Représentations des groupes finis

Prof. J. Thévenaz
TEXé par Cédric Ho Thanh

Printemps 2013

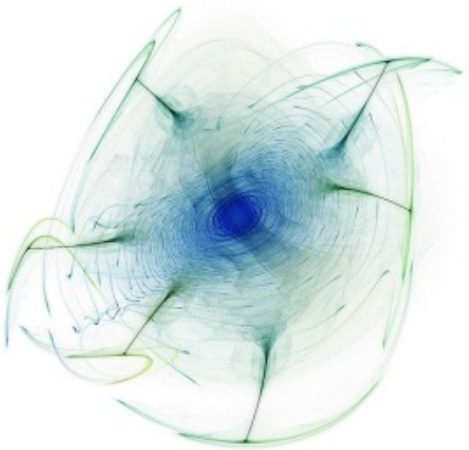


Table des matières

Introduction

Définition. Ce polycopié est le retranscription des notes du cours de représentations des groupes finis donné par le professeur J. Thévenaz durant le semestre de printemps 2013.

Corollaire. Malgré de nombreuses relectures, des erreurs peuvent subsister... ce polycopié est donc fourni sans garantie !

Chapitre 1

Représentations de groupes

1.0.1 Rappel. Soit V un espace vectoriel. Alors $\mathrm{GL}(V)$ est le groupe des transformations linéaires de V.

1.0.2 Définition ($\mathbb{K}$-représentation linéaire)**.** Soit G un groupe et $\mathbb{K}$ un corps. Une **$\mathbb{K}$-représentation linéaire** de G est un couple (V, ρ) où V est un $\mathbb{K}$-espace vectoriel et où $\rho : G \longrightarrow \mathrm{GL}(V)$ est un homomorphisme de groupes.

1.0.3 Convention. On supposera toujours que V est de dimension finie.

1.0.4 Définition (Degré d'une représentation)**.** Si (V, ρ) est une représentation de G, alors $\dim V$ s'appelle le **degré** de la représentation.

1.0.5 Définition (Représentation fidèle)**.** Une représentation (V, ρ) est **fidèle** si ρ est injective.

1.0.6 Définition (Représentation matricielle)**.** Une **$\mathbb{K}$-représentation matricielle** d'un groupe G est un homomorphisme de groupes $G \longrightarrow \mathrm{GL}_n(\mathbb{K})$.

1.0.7 Remarque. Si (V, ρ) est une $\mathbb{K}$-représentation de G et si l'on choisit une base E de V, alors on obtient une représentation matricielle

$$\begin{aligned} G &\longrightarrow \mathrm{GL}_n(\mathbb{K}) \\ g &\longmapsto \rho(g)_E^E. \end{aligned}$$

Pour chaque choix de base, on trouve une autre représentation matricielle.

1.0.8 Exemples.

1. Posons $G = \mathfrak{S}_3$. Alors $a = (123)$ et $b = (12)$ génèrent $\mathfrak{S}_3 = \{\mathrm{id}, a, a^2, b, ab, a^2b\}$. Soit

$$\begin{aligned} \rho_1 : \mathfrak{S}_3 &\longrightarrow \mathrm{GL}_3(\mathbb{R}) \\ a &\longmapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \\ b &\longmapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

que l'on étend. C'est bien un homomorphisme. On a ainsi représenté $\mathfrak{S}_3$ comme un groupe de matrices. De plus, ρ_1 est fidèle et $\mathfrak{S}_3 \cong \rho(\mathfrak{S}_3) \leq \mathrm{GL}_3(\mathbb{R})$.

2. Posons

$$\begin{aligned} \rho_2 : \mathfrak{S}_3 &\longrightarrow \mathrm{GL}_2(\mathbb{R}) \\ a &\longmapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \\ b &\longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

que l'on étend. Alors ρ_2 est aussi fidèle.

3. Posons

$$\begin{aligned} \rho_3 : \mathfrak{S}_3 &\longrightarrow \mathrm{GL}_2(\mathbb{R}) \\ a &\longmapsto \frac{1}{2}\begin{pmatrix} -1 & -\sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} && \text{rotation d'angle } \frac{2\pi}{3} \\ b &\longmapsto \frac{1}{2}\begin{pmatrix} -1 & \sqrt{3} \\ \sqrt{3} & 1 \end{pmatrix} && \text{symétrie.} \end{aligned}$$

Alors ρ_3 est fidèle.

4. Posons

$$\begin{aligned} \rho_4 : \mathfrak{S}_3 &\longrightarrow \mathrm{GL}_1(\mathbb{R}) = \mathbb{R}^* \\ a &\longmapsto 1 \\ b &\longmapsto -1. \end{aligned}$$

Pour tout $\tau \in \mathfrak{S}_3$, on a que $\rho_4(\tau)$ est la signature de τ. Cette représentation n'est pas fidèle.

5. Posons $G = D_{2n}$ le groupe dihédral d'ordre $2n$, i.e. le groupe des isométries d'un n-gône régulier. On a $D_{2n} = \{\mathrm{id}, r, r2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$. Soit C la base canonique de $\mathbb{R}^2$. On a la représentation naturelle

$$\begin{aligned} \rho_5 : D_{2n} &\longrightarrow \mathrm{GL}_2(\mathbb{R}) \\ r &\longmapsto r_C^C \\ s &\longmapsto s_C^C. \end{aligned}$$

6. Posons

$$\begin{aligned} \rho_6 : D_{2n} &\longrightarrow \mathrm{GL}_2(\mathbb{R}) \\ r &\longmapsto \text{rotation d'angle } \frac{2\pi}{n} \text{ d'axe } z \\ s &\longmapsto \text{symétrie de plan } xz. \end{aligned}$$

7. Posons

$$\begin{aligned} \rho_7 : D_{2n} &\longrightarrow \mathrm{GL}_2(\mathbb{R}) \\ r &\longmapsto \text{rotation d'angle } \frac{2\pi}{n} \text{ d'axe } z \\ s &\longmapsto \text{symétrie d'axe } x. \end{aligned}$$

1.0.9 Remarque. La donnée d'une $\mathbb{K}$-représentation linéaire (V, ρ) est équivalente à la donnée d'une action linéaire de G sur V.

1.0.10 Définition (Homomorphisme, isomorphisme de représentations)**.** Soient $\rho_V : G \longrightarrow \mathrm{GL}(V)$ et $\rho_W : G \longrightarrow \mathrm{GL}(W)$ deux $\mathbb{K}$-représentations de G. Un **homomorphisme** ϕ entre ρ_V et ρ_W est une application linéaire $\phi : V \longrightarrow W$ telle que

$$\phi \circ \rho_V(g) = \rho_W(g) \circ \phi, \qquad \forall g \in G.$$

Autrement dit, le diagramme suivant commute :

$$\begin{array}{ccc} V & \xrightarrow{\rho_V(g)} & V \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ W & \xrightarrow{\rho_W(g)} & W \end{array} .$$

Si de plus ϕ est bijective, alors c'est un **isomorphisme** entre les deux représentations. On dit aussi que les deux représentations sont équivalentes .

1.0.11 Remarque. Si ϕ est un isomorphisme de représentations, alors ϕ^{-1} l'est aussi.

1.0.12 Définition. Deux représentations matricielles $\rho_1, \rho_2 : G \longrightarrow \mathrm{GL}_n(\mathbb{K})$ sont équivalentes s'il existe une matrice inversible S telle que

$$\rho_2(g) = S\rho_1(g)S^{-1}, \qquad \forall g \in G.$$

1.0.13 Remarque. Soit $\rho : G \longrightarrow \mathrm{GL}(V)$ une représentation de G, E et F deux bases de V et $\rho_E, \rho_F : G \longrightarrow \mathrm{GL}_n(\mathbb{K})$ les représentations matricielles correspondantes. Alors ρ_E et ρ_F sont équivalentes.

1.0.14 Définitions (Quelques représentations particulières)**.** Soit G un groupe.

Représentation triviale : posons

$$\begin{aligned} \rho : G &\longrightarrow \mathrm{GL}_1(\mathbb{K}) = \mathbb{K}^* \\ g &\longmapsto 1_{\mathbb{K}}. \end{aligned}$$

Représentation régulière : on prend pour V un $\mathbb{K}$-espace vectoriel de dimension $\sharp G$ muni d'une base $E = \{e_g\}_{g\in G}$ dont les éléments sont indexés par les éléments de G. On fait agir G sur E par multiplication :

$$g \cdot e_h = e_{gh}$$

et on étend cette action par linéarité. Ceci définit la représentation régulière ρ_{reg} de G.

Représentation de permutations : On se donne X un G-ensemble (i.e. un ensemble X muni d'une action de G sur X). On prend pour V un $\mathbb{K}$-espace vectoriel de dimension $\sharp X$ muni d'une base $E = \{e_x\}_{x\in X}$ dont les éléments sont indexés par les éléments de X. On fait agir G sur E par multiplication :

$$g \cdot e_x = e_{g\cdot x}$$

et on étend cette action par linéarité.

1.0.15 Exemple. Posons $G = \mathfrak{S}_n$. Alors $\mathfrak{S}_n$ agit de manière évidente sur l'ensemble $\{1, \ldots, n\}$. On obtient dont une représentation de permutations de degré n qui est appelée la représentation naturelle de $\mathfrak{S}_n$.

1.0.16 Définition (Sous représentation)**.** Soit $\rho : G \longrightarrow \mathrm{GL}(V)$ une $\mathbb{K}$-représentation de G. Soit $W \leq V$ un sous espace vectoriel de V. On dit que W est G-invariant si $\rho(g)(W) \subseteq W$, $\forall g \in G$. Dons ce cas, on peut restreindre l'action de G au sous espace W et cela définit une **sous représentation** de ρ :

$$\begin{aligned} \rho_W : G &\longrightarrow \mathrm{GL}(W) \\ g &\longmapsto \rho(g)|_W^W. \end{aligned}$$

Matriciellement, on choisit une base de W que l'on complète en une base de V :

$$\rho(g) = \begin{pmatrix} \rho(g)|_W^W & * \\ 0 & * \end{pmatrix}.$$

1.0.17 Exercice. La représentation triviale est équivalente à une sous représentation de n'importe quelle représentation de permutations.

1.0.18 Définition (Somme directe)**.** Soit $\rho : G \longrightarrow \mathrm{GL}(V)$ une $\mathbb{K}$-représentation d'un groupe G. Soient W_1 et W_2 deux sous espaces G-invariants de V et ρ_{W_i} les sous représentations correspondantes. On dit que V est la **somme directe** de W_1 et W_2 si $V = W_1 \oplus W_2$. Matriciellement, on choisit une base de V formae de la réunion d'une base de W_1 et d'une base de W_2. Alors :

$$\rho(g) = \begin{pmatrix} \rho(g)|_{W_1}^{W_1} & 0 \\ 0 & \rho(g)|_{W_2}^{W_2} \end{pmatrix}.$$

Ainsi, une somme directe est équivalente à une décomposition de la matrice de $\rho(g)$ en blocs.

1.0.19 Définition (Somme directe externe)**.** On se donne deux $\mathbb{K}$-représentations $\rho_{V_1} : G \longrightarrow \mathrm{GL}(V_1)$ et $\rho_{V_2} : G \longrightarrow \mathrm{GL}(V_2)$. On construit la **somme directe externe** $V = V_1 \times V_2$ et on identifie V_1 avec $V_1 \times \{0\}$ et $V_2 = \{0\} \times V_2$. On a deux sous espaces de V et $V = (V_1 \times \{0\}) \oplus (\{0\} \times V_2)$. On définit une représentation sur V :

$$\begin{aligned} \rho : G &\longrightarrow \mathrm{GL}(V) \\ g &\longmapsto (\rho_{V_1}(g), \rho_{V_2}(g)). \end{aligned}$$

1.0.20 Exemple. Posons $G = C_3$, le groupe cyclique d'ordre 3 généré par c. Posons $\rho : C_3 \longrightarrow \mathrm{GL}(V)$ la représentation régulière de C_3, où V est de base $\{e_1, e_c, e_{c^2}\}$. Posons $W_1 = \mathrm{Vect}(e_1 + e_c + e_{c^2})$ et $W_2 = \mathrm{Vect}(e_1 - e_c, e_1 - e_{c^2})$. Ce sont deux sous espaces C_3-invariants. Si $\mathbb{K}$ n'est pas de caractéristique 3, alors $\{e_1 + e_c + e_{c^2}, e_1 - e_c, e_1 - e_{c^2}\}$ forme une base de V et $V = W_1 \oplus W_2$.

1.0.21 Définition (Représentation irréductible)**.** Une représentation $\rho : G \longrightarrow \mathrm{GL}(V)$ est dite **irréductible** si :

1. $V \neq \{0\}$,
2. ρ n'admet pas de sous représentation, i.e. il n'existe pas de sous espace strict de V qui soit G-invariant.

1.0.22 Exemple. Toute représentation de degré 1 est irréductible.

1.0.23 Théorème (Maschke)**.** Soit G un groupe fini. Soit $\rho : G \longrightarrow \mathrm{GL}(V)$ une $\mathbb{K}$-représentation de G. Soit W un sous espace G-invariant de V. Si $|G| \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$ (i.e. $\mathrm{car}\,\mathbb{K} \not| |G|$), alors W possède un supplémentaire G-invariant U.

Démonstration. Soit U_0 un supplémentaire de W. Soit $p_0 : V \longrightarrow V$ la projection associée, i.e. $p_0(w+u_0) = w$, $\forall w \in W, \forall u_0 \in U_0$. On a $\operatorname{im} p_0 = W$ et $\ker p_0 = U_0$. On définit $p : V \longrightarrow V$ par

$$p(v) = \frac{1}{|G|} \sum_{g\in G} \rho(g) \circ p_0 \circ \rho(g^{-1})(v).$$

Remarquer que $\frac{1}{|G|}$ est bien définit par hypothèse. On procède ensuite en plusieurs étapes :

1. On a
$$p(w) = \frac{1}{|G|} \sum_{g\in G} \underbrace{\rho(g) \circ p_0 \circ \underbrace{\underbrace{\rho(g^{-1})(w)}_{\in W}}_{\in W}}_{\in W} \in W.$$
Ainsi, $\operatorname{im} p \subseteq W$. Montrons que $p|_W = \mathrm{id}_W$. Soit $w \in W$. On a
$$p(w) = \frac{1}{|G|} \sum_{g\in G} \underbrace{\rho(g) \circ \underbrace{p_0 \circ \rho(g^{-1})(w)}_{=\rho(g^{-1})(w)}}_{=w} = w.$$
Donc $\operatorname{im} p = W$. De plus, p est un projecteur sur W.
2. Comme p est un projecteur, on a $V = \ker p \oplus \operatorname{im} p$.
3. Soit $h \in G$. On veut montrer que $p \circ \rho(h) = \rho(h) \circ p$. On a
$$\begin{aligned}
\rho(h) \circ p &= \frac{1}{|G|} \sum_{g\in G} \rho(h) \circ \rho(g) \circ p_0 \circ \rho(g^{-1}) \\
&= \frac{1}{|G|} \sum_{g\in G} \underbrace{\rho(h) \circ \rho(g)}_{=\rho(hg)} \circ p_0 \circ \underbrace{\rho(g^{-1}) \circ \rho(h^{-1})}_{=\rho((hg)^{-1})} \circ \rho(h) \\
&= \frac{1}{|G|} \sum_{s\in G} \rho(s) \circ p_0 \circ \rho(s^{-1}) \circ \rho(h) \qquad\qquad s = hg \\
&= p \circ \rho(h).
\end{aligned}$$
4. Soit $h \in G$ et $u \in U = \ker p$. Alors
$$\begin{aligned}
p \circ \rho(h)(u) &= \rho(h) \circ p(u) \\
&= 0.
\end{aligned}$$
Donc $\rho(h)(u) \in \ker p = U$, ce qui montre que U est G-invariant.

□

1.0.24 Corollaire. Si $|G| \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$, alors toute $\mathbb{K}$-représentation de G de degré fini est somme directe de représentations irréductibles.

Démonstration. Soit $\rho : G \longrightarrow \mathrm{GL}(V)$ une $\mathbb{K}$-représentation de G. Si ρ est irréductible, alors c'est bon. Sinon, il existe un sous espace strict W de V qui est G-invariant. Par le théorème de Maschke, W possède un supplémentaire G-invariant U. Par récurrence sur la dimension, on prouve le résultat. □

Si $\mathbb{K} = \mathbb{C}$, alors le théorème de Maschke peut aussi être prouvé grâce aux deux propositions suivantes.

1.0.25 Proposition. Soit $\rho : G \longrightarrow \mathrm{GL}(V)$ une $\mathbb{C}$-représentation d'un groupe fini G. Alors il existe sur V une produit scalaire (i.e. une forme sesquilinéaire hermitienne définie positive) $\langle -, - \rangle$ invariant par G, i.e. $\langle \rho(g)(v), \rho(g)(w) \rangle = \langle v, w \rangle$. Ainsi, $\rho(g)$ est une application unitaire $\forall g \in G$.

Démonstration. Soit $\langle -, - \rangle_0$ un produit scalaire quelconque sur V. On définit

$$\langle v, w \rangle = \sum_{g \in G} \langle \rho(g)(v), \rho(g)(w) \rangle_0.$$

Il est claire que c'est de nouveau un produit scalaire et qu'il est invariant par l'action de G. □

1.0.26 Proposition. Soit $\rho : G \longrightarrow U(V)$, une représentation de G (où $U(V)$ est le groupe des transformations unitaires de V). Si W est un sous espace de V qui est G-invariant, alors W possède un supplémentaire G-invariant.

Démonstration. Considérer $W^{\perp}$. □

1.0.27 Théorème. Soit G un groupe fini. Les conditions suivantes sont équivalentes :

1. $|G| \cdot 1_{\mathbb{K}} = 0_{\mathbb{K}}$,
2. Pour toute représentation $\rho : G \longrightarrow \mathrm{GL}(V)$ et pour tout sous espace invariant $W \subseteq V$, il existe un supplémentaire invariant de W,
3. Pour tout représentation régulière de G sur $V = \mathrm{Vect}(e_g \mid g \in G)$, le sous espace G-invariant $W = \mathrm{Vect}(e_1 - e_g \mid g \in G \setminus \{1\})$ possède un supplémentaire orthogonal.

Démonstration. $1 \implies 2$: Par le théorème de Maschke.

$2 \implies 3$: Trivial.

$3 \implies 1$: W est bien un sous espace invariant car $\rho(g)(e_1 - e_h) = e_g - e_{gh} = (e_1 - e_{gh}) - (e_1 - e_g) \in W$. Par hypothèse, W possède un supplémentaire invariant U. Remarquons que $\dim V = |G|$ et que $\dim W = |G| - 1$. Donc $\dim U = 1$. Soit $u \in U$ et écrivons $u = \sum_{g \in G} \lambda_g e_g$. Soit $h \in G$. Alors

$$\rho(h)(u) - u = \sum_{g \in G} \lambda_g \underbrace{(e_{gh} - e_g)}_{\in W} \in W.$$

Or U est invariant, et donc $\rho(h)(u) - u \in W \cap U = \{0\}$ ce qui implique que $u = \rho(h)(u)$ et G agit trivialement sur U. Par ailleurs

$$\begin{aligned} u = \sum_{g \in G} \lambda_g e_g = \rho(h)(u) = \sum_{g \in G} \lambda_g e_{hg} = \sum_{s \in G} \lambda_{h^{-1}s} e_s \\ \implies \lambda_s = \lambda_{h^{-1}s}, \quad \forall s, h \in G \\ \implies \lambda_h = \lambda_1, \quad \forall h \in G \qquad \implies U = \mathrm{Vect}(\sum_{g \in G} e_g). \end{aligned}$$

On sait que $W \oplus U = V$ et on écrit e_1 dans cette décomposition :

$$\begin{aligned} e_1 &= \underbrace{\sum_{g \in G \setminus \{1\}} \mu_g (e_1 - e_g)}_{\in W} + \underbrace{\lambda \sum_{g \in G} e_g}_{\in U} \\ &= \underbrace{\sum_{g \in G \setminus \{1\}} (\lambda - \mu_g) e_g}_{=0} + \underbrace{\left(\lambda + \sum_{g \in G \setminus \{1\}} \mu_g \right)}_{=1_{\mathbb{K}}} e_1. \end{aligned}$$

Donc $\lambda - \mu_g = 0, \quad \forall g \in G \setminus \{1\}$ ce qui implique $\lambda = \mu_g$. Puis,

$$\begin{aligned} 1_{\mathbb{K}} &= \lambda + \sum_{g \in G \setminus \{1\}} \lambda \\ &= |G| \cdot \lambda \\ &\implies |G| \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}. \end{aligned}$$

□

Chapitre 2

Algèbre de groupe et modules

2.0.28 Rappels. Soit A un anneau et M un A-module. On dit que
- M est **simple** s'il n'admet pas de sous module strict,
- M est **semi simple** s'il est somme directe de sous modules simples.

2.0.29 Définition (Algèbre d'un groupe)**.** Soit G un groupe et $\mathbb{K}$ un corps. L'**algèbre du groupe** $\mathbb{K}G$ est le $\mathbb{K}$-espace vectoriel de base G, où la multiplication est donnée par celle du groupe, puis étendue par bilinéarité. On obtient une $\mathbb{K}$-algèbre. On identifie $\mathbb{K}$ à une sous algèbre de $\mathbb{K}G$ via :

$$\begin{aligned} \mathbb{K} &\hookrightarrow \mathbb{K}G \\ \lambda &\mapsto \lambda \cdot 1_G. \end{aligned}$$

2.0.30 Propriété. Soit G un groupe et $\mathbb{K}$ un corps. La donnée d'une $\mathbb{K}$-représentation $\rho : G \longrightarrow \mathrm{GL}(V)$ est équivalente à la donnée d'une structure de $\mathbb{K}G$-module à gauche sur V.

Démonstration.
1. On se donne une $\mathbb{K}$-représentation $\rho : G \longrightarrow \mathrm{GL}(V)$. On définit une structure de $\mathbb{K}G$-module à gauche sur V par :
$$\begin{aligned} \mathbb{K}G \times V &\longrightarrow V \\ (g, v) &\longmapsto \rho(g)(v) \end{aligned}$$
étendue par linéarité. On vérifie les axiomes.
2. On se donne une $\mathbb{K}G$-module à gauche V et on définit
$$\begin{aligned} \rho : G &\longrightarrow \mathrm{GL}(V) \\ g &\longmapsto \begin{pmatrix} \rho(g) : & V & \longrightarrow & V \\ & v & \longmapsto & g \cdot v \end{pmatrix}. \end{aligned}$$
On vérifie que $\rho(g)$ est bien $\mathbb{K}$-linéaire et on vérifie le reste des axiomes.

□

2.0.31 Exercice. Faire tous les détails de la preuve précédente.

2.0.32 Convention. Désormais, on parlera de $\mathbb{K}G$-modules à gauche. On écrira $g \cdot v = gv$ au lieu de $\rho(g)(v)$. Si nécessaire, on utilisera la représentation correspondante $\rho_V : G \longrightarrow \mathrm{GL}(V)$.

Voici un petit dictionnaire :

$\mathbb{K}$-représentation de G	$\mathbb{K}G$-module à gauche
Homomorphisme de représentation	Homomorphisme de $\mathbb{K}G$-module
Sous représentation	Sous $\mathbb{K}G$-module
Somme directe de représentations	Somme directes de modules
Représentation irréductible	$\mathbb{K}G$-module simple
Représentation complètement réductible	$\mathbb{K}G$-module semi simple
Représentation régulière	$\mathbb{K}G$ vu comme une $\mathbb{K}G$-module

2.0.33 Corollaire (du théorème de Mashke)**.** Si G est fini et $|G| \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$, alors tout $\mathbb{K}G$-module est semi simple.

2.0.34 Lemme (de Schur, général)**.** Soit A un anneau et soient S, T deux A-modules simples et non isomorphes. Alors

1. $\mathrm{Hom}_A(S,T) = \{0\}$,
2. $\mathrm{End}_A(S)$ est un anneau de division.

Démonstration.
1. Soit $\phi : S \longrightarrow T$ un homomorphisme. Supposons ϕ non nul et montrons que $S \cong T$. Comme ϕ est non nul, $\ker\phi \neq S$. Mais c'est un sous module de S. Donc $\ker\phi = \{0\}$ et ϕ est injectif. Puis, $\mathrm{im}\,\phi \neq \{0\}$ et est un sous module de T. Donc $\mathrm{im}\,\phi = T$ et ϕ est surjective, et par conséquent un isomorphisme.
2. Soit $\phi \in \mathrm{End}_A(S)$. Par exactement le même raisonnement, on montre que ϕ est un automorphisme, donc inversible.

□

2.0.35 Lemme (de Schur, sur un corps algébriquement clos)**.** Soit A une $\mathbb{K}$-algèbre de dimension finie où $\mathbb{K}$ est un corps algébriquement clos. Soit S un A-module simple. Alors

$$\mathrm{End}_A(S) = \{\lambda\,\mathrm{id}_S \mid \lambda \in \mathbb{K}\}.$$

On a donc que $\mathrm{End}_A(S) \cong \mathbb{K}$.

Démonstration. On constate d'abord que S est un $\mathbb{K}$-espace vectoriel de dimension finie, car $S \cong A/I$ où I est un certain idéal de A (cf. série 4) et car A est de dimension finie. Alors $\mathrm{End}_A(S) \cong M_n(\mathbb{K})$, où $n = \dim S$. Donc $\mathbb{K}\,\mathrm{id}_S \subseteq \mathrm{End}_A(S) \subseteq \mathrm{End}_{\mathbb{K}}(S)$. Par conséquent, $\mathrm{End}_A(S)$ est une $\mathbb{K}$-algèbre de dimension finie. De plus, $\mathrm{End}_A(S)$ est un anneau (algèbre) de division. Soit $\phi \in \mathrm{End}_A(S)$. Comme $\mathbb{K}$ est algébriquement clos, ϕ possède au moins une valeur propre λ. Alors

$$\begin{aligned} \ker(\phi - \lambda\,\mathrm{id}_S) \neq \{0\} &\implies \ker(\phi - \lambda\,\mathrm{id}_S) = S \\ &\implies \phi = \lambda\,\mathrm{id}_S\,. \end{aligned}$$

□

2.0.36 Remarque. Si A est
- une algèbre de division,
- de dimension finie,
- sur un corps $\mathbb{K}$ algébriquement clos,

alors $A \cong \mathbb{K}$.

2.0.37 Corollaire (Cas particulier)**.** Si S est un $\mathbb{C}G$-module simple (où G est un groupe fini), alors $\mathrm{End}_{\mathbb{C}G}(S) = \mathbb{C}\,\mathrm{id}_S$.

2.0.38 Proposition. Soient G un groupe fini tel que $|G| \cdot 1_{\mathbb{K}} \neq 0_{\mathbb{K}}$. On se donne deux $\mathbb{K}G$-modules M et N. On prend une application $\mathbb{K}$-linéaire $\psi : M \longrightarrow N$. On effectue la "**moyenne** sur G" :

$$\phi = \frac{1}{|G|} \sum_{g \in G} g\phi g^{-1} = \frac{1}{|G|} \sum_{g \in G} \rho_N(g) \circ \psi \circ \rho_M(g^{-1}).$$

Alors ϕ est $\mathbb{K}G$-linéaire.

Démonstration. Déja vue dans la preuve du théorème de Mashke. Soit $h \in G$. Alors

$$\begin{aligned} \rho_N(h) \circ \phi &= \sum_{g \in G} \underbrace{\rho_N(h) \circ \rho_N(g)}_{=\rho_N(hg)} \circ \psi \circ \rho_M(g^{-1}) \\ &= \sum_{s \in G} \rho_N(s) \circ \psi \circ \rho_M(s^{-1}h) \\ &= \phi \circ \rho_M(h). \end{aligned}$$

Donc $\phi(hm) = h\phi(m)$. On étend le résultat par $\mathbb{K}G$-linéarité. □

2.0.39 Lemme (de Schur, pour les représentations)**.** Soient S et T deux $\mathbb{C}G$-modules non isomorphes.

1. Pour toute application $\mathbb{C}$-linéaire $\psi : S \longrightarrow T$, on a
$$\frac{1}{|G|} \sum_{g \in G} g\psi g^{-1} = 0.$$
2. Pour toute application $\mathbb{C}$-linéaire $\psi : S \longrightarrow S$, on a
$$\frac{1}{|G|} \sum_{g \in G} g\psi g^{-1} = \lambda \operatorname{id}_S, \qquad \text{où } \lambda = \frac{\operatorname{tr} \psi}{\dim S}.$$

Démonstration.
1. La moyenne est $\mathbb{C}G$-linéaire, donc nulle par le lemme de Schur.
2. La moyenne est un endomorphisme $\mathbb{C}G$-linéaire et $\mathbb{C}$ est algébriquement clos. On applique le lemme de Schur. Pour trouver la valeur de λ, posons $n = \dim S$:

$$\begin{aligned} n\lambda &= \operatorname{tr}(\lambda \operatorname{id}_S) \\ &= \operatorname{tr}\left(\frac{1}{|G|} \sum_{g \in G} g\psi g^{-1} \right) \\ &= \frac{1}{|G|} \sum_{g \in G} \operatorname{tr}(g\psi g^{-1}) \\ &= \frac{1}{|G|} |G| \operatorname{tr}(\psi) \\ \implies \lambda &= \frac{\operatorname{tr} \psi}{\dim S}. \end{aligned}$$

□

2.0.40 Théorème. Soit G un groupe fini abélien. Alors tout $\mathbb{C}G$-module simple est de dimension 1.

Démonstration. Soit S un $\mathbb{C}G$-module simple de $g \in G$. Alors

$$\begin{aligned} \rho_S(g) : S &\longrightarrow S \\ s &\longmapsto gs \end{aligned}$$

est $\mathbb{C}G$-linéaire car G est abélien. En effet, $\mathbb{C}G$ est un anneau commutatif, et $\forall a \in \mathbb{C}G$,

$$\begin{aligned} \rho_S(g)(as) &= gas \\ &= ags \\ &= a\rho_S(g)(s). \end{aligned}$$

Par le lemme de Schur, $\rho_S(g) = \lambda \,\mathrm{id}_S$. En particulier, tout sous espace de S est invariant par action à gauche de g, pour tout $g \in G$. Donc tout sous espace de S est un sous $\mathbb{C}G$-module de S. Or S est simple, donc $\dim S = 1$. □

2.0.41 Théorème (de diagonalisation)**.** Soit M un $\mathbb{C}G$ module. Fixons $g \in G$. Alors il existe une base B par rapport à laquelle la matrice de l'action de g (i.e. $\rho_M(g)$) est diagonale :

$$\rho_M(g)_B^B = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n \end{pmatrix}.$$

De plus, chaque ε_i est une racine k-ième de l'unité, où k est l'ordre de g.

Démonstration. Soit $H = \langle g \rangle$, le sous groupe cyclique d'ordre k engendré par g. C'est un groupe abélien. On considère M comme un $\mathbb{C}H$-module, par restriction. On décompose ce $\mathbb{C}H$-module en somme directe de modules simples :

$$M = S_1 \oplus \cdots \oplus S_r.$$

Par le théorème précédent, $\dim S = 1, \forall 1 \leq i \leq r$. On choisi une base $B = \{v_i\}_{1 \leq i \leq r}$, où $v_i \in S_i \backslash \{0\}$ de M. L'action de g préserve chaque S_i (car S_i est un sous $\mathbb{C}H$-module), donc $gv_i \in S_i$, c'est à dire $gv_i = \varepsilon_i v_i$, avec $\varepsilon_i \in \mathbb{C}$. Donc l'action de g est diagonale :

$$\rho_M(g)_B^B = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n \end{pmatrix}.$$

De plus, $\rho_M(g)^k = \rho_M(g^k) = \rho_M(1_G) = \mathrm{id}_M$. Matriciellement, $(\rho_M(g)_B^B)^k = \mathrm{Id}_r$ ce qui comme $\varepsilon_i^k = 1_{\mathbb{K}}$. □

Chapitre 3

Caractère d'un groupe fini

3.0.42 Définition (Caractère)**.** Soit G un groupe fini, V un $\mathbb{C}G$ module et $\rho_V : G \longrightarrow \mathrm{GL}(V)$ la représentation correspondante. Le **caractère** de V est la fonction

$$\begin{aligned} \chi_V : G &\longrightarrow \mathbb{C} \\ g &\longmapsto \operatorname{tr} \rho_V(g). \end{aligned}$$

3.0.43 Rappels.

1. La **classe de conjugaison** d'un élément $g \in G$ est l'ensemble $\{xgx^{-1} \mid x \in G\}$. Ces classes partitionnent G.
2. Un **fonction centrale** $f : G \longrightarrow X$ est une fonction qui est constante sur les classes de conjugaisons. De manière équivalente, une fonction est centrale si

$$f(xy) = f(yx), \qquad \forall x, y \in G.$$

3.0.44 Proposition. Un caractère χ_V est une fonction centrale.

Démonstration. On a :

$$\begin{aligned} \chi_V(xgx^{-1}) &= \operatorname{tr}\left(\rho_V(x)\rho_V(g)\rho_V(x)^{-1}\right) \\ &= \operatorname{tr} \rho_V(g) \\ &= \chi_V(g). \end{aligned}$$

□

3.0.45 Proposition. Soit $V \oplus W$ une somme directe de deux $\mathbb{C}G$ modules V et W. Alors

$$\chi_{V\oplus W} = \chi_V + \chi_W.$$

Démonstration. Soit E une base de V et F une base de W. Alors $E \cup F$ est une base de $V \oplus W$. On écrit les matrices par rapport à cette base :

$$\rho_{V\oplus W}(g)^{E\cup F}_{E\cup F} = \begin{pmatrix} \rho_V(g)^E_E & 0 \\ 0 & \rho_W(g)^F_F \end{pmatrix}.$$

Donc

$$\begin{aligned} \chi_{V\oplus W}(g) &= \operatorname{tr} \rho_{V\oplus W}(g) \\ &= \operatorname{tr} \rho_V(g) + \operatorname{tr} \rho_W(g) \\ &= \chi_V(g) + \chi_W(g). \end{aligned}$$

□

3.0.46 Proposition. Soit V un $\mathbb{C}G$ module. Alors :

1. $\chi_V(1_G) = \dim V$,
2. $\chi_V(g)$ est une somme de racines $|g|$-ièmes de l'unité,
3. $|\chi_V(g)| \leq \dim V$,
4. $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.

Démonstration. 1. $\chi_V(1_G) = \operatorname{tr} \rho_V(1_G) = \operatorname{tr} \mathrm{Id}_{\dim V} = \dim V$.

2. Par le théorème de diagonalisation.
3. En prenant les mêmes notations que dans le théorème de diagonalisation, on a $|\chi_V(g)| = |\varepsilon_1 + \cdots + \varepsilon_n| \leq |\varepsilon_1| + \cdots + |\varepsilon_n| = n$.
4. Avec une bonne base B, le théorème de diagonalisation dit que

$$\rho_M(g)_B^B = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n \end{pmatrix},$$

avec ε_i une racine $|g|$-ième de l'unité. On a alors :

$$\begin{aligned} \rho_V(g^{-1})_B^B &= \left(\rho_V(g)_B^B\right)^{-1} \\ &= \begin{pmatrix} \varepsilon_1^{-1} & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n^{-1} \end{pmatrix} \\ &= \begin{pmatrix} \overline{\varepsilon_1} & & 0 \\ & \ddots & \\ 0 & & \overline{\varepsilon_n} \end{pmatrix} \qquad \text{car } |\varepsilon_i| = 1 \\ &= \overline{\rho_V(g)_B^B} \\ &\implies \chi_V(g^{-1}) = \overline{\chi_V(g)}. \end{aligned}$$

□

Notons $\mathcal{F}(G, \mathbb{C})$ l'ensemble des fonctions (ensemblistes) $f : G \longrightarrow \mathbb{C}$. C'est un $\mathbb{C}$-espace vectoriel donc une base est donnée par

$$B = \{\delta_g \mid g \in G\}, \qquad \text{où } \delta_g(h) = \begin{cases} 1 & \text{si } g = h \\ 0 & \text{sinon.} \end{cases}$$

C'est même un espace hermitien, avec produit scalaire

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}, \qquad \forall f_1, f_2 \in \mathcal{F}(G, \mathbb{C}).$$

On passe au sous espace $\mathcal{F}_C(G, \mathbb{C})$ des fonctions centrales, muni du même produit scalaire. Une base est donnée par

$$B' = \{\gamma_c \mid c \text{ est une classe de conjugaison de } G\},$$

où γ_c est la fonction caractéristique de l'ensemble c. On a que

$$\begin{aligned} \dim \mathcal{F}(G, \mathbb{C}) &= |G|, \\ \dim \mathcal{F}_C(G, \mathbb{C}) &= \sharp\{\text{classes de conjugaison de } G\}. \end{aligned}$$

3.0.47 Définition (Caractère irréductible)**.** Un caractère χ_V d'un groupe fini G est dit **irréductible** si V est un $\mathbb{C}G$ module simple, ou, de manière équivalente, si ρ_V est irréductible.

3.0.48 Remarque. Tout caractère χ_V est une somme de caractères irréductibles, par le corollaire 2.0.33.

3.0.49 Lemme (Orthogonalité des coefficients matriciels)**.** Soit $P : G \longrightarrow \mathrm{GL}_m(\mathbb{C})$ et $Q : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$ deux représentations matricielles irréductibles de G. On fixe des entiers $1 \leq i, r \leq m$, $1 \leq j, s \leq n$.

1. Si P et Q sont non équivalentes, alors
$$\sum_{g\in G} P(g)_{ri}Q(g^{-1})_{js} = 0.$$
2. On a :
$$\frac{1}{|G|}\sum_{g\in G} P(g)_{ri}P(g^{-1})_{jr} = \begin{cases} \frac{1}{m} & \text{si } i = j \\ 0 & \text{sinon.} \end{cases}$$

Démonstration. 1. On considère la matrice $E_{ij} \in M_{m,n}(\mathbb{C})$ où $(E_{ij})_{ab} = \delta_{ia}\delta_{jb}$. C'est la matrice d'une application linéaire $\psi : T \longrightarrow S$, où S et T sont des $\mathbb{C}G$ modules simples associés à P et Q respectivement. On sait que
$$\widehat{\psi} = \sum_{g\in G} \rho_S(g)\psi\rho_T(g^{-1})$$
est $\mathbb{C}G$ linéaire. Comme S et T sont simples et non isomorphes, on a par le lemme de Schur que $\widehat{\psi} = 0$. On passe à la matrice de $\widehat{\psi}$ (par rapport à une base B bien choisie) :
$$\begin{aligned} 0 &= (\widehat{\psi}^B_B)_{rs} \\ &= \sum_{g\in G} \big(P(g)E_{ij}Q(g^{-1})\big)_{rs} \\ &= \sum_{g\in G} P(g)_{ri}Q(g^{-1})_{js}. \end{aligned}$$

2. On applique la même démarche en partant de $\psi : S \longrightarrow S$ de matrice E_{ij}. Alors
$$\widehat{\psi} = \frac{1}{|G|}\sum_{g\in G} \rho_S(g)\psi\rho_S(g{-}1)$$
est $\mathbb{C}G$ linéaire et sont par le lemme de Schur, $\widehat{\psi} = \frac{\operatorname{tr}\psi}{m}\,\mathrm{id}_S$. Or
$$\operatorname{tr}\psi = \operatorname{tr}E_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon.} \end{cases}$$
On a donc
$$\begin{aligned} \frac{\operatorname{tr}\psi}{m} &= (\widehat{\psi}^B_B)_{rs} \\ &= \frac{1}{|G|}\sum_{g\in G} P(g)_{ri}P(g^{-1})_{jr}. \end{aligned}$$

□

3.0.50 Théorème (1ère relation d'orthogonalité)**.** L'ensemble des caractères irréductibles forme un système orthonormé de vecteurs dans $\mathcal{F}_C(G,\mathbb{C})$. Explicitement, si S et T sont deux $\mathbb{C}G$ modules simples non isomorphes, alors

1. $\langle \chi_S, \chi_T \rangle = 0$,
2. $\langle \chi_S, \chi_S \rangle = \langle \chi_T, \chi_T \rangle = 1$.

Démonstration. 1. Soient S et T deux $\mathbb{C}G$ modules simples non isomorphes, χ_S et χ_T leur caractères irréductibles respectivement associés, et P et Q leur représentation matricielles respectivement associés. On a

$$\begin{aligned}
\langle \chi_S, \chi_T \rangle &= \frac{1}{|G|} \sum_{g\in G} \chi_S(g)\overline{\chi_T(g)} \\
&= \frac{1}{|G|} \sum_{g\in G} \chi_S(g)\chi_T(g^{-1}) \\
&= \frac{1}{|G|} \sum_{g\in G} \operatorname{tr}(\rho_S(g)) \operatorname{tr}(\rho_T(g^{-1})) \\
&= \frac{1}{|G|} \sum_{g\in G} \sum_{i=1}^{m}\sum_{j=1}^{n} P(g)_{ii} Q(g^{-1})_{jj} \\
&= \sum_{i=1}^{m}\sum_{j=1}^{n} \frac{1}{|G|} \sum_{g\in G} P(g)_{ii} Q(g^{-1})_{jj} \qquad\qquad = 0.
\end{aligned}$$

2. On applique la même démarche.

$$\begin{aligned}
\langle \chi_S, \chi_S \rangle &= \frac{1}{|G|} \sum_{g\in G} \chi_S(g)\chi_S(g^{-1}) \\
&= \sum_{i=1}^{m}\sum_{j=1}^{m} \frac{1}{|G|} \sum_{g\in G} P(g)_{ii} P(g^{-1})_{jj} \\
&= \sum_{i=1}^{m} \frac{1}{|G|} \sum_{g\in G} P(g)_{ii} P(g^{-1})_{ii} \\
&= m\frac{1}{m} \\
&= 1.
\end{aligned}$$

□

3.0.51 Remarque. On verra qu'il s'agit en réalité d'une base orthonormée...

3.0.52 Corollaire (Indépendence linéaire)**.** Les caractères irréductibles sont linéairement indépendants.

Démonstration. Si $\sum_i \lambda_i \chi_{S_i} = 0$, alors

$$0 = \left\langle \sum_i \lambda_i \chi_{S_i}, \chi_{S_j} \right\rangle = \lambda_j,$$

et donc $\lambda_j = 0$ pour tout j. □

3.0.53 Corollaire (Finitude)**.** Il n'y a qu'un nombre fini de caractères irréductibles. Grâce au corollaire 3.0.55, on a alors qu'il n'existe qu'un nombre fini de $\mathbb{C}G$ modules simples à isomorphisme près.

Démonstration. La dimension de $\mathcal{F}_C(G,\mathbb{C})$ est finie et les caractères irréductibles forment une famille libre, par le corollaire 3.0.52. □

3.0.54 Corollaire (Multiplicité)**.** Soit V un $\mathbb{C}G$ module de dimension finie. Ecrivons $V = S_1 \oplus \cdots \oplus S_m$ où S_i est simple. Alors :

1. la multiplicité de S (à isomorphisme près) dans cette décomposition est égale à $\langle \chi_V, \chi_S \rangle$,
2. cette multiplicité est indépendante du choix de la décomposition.

Démonstration. 1. On a $\chi_V = \sum_{k=1}^m \chi_{S_k}$. Donc

$$\langle \chi_V, \chi_S \rangle = \sum_{k=1}^m \langle \chi_{S_i}, \chi_S \rangle = \text{ la multiplicité de } S.$$

2. Clairement, $\langle \chi_V, \chi_S \rangle$ est indépendante de la décomposition choisie.

□

3.0.55 Corollaire (Egalité)**.** Soient V et W deux $\mathbb{C}G$ modules. Alors

$$V \cong W \iff \chi_V = \chi_W.$$

Démonstration. $\Rightarrow$: Soit $\alpha : V \xrightarrow{\cong} W$ un isomorphisme de $\mathbb{C}G$ modules. Alors

$$\alpha \circ \rho_V(g) = \rho_W(g) \circ \alpha \implies \alpha \circ \rho_V(g) \circ \alpha^{-1} = \rho_W(g).$$

Donc

$$\begin{aligned} \chi_W(g) &= \operatorname{tr} \rho_W(g) \\ &= \operatorname{tr} \left(\alpha \circ \rho_V(g) \circ \alpha^{-1} \right) \\ &= \operatorname{tr} \rho_V(g) \\ &= \chi_V(g). \end{aligned}$$

$\Leftarrow$: On décompose V comme suit :

$$V = (S_{11} \oplus \cdots \oplus S_{1m_1}) \oplus \cdots \oplus (S_{r1} \oplus \cdots \oplus S_{rm_r}) \cong T_1^{\oplus m_1} \oplus \cdots \oplus T_r^{\oplus m_r},$$

où $S_{ik} \cong S_{ik'} \cong T_i$ et où $T_i \ncong T_j$ si $i \neq j$. De même, $W \cong (T_1')^{\oplus n_1} \oplus \cdots \oplus (T_r')^{\oplus n_r}$. On a alors

$$\begin{aligned} &\chi_V = \chi_W \\ \iff &\sum_{k=1}^r m_k \chi_{T_k} = \sum_{k=1}^r n_r \chi_{T_k'} \\ \iff &m_k = n_k, \quad \forall 1 \leq k \leq r \\ \iff &V \cong W. \end{aligned}$$

□

3.0.56 Corollaire (Critère d'irreductibilité)**.** Soit V un $\mathbb{C}G$ module. Alors V est simple si et seulement si $\langle \chi_V, \chi_V \rangle = 1$.

Démonstration. On décompose comme dans la démonstration précédente :

$$V \cong T_1^{\oplus m_1} \oplus \cdots \oplus T_r^{\oplus m_r},$$

et on a :

$$\langle \chi_V, \chi_V \rangle = \left\langle \sum_{k=1}^{r} m_k \chi_{T_k}, \sum_{k=1}^{r} m_k \chi_{T_k} \right\rangle = \sum_{k=1}^{r} m_k^2.$$

Ainsi, $\langle \chi_V, \chi_V \rangle = 1$ si et seulement si V est simple. □

3.0.57 Remarque. Le **centre** de $\mathbb{C}G$, noté $Z(\mathbb{C}G)$, est

$$Z(\mathbb{C}G) = \{a \in \mathbb{C}G \mid ab = ba, \forall b \in \mathbb{C}G\}.$$

Si $a = \sum_{g\in G} \lambda_g g \in Z(\mathbb{C}G)$, alors $\forall x \in G$ on a

$$a = xax^{-1} = \sum_{g\in G} \lambda_g xgx^{-1},$$

donc $\lambda_{xgx^{-1}} = \lambda_g$. Ainsi,

$$a = \sum_{C \text{ classe de conjugaison}} \lambda_C \widehat{C}, \qquad \text{où} \widehat{C} = \sum_{g\in C} g.$$

Réciproquement, si $a = \sum_C \lambda_C \widehat{C}$, alors $a \imath Z(\mathbb{C}G)$ car $\forall x \in G$, on a $x\widehat{C}x^{-1} = \widehat{C}$, et donc

$$ax = \sum_C \lambda_C \widehat{C}x = \sum_C \lambda_C x\widehat{C} = xa,$$

et par $\mathbb{C}G$ linéarité, $ab = ba$, $\forall b \in \mathbb{C}G$. Donc $Z(\mathbb{C}G)$ a une base formée de tous les $\widehat{C}$ (class sums).

3.0.58 Lemme. Soit $f \in \mathcal{F}_C(G, \mathbb{C})$ une fonction centrale sur G. On pose

$$\check{f} = \sum_{g\in G} \overline{f(g)} g.$$

Alors

1. $\check{f} \in Z(\mathbb{C}G)$,
2. l'action de $\check{f}$ sur un $\mathbb{C}G$ module simple S est égale à la multiplication par le scalaire

$$\frac{|G|}{\dim S} \langle \chi_S, f \rangle.$$

Démonstration. 1. Par la remarque précédente.

2. La multiplication par $\check{f}$ dans S est une application

$$\begin{aligned} \psi : S &\longrightarrow S \\ s &\longmapsto \check{f}s \end{aligned}$$

qui est $\mathbb{C}G$ linéaire car $\check{f} \in Z(\mathbb{C}G)$. Par le lemme de Schur, ψ est une multiplication par un scalaire, à savoir $\frac{\operatorname{tr}\psi}{\dim S}$. Or,

$$\begin{aligned}\operatorname{tr}\psi &= \sum_{g\in G} \overline{f(g)} \operatorname{tr}\rho_S(g) \\ &= |G|\langle \chi_S, f\rangle.\end{aligned}$$

Donc

$$\psi = \frac{|G|}{\dim S}\langle \chi_S, f\rangle \operatorname{id}_S .$$

□

3.0.59 Théorème. Les caractères irréductibles forment une base de l'espace $\mathcal{F}_C(G,\mathbb{C})$.

Démonstration. Soit W le sous espace de $\mathcal{F}_C(G,\mathbb{C})$ engendré par les caractères irréductibles (qui forment donc une base de W, par le corollaire 3.0.52). On décompose $\mathcal{F}_C(G,\mathbb{C}) = W \oplus W^\perp$. Montrons que $W^\perp = \{0\}$. Soit $f \in W^\perp$, et posons

$$\check{f} = \sum_{g\in G} \overline{f(g)} g.$$

L'action de $\check{f}$ sur un $\mathbb{C}G$ module simple S est égale à la multiplication par $\frac{|G|}{\dim S}\langle \chi_S, f\rangle$. Mais $\langle \chi_S, f\rangle = 0$ car $f \in W^\perp$. Ainsi, l'action de $\check{f}$ est nulle sur tout $\mathbb{C}G$ module simple, donc sur tout toute somme directe (finie) de $\mathbb{C}G$ modules simples, i.e. sur tout $\mathbb{C}G$ module semi simple, et donc finalement sur tout $\mathbb{C}G$ module, par le théorème de Mashke. On applique cela au module $\mathbb{C}G$ (représentation régulière). On trouve

$$\begin{aligned}&\check{f}1 = 0 \\ \Longrightarrow\ &\check{f} = 0 \\ \Longrightarrow\ &\sum_{g\in G} \overline{f(g)} g = 0.\end{aligned}$$

Or G est une famille libre dans $\mathbb{C}G$, donc $f(g) = 0$, $\forall g \in G$. Ainsi, $W^\perp = \{0\}$, $W = \mathcal{F}_C(G,\mathbb{C})$ et les caractères irréductibles forment une base de $\mathcal{F}_C(G,\mathbb{C})$. □

3.0.60 Corollaire. Le nombre de caractères irréductibles, et donc le nombre de $\mathbb{C}G$ modules simples à isomorphisme près, est le nombre de classe de conjugaison de G.

Démonstration. Une base de $\mathcal{F}_C(G,\mathbb{C})$ est donnée par $\{\gamma_C\}_C$, où γ_C est la fonction caractéristique que C, une classe de conjugaison de G. □

3.1 Table de caractères de G

Soient
- $C_1, \dots, C_r$ les classes de conjugaison de G, $g_i \in C_i$ un représentant, avec $C_1 = \{1\}$,
- $\chi_1, \dots, \chi_r$ les caractères irréductibles de G, $n_1, \dots, n_r$ leur degrés respectivement associés ($n_i = \chi_i(1)$), avec χ_1 le caractère trivial (i.e. $\chi_1(g) = 1$, $\forall g \in G$).

On construit la **table des caractères** de G :

	C_1	C_2	$\cdots$	C_j	$\cdots$	C_r
	g_1	g_2	$\cdots$	g_j	$\cdots$	g_r
χ_1	$\chi_1(g_1) = n_1 = 1$	1	$\cdots$	1	$\cdots$	1
χ_2	n_2	$\ddots$				$\vdots$
$\vdots$	$\vdots$		$\ddots$			$\vdots$
χ_i	n_i			$\chi_i(g_j)$		$\vdots$
$\vdots$	$\vdots$				$\ddots$	$\vdots$
χ_r	n_r	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\chi_r(g_r)$

3.1.1 Théorème. La multiplicité d'un $\mathbb{C}G$ module simple dans la représentation régulière est égale à son degré. En d'autres termes

$$\chi_{\text{reg}} = \sum_{i=1}^{r} n_i \chi_i.$$

Démonstration. On sait que $\chi_{\text{reg}}(g) = \operatorname{tr} \rho_{\text{reg}}(g)$. Posons $B = \{e_g\}_{g \in G}$ une base. On a $\rho_{\text{reg}}(h)(e_g) = e_{hg}$ par définition. Puis, il vient que

$$\chi_{\text{reg}}(h) = \begin{cases} |G| & \text{si } h = 1_G \\ 0 & \text{sinon.} \end{cases}$$

Puis,

$$\begin{aligned} \langle \chi_{\text{reg}}, \chi_i \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi_{\text{reg}}(g) \overline{\chi_i(g)} \\ &= n_i. \end{aligned}$$

□

3.1.2 Corollaire. On a

$$\sum_{i=1}^{r} n_i^2 = |G|.$$

Démonstration. On a

$$\begin{aligned} |G| &= \chi_{\text{reg}}(1) \\ &= \sum_{i=1}^{r} n_i \chi_i(1) \\ &= \sum_{i=1}^{r} n_i^2. \end{aligned}$$

□

3.1.3 Rappel (1ère relation d'orthogonalité)**.** On a

$$\begin{aligned} \delta_{ij} &= \langle \chi_i, \chi_j \rangle \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \chi_j(g^{-1}) \\ &= \frac{1}{|G|} \sum_{k=1}^{r} |C_k| \chi_i(g_k) \chi_j(g_k^{-1}), \end{aligned}$$

où $C_1, \ldots, C_r$ sont les classes de conjugaison de G, et où g_k est un représentant de C_k.

3.1.4 Rappel. On a

$$|C_k| = \frac{|G|}{|C_G(g_k)|},$$

où $C_G(g_k)$ est le centralisateur de g_k.

3.1.5 Théorème (2ème relation d'orthogonalité)**.** On a

$$\sum_{i=1}^{r} \chi_i(g_k)\chi_i(g_l^{-1}) = |C_G(g_k)|\delta_{kl}.$$

Démonstration. On part de la première relation d'orthogonalité :

$$\sum_{k=1}^{r} \underbrace{\chi_i(g_k)}_{A_{ik}} \underbrace{\frac{|C_k|}{|G|}\chi_j(g_k^{-1})}_{B_{kj}} = \delta_{ij}.$$

Remarquer que A correspond à la table des caractères. On a $AB = I_r$. Donc $B = A^{-1}$ et $BA = I_r$. Puis :

$$\begin{aligned}
\delta_{kl} &= (BA)_{kl} \\
&= \sum_{i=1}^{r} B_{ki}A_{il} \\
&= \sum_{i=1}^{r} \frac{|C_k|}{|G|}\chi_i(g_k^{-1})\chi_i(g_l) \\
&= \frac{1}{|C_G(g_k)|}\sum_{i=1}^{r} \chi_i(g_l)\chi_i(g_k^{-1}) \\
&\implies \sum_{i=1}^{r} \chi_i(g_k)\chi_i(g_l^{-1}) = |C_G(g_k)|\delta_{kl}.
\end{aligned}$$

□

3.1.6 Exemple (Cas particulier)**.** Si l'on utilise cette relation avec la première colonne et elle-même, on obtient $\sum_{i=1}^{r} n_i^2 = |G|$.

3.1.7 Exemples. 1. $G = C_2 = \{1, g\}$,

	1	g
χ_1	1	1
χ_2	1	-1

2. $G = \mathfrak{S}_3$. Posons χ_1 le caractère trivial, χ_2 le caractère signature et χ_3 le caractère de degré 3, vu en exercices.

$\lvert C_j\rvert$	1	2	3
	id	(1 2 3)	(1 2)
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

3. $G = \mathfrak{S}_4$. Posons
$$V_4 = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}.$$
On a $V_4 \triangleleft \mathfrak{S}_4$, $\mathfrak{S}_3 < \mathfrak{S}_4$ et $\mathfrak{S}_3 \cap V_4 = \{\mathrm{id}\}$. Donc $\mathfrak{S}_3 V_4 = \mathfrak{S}_4$. Par le 2ème théorème d'isomorphisme, on a
$$\mathfrak{S}_4/V_4 = (\mathfrak{S}_3 V_4)/V_4 \cong \mathfrak{S}_3/(\mathfrak{S}_3 \cap V_4) = \mathfrak{S}_3.$$
Toute représentation de $\mathfrak{S}_3$ donne une représentation de $\mathfrak{S}_4$, via le quotient
$$\mathfrak{S}_4 \xrightarrow{\pi} \mathfrak{S}_4/V_4 \xrightarrow{\cong} \mathfrak{S}_3 \xrightarrow{\rho} \mathrm{GL}(V)\,.$$
On sait que $\sigma(a_1\ a_2\ \cdots\ a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k))$. Les représentants les classes de conjugaison sont donc id, (1 2), (1 2 3), (1 2 3 4) et (1 2)(3 4), avec $r = 5$. Dans $\mathfrak{S}_3 \cong \mathfrak{S}_4/V_4$, on trouve
$$\begin{aligned}[\mathrm{id}] &= \mathrm{id}\\ [(1\,2)] &= (1\,2)\\ [(1\,2\,3)] &= (1\,2\,3)\\ [(1\,2\,3\,4)] &= (1\,3)\\ [(1\,2)(3\,4)] &= \mathrm{id}\,.\end{aligned}$$
On a la table des caractères :

$\lvert C_j\rvert$	1	3	8	6	6
	id	(1 2)(3 4)	(1 2 3)	(1 2)	(1 2 3 4)
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	2	2	-1	0	0
χ_4	n_4	a	b	c	d
χ_5	n_5	a'	b'	c'	d'

Puis :
- on sait que $\sum_{i=1}^r n_i^2 = |G| = 24$, donc $n_4 = n_5 = 3$,
- colonnes 1 et 5 (2ème relation d'orthogonalité) : $d = -d'$,
- colonne 3 :
$$\begin{aligned}&1 + 1 + 1 + b\bar{b} + b'\overline{b'} = 3\\ &\implies b = b' = 0,\end{aligned}$$
- colonnes 1 et 4 : $c = -c'$,
- lignes 1 et 4 (1ère relation d'orthogonalité) :
$$\begin{aligned}&3 + 3a + 0 + 6c + 6d = 0\\ &\implies 1 + 2(a + c + d) = 0,\end{aligned}$$
- lignes 2 et 4 :
$$\begin{aligned}&3 + 3a + 0 - 6c - 6d = 0\\ &\implies 1 + 2(a - c - d) = 0,\\ &\implies a = -1 \text{ et } c = -d,\end{aligned}$$

– lignes 3 et 5 :

$$\begin{aligned} &6 + 6a' + 0 + 0 + 0 = 0 \\ \Longrightarrow\ &a' = -1, \end{aligned}$$

– colonnes 4 et 5 :

$$\begin{aligned} &1 + 1 + cd + c'd' = 0 \\ \Longrightarrow\ &c^2 = 1 \\ \Longrightarrow\ &c = \pm 1, c' = d = \mp 1, d' = \pm 1. \end{aligned}$$

Sans perte de généralité, on choisi $c = 1$. On obtient :

$\lvert C_j \rvert$	1	3	8	6	6
	id	(1 2)(3 4)	(1 2 3)	(1 2)	(1 2 3 4)
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	2	2	-1	0	0
χ_4	3	-1	0	1	-1
χ_5	3	-1	0	-1	1

4. $C_4 = \{1, g, g^2, g^3\}$ est abélien. De plus, toute représentation irréductible ρ est de degré 1, et envoie g sur une racine 4ème de l'unité. On a donc

	1	g	g^2	g^3
χ_1	1	1	1	1
χ_2	1	i	-1	$-i$
χ_3	1	-1	1	-1
χ_4	1	$-i$	-1	i

Chapitre 4

Intégralité

4.0.8 Définition (Entier, entier algébrique)**.** 1. Soit B un anneau commutatif et A un sous anneau de B. On dit que $b \in B$ est **entier** s'il est racine d'un polynome unitaire à coefficiebts dans B.

2. Un nombre complexe est un **entier algébrique** s'il est entier sur $\mathbb{Z}$.

4.0.9 Remarque. Un nombre complexe b est algébrique s'il est racine d'un polynome à coefficients dans $\mathbb{Q}$. En divisant pas le coefficient dominant, on otient un polynome unitaire. On peut aussi chasser les dénominateurs des coefficients pour obtenir un polynome à coefficients entiers. Mais on ne peut pas en général faire les deux simultanément.

4.0.10 Exemples. 1. Les éléments de $\mathbb{Z}$ sont des entiers algébriques (duh).

2. Les entiers de Gauss $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$ sont tous des entiers algébriques. En effet, $a+ib$ est racine de $X^2 - 2aX + a^2 + b^2$.

4.0.11 Définition (Intégralement clos)**.** Un anneau B est **intégralement clos** si aucun élément de $F \setminus A$ est entier sur B, où F est le corps des fractions de B.

4.0.12 Proposition. $\mathbb{Z}$ est intégralement clos.

Démonstration. Posons $b = p/q \in \mathbb{Q}$, avec $p, q \in \mathbb{Z}$, $q \geq 1$ et $(p, q) = 1$. Alors

$$\begin{aligned} b \text{ est un entier algébrique} &\implies \exists a_0, \ldots, a_{n-1} \text{ tels que } b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \\ &\implies p^n + \underbrace{a_{n-1}p^{n-1}q + \cdots + a_0 q^n = 0}_{q \text{ diviseur}}. \end{aligned}$$

Donc q divise p, donc $q = 1$ et donc $b \in \mathbb{Z}$. □

4.0.13 Exemple. $1/2 \in \mathbb{Q}$ est algébrique, mais pas entier sur $\mathbb{Z}$.

4.0.14 Proposition. Soit B un anneau commutatif, A un sous anneau de B et $b \in B$. Les conditions suivantes sont équivalentes :

1. b est entier sur A,
2. l'anneau $A[b]$ est un A-module de type fini, i.e. finiment généré,
3. il existe un sous anneau S de B contenant A et b tel que S est un A-module de type fini.

Démonstration. 1. $\Longrightarrow$ 2. : Si b est entier sur A, alors $\exists a_0, \dots, a_{n-1} \in A$ tel que $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. On va montrer que $A[b]$ est engendré comme A-module par $\{1, b, \dots, b^{n-1}\}$. Il suffit de montrer que $b^k \in A1 + \cdots + Ab^{n-1}$, $\forall k \in \mathbb{N}$. Par récurrence sur k. Si $k \leq n-1$ c'est évident. Puis,

$$b^n = -a_{n-1}b^{n-1} - \cdots - a_0.$$

Si $k > n$, on multiplie l'égalité précédente par b^{k-n} pour obtenir

$$b^k = -a_{n-1}b^{k-1} - \cdots - a_0 b^{k-n}.$$

2. $\Longrightarrow$ 3. : Trivial, en prenant $S = A[b]$.
3. $\Longrightarrow$ 1. : On a S un sous anneau de B, de type fini comme A-module et qui contient A et b. Donc $S = Ay_1 + \cdots + Ay_n$. Comme $b \in S$, on a $by_i \in S$. Donc

$$by_i = c_{i,1}y_1 + \cdots + c_{i,n}y_n,$$

et

$$b \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = C \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},$$

où $C = (c_{i,j})_{1 \leq i,j \leq n}$. Posons $D = C - bI_n \in M_n(S)$. Posons $\operatorname{cof} D$ la matrice des cofacteurs de D. On a

$$\begin{aligned} (\operatorname{cof} D)^t D \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (\det D) \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} &= \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \\ \Longrightarrow (\det D) y_i = 0, \quad \forall i \leq n & \\ \Longrightarrow (\det D) s = 0, \quad \forall s \in S & \\ \Longrightarrow \det D = \det(C - bI_n) = 0. & \end{aligned}$$

Ainsi, b est une racine du polynome caractéristique de C, qui, à signe près, est unitaire. Donc b est entier sur A.

□

4.0.15 Corollaire. Si $x, y \in B$ sont entiers sur A, alors $x + y$ et xy le sont aussi. En d'autres termes, $\{x \in B \mid x \text{ est entier sur } A\}$ est un sous anneau de B.

Démonstration. On a $A[x] = A1 + \cdots + Ax^{n-1}$, $A[y] = A1 + \cdots + Ay^{m-1}$, par hypothèses et la proposition précédente. Alors $A[x, y]$ est un A-module de type fini car engendré par $\{x^i y^j\}_{1 \leq i \leq n-1, 1 \leq j \leq m-1}$. Puis, $x + y, xy \in A[x, y]$ et donc $x + y$ et xy sont entiers sur A. □

4.0.16 Lemme. Si χ est un caractère d'un groupe fini G et si $g \in G$, alors $\chi(g)$ est un entier algébrique.

Démonstration. $\chi(g)$ est une somme de racines de l'unité, par le théorème de diagonalisation. □

4.0.17 Remarque. Soit $\rho : G \longrightarrow \mathrm{GL}(V)$ une représentation d'un groupe fini G. Alors ρ s'étend par $\mathbb{C}$-linéarité en un homomorphisme de $\mathbb{C}$-algèbre

$$\begin{aligned} \rho : \mathbb{C}G &\longrightarrow \operatorname{End}_{\mathbb{C}}(V) \\ \sum_{g \in G} \lambda_g g &\longmapsto \sum_{g \in G} \lambda_g \rho(g). \end{aligned}$$

On suppose que ρ est irréductible, et on restreint au centre $Z(\mathbb{C}G) : \rho|_{Z(\mathbb{C}G)} : Z(\mathbb{C}G) \longrightarrow \mathrm{End}_{\mathbb{C}}(V)$. Pour tout $z \in Z(\mathbb{C}G)$, $\rho(z)$ commute avec $\rho(g)$, $\forall g \in G$. Par le lemme de Schur, $\rho(z) = \lambda \,\mathrm{id}_V$ pour tout $\lambda \in \mathbb{C}$. Donc $\mathrm{End}_{\mathbb{C}G}(V) = \mathbb{C}\,\mathrm{id}_V$. Donc il existe $\omega : Z(\mathbb{C}G) \longrightarrow \mathbb{C}$ telle que $\rho(z) = \omega(z)\,\mathrm{id}_V$. Clairement, ω est un homomorphisme de $\mathbb{C}$-algèbre.

4.0.18 Lemme. Si $C_1, \dots, C_r$ sont les classes de conjugaison de G, alors

$$Z(\mathbb{Z}G) = \left\{ \sum_{i=1}^{r} \mu_i \widehat{C}_i \mid \mu_i \in \mathbb{Z}, \forall 1 \leq i \leq r \right\}.$$

Démonstration. On sait que $\{\widehat{C}_1, \dots, \widehat{C}_r\}$ forme une base de $Z(\mathbb{C}G)$ comme $\mathbb{C}$-espace vectoriel. Clairement, $\widehat{C}_i \in Z(\mathbb{Z}G)$, $\forall 1 \leq i \leq r$. Donc $\left\{ \sum_{i=1}^{r} \mu_i \widehat{C}_i \mid \mu_i \in \mathbb{Z}, \forall 1 \leq i \leq r \right\} \subseteq Z(\mathbb{Z}G)$. De plus, si $z \in Z(\mathbb{Z}G)$, alors z commute avec tout $g \in G$. Donc z commute avec tout élément de $\mathbb{C}G$ et $z \in Z(\mathbb{C}G)$. Ainsi, $z = \sum_{i=1}^{r} a_i \widehat{C}_i$, où $a_i \in \mathbb{C}$. Mais $z \in \mathbb{Z}G$, d'où $a_i \in \mathbb{Z}$. □

4.0.19 Théorème (Intégralité)**.** Soit χ_i un caractère irréductible de G, soit $g_i \in G$ et soit C_j la classe de conjugaison de g_j. Alors

$$\frac{|C_j|}{n_i} \chi_i(g_j)$$

est un entier algébrique.

Démonstration. Par le lemme précédent, $Z(\mathbb{Z}G)$ est un $\mathbb{Z}$-module de type fini, engendré par $\widehat{C}_1, \dots, \widehat{C}_r$. Il s'ensuit que $\widehat{C}_j$ est entier sur $\mathbb{Z}$, et donc il existe un polynôme unitaire $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0$ à coefficients dans $\mathbb{Z}$, tel que $f(\widehat{C}_j) = 0$. On sait qu'il existe un homomorphisme d'anneau $\omega_i : Z(\mathbb{C}G) \longrightarrow \mathbb{C}$ tel que $\rho_i(z) = \omega_i(z) I_{n_i}$, $\forall z \in Z(\mathbb{C}G)$. On applique l'homomorphisme ω_i à $\widehat{C}_j \in Z(\mathbb{Z}G) \subset Z(\mathbb{C}G)$:

$$\begin{aligned} 0 &= \omega_i(0) \\ &= \omega_i(f(\widehat{C}_j)) \\ &= f(\omega_i(\widehat{C}_j)) && \text{car } \omega_i \text{ est un homomorphisme d'anneaux} \end{aligned}$$

et donc $\omega_i(\widehat{C}_j)$ est un entier algébrique. Or

$$\begin{aligned} \omega_i(\widehat{C}_j) I_{n_i} &= \rho_i(\widehat{C}_j) \\ &= \sum_{g \in G} \rho_i(g) \\ &\implies n_i \omega_i(\widehat{C}_j) = \mathrm{tr}\left(\omega_i(\widehat{C}_j) I_{n_i}\right) \\ &= \mathrm{tr} \sum_{g \in G} \rho_i(g) \\ &= \sum_{g \in G} \chi_i(g) \\ &= |C_j| \chi_i(g_j) \\ &\implies \omega_i(\widehat{C}_j) = \frac{|C_j|}{n_i} \chi_i(g_j) \end{aligned}$$

et donc $\frac{|C_j|}{n_i} \chi_i(g_j)$ est un entier algébrique. □

4.0.20 Théorème. Soit n_i le degré d'un caractère irréductible χ_i de G. Alors n_i divise $|G|$.

Démonstration. On a :

$$\begin{aligned}\frac{|G|}{n_i} &= \frac{|G|}{n_i}\langle\chi_i,\chi_i\rangle \\ &= \frac{1}{n_i}\sum_{j=1}^{r}|C_j|\chi_i(g_j)\chi_i(g_j^{-1}) \\ &= \sum_{j=1}^{r}\underbrace{\frac{|C_j|}{n_i}\chi_i(g_j)}_{\text{Entier algébrique}}\underbrace{\chi_i(g_j^{-1})}_{\text{Entier algébrique}}.\end{aligned}$$

Ainsi, $\frac{|G|}{n_i}$ est un entier algébrique rationnel. Donc $\frac{|G|}{n_i}\mathbb{1}\mathbb{Z}$ et n_i divise $|G|$. □

4.0.21 Remarque. Il n'existe pas, à ce jour , de preuve directe de ce théorème.

4.0.22 Exemple. Soit G un groupe d'ordre pq, où p et q sont deux nombres premiers, et où $p<q$. On va montrer que si G n'est pas abélien, alors $q\equiv 1\ (p)$. Soit $a=[G:[G;G]]$, le nombre de caractères irréductibles de degré 1 (cf exercices). Les caractères irréductibles χ_i satisfont $n_i||G|=pq$ et $\sum_{i=1}^{r}n_i^2=|G|$. Donc $n_i\in\{q,pq\}$ est impossible. On doit donc avoir $n\in\{1,p\}$. Soit b le nombre de caractères irréductibles de degré p. On a que $b\neq 0$ car G n'est pas abélien. Puis,

$$\begin{aligned}pq &= |G| \\ &= \sum_{j=1}^{r}n_i^2 \\ &= a+bp^2.\end{aligned}$$

On a donc que $p|a$, ce qui entraine de $p=a$ (car $b\neq 0$). Ainsi, $q=1+bp$, ce qui montre que $q\equiv 1\ (p)$. De plus,

$$b=\frac{q+1}{p}.$$

Chapitre 5

Le théorème $p^a q^b$ de Burnside

5.0.23 Conjecture (de Burnside)**.** Si G est simple non abélien, alors $2||G|$.

Démontré par Feit et Thompson en 1962, 250 pages. On assiste dans la période 1960-1980 à un "boom" de la classification des groupes finis simples, pour aboutir en 1980 au Théorème de classification (environ 10000 pages). La liste est globalement :

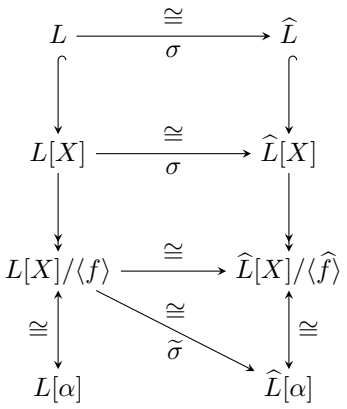
- C_p, avec p premier,
- A_n, avec $n \geq 5$,
- $\mathrm{PSL}_n(\mathbb{F}_p)$,
- $\mathrm{PS}_p(\mathbb{F}_q)$,
- etc...
- et 26 exceptions, appelées **groupes sporadiques**, dont le fameux Monstre (environ 10^{50} éléments).

5.0.24 Proposition. Soit E une extension fini (donc algébrique) d'un corps L. Soit $\sigma : L \longrightarrow C$ un homomorphisme de corps, où C est algébriquement clos. Alors il existe un plongement $\widetilde{\sigma} : E \longrightarrow C$ tel que $\widetilde{\sigma}|_L = \sigma$.

Démonstration. Comme $[E : L]$ est fini, on a que $E = L[\alpha_1][\alpha_2]\cdots[\alpha_m]$. Donc il suffut de montrer la proposition pour une extension monogène $L[\alpha]$. Pour rappel, $L[\alpha] \cong L[X]/\langle f\rangle$, où f est le polynôme minimal de α (donc irréductible). Soit $\widehat{L} = \sigma(L)$, qui est un sous corps de C. On a $L \cong \widehat{L}$, car tout homomorphisme de corps est injectif. Alors l'isomorphisme $\sigma : L \xrightarrow{\cong} \widehat{L}$ induit un isomorphisme d'anneaux $\sigma : L[X] \xrightarrow{\cong} \widehat{L}[X]$. Soit $\widehat{f} = \sigma(f) \in \widehat{L}[X]$. Comme f est irréductible, on a que $\widehat{f}$ est irréductible. Donc $\widehat{L}[X]/\langle\widehat{f}\rangle$ est un corps, isomorphe à $\widehat{L}[\widehat{\alpha}]$, où $\widehat{\alpha}$ est un racine de $\widehat{f}$ dans C (qui existe car C est algébriquement clos). Posons

$$\begin{aligned} \widetilde{\sigma} : \widehat{L}[X]/\langle\widehat{f}\rangle &\xrightarrow{\cong} \widehat{L}[\widehat{\alpha}] \\ [X] &\longmapsto \widehat{\alpha}. \end{aligned}$$

On a finalement



.

□

5.0.25 Lemme. Soit $\beta \in \mathbb{C}$, $\beta = \varepsilon_1 + \cdots + \varepsilon_n$, où ε_i est une racine m-ième de l'unité. Soit $f \in \mathbb{Q}[X]$ le polynome minimal de β sur $\mathbb{Q}$. Si β' est un autre racine de f, alors

$$\beta' = \sum_{i=1}^{n} \varepsilon_i^k,$$

avec $(k, m) = 1$.

Démonstration. Posons $L = \mathbb{Q}[\beta]$. C'est une extension finie de $\mathbb{Q}$. Soit $\varepsilon = e^{2i\pi/m}$, la racine primitive m-ième de l'unité. Comme β' est une autre racine de f, on a une isomorphisme de corps

$$\begin{aligned} \sigma : L = \mathbb{Q}[\beta] &\longrightarrow L' = \mathbb{Q}[\beta'] \\ q &\longmapsto q \qquad\qquad \text{si } q \in \mathbb{Q} \\ \beta &\longmapsto \beta'. \end{aligned}$$

Comme chaque ε_i est une puissance de ε, on a que $\beta \in \mathbb{Q}[\varepsilon]$, et donc $L \subseteq \mathbb{Q}[\varepsilon]$. Par le résultat précédent, il existe un prolongement $\widetilde{\sigma} : \mathbb{Q}[\varepsilon] \longrightarrow \mathbb{C}$ de σ. On a $\operatorname{im} \widetilde{\sigma} = \mathbb{Q}[\widetilde{\sigma}(\varepsilon)] \subseteq \mathbb{C}$. Comme $\varepsilon^m = 1$, on a que $\widetilde{\sigma}(\varepsilon)^m = 1$, et donc $\widetilde{\sigma}(\varepsilon)$ est une racine primitive m-ième de l'unité, $\widetilde{\sigma}(\varepsilon) = \varepsilon^k$ pour un certain $k \in \mathbb{N}$. Remarquer que $(k, m) = 1$. Il s'ensuit que $\widetilde{\sigma}(\varepsilon_i) = \varepsilon_i^k$. Finalement,

$$\begin{aligned} \beta' &= \sigma(\beta) \\ &= \widetilde{\sigma}(\beta) \\ &= \sum_{i=1}^{n} \varepsilon_i^k. \end{aligned}$$

□

5.0.26 Remarque. En fait, $\mathbb{Q}[\widetilde{\sigma}(\varepsilon)] = \mathbb{Q}[\varepsilon^k] = \mathbb{Q}[\varepsilon]$.

5.0.27 Lemme. Soit $\tau : H \longrightarrow \mathrm{GL}(V)$ une représentation irréductible de degré n d'un groupe fini H. Soit $h \in H$. Alors :

1. $|\chi_V(h)| \leq n$,
2. si $h \in Z(H)$, alors $|\chi_V(h)| = n$,

3. si $|\chi_V(h)| = n$ et si τ est fidèle, alors $h \in Z(H)$.

Démonstration. 1. Déja fait. On sait que $\chi_V(h) = \sum_{i=1}^n \varepsilon_i$, où ε_i est une racine $|h|$-ième de l'unité. Donc

$$\begin{aligned} |\chi_V(h)| &= \left|\sum_{i=1}^n \varepsilon_i\right| \\ &\leq \sum_{i=1}^n |\varepsilon_i| \\ &= n. \end{aligned}$$

2. Si $h \in Z(H)$, alors $\tau(h)$ commute avec $\tau(g)$, $\forall g \in H$. Donc $\tau(h)$ est une multiplication par un scalaire par le lemme de Schur. Posons $\tau(h) = \varepsilon \,\mathrm{id}_V$ et $m = |h|$. On a que $h^m = 1$ et donc $\varepsilon^m = 1$. Ainsi, ε est une racine m-ième de l'unité. Puis, $\chi_V(h) = n\varepsilon$ ce qui montre que $|\chi_V(h)| = n$.

3. Réciproquement, supposons que $|\chi_V(h)| = |\sum_{i=1}^n \varepsilon_i| = n$. La seule possibilité est que $\varepsilon_1 = \cdots = \varepsilon_n = \varepsilon$. On déduit que $\tau(h) = \varepsilon \,\mathrm{id}_V$. Ainsi, $\tau(h) \in Z(\mathrm{GL}(V))$. Comme τ est fidèle, on a que $h \in Z(H)$.

□

5.0.28 Théorème (Burnside)**.** Soit G un groupe fini, $g \in G$, C la classe de conjugaison de g, $\rho : G \longrightarrow \mathrm{GL}(V)$ une représentation irréductible de degré n et χ le caractère associé. Supposons que $(n, |C|) = 1$. Alors

$$\chi(g) = 0 \quad \text{ou bien} \quad \overline{g} \in Z(G/\ker\rho).$$

Démonstration. Reparquer que ρ induit une représentation fidèle $\overline{\rho} : G/\ker\rho \longrightarrow \mathrm{GL}(V)$. Supposons que $\overline{g} \notin Z(G/\ker\rho)$ et montrons que $\chi(g) = 0$. Par le lemme précédent, on a que $|\chi(g)| < n$. Comme $(n, |C|) = 1$, $\exists a, b \in \mathbb{Z}$ tels que $an + b|C| = 1$ (par l'identité de Bézout). Puis, par le théorème d'intégralité,

$$\frac{\chi(g)}{n} = a \underbrace{\chi(g)}_{\text{ent. alg.}} + b \underbrace{\frac{|C|\chi(g)}{n}}_{\text{ent. alg.}}.$$

Ainsi, $\alpha = \chi(g)/n$ est un entier algébrique. On a que $|\alpha| < 1$ et

$$\alpha = \frac{\sum_{i=1}^n \varepsilon_i}{n},$$

où ε_i est une racine m-ième de l'unité. Soit $f \in \mathbb{Q}[X]$ le polynome minimal de α, et $q = \deg f$. Soit $\alpha = \alpha_1, \ldots, \alpha_q$ les racines de f dans $\mathbb{C}$. Chaque α_i est un entier algébrique, car α l'est, et que tout polynome qui s'annule en α est un multiple du polynome minimal f de α. Or $n\alpha = \sum_{i=1}^n \varepsilon_i$, donc si $2 \leq i \leq q$, $n\alpha_i = \sum_{j=1}^n \varepsilon_j^{k_i}$, pour un certain k_i. Donc $|\alpha_i| = \frac{\sum_{j=1}^n \varepsilon_j^{k_i}}{n} \leq 1$. Ainsi, $|\alpha| < 1$, $|\alpha_i| \leq 1$, $\forall 2 \leq i \leq q$. Clairement, $\prod_{i=1}^q \alpha_i = \pm f_0$, où f_0 est le terme constant de f. Donc $\prod_{i=1}^q \alpha_i \in \mathbb{Q}$ est

aussi un entier algébrique. Donc, comme $\mathbb{Z}$ est intégralement clos, $\prod_{i=1}^{q} \alpha_i \in \mathbb{Z}$. Puis

$$\begin{aligned}\left|\prod_{i=1}^{q} \alpha_i\right| &= \prod_{i=1}^{q} |\alpha_i| \\ &= \underbrace{|\alpha|}_{<1}\underbrace{|\alpha_2|}_{\leq 1}\cdots\underbrace{|\alpha_q|}_{\leq 1} \\ &\leq 1 \\ \implies \prod_{i=1}^{q} \alpha_i &= 0.\end{aligned}$$

Donc $f(X) = Xh(X)$, car le terme constant f_0 est nul. Or, f est irréductible, d'où $f(X) = X$. Il s'ensuit que $q = 1$ et que $\alpha = 0$. Donc $\chi(g) = n\alpha = 0$. □

5.0.29 Théorème (de Burnside, sur les groupes simples)**.** Soit G un groupe simple non abélien, $g \in G \setminus \{1\}$ et C la classe de conjugaison de g. Alors $|C|$ n'est pas une puissance d'un nombre premier.

Démonstration. On suppose que G est non abélien et que $|C| = p^m$, avec p premier. On va montrer que G n'est pas simple. Les caractères de G sont $\chi_1, \ldots, \chi_s, \chi_{s+1}, \ldots, \chi_r$, avec

$$\begin{aligned} p \not| n_i = \chi_i(1) \quad &\text{si } 1 \leq i \leq s, \\ p | n_i = \chi_i(1) \quad &\text{si } s+1 \leq i \leq r. \end{aligned}$$

Affirmation : $\exists 2 \leq i \leq s$ tel que $\chi_i(g) \neq 0$. Par l'absurde, supposons que $\chi_2(g) = \cdots = \chi_s(g) = 0$. On utilise les 2èmes relations d'orthogonalité pour les colonnes g et 1. Comme $g \neq 1$, on a

$$\begin{aligned} &\sum_{i=1}^{r} \chi_i(g)\chi_i(1) = 0 \\ \implies &1 + \sum_{i=1}^{r} n_i \chi_i(g) = 0 \\ \implies &\frac{1}{p} + \sum_{i=1}^{r} \underbrace{\frac{n_i}{p}}_{\in\mathbb{N}} \chi_i(g) = 0 \end{aligned}$$

ce qui est absurde. On a montré l'affirmation. Soit donc $2 \leq i \leq s$ tel que $\chi_i(g) \neq 0$. On est dans les hypothèses du théorème précédent : $|C| = p^m$, $p \not| n_i$ et donc $(n_i, |C|) = 1$. Or $\chi_i(g) \neq 0$ ce qui montre que $\overline{g} \in Z(G/\ker\rho_i)$. Si $\ker\rho_i \neq \{1\}$, c'est un sous groupe normal de G distinct de G (car $i \neq 1$) et donc G n'est pas simple. Si $\ker\rho_i = \{1\}$, alors $G/\ker\rho_i = G$ et $g \in Z(G)$. Ainsi, G a un centre non trivial est n'est donc pas simple. □

5.0.30 Théorème ($p^a q^b$ de Burnside)**.** Soit G un groupe fini d'ordre $p^a q^b$, où p et q sont premiers, et $p^a q^b$ n'est pas premier. Alors G n'est pas simple.

Démonstration.
- Si $|G| = 1$, alors par définition, G n'est pas simple.
- Si $|G| = p^a$, avec $a \geq 2$, alors $Z(G)$ n'est pas trivial. Si $Z(G) = G$, alors G est abélien et donc d'ordre premier (C_p), ce qui est absurde.

– Supposons que $|G|$ est divisible par p et q, (donc $a, b \geq 1$). Il existe un p-Sylow H d'ordre p^a. Alors $Z(H)$ n'est pas trivial, car H est un p-groupe, et donc $\exists h \in Z(H) \setminus \{1\}$. Alors $C_G(h)$ contient H car h est central. Ainsi

$$\underbrace{H}_{p^a} \subseteq C_G(h) \subseteq \underbrace{G}_{p^a q^b},$$

et $|C_G(h)|$ est divisible par q. Par le théorème précédent, G n'est pas simple.

□

5.0.31 Définition (Groupe résoluble)**.** Un groupe G est **résoluble** s'il existe une suite de sous groupes emboités $G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}$ telle que

- $G_{i+1} \trianglelefteq G_i$,
- G_i/G_{i+1} est abélien.

5.0.32 Propriétés. 1. Si H est un sous groupe d'un groupe résoluble, alors H est résoluble.

2. Si $N \trianglelefteq G$ et si G est résoluble, alors G/N est résoluble.
3. Si $N \trianglelefteq G$ et si N et G/N sont résolubles, alors G est résoluble.

Démonstration. 1. On a une suite $G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}$ satisfaisant les conditions de la définition. Posons $H_i = H \cap G_i$. Alors la suite $H = H_0 \geq H_1 \geq \cdots \geq H_r = \{1\}$ satisfait aussi les conditions de la définition, et donc H est résoluble.

2. On a une suite $G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}$ satisfaisant les conditions de la définition. Soit $\pi : G \longrightarrow G/N$ la projection canonique. Posons $\overline{G}_i = \pi(G_i)$. Alors la suite $G/N = \overline{G}_0 \geq \overline{G}_1 \geq \cdots \geq \overline{G}_r = \{1\}$ satisfait aussi les conditions de la définition, et donc G/N est résoluble.
3. On a deux suites $N = N_0 \geq N_1 \geq \cdots \geq N_s = \{1\}$ et $G/N = \overline{G}_0 \geq \overline{G}_1 \geq \cdots \geq \overline{G}_r = \{\overline{1}\}$. Soit $\pi : G \longrightarrow G/N$ la projection canonique. Alors la suite $G = \pi^{-1}(\overline{G}_0) \geq \pi^{-1}(\overline{G}_1) \geq \cdots \geq \pi^{-1}(\overline{G}_r) = \ker \pi = N = N_0 \geq N_1 \geq \cdots \geq N_s = \{1\}$ satisfait les conditions de la définition, et donc G est résoluble.

□

5.0.33 Exemples. 1. Si G est simple non abélien, alors il n'est pas résoluble.

2. Le groupe $\mathfrak{S}_4$ est résoluble :

$$\mathfrak{S}_4 \trianglerighteq A_4 \trianglerighteq V_4 \trianglerighteq C_2 \trianglerighteq \{\mathrm{id}\}.$$

5.0.34 Théorème (p^aq^b de Burnside, version 2)**.** Tout groupe d'ordre p^aq^b est résluble, avec p et q premiers.

Démonstration. Par récurrence sur $|G|$. On démarre sur le cas $|G| = p$, avec p premier. Dans ce cas, G est abélien, et donc résoluble. Si $|G|$ n'est pas premier, alors il existe un sous groupe normal $N \trianglelefteq G$, avec $N \neq \{1\}, G$, par le théorème p^aq^b. Par hypothèse de récurrence, N et G/N sont d'ordre plus petits et donc résolubles. Ainsi, G est résoluble. □

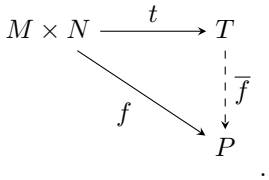
Chapitre 6

Produit tensoriel

6.0.35 Définition (Application équilibré)**.** Soit A un anneau, M un A-module à droite, N un A-moduole à gauche, et P un groupe abélien. On dit qu'une application $f : M \times N \longrightarrow P$ est **A-équilibré** si

- $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$, $\forall m_1, m_2 \in M$, $\forall n \in N$,
- $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$, $\forall m \in M$, $\forall n_1, n_2 \in N$,
- $f(ma, n) = f(m, an)$, $\forall m \in M$, $\forall n \in N$, $\forall a \in A$.

6.0.36 Définition (Produit tensoriel)**.** Soit A un anneau, M un A-module à droite, et N un A-module à gauche. Un **produit tensoriel** de M et N est un couple (T, t), où T est un groupe abélien, $t : M \times N \longrightarrow P$ est A-équilibré, tel que pour tout groupe abélien P et toute application équilibré $f : M \times N \longrightarrow P$, $\exists : \overline{f} : T \longrightarrow P$ telle que $f = \overline{f} \circ t$.



.

6.0.37 Propriétés. Le produit tensoriel existe toujours. De plus, il est unique à isomorphisme unique près. On le note $M \otimes_A N$.

6.0.38 Propriétés.

1. $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$, $\forall m_1, m_2 \in M$, $\forall n \in N$,
2. $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$, $\forall m \in M$, $\forall n_1, n_2 \in N$,
3. $(ma) \otimes n = m \otimes (an)$, $\forall m \in M$, $\forall n \in N$, $\forall a \in A$,
4. $m \otimes 0 = 0$, $\forall m \in M$,
5. $0 \otimes n = 0$, $\forall n \in N$
6. $(-m) \otimes n = -(m \otimes n) = m \otimes (-n)$,
7. tout élément de $M \otimes_A N$ s'écrit
$$\sum_i z_i (m_i \otimes n_i),$$
avec $m_i \in M$, $n_i \in N$, $z_i \in \mathbb{N}$.

6.0.39 Remarque. Si A est un anneau commutatif, alors $M \otimes_A N$ peut être muni d'une structure de A-module :

$$\begin{aligned} A \times (M \otimes_A N) &\longrightarrow M \otimes_A N \\ (a, m \otimes n) &\longmapsto (ma) \otimes n. \end{aligned}$$

6.0.40 Proposition. Soit N un A-module à gauche.

1. $A \otimes_A N$ est muni d'une structure de A-module à droite via
$$a(b \otimes n) = (ab) \otimes n.$$
2. On a un isomorphisme de A-modules
$$\begin{aligned} \phi : A \otimes_A N &\xrightarrow{\cong} N \\ a \otimes n &\longmapsto an, \end{aligned}$$
d'inverse
$$\begin{aligned} \psi : N &\xrightarrow{\cong} A \otimes_A N \\ n &\longmapsto 1 \otimes n. \end{aligned}$$

6.0.41 Proposition. Soient M_1 et M_2 deux A-modules à droite, et N un A-module à gauche. Alors on a un isomorphisme

$$\begin{aligned} \phi : (M_1 \oplus M_2) \otimes_A N &\xrightarrow{\cong} (M_1 \otimes_A N) \oplus (M_2 \otimes_A N) \\ (m_1 + m_2) \otimes n &\longmapsto (m_1 \otimes n) + (m_2 \otimes n). \end{aligned}$$

6.0.42 Remarque. En réalité, on a même l'isomorphisme suivant :

$$\left(\bigoplus_{i \in I} M_i \right) \otimes_A N \cong \bigoplus_{i \in I} (M_i \otimes_A N).$$

6.0.43 Proposition. Supposons que A est commutatif. Soit M un A-module libre de base $\{e_i\}_{i \in I}$, et N un A-module libre de base $\{f_j\}_{j \in J}$. Alors $M \otimes_A N$ est libre de base $\{e_i \otimes f_j\}_{(i,j) \in I \times J}$.

6.1 Produit tensoriel de représentations

Soit G un groupe fini.

6.1.1 Définition (Produit tensoriel de représentations)**.** Soit $\mathbb{K}$ un corps, et V et W deux $\mathbb{K}G$-modules à gauche. Le **produit tensoriel** de V et W est le $\mathbb{K}$-espace vectoriel $V \otimes_{\mathbb{K}} W = V \otimes W$, muni de la structure de $\mathbb{K}G$-module suivante :

$$g(v \otimes w) = (gv) \otimes (gw),$$

étendue par linéarité (des deux cotés).

6.1.2 Remarque. Cette action de g correspond au produit tensoriel $\rho_V(g) \otimes \rho_W(g)$.

6.1.3 Proposition. Soient V et W deux $\mathbb{C}G$-modules. Alors

$$\chi_{V \otimes W} = \chi_V \chi_W.$$

Démonstration. Soit $E = \{e_i\}_{1\leq i\leq n}$ une base de V, et $F = \{f_j\}_{1\leq j\leq m}$ une base de W. Posons $A = \rho_V(g)_E^E$ et $B = \rho_W(g)_F^F$. Alors

$$\begin{aligned} ge_j &= \sum_{i=1}^{n} A_{ij} e_i \\ gf_s &= \sum_{r=1}^{m} B_{rs} f_r. \end{aligned}$$

Par la proposition précédente, $C = \{e_i \otimes f_r\}_{1\leq i\leq n, 1\leq r\leq m}$ forme une base de $V \otimes W$. L'action de g sur $V \otimes W$ est donnée par

$$\begin{aligned} g(e_j \otimes f_s) &= (ge_j) \otimes (gf_s) \\ &= \left(\sum_{i=1}^{n} A_{ij} e_i\right) \otimes \left(\sum_{r=1}^{m} B_{rs} f_r\right) \\ &= \sum_{i=1}^{n}\sum_{r=1}^{m} A_{ij} B_{rs} (e_i \otimes f_r) \\ &= A_{jj} B_{ss} (e_j \otimes f_s) + \sum_i \sum_r \cdots . \end{aligned}$$

Ainsi,

$$\begin{aligned} \chi_{V\otimes W}(g) &= \operatorname{tr} \rho_{V\otimes W}(g) \\ &= \sum_{j=1}^{n}\sum_{s=1}^{m} A_{jj} B_{ss} \\ &= \left(\sum_{j=1}^{n} A_{jj}\right)\left(\sum_{s=1}^{m} B_{ss}\right) \\ &= \chi_V(g)\chi_W(g). \end{aligned}$$

□

6.1.4 Corollaire. Soit r le nombre de classes de conjugaison de G, et soient $\chi_1, \ldots, \chi_r$ les caractères irréductibles de G. Posons

$$R(G) = \left\{ \sum_{i=1}^{r} m_i \chi_i \mid m_i \in \mathbb{Z}, \forall 1 \leq i \leq r \right\}.$$

On a que $R(G) \subseteq \mathcal{F}_C(G, \mathbb{C}) = \{\sum_{i=1}^{r} \lambda_i \chi_i \mid \lambda_i \in \mathbb{C}, \forall 1 \leq i \leq r\}$. De plus, $R(G)$ est un anneau commutatif, avec élément neutre χ_1, le caractère trivial.

Démonstration. Il est clair que c'est un groupe. Définissons la multiplication par

$$\chi_i \chi_j = \chi_{S_i \otimes S_j}.$$

On a alors que $\chi_i\chi_j = \sum_{k=1}^{r} m_k S_k$, où $S_i \otimes S_j = \bigoplus S_k^{\oplus m_k}$. Il est clair χ_1 est l'élément neutre ce cette multiplication, et que $R(G)$ est alors un anneau commutatif. □

6.1.5 Définition (Anneau des représentations)**.** L'anneau $R(G)$ s'appelle l'**anneau des représentations** de G.

6.1.6 Corollaire. L'ensemble $\{\chi \mid \chi \text{ est un caractère irréductible de degré } 1\}$ est un sous groupe de $R(G)^*$.

Démonstration. Montrons que cet ensemble est contenu dans $R(G)^*$. Soit χ_i un caractère irréductible de degré 1, et S_i sont $\mathbb{C}G$-module simple associé. Alors χ_i a pour inverse $\overline{\chi_i}$. En effet, si B est une base de S_i, alors $\rho_{S_i}(g)_B^B = (\varepsilon)$, pour un certain ε, racine de l'unité. On sait que $\varepsilon\overline{\varepsilon} = \overline{\varepsilon}\varepsilon = 1$. Donc $\chi_i\overline{\chi_i} = \overline{\chi_i}\chi = \chi_1$.

Montrons maintenant que cet ensemble est stable par addition. Si χ_j est un autre caractère irréductible de degré 1, et de module associé S_j, alors

$$\begin{aligned}\dim S_i \otimes S_j &= \dim S_i \dim S_j \\ &= 1,\end{aligned}$$

car S_i et S_j sont des $\mathbb{C}$-modules libres (i.e. des espaces vectoriels). □

6.1.7 Corollaire. Si χ est un caractère de degré 1, alors $\chi\chi_i$ est un caractère irréductible, pour tout caractère irréductible χ_i.

Démonstration. Si $\chi\chi_i$ se décompose, alors χ_i se décompose aussi, ce qui est absurde. □

6.1.8 Proposition. 1. Soient ϕ, χ, ψ trois caractères de G. Alors

$$\langle \phi\chi, \psi\rangle = \langle \phi, \overline{\chi}\psi\rangle.$$

2. Soient U, V, W trois $\mathbb{C}G$-modules. Alors

$$\langle \chi_{U\otimes V}, \chi_W\rangle = \langle \chi_U, \chi_{V^*\otimes W}\rangle.$$

Démonstration. 1. On a :

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

2. On a :

$$\begin{aligned}\langle \chi_{U\otimes V}, \chi_W\rangle &= \langle \chi_U\chi_V, \chi_W\rangle \\ &= \langle \chi_U, \overline{\chi_V}\chi_W\rangle \\ &= \langle \chi_U, \chi_{V^*}\chi_W\rangle \\ &= \langle \chi_U, \chi_{V^*\otimes W}\rangle.\end{aligned}$$

□

6.2 Représentation d'un produit direct

Soient G et H deux groupes finis. Soit V un $\mathbb{C}G$-module et W un $\mathbb{C}H$-module. On met sur $V \otimes W = V \otimes_{\mathbb{C}} W$ une structure de $\mathbb{C}(G \times H)$ module comme suit :

$$(g, h)(v \otimes w) = (gv) \otimes (hw),$$

qui est une action bien définie que l'on étend par linéarité.

6.2.1 Remarque. On peut munir V d'une structure de $\mathbb{C}(G \times H)$-module comme suit :

$$(g, h)v = gv.$$

On peut faire de même avec W. On a que $V \otimes W$ est alors le même $\mathbb{C}(G \times H)$-module que précédemment.

6.2.2 Proposition. Soit V un $\mathbb{C}G$-module, et W un $\mathbb{C}H$-module. Alors

$$\chi_{V\otimes W}(g, h) = \chi_V(g)\chi_W(h).$$

Démonstration. Par la remarque précédente. □

6.2.3 Notations.
- Le caractère du $\mathbb{C}(G \times H)$-module $V \otimes W$ se note $\chi_V \times \chi_W$. On a donc que $(\chi_V \times \chi_W)(g, h) = \chi_V(g)\chi_W(h)$.
- On note $\langle -, - \rangle_G$ le produit scalaire des caractères de G.

6.2.4 Théorème. Soient $\chi_1, \ldots, \chi_r$ les caractères irréductuble de G, et $\psi_1, \ldots, \psi_s$ les caractères irréductibles de H. Alors :

1. $\chi_i \times \psi_j$ est un caractère irréductible de $G \times H$, $\forall 1 \leq i \leq r, \forall 1 \leq j \leq s$,
2. $\{\chi_i \times \psi_j\}_{1\leq i\leq r, 1\leq j\leq s}$ est l'ensemble de tous les caractères irréductibles de $G \times H$.

Démonstration. 1. On a :

$$\begin{aligned}
\langle \chi_i \times \psi_j, \chi_i \times \psi_j \rangle_{G\times H} &= \frac{1}{|G \times H|} \sum_{(g,h)\in G\times H} (\chi_i \times \psi_j)(g, h)\overline{(\chi_i \times \psi_j)(g, h)} \\
&= \frac{1}{|G||H|} \sum_{g\in G} \sum_{h\in H} \chi_i(g)\psi_j(h)\overline{\chi_i(g)\psi_j(h)} \\
&= \left(\frac{1}{|G|} \sum_{g\in G} \chi_i(g)\overline{\chi_i(g)} \right) \left(\frac{1}{|H|} \sum_{h\in H} \psi_j(h)\overline{\psi_j(h)} \right) \\
&= \langle \chi_i, \chi_i \rangle_G \langle \psi_j, \psi_j \rangle_H \\
&= 1.
\end{aligned}$$

   Donc $\chi_i \times \psi_j$ est irréductible.

2. Le nombre de classes de conjugaison de $G \times H$ est $r \times s$ car toute classe de $G \times H$ est de la forme $C \times D$, où C et D sont des classes de G et H respectivement.

□

6.2.5 Remarque. Ce théorème fonctionne sur $\mathbb{C}$, mais pas sur un autre corps $\mathbb{K}$. On peut avoir V un $\mathbb{K}G$-module simple, W un $\mathbb{K}H$-module simple, mais $V \otimes W$ un $\mathbb{K}(G \times H)$-module non simple. Par exemple, $G = H = C_3 = \langle g \rangle$ et $\mathbb{K} = \mathbb{R}$. Posons $V = W = \mathbb{R}[X]/\langle X^2 + X + 1 \rangle$, où l'action par g correspond à la mltiplication par X. Alors V et W sont des $\mathbb{R}C_3$-modules simples de dimension 2 (malgré le fait que C_3 est abélien !), mais $V \otimes W$ n'est pas un $\mathbb{R}(C_3 \times C_3)$-module simple.

Chapitre 7

Représentation induite

7.0.6 Définition (Module induit)**.** Soit H un sous groupe d'un groupe fini G. Soit $\mathbb{K}$ un corps et V un $\mathbb{K}H$-module à gauche. On définit le $\mathbb{K}G$-module suitant :

$$\mathrm{Ind}_H^G(V) = \mathbb{K}G \otimes_{\mathbb{K}H} V,$$

l'**induite** de H à G de V, avec la structure de $\mathbb{K}G$-module suivante :

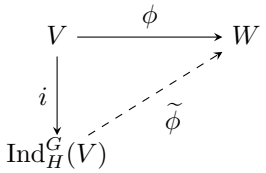
$$g(x \otimes v) = (gx) \otimes v.$$

On note

$$\begin{aligned} i : V &\longrightarrow \mathrm{Ind}_H^G(V) \\ v &\longmapsto 1 \otimes v \end{aligned}$$

qui est $\mathbb{K}H$-linéaire.

7.0.7 Propriété (universelle de l'induite)**.** Pour tout $\mathbb{K}G$-module W et pour toute application $\mathbb{K}H$-linéaire $\phi : V \longrightarrow W$, $\exists! \widetilde{\phi} : \mathrm{Ind}_H^G(V) \longrightarrow W$ qui est $\mathbb{K}G$-linéaire et telle que la diagramme suivant commute :



.

Démonstration. On définit

$$\begin{aligned} \widetilde{\phi} : \mathrm{Ind}_H^G(V) = \mathbb{K}G \otimes_{\mathbb{K}H} V &\longrightarrow W \\ g \otimes v &\longmapsto g\phi(v), \end{aligned}$$

qui est bien définit et étendu par linéarité. Clairement, $\widetilde{\phi} \circ i = \phi$. On vérifie que $\widetilde{\phi}$ est $\mathbb{K}G$-linéaire :

$$\begin{aligned} \widetilde{\phi}(g(x \otimes v)) &= \widetilde{\phi}((gx) \otimes v) \\ &= gx\phi(v) \\ &= g(x\phi(v)) \\ &= g\widetilde{\phi}(x \otimes v). \end{aligned}$$

On vérifie que $\widetilde{\phi}$ est unique :

$$\begin{aligned}\widetilde{\phi}(g \otimes v) &= \widetilde{\phi}(g(1 \otimes v)) \\ &= g\widetilde{\phi}(1 \otimes v) \\ &= g(\widetilde{\phi} \circ i)(v) \\ &= g\phi(v),\end{aligned}$$

ce qui montre que $\widetilde{\phi}$ est unique. □

7.0.8 Remarque (Autre formulation)**.** Si W est un $\mathbb{K}G$-module à gauche, alors $\mathrm{Res}_H^G(W)$ désigne le $\mathbb{K}H$-module obtenu en restreignant la structure de module. La propriété universelle : on a isomorphisme de $\mathbb{K}$-espaces vectoriels

$$\begin{aligned}\mathrm{Hom}_{\mathbb{K}G}(\mathrm{Ind}_H^G(V), W) &\xrightarrow{\cong} \mathrm{Hom}_{\mathbb{K}H}(V, \mathrm{Res}_{H,G}(W)) \\ \psi &\longmapsto \psi \circ i.\end{aligned}$$

7.0.9 Corollaire (Réciprocité de Frobenius)**.** On a

$$\langle \chi_{\mathrm{Ind}_H^G(V)}, \chi_W \rangle_G = \langle \chi_V, \chi_{\mathrm{Res}_H^G(W)} \rangle_H.$$

Démonstration. Rappelons que $\langle \chi_U, \chi_T \rangle = \dim \mathrm{Hom}_{\mathbb{C}G}(U, T)$ (série 7, ex. 4), où U et T sont des $\mathbb{C}G$-modules. □

7.1 Description de l'induite

On a $G = \coprod_{i=1}^m g_i H$, où $g_1, \ldots, g_m$ sont les représentants des classes à gauche. Alors $\mathbb{K}G$ se décompose comme $\mathbb{K}H$-module à droite :

$$\begin{aligned}\mathbb{K}G &= \mathbb{K}\left(\coprod_{i=1}^m g_i H\right) \\ &= \bigoplus_{i=1}^m \mathbb{K}(g_i H) \\ &= \bigoplus_{i=1}^m g_i \mathbb{K}H.\end{aligned}$$

On en déduit que

$$\begin{aligned}\mathrm{Ind}_H^G(V) &= \mathbb{K}G \otimes_{\mathbb{K}H} V \\ &= \left(\bigoplus_{i=1}^m g_i \mathbb{K}H\right) \otimes_{\mathbb{K}H} V \\ &= \bigoplus_{i=1}^m (g_i \mathbb{K}H \otimes_{\mathbb{K}H} V) \\ &= \bigoplus_{i=1}^m g_i \otimes V,\end{aligned}$$

où $g_i \otimes V = \{g_i \otimes v \mid v \in V\}$. Donc $\mathrm{Ind}_H^G(V)$ est une somme directe de sous espaces vectoriels.

7.1.1 Proposition. Soit $H \leq G$.

1. $g_i \otimes V \cong V$ comme $\mathbb{K}$-espaces vectoriels, via $g_i \otimes v \longmapsto v$.
2. $g_i \otimes V$ est muni d'une structure de $\mathbb{K}(g_i H g_i^{-1})$ via $g_i h g_i^{-1} v = g_i \otimes hv$.
3. $\dim \mathrm{Ind}_H^G(V) = [G : H] \dim V$.

Démonstration. 1. Remarquer que $\mathbb{K}G$ est un $\mathbb{K}H$-module libre à droite, de base $g_1, \ldots, g_m$.

2. Soit $h \in H$.

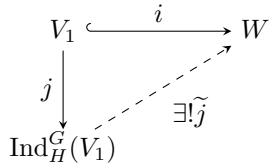
$$\begin{aligned}(g_i h g_i^{-1})(v \otimes g_i) &= g_i h(1 \otimes v) \\ &= g_i h \otimes v \\ &= g_i \otimes hv.\end{aligned}$$

3. Voire avant.

□

7.1.2 Proposition. On se donne un $\mathbb{K}G$-module W. On suppose que $W = V_1 \oplus \cdots \oplus V_m$ comme $\mathbb{K}$-espace vectoriel, tel que l'action de G permute transitivement les sous espaces V_i. Alors $W \cong \mathrm{Ind}_H^G(V_1)$, où $H = \mathrm{Stab}\, V_1$.

Démonstration. V_1 est un $\mathbb{K}H$-modules, puisque $hV_1 = V_1, \forall h \in H$. On a



,

i.e. $j \circ i(v) = \widetilde{j}(1 \otimes v) = j(v) = v$, $\forall v \in V_1$. Alors

$$\begin{aligned}\widetilde{j}(g \otimes V_1) &= g\widetilde{j}(1 \otimes V_1) \\ &= gV_1 \\ &= V_k,\end{aligned}$$

pour un certain k. Comme G agit transitivement sur les V_i, on a $V_l = gV_1$, pour un $g \in G$ bien choisi. Ainsi, $\widetilde{j}$ est surjective. Or $\dim \mathrm{Ind}_H^G(V_1) = m \dim V_1 = \dim W$. Par le théorème du rang, $\widetilde{j}$ est un isomorphisme et $W \cong \mathrm{Ind}_H^G(V_1)$. □

7.2 Caractère d'une induite

Rappelons que

$$\mathrm{Ind}_H^G(V) = \bigoplus_{i=1}^{m} g_i \otimes V,$$

où $g_1, \ldots, g_m$ sont les représentants des classes à gauche de H dans G. Pour tout $g \in G$, on a :

$$\begin{aligned}g(g_i \otimes V) &= gg_i \otimes V \\ &= g_j h \otimes V && \text{pour une unique paire } g_j, h \\ &= g_j \otimes hV \\ &= g_j \otimes V.\end{aligned}$$

Soit $E = \{e_1, \dots, e_p\}$ une base de V. Alors $\{g_i \otimes e_k\}_{1 \le k \le p}$ forme une base de $g_i \otimes V$. Donc $\{g_i \otimes e_k\}_{1 \le i \le m, 1 \le k \le p}$ forme une base de $\mathrm{Ind}_H^G(V)$. La matrice de $\rho_{\mathrm{Ind}_H^G(V)}(g)$ est, dans cette base, par bloc :

	$g_1 \otimes V$	$\cdots$	$g_i \otimes V$	$\cdots$	$g_m \otimes V$
$g_1 \otimes V$	?	$\cdots$	0	$\cdots$	?
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$g_j \otimes V$	?	$\cdots$	$*$	$\cdots$	?
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$g_m \otimes V$	?	$\cdots$	0	$\cdots$	?

si $g(g_j \otimes V) = g_i \otimes V$. Cela signifie qu'il n'y a qu'un seul bloc non nul par colonne bloc. Pour le calcul de la trace, il ne reste que les blocs diagonaux.

- Si $g(g_j \otimes V) \neq g_j \otimes V$, alors la j-ème colonne pas bloc ne contribue pas.
- Si $g(g_j \otimes V) = g_j \otimes V$, alors on a un bloc diagonal et $gg_j = g_j h$, pour un certain $h \in H$, i.e. $g_j g g_j^{-1} \in H$. Dans ce cas, la contribution de ce bloc dans le calcul de la trace est la trace de l'action de h sur V car $g(g_j \otimes V) = g_j \otimes hV$.

Par conséquent :

$$\chi_{\mathrm{Ind}_H^G(V)}(g) = \sum_{g_j g g_j^{-1} \in H} \chi_V(g_j g g_j^{-1}).$$

On a aunsi la formule du caractère de l'induite.

7.2.1 Remarque. On peut définir l'induite d'une fonction centrale $f \in \mathcal{F}_C(H, \mathbb{C})$ par la formule

$$\mathrm{Ind}_H^G(f)(g) = \sum_{g_j g g_j^{-1} \in H} f(g_j g g_j^{-1}).$$

Cela donne une fonction centrale sur G. Remarquer que $\mathrm{Ind}_H^G(\chi_V) = \chi_{\mathrm{Ind}_H^G(V)}$. On a en particulier la réciprocité de Frobenius :

$$\Big\langle \mathrm{Ind}_H^G(f_1), f_2 \Big\rangle_G = \big\langle f_1, \mathrm{Res}_H^G(f_2) \big\rangle_H ,$$

où $\mathrm{Res}_H^G(f_2) = f_2|_H$.

7.2.2 Théorème. Soit $H \trianglelefteq G$. On se donne un $\mathbb{C}G$-module simple V. On suppose que $V \ncong g \otimes V$, $\forall g \notin H$. Alors $\mathrm{Ind}_H^G(V)$ est un $\mathbb{C}G$-module simple.

Démonstration. Soit $g_1, \dots, g_m$ les représentants des classes de H dans G. Sans perte de généralité, $g_1 = 1$. On a

$$\mathrm{Res}_H^G \mathrm{Ind}_H^G(V) = \bigoplus_{i=1}^{m} \underbrace{g_i \otimes V}_{\mathbb{K}H\text{-mod conj.}} .$$

Puis :

$$\begin{aligned}
\left\langle \chi_{\mathrm{Ind}_H^G(V)}, \chi_{\mathrm{Ind}_H^G(V)} \right\rangle_G &= \left\langle \mathrm{Ind}_H^G(\chi_V), \mathrm{Ind}_H^G(\chi_V) \right\rangle_G \\
&= \left\langle \chi_V, \mathrm{Res}_H^G \mathrm{Ind}_H^G(\chi_V) \right\rangle_H \\
&= \left\langle \chi_V, \chi_{\mathrm{Res}_H^G \mathrm{Ind}_H^G(V)} \right\rangle_H \\
&= \left\langle \chi_V, \sum_{i=1}^m \chi_{g_i \otimes V} \right\rangle_H \\
&= \sum_{i=1}^m \langle \chi_V, \chi_{g_i \otimes V} \rangle_H \\
&= \langle \chi_V, \chi_{g_1 \otimes V} \rangle_H + \sum_{i=2}^m \underbrace{\langle \chi_V, \chi_{g_i \otimes V} \rangle_H}_{=0 \text{ car } V \ncong g_i \otimes V} \\
&= \langle \chi_V, \chi_{1 \otimes V} \rangle_H \\
&= \langle \chi_V, \chi_V \rangle_H \\
&= 1.
\end{aligned}$$

□

7.2.3 Remarque. On sait que $g \otimes V$ est un $\mathbb{K}(gHg^{-1})$-module, donc un $\mathbb{K}H$-module, car $H \trianglelefteq G$. On l'appelle **module conjugué** de V. L'action de h sur $g \otimes V$ est égale à l'action de $g^{-1}hg$ sur V.

7.2.4 Exemples. Posons $G = \mathfrak{S}_3$, $H = \langle h \rangle \trianglelefteq \mathfrak{S}_3$, où $h = (1\,2\,3)$,

$$\begin{aligned}
\rho_V : H &\longrightarrow \mathbb{C}^* \\
h &\longmapsto e^{\frac{2i\pi}{3}} = \omega.
\end{aligned}$$

On a $\mathfrak{S}_3 = H \cup gH$, où $g = (1\,2)$. L'action $\rho_{g \otimes V} : H \longrightarrow \mathbb{C}^*$ est donnée par

$$\begin{aligned}
h(g \otimes v) &= hg \otimes v \\
&= gg^{-1}hg \otimes v \\
&= g \otimes g^{-1}hgv.
\end{aligned}$$

Ainsi, h agit sur $g \otimes V$ comme $g^{-1}hg$ agissant sur V. Or $g^{-1}hg = h^{-1}$. Il vient que h^{-1} agit par $\omega^{-1} \neq \omega$, et donc que $g \otimes V \ncong V$. On utilise le théorème précédent et on obtient que $\mathrm{Ind}_H^{\mathfrak{S}_3}(V)$ est un $\mathbb{C}\mathfrak{S}_3$-module simple de dimension 2. Son caractère est par exemple :

$$\begin{aligned}
\chi_{\mathrm{Ind}_H^{\mathfrak{S}_3}(V)}(1) &= 2 \\
\chi_{\mathrm{Ind}_H^{\mathfrak{S}_3}(V)}((1\,2)) &= 0 \\
\chi_{\mathrm{Ind}_H^{\mathfrak{S}_3}(V)}((1\,2\,3)) &= \omega + \omega^{-1} = -1.
\end{aligned}$$

Index

— Symboles —

— A —

— C —

— D —

— E —

— F —

— G —

— H —

— I —

— M —

— P —

— R —

— S —

— T —