Théorie des charactères

Soit $\mathbb{C}$ le corps de nombres complexes et G un groupe
Une représentation de G sur $\mathbb{C}$ de dimension n est un morphisme

$$\rho : G \longrightarrow Gl_n(\mathbb{C}).$$

Le caractère de la representation ρ évalué à $g \in G$ est la trace de la matrice $\rho(g)$.

On dit que deux représentations ρ et ρ' sont <u>équivalentes</u> si il existe une matrice $A \in Gl_n(\mathbb{C})$ telle que $A\rho(g)A^{-1} = \rho(g^{-1})$, $\forall g \in G$.

<u>Lemme</u> :

1) Deux representations équivalentes ont les mêmes caractères
2) Un caractère est constant sur les classes de conjugaison de G.

<u>Preuve</u>

Un fait très important est que $tr(A \circ B) = tr(B \circ A)$
Donc $tr(A \cdot B \cdot A^{-1}) = tr(AA^{-1}B) = tr(B)$.

Il est maintenant claire que si $A\rho(g)A^{-1} = \rho'(g)$ alors $tr(\rho(g)) = tr(\rho'(g))$.

De plus $tr(\rho(xgx^{-1})) = tr(\rho(x)\rho(g)g(x)^{-1}) = tr(\rho(g))$

Lemme Si χ est un caractère de G alors $\chi(g)$ est somme des $|G|^{\text{ème}}$ racines de l'unité, $\forall g \in G$.

Preuve Soit ρ une représentation linéaire de G et $A = \rho(g)$. Si λ est une valeur propre de $A \in G$ alors $A v = \lambda v$, où v est un vecteur propre associé à λ.
Donc $A^n v = \lambda^n v$. Mais $A^n = \rho(g)^n = \rho(g^n)$.
Si $n = |G|$ alors $g^n = 1$, donc $\lambda^n v = v$, donc $\lambda^n = 1$.
Ceci entraine que λ est une racine $n^{\text{ème}}$ de l'unité.

Maintenant $\rho(g)$ est conjugué à sa forme de Jordan (car $\mathbb{C}$ est algébriquement clos), donc $\chi(g) = tr(\rho(g))$ est la somme des valeurs propres de $\chi(g)$, comptées avec leur multiplicités.

Corollaire Soit χ le caractère d'une représentation ρ de degré n de G et soit $g \in G$. Alors on a :

1) $|\chi(g)| \leq n$
2) $|\chi(g)| = n$ si et seulement si $\rho(g)$ est une matrice scalaire.
3) $\chi(g) = n$ si et seulement si $\rho(g) = I_n$, la matrice identité.

Preuve

Par le théorème précédant on a que
$$\chi(g) = \sum_{i=1}^{n} \lambda_i \quad \text{avec } \lambda_i \text{ racine } |G|\text{-ème de l'unité.}$$
Par l'inégalité du triangle, on obtient $|\chi(g)| = \sum_{i=1}^{n} |\lambda_i| \leq n$

Donc (1) est vérifié. Si la matrice $\rho(g)$ est scalaire alors $\lambda_i = \lambda, \forall i$. Si $\lambda_i = \lambda, \forall i$ alors $|\chi(g)| = |n\lambda| = n$. Réciproquement, si $|\chi(g)| = n$ alors $\lambda_i = \lambda, \forall i$. On en déduit que le polynôme caractéristique de $\rho(g)$ est $(X-\lambda)^n$. D'autre part, $g^m = 1$ pour $m = |G|$, donc $\rho(g)$ satisfait aussi la relation $(\rho(g))^m - 1 = 0$. Comme le diviseur commun de $X^m - 1$ est $(X-\lambda)^n$ est $X-\lambda$, il en résulte que $\rho(g)$ est aussi racine de $X-\lambda$. Donc $\rho(g) = \lambda I_n$ est une matrice scalaire. Donc (2) est vérifié. Pour (3) on procède comme pour (2) avec la precision que $\chi(g) = \sum_{i=1}^{n} \lambda_i = n$ est équivalent à $\lambda_i = 1, \forall i$.

<u>Lemme</u> Soit χ un caractère de G alors le sous-groupe

$$H := \{ g \in G \mid \chi(g) = \chi(1) \}$$

est un sous-groupe normal de G.

<u>Preuve</u>

Démontrons premièrement que H est un sous-groupe de G. On a $\chi(g) = \chi(1) = n$. Donc $g \in H$ si et seulement si $\chi(g) = n$. Par le corollaire précédent, ceci est equivalent a demander que $\rho(g) = I_n$. Donc $H = \operatorname{Ker} \rho$, qui est un sous-groupe normal de G.

<u>Définition</u> 1) Soit ρ une représentation de G sur $\mathbb{C}$. On dit que ρ est <u>irréductible</u> s'il n'y a pas de sous-espace propre nontrivial V de $\mathbb{C}^n$ tel que $\rho(g) V \subseteq V, \forall g \in G$.

On dit que ρ est *fidèle* si $\operatorname{Ker}\rho \neq 1$. On dit que ρ est *linéaire* si sa dimension est 1.
Soit χ le caractère de ρ. On dit que χ est *irréductible*, *fidèle*, respectivement, *linéaire* si ρ est irréductible, fidèle, respectivement, linéaire

Remarque

1) Un caractère linéaire est irréductible et de dimension 1 (i.e. $\chi(1) = 1$).
2) Le seuls caractères irréductibles d'un groupe abélien sont les caractères linéaires. Ceci relève de la décomposition des lemmes suivantes.

Lemme: Soit ρ une représentation irréductible de G. Soit $z \in Z(G)$ et λ une valeur propre de $\rho(z)$. Alors $\rho(z) = \lambda I_n$. En particulier, si ρ est fidèle, alors, ou bien $z = 1$, ou $\lambda \neq 1$.

Preuve: Soit $W = \{ w \in \mathbb{C}^n \mid \rho(z) w = \lambda w \}$. Par supposition $W \neq \phi$. De plus, pour tout $g \in G$. et $w \in W$ on a $\rho(z)(\rho(x) w) = \rho(zx) w = \rho(xz) w =$
$= \rho(x)(\rho(z) w) = \lambda \rho(x) w$; donc $\rho(x) w \in W$ et W est $\rho(G)$-invariant. Comme ρ est irréductible on a $W = \mathbb{C}^n$. Si ρ est fidèle $\operatorname{Ker}\rho = 1$ donc, si $z \neq 1$ il faut que $\lambda \neq 1$.

Lemme Si ρ est fidèle, irréductible, alors $Z(G)$ est cyclique.

Preuve Par le lemme précédant, pour tout $z \in Z(G)$ $\rho(z) = \lambda_z \cdot I_n$. De plus, comme ρ est fidèle le morphisme
$$\begin{aligned} Z(G) &\longrightarrow \mathbb{C}^\times \\ z &\longmapsto \lambda_z \end{aligned}$$
est injectif.

Donc $Z(G)$ est isomorphe à un sous-groupe du groupe des racines $|G|$-èmes de l'unité, donc il est cyclique.

Lemme Si ρ est une représentation irréductible d'un groupe abélien G, alors $G/\ker\rho$ est cyclique.
En particulier, toute representation irreductible d'un groupe abelien est linéaire, et il n'y a pas des représentations fidèles irréductibles des groupes non-cycliques.

Preuve Soit $K = \ker\rho$. On a que ρ induit une représentation irréductible, fidèle de G/K. Mais $Z(G/K) = G/K$ car G est abélien, donc G/K est cyclique par le lemme précédant.

On choisit $x \in G$, tel que xK est un générateur de G/K, qui est un groupe cyclique. Soit v un vecteur propre pour $\rho(x)$. Donc $\rho(x)v = \lambda v$ et $\rho(x^m)v = \lambda^m v$. Ainsi $\rho(G)\langle v\rangle \subseteq \langle v\rangle$, donc $\langle v\rangle$ le sous-espace engendré par v est $\rho(G)$-invariant. Comme ρ est irréductible, on obtient que $\langle v\rangle = \mathbb{C}^n$, donc $n=1$.

Comme réciproque partielle on a le résultat suivant:

Lemme Si ρ est une représentation linéaire de G alors $G/\ker\rho$ est cyclique. En particulier, un groupe non-cyclique ne possède pas de représentation linéaire fidèle.

Preuve Pour un $v \in \mathbb{C}\setminus\{0\}$, on a $\rho(x)v = \lambda_x v$; en particulier, l'application $x \longmapsto \lambda_x$ est un monomorphisme de G dans $\mathbb{C}^\times$, donc $G/\ker\rho$ est cyclique.

Fait (accepté sans preuve)

Soit G un groupe, r le nombre de classes de conjugaison. Alors il existe r représentations de G irréductibles, 2-à-2 non-équivalentes ρ_i de degré n_i. De plus, on a :

1) $\rho = \sum n_i \rho_i$, où ρ est la représentation régulière de G.

2) $\sum n_i^2 = |G|$.

3) $\{\rho_i\}$ est une base de l'espace des fonctions de classe.

Corollaire

Soit χ_i le caractère associé avec ρ_i, $1 \leq i \leq r$.

Alors :

1) $\displaystyle\sum_{i=1}^{r} n_i \chi_i(g) = \begin{cases} 0 & \text{si } g \neq 1 \\ |G| & \text{si } g = 1 \end{cases}$

2) $\displaystyle\sum_{g\in G} \chi_i(g) = \begin{cases} 0 & \text{si } i > 1 \\ |G| & \text{si } i = 1 \end{cases}$

Preuve

1) est immédiat car $\sum_i n_i\rho_i = \rho$ et $tr(\rho(g)) = \begin{cases} 0 & g \neq 1 \\ |G| & g = 1 \end{cases}$

2) Soit $u = \sum_{g\in G} g$. Alors $\sum_{g\in G} \chi_i(g) = tr(\sum \rho_i(g)) = tr(\lambda I_n)$

la dernière égalité vient du fait que $\rho_i(u)$ commute avec $\rho_i(g)\ \forall g \in G$. mais $\exists\, g$ t.q. $\chi_i(g) \neq I_n$ De plus $\chi_i(u)\chi_i(g) = \chi_i(ug) = \chi_i(u)$. Donc $\chi_i(u)(\chi_i(g) - I_n) = 0$. Ainsi $\lambda\cdot(\chi_i(g) - I_n) = 0$ implique $\lambda = 0$ $\square$

Théorème

Soit $\varphi : G \to Mat_n(\mathbb{C})$ une représentation de G sur $\mathbb{C}$. Considérons l'ensemble de matrices $\mathcal{X} = \{A \mid \varphi(g)A = A\varphi(g) \ \forall g \in G\}$.

1) Alors $\mathcal{X}$ est un espace vectoriel de dim finie.

2) Supposons que φ est irréductible. Alors toute matrice non-nulle de $\mathcal{X}$ est inversible.

3) La dimension de $\mathcal{X}$ sur $\mathbb{C}$ est 1. En particulier, toutes les matrices dans $\mathcal{X}$ sont scalaires.

4) $\langle \varphi(g) \mid g \in G \rangle = Mat_n(\mathbb{C})$.

Preuve

1) $\lambda A + \mu B$ satisfont les mêmes propriétés. Il est clair que $\mathcal{X}$ a dimension finie.

2) Soit $A \in \mathcal{X}$. On veut démontrer que $\dim(A \cdot \mathbb{C}^n) = n$, ce qui entraînerait que A est inversible.

Soit $A \cdot \mathbb{C}^n = V$. Mais alors, $\forall v \in V$.
$\varphi(g)v = \varphi(g)A \cdot w = A\varphi(g)\underline{w} \in V$, $\forall g \in G$.
Donc V est un sous-espace invariant et, comme φ est irréductible, on a $V = \mathbb{C}^n$

3) $\mathcal{X}$ est de dimension finie. De plus, si $A, B \in \mathcal{X}$ alors $A \cdot B \in \mathcal{X}$. Donc, il existe n, t.q. $I, A, A^2, \dots, A^n$ soit linéairement dépendantes. Donc A sera racine de $X^m + a_1 X^{m-1} + \dots + a_m$ avec $a_i \in \mathbb{C}$, $\forall i$. Comme $\mathbb{C}$ est alg. clos, ce polynôme admet des racines $\alpha_1, \alpha_2, \dots, \alpha_m \in \mathbb{C}$.

$(A - \alpha_1 I_n) \cdots (A - \alpha_m I_n) = 0$

Mais $A - \alpha_i I_n \in \mathcal{X}$, donc elles sont zéro ou inversibles. Donc $\exists \alpha$, tel que $A = \alpha I_n$

4) Soit W un sous-espace propre de $\mathbb{C}^n$ et $w \in \mathbb{C}^n \setminus W$.
Il suffit de voir que il existe $A \in \mathcal{Y} = \langle \varphi(g) | g \in G \rangle$
tel que $A \cdot W = 0$ mais $A \cdot w \neq 0$. (*)

Ceci nous aide à construire recursivement une matrice dans $\mathcal{Y}$ pour toute transformation linéaire de plan : Considérons, par exemple, $\{w_1, \dots, w_n\}$ une base de $\mathbb{C}^n$ et $v_1, \dots, v_n$ arbitraires. On veut construire $B \in \mathcal{Y}$ tel que $B(w_i) = v_i \ \forall i$.

- Premièrement on voit qu'on peut trouver $B' \in \mathcal{Y}$ t.q. $B' \cdot W = 0$ et $B' \cdot w = v$.
En effet, $\langle \varphi(g) A w \mid g \in G \rangle$ est un sous espace invariant, donc $\langle \varphi(g) A w \mid g \in G \rangle = \mathbb{C}^n$
Donc $\exists\, B' \in \mathcal{Y}$, t.q. $B'A w = v$
Maintenant on applique ceci pour $w = w_i$, $v = v_i$ et $W = W_i = \langle w_j \mid j \neq i \rangle$, $w_i \in \mathbb{C}^n \setminus W_i$. Donc,
$\exists\, B_i$ t.q. $B_i \cdot W_i = 0$, $B_i \cdot w_i = v_i$
Ainsi, $\left(\sum B_i\right) w_j = B_j w_j = v_j$. On pose $B = \sum_i B_i$.

- Demontrons maintenant (*)
Par induction sur $\dim_{\mathbb{C}}(W)$. Si $W = \{0\}$, alors on prend $A = I_n$
Sinon, on ecrit $W = U + \mathbb{C}u$, $\dim_{\mathbb{C}} U = \dim_{\mathbb{C}} W - 1$
Par induction $\exists\, A_1$ t.q. $A_1 U = 0$, $A_1 u \neq 0$.
Soit $N(U) := \{A \in \mathcal{Y} \mid A \cdot U = 0\}$. Alors, $N(U)u$ est un sous-espace invariant, donc $N(U)u = V$, car, par recurrence, $N(U)u \neq \{0\}$. Soit $w \in \mathbb{C}^n \setminus W$ et supp. $C w = 0$, $\forall C \in \mathcal{Y}$ $C \cdot W = 0$

- Définissons $T : \mathbb{C}^n \to \mathbb{C}^n$, $v \mapsto D w$ où $D \in N(U)$ est choisi tel que $Du = v$ et $w \in \mathbb{C}^n \setminus W$ fixé
T est bien défini (exercice) et $T \in \mathcal{X}$. En effet, pour tout $g \in G$, $\varphi(g) \cdot T \in N(U)$, donc :
$T(\varphi(g) v) = D' \varphi(g) w = \varphi(g) D' w = \varphi(g) T v$
Maintenant $\mathcal{X} = \{\lambda I_n \mid \lambda \in \mathbb{C}\}$ donc $T = \lambda I_n$.
Donc $N(U)(w - \lambda u) = 0$ ce qui entraine $w - \lambda u \in U$
et, $w \in U + u\mathbb{C} = W \Rightarrow\Leftarrow$ $\square$

Théorème Soit K une classe de conjugaison de G et $y \in K$. Alors $|K|\, \chi(y)/n$ est un entier algébrique, où χ est un caractère irréductible de G et n est le degré de la représentation irréductible ρ associée.

Preuve

Comme χ est irréductible, on a que $\Phi := \langle \varphi(g) \mid g \in G \rangle$ est isomorphe à $Mat_n(\mathbb{C})$.

Notons $K_1, \dots, K_r$ les classes de conjugaison de G et soit $\psi_j = \sum_{y \in K} \varphi(y)$. Les ψ_j forment une base du $Z(Mat_n(\mathbb{C})) \simeq \{\lambda I_n\}$.

Donc $\psi_j = \omega_j I_n$ pour $\omega_j \in \mathbb{C}$.
De plus on a $\psi_i \circ \psi_j = \sum \lambda_{ijk} \psi_k$. $\lambda_{ijk} \in \mathbb{Z}_+$
donc $\omega_i \cdot \omega_j = \sum \lambda_{ijk} \omega_k$ dans $\mathbb{C}$.

En fixant i, on obtient le système d'équations de matrice :

$$\begin{pmatrix} \lambda_{i11} - \omega_i & \lambda_{i12} & \cdots & \lambda_{i1r} \\ \lambda_{i21} & \lambda_{i22} - \omega_i & \cdots & \lambda_{i2r} \\ \vdots & & & \\ \lambda_{ir1} & \lambda_{ir2} & \cdots & \lambda_{irr} - \omega_i \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0.$$

avec solution non-triviale $(\omega_1, \omega_2, \dots, \omega_r)$.

Donc $\det \Delta_i = 0 \Rightarrow \omega_i$ est racine d'un polynôme unitaire avec coefficients dans $\mathbb{Z}$, ce qui entraîne que ω_i est un entier algébrique.

Donc, $tr\left(\sum_{y \in K_j} \varphi(y)\right) = tr(\psi_j) = tr(\omega_j I_n) = n\omega_j$

$$\| \qquad\qquad\qquad\qquad$$

$|K_j| \cdot tr(\varphi(y)) = |K_j|\, \chi(y) \Rightarrow \dfrac{|K_j|\, \chi(y)}{n}$ est entier alg.

__Théorème__ Soit χ un caractère irréductible, de degré n et K une classe de conjugaison de G telle que $(n,|K|)=1$. Alors, pour tout $y\in K$ on a $\chi(y)=0$ ou $|\chi(y)|=n$.

__Preuve__ :

Soit $h=|K|$. Alors $\beta = h\chi(y)/n$ est un entier algébrique. De même pour $\alpha=\chi(y)$.
Supposons $\alpha = 0$ et soit

$$f(X)=X^m + a_1 X^{m-1} + \cdots + a_m \in \mathbb{Z}[X]$$

f irréductible et $f(\alpha)=0$.

$$g(X)=X^m + a_1\left(\frac{h}{n}\right)X^{m-1} + \cdots + a_m\left(\frac{h}{n}\right)^m$$

$g(\beta)=\left(\frac{h}{n}\right)^m \cdot f(\alpha)=0$, de plus g doit être irréductible (car le poly. unitaire de β doit aussi avoir degré m).

$(h,n)=1$, et comme les coeffs de g doivent être entiers on a $n^i \mid a_i$

$\left|\frac{\chi(y)}{n}\right| \leq 1$ et $\frac{\chi(y)}{n}$ et ses conjugués algébriques sont solution de

$$h(X) = X^m + \frac{a_1}{n}X^{m-1} + \cdots + \frac{a_m}{n^m} \in \mathbb{Z}$$

$$\prod_{\sigma\in Gal(h)} \sigma\left(\frac{\chi(y)}{n}\right) = \frac{a_m}{n^m} \Rightarrow 1 \geq \left|\frac{\chi(y)}{n}\right|^m \geq \left|\frac{a_m}{n^m}\right| \in \mathbb{Z}$$

$$\Rightarrow \left|\frac{\chi(y)}{n}\right| = 1, \text{ donc } |\chi(y)|=n.$$

__Lemme__ Soit G un groupe d'ordre composé, avec une classe de conjugaison de cardinalité une puissance de nombre premier.
Alors G n'est pas simple.

__Preuve__

Supposons par l'absurde que G soit simple. Soit $\chi_1, \dots, \chi_r$ ses caractères irreductibles, et $\varphi_1, \dots, \varphi_r$ les repres associées de degres $n_1, \dots, n_r$ respectivement.

$\operatorname{Ker} \varphi_1 = G$, $\operatorname{Ker} \varphi_i = 1$, $i \geq 2$

Soit $H_i := \{y \in G \mid \varphi_i(y) = \lambda I\}$. Donc $\varphi_i(H_i)$ est un sous-groupe abélien normal de $\varphi_i(G)$ et, comme φ_i est fidèle, H_i est un sous-groupe abélien normal de G. G est simple, d'ordre composé, donc $H_i = 1$. Thus $|\chi_i(y)| \neq n$, pour tout $y \in G \setminus \{1\}$. En particulier, either $p \mid n_i$ or $\chi(y) = 0$.

On a $n_1 = \chi_1(y) = 1$. Donc $1 + \sum_{i \neq 1} n_i \chi_i(y) = 0$

p / n_i (autrement $\chi_i(y) = 0$)

$1 + p \sum \frac{n_i}{p} \chi_i(y) = 0$

$\Rightarrow -\frac{1}{p}$ est un entier algébrique $\Rightarrow \Leftarrow$

Théorème Tout groupe d'ordre $q^a p^b$ est résoluble.

Preuve Si G n'est pas simple, on le décompose en facteurs qui sont résoluble par induction. Si $p = q$ G est nilpotent.

Soit $Q \in Syl_q(G)$, $y \in Z(Q) \setminus \{1\}$
Soit K la classe de conj de y dans G.
Alors $|K| = [G : C_G(y)] = n'$ et $(n', q) = 1$
Donc n' est une puissance de p différente de 1
Donc K a ordre une puissance de premier, ce que, par le Lemme précédent entraine que G n'est pas simple.
Donc il est résoluble.

$\square$