Préparation à l'agrégation

Représentation des groupes

2 Février 2011

Action de groupes

Une action d'un groupe G sur un ensemble X est une application

$$m\colon \begin{cases} G \times X \longrightarrow X \\ (g, x) \longmapsto g \cdot x \end{cases}$$

vérifiant les deux axiomes suivants :

1. $1_G \cdot x = x$ pour tout $x \in X$
2. $(g'g) \cdot x = g' \cdot (g \cdot x)$ pour tous $g, g' \in G$ et $x \in X$

Chaque élément $g \in G$ définit alors une application $\alpha_g : X \to X$ donnée par $\alpha_g(x) = g \cdot x$. L'axiome (**1**) se réécrit alors $\alpha_{1_G} = \mathrm{id}_X$. L'axiome (**2**) se réécrit $\alpha_{g'g} = \alpha_{g'} \circ \alpha_g$ pour tout $g, g' \in G$. On en déduit que les α_g sont des bijections de X. Finalement une action de G est équivalente à la donnée d'un morphisme de groupes

$$\alpha\colon \begin{cases} G \longrightarrow \mathfrak{S}_X \\ g \longmapsto \alpha_g : (x \mapsto g \cdot x) \end{cases}$$

Si X est structuré

Lorsque l'espace X est muni d'une structure (groupe, anneau, espace vectoriel, topologie), les actions « respectant cette structure » sont particulièrement intéressantes. Que signifie donc ce « respectant la structure » ? De manière concrète, les α_g ne pas simplement des bijections de X mais des automorphismes pour la structure sur X. Par exemple, l'action de G sur lui-même (ou sur un de ses sous-groupes distingués) par conjugaison respecte la structure de groupe : pour tout $g \in G$, l'application $\alpha_g : x \mapsto gxg^{-1}$ est un automorphisme de groupes.

Une action respectant la structure (ou compatible avec la structure) se résume ainsi à un morphisme de groupe pas uniquement à valeurs dans $\mathfrak{S}_X$ mais à valeurs dans le sous-groupe des automorphismes de X pour la structure considérée.

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[dr, "\alpha"'] & \mathfrak{S}_X \\ & \cup \\ & \mathrm{Aut}(X) \end{tikzcd}$$

Action linéaire

Dans la suite du cours, on s'intéresse aux actions d'un groupe G sur un espace vectoriel V qui sont compatibles cette structure.

Définition – G-module. Un G-module (sur k) est un couple (V, ρ) où V est un espace vectoriel sur k et $\rho : G \to \mathrm{GL}(V)$ un morphisme de groupes. On dit aussi que (V, ρ) est une *représentation linéaire de G sur k*.

En d'autres termes une représentation linéaire (sur k) est une application

$$m : \begin{cases} G \times V \longrightarrow V \\ (g, v) \longmapsto gv \end{cases}$$

où V est un k-espace vectoriel vérifiant

1. $1_G \cdot v = v$ pour tout $v \in V$
2. $(g'g) \cdot v = g' \cdot (g \cdot v)$ pour tous $g, g' \in G$ et $v \in V$
3. $g \cdot (\lambda v + v') = \lambda g \cdot v + g \cdot v'$ pour tous $g \in G$, $v, v' \in V$ et $\lambda \in k$

G-module

Remarque Le morphisme « structurel » ρ est toujours omis et on dit « soit V un G-module » ou « soit V une représentation linéaire de G » et non « soit (V, ρ) un G-module ».

Définition – Degré. Soit V une représentation (linéaire) de G. La dimension de V est appelé le degré de V.

G-morphisme

Définition – Morphisme de G-modules. Soient V, W deux représentations linéaires de G sur k. Un morphisme de G-modules (sur k) (on dit aussi application G-linéaire, ou G-morphisme) de V dans W est une application k-linéaire et G-équivariante c'est-à-dire

$$f(\lambda v + v') = \lambda f(v) + f(v') \qquad \text{et} \qquad f(gv) = gf(v)$$

pour tout $\lambda \in k$, $v, v' \in V$ et $g \in G$.

On note $\mathrm{Hom}_G(V, W)$ l'ensemble des G-morphismes de V dans W. C'est un sous-k-espace vectoriel de $\mathrm{Hom}_k(V, W)$.

Définition – Isomorphisme de G-modules. Soit V, W deux représentations linéaires de G sur k. Un isomorphisme de G-modules de V dans W est un morphisme de G-module $\varphi : V \to W$ tel qu'il existe un morphisme de G-module $\psi : W \to V$ tel que $\psi\varphi = \mathrm{id}_V$ et $\varphi\psi = \mathrm{id}_W$.
On dit alors que V et W sont des G-modules isomorphes.

Sous-G-module

Définition – Sous-G-module. Soit (V, ρ) une représentation linéaire de G. On dit que $W \subset V$ est un sous-G-module (une sous-représentation) de V si W est un sous-espace vectoriel de V stable par $\rho(g)$ pour tout $g \in G$ c'est-à-dire $\rho(g)w \in W$ pour tous $w \in W$ et $g \in G$.
L'inclusion $i : w \in W \mapsto w \in V$ est alors un morphisme de G-modules.

Définition – Module quotient. Soit V un G-module et W un sous-G-module et $\pi : V \to V/W$ la surjection canonique. Il existe sur V/W une unique structure de G-module telle que π soit un morphisme de G-modules. On dit que V/W est le G-module quotient de V par W.

Machinerie structurelle

1. id_V, composition des G-morphismes
2. Isomorphisme = Morphisme bijectif
3. Sous-G-module engendré
4. Image directe et image réciproque, noyau et image
5. Théorème de correspondance
6. Théorèmes d'isomorphisme : $V/\mathrm{Ker}\, f \overset{G\text{-mod.}}{\simeq} \mathrm{Im}\, f$,
   $(W + W')/W \overset{G\text{-mod.}}{\simeq} W'/(W \cap W')$,
   $(V/W)/(W'/W) \overset{G\text{-mod.}}{\simeq} V/W'$ (si $W \subset W'$)

Des G-modules isomorphes ont le même degré. La réciproque est bien sûr fausse en général.

Produit et somme directe

Définition – Produit et somme directe. Soient V et W deux G-modules, on définit sur l'espace vectoriel $V \times W$ une structure de G-module par

$$\begin{cases} G \times (V \times W) \longrightarrow V \times W \\ (g,(v,w)) \quad \longmapsto (g_V v, g_W w) \end{cases}$$

Les applications $p_V : (v,w) \in V \times W \to v \in V$ et $p_W : (v,w) \in V \times W \to w \in W$ sont des morphismes surjectifs de G-modules. Les applications $i_V : v \in V \to (v,0) \in V \times W$ et $i_W : w \in W \to (0,w)$ sont des morphismes injectifs de G-modules qui permettent d'identifier V et W à des sous-G-modules de $V \times W$ (qui sont respectivement $V \times \{0\}$ et $\{0\} \times W$) vérifiant $V \times W = V \oplus W$.

Pour cette raison, on note lorsqu'on étudie les représentations des groupes, on note le produit de deux G-modules par $V \oplus W$ plutôt que $V \times W$ (même si V et W ne sont pas des sous-espaces vectoriels d'un même espace vectoriel).

G-module et morphisme

Proposition Soient V, W deux G-modules. L'application

$$\begin{cases} G \times \mathrm{Hom}_k(V,W) \longrightarrow \mathrm{Hom}_k(V,W) \\ \qquad (g,f) \qquad\qquad \longmapsto g \cdot f := gfg^{-1} = \rho_W(g) \circ f \circ \rho_V(g^{-1}) \end{cases}$$

munit $\mathrm{Hom}_k(V,W)$ d'une structure de G-module dont l'ensemble des points fixes est $\mathrm{Hom}_G(V,W)$.

Exemple – Un exemple de G-module. On considère l'action triviale de G sur k : $gx = x$ pour tous $g \in G$ et $x \in k$. On obtient ainsi une structure de G-module sur k (le morphisme de groupes $\rho : G \to \mathrm{GL}(k)$ correspondant est le morphisme trivial). Le module obtenu est appelé le G-module trivial.

Application – Représentation contragrédiente. Soit (V, ρ) un G-module. La représentation contragrédiente est la représentation associée à $V^* = \mathrm{Hom}_k(V,k)$ où G agit sur V par ρ et trivialement sur k. On a donc $\rho_{V^*}(g) = {}^t\rho(g)^{-1}$.

Construction de représentations

Définition – Module de permutation. Soit G un groupe et X un ensemble sur lequel G agit. On définit sur l'espace vectoriel $\mathscr{F}(X,k)$ des fonctions de X dans k une structure de G-module par la relation $(g \cdot f)(x) = f(g^{-1}x)$ où $f : X \to k$ et $g \in G$.
Le sous-espace vectoriel kX des fonctions à support fini est un sous-G-module de $\mathscr{F}(X,k)$ dont une base est $(\delta_x)_{x\in X}$ où $\delta_x(y) = \delta_{x,y}$ pour tout $y \in Y$.
On vérifie que $g\delta_x = \delta_{gx}$ pour tous $x \in X$ et $g \in G$.
On a construit ainsi à partir de X un espace vectoriel dont une base est formée « des éléments de X » et l'action de G sur kX s'obtient par linéarisation de celle de G sur X. On dit que kX est le G-module de permutation associé à X. Un élément de kX s'écrit

$$\sum_{x\in X} \lambda_x \delta_x = \sum_{x\in X} \lambda_x x$$

Exemples

Exemple – G-module trivial. Le G-module trivial est le G-module de permutation associé au G-ensemble trivial $X = \{x\}$.

Exemple – Représentation régulière. On considère kG le G-module de permutation associé à l'action de G sur lui-même par translation à gauche. C'est un G-module de dimension $|G|$ appelé représentation régulière de G. Un élément de kG s'écrit

$$v = \sum_{g \in G} \lambda_g \delta_g = \sum_{g \in G} \lambda_g g$$

où les $\lambda_g \in k$ sont uniquement déterminés. De plus, on a $g'v = \sum_{g \in G} \lambda_g g' g$.

En fait, kG peut être muni d'une structure de k-algèbre (voir MG 92) par la relation $\delta_g \cdot \delta'_g = \delta_{gg'}$ entendue par bilinéarité ou encore

$$\left(\sum_{g \in G} \lambda_g g\right)\left(\sum_{g \in G} \mu_g g\right) = \sum_{g, g' \in G} \lambda_g \mu_{g'} g g' = \sum_{g \in G} \left(\sum_{h \in G} \lambda_h \mu_{h^{-1}g}\right) g$$

Problématique

Étant donné deux représentations d'un même groupe G, on cherche à savoir quand est-ce qu'elles sont isomorphes. Pour les espaces vectoriels, on écrit $V = k \oplus \cdots \oplus k$ et le nombre de termes caractérise la classe d'isomorphisme : c'est la théorie de la dimension.
Pour les G-modules, la méthode va reposer sur des arguments similaires, on va montrer qu'on peut décomposer V en une somme directe (ce sera le théorème de Maschke) de G-modules « simples » qu'on appellera justement les G-modules simples ou irréductibles.

À partir de maintenant, G désigne un groupe fini et les représentations sont toutes de dimension finie sur le corps $\mathbb{C}$ (corps algébriquement clos de caractéristique nulle).

Module simple ou irréductible

Définition – G-module simple. Soit V une représentation linéaire d'un groupe G. Si V a exactement deux sous-G-modules (qui sont alors $\{0\}$ et V), on dit que V est un G-module simple ou irréductible.

Remarque « Les G-modules simples sont aux G-modules ce que les vecteurs propres sont aux endomorphismes diagonalisables ».

Lemme de Schur

Proposition – Lemme de Schur. Soit V un G-module simple et W un G-module.

1. Si $f \in \mathrm{Hom}_G(V, W)$ alors f est nul ou injectif.
2. Si $f \in \mathrm{Hom}_G(W, V)$ alors f est nul ou surjectif.
3. Si, de plus, W est simple et que $0 \neq f \in \mathrm{Hom}_G(V, W)$ alors f est isomorphisme.

Preuve. Un sous-G-module de V est 0 ou V. Ainsi dans (**1**), $\mathrm{Ker}\, f = \{0\}$ ou $\mathrm{Ker}\, f = V$. Dans (**2**), $\mathrm{Im}\, f = \{0\}$ ou $\mathrm{Im}\, f = V$. Dans (**3**), on a $\mathrm{Im}\, f = W$ et $\mathrm{Ker}\, f = \{0\}$.

Corollaire – Lemme de Schur. Si V est un G-module simple alors $\mathrm{End}_G(V) = \mathbb{C}\mathrm{id}_V$.

Corollaire – Lemme de Schur. Si V et W sont deux G-modules simples non isomorphes alors $\mathrm{Hom}_G(V, W) = \{0\}$.

Lemme de Schur (suite)

Preuve. *Preuve 1.* Soit $f \in \mathrm{End}_G(V)$. Comme $\mathbb{C}$ est algébriquement clos, f admet une valeur propre λ (c'est un endomorphisme d'un espace vectoriel de dimension finie). Ainsi $f - \lambda \mathrm{id}_V$ est un G-endomorphisme de V non injectif. Donc $f - \lambda \mathrm{id}_V = 0$.

Preuve 2. D'après (3), $\mathrm{End}_G(V)$ est une sous-algèbre à division (c'est-à-dire un corps non nécessairement commutatif) de $\mathrm{End}_{\mathbb{C}}(V)$. Comme V est de dimension finie, f est algébrique sur $\mathbb{C}$ (dans la $\mathbb{C}$-algèbre $\mathrm{End}_G(V)$). Mais $\mathbb{C}$ est algébriquement clos, ainsi $f \in \mathbb{C} = \mathbb{C}\mathrm{id}_V$.

Lemme de Schur (fin)

Remarque – Espace de morphismes. Si V et W sont deux G-modules isomorphes et $f : V \to W$ un G-isomorphisme. On a $\mathrm{Hom}_G(V, W) = f\mathrm{End}_G(V) = \mathrm{End}_G(W)f$.
En effet, si $f' \in \mathrm{Hom}_G(V, W)$, on a $f^{-1}f' \in \mathrm{End}_G(V)$ et $f'f^{-1} \in \mathrm{End}_G(W)$.

Corollaire – Lemme de Schur. Si V et W sont deux G-modules simples isomorphes et $0 \neq f \in \mathrm{Hom}_G(V, W)$. Alors $\mathrm{Hom}_G(V, W) = \mathbb{C}f$ est une droite vectorielle.

Point fixe

Moyenner pour rendre invariant ! : la technique du moyennage introduite au XIXe siècle.

Proposition Soit (V, ρ) un G-module. L'application

$$p_V = \frac{1}{|G|} \sum_{g \in G} \rho(g) \in \mathrm{End}_{\mathbb{C}}(V)$$

est un projecteur G-linéaire d'image
$V^G := \{v \in V, \ \ \forall, g \in G, \ gv = v\}$.

Preuve. Comme ρ est un morphisme de groupes et que $\rho(g)$ est $\mathbb{C}$-linéaire, on a $\rho(g) \circ p_V = p_V = p_V \circ \rho(g)$ ce qui donne le fait que p_V est un projecteur G-linéaire.
Par ailleurs, si $gv = v$ pour tout $g \in G$, on a alors $p_V(v) = v$.
Ainsi $V^G \subset \mathrm{Im}\, p_V$. Réciproquement, si $v = p_V(w)$ alors
$gv = gp_V(w) = p_V(w)$ et $\mathrm{Im}\, p_V \subset V^G$.

Théorème de Maschke

Proposition – Théorème de Maschke. Soit V un G-module et W un sous-G-module de V. Alors W admet un sous-G-module supplémentaire : il existe W' un sous-G-module de V tel que $V = W \oplus W'$.

Preuve. On considère $p : V \to V$ un projecteur d'image W et on pose

$$q := p_{\mathrm{End}_{\mathbb{C}}(V)}(\varepsilon)(p) = \frac{1}{|G|} \sum_{g \in G} \rho_{\mathrm{End}_{\mathbb{C}}(V)}(g)(p)$$

c'est-à-dire

$$q = \frac{1}{|G|} \sum_{g \in G} \rho_V(g) \circ p \circ \rho_V(g^{-1}) \in \mathrm{End}_{\mathbb{C}}(V)^G = \mathrm{End}_G(V)$$

Ainsi q est un G-endomorphisme de V. Montrons que q est un projecteur d'image W. En posant $W' = \mathrm{Ker}\, q$, on aura alors le résultat souhaité.

q est un projecteur

On commence par remarquer que $p \circ \rho_V(g^{-1})(V) \subset W$ et donc $\rho_V(g) \circ p \circ \rho_V(g^{-1})(V) \subset W$ pour tout $g \in G$ (puisque W est G-stable). Ainsi $\operatorname{Im} q \subset W$.
Considérons à présent $v \in W$. Comme $\rho_V(g^{-1})(v) \in W$ (puisque W est un G-module), on a

$$q(v) = \frac{1}{|G|} \sum_{g \in G} \rho_V(g) p(\rho_V(g^{-1})(v)) = \frac{1}{|G|} \sum_{g \in G} \rho_V(g)(\rho_V(g^{-1})(v)) = v$$

Ainsi $q_{|W} = \mathrm{id}_W$ et $W \subset \operatorname{Im} q$.
Finalement $W = \operatorname{Im} q$ et $q_{|\operatorname{Im} q} = \mathrm{id}$. Ainsi q est un projecteur d'image W.

Semisimplicité

Proposition – Semisimplicité. Tout G-module est somme directe finie de G-module simple.

Preuve. On raisonne par récurrence sur la dimension de V. Si $\dim V = 0$ alors V est somme directe de 0 module simple. On suppose le résultat vrai pour les G-modules de dimension inférieure ou égale à n et on considère V un G-module de dimension $n+1$. Si V est irréductible alors le résultat est clair. Sinon, il existe W un sous-G-module de V vérifiant $0 \neq W \neq V$. D'après le théorème de Maschke, il existe un sous-G-module W' vérifiant $W \oplus W' = V$. En appliquant l'hypothèse de récurrence à W et W', on obtient le résultat.

Décomposition

Proposition – Décomposition en irréductible. Soit V un G-module. On peut écrire $V = {V_1}^{a_1} \oplus \cdots \oplus {V_s}^{a_s}$ où les V_i sont des G-modules irréductibles deux à deux non isomorphes et les $a_i \in \mathbb{N}$. Si $V = {V_1}^{a_1} \oplus \cdots \oplus {V_s}^{a_s} = {W_1}^{b_1} \oplus \cdots \oplus {W_r}^{b_r}$ sont deux tels écritures avec $a_i, b_j \in \mathbb{N}^*$ alors $r = s$ et il existe une permutation de $[\![1\,,\, s]\!]$ tel que $V_i = W_{\sigma(i)}$ et $a_i = b_{\sigma(i)}$.

Preuve. On a vu que V peut se décomposer en somme directe de représentations simples. En regroupant les termes identiques suivant leur classe d'isomorphisme, on obtient la décomposition voulue.
Si W est un G-module simple, on a

$$\mathrm{Hom}_G(W, V) = \bigoplus_{i=1}^{s} \mathrm{Hom}_G(W, V_i)^{a_i} = \bigoplus_{i=1}^{r} \mathrm{Hom}_G(W, W_i)^{b_i}$$

Si $W = V_i$ alors, d'après le lemme de Schur, on a $\mathrm{Hom}_G(W, V_j) = \{0\}$ si $j \neq i$ et $\mathrm{Hom}_G(W, V_i) \overset{\mathbb{C}\text{-ev.}}{\simeq} \mathbb{C}$. Ainsi $\dim_{\mathbb{C}} \mathrm{Hom}_G(W, V) = a_i > 0$.

Suite de la preuve

Si $W = V_i$ n'est isomorphe à aucun des W_i alors, toujours avec le lemme de Schur, on a $\mathrm{Hom}_G(W, V) = 0$ ce qui est absurde. Ainsi, il existe un unique $\sigma(i)$ tel que $V_i = W_{\sigma(i)}$. Et on obtient alors $a_i = b_{\sigma(i)}$ en calculant $\dim \mathrm{Hom}_G(W, V)$.
En échangeant le rôle de W_i et V_i, on obtient que σ est une bijection et que donc $r = s$.

Remarque – Unicité. Attention, il est important de bien comprendre le sens de l'unicité dans la proposition précédente. Elle ne dit pas du tout que les sous-G-modules isomorphes à V_i contenus dans V sont uniquement déterminés et au nombre de a_i. Il faut comparer cette décomposition à la décomposition en sous-espace propre d'un endomorphisme diagonalisable (qui correspond en gros au cas où G est le groupe cyclique). Dans ce cas, les V_i sont vus dans V comme des droites propres de valeurs propres fixées λ_i et a_i est la dimension du sous-espace propre associé à la valeur propre λ_i.

Nombre de simples

On a vu qu'on pouvait caractériser la classe d'isomorphisme d'un G-module par une famille d'entiers indexées par les classes d'isomorphismes de représentations irréductibles de G : si $(V_i)_{i\in I}$ est une famille de représentants des classes d'isomorphismes des G-modules simples alors la famille V se décompose de façon unique sous la forme $V = \bigoplus_{i\in I} {V_i}^{a_i}$.

L'objectif est maintenant de s'intéresser d'un peu plus près à l'ensemble I : Est-il fini ? Combien a-t-il d'éléments ? De façon précise, on va montrer que le nombre de classes d'isomorphismes de représentations simples de G est le nombre de classes de conjugaison de G. L'outil crucial est celui de caractère d'une représentation.

Caractère

Définition – Caractère d'une représentation linéaire. Soit G un groupe et V une représentation de dimension finie de G sur k. On définit le caractère de V comme la fonction

$$\chi_V : \begin{cases} G \longrightarrow k \\ g \longmapsto \chi_V(g) := \mathrm{tr}\left(\rho_V(g)\right) \end{cases}$$

Remarque – Valeur d'un caractère. Pour tout $g \in G$, $\rho_V(g)$ est un endomorphisme diagonalisable de V dont les valeurs propres sont des racines $|G|^{\mathrm{e}}$ de l'unité.
En effet, d'après le théorème de Lagrange, on a $\rho_V(g)^{|G|} = \mathrm{id}_V$ et le polynôme $X^{|G|} - 1$ est scindé à racines simples dans $\mathbb{C}$.
Ainsi $\chi_V(g)$ est une somme de racine $|G|^{\mathrm{e}}$ de l'unité. En particulier, $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.

Tout est contenu dans les caractères

Théorème Soit G un groupe **fini** et k un corps de caractéristique **nulle**. Alors deux représentations (de dimension finie) de G sur k sont isomorphes si et seulement si elles ont les mêmes caractères.

Preuve. **($\Rightarrow$)** Soient $f : V \to W$ un G-isomorphisme et $\mathscr{B}$ une base de V. On a donc $\rho_W(g) = f\rho_V(g)f^{-1}$. Ainsi pour tout $g \in G$, la matrice de $\rho_V(g)$ dans la base $\mathscr{B}$ coïncide avec la matrice de $\rho_W(g)$ dans la base $f(\mathscr{B})$.
($\Leftarrow$) La réciproque demande du travail. On va la démontrer en même temps qu'on calcule le nombre de représentations irréductibles.

Calcul de caractères

Lemme – Somme directe. Soient V et W deux représentations linéaires de dimension finie de G. On a alors

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

et $\forall g \in G, \quad \chi_{V^*}(g) = \chi_V(g^{-1})$ et $\chi_{\mathrm{Hom}_k(V,W)} = \chi_{V^*}\chi_W$

La fonction de G dans k constante et égale à 1 est le caractère de la représentation triviale. On l'appelle le caractère trivial.

Si X est un G-ensemble alors le caractère de la représentation kX est donné par $\chi_{kX}(g) = |\{x \in X,\ gx = x\}| = |X^g|$.

On a
$$\chi_V(1_G) = \dim V.$$

On a
$$\chi_V(g) = \dim V \iff \rho_V(g) = \mathrm{id}_V$$

et
$$|\chi_V(g)| = \dim V \iff \rho_V(g) \text{ est une homothétie.}$$

Preuve

Preuve. En concaténant une base de V à une base de W, on obtient une base de $V \oplus W$ dans laquelle la matrice de $\rho_{V \oplus W}(g)$ est de la forme

$$\begin{bmatrix} \rho_V(g) & \\ & \rho_W(g) \end{bmatrix}$$

Soit $\mathscr{B}$ une base de V. Par définition, on a $\rho_{V^*}(g) = {}^t\rho_V(g^{-1})$.
La matrice de $\rho_{V^*}(g)$ dans la base duale de $\mathscr{B}$ est la transposée de celle de $\rho_V(g^{-1})$ dans la base $\mathscr{B}$.
En calculant la matrice de $\rho_{\mathrm{Hom}_k(V,W)}(g)$ dans la base des E_{ij}, on obtient l'égalité pour le caractère de $\mathrm{Hom}_k(V, W)$.
En calculant la matrice de $\rho_{kX}(g)$ dans la base $(\delta_x)_{x \in X}$, on obtient le caractère de kX.
On a $\rho_V(1_G) = \mathrm{id}_V$.
Par ailleurs, $\chi_V(g)$ est une somme de $\dim V$ racines $|G|^{\mathrm{e}}$ de l'unité.
Le résultat s'obtient alors comme conséquence du cas d'égalité dans l'inégalité triangulaire.

Fonction centrale

Définition – Fonction centrale. Soit $f : G \to \mathbb{C}$ une application. On dit que f est une fonction centrale sur G si $f(g) = f(g')$ dès que g et g' sont conjugués (c'est-à-dire il existe $h \in G$ tel que $g' = hgh^{-1}$). Autrement dit, une fonction centrale est une fonction constante sur chacune des classes de conjugaison de G ou encore une fonction qui passe au quotient par la relation d'équivalence $\sim$ de conjugaison.

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\pi"'] & \mathbb{C} \\
G/\sim \arrow[ur, "\overline{f}"'] &
\end{tikzcd}$$

L'ensemble des fonctions centrales forme un espace vectoriel dont la dimension est le nombre de classes de conjugaison de G.

Caractère et fonction centrale

Proposition Tout caractère est une fonction centrale.

Preuve. Cela résulte simple de la relation $\mathrm{tr}\,(AB) = \mathrm{tr}\,(BA)$. En effet, on a $\rho_V(g') = \rho_V(h)\rho_V(g)\rho_V(h^{-1})$. En calculant la trace, on obtient le résultat.

Dans la suite, on va comparer l'espace vectoriel des fonctions centrales avec l'espace vectoriel engendré par les caractères. Pour cela, on va utiliser un peu d'algèbre bilinéaire ainsi que la notion de point fixe.

Forme hermitienne

Sur l'espace vectoriel $\mathscr{F}(G, \mathbb{C})$ des fonctions de G dans $\mathbb{C}$, on définit la forme hermitienne définie positive canonique

$$\langle f, f' \rangle_G = \frac{1}{|G|} \sum_{g \in G} f(g) \overline{f'(g)}$$

Elle induit par restriction une forme hermitienne définie positive sur l'espace vectoriel des fonctions centrales.

Les deux calculs cruciaux

Proposition – Produit scalaire de caractères. Soient V, W deux caractères de G. On a

$$\langle \chi_V, \mathbf{1} \rangle_G = \dim_{\mathbb{C}} V^G \in \mathbb{N}$$

et

$$\langle \chi_V, \chi_W \rangle = \dim_{\mathbb{C}} \mathrm{Hom}_G(W, V) \in \mathbb{N}$$

Preuve. On a

$$\langle \chi_V, \mathbf{1} \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\,(\rho_V(g)) = \mathrm{tr}\left(\frac{1}{|G|} \sum_{g \in G} \rho_V(g) \right)$$

Ainsi

$$\langle \chi_V, \mathbf{1} \rangle_G = \mathrm{tr}\,(p_V)$$

où p_V est le projecteur d'image V^G introduit plus haut.

Le deuxième calcul crucial

On a

$$\langle \chi_V, \chi_W \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \overline{\chi_W(g)} = \frac{1}{|G|} \sum_{g \in G} \chi_V(g) \chi_W(g^{-1})$$

Or
$$\chi_V(g)\chi_W(g^{-1}) = \chi_{\mathrm{Hom}_{\mathbb{C}}(W,V)}(g),$$

ainsi $\langle \chi_V, \chi_W \rangle_G = \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{Hom}_{\mathbb{C}}(W,V)}(g) = \langle \chi_{\mathrm{Hom}_{\mathbb{C}}(W,V)}, \mathbf{1} \rangle$.

On conclut avec le première égalité et le fait que
$\mathrm{Hom}_{\mathbb{C}}(W, V)^G = \mathrm{Hom}_G(W, V)$.

le Lemme de Schur revisité

Proposition Soient V et W deux représentations simples. On a $\langle \chi_V, \chi_W \rangle_G = 1$ si V et W sont isomorphes et 0 sinon.

Preuve. On a $\langle \chi_V, \chi_W \rangle_G = \dim GWV$ qui vaut 1 si V et W sont isomorphes et 0 sinon d'après le lemme de Schur.

Définition Un caractère irréductible de G est le caractère d'une représentation irréductible de G.

Corollaire Il y a autant de caractères irréductibles de G que de classes d'isomorphismes de G-modules simples.

Preuve. Deux G-modules isomorphes donnent toujours le même caractère irréductibles. Réciproquement si $\chi_V = \chi_W$ avec V et W irréductibles alors $\langle \chi_V, \chi_W \rangle_G = \langle \chi_V, \chi_V \rangle_G = 1 \neq 0$. Ainsi V et W sont isomorphes.

Nombre de simples

Proposition Les caractères irréductibles de G forment une base orthonormée de l'espace vectoriel des fonctions centrales de G dans $\mathbb{C}$.

Preuve. On a vu que les caractères irréductibles formaient une famille orthonormée donc libre de l'espace vectoriels des fonctions centrales. On a donc un nombre fini de représentations simples de G majoré par le nombre de classes de conjugaison de G.
Il s'agit à présent de montrer que si $f : G \to \mathbb{C}$ est une fonction centrale orthogonale à tous les caractères irréductibles alors $f = 0$.
Pour cela, on considère V une représentation de G et on considère l'endomorphisme de V

$$\varphi_V = \frac{1}{|G|} \sum_{g \in G} f(g) \rho_V(g^{-1}) \in \mathrm{End}_{\mathbb{C}}(V)$$

Comme f est une fonction centrale, $\varphi_V \in \mathrm{End}_G(V)$.

Fin de la preuve

On suppose que V est irréductible. Le lemme de Schur dit alors que $\mathrm{End}_G(V)$ est formé des homothéties de V. Ainsi $\varphi_V = \lambda \mathrm{id}_V$ avec $\lambda = \mathrm{tr}\,(\varphi_V)/\dim V$.

Or $\mathrm{tr}\,(\varphi_V) = \dfrac{1}{|G|}\sum_{g\in G} f(g)\mathrm{tr}\,(\rho_V(g^{-1})) = \dfrac{1}{|G|}\sum_{g\in G} f(g)\chi_V(g^{-1})$

Ainsi
$$\mathrm{tr}\,(\varphi_V) = \langle f, \chi_V\rangle_G = 0$$

puisque par hypothèse f est orthogonale à tous les caractères irréductibles.

Finalement, pour tout G-module irréductible V, on a $\varphi_V = 0$.

Comme tout G-module est somme directe de G-modules irréductibles, on a $\varphi_V = 0$ pour tout G-module V. En particulier, si $V = \mathbb{C}G$ est la représentation régulière, on obtient que $\varphi_{\mathbb{C}G} = 0$.

Mais
$$\varphi_{\mathbb{C}G}(1_G) = \frac{1}{|G|}\sum_{g\in G} f(g)\rho_{\mathbb{C}G}(g^{-1})(1_G) = \frac{1}{|G|}\sum_{g\in G} f(g)g^{-1}.$$

Ainsi $f = 0$.

Conséquences

On note $\chi_1, \ldots, \chi_s$ les caractères irréductibles de G et V_i une représentation irréductible de caractère χ_i.

On a s qui est la dimension de l'espace vectoriel des fonctions centrales c'est-à-dire le nombre de classes de conjugaison de G. Si f est une fonction centrale sur G, on a $f = \sum_{i=1}^{s} \langle f, \chi_i \rangle_G \chi_i$ qui donne la décomposition de f dans la base orthonormée des fonctions centrales formée des caractères irréductibles de G.

Soit $V = V_1^{a_1} \oplus \cdots \oplus V_s^{a_s}$ une décomposition de V en somme directe d'irréductibles. On a alors $\chi_V = \sum_{i=1}^{s} a_i \chi_i$ (le caractère d'une somme directe est la somme des caractères). Ainsi, on obtient $a_i = \langle \chi_V, \chi_i \rangle_G$.
Finalement, si $W = V_1^{b_1} \oplus \cdots \oplus V_s^{b_s}$ vérifie $\chi_V = \chi_W$, on obtient alors $a_i = b_i$ et V et W sont bien isomorphes.

Représentation régulière

Proposition Le caractère de la représentation régulière est donné par $\chi_{\mathbb{C}G}(g) = 0$ si $g \neq 1$ et $\chi_{\mathbb{C}G}(1) = |G|$.

On a
$$\mathbb{C}G = {V_1}^{\dim V_1} \oplus \cdots \oplus {V_s}^{\dim V_s}$$

et
$$|G| = \dim {V_1}^2 + \cdots + \dim {V_s}^2.$$

Preuve. En effet, $\chi_{\mathbb{C}G}(g) = |\{g' \in G,\ gg' = g'\}|$.
La multiplicité de V_i dans $\mathbb{C}G$ est donnée par
$\langle \chi_{kG}, \chi_i \rangle_G = \dfrac{1}{|G|} \chi_{\mathbb{C}G}(1)\chi_i(1) = \dim V_i$.

Comment trouver les simples ?

Il est en général difficile de trouver-construire toutes les représentations irréductibles d'un groupe donné. Ainsi pour déterminer les représentations d'un groupe, on commence par déterminer les représentations irréductibles de degré 1. Pour les « groupes de petits cardinal », il manque alors assez peu de représentations irréductibles et quelques raisonnements d'orthogonalité permettent de conclure.

Exemple – Le cas de $\mathfrak{S}_3$. Une représentation de dimension 1 de $\mathfrak{S}_3$ est par définition un morphisme de groupe de $\mathfrak{S}_3 \to \mathbb{C}^\times$. On a donc 2 représentations irréductibles de dimension 1 de $\mathfrak{S}_3$ qui sont la représentation triviale et la signature. Comme on a trois classes de conjugaison dans $\mathfrak{S}_3$, il ne reste plus qu'à déterminer le dernier caractère irréductible χ_V.
Ainsi, on obtient la table de caractère suivante :

	id	Transposition	$3-$cycle
$\mathbf{1}$	1	1	1
ε	1	-1	1
V	a	b	c

Comme $\dim {V_1}^2 + \dim {V_2}^2 + \dim {V_3}^2 = 6$, on obtient que $\chi_V(1) = a = 2$. Comme $\langle \chi_V, \mathbf{1} \rangle_{\mathfrak{S}_3} = \langle \chi_V, \varepsilon \rangle_{\mathfrak{S}_3} = 0$, on obtient $2 + 3 \cdot 1 \cdot b + 2 \cdot 1 \cdot c = 0$ et $2 + 3 \cdot (-1) \cdot b + 2 \cdot 1 \cdot c = 0$ ce qui donne $b = 0$ et $c = -1$.

Groupes commutatifs

Corollaire Soit G un groupe commutatif fini. Alors toutes les représentations irréductibles de G sur $\mathbb{C}$ sont de dimension 1.

Preuve. *Preuve 1.* Soit V une représentation de G sur k. Les éléments de G agissent sur V de façon diagonalisable (ils annulent le polynôme $X^{|G|} - 1$ qui est scindé à racines simples) et commutent deux à deux. Ils sont donc codiagonalisables. Chaque vecteur d'une base de diagonalisabilité commune engendre alors une droite qui est un sous-G-module de V. Ainsi si V est un G-module simple alors V est de dimension 1.
Preuve 2. Le nombre de représentations irréductibles est le nombre de classes de conjugaison qui est donc le nombre d'éléments de G puisque G est commutatif. Or on a $\dim {V_1}^2 + \cdots + \dim V_{|G|}^2 = |G|$ avec $1 \leqslant \dim V_i$. Ainsi $\dim V_i = 1$ pour tout i.

Caractère linéaire

Définition – Caractère linéaire. Soit G un groupe. On appelle caractère linéaire de G à valeurs dans $\mathbb{C}$ un morphisme de groupe $\chi : G \to \mathbb{C}^\times$.

Remarque – Représentation de dimension 1. Si V est un G-module de dimension 1 alors $\mathrm{GL}(V)$ s'identifie canoniquement à $\mathbb{C}^\times$. En effet, l'application

$$\begin{cases} \mathbb{C}^\times \longrightarrow \mathrm{GL}(V) \\ \lambda \longmapsto \lambda \mathrm{id}_V . \end{cases}$$

est un isomorphisme de groupes.

Ainsi toute représentation linéaire de G de dimension 1 détermine un caractère linéaire de G. Inversement, si χ est un caractère linéaire de G, l'action de G sur $\mathbb{C}$ donnée par

$$\begin{cases} G \times \mathbb{C} \longrightarrow \mathbb{C} \\ (g, \lambda) \longmapsto \chi(g)\lambda \end{cases}$$

détermine une structure de G-module sur $\mathbb{C}$ souvent notée $\mathbb{C}_\chi$ Le morphisme de groupes associé est donnée par

Représentation de dimension 1

On vient de voir qu'un caractère linéaire et une représentation de G de dimension 1 c'est la même chose. Prolongeons cette identification

Remarque – Isomorphisme de représentation de dimension 1. Si V et W sont deux G-modules isomorphes de dimension 1 associé respectivement à χ et χ' alors V et W sont G-isomorphes si et seulement si $\chi = \chi'$.
En effet, si $f : V \to W$ est un G-isomorphisme et v une base de V, on a alors

$$\chi(g)f(e_1) = f(\chi(g)e_1) = f(ge_1) = gf(e_1) = \chi'(g)f(e_1).$$

Inversement si $\chi = \chi'$, on considère v une base de V et w une base de W. Vérifions que l'unique application linéaire f de V dans W envoyant v sur w est un G-isomorphisme. Elle est évidemment bijective et $\mathbb{C}$-linéaire. Pour $x \in V$, on a

$$f(gx) = f(\chi(g)x) = \chi(g)f(x) = \chi'(g)f(x) = gf(x).$$

Un premier bilan

Finalement, il y a autant de classe d'isomorphismes de représentations de G de dimension 1 que de caractères linéaires de G.
Par ailleurs, une représentation de dimension 1 est bien sûr simple.
Ainsi, on peut déterminer ainsi un certain nombre de représentations simples de G. Combien ?

Groupe dérivé

Définition – Groupe dérivé. Soit G un groupe. On définit le groupe dérivée de G noté $D(G)$ ou $[G, G]$ comme le sous-groupe engendré par les commutateurs c'est-à-dire les éléments de la forme $ghg^{-1}h^{-1}$ pour $g, h \in G$: on a

$$D(G) = \langle ghg^{-1}h^{-1}, \quad g, h \in G \rangle$$

$D(G)$ est un sous-groupe distingué de G.

Remarque – Groupe dérivé et abélianisé. On a $D(G) = \{1\}$ si et seulement si $ghg^{-1}h^{-1} = 1$ pour tous g, h si et seulement si $gh = hg$ pour tous g, h. Ainsi $D(G) = \{1\}$ si et seulement si G est commutatif.

Remarque – Abélianisé. Le groupe $G^{\mathrm{ab}} := G/D(G)$ est appelé abélianisé de G. C'est un groupe commutatif. En effet, on désigne par $\pi : G \to G/D(G)$ la surjection canonique et si $x = \pi(g)$ et $y = \pi(h)$ sont des éléments de G^{ab}, on a $xyx^{-1}y^{-1} = \pi(ghg^{-1}h^{-1}) = 1$ car $ghg^{-1}h^{-1} \in D(G)$.

P.U. de l'abélianisé

Proposition – Propriété universelle de l'abélianisé. Pour tout groupe abélien A et tout morphisme de groupes $f : G \to A$, il existe un unique morphisme de groupes $\overline{f} : G^{\mathrm{ab}} \to A$ tel que $\overline{f} \circ \pi = f$ où $\pi : G \to G^{\mathrm{ab}}$ est la surjection canonique

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & A \\ G^{\mathrm{ab}} \arrow[ur, dotted, "\overline{f}"] & \end{tikzcd}$$

Preuve. Comme A est abélien, on a $f(ghg^{-1}h^{-1}) = f(g)f(h)f(g)^{-1}f(h)^{-1} = f(g)f(g)^{-1}f(h)f(h)^{-1} = 1$. Ainsi $D(G) \subset \mathrm{Ker}\, f$ et la propriété universelle du quotient donne le résultat.

Compléments

Exercice – Sous-groupe dérivé. En déduire que $D(G)$ est le plus petit sous-groupe H de G tel que G/H est commutatif.
Montrer aussi que tout sous-groupe H de G contenant $D(G)$ est distingué et que le quotient G/H est commutatif. En déduire que G/H est commutatif si et seulement si $D(G) \subset H$.
Soient G, H deux groupes et $f : G \to H$ un morphisme de groupes. Montrer que $f(D(G)) \subset D(H)$. En déduire un morphisme $\overline{f} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.

Exemple – Groupe linéaire et groupe symétrique. Le groupe dérivé de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.
Sauf si $n = 2$ et $k = \mathbb{F}_2$ ou $\mathbb{F}_3$, le groupe dérivé de $\mathrm{GL}(V)$ est $\mathrm{SL}(V)$.

Applications

Application – Caractère linéaire. Soit G un groupe. On note $\pi : G \to G^{\mathrm{ab}}$ la surjection canonique. On note $\widehat{G}$ l'ensemble des caractères linéaires de G à valeurs dans $\mathbb{C}$ et $\widehat{G^{\mathrm{ab}}}$ l'ensemble des caractères linéaires de G^{ab} à valeurs dans $\mathbb{C}$. L'application

$$\begin{cases} \widehat{G^{\mathrm{ab}}} \longrightarrow \widehat{G} \\ \chi \longmapsto \chi \circ \pi \end{cases}$$

est une bijection dont la bijection réciproque est donnée par $\chi \mapsto \overline{\chi}$ ($\mathbb{C}^\times$ est commutatif).

Remarque Si $\chi : G \to k^\times$ et $\chi' : G \to k^\times$ sont deux caractères linéaires, l'application $\chi\chi' : g \mapsto \chi(g)\chi'(g)$ est un caractère linéaire de G (car $k^\times$ est commutatif). On munit ainsi $\widehat{G}$ d'une structure de groupe (sous-groupe des fonctions de G dans $k^\times$). L'élément neutre est le caractère trivial ($\chi(g) = 1$ pour tout g). Et $\chi^{-1} : g \mapsto \chi(g)^{-1} = \chi(g^{-1})$.
La bijection ci-dessus est en fait un isomorphisme de groupes.

Représentations de dimension 1 : bilan

Le nombre de représentations (irréductibles) de dimension 1 de G est le nombre de caractères linéaires de G qui est aussi le nombre de caractères linéaires de G^{ab}. Mais G^{ab} est commutatif et donc toute représentation irréductible est de dimension 1 et donc un caractère linéaire. Ainsi, G^{ab} a autant de caractère linéaire que de classes de conjugaison qui sont réduites à un singleton puisque G^{ab} est commutatif. Finalement le nombre de représentations de dimension 1 de G est $|G^{\mathrm{ab}}| = |G|/|D(G)|$.

Groupe cyclique

La suite des transparents propose une démonstration « élémentaire » (sans faire appel à la théorie des représentations) du fait que pour un groupe abélien fini G, le nombre de caractères linéaires est égal à l'ordre du groupe.
Commençons par le cas d'un groupe cyclique.

Proposition – Groupe cyclique d'ordre n. Soit $n \in \mathbb{N}^*$. Le groupe $\widehat{\mathbb{Z}/n\mathbb{Z}}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Preuve. D'après la propriété universelle de $\mathbb{Z}/n\mathbb{Z}$, se donner un morphisme de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}^\times$ revient à se donner un élément x de $\mathbb{C}^\times$ (l'image de $\overline{1}$) tel que $x^n = 1$ c'est-à-dire une racine du polynôme $X^n - 1 \in \mathbb{C}[X]$.
Or ce polynôme est scindé (puisque $\mathbb{C}$ est algébriquement clos) et à racines simples (puisque $(X^n - 1)' = nX^{n-1}$ a 0 comme unique racine).

Fin de la preuve

Finalement on a une bijection

$$\begin{cases} \widehat{\mathbb{Z}/n\mathbb{Z}} \longrightarrow \{\text{Racines de } X^n - 1\} \\ \quad \chi \quad \longmapsto \chi(\overline{1}) \end{cases}$$

où $\{\text{Racines de } X^n - 1\}$ a exactement n éléments.
Par ailleurs, l'ensemble des racines de $X^n - 1$ forme un sous-groupe de $\mathbb{C}^\times$ qui est d'ordre n et donc fini et cyclique (comme sous-groupe fini du groupe multiplicatif d'un corps). De plus, la bijection ci-dessus est un morphisme de groupes. Ainsi $\widehat{\mathbb{Z}/n\mathbb{Z}}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Application

Exercice Soient G et H deux groupes. Montrer que les applications

$$\begin{cases} \widehat{G \times H} \longrightarrow \widehat{G} \times \widehat{H} \\ \quad \chi \quad \longmapsto (g \mapsto \chi(g,1), h \mapsto \chi(1,h)) \end{cases}$$

et

$$\begin{cases} \widehat{G} \times \widehat{H} \longrightarrow \widehat{G \times H} \\ (\phi, \psi) \longmapsto (g,h) \mapsto \phi(g)\psi(h) \end{cases}$$

sont des isomorphismes de groupes inverses l'un de l'autre.

En utilisant le résultat suivant : tout groupe abélien fini est isomorphe à un produit de groupes cycliques, démontrer que si G est un groupe abélien fini alors $\widehat{G} \simeq G$.
Cela donne une deuxième démonstration du nombre de représentations irréductibles d'un groupe abélien.

Dénombrement

La suite propose une troisième démonstration (élémentaire : qui ne fait pas appel au théorème de classification des groupes abéliens fini) que, lorsque G est un groupe abélien fini, on a l'égalité $|G| = |\widehat{G}|$.

Remarque – Fonctorialité. Soient G et G' deux groupes et $f : G \to G'$ un morphisme de groupes. L'application

$$f^* : \begin{cases} \widehat{G'} \longrightarrow \widehat{G} \\ \chi \longmapsto \chi \circ f \end{cases}$$

est un morphisme de groupes.
De plus, on a ${\mathrm{id}_G}^* = \mathrm{id}_{\widehat{G}}$ et $(f' \circ f)^* = f^* \circ f'^*$ où $f' : G' \to G''$ est un morphisme de groupes.

Caractère linéaire et prolongement

Proposition – Sous-groupe. Soit G un sous-groupe abélien fini et H un sous-groupe (donc distingué) de G. On a donc la suite exacte

$$0 \longrightarrow H \xrightarrow{i} G \xrightarrow{\pi} G/H \longrightarrow 0$$

La suite $$0 \longrightarrow \widehat{G/H} \xrightarrow{\pi^*} \widehat{G} \xrightarrow{i^*} \widehat{H} \longrightarrow 0$$

est alors aussi exacte.

Preuve

La propriété universelle du quotient (pour les groupes) dit précisément que π^* est injective et d'image l'ensemble des caractères linéaires de G triviaux sur H ce qui est précisément le noyau de i^* (puisque i^* est l'application de restriction à H).

Il reste donc à montrer la surjectivité de i^*. Raisonnons par récurrence sur $|G/H|$. Si $|G/H| = 1$, on a $G = H$ et l'application $i^* = \mathrm{id}_{\widehat{G}}$ est évidemment bijective dans ce cas. Considérons à présent H un sous-groupe d'indice $\ell > 1$ et $x \notin H$. Soit j le plus petit entier m (strictement positif tel que) $x^m \in H$ (c'est-à-dire que j est l'ordre de $\pi(x)$ dans G/H).

Montrons alors que tout caractère linéaire de H se prolonge en un caractère linéaire de $\langle H, x\rangle$. Soit $\chi \in \widehat{H}$, comme $\mathbb{C}$ est algébriquement clos, il existe $t \in \mathbb{C}$ tel que $t^j = \chi(x^j)$ ($\chi(x^j)$ admet une racine j^{e}).

Fin de la preuve

On va alors montrer que l'application

$$\chi' : \begin{cases} \langle H, x \rangle & \longrightarrow \mathbb{C}^\times \\ hx^\ell & \longmapsto \chi(h)t^\ell \end{cases}$$

est bien définie et que c'est un caractère linéaire de $\langle H, x \rangle$.
Si elle est bien définie, c'est évidemment un morphisme de groupes.
Il suffit de vérifier qu'elle est bien définie. Si $hx^\ell = h'x^{\ell'}$, on a $hh'^{-1} = x^{\ell'-\ell} \in H$. Ainsi $\ell' - \ell = jn$ et donc $\chi(hh'^{-1}) = \chi(x^{\ell'-\ell}) = \chi(x^j)^n = t^{jn} = t^{\ell'-\ell}$. Et finalement $\chi(h)t^\ell = \chi(h')t^{\ell'}$.
On applique alors l'hypothèse de récurrence au sous-groupe $\langle H, x \rangle$ qui est d'indice strictement plus petit que H et on peut prolonger χ' en un caractère de G. Finalement i^* est bien surjective.

Et lorsque G n'est pas fini

Remarque Dans la proposition précédente, on peut retirer l'hypothèse G fini à l'aide du lemme de Zorn.

En effet, soit $\chi \in \widehat{H}$. On considère l'ensemble X formé des couples (H', χ') où H' est un sous-groupe de G contenant H et $\chi' : H' \to \mathbb{C}^\times$ un morphisme de groupes prolongeant χ.

On munit alors X de l'ordre $(H', \chi') \leqslant (H'', \chi'')$ si $H' \subset H''$ et $\chi''_{|H'} = \chi'$.

On obtient ainsi un ensemble non vide (X contient (H, χ)) et inductif : si (H_t, χ_t) est une famille totalement ordonnée de H alors $\cup_t H_t = H'$ est un sous-groupe de G contenant H et on pose $\chi'(h') = \chi'_t(h')$ si $h' \in H_t$. On définit bien un morphisme de groupes ainsi.

Et lorsque G n'est pas fini

Par le lemme de Zorn, X admet un élément maximal (H', χ'). Montrons que $H' = G$. Supposons qu'il existe $x \in G \smallsetminus H'$. On distingue alors deux cas

- 0 est le seul entier m tel que $x^m \in H'$. On choisit alors $t \in \mathbb{C}^\times$ quelconque.
- Sinon, il existe un plus petit entier $m > 0$ tel que $x^m \in H'$ qu'on appelle j. On choisit alors $t \in \mathbb{C}^\times$ tel que $\chi'(x^j) = t^j$.

Comme précédemment, on montre alors que l'application

$$\chi'' \colon \begin{cases} \langle H, x \rangle & \longrightarrow \mathbb{C}^\times \\ hx^\ell & \longmapsto \chi'(h)t^\ell \end{cases}$$

est bien définie et que c'est un caractère linéaire de $\langle H, x \rangle$ ce qui contredit la maximalité de (H', χ').

Contre-exemples

Remarque – Lorsque G n'est pas abélien. Si G n'est pas abélien et $H \lhd G$ alors i^* n'est pas forcément surjective. Par exemple si $G = \mathfrak{S}_3$ et $H = \mathfrak{A}_3$, le caractère linéaire donnée par $(1,2,3)^\ell \mapsto j^\ell$ (où $j \in \mathbb{C}^\times$ est une racine cubique primitive de l'unité) ne se prolonge pas à $\mathfrak{S}_3$.
Cela résulte du fait que l'application $\bar{i} : H^{\mathrm{ab}} \to G^{\mathrm{ab}}$ n'est pas nécessairement injective.
Démontrer que i^* est surjective si et seulement si $\bar{i}$ est injective.

Remarque L'hypothèse « $\mathbb{C}$ est algébriquement clos » est importante pour extraire une racine j^{e} de l'unité.

Applications

Corollaire Soit G un groupe abélien fini. On a $|G| = |\widehat{G}|$.

Preuve. On raisonne par récurrence sur le cardinal de G. On a vu que le résultat est vrai si G est cyclique. Si G n'est pas cyclique et $1 \neq x \in G$ alors $\{1\} \neq \langle x \rangle \neq G$ est un sous-groupe strict et non trivial de G. Avec $H = \langle x \rangle$, on a alors $|\widehat{G}| = |\widehat{H}||\widehat{G/H}|$ c'est la proposition précédente. Par ailleurs, par hypothèse de récurrence, on a $|H| = |\widehat{H}|$ et $|\widehat{G/H}| = |G/H|$ et donc $|\widehat{G}| = |H||G/H| = |G|$.

Références

1. Jean-Pierre Serre, *Représentations linéaires des groupes finis*
2. William Fulton & Joe Harris, *Representation Theory*
3. Serge Lang, *Algebra*