Représentations linéaires des groupes finis

Soutenance de stage

Perrine Jouteur

26 août 2020

Motivation

(a) Niels Henrik Abel

(b) Évariste Galois

(c) William Burnside

Groupes résolubles

Définition

On dit qu'un groupe G est résoluble lorsque sa suite dérivée atteint $\{1\}$:

$$G \rhd D(G) \rhd D(D(G)) \rhd \ldots \rhd \{1\}$$

Théorème de Burnside

Tout groupe d'ordre $p^\alpha q^\beta$ est résoluble.

Représentation linéaire d'un groupe G

Représentation linéaire d'un groupe G

- (V, ρ) avec V un $\mathbb{C}$-e.v. de dimension finie, et un morphisme

$$\rho : G \longrightarrow GL(V)$$

Représentation linéaire d'un groupe G

- (V, ρ) avec V un $\mathbb{C}$-e.v. de dimension finie, et un morphisme

$$\rho : G \longrightarrow GL(V)$$

- Morphisme de représentation : $f : (V_1, \rho_1) \to (V_2, \rho_2)$, tel que $f \in \mathcal{L}(V_1, V_2)$ et $\forall g \in G,\ f \circ \rho_1(g) = \rho_2(g) \circ f$.

$$\begin{tikzcd} V_1 \arrow[r, "f"] \arrow[d, "\rho_1(g)"'] & V_2 \arrow[d, "\rho_2(g)"] \\ V_1 \arrow[r, "f"] & V_2 \end{tikzcd}$$

Notation : $(\mathrm{Hom}(V_1, V_2))^G$

- **Représentations équivalentes** : $(V_1, \rho_1) \simeq (V_2, \rho_2)$ lorsqu'il existe un isomorphisme de représentations entre (V_1, ρ_1) et (V_2, ρ_2).

- **Sous-représentation** : W un sous-espace vectoriel de V, stable par G :

$$\forall g \in G, \quad \rho(g)(W) \subset W$$

- **Représentation irréductible** : pour $V \neq \{0\}$, lorsque les seules sous-représentations de V sont $\{0\}$ et V.

Théorèmes de Maschke et de Schur

Maschke

Soit V une représentation de G, et W une sous-représentation de V.
Alors il existe une sous-représentation W^o de V telle que $V = W \oplus W^o$.

Théorèmes de Maschke et de Schur

Maschke

Soit V une représentation de G, et W une sous-représentation de V.
Alors il existe une sous-représentation W^o de V telle que $V = W \oplus W^o$.

Schur

Soient deux représentations de G irréductibles, V_1 et V_2.

- Si elles ne sont pas équivalentes, $(\mathrm{Hom}(V_1, V_2))^G = \{0\}$;
- Si elles sont égales, $(\mathrm{Hom}(V_1, V_2))^G = \mathbb{C}\,\mathrm{id}$.

Caractère d'une représentation

Caractère de la représentation $\rho : G \longrightarrow GL(V)$:

$$\begin{array}{rccc} \chi : & G & \longrightarrow & \mathbb{C} \\ & g & \longmapsto & \mathrm{Tr}(\rho(g)) \end{array}$$

- $\chi(1) = \dim(V)$
- $\forall g, h \in G$, $\chi(hgh^{-1}) = \chi(g)$ (fonction de classe)
- $\forall g \in G$, $\chi(g^{-1}) = \overline{\chi(g)}$
- $\forall g \in G$, $|\chi(g)| \leqslant \chi(1)$

Caractère d'une représentation

Caractère de la représentation $\rho : G \longrightarrow GL(V)$:

$$\begin{array}{rccc} \chi : & G & \longrightarrow & \mathbb{C} \\ & g & \longmapsto & \mathrm{Tr}(\rho(g)) \end{array}$$

- $\chi(1) = \dim(V)$
- $\forall g, h \in G$, $\chi(hgh^{-1}) = \chi(g)$ (fonction de classe)
- $\forall g \in G$, $\chi(g^{-1}) = \overline{\chi(g)}$
- $\forall g \in G$, $|\chi(g)| \leqslant \chi(1)$

Propriété

Soient (V_1, ρ^1), (V_2, ρ^2) des représentations, de caractères χ_1, χ_2.

- Le caractère de $V_1 \oplus V_2$ vaut $\chi_1 + \chi_2$
- Le caractère de $V_1 \otimes V_2$ vaut $\chi_1 \cdot \chi_2$

Relations d'orthogonalité

Première relation

Soient V, W des représentations irréductibles, de caractères χ_V et χ_W.

$$\frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_W(g) = \begin{cases} 1 \text{ si } V \simeq W \\ 0 \text{ sinon} \end{cases}$$

Deuxième relation

Soient $g, h \in G$.

$$\sum_{\chi\in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \begin{cases} 0 \text{ si } g \text{ et } h \text{ ne sont pas conjugués} \\ \dfrac{|G|}{|Cl(g)|} \text{ sinon} \end{cases}$$

Centre et noyau d'un caractère

Définition

Pour $\chi \in \mathrm{Irr}(G)$, on pose

$$Z(\chi) = \{g \in G \mid |\chi(g)| = \chi(1)\}$$

$$\mathrm{Ker}(\chi) = \{g \in G \mid \chi(g) = \chi(1)\}$$

Propriétés

Soit $\chi \in \mathrm{Irr}(G)$. Alors $Z(\chi)$ et $\mathrm{Ker}(\chi)$ sont des sous-groupes de G et

$$Z(\chi)/\mathrm{Ker}(\chi) = Z(G/\mathrm{Ker}(\chi))$$

Un premier lemme

Lemme 1

Soit G un groupe fini. Soient χ un caractère irréductible de G et C une classe de conjugaison. On suppose que $\mathrm{pgcd}(\chi(1), |C|) = 1$. Alors pour tout $g \in C$, on a $g \in Z(\chi)$ ou $\chi(g) = 0$.

Un premier lemme

Lemme 1

Soit G un groupe fini. Soient χ un caractère irréductible de G et C une classe de conjugaison. On suppose que $\text{pgcd}(\chi(1), |C|) = 1$. Alors pour tout $g \in C$, on a $g \in Z(\chi)$ ou $\chi(g) = 0$.

Démonstration : Soit $g \in C$, d'ordre n.

$$u\chi(1) + v|C| = 1 \quad \textit{(Relation de Bézout)}$$

$$\frac{\chi(g)}{\chi(1)} = u\chi(g) + v\frac{|C|\chi(g)}{\chi(1)} \ (*)$$

Posons $\alpha := \dfrac{\chi(g)}{\chi(1)}$. On montre que α est algébrique.

Supposons que $|\alpha| < 1$.
Soit E le corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$, et $\mathcal{G}$ le groupe de Galois de $E/\mathbb{Q}$.
$\forall \sigma \in \mathcal{G},\ |\sigma(\alpha)| \leqslant 1$, donc :

$$\left| \beta := \prod_{\sigma \in \mathcal{G}} \sigma(\alpha) \right| < 1$$

Or β est laissé fixe par tous les morphismes de $\mathcal{G}$, et l'extension $E/\mathbb{Q}$ est galoisienne, donc $\beta \in \mathbb{Q}$, puis $\beta \in \mathbb{Z}$.
Donc $\beta = 0$, et

$$\boxed{\chi(g) = 0}$$

Un deuxième lemme

Lemme 2

Soit G un groupe simple non abélien. Alors la seule classe de conjugaison de cardinal une puissance d'un nombre premier est $\{1\}$.

Un deuxième lemme

Lemme 2

Soit G un groupe simple non abélien. Alors la seule classe de conjugaison de cardinal une puissance d'un nombre premier est $\{1\}$.

Démonstration : (par l'absurde)
Supposons qu'il existe $g \in G$, $g \neq 1$ tel que $|Cl(g)| = p^\alpha$.

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) = 0 \quad \textit{(Relation d'orthogonalité)}$$

Soit $\chi \in \mathrm{Irr}(G)$, non trivial. Si $p \nmid \chi(1)$, alors $g \in Z(\chi)$ ou $\chi(g) = 0$ (lemme 1).
Or G est simple et non abélien, donc $Z(\chi) = Z(G) = \{1\}$ et $\chi(g) = 0$. La relation d'orthogonalité

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) = 0$$

Devient

$$\sum_{\chi \in \mathrm{Irr}(G),\ p \mid \chi(1)} \chi(1)\chi(g) + 1 = 0$$

On en déduit que $\dfrac{1}{p}$ est entier algébrique, ce qui est absurde.

Démonstration du théorème de Burnside

Théorème de Burnside

Tout groupe d'ordre $p^\alpha q^\beta$ est résoluble.

Démonstration du théorème de Burnside

Théorème de Burnside

Tout groupe d'ordre $p^\alpha q^\beta$ est résoluble.

Démonstration : Par récurrence sur $|G|$
- Si $|G| = 1$, G est résoluble.

- Si $|G| = p^a q^b$: Soit $N \triangleleft G$ propre maximal.

Cas 1 : $N = \{1\}$. Soit P un Sylow de G non trivial, et $g \in Z(P)$, $g \neq 1$.
Alors $|Cl(g)| \mid [G : P]$ donc $|Cl(g)| = q^\gamma$.
Lemme 1 : G est abélien donc résoluble.

Cas 2 : $N \neq \{1\}$.
Hypothèse de récurrence : N et G/N sont résolubles, donc G l'est aussi.

Exemple

Propriété

Le plus petit groupe non résoluble est $\mathcal{A}_5$.

Nombres strictement inférieurs à 60 contenant au moins 3 facteurs premiers : $30 = 2 \times 3 \times 5$ et $42 = 2 \times 3 \times 7$.

Si G est d'ordre 30 ou 42, G n'est pas simple (théorèmes de Sylow), donc il possède un sous-groupe propre distingué N.
Par théorème de Burnside, N et G/N sont résolubles, et donc G l'est aussi.

$\mathcal{A}_5$ est simple et non commutatif, donc non résoluble.