-Théophile Vandermonde (1745–1796), mathématicien français qui semble-t-il n'a jamais étudié les matrices qui portent son nom.

Les petits indices correspondent au cardinal de chaque classe de conjugaison. D'après la proposition 4.18,

$$1^2 + 1^2 + a^2 = 6,$$

donc $a = 2$. On calcule enfin b et c utilisant l'orthonormalité des caractères irréductibles :

$$\begin{cases} 0 = 6\langle T, \chi\rangle = 2 + 3b + 2c, \\ 0 = 6\langle \varepsilon, \chi\rangle = 2 - 3b + 2c \end{cases} \iff \begin{cases} b = 0, \\ c = -1. \end{cases}$$

On obtient finalement

	Id_1	$(12)_3$	$(123)_2$
T	1	1	1
ε	1	-1	1
St	2	0	-1

On a trouvé le caractère de la troisième représentation irréductible mais on ne la connaît pas explicitement pour l'instant. Pour la trouver, on s'aide de la représentation de $\mathfrak{S}_3$ par permutations : $E = \mathbb{C}^3$ et en notant (e_1, e_2, e_3) la base canonique de E, $\sigma.e_i = e_{\sigma(i)}$. Matriciellement, Id, (12) et (123) sont représentés par les matrices de permutations

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Le caractère de cette représentation est donc donné par

$$\chi(\mathrm{Id}) = 3, \qquad \chi((12)) = 1, \qquad \chi((123)) = 0.$$

Donc

$$\begin{aligned} \langle \chi_T, \chi\rangle &= \frac{1.3 + 3.1.1 + 0}{6} = 1, \\ \langle \chi_S, \chi\rangle &= \frac{1.3 - 3.1.1 + 0}{6} = 0, \\ \langle \chi_{St}, \chi\rangle &= \frac{2.3 + 0 + 0}{6} = 1. \end{aligned}$$

Par suite, la décomposition de θ est $T \oplus St$. Cette représentation contient donc un sous-espace E_T invariant isomorphe à T et un autre noté E_{St}, isomorphe à St. Décrivons les explicitement. Pour tout $\sigma \in \mathfrak{S}_3$,

$$\theta(\sigma)(e_1 + e_2 + e_3) = e_{\sigma(1)} + e_{\sigma(2)} + e_{\sigma(3)} = e_1 + e_2 + e_3$$

et on en déduit que $E_T = \mathrm{Vect}(e_1 + e_2 + e_3)$. On considère la forme linéaire

$$f : \left\{ \begin{array}{rcl} E & \longrightarrow & \mathbb{C} \\ \lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3 & \longmapsto & \lambda_1 + \lambda_2 + \lambda_3. \end{array} \right.$$

Pour tout $\sigma \in \mathfrak{S}_3$, pour tout $\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3 \in E$,

$$\begin{aligned} f \circ \theta(\sigma)(\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3) &= f(\lambda_1 e_{\sigma(1)} + \lambda_2 e_{\sigma(2)} + \lambda_3 e_{\sigma(3)}) \\ &= \lambda_1 + \lambda_2 + \lambda_3 \\ &= f(\lambda_1 e_1 + \lambda_2 e_2 + \lambda_3 e_3), \end{aligned}$$

donc f est un morphisme de représentations de θ vers la représentation triviale. Son noyau E_{St} est une sous-représentation de θ de dimension 2. De plus, dans la base $(e_1 - e_2, e_1 - e_3)$ de E_{St}, Id, (12) et (123) sont représentés par les matrices

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

et donc E_{st} est une sous-représentation de caractère donné par la troisième ligne de la table de caractères. Cette représentation est appelée représentation standard de $\mathfrak{S}_3$.

6 Intégralité des caractères

6.1 Entiers algébriques

Définition 6.1. *Soit $z \in \mathbb{C}$. On dit que z est un entier algébrique s'il existe un polynôme P à coefficients dans $\mathbb{Z}$,* ***unitaire****, tel que $P(z) = 0$.*

Exemple 6.1. — $\sqrt{2}$ est un entier algébrique, car racine de $X^2 - 2$.
— Les racines de l'unité sont des entiers algébriques, car racines de $X^n - 1$ pour un certain entier n.

Les entiers algébriques sont donc des nombres algébriques, mais la réciproque est fausse. Les rationnels sont tous des nombres algébriques, mais :

Proposition 6.2. *Soit $a \in \mathbb{Q}$. Alors a est un entier algébrique si, et seulement si, $a \in \mathbb{Z}$.*

Démonstration. Supposons que a est un entier algébrique. Posons $a = \frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, p et q premiers entre eux. Soit $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \mathbb{Z}[X]$ tel que $P(a) = 0$. Alors

$$P(a) = \frac{p^n + a_{n-1}qp^{n-1} + \ldots + a_0 q^n}{q^n} = 0 \Longrightarrow -q(a_{n-1}p^{n-1} + \ldots + a_0 q^{n-1}) = p^n.$$

donc q divise p^n. Comme q et p sont premiers entre eux, $q = 1$ et $a \in \mathbb{Z}$.

Réciproquement, si $a \in \mathbb{Z}$, alors a est racine de $X - a$, donc a est un entier algébrique. □

Proposition 6.3. *Soit a un nombre algébrique et P son polynôme minimal (supposé unitaire). Les conditions suivantes sont équivalentes :*

1. *a est un entier algébrique.*
2. *$P \in \mathbb{Z}[X]$.*

Démonstration. 2. $\Longrightarrow$ 1. Évident, car $P(a) = 0$.

1. $\Longrightarrow$ 2. Soit $Q \in \mathbb{Z}[X]$, unitaire, tel que $Q(a) = 0$. On décompose Q en polynômes irréductibles de $\mathbb{Z}[X]$: $Q = Q_1 \ldots Q_k$. Comme Q est unitaire, le coefficient dominant de chacun des Q_i vaut 1 ou -1. Quitte à normaliser, on suppose que les Q_i sont tous unitaires. Comme $Q(a) = 0$, $Q_1(a) \ldots Q_k(a) = 0$, donc au moins l'un des Q_i s'annule en a : quitte à remplacer Q par Q_i, on peut supposer Q irréductible dans $\mathbb{Z}[X]$, et donc aussi dans $\mathbb{Q}[X]$ [10]. Par définition du polynôme minimal, $Q = P$. □

Théorème 6.4. *Soit $a \in \mathbb{C}$. On dénote par $\mathbb{Z}[a]$ le plus petit sous-anneau de $\mathbb{C}$ qui contient a :*

$$\mathbb{Z}[a] = \{a_0 + a_1 a + \ldots + a_n a^n \mid n \in \mathbb{N},\ a_0, \ldots, a_n \in \mathbb{Z}\}.$$

Les conditions suivantes sont équivalentes :

1. *a est un entier algébrique.*
2. *$(\mathbb{Z}[a], +)$ est un groupe abélien libre de type fini.*
3. *Il existe un sous-groupe M non nul de $(\mathbb{C}, +)$ de type fini, tel que $aM \subseteq M$.*

Démonstration. 1. $\Longrightarrow$ 2. On considère le morphisme d'anneaux

$$\psi : \left\{ \begin{array}{ccc} \mathbb{Z}[X] & \longrightarrow & \mathbb{C} \\ Q(X) & \longrightarrow & Q(a). \end{array} \right.$$

Par définition, l'image de ψ est $\mathbb{Z}[a]$. En notant $P(X)$ le polynôme minimal de a, le noyau de ψ est $\langle P(X) \rangle$. En conséquence, les anneaux $\mathbb{Z}[a]$ et $\mathbb{Z}[X]/\langle P(X) \rangle$ sont isomorphes. Posons $x = \overline{X}$ dans $\mathbb{Z}[X]/\langle P(X) \rangle$. Soit n le degré de $P(X)$; montrons que $(1, x, \ldots, x^{n-1})$ est une $\mathbb{Z}$-base de

10. C'est un résultat classique sur les polynômes à coefficients dans un anneau factoriel.

$\mathbb{Z}[X]/\langle P(X)\rangle$. Soit $Q(X) \in \mathbb{Z}[X]$. posons $Q(X) = P(X)R(X) + S(X)$ la division euclidienne de $Q(X)$ par $P(X)$ dans $\mathbb{Q}[X]$. Comme $P(X)$ est unitaire, il est facile de montrer que $R(X)$ et $S(X)$ sont dans $\mathbb{Z}[X]$. Comme $\deg(S(X)) < n$, posons $S(X) = a_0 + \ldots + a_{n-1}X^{n-1}$, avec $a_0, \ldots, a_{n-1} \in \mathbb{Z}$. Alors

$$\overline{Q(X)} = \overline{P(X)Q(X)} + \overline{S(X)} = a_0 + \ldots + a_{n-1}x^{n-1}.$$

Donc $(1, x, \ldots, x^{n-1})$ engendre $(\mathbb{Z}[X]/\langle P(X)\rangle, +)$.

Soient $a_0, \ldots, a_{n-1} \in \mathbb{Z}$, tels que $a_0 + \ldots + a_{n-1}x^{n-1} = \overline{0}$. Alors, dans $\mathbb{Z}[X]$, $P(X)$ divise $a_0 + \ldots + a_{n-1}X^{n-1}$. Comme $\deg(P(X)) = n$, nécessairement $a_0 + \ldots + a_{n-1}X^{n-1} = 0$, donc $a_0 = \ldots = a_{n-1} = 0$.

On obtient donc que $(\mathbb{Z}[X]/\langle P(X)\rangle, +)$ est un groupe abélien libre de rang n et de $\mathbb{Z}$-base $(1, x, \ldots, x^{n-1})$. Par isomorphisme, $(\mathbb{Z}[a], +)$ est un groupe abélien libre de rang n et de de $\mathbb{Z}$-base $(1, a, \ldots, a^{n-1})$.

2. $\Longrightarrow$ 3. On peut prendre $M = \mathbb{Z}[a]$.

3. $\Longrightarrow$ 1. Soit $(e_1, \ldots, e_n) \in \mathbb{C}^n$ une famille génératrice de M, formée d'éléments tous non nuls. Comme $aM \subseteq M$, pour tout i, $ae_i \in M$, donc il existe des entiers relatifs $a_{i,j}$ tels que

$$ae_i = \sum_{j=1}^{n} a_{i,j}e_j.$$

Soit $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in M_n(\mathbb{Z})$. Dans $\mathbb{C}^n$,

$$a \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix},$$

donc a est valeur propre de la matrice A, le vecteur $\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$ étant non nul. Par suite, a est racine du polynôme caractéristique χ_A de A. Comme A est à coefficients entiers, ce polynôme est à coefficients entiers et unitaire, au signe près. donc a est un entier algébrique. □

Théorème 6.5. *Soient a et b deux entiers algébriques. Alors $a + b$ et ab sont des entiers algébriques.*

Démonstration. Une première preuve. Par le théorème 6.4, il existe des sous-groupes M et N non nuls de $\mathbb{C}$, de type fini, tel que $aM \subseteq M$ et $bN \subseteq N$. Soient $(x_1, \ldots, x_k)$ un système de générateurs de M et $(y_1, \ldots, y_l)$ un système de générateurs de N. On considère le sous-groupe MN de $\mathbb{C}$ engendré par les éléments x_iy_j, avec $1 \leqslant i \leqslant k$ et $1 \leqslant j \leqslant l$. Alors MN est un sous-groupe non nul de $\mathbb{C}$ de type fini. Soient $1 \leqslant i \leqslant k$ et $1 \leqslant j \leqslant l$. Alors $ax_i \in M$, donc peut s'écrire sous la forme

$$ax_i = \sum_{p=1}^{k} a_p x_p.$$

Donc $ax_iy_j = \sum_{p=1}^{k} a_p x_p y_j \in MN$. Donc $aMN \subseteq MN$. De même, $bMN \subseteq MN$. En conséquence, $(a+b)MN \subseteq aMN + bMN \subseteq MN + MN \subseteq MN$ et $abMN = a(bMN) \subseteq aMN \subseteq MN$. Par le théorème 6.4, $a + b$ et ab sont des entiers algébriques.

Une seconde preuve, utilisant l'élimination. Soit P le polynôme minimal de a et Q celui de b. Le degré de P est noté p et celui de Q est noté q. Comme a et b sont des entiers algébriques,

P et Q sont des polynômes de $\mathbb{Z}[X]$, unitaires. Les polynômes $P(X)$ et $Q(a+b-X)$ ont a pour racine commune. Par suite, le résultant de ces deux polynômes est nul :

$$\mathrm{res}(P(X), Q(a+b-X)) = 0.$$

Comme $\deg_X Q(a+b-X) = \deg_X Q(Y-X)$, on obtient

$$\mathrm{res}_X(P(X), Q(Y-X))_{|Y=a+b} = \mathrm{res}(P(X), Q(a+b-X)) = 0.$$

Posons $\mathrm{res}_X(P(X), Q(Y-X)) = R(Y)$, alors $R(a+b) = 0$. De plus, R est donné par un déterminant de la forme

$$R(Y) = \begin{vmatrix} 1 & & & * & & & \\ \vdots & \ddots & & \vdots & \ddots & & \\ \vdots & & 1 & \vdots & & \ddots & \\ \vdots & & \vdots & Y^q + * & & & * \\ * & & \vdots & & \ddots & & \vdots \\ & \ddots & \vdots & & & \ddots & \vdots \\ & & * & & & & Y^q + * \end{vmatrix}$$

où les $*$ sont des entiers relatifs ou des polynômes de $\mathbb{Z}[Y]$ de degré $< q$. En développant, on obtient que $R(Y)$ est un polynôme de degré pq de $\mathbb{Z}[X]$, unitaire. Par suite, $a+b$ est un entier algébrique. On montre de même que ab est un entier algébrique en considérant $P(X)$ et $X^q Q(ab/X)$, tous deux ayant a pour racine (en se limitant au cas où $a \neq 0$). Par suite, le résultant en X de $P(X)$ et de $X^q Q(Y/X)$ est un polynôme unitaire de $\mathbb{Z}[X]$ qui s'annule en $\alpha\beta$. □

6.2 Intégralité des caractères

Proposition 6.6. *Soit χ le caractère d'une représentation d'un groupe fini G. Pour tout $g \in G$, $\chi(g)$ est un entier algébrique.*

Démonstration. Comme $\chi(g)$ est une somme de racines de l'unité, c'est un entier algébrique. □

Théorème 6.7. *Soit χ un caractère irréductible d'un groupe fini G. Pour tout $g \in G$, on note $c(g)$ le cardinal de la classe de conjugaison de g. Le nombre suivant est un entier algébrique :*

$$\frac{c(g)\chi(g)}{\chi(e_G)}.$$

Démonstration. On munit $\mathscr{C}(G)$ d'un produit (dit produit de convolution), défini de la manière suivante :

$$\forall \lambda, \mu \in \mathscr{C}(G),\ \forall g \in G, \qquad \lambda * \mu(g) = \sum_{\substack{h,k \in G, \\ hk=g}} \lambda(h)\mu(k) = \sum_{h \in G} \lambda(h)\mu(h^{-1}g).$$

Comme G est fini, ceci a bien un sens. Montrons que $\lambda * \mu$ est bien une fonction centrale : si

$g, h \in G$

$$\begin{aligned}
\lambda * \mu(gh) &= \sum_{k\in G} \lambda(k)\mu(k^{-1}gh) \\
&= \sum_{k\in G} \lambda(k)\mu(hk^{-1}g) \\
&= \sum_{l\in G} \lambda(l^{-1}h)\mu(lg) \\
&= \sum_{l\in G} \lambda(hl^{-1}\mu(lg) \\
&= \sum_{m\in G} \lambda(m)\mu(m^{-1}hg) \\
&= \lambda * \mu(hg).
\end{aligned}$$

Donc $*$ est bien un produit interne. Soient $\lambda, \mu, \nu \in \mathscr{C}(G)$. Pour tout $g \in G$,

$$\begin{aligned}
(\lambda * \mu) * \nu(g) &= \sum_{hh'=g, kk'=h} \lambda(k)\mu(k')\nu(h') \\
&= \sum_{hkl=g} \lambda(h)\mu(k)\nu(l) \\
&= \sum_{hh'=g, kk'=h'} \lambda(h)\mu(k)\nu(k') \\
&= \lambda * (\mu * \nu)(g).
\end{aligned}$$

Donc $*$ est associatif. Si $\lambda, \mu \in \mathscr{C}(G)$, pour tout $g \in G$,

$$\begin{aligned}
\lambda * \mu(g) &= \sum_{k\in G} \lambda(k)\mu(gk^{-1}) \\
&= \sum_{k\in G} \lambda(k)\mu(k^{-1}g) \\
&= \sum_{k\in G} \mu(h)\lambda(gh^{-1}) \\
&= \sum_{k\in G} \mu(h)\lambda(h^{-1}g) \\
&= \mu * \lambda(g).
\end{aligned}$$

Donc $*$ est commutative. L'élément neutre est l'application $\delta_{\{e_G\}}$. Ainsi, $\mathscr{C}(G)$ devient un anneau commutatif. En notant $C_{\mathbb{Z}}(G)$ le sous-ensemble des fonctions centrales de G prenant leurs valeurs dans $\mathbb{Z}$, on obtient un sous-anneau de $\mathscr{C}(G)$.

On note $\theta : G \longrightarrow \mathrm{GL}(E)$ une représentation de G de caractère χ. Soit $\lambda \in \mathscr{C}(G)$. On lui associe l'endomorphisme de E défini par

$$\phi_\lambda = \sum_{g\in G} \lambda(g)\theta(g)$$

Pour tout $h \in G$,

$$\begin{aligned}
\phi_\lambda \circ \theta(h) &= \sum_{g\in G} \lambda(g)\theta(g)\circ\theta(h) \\
&= \sum_{g\in G} \lambda(g)\theta(gh) \\
&= \sum_{g'\in G} \lambda(g'h^{-1})\theta(g') \\
&= \sum_{g'\in G} \lambda(h^{-1}g')\theta(g') \\
&= \sum_{g''\in G} \lambda(g'')\theta(hg) \\
&= \sum_{g''\in G} \lambda(g'')\theta(h)\circ\theta(g) \\
&= \theta(h)\circ\phi_\lambda,
\end{aligned}$$

avec les changements de variables $gh = g'$ puis $h^{-1}g' = g''$. Donc ϕ_λ est un endomorphismes de représentations de θ. Comme θ est irréductible, ϕ_λ est une homothétie : il existe un scalaire a_λ tel que $\phi_\lambda = a_\lambda$.

Soient $\lambda, \mu \in \mathscr{C}(G)$.

$$\begin{aligned}
\phi_\lambda \circ \phi_\mu &= \sum_{g\in G} \mu(g)\phi_\lambda \circ \theta(g) \\
&= \sum_{g\in G}\sum_{h\in G} \mu(g)\lambda(h)\theta(h)\circ\theta(g) \\
&= \sum_{g\in G}\sum_{h\in G} \mu(g)\lambda(h)\theta(hg) \\
&= \sum_{g'\in G}\sum_{g,h\in G,\ gh=g'} \mu(g)\lambda(h)\theta(g') \\
&= \phi_{\lambda*\mu}.
\end{aligned}$$

Par suite, $a_{\lambda*\mu} = a_\lambda a_\mu$. On obtient donc un morphisme d'anneaux

$$\Lambda : \left\{ \begin{array}{ccc} \mathscr{C}(G) & \longrightarrow & \mathbb{C} \\ \lambda & \longrightarrow & a_\lambda. \end{array} \right.$$

L'image de $C_\mathbb{Z}(G)$ par ce morphisme est notée M. Comme $C_\mathbb{Z}(G)$ est un groupe abélien de type fini, A aussi. De plus, M est un sous-anneau de $\mathbb{C}$: si $a \in M$, alors $aM \subseteq M$. D'après le théorème 6.4, a est un entier algébrique, donc tout élément de M est un entier algébrique.

Pour toute classe de conjugaison C de G, on pose

$$\delta_C : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ g & \longrightarrow & \begin{cases} 1 \text{ si } g \in C, \\ 0 \text{ sinon.} \end{cases} \end{array} \right.$$

Ces fonctions centrales forment une base de $\mathscr{C}(G)$. De plus, si λ est une fonction centrale, en notant $\lambda(C)$ la valeur commune de λ sur chaque élément de C, on obtient

$$\lambda = \sum \lambda(C)\delta_C.$$

Prenons $\lambda = \delta_C$. Alors

$$\phi_\lambda = \sum_{g\in C} \theta(g).$$

Par suite,

$$a_\lambda = \frac{\mathrm{Tr}(\phi_\lambda)}{\dim(E)} = \frac{1}{\dim(E)} \sum_{g \in C} \mathrm{Tr}(\theta(g)) = \frac{1}{\chi(e_G)} \sum_{g \in C} \chi(g) = \frac{\chi(g)|C|}{\chi(e_G)},$$

où g est un élément quelconque de C. Comme $a_\lambda \in M$, c'est un entier algébrique. □

Corollaire 6.8. *Soit χ un caractère irréductible d'un groupe fini G. Soit λ une fonction centrale sur G dont toutes les valeurs sont des entiers algébriques. Le nombre suivant est un entier algébrique :*

$$\frac{1}{\chi(1)} \sum_{g \in G} \lambda(g)\chi(g).$$

Démonstration. On pose $n = \chi(1)$. Alors, en décomposant dans la base des δ_C,

$$\frac{1}{n} \sum_{g \in G} \lambda(g)\chi(g) = \sum_C \lambda(C) \sum_{g \in G} \delta_C(g)\chi(g).$$

Comme les sommes et produits d'entiers algébriques sont des entiers algébriques, pour obtenir le résultat on peut se limiter à $\lambda = \delta_C$ pour une certaine classe de conjugaison C. Dans ce cas,

$$\frac{1}{n} \sum_{g \in G} \lambda(g)\chi(g) = \frac{1}{n} \sum_{g \in C} \chi(g) = \frac{|C|\chi(C)}{n},$$

en notant $\chi(C)$ la valeur commune de χ sur chaque élément de C. Ceci découle du théorème précédent. □

Corollaire 6.9. *Soit θ une représentation irréductible d'un groupe fini G. Alors le degré de θ divise le cardinal de G.*

Démonstration. Soit χ le caractère de θ et soit $\lambda : G \longrightarrow \mathbb{C}$ défini par $\lambda(g) = \chi(g^{-1})$. Comme χ est une fonction centrale, λ aussi. De plus, comme les valeurs prises par χ sont des entiers algébriques, il en est de même pour λ. On applique le corollaire 6.8, qui implique que le nombre suivant est un entier algébrique :

$$a = \frac{1}{\dim(E)} \sum_{g \in G} |\chi(g)|^2 = \frac{|G|}{\dim(E)} \langle \chi, \chi \rangle = \frac{|G|}{\dim(E)}.$$

Comme $a \in \mathbb{Q}$ et que a est un entier algébrique, nécessairement $a \in \mathbb{Z}$. Don $\dim(E)$ divise $|G|$. □

7 Produit tensoriel

Le produit de deux fonctions centrales sur G est encore une fonction centrale : $\mathscr{C}(G)$ est une algèbre. Si χ_1 et χ_2 sont les caractères de deux représentations de G, qu'en est-il de $\chi_1\chi_2$?

7.1 Produit tensoriel de deux espaces vectoriels

Proposition 7.1. *Soit B un ensemble. Il existe un espace vectoriel V dont B est une base.*

Démonstration. Soit V_1 l'espace vectoriel des applications de B dans $\mathbb{K}$. Pour tout $b \in B$, on considère l'application

$$\delta_b : \left\{ \begin{array}{ccc} B & \longrightarrow & \mathbb{K} \\ b' & \longrightarrow & \delta_{b,b'}. \end{array} \right.$$

Il s'agit d'une famille libre de V_1 : si $b1, \ldots, b_2 \in B$ sont distincts et si $\alpha_1, \ldots, \alpha_2 \in \mathbb{K}$ tels que $f = \alpha_1\delta_{b_1} + \ldots + \alpha_k\delta_{b_k} = 0$, alors, pour tout $i \in \{1, \ldots, k\}$,

$$f(b_i) = \alpha_i = 0.$$

Soit V_2 le sous-espace de V_1 engendré par la famille $(\delta_b)_{b\in B}$. Alors $(\delta_b)_{b\in B}$ est une base de V_2. Soit maintenant

$$V = (V_2 \setminus \{\delta_b, b \in B\}) \sqcup B.$$

Il existe une bijection de V dans V_2 :

$$\psi : \left\{ \begin{array}{rcl} V & \longrightarrow & V_2 \\ v \in V_2 \setminus \{\delta_b, b \in B\} & \longrightarrow & v \\ b \in B & \longrightarrow & \delta_b. \end{array} \right.$$

On définit alors une structure d'espace vectoriel sur V de la façon suivante :

$$\begin{aligned} v + w &= \psi^{-1}(\psi(v) + \psi(w)), \\ \lambda v &= \psi^{-1}(\lambda\psi(v)). \end{aligned}$$

De plus, ψ est un isomorphisme. Comme $(\delta_b)_{b\in B}$ est une base de V_2, son image par ψ^{-1}, c'est-à-dire B, est une base de V. □

Remarque 7.1. Si $b_1, \ldots, b_k \in B$ et si $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$, alors $\alpha_1 b_1 + \ldots + \alpha_k b_K$ est, soit un élément de B, soit une application de B dans $\mathbb{K}$.

Théorème 7.2. *Soient X et Y deux espaces vectoriels. Il existe un couple $(V, \otimes)$ où V est un espace vectoriel et $\otimes : X \times Y \longrightarrow V$ est une application bilinéaire, tel que pour toute application bilinéaire $F : X \times Y \longrightarrow Z$, il existe une unique application linéaire $f : V \longrightarrow Z$ telle que*

$$F = f \circ \otimes.$$

Ce couple $(V, \otimes)$ est unique à isomorphisme près.

Démonstration. Existence de $(V, \otimes)$. Soit W un espace vectoriel ayant pour base $X \times Y$ et soit W' le sous-espace de W engendré par les éléments suivants :

$$\begin{aligned} (x + x', y) - (x, y) - (x', y), & x, x' \in X,\ y \in Y, \\ (x, y + y') - (x, y) - (x, y'), & x \in X,\ y, y' \in Y, \\ (\alpha_x, y) - \alpha(x, y), & \alpha \in \mathbb{K},\ x \in X,\ y \in Y, \\ (x, \alpha_y) - \alpha(x, y), & \alpha \in \mathbb{K},\ x \in X,\ y \in Y. \end{aligned}$$

On pose $V = W/W'$ et

$$\otimes : \left\{ \begin{array}{rcl} X \times Y & \longrightarrow & V \\ (x, y) & \longrightarrow & x \otimes y = \overline{(x, y)}. \end{array} \right.$$

Pour tous $x, x' \in X$, $y, y' \in Y$, $\alpha_{\in}\mathbb{K}$,

$$\begin{aligned} \overline{(x + x', y)} &= \overline{(x, y)} + \overline{(x', y)}, \\ \overline{(x, y + y')} &= \overline{(x, y)} + \overline{(x, y')}, \\ \overline{(\alpha x, y)} &= \alpha\overline{(x, y)}, \\ \overline{(x, \alpha y)} &= \alpha\overline{(x, y)}, \end{aligned}$$

donc $\otimes$ est bilinéaire.

Soit $F : X \times Y \longrightarrow Z$ une application bilinéaire.

Existence de f. Soit $g : W \longrightarrow Z$ l'unique application linéaire envoyant (x, y) sur $F(x, y)$: ceci existe, car $X \times Y$ est une base de W. Soient $x, x' \in X$, $y, y' \in Y$, $\alpha_{\in}\mathbb{K}$. Comme F est bilinéaire,

$$\begin{aligned} g((x + x', y) - (x, y) - (x', y)) &= F(x + x', y) - F(x, y) - F(x', y) = 0, \\ g((x, y + y') - (x, y) - (x, y')) &= F(x, y + y') - F(x, y) - F(x, y') = 0, \\ g((\alpha x, y) - \alpha(x, y)) &= F(\alpha x, y) - \alpha(x, y)) = 0, \\ g((x, \alpha y) - \alpha(x, y)) &= F(x, \alpha y) - \alpha(x, y)) = 0. \end{aligned}$$

Donc $W' \subseteq \mathrm{Ker}(g)$. Par suite, on obtient une application linéaire $F : V \longrightarrow Z$, par passage au quotient de g. Pour tous $x \in X$, $y \in Y$,

$$f(x \otimes y) = f(\overline{(x,y)}) = g(x,y) = F(x,y).$$

Unicité de f. Soit $f' : V \longrightarrow Z$ une autre application linéaire telle que $f'(x \otimes y) = F(x,y)$ pour tout $(x,y) \in X \times Y$. Comme $X \times Y$ engendre W, $V = W/W'$ est engendré par les classes $\overline{(x,y)}$, avec $x \in X$, $y \in Y$. Or $f(\overline{(x,y)}) = F(x,y) = f'(\overline{(x,y)})$. Comme f et f' sont linéaires, $f = f'$.

Unicité de $(V, \otimes)$. Soit $(V', \otimes)$ un autre couple convenant. Comme $\otimes' : X \times Y \longrightarrow V'$ est bilinéaire, il existe une application linéaire $f : V \longrightarrow V'$ telle que $f \circ \otimes = \otimes'$. Comme $\otimes : X \times Y \longrightarrow V$ est bilinéaire, il existe une application linéaire $f' : V' \longrightarrow V$ telle que $f' \circ \otimes' = \otimes$. Considérons $f \circ f' : V' \longrightarrow V'$. Alors $f \circ f' \circ \otimes' = f \circ \otimes = \otimes'$. Donc $f \circ f'$ est l'unique application $g : V' \longrightarrow V'$ telle que $g \circ \otimes' = \otimes'$: il s'agit évidemment de $\mathrm{Id}_{V'}$. De même, $f' \circ f = \mathrm{Id}_V$. Donc V et V' sont isomorphes, via les bijections inverses l'une de l'autre f et f'. □

Définition 7.3. *Cet espace V est appelé produit tensoriel de X et Y et est noté $X \otimes Y$. Il est muni d'une application bilinéaire*

$$\otimes : \left\{ \begin{array}{ccc} X \times Y & \longrightarrow & X \otimes Y \\ (x,y) & \longrightarrow & x \otimes y. \end{array} \right.$$

Proposition 7.4. *Soit $(x_i)_{i \in I}$ une base de X et $(y_j)_{j \in J}$ une base de Y . Alors $(x_i \otimes y_j)_{i \in I, j \in J}$ est une base de $X \otimes Y$.*

Démonstration. Par construction, tout élément de $X \otimes Y$ est une combinaison linéaire d'éléments $x \otimes y = \overline{(x,y)}$ avec $x \in X$, $y \in Y$. Il existe des scalaires $(a_i)_{i \in I}$, $(b_j)_{j \in J}$, tous nuls sauf un nombre fini, tels que

$$x = \sum_{i \in I} a_i x_i, \qquad\qquad y = \sum_{j \in J} b_j y_j.$$

Comme $\otimes$ est bilinéaire,

$$x \otimes y = \sum_{i \in I, j \in J} a_i b_j x_i \otimes y_j.$$

Tout élément de $X \otimes Y$ est une combinaison linéaire de termes $x_i \otimes y_j$: la famille $(x_i \otimes y_j)_{i \in I, j \in J}$ est génératrice. Soient $(a_{i,j})_{i \in I, j \in J}$ des scalaires tous nuls sauf un nombre fini, tels que

$$a = \sum_{i \in I, j \in J} a_{i,j} x_i \otimes y_j = 0.$$

Soit $i_0 \in I, j_0 \in J$. On considère l'application bilinéaire

$$F : \left\{ \begin{array}{ccc} X \times Y & \longrightarrow & \mathbb{K} \\ \left(\sum_{i \in I} a_i x_i, \sum_{j \in J} b_j y_j \right) & \longrightarrow & a_{i_0} b_{j_0}. \end{array} \right.$$

Il existe une application linéaire $f : X \otimes Y \longrightarrow \mathbb{K}$ telle que $F = f \circ \otimes$. Alors

$$f(a) = 0 = \sum_{i \in I, j \in J} a_{i,j} F(x_i, y_j) = a_{i_0, j_0}.$$

Donc $(x_i \otimes y_j)_{i \in I, j \in J}$ est une famille libre. □

Remarque 7.2. En particulier, si X et Y sont de dimension finie, $X \otimes Y$ également et

$$\dim(X \otimes Y) = \dim(X) \dim(Y).$$

Proposition 7.5. *Soit $f : X \longrightarrow X'$ et $g : Y \longrightarrow Y'$ deux applications linéaires. Il existe une unique application linéaire $f \otimes g : X \otimes Y \longrightarrow X' \otimes Y'$ telle que pour tous $x \in X$, $y \in Y$,*

$$f \otimes g(x \otimes y) = f(x) \otimes g(y).$$

De plus, si $X = X', Y = Y'$ sont des espaces de dimension finie,

$$\mathrm{Tr}(f \otimes g) = \mathrm{Tr}(f)\mathrm{Tr}(g).$$

Démonstration. Soit $F : X \times Y \longrightarrow X' \otimes Y'$, définie par $F(x, y) = f(x) \otimes g(y)$. Comme f et g sont linéaires et $\otimes$ est bilinéaire, F est bilinéaire. Donc il existe une unique application linéaire $f \otimes g : X \otimes Y \longrightarrow X' \otimes Y'$ telle que si $x \in X$, $y \in Y$, $f \otimes g(x \otimes y) = f(x) \otimes g(y)$. Supposons $X = X'$ et $Y = Y'$, de dimension finie. Soit $(x_i)_{i\in I}$ une base de X, A la matrice de f dans cette base, $(y_j)_{j\in J}$ une base de Y et B la matrice de g dans cette base. Si $i_0 \in I$ et $j_0 \in J$,

$$\begin{aligned} f \otimes g(x_{i_0} \otimes y_{j_0}) &= \left(\sum_{i\in I} a_{i,i_0} x_i\right) \otimes \left(\sum_{j\in J} b_{j,j_0} y_j\right) \\ &= \sum_{i\in I,\, j\in J} a_{i,i_0} b_{j,j_0} x_i \otimes y_j. \end{aligned}$$

Donc

$$\mathrm{Tr}(f \otimes g) = \sum_{i\in I,\, j\in J} a_{i,i} b_{j,j} = \left(\sum_{i\in I} a_i\right)\left(\sum_{j\in J} b_j\right) = \mathrm{Tr}(f)\mathrm{Tr}(g). \qquad \square$$

7.2 Produit tensoriel de deux représentations

Théorème 7.6. *Soient $\theta : G \longrightarrow GL(E)$ et $\theta' : G \longrightarrow GL(E')$ deux représentations d'un même groupe fini G, de caractères respectifs χ et χ'. On définit une représentation de G sur $E \otimes E'$ par*

$$\forall g \in G,\ \forall x \in E,\ \forall y \in E', \qquad \theta \otimes \theta'(g)(x \otimes y) = \theta(g)(x) \otimes \theta'(g)(y).$$

Le caractère de cette représentation est $\chi\chi'$.

Démonstration. Pour tout $g \in G$, $\theta(g) \otimes \theta'(g)$ est une application linéaire de $E \otimes E'$ dans $E \otimes E'$. Si $g, h \in G$, $x \in E$, $y \in E'$,

$$\begin{aligned} (\theta \otimes \theta')(g) \circ (\theta \otimes \theta')(h)(x \otimes y) &= \theta(g) \circ \theta(h)(x) \otimes \theta'(g) \circ \theta'(h)(y) \\ &= \theta(gh)(x) \otimes \theta'(gh)(y) \\ &= (\theta \otimes \theta')(gh)(x \otimes y). \end{aligned}$$

Donc $(\theta \otimes \theta')(g) \circ (\theta \otimes \theta')(h) = (\theta \otimes \theta')(gh)$. De plus, si $x \in E$, $y \in E'$,

$$(\theta \otimes \theta')(e_G)(x \otimes y) = \theta(e_G)(x) \otimes \theta'(e_G)(y) = x \otimes y,$$

donc $(\theta \otimes \theta')(e_G) = \mathrm{Id}_{E\otimes E'}$. Il s'agit bien d'une représentation de G par le lemme 1.2. De plus, pour tout $g \in G$, en notant χ'' le caractère de cette représentation,

$$\chi''(g) = \mathrm{Tr}(\theta(g) \otimes \theta'(g)) = \mathrm{Tr}(\theta(g))\mathrm{Tr}(\theta'(g)) = \chi(g)\chi'(g),$$

donc $\chi'' = \chi\chi'$. $\square$

8 Rappels sur les polynômes à n indéterminées

Dans toute cette section, on fixe un entier $n \geqslant 1$. On désigne par $\mathbb{A}$ un anneau commutatif.

8.1 Construction

On fixe un entier $n \geqslant 1$. On considère les $\mathbb{A}$-modules produit direct et somme directe

$$\mathbb{A}^{\mathbb{N}^n} = \prod_{n\in\mathbb{N}^n} \mathbb{A} = \{(a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n},\ \forall (k_1,\dots,k_n)\in\mathbb{N}^n,\ a_{(k_1,\dots,k_n)}\in\mathbb{A}\}$$
$$\mathbb{A}^{(\mathbb{N}^n)} = \bigoplus_{n\in\mathbb{N}^n} \mathbb{A} = \{(a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n} \in \mathbb{A}^{\mathbb{N}^n} \mid (a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n} \text{ à support fini}\}.$$

On rappelle que leur structure de $\mathbb{A}$-module est donnée par

$$(a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n} + (b_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n} = (a_{(k_1,\dots,k_n)} + b_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n},$$
$$\lambda.(a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n} = (\lambda a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n}.$$

Si $(i_1,\dots,i_n)\in\mathbb{N}^n$, on définit $e^{(i_1,\dots,i_n)}\in\mathbb{A}^{(\mathbb{N}^n)}$ par

$$e^{(i_1,\dots,i_n)}_{(k_1,\dots,k_n)} = \delta_{(i_1,\dots,i_n),(k_1,\dots,k_n)} = \begin{cases} 1 \text{ si } i_1 = k_1,\dots,i_n = k_n, \\ 0 \text{ sinon.} \end{cases}$$

La famille $(e^{(i_1,\dots,i_n)})_{(i_1,\dots,i_n)\in\mathbb{N}^n}$ est une base de $\mathbb{A}^{(\mathbb{N}^n)}$, qui est donc un $\mathbb{A}$-module libre. Les éléments de $\mathbb{A}^{(N^n)}$ sont appelés *polynômes à n indéterminées à coefficients dans $\mathbb{A}$*.

Proposition 8.1. *On munit $\mathbb{A}^{(\mathbb{N}^n)}$ d'un produit par*

$$(a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n}.(b_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n}$$
$$= \left(\sum_{(i_1,\dots,i_n)+(j_1,\dots,j_n)=(k_1,\dots,k_n)} a_{(i_1,\dots,i_n)}b_{(j_1,\dots,j_n)}\right)_{(k_1,\dots,k_n)\in\mathbb{N}^n}.$$

Ainsi $\mathbb{A}^{(N^n)}$ devient une $\mathbb{A}$-algèbre commutative unitaire, d'élément neutre $e_{(0,\dots,0)}$. On l'appelle algèbre des polynômes à une indéterminée à coefficients dans $\mathbb{A}$.

Remarque 8.1.

1. L'application suivante est donc un morphisme de $\mathbb{A}$-algèbres injectif
$$\phi : \begin{cases} \mathbb{A} & \longrightarrow & \mathbb{A}^{(N^n)} \\ a & \longrightarrow & a.e_{(0,\dots,0)}. \end{cases}$$
Son image est l'ensemble des *polynômes constants*, qui est donc une sous-algèbre de $\mathbb{A}^{(\mathbb{N}^n)}$. Par la suite, on identifiera via ce morphisme les éléments de $\mathbb{A}$ et les polynômes constants.
2. Pour tout $(i_1,\dots,i_n),(j_1,\dots,j_n)\in\mathbb{N}^n$,
$$e^{(i_1,\dots,i_n)}.e^{(j_1,\dots,j_n)} = e^{(i_1+j_1,\dots,i_n+j_n)}.$$
Ceci justifie la définition suivante :

Définition 8.2.

1. *Pour tout $1\leqslant i\leqslant n$, on pose $X_i = e^{(0,\dots,0,1,0,\dots,0)}$ (le 1 étant en i-ième position) ; $X_1,\dots,X_n$ sont appelées* indéterminées.
2. *Tout élément f non nul de $\mathbb{A}^{(N^n)}$ de degré k s'écrit de manière unique*
$$f = \sum_{(k_1,\dots,k_n)\in\mathbb{N}^n} a_{(k_1,\dots,k_n)}X_1^{k_1}\dots X_n^{k_n}.$$
Notons que, dans ce cas, $f = (a_{(k_1,\dots,k_n)})_{(k_1,\dots,k_n)\in\mathbb{N}^n}$.
3. *L'algèbre des polynômes à n indéterminées à coefficients dans $\mathbb{A}$ sera maintenant notée $\mathbb{A}[X_1,\dots,X_n]$.*

Remarque 8.2. Le noms donnés aux indéterminées sont arbitraires. En conséquence, les algèbres $\mathbb{A}[X_1,\dots,X_n]$, $\mathbb{A}[Y_1,\dots,Y_n]$, $\mathbb{A}[T_1,\dots,T_n]$, ... sont égales.

Théorème 8.3 (Propriété universelle). *Soit B un anneau commutatif, $\phi : \mathbb{A} \longrightarrow B$ un morphisme d'anneaux et $x_1, \ldots, x_n$ des éléments de B. Il existe un unique morphisme d'anneaux $\Phi : \mathbb{A}[X_1, \ldots, X_n] \longrightarrow B$, tel que $\Phi_{|\mathbb{A}} = \phi$ et $\phi(X_i) = x_i$ si $1 \leqslant i \leqslant n$.*

Démonstration. Ce morphisme Φ est défini par

$$\Phi\left(\sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} a_{(i_1,\ldots,i_n)} X_1^{i_1} \ldots X_n^{i_n}\right) = \sum_{(i_1,\ldots,i_n)\in\mathbb{N}^n} \phi(a_{(i_1,\ldots,i_n)}) x_1^{i_1} \ldots x_n^{i_n}. \qquad \square$$

Exemple 8.1. Dans le cas particulier où $\mathbb{A} = B$ et $\phi = \mathrm{Id}_{\mathbb{A}}$, on obtient un morphisme d'anneaux

$$\left\{ \begin{array}{ccc} \mathbb{A}[X_1, \ldots, X_n] & \longrightarrow & \mathbb{A} \\ f(X_1, \ldots, X_n) & \longrightarrow & f(x_1, \ldots, x_n). \end{array} \right.$$

8.2 Autres écritures dans $\mathbb{A}[X_1, \ldots, X_n]$

Proposition 8.4. *Les algèbres $\mathbb{A}[X_1, \ldots, X_n]$ et $\mathbb{A}[X_1, \ldots, X_{n-1}][X_n]$ sont isomorphes.*

Démonstration. Remarquons d'abord que, contrairement à ce qu'on pourrait croire, $\mathbb{A}[X_1, \ldots, X_n]$ et $\mathbb{A}[X_1, \ldots, X_{n-1}][X_n]$ ne sont pas égales. Les éléments de $\mathbb{A}[X_1, \ldots, X_n]$ s'écrivent sous la forme $(a_{(k_1,\ldots,k_n)})_{(k_1,\ldots,k_n)\in\mathbb{N}^n}$, alors que les éléments de $\mathbb{A}[X_1, \ldots, X_{n-1}][X_n]$ s'écrivent sous la forme $((a_{(k_1,\ldots,k_n)})_{(k_1,\ldots,k_{n-1})\in\mathbb{N}^{n-1}})_{k_n\in\mathbb{N}}$. On définit une application entre les deux par

$$\left\{ \begin{array}{rcl} \mathbb{A}[X_1, \ldots, X_{n-1}][X_n] & \longrightarrow & \mathbb{A}[X_1, \ldots, X_n] \\ f_0(X_1, \ldots, X_{n-1}) + \ldots + f_k(X_0, \ldots, X_{n-1}) X_n^k & \longrightarrow & f_0(X_1, \ldots, X_{n-1}) + \\ & & \vdots \\ & & + f_k(X_0, \ldots, X_{n-1}) X_n^k. \end{array} \right.$$

Attention aux notations, $X_1, \ldots, X_n$ n'ont pas la même signification à gauche et à droite ! On vérifie facilement que cette application est un isomorphisme d'algèbres. $\square$

Plus généralement, on peut montrer de la même manière (ou par une récurrence...) que si $I \sqcup J = \{1, \ldots, n\}$, alors $\mathbb{A}[X_1, \ldots, X_n] \approx \mathbb{A}[X_i, i \in I][X_j, j \in J]$. Par la suite, on identifiera ces algèbres et on considèrera qu'elles sont égales et non plus seulement isomorphes. Ceci permettra d'utiliser des méthodes liées aux polynômes à une indéterminée, par exemple les théorèmes de transfert ou les divisions pseudo-euclidiennes.

Exemple 8.2. Par exemple, $\mathbb{R}[X, Y] = \mathbb{R}[X][Y] = \mathbb{R}[Y][X]$. Chaque polynôme de cette algèbre peut donc s'écrire de trois façons différentes :

$$f(X, Y) = \left\{ \begin{array}{l} 1 + 4X^2 - 3XY + Y^5 - 2X^2Y \in \mathbb{R}[X, Y], \\ (1 + 4X^2) + (-3X + 2X^2)Y + Y^5 \in \mathbb{R}[X][Y], \\ (1 + Y^5) + (-3Y)X + (4 - 2Y)X^2 \in \mathbb{R}[Y][X]. \end{array} \right.$$

On rappelle les résultats suivants, valable pour tout anneau commutatif $\mathbb{A}$:

1. $\mathbb{A}[X]$ est intègre si, et seulement si, $\mathbb{A}$ est intègre.
2. $\mathbb{A}[X]$ est principal si, et seulement si, $\mathbb{A}$ est un corps.
3. $\mathbb{A}[X]$ est factoriel si, et seulement si, $\mathbb{A}$ est factoriel.

En conséquence :

Théorème 8.5. *Soit $\mathbb{A}$ un anneau commutatif et $n \geqslant 1$.*

1. *$\mathbb{A}[X_1, \ldots, X_n]$ est intègre si, et seulement si, $\mathbb{A}$ est intègre.*
2. *$\mathbb{A}[X_1, \ldots, X_n]$ est principal si, et seulement si, $\mathbb{A}$ est un corps et $n = 1$.*
3. *$\mathbb{A}[X_1, \ldots, X_n]$ est factoriel si, et seulement si, $\mathbb{A}$ est factoriel.*

8.3 degrés partiels et degré total

Définition 8.6. *Soit* $f = \in \mathbb{A}[X_1, \ldots, X_n]$.

1. *Le* degré partiel en X_i *de* f *est son degré dans* $\mathbb{A}[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n][X_i]$. *On le note* $\deg_{X_i}(f)$.
2. *Le* degré total *de* f *est*

$$\deg(f) = \max\{k_1 + \ldots + k_n \mid a_{(k_1,\ldots,k_n)} \neq 0\},$$

où les $a_{(k_1,\ldots,k_n)}$ *sont les coefficients de* f. *Par convention,* $\deg(0) = -\infty$.

Exemple 8.3. Soit $f = 4X^2 - XY^3 \in \mathbb{R}[X, Y]$. Alors $\deg_X(f) = 2$, $\deg_Y(f) = 3$, $\deg(f) = 4$.

Remarque 8.3.
1. En particulier, f est constant et non nul si, et seulement si, il son degré total est 0, si, et seulement si, son degré partiel en X_i est 0 pour tout i.
2. En général, $\deg(f) \neq \deg_{X_1}(f) + \ldots + \deg_{X_n}(f)$.

Proposition 8.7. *Soient* $f, g \in \mathbb{A}[X_1, \ldots, X_n]$.

1. $\deg_{X_i}(f+g) \leqslant \max(\deg_{X_i}(f), \deg_{X_i}(g))$ *pour tout* i, *avec égalité si* $\deg_{X_i}(f) \neq \deg_{X_i}(g)$.
2. $\deg_{X_i}(fg) \leqslant \deg_{X_i}(f) + \deg_{X_i}(g)$. *Si* $\mathbb{A}$ *est intègre, on a l'égalité.*
3. $\deg(f+g) \leqslant \max(\deg(f), \deg(g))$, *avec égalité si* $\deg(f) \neq \deg(g)$.
4. $\deg(fg) \leqslant \deg(f) + \deg(g)$, *avec égalité si* $\mathbb{A}$ *est intègre.*

Démonstration. Les deux premiers points proviennent des résultat à une indéterminée. Pour les deux autres points, on remarque si $f \in \mathbb{A}[X_1, \ldots, X_n]$, de degré d, on peut l'écrire sous la forme

$$f = \sum_{k=0}^{d} \underbrace{\sum_{k_1+\ldots+k_n=k} a_{(k_1,\ldots,k_n)} X_1^{k_1} \ldots X_n^{k_n}}_{f_k}.$$

Par définition du degré, f_d est non nulle. On a alors

$$f + g = \sum_{k \leqslant \max(\deg(f),\deg(g))} f_k + g_k,$$

donc $\deg(f+g) \leqslant \max(\deg(f), \deg(g))$. Si on suppose par exemple $\deg(f) < \deg(g)$, le dernier terme de cette somme est $g_{\deg(g)}$, qui est non nul, donc on a l'égalité.

On remarque facilement que le produit de deux monômes de degrés respectifs k et l est un monôme de degré $k+l$. En conséquence,

$$fg = \sum_{p=0}^{\deg(f)+\deg(g)} \underbrace{\sum_{k+l=p} f_k g_l}_{\text{somme de monômes de degré } p}.$$

Donc fg est de degré $\leqslant \deg(g) + \deg(g)$. Si $\mathbb{A}$ est intègre,

$$fg = \sum_{p=0}^{\deg(f)+\deg(g)-1} \underbrace{\sum_{k+l=p} f_k g_l}_{\text{somme de monômes de degré } p} + \underbrace{f_{\deg(f)} g_{\deg(g)}}_{\text{somme de monômes de degré } \deg(f)+\deg(g)}.$$

Comme $\mathbb{A}$ est intègre, $\mathbb{A}[X_1, \ldots, X_n]$ aussi, donc $f_{\deg(f)} g_{\deg(g)} \neq 0$. On en déduit que l'écriture de f contient au moins un monôme de degré $\deg(f) + \deg(g)$, donc $\deg(fg) = \deg(f) + \deg(g)$. □

8.4 Homogénéité

Formalisons les notations f_k utilisées dans la preuve précédente.

Définition 8.8. *Soit $f \in \mathbb{A}[X_1, \ldots, X_n]$ et soit $k \geqslant 0$. On dit que f est* homogène de degré k *si tous les monômes apparaissant dans son écriture sont de degré total k. Par convention, on conviendra que le polynôme nul est homogène de tout degré.*

Exemple 8.4. Le polynôme $X^5 + 4X^4Y - 2XY^4 + Y^5$ est homogène de degré 5 dans $\mathbb{R}[X, Y]$.

Remarque 8.4. Notons que si f est non nul, homogène de degré k, alors $\deg(f) = k$ (et donc k est unique).

Les observations de la preuve précédente impliquent :

Proposition 8.9.
1. *Si f et g sont homogènes de degré k, $f+g$ est homogène de degré k et pour tout $a \in \mathbb{A}$, af est homogène de degré k (autrement dit, l'ensemble $\mathbb{A}_k[X_1, \ldots, X_n]$ des polynômes homogènes de degré k est un sous $\mathbb{A}$-module de $\mathbb{A}[X_1, \ldots, X_n]$).*
2. *Si f est homogène de degré k et g est homogène de degré l, fg est homogène de degré $k + l$.*
3. *Soit $f \in \mathbb{A}[X_1, \ldots, X_n]$. Alors f s'écrit de manière unique $f = f_0 + \ldots + f_d$, avec $d = \deg(f)$, pour tout i, f_i est homogène de degré i, et $f_d \neq 0$. Les f_i sont appelés* composantes homogènes de f.

Démonstration. Seule l'unicité des composantes homogènes de f n'a pas été faite. On suppose que $f = f_0 + \ldots + f_d = f'_0 + \ldots + f'_d$. Alors $(f_0 - f'_0) + \ldots + (f_d - f'_d) = 0$. Chaque terme du membre de gauche est une somme de monômes de degré i, $0 \leqslant i \leqslant d$. Par unicité des coefficients, $f_0 - f'_0 = \ldots = f_d - f'_d = 0$, donc $(f_0, \ldots, f_d) = (f'_0, \ldots, f'_d)$. □

Proposition 8.10. *On suppose $\mathbb{A}$ intègre. Soit $f \in \mathbb{A}[X_1, \ldots, X_n]$, non nul, homogène. Alors tous les diviseurs de f sont eux-mêmes homogènes.*

Démonstration. Soit g un diviseur de f, de degré k. On pose $f = gh$, h étant de degré l. $\mathbb{A}$ étant intègre, f est homogène de degré $k + l$. Alors

$$f = \sum_{p=0}^{k+l} \sum_{i+j=p} g_i h_j + g_k h_l.$$

En identifiant les composantes homogènes de f,

$$\begin{cases} \displaystyle\sum_{i+j=p} g_i h_j = 0 \text{ si } 0 \leqslant p \leqslant k + l - 1, \\ g_k h_l = f. \end{cases}$$

Soit r le plus petit indice tel que $g_r \neq 0$ et s le plus petit indice tel que $h_s \neq 0$. Si $r < k$, la composante de degré $r + s < k + l - 1$ donne $g_r h_s = 0$. Par intégrité, $g_r = 0$ ou $h_s = 0$: absurde. Donc $r = k$ et $g = g_k$: g est homogène. □

Proposition 8.11. *Soit $f \in \mathbb{A}[X_1, \ldots, X_n]$. Alors f est homogène de degré k si, et seulement si, $f(TX_1, \ldots, TX_n) = T^k f(X_1, \ldots, X_n)$ dans $\mathbb{A}[X_1, \ldots, X_n, T]$.*

Démonstration. $\Longrightarrow$. Supposons f homogène de degré k. On pose alors

$$f = \sum_{k_1 + \ldots + k_n = k} a_{(k_1, \ldots, k_n)} X_1^{k_1} \ldots X_n^{k_n}.$$

Alors

$$\begin{aligned} f(TX_1,\dots,TX_n) &= \sum_{k_1+\dots+k_n=k} a_{(k_1,\dots,k_n)}(TX_1)^{k_1}\dots(TX_n)^{k_n} \\ &= \sum_{k_1+\dots+k_n=k} a_{(k_1,\dots,k_n)}T^{k_1+\dots+k_n}X_1^{k_1}\dots X_n^{k_n} \\ &= T^k \sum_{k_1+\dots+k_n=k} a_{(k_1,\dots,k_n)}X_1^{k_1}\dots X_n^{k_n} \\ &= T^k f. \end{aligned}$$

$\Longleftarrow$. Décomposons $f = f_0 + \dots + f_d$ en composantes homogènes. Par le premier point (sens direct),

$$\begin{aligned} f(TX_1,\dots,TX_n) &= f_0(TX_1,\dots,TX_n) + \dots + f_0(TX_1,\dots,TX_n) \\ &= f_0(X_1,\dots,X_n)T^0 + \dots + f_d(X_1,\dots,X_n)T^d \\ &= f(X_1,\dots,X_n)T^k. \end{aligned}$$

En identifiant les coefficients dans $\mathbb{A}[X_1,\dots,X_n][T]$, $f_i = 0$ si $i \neq k$ et $f = f_k$, donc f est homogène de degré k. □

9 Polynômes symétriques

9.1 Introduction et exemples

Le groupe symétrique $\mathfrak{S}_n$ agit sur $\mathbb{A}[X_1,\dots,X_n]$ par permutations des variables : si $\sigma \in \mathfrak{S}_n$,

$$\sigma.f(X_1,\dots,X_n) = f(X_{\sigma(1)},\dots,X_{\sigma(n)}).$$

Lorsque $\mathbb{A}$ est un corps, on obtient ainsi une représentation de $\mathfrak{S}_n$ de dimension infinie. On peut noter que l'espace $\mathbb{A}_k[X_1,\dots,X_n]$ des polynômes homogènes de degré k est un sous-espace invariant de $\mathfrak{S}_n$, de dimension finie. et on cherche la sous-représentations triviale de cette représentation, autrement dit les polynômes symétriques :

Définition 9.1. *Soit $f \in \mathbb{A}[X_1,\dots,X_n]$. On dira que f est* symétrique *si*

$$\forall \sigma \in \mathfrak{S}_n, \qquad f(X_{\sigma(1)},\dots,X_{\sigma(n)}) = f(X_1,\dots,X_n).$$

L'ensemble des polynômes symétriques de $\mathbb{A}[X_1,\dots,X_n]$ est noté $\mathbb{A}[X_1,\dots,X_n]^{Sym}$. Il s'agit d'une sous-algèbre de $\mathbb{A}[X_1,\dots,X_n]$.

Démonstration. Si f et g sont symétriques et si $a \in \mathbb{A}$, pour tout $\sigma \in \mathfrak{S}_n$,

$$\begin{aligned} (f+ag)(X_{\sigma(1)},\dots,X_{\sigma(n)}) &= f((X_{\sigma(1)},\dots,X_{\sigma(n)})) + ag((X_{\sigma(1)},\dots,X_{\sigma(n)}) \\ &= f(X_1,\dots,X_n) + ag(X_1,\dots,X_n) \\ &= (f+ag)(X_1,\dots,X_n), \end{aligned}$$

$$\begin{aligned} (fg)(X_{\sigma(1)},\dots,X_{\sigma(n)}) &= f(X_{\sigma(1)},\dots,X_{\sigma(n)})g(X_{\sigma(1)},\dots,X_{\sigma(n)}) \\ &= f(X_1,\dots,X_n)g(X_1,\dots,X_n) \\ &= (fg)(X_1,\dots,X_n). \end{aligned}$$

Donc $f+ag$ et fg sont symétriques. Le polynôme constant 1 est évidemment symétrique, donc $\mathbb{A}[X_1,\dots,X_n]^{Sym}$ est une sous-algèbre de $\mathbb{A}[X_1,\dots,X_n]$. □

Exemple 9.1. Voici quelques exemples de polynômes symétriques :

1. (Polynômes de Newton) : pour tout $k \geqslant 0$, $N_k^{(n)} = X_1^k + \dots + X_n^k$ est symétrique.

2. (Polynômes symétriques élémentaires) : si $1 \leqslant k \leqslant n$, on pose

$$\Sigma_k^{(n)} = \sum_{1 \leqslant i_1 < \ldots i_k \leqslant n} X_{i_1} \ldots X_{i_k}.$$

Ce sont des polynômes symétriques. Par exemple, si $n = 3$:

$$\Sigma_1^{(3)} = X_1 + X_2 + X_3, \qquad \Sigma_2^{(3)} = X_1X_2 + X_1X_3 + X_2X_3, \qquad \Sigma_3^{(3)} = X_1X_2X_3.$$

D'une manière générale, $\Sigma_1^{(n)} = X_1 + \ldots + X_n$ et $\Sigma_n^{(n)} = X_1 \ldots X_n$.

Proposition 9.2 (Relations coefficients-racines). *Dans* $\mathbb{A}[X_1, \ldots, X_n, T]$,

$$(T - X_1) \ldots (T - X_n) = T^n - \Sigma_1^{(n)} T^{n-1} + \Sigma_2^{(n)} T^{n-2} + \ldots + (-1)^n \Sigma_n^{(n)}.$$

Démonstration. Calcul direct. □

Remarque 9.1. Il est facile de voir que $\Sigma_k^{(n)}(X_1, \ldots, X_{n-1}, 0) = \Sigma_k^{(n-1)}$ si $0 \leqslant k < n$.

9.2 Indépendance algébrique des polynômes symétriques élémentaires

Théorème 9.3. *Soient* $f, g \in \mathbb{A}[Y_1, \ldots, Y_n]$. *Si* $f\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right) = g\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right)$, *alors* $f = g$. *On dit que* $\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}$ *sont* algébriquement indépendants.

Démonstration. Première étape. On montre d'abord que si $f \neq 0$, alors $f\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right) \neq 0$ par récurrence sur n. Si $n = 1$, comme $\Sigma_1^{(1)} = X_1$, $f\left(\Sigma_1^{(1)}\right) = f \neq 0$. Supposons le résultat vrai au rang $n-1$. Montrons alors le résultat par récurrence sur $deg(f)$. Si $deg(f) = 0$, f est constant et non nul, donc $f\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right)$ aussi. Supposons le résultat vrai pour tout polynôme de degré $deg(f) - 1$. On considère $f_1 = f(Y_1, \ldots, Y_{n-1}, 0)$. En évaluant $f\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right)$ en $X_n = 0$, on obtient

$$f\left(\Sigma_1^{(n-1)}, \ldots, \Sigma_{n-1}^{(n-1)}, 0\right) = f_1\left(\Sigma_1^{(n-1)}, \ldots, \Sigma_{n-1}^{(n-1)}\right).$$

Deux cas sont possibles :

1. Supposons $f_1 \neq 0$. Par l'hypothèse de récurrence sur n, $f_1\left(\Sigma_1^{(n-1)}, \ldots, \Sigma_{n-1}^{(n-1)}\right) \neq 0$, donc nécessairement $f(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}) \neq 0$.
2. Supposons $f_1 = 0$. En travaillant dans $\mathbb{K}[Y_1, \ldots, Y_{n-1}][Y_n]$, Y_n divise f : posons $f = Y_n g$. En considérant l'écriture en mônomes, on déduit que $deg(g) = deg(Y_n) - 1$, donc l'hypothèse de récurrence sur le degré s'applique à g : $g\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right) \neq 0$. En conséquence,

$$f\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right) = \Sigma_n^{(n)} g\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right) \neq 0,$$

même si $\mathbb{A}$ n'est pas intègre (il suffit de considérer l'écriture en monômes, comme $\Sigma_n^{(n)} = X_1 \ldots X_n$).

Seconde étape. Si $f\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right) = g\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right)$, $(f - g)\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right) = 0$. Par la première étape, nécessairement $f = g$. □

Remarque 9.2. Comme $\mathbb{A}[X_1, \ldots, X_n]^{Sym}$ est une algèbre, pour tout $f \in \mathbb{A}[Y_1, \ldots, Y_n]$, le polynôme $f\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right)$ est donc symétrique. On va voir (théorème fondamental) que la réciproque est vraie, c'est-à-dire que tout polynôme symétrique s'écrit sous la forme $f\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right)$.

Soit $f \in \mathbb{A}[Y_1, \ldots, Y_n]$. Quand $f\left(\Sigma_n^{(n)}, \ldots, \Sigma_n^{(n)}\right)$ est-il homogène ?

Définition 9.4. *1. Soit $Y_1^{a_1} \dots Y_n^{a_n}$ un monôme de $\mathbb{A}[Y_1, \dots, Y_n]$. Son* poids *est $1a_1 + \dots + na_n$.*

2. Soit $f \in \mathbb{A}[Y_1, \dots, Y_n]$, non nul. On dira qu'il est homogène de poids k *si tous les monômes apparaissant dans son écriture son de poids k. Par convention, 0 est homogène de tout poids k.*

Exemple 9.2. $Y_3 - Y_1Y_2 + 4Y_1^3$ est homogène de poids 3. Attention, il n'est pas homogène au sens de la définition 8.8.

Lemme 9.5. *Soit $f \in \mathbb{A}[Y_1, \dots, Y_n]$ et soit $k \geqslant 0$. Le polynôme $f\left(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}\right)$ est homogène de degré k si, et seulement si, f est homogène de poids k.*

Démonstration. $\Longleftarrow$. Soit $Y_1^{a_1} \dots Y_n^{a_n}$ un monôme de poids $1a_1 + \dots + na_n = k$. En remarquant que $\Sigma_i^{(n)}$ est homogène de degré i pour tout i, $\left(\Sigma_1^{(n)}\right)^{a_1} \dots \left(\Sigma_n^{(n)}\right)^{a_n}$ est homogène de degré $1a_1 + \dots + na_n = k$. Par suite, si f est homogène de poids k, en utilisant son écriture en monôme, $f\left(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}\right)$ est une combinaison linéaire de polynômes homogènes de degré k, donc est homogène de degré k.

$\Longrightarrow$. Comme pour le degré, en séparant les monômes suivant leurs poids, on peut écrire $f = f_0 + \dots + f_p$, où f_i est homogène de poids i pour i. En conséquence,

$$f\left(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}\right) = \underbrace{f_0\left(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}\right)}_{\text{homogène de degré } 0} + \dots + \underbrace{f_p\left(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}\right)}_{\text{homogène de degré } p}.$$

Comme $f\left(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}\right)$ est homogène de degré k, en identifiant les composantes homogènes, $f\left(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}\right) = f_k\left(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}\right)$. Par le théorème 9.3, $f = f_k$ est homogène de poids k. □

9.3 Théorème fondamental

Lemme 9.6. *1. Soit $\mathbb{A} \in \mathbb{A}[X_1, \dots, X_n]$. Alors $\mathbb{A}$ est symétrique si, et seulement si, toutes ses composantes homogènes sont symétriques.*

2. Soit $f \in \mathbb{A}[X_1, \dots, X_n]^{Sym}$. Alors $f(X_1, \dots, X_{n-1}, 0) \in \mathbb{A}[X_1, \dots, X_{n-1}]^{Sym}$. De plus, si f est homogène de degré k, alors $f(X_1, \dots, X_{n-1}, 0)$ est homogène de degré k.

Démonstration. Il est clair que si f est homogène de degré k, alors $f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ est aussi homogène de degré k. Par suite, les composantes homogènes de $f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ sont les $f_i(X_{\sigma(1)}, \dots, X_{\sigma(n)})$. En conséquence, en identifiant les composantes homogènes, on obtient l'équivalence de 1.

2. Posons $f_1 = f(X_1, \dots, X_{n-1}, 0)$. Soit $\sigma \in \mathfrak{S}_{n-1}$. Alors, comme f est symétrique, on a $f(X_{\sigma(1)}, \dots, X_{\sigma(n-1)}, X_n) = f$. En évaluant en $X_n = 0$, $f_1(X_{\sigma(1)}, \dots, X_{\sigma(n-1)}) = f_1$, donc f_1 est symétrique.

Supposons f homogène de degré k. Si $X_1^{a_1} \dots X_n^{a_n}$ est un monôme apparaissant dans f, alors $a_1 + \dots + a_n = k$. En évaluant ce monôme en $X_n = 0$, on trouve, soit lui-même si $a_n = 0$, soit 0 si $a_n \geqslant 1$. Donc dans f_1 n'apparaissent que des monômes de degré k : f_1 est homogène de degré k. □

Théorème 9.7. *Soit $f \in \mathbb{A}[X_1, \dots, X_n]^{Sym}$. Il existe un unique $g \in \mathbb{A}[Y_1, \dots, Y_n]$, tel que $f = g\left(\Sigma_1^{(n)}, \dots, \Sigma_n^{(n)}\right)$.*

Démonstration. Unicité. C'est le théorème 9.3.

Existence. Soit $f \in \mathbb{A}[X_1, \ldots, X_n]^{Sym}$. On va montrer qu'il existe $g \in \mathbb{K}[X_1, \ldots, X_n]$, tel que $f = g\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right)$. Par le lemme 9.6-1, en décomposant f en ses composantes homogènes, chacune d'elles est symétrique. Il suffit alors de prouver l'existence d'un g convenable pour chacune d'elles, puis de sommer : on est ainsi ramené au cas où f est homogène de degré k. On procéde par récurrence sur $n + k$. Plus précisément, montrons que pour tout polynôme $f \in \mathbb{A}[X_1, \ldots, X_n]^{Sym}$, homogène de degré k, il existe $g \in \mathbb{A}[Y_1, \ldots, Y_n]$, homogène de poids k, tel que $f = g\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right)$.

Initiation. Si $n = 1$, $X_1 = \Sigma_1^{(1)}$ et le résultat est évident, en prenant $g = f$. Si $k = 0$, f est constant et c'est évident. Si $k = 1$, par symétrie $f = a(X_1 + \ldots + X_n) = a\Sigma_1^{(n)}$ en on prend $g = aY_1$. Ces cas incluent $n + k = 1$.

Hérédité. Supposons le résultat vrai pour tout f' tel que $n' + k' \leqslant n + k - 1$. Posons $f_1 = f(X_1, \ldots, X_{n-1}, 0)$. Par le lemme 9.6-2, $f_1 \in \mathbb{A}[X_1, \ldots, X_{n-1}]^{Sym}$ et est homogène de degré k. L'hypothèse de récurrence s'applique à f_1, qu'on écrit donc sous la forme

$$f_1 = g_1\left(\Sigma_1^{(n-1)}, \ldots \Sigma_{n-1}^{(n-1)}\right),$$

avec g_1 homogène de poids k. Considérons $f_2 = f - g_1\left(\Sigma_1^{(n)}, \ldots, \Sigma_{n-1}^{(n)}\right)$. Alors f_2 est symétrique. Par le lemme 9.5, f_2 est homogène de degré k. De plus, $f_2(X_1, \ldots, X_{n-1}, 0) = f_1 - f_1 = 0$. En se plaçant dans $\mathbb{A}[X_1, \ldots, X_{n-1}][X_n]$, on obtient que X_n divise f_2. Comme f_2 est symétrique, $X_1, \ldots, X_{n-1}$ divisent f_2, et on déduit (même si $\mathbb{A}$ n'est pas intègre), en considérant l'écriture en monômes, que $X_1 \ldots X_n$ divise f_2. Donc $f_2 = \Sigma_n^{(n)} f_3(X_1, \ldots, X_n)$. De plus, $f_3(X_1, \ldots, X_n)$ est homogène de degré $k - n$. D'autre part, pour tout $\sigma \in \mathfrak{S}_n$, comme f_2 est symétrique, $X_1 \ldots X_n f_3(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = X_1 \ldots X_n f_3$. Comme $X_1, \ldots, X_n$ ne sont pas diviseurs de zéro, f_3 est symétrique. Par l'hypothèse de récurrence au rang $k - n + n < k + n$, il existe $g_3 \in \mathbb{A}[X_1, \ldots, X_n]$, homogène de poids $k - n$, tel que $f_3 = g_3\left(\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}\right)$. On prend alors $g = g_1 + Y_n g_3$, qui est bien homogène de poids k. □

9.4 Ordre lexicographique

On ordonne totalement les monômes de $\mathbb{A}[X_1, \ldots, X_n]$ par l'ordre lexicographique, avec $X_1 > \ldots > X_n$. Autrement dit, $X_1^{k_1} \ldots X_n^{k_n} > X_1^{l_1} \ldots X_n^{l_n}$ si $k_1 = l_1, \ldots, k_i = l_i$, $k_{i+1} > l_{i+1}$ pour un certain indice i.

Exemple 9.3. Si $n = 3$: $X_1 > X_2 > X_3$; $X_1^2 > X_1X_2 > X_1X_3 > X_2^2 > X_2X_3 > X_3^2$.

Définition 9.8. *Si $f = \sum a_{(k_1,\ldots,k_n)} X_1^{k_1} \ldots X_n^{k_n} \in \mathbb{A}[X_1, \ldots, X_n]$, non nul, le* monôme dominant *de f est $a_{(k_1,\ldots,k_n)} X_1^{k_1} \ldots X_n^{k_n}$, avec $X_1^{k_1} \ldots X_n^{k_n}$ maximal pour l'ordre lexicographique parmi les monômes apparaissant dans l'écriture de f. On le note* $\mathrm{MD}(f)$.

Exemple 9.4. Si $f = -5X_1^2X_3^4 + 2X_1^2X_2X_3 + 7X_1X_2^6X_3^2$, $\mathrm{MD}(f) = 2X_1^2X_2X_3$.

Proposition 9.9. *1. Si $X_1^{i_1} \ldots X_n^{i_n} < X_1^{j_1} \ldots X_n^{j_n}$, alors pour tous $k_1, \ldots, k_n$,*

$$X_1^{i_1+k_1} \ldots X_n^{i_n+k_n} < X_1^{j_1+k_1} \ldots X_n^{j_n+k_n}.$$

2. Si $X_1^{i_1} \ldots X_n^{i_n} < X_1^{j_1} \ldots X_n^{j_n}$ et si $X_1^{k_1} \ldots X_n^{k_n} < X_1^{l_1} \ldots X_n^{l_n}$, alors

$$X_1^{i_1+k_1} \ldots X_n^{i_n+k_n} < X_1^{j_1+l_1} \ldots X_n^{j_n+l_n}.$$

Démonstration. 1. Découle de la définition de l'ordre lexicographique.

2. D'après le premier point (appliqué deux fois),

$$X_1^{i_1+k_1}\dots X_n^{i_n+k_n} < X_1^{j_1+k_1}\dots X_n^{j_n+k_n} < X_1^{j_1+l_1}\dots X_n^{j_n+l_n}.$$

Comme l'ordre lexicographique est un ordre, on obtient le résultat. □

Proposition 9.10. *1. Soient f et $g \in \mathbb{A}[X_1,\dots,X_n]$, non nuls, tels que le coefficient de $\mathrm{MD}(f)$ ne soit pas un diviseur de zéro. Alors $\mathrm{MD}(fg) = \mathrm{MD}(f)\mathrm{MD}(g)$.*

2. Si $\mathbb{A}$ est intègre, pour tous f et $g \in \mathbb{A}[X_1,\dots,X_n]$, non nuls, $\mathrm{MD}(fg) = \mathrm{MD}(f)\mathrm{MD}(g)$.

Démonstration. 1. On pose $\mathrm{MD}(f) = aX_1^{k_1}\dots aX_n^{k_n}$ et $\mathrm{MD}(g) = bX_1^{l_1}\dots X_n^{l_n}$. Soit $X_1^{p_1}\dots X_n^{p_n}$ un monôme apparaissant dans fg. Par définition du produit, il existe $(i_1,\dots,i_n)$ et $(j_1,\dots,j_n)$, tels que $(i_1,\dots+i_n)+(j_1,\dots,j_n) = (p_1,\dots,p_n)$ et $X_1^{i_1}\dots X_n^{i_n}$ apparaît dans f, $X_1^{j_1}\dots X_n^{j_n}$ apparaît dans g. Par définition des monômes dominant, $X_1^{i_1}\dots X_n^{i_n} \leqslant X_1^{k_1}\dots X_n^{k_n}$ et $X_1^{j_1}\dots X_n^{j_n} \leqslant X_1^{l_1}\dots X_n^{l_n}$. D'après la proposition précédente, $X_1^{p_1}\dots X_n^{p_n} \leqslant X^{i_1+j_1}\dots X^{i_n+j_n}$, avec égalité si, et seulement si, $(i_1,\dots,i_n) = (k_1,\dots,k_n)$ et $(j_1,\dots,j_n) = (l_1,\dots,l_n)$. En conclusion, les monômes apparaissant dans fg sont tous $\leqslant X^{i_1+j_1}\dots X^{i_n+j_n}$ et le coefficient de $X^{i_1+j_1}\dots X^{i_n+j_n}$ est ab. Comme a ou b n'est pas un diviseur de zéro, $ab \neq 0$. Donc le monôme dominant de fg est $abX^{i_1+j_1}\dots X^{i_n+j_n} = \mathrm{MD}(f)\mathrm{MD}(g)$.

2. Car dans ce cas, les coefficients non nuls sont tous non diviseurs de zéro. □

Donnons maintenant une autre preuve de l'existence dans le théorème fondamental.

Démonstration. Soit $f \in \mathbb{A}[X_1,\dots,X_n]^{Sym}$, homogène de degré k. Montrons l'existence d'un g convenable pour ce f.

On considère l'ensemble des monômes de degré k de $\mathbb{A}[X_1,\dots,X_n]$. C'est un ensemble fini, totalement ordonné par l'ordre lexicographique : soient $M_1 < \dots < M_p$ ses éléments. Le monôme dominant de f est de la forme $\mathrm{MD}(f) = aM_i$. Posons $M_i = X_1^{k_1}\dots X_n^{k_n}$. On commence par décrire un processus permettant d'abaisser le monôme dominant.

Première étape. Montrons que $k_1 \geqslant k_2 \geqslant \dots \geqslant k_n$. Si ce n'est pas le cas on obtient par exemple $k_1 \geqslant k_2 \geqslant \dots \geqslant k_i$ et $k_i < k_{i+1}$. Par permutation des indéterminées X_i et X_{i+1}, comme f est symétrique, le monôme $X_1^{k_1}\dots X_i^{k_i+1}X_{i+1}^{k_i}\dots X_n^{k_n}$ apparaît aussi dans l'écriture de f. Or, il est plus grand strictement que $X_1^{k_1}\dots X_n^{k_n}$ pour l'ordre lexicographique : ceci contredit la définition du monôme dominant.

Seconde étape. Le monôme dominant de $\Sigma_i^{(n)}$ est $X_1\dots X_i$. D'après la proposition 9.10-1, le monôme dominant de $a\left(\Sigma_1^{(n)}\right)^{k_1-k_2}\dots\left(\Sigma_{n-1}^{(n)}\right)^{k_{n-1}-k_n}\left(\Sigma_n^{(n)}\right)^{k_n}$ est :

$$aX_1^{k_1-k_2+k_2-k_3+\dots+k_{n-1}-k_n+k_n}X_2^{k_2-k_3+\dots+k_{n-1}-k_n+k_n}\dots X_n^{k_n} = aX_1^{k_1}\dots X_n^{k_n} = \mathrm{MD}(f).$$

De plus, comme les $\Sigma_n^{(i)}$ sont homogènes de degré i, ce polynôme est homogène de degré

$$\begin{aligned}
&k_1 - k_2 + 2(k_2-k_3) + \dots + (n-1)(k_{n-1}-k_n) + nk_n\\
&= k_1 + (2-1)k_2 + (3-2)k_3 + \dots + (n-1-n+2)k_{n-1} + (n-n+1)k_n\\
&= k_1 + \dots + k_n\\
&= k.
\end{aligned}$$

Par suite, le polynôme $f_1 = f - a\left(\Sigma_1^{(n)}\right)^{k_1-k_2}\dots\left(\Sigma_{n-1}^{(n)}\right)^{k_{n-1}-k_n}\left(\Sigma_n^{(n)}\right)^{k_n}$ est symétrique et homogène de degré k et ne s'écrit qu'avec des monômes strictement inférieur à M_i.

Montrons maintenant le résultat par récurrence sur i. Si $i = 1$, alors f_1 ne s'écrit qu'avec des monômes strictement inférieur à M_1 : il est donc nul. Donc $f = a\left(\Sigma_1^{(n)}\right)^{k_1-k_2}\dots\left(\Sigma_n^{(n)}\right)^{k_n}$ et on prend $g = aX_1^{k_1-k_2}\dots X_{n-1}^{k_n-k_{n-1}}X_n^{k_n}$. Supposons le résultat vrai à tous les rangs $< i$. Alors l'hypothèse de récurrence s'applique à f_1. Par suite, on peut écrire $f_1 = g_1\left(\Sigma_1^{(n)},\dots,\Sigma_n^{(n)}\right)$ et on prend alors $g = g_1 + aX_1^{k_1-k_2}\dots X_{n-1}^{k_n-k_{n-1}}X_n^{k_n}$. □

Cette preuve est algorithmique. On en déduit aussi le résultat suivant :

Théorème 9.11. *L'algorithme suivant permet de calculer g dans le théorème fondamental. On considère un polynôme $f \in \mathbb{A}[X_1,\dots,X_n]^{Sym}$, homogène.*

- $g \leftarrow 0$.
- *Tant que f est non nul :*
  - *Trouver le monôme dominant $aX_1^{k_1}\dots X_n^{k_n}$ de f.*
  - $g \leftarrow g + aY_1^{k_1-k_2}Y_2^{k_2-k_3}\dots Y_{n-1}^{k_{n-1}-k_n}Y_n^{k_n}$.
  - $f \leftarrow f - a\left(\Sigma_1^{(n)}\right)^{k_1-k_2}\dots\left(\Sigma_{n-1}^{(n)}\right)^{k_{n-1}-k_n}\left(\Sigma_n^{(n)}\right)^{k_n}$.
- *Rendre g.*

Exemple 9.5. On prend $n = 3$ et

$$f = 2(X_1^3 + X_2^3 + X_3^3) + 7(X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2) + 11X_1X_2X_3.$$

Ce polynôme est bien symétrique, homogène de degré 3.

Première itération. Le monôme dominant de f est $2X_1^3$.

$$\begin{aligned}
g_1 &= 2Y_1^{3-0}Y_2^{0-0}Y_3^0 = 2Y_1^3,\\
f_1 &= f - 2\left(\Sigma_1^{(3)}\right)^3\\
&= f - 2((X_1^3 + X_2^3 + X_3^3) + 3(X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2) + 6X_1X_2X_3)\\
&= (X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2) - X_1X_2X_3.
\end{aligned}$$

Deuxième itération. Le monôme dominant de f_1 est $X_1^2X_2$.

$$\begin{aligned}
g_2 &= g_1 + Y_1^{2-1}Y_2^{1-0}Y_3^0 = 2Y_1^3 + Y_1Y_2,\\
f_2 &= f_1 - \Sigma_1^{(3)}\Sigma_2^{(3)}\\
&= f_1 - (X_1 + X_2 + X_3)(X_1X_2 + X_1X_3 + X_2X_3)\\
&= f_1 - (((X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2) + 3X_1X_2X_3)\\
&= -4X_1X_2X_3.
\end{aligned}$$

Troisième itération. Le monôme dominant de f_2 est $-4X_1X_2X_3$.

$$\begin{aligned}
g_3 &= g_2 - 4Y_1^{1-1}Y_2^{1-1}Y_3^1 = 2Y_1^3 + Y_1Y_2 - 4Y_3,\\
f_3 &= f_2 + 4\Sigma_3^{(3)}\\
&= f_2 + 4X_1X_2X_3\\
&= 0.
\end{aligned}$$

Donc $g = g_3 = 2Y_1^3 + Y_1Y_2 - 4Y_3$.

9.5 Formules de Newton

Dans le cas particulier des polynômes de Newton $N_k^{(n)} = X_1^k + \dots + X_n^k$, on dispose de formules permettant de calculer le polynôme g du théorème fondamental.

Théorème 9.12 (Formules de Newton). *1. Si $k \geqslant n$,*

$$N_k^{(n)} - \Sigma_1^{(n)} N_{k-1}^{(n)} + \ldots + (-1)^p \Sigma_p^{(n)} N_{k-p}^{(n)} + \ldots + (-1)^n \Sigma_n^{(n)} N_{k-n}^{(n)} = 0.$$

2. Si $k < n$,

$$N_k^{(n)} - \Sigma_1^{(n)} N_{k-1}^{(n-1)} + \ldots + (-1)^p \Sigma_p^{(n)} N_{k-p}^{(n)} + \ldots + (-1)^{k-1} \Sigma_{k-1}^{(n)} N_1^{(n)} + (-1)^k k \Sigma_k^{(n)} = 0.$$

Démonstration. 1. On considère le polynôme suivant dans $\mathbb{A}[X_1, \ldots, X_n, T]$,

$$f = T^{k-n}(T - X_1)\ldots(T - X_n) = T^k - \Sigma_1^{(n)} T^{k-1} + \ldots + (-1)^n \Sigma_n^{(n)} T^{k-n}.$$

On évalue T en X_i pour tout $1 \leqslant i \leqslant n$. On obtient

$$0 = X_i^k - \Sigma_1^{(n)} X_i^{k-1} + \ldots + (-1)^n \Sigma_n^{(n)} X_i^{k-n}.$$

En sommant ces n égalités,

$$0 = N_k^{(n)} - \Sigma_i^{(n)} N_{k-1}^{(n)} + \ldots + (-1)^n \Sigma_n^{(n)} N_{k-n}^{(n)}.$$

2. Soit $1 \leqslant k \leqslant n-1$. Pour tout $1 \leqslant i \leqslant n$,

$$\begin{aligned}
\frac{\partial \Sigma_{k+1}^{(n)}}{\partial X_i} &= \sum_{1 \leqslant j_1 < \ldots < j_{k+1} \leqslant n} \frac{\partial (X_{j_1} \ldots X_{j_{k+1}})}{\partial X_i} \\
&= \sum_{\substack{1 \leqslant i_1 < \ldots < i_k \leqslant n \\ \forall p, i_k \neq i}} X_{i_1} \ldots X_{i_k} \\
&= \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} X_{i_1} \ldots X_{i_k} - \sum_{\substack{1 \leqslant i_1 < \ldots < i_k \leqslant n \\ \exists p, i_k = i}} X_{i_1} \ldots X_{i_k} \\
&= \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} X_{i_1} \ldots X_{i_k} - X_i \sum_{\substack{1 \leqslant i_1 < \ldots < i_{k-1} \leqslant n \\ \forall p, i_p \neq i}} X_{i_1} \ldots X_{i_{k-1}} \\
&= \Sigma_k^{(n)} - X_i \frac{\partial \Sigma_{k-1}^{(n)}}{\partial X_i}.
\end{aligned}$$

Par une récurrence simple, on démontrerait que

$$\frac{\partial \Sigma_k^{(n)}}{\partial X_i} = \sum_{j=1}^{k} (-1)^{k-j} \Sigma_{j-1}^{(n)} X_i^{k-j},$$

avec la convention $\Sigma_0^{(n)} = 1$. En multipliant par X_i et en sommant,

$$\sum_{i=1}^{n} X_i \frac{\partial \Sigma_k^{(n)}}{\partial X_i} = \sum_{j=1}^{k} (-1)^{k-j} \Sigma_{j-1}^{(n)} N_{k-j+1}^{(n)} = \sum_{j=0}^{k-1} (-1)^{k-j+1} \Sigma_j^{(n)} N_{k-j}^{(n)}.$$

Par la formule d'Euler, ceci est égal à $k\Sigma_k^{(n)}$, car $\Sigma_k^{(n)}$ est homogène de degré k. En passant tout dans le membre de gauche et en multipliant par $(-1)^k$, on obtient la seconde formule de Newton. □

Ces formules permettent d'exprimer $N_k^{(n)}$ en fonction de $\Sigma_1^{(n)}, \ldots, \Sigma_n^{(n)}$ par récurrence sur n. Si $\mathbb{K}$ est un corps de caractéristique nulle, la seconde formule de Newton permet à l'inverse de calculer $\Sigma_k^{(n)}$ en fonction de $N_1^{(n)}, \ldots, N_n^{(n)}$ par récurrence sur k. On a besoin d'inverser un coefficient k, la caractéristique nulle est donc nécessaire. En combinant avec le théorème fondamental :

Corollaire 9.13. *Si $\mathbb{K}$ est un corps de caractéristique nulle, pour tout $f \in \mathbb{K}[X_1, \ldots, X_n]^{Sym}$, il existe un unique $h \in \mathbb{K}[Z_1, \ldots, Z_n]$ tel que $f = h\left(N_1^{(n)}, \ldots, N_n^{(n)}\right)$. Autrement dit, $N_1^{(n)}, \ldots, N_n^{(n)}$ engendrent $\mathbb{K}[X_1, \ldots, X_n]^{Sym}$ et sont algébriquement indépendants.*

Remarque 9.3. En caractéristique non nulle, les élements $N_1^{(n)}, \ldots, N_n^{(n)}$ ne sont pas nécessairement algébriquement indépendants. En effet, par l'endomorphisme de Frobenius,

$$N_p^{(n)} = X_1^p + \ldots + X_n^p = (X_1 + \ldots + X_n)^p = \left(N_1^{(n)}\right)^p.$$