10.3. **Théorèmes de Mackey.** Soient maintenant deux sous groupes H et K de G et V un kH-module (où k est un corps). Alors on obtient le kG-module $\mathrm{Ind}_H^G V$ par induction et puis le kK-module $\mathrm{Res}_K^G \mathrm{Ind}_H^G V$ par restriction. On peut partiellement décomposer ce kK-module.

Fixons pour le moment un élément $s \in G$. On obtient un sousgroupe $K_s < K$ défini par

$$K_s := K \cap sHs^{-1}.$$

Sur l'espace vectoriel V on a une action par H; nous l'utilisons pour définir une action de K_s sur V par

$$\sigma \cdot v := (s^{-1}\sigma s)v,\ \sigma \in K_s, v \in V.$$

Il y a un sens parce que $s^{-1}\sigma s \in H$. Nous notons V avec cette structure de kK_s-module par V_s.

Proposition 10.1 (Mackey)**.** *Soient $s_1, \ldots, s_r \in G$ des représentants des double-translatés $K\backslash G/H$.*

Alors il y a un isomorphisme de kK-modules

$$\mathrm{Res}_K^G \mathrm{Ind}_H^G V \simeq \bigoplus_{i=1}^{r} \mathrm{Ind}_{K_{s_i}}^K V_{s_i}.$$

Preuve. Fixons $s \in G$ encore. Considérons l'espace de fonctions

$$W_s := \{f : KsH \longrightarrow V;\ \forall x \in KsH, \forall h \in H : f(xh^{-1}) = hf(x)\}.$$

Comme pour les modules d'induction on montre que c'est un espace vectoriel et K agit linéairement sur W_s par

$$(\sigma \cdot f)(x) := f(\sigma^{-1}x),$$

pour $\sigma \in K$, $f \in W_s$ et $x \in KsH$. Montrons que $W_s \simeq \mathrm{Ind}_{K_s}^K V_s$.

Rappelons que

$$\mathrm{Ind}_{K_s}^K V_s = \{f : K \longrightarrow V_s; \forall x \in K, \forall \sigma \in K_s : f(x\sigma^{-1}) = \sigma v\}.$$

Pour $f \in W_s$ définissons $\overline{f} : K \longrightarrow V_s$ par $\overline{f}(x) := f(xs)$, où $x \in K$. Vérifions que $\overline{f} \in \mathrm{Ind}_{K_s}^K V_s$. Soit $\sigma \in K_s$ et $x \in K$ alors

$$\overline{f}(x\sigma^{-1}) = f(x\sigma^{-1}s) = f(xs \cdot s^{-1}\sigma^{-1}s) = s^{-1}\sigma s f(xs) = \sigma \cdot (\overline{f}(x)).$$

L'application $f \mapsto \overline{f}$ est un kK-module homomorphisme:

$$\overline{g \cdot f}(x) = (g \cdot f)(xs) = f(g^{-1}xs) = \overline{f}(g^{-1}x) = (g \cdot \overline{f})(x)$$

pour $g \in K$, $x \in K$. C'est un isomorphisme, son inverse est l'application $f \mapsto \tilde{f}$, où

$$\tilde{f}(xsh) := h^{-1}f(x),$$

où $x \in K$, $h \in H$. Par construction l'application $\tilde{f}$ est dans W_s, et

$$\tilde{\overline{f}}(xsh) = h^{-1}\overline{f}(x) = h^{-1}f(xs) = f(xsh)$$

et

$$\overline{\tilde{f}}(x) = \tilde{f}(xs) = f(x).$$

Sauf possiblement $f \mapsto \tilde{f}$ n'est pas bien définie, parce que'elle dépend des choix. Supposons $xsh = x_1sh_1$, où $x, x_1 \in K$ et $h, h_1 \in H$. Alors $x_1^{-1}x = sh_1h^{-1}s^{-1} \in K \cap sHs^{-1} = K_s$. Mais f a une symétrie par rapport à K_s: $f(x) = f(x_1(x_1^{-1}x)) = (x_1^{-1}x)^{-1}f(x_1)$ pour l'action de K_s sur V_s,

donc $h^{-1}f(x) = h^{-1}s^{-1}(x_1^{-1}x)^{-1}sf(x_1) = h_1^{-1}f(x)$ pour l'action de H sur V. Alors l'application $f \mapsto \tilde{f}$ était bien-définie.

On a une inclusion $W_s \longrightarrow \mathrm{Res}_K^G \mathrm{Ind}_H^G V$ de kH-modules si on étend une application $f : KsH \longrightarrow V$ vers une fonction $f : G \longrightarrow V$ où on définit $f(x) = 0$ si $x \notin KsH$. Si Ks_1H et Ks_2H sont disjoints, alors $W_{s_1} \cap W_{s_2} = \{0\}$. De l'autre côté chaque $f : G \longrightarrow V$ est uniquement déterminée par ses restrictions sur tous les double-translatés KsH.

Si $s_1, \ldots, s_r \in G$ sont des représentants des double-translatés $K\backslash G/H$ on obtient une bijection $\oplus_{i=1}^r W_{s_i} \simeq \mathrm{Res}_K^G \mathrm{Ind}_H^G V$. Et la preuve est complète. □

On obtient le critère d'irréductibilité de Mackey, en prenant $K = H$.

Corollaire 10.3. *Soit H un sous-groupe du groupe fini G et V un $\mathbb{C}H$-module.*

Alors $\mathrm{Ind}_H^G V$ est un $\mathbb{C}G$-module simple si et seulement si

(i) V est simple comme $\mathbb{C}H$-module, et

(ii) Pour chaque $s \in G\backslash H$ les deux $\mathbb{C}H_s$-modules V_s (défini plus haut) et $\mathrm{Res}_{H_s}^H V$ sont disjoint (c-à-d, il n'existe pas un $\mathbb{C}H_s$-module simple qui apparaît dans ces deux $\mathbb{C}H_s$-modules).

Preuve. On utilise la réciprocité de Frobenius plusieurs fois. Soient $s_1, \ldots, s_r$ des représentants des double-translatés $H\backslash G/H$, en supposant que $s_1 = \mathbf{1}$. Nous avons $H_{s_1} = H$, et donc $V = V_{s_1} = \mathrm{Res}_H^H V$.

$$(\mathrm{Ind}_H^G \chi_V, \mathrm{Ind}_H^G \chi_V)_G = (\mathrm{Res}_H^G \mathrm{Ind}_H^G \chi_V, \chi_V)_H = \sum_i (\mathrm{Ind}_{H_{s_i}}^H \chi_{V_{s_i}}, \chi_V)_H =$$

$$= (\chi_V, \chi_V)_H + \sum_{i>1} (\chi_{V_{s_i}}, \mathrm{Res}_{H_s}^H \chi_V)_{H_s}$$

Il suit que $\mathrm{Ind}_H^G V$ est simple $\iff$ $(\mathrm{Ind}_H^G \chi_V, \mathrm{Ind}_H^G \chi_V)_G = 1$ $\iff$ $(\chi_V, \chi_V)_H = 1$ et pour chaque $i > 1$: $(\chi_{V_{s_i}}, \mathrm{Res}_{H_s}^H \chi_V) = 0$. Et on obtient le résultat voulu. □

Si V est un kH-module, $H \lhd G$, alors pour chaque $s \in G$ on obtient un kH-module V_s, *son module conjugué*, par $g \cdot v := sgs^{-1}v$.

Corollaire 10.4. *Soit $H \lhd G$ un sous-groupe normal du groupe fini G et V un $\mathbb{C}H$-module.*

Alors $\mathrm{Ind}_H^G V$ est un $\mathbb{C}G$-module simple si et seulement si

(i) V est simple comme $\mathbb{C}H$-module, et

(ii) Pour chaque $s \in G\backslash H$ le module conjugué V_s n'est pas isomorphe à V.

Exemple 10.4. Considérons $\mathrm{Alt}_5 \lhd S_5$. Ils existent deux représentations simples complexes pour Alt_5 de degré 3, disons χ_2 (avec $\mathbb{C}\,\mathrm{Alt}_5$-module V) et χ_3. Soit $g_1 = (1,2,3,4,5)$ et $g_2 = (2,1,3,4,5) = (12)g_1(12)^{-1}$, alors g_1 et g_2 ne sont pas conjugués dans Alt_5. On a $\chi_2(g_2) = \chi_3(g_1) \neq \chi_2(g_1)$, donc $V_{(12)}$ n'est pas isomorphe à V (mais à l'autre $\mathbb{C}\,\mathrm{Alt}_5$-module de dimension 3). Alors $\mathrm{Ind}_{\mathrm{Alt}_5}^{S_5} V$ est un $\mathbb{C}S_n$-module simple de dimension 6.

11. Entiers algébriques

On rappelle que $a \in \mathbb{C}$ est un *entier algébrique* s'il existe un polynôme unitaire

$$f(T) = T^n + m_1 T^{n-1} + \ldots + m_{n-1}T + m_n$$

avec coefficients $m_i \in \mathbb{Z}$ tel que $f(a) = 0$.

Nous avons le critère suivant pour les entiers algébriques, une conséquence du théorème de Cayley-Hamilton de l'algèbre linéaire.

Proposition 11.1. *Soit $a \in \mathbb{C}$. Alors a est un entier algébrique si et seulement si il existe un sous-anneau $A \subset \mathbb{C}$ de rang fini sur $\mathbb{Z}$, tel que $a \in A$.*

Preuve. Si a est une racine du polynôme $T^n + m_1 T^{n-1} + \ldots + m_{n-1}T + m_n \in \mathbb{Z}[T]$, alors $a^n = -m_1 a^{n-1} - \ldots - m_{n-1}a - m_n$ et donc le $\mathbb{Z}$-module A engendré par $1, a, \ldots, a^{n-1}$ est un sous-anneau de $\mathbb{C}$ de rang $n < \infty$ sur $\mathbb{Z}$.

Par contre, soit $A \subset \mathbb{C}$ un sous-anneau qui a rang $n < \infty$ sur $\mathbb{Z}$ et $a \in A$. Alors il existe une $\mathbb{Z}$-base $x_1, \ldots, x_n$ de A. Il existe une matrice $M = (m_{ij})$ d'entiers telle que

$$ax_j = \sum_{i=1}^{n} m_{ij} x_i.$$

La puissance M^i correspond à a^i. Soit $f(T) = \chi_M(T) = \det(T\mathbf{1} - M)$ le polynôme caractéristique de la matrice M. C'est un polynôme unitaire de degré n dans $\mathbb{Z}[T]$, car le coefficient de la matrice sont entiers. Par le théorème de Cayley-Hamilton $f(M) = 0$. Donc aussi $f(a)$ correspond à la matrice 0, donc $f(a) = 0$. Et donc a est un entier algébrique. □

Exemple 11.1. Les exemples les plus importants dans la théorie de la représentation sont les suivants. Les entiers algébriques contenus dans $\mathbb{Q}$ sont les entiers ordinaires, c.-à-d.les éléments de $\mathbb{Z}$.

Preuve. Soit $a = \frac{r}{s}$ une fraction qui est aussi un entier algébrique avec polynôme $T^n + m_1 T^{n-1} + \ldots + m_{n-1}T + m_n \in \mathbb{Z}[T]$. On peut supposer que r et s sont relativement premiers. Supposons $a \notin \mathbb{Z}$, c.-à-d., $s \neq \pm 1$. En substituant a et en multipliant par s^n on obtient

$$r^n + m_1 r^{n-1} s + \ldots + m_{n-1} r s^{n-1} + m_n s^n = 0$$

et il suit que s divise r^n. Contradiction. Donc $a \in \mathbb{Z}$. □

Soit $n \in \mathbb{N}$. Définissons le nombre complexe $\epsilon_n = e^{2\pi i/n} \in \mathbb{C}$; c'est une solution de l'équation $T^n - 1 = 0$, donc ϵ est un entier algébrique. Les entiers algébriques contenus dans le corps $\mathbb{Q}(\epsilon_n)$ (le plus petit sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ et ϵ_n) forment le sous-anneau $\mathbb{Z}[\epsilon_n] = \mathbb{Z} + \mathbb{Z}\epsilon_n + \mathbb{Z}\epsilon_n^2 + \ldots + \mathbb{Z}\epsilon_n^{n-1}$ engendré par ϵ_n; $\mathbb{Z}[\epsilon_n]$ est de rang $\leq n$ sur $\mathbb{Z}$. Le groupe multiplicatif $\Gamma_n = (\mathbb{Z}/n\mathbb{Z})^\times$ agit sur $\mathbb{Q}(\epsilon)$ $\mathbb{Q}$-linéaire par

$$(m + n\mathbb{Z}) \bullet \sum_i q_i \epsilon^i := \sum_i q_i \epsilon^{mi},$$

où $q_i \in \mathbb{Q}$. On a $\mathbb{Q}(\epsilon_n)^{\Gamma_n} = \mathbb{Q}$ et $\mathbb{Z}[\epsilon_n]^{\Gamma_n} = \mathbb{Z}$.

Preuve. Soit $\Phi_n(T) := \prod_{\overline{m} \in \Gamma_n} (T - \epsilon_n^m)$. Alors par exemple $\Phi_1(T) = T - 1$, $\Phi_2(T) = T + 1$, $\Phi_3(T) = T^2 + T + 1$, $\Phi_4(T) = T^2 + 1$. On a $\prod_{d|n} \Phi_d(T) = T^n - 1$. On utilise cet identité pour montrer par induction que chaque $\Phi_d(T)$ est unitaire, dans $\mathbb{Z}[T]$ et irréductible (cf. [3, §13.6]).

Il suit que $\mathbb{Q}(\epsilon_n) \simeq \mathbb{Q}[T]/(\Phi_n(T)$ et aussi que $\sum_{\overline{m} \in \Gamma_n} \epsilon_n^m \in \mathbb{Z}$.

Soit $\alpha = \sum_i q_i \epsilon^i \in \mathbb{Q}(\epsilon)^{\Gamma_n}$, où $g_i \in \mathbb{Q}$. Alors

$$\alpha = \frac{1}{|\Gamma_n|} \sum_{\overline{m} \in \Gamma_n} \sum_i q_i \epsilon_n^m = \sum_i q_i \left(\frac{1}{|\Gamma_n|} \sum_{\overline{m} \in \Gamma_n} \epsilon_n^m \right) \in \mathbb{Q}.$$

Alors $\mathbb{Q}(\epsilon_n)^{\Gamma_n} = \mathbb{Q}$ et aussi $\mathbb{Z}[\epsilon_n]^{\Gamma_n} = \mathbb{Z}$.

Un élément général de $\mathbb{Q}(\epsilon)$ s'écrit uniquement comme

$$a = \frac{r_0 + r_1\epsilon_n + r_2\epsilon^2 + \ldots + r_{\phi(n)-1}\epsilon^{\phi(n)-1}}{s},$$

où les r_i et s sont entiers et $\phi(n) := |\Gamma_n|$. Supposons a est un entier algébrique et $a \notin \mathbb{Z}[\epsilon]$, c.-à-d., s ne divise pas tous les coefficients r_i. Comme avant, en substituant $a = \frac{r}{s}$ dans son polynôme d'intégrité et en multipliant par s^n on obtient

$$r^n + m_1 r^{n-1}s + \ldots + m_{n-1}rs^{n-1} + m_n s^n = 0$$

et il suit que s divise r^n. Contradiction. Donc $a \in \mathbb{Z}[\epsilon]$. □

Maintenant nous commençons à donner des applications dans la théorie des représentations.

Proposition 11.2. *Soit $\rho : G \longrightarrow \mathrm{GL}(d, \mathbb{C})$ une représentation complexe d'un groupe fini avec le caractère $\chi : G \longrightarrow \mathbb{C}$. Soit $g \in G$ d'ordre n et posons $\epsilon_n = e^{2\pi i/n} \in \mathbb{C}$. Alors $\chi(g) \in \mathbb{Z}[\epsilon_n]$.*

Si pour chaque $m \in \mathbb{Z}$ relativement premier avec n on a que g^m est conjugué à g, alors on a même que $\chi(g) \in \mathbb{Z}$.

Preuve. On peut diagonaliser la matrice $\rho(g)$ d'ordre fini. Les coefficients sur le diagonal sont tous de la forme $\epsilon_n^{r_i}$, pour certaines r_i, $1 \leq i \leq N$. Donc la trace est $\sum_i \epsilon_n^{r_i} \in \mathbb{Z}[\epsilon_n]$.

Si m est relativement premier avec n, alors $\chi(g^m) = \sum_i \epsilon^{mr_i} = \chi(g)$, donc $\chi(g) \in \mathbb{Z}[\epsilon]^{\Gamma_n} = \mathbb{Z}$, par l'exemple précédent. □

Proposition 11.3. *Soit $\chi : G \longrightarrow \mathbb{C}$ un caractère simple et $C(g)$ la classe de conjugaison de g. Alors $\frac{|C(g)|\chi(g)}{\chi(\mathbf{1}_G)}$ est un entier algébrique.*

Preuve. Soient $C_1, \ldots, C_c$ les classes de conjugaison, et $[C_i] = \sum_{g \in C_i}[g] \in \mathbb{C}G$. Choisissons des représentants $c_i \in C_i$. Alors $[C_i][C_j] = \sum_r a_{ijr}[C_r]$, où $a_{ijr} = |\{x \in C_i, y \in C_j; xy = c_r\}|$. Donc $\sum_i \mathbb{Z}[C_i]$ est un sous-anneau du centre de $\mathbb{C}G$ de rang fini. Fixons maintenant une représentation simple ρ de caractère χ. Alors par le lemme de Schur $\rho(c)$ est scalaire, pour chaque c dans le centre de $\mathbb{C}G$, disons $a(c)\,\mathrm{Id}$. Par restriction, $\sum_i \mathbb{Z}[C_i] \longrightarrow \mathbb{C} : c \mapsto a(c)$ est un homomorphisme d'anneau. L'image est donc un sous-anneau de $\mathbb{C}$ de rang fini sur $\mathbb{Z}$. Alors par le critère de prop. 11.1, chaque image est un entier algébrique. En particulier, $a([C_i])$ est un entier algébrique. On calcule $a([C_i]) = \chi([C_i])/\chi(\mathbf{1}_G) = |C_i|\chi(c_i)/\chi(\mathbf{1}_G)$ et on conclut. □

Proposition 11.4. *La dimension de chaque représentation simple complexe divise l'ordre du groupe.*

Preuve. Soit χ un tel caractère simple. On a

$$\frac{|G|}{\chi(1)} = \frac{|G|}{\chi(1)} < \chi, \chi >= \frac{1}{\chi(1)} \sum_{i=1}^{c} |C_i|\chi(c_i)\chi(c_i^{-1}) = \sum_{i=1}^{c} \frac{|C_i|\chi(c_i)}{\chi(1)}\chi(c_i^{-1})$$

est un entier algébrique inclu dans $\mathbb{Q}$, donc est un entier ordinaire. Alors $\chi(1)$ divise $|G|$ dans $\mathbb{Z}$. □

11.1. **Le théorème p^aq^b de Burnside.** Une des premières applications importantes de la théorie des caractères était le théorème de Burnside disant que chaque groupe d'ordre p^aq^b, où p, q premiers, est résoluble. Dans la preuve le prochain résultat est utilisé.

Soit $\rho : G \longrightarrow \mathrm{GL}(V)$ une représentation simple complexe. Le centre de ρ, noté $Z(\rho)$ est par définition $Z(\rho) := \rho^{-1}(Z(\mathrm{GL}(V)))$, c-à-d, les $g \in G$ qui sont envoyé sur une matrice scalaire. Donc $Z(\rho) \lhd G$.

Proposition 11.5 (Burnside)**.** *Soit ρ une représentation simple d'un groupe fini G avec caractère χ et $g \in G$. Supposons que* $\mathrm{pgcd}(\chi(1), |C(g)|) = 1$. *Alors $g \notin Z(\rho)$ si et seulement si $\chi(g) = 0$.*

Preuve. Par l'hypothèse ils existent deux entiers $a, b \in \mathbb{Z}$ tels que $a\chi(1) + b|C(g)| = 1$. Donc par prop. 11.3

$$\frac{b|C(g)|\chi(g)}{\chi(1)} = \frac{(1 - a\chi(1))\chi(g)}{\chi(1)} = \frac{\chi(g)}{\chi(1)} - a\chi(g)$$

est un entier algébrique, et donc aussi $\alpha := \frac{\chi(g)}{\chi(1)}$ est un entier algébrique.

Soit $n = O(g)$, l'ordre de g. Posons $\epsilon := e^{2\pi i/n} \in \mathbb{C}$. L'extension de corps $\mathbb{Q} \subset \mathbb{Q}(\epsilon)$ a $\Gamma_n = (\mathbb{Z}/n\mathbb{Z})^\times$ comme groupe de Galois. L'automorphisme $\gamma = \overline{m}$ (m est relativement premier avec n) est induite par $\gamma(\epsilon) = \epsilon^m$. Le nombre $\gamma(\alpha)$ est aussi un entier algébrique, et si $\alpha \neq 0$ alors aussi $\gamma(\alpha) \neq 0$. Le produit $N(\alpha) := \prod_{\gamma \in \Gamma} \gamma(\alpha)$ est Γ-invariant, donc $N(\alpha) \in \mathbb{Q}(\epsilon)_n^\Gamma = \mathbb{Q}$ et $N(\alpha)$ est un entier algébrique. Donc $N(\alpha) \in \mathbb{Z}$.

Supposons que $g \in Z(\rho)$, alors par Schur il existe un $c \in \mathbb{C}$, $|c| = 1$, tel que $\rho(g) = c\mathbf{1}$, donc $|\chi(g)| = |c|\chi(1) = \chi(1) \neq 0$.

Par contre si $g \notin Z(\rho)$ alors par l'inégalité du triangle on a $|\chi(g)| < \chi(1)$, donc $|\alpha| < 1$. Pour chaque $\gamma \in \Gamma$ on a aussi $|\gamma(\alpha)| < 1$ et donc $|N(\alpha)| < 1$. Mais $N(\alpha) \in \mathbb{Z}$, donc $N(\alpha) = 0$. Alors $\alpha = 0$ et $\chi(g) = 0$. □

Corollaire 11.1. *Soit G un groupe simple et non-abélien. Supposons $|C(g)| = p^r$ pour un $g \in G$ et un nombre premier p. Alors $g = \mathbf{1}$.*

Preuve. Supposons $g \neq \mathbf{1}$. Soit ρ une représentation simple non-triviale avec caractère χ. Le sous-groupe $Z(\rho)$ est normal dans G, donc $Z(\rho) = \{\mathbf{1}\}$ ou $Z(\rho) = G$, parce que G est simple. Mais si $Z(\rho) = G$, nécessairement $\chi(1) = 1$ et on obtient un homomorphisme non-triviale $G \longrightarrow \mathbb{C}^\times$, injectif parce que G est simple. Donc G est abélien; contradiction avec l'autre hypothèse. Donc $g \notin Z(\rho)$. Par prop. 11.5 si p ne divise pas $\chi(1)$ alors $\chi(g) = 0$. On applique une relation d'orthogonalité du tableau de caractères simples:

$$0 = \sum_{\chi \text{ irr.}} \chi(1)\chi(g) = 1 + \sum_{\chi \text{ irr.; } p|\chi(1)} \chi(1)\chi(g)$$

Alors

$$\frac{-1}{p} = \sum_{\chi \text{ irr.; } p|\chi(1)} \frac{\chi(1)}{p}\chi(g)$$

est un entier algébrique et donc dans $\mathbb{Z}$. Une contradiction. Alors $g = \mathbf{1}$. □

Théorème 11.1 (Burnside)**.** *Supposons $|G| = p^aq^b$, où p, q premier. Alors G est résoluble.*

Preuve. On va utiliser induction sur l'ordre du groupe et on peut supposer que G n'est pas trivial. Soit $N \lhd G$ un sous-groupe normal propre maximal de G. Si $N \neq \{\mathbf{1}\}$ alors par induction N et G/N sont résolubles, donc aussi G est résoluble.

Supposons donc que $N = \{\mathbf{1}\}$, c-à-d, G est un groupe simple. Soit P un p-Sylow sous-groupe de G. Le centre de chaque p-groupe contient un élément non-trivial. Soit g un élément non-trivial dans le centre de P, alors son centralisateur contient P et donc $C(g) = q^c$ pour un certain $c \leq b$. Par le corollaire il suit que G est simple et abélien, donc résoluble. □

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA