Algèbre 2
Cours de Master 1 Grenoble
2me semestre 2011–2012

Chris Peters

Avril 2012

Introduction

Voici un résumé du cours Algèbre pour Master 2. Le sujet principal est la théorie des représentations des groupes finis. J'ai largement suivi les Chapitres 1, 2, 5 et 6 du livre excellent de Serre [Se].

Au programme était des sujets supplémentaires :

- les transformés de Fourier rapide, sujet lié aux calculs sur machine : voir le § 3.3 ;
- plus de détails sur les tables de caractères, voir le Chap. 4 ;
- applications sur la structure des groupes (théorème "pq" de Burnside) : voir le Chap. 6 .

Bibliographie

[Se] J.-P. Serre : *Linear representations of finite groups*, Springer-Verlag, New York etc. 1977.

Table des matières

Chapitre 1

Notions de base

1.1 Représentations

Soit G un groupe, K un corps et V un K-espace vectoriel.

Définition 1.1.1. V est une représentation de G si on a un homomorphisme de groupes

$$\rho : G \to \mathrm{GL}(V).$$

Si $n = \dim_K V < \infty$ on dit que n est le **degré** de la représentation.
On écrit $V^G = \{\rho_g(x) = x; g \in G\}$, le sous-espace des G-**invariants**.

On écrira plutôt ρ_g au lieu de $\rho(g)$. Écrivant $1 \in G$ pour l'unité de G et $\cdot$ pour la composition dans G, on a alors :

$$\rho_1 = \mathrm{id}_V, \quad \rho_{g\cdot h} = \rho_g \circ \rho_h, \quad \rho_{g^{-1}} = \rho_g^{-1}, \quad g, h \in G.$$

Si ρ est de degré n, choisant une K-base $\{e_1, \ldots, e_n\}$ de V, on peut identifier $\mathrm{GL}(V)$ avec $\mathrm{GL}(n, K)$ et

$$\rho_g(e_j) = \sum_{i=1}^{n} R_{ij}(g) e_i,$$

la matrice $(R_{ij}(g))_{i,j=1,\ldots,n}$ correspondant à ρ_g.

Cas spécial : $\dim_K V = 1$. Puisque $\mathrm{GL}(1, K) = K^\times$ une représentation de degré 1 est un homomorfisme $\chi : G \to K$. On l'appelle un *caractère mutiplicatif.*

Lemme 1.1.2. *L'ensemble $\widehat{G}$ des caractères multiplicatifs de G est un groupe abélien avec opération de groupe $(\chi.\chi_2)(g) := \chi_1(g) \cdot \chi_2(g)$ (produit dans K).*

On montre

Proposition 1.1.3. *1) Si G est un groupe abélien fini G, le groupe G et $\widehat{G}$ sont isomorphes (mais pas canoniquement) ;*
2) L'application

$$\begin{array}{rcl} G & \to & \widehat{\widehat{G}} \quad \text{(double dual de } G\text{)} \\ g & \mapsto & (\chi \mapsto \chi(g)) \text{ evaluation en } g \end{array}$$

est bien-definie, c'est en effet un isomorfisme de groupes.

1.2 Exemples de base

Soit X un ensemble fini tel que G agit sur X, i.e. on a un homomorphisme

$$\sigma : G \to \mathrm{Perm}(X) \quad \text{(permutations de } X\text{)}.$$

On prend $V = \sum_{x\in X} Ke_x$ et on fait agir G de façon naturelle sur la base $\sigma_g(e_x) = e_{\sigma(x)}$ et on étend par K-linéarité.

Exemples 1.2.1. 1) $G = \mathfrak{S}_n$, le groupe symétrique opérant sur $\{1, \ldots, n\}$.
2) **Représentation régulière** R_G du groupe fini G : on prend $V = G$ avec l'action donnée par multiplication à gauche : $R_g(h) = g \cdot h$.
3) **Somme directe** Si V et V' sont deux représentations de G aussi la somme $V \oplus V'$ l'est.
3) Si (V, ρ) et (V', ρ') sont deux représentations de G l'espace K-vectoriel des applications K-linéaires de V vers V' l'est. On définit l'action comme suit :

$$\tau_g := {\rho'_g}^{-1} \circ \tau \circ \rho_g, \quad \tau \in \mathrm{Hom}(V, V').$$

Si $\tau \in \mathrm{Hom}^G(V, V')$, i.e. si τ est G-invariant on dit que τ est G-**équivariant**.

On a aussi des exemples géométriques.

Exemples 1.2.2. 1) Le groupe **cyclique** C_n d'ordre n avec générateur r s'identifie avec le groupe des rotations du plan euclidien engendré par la rotation r d'angle $2\pi/n$. Si on identifie $\mathbb{R}^2$ et $\mathbb{C}$ on peut identifier r avec la multiplication par le nombre complexe $e^{\frac{2\pi \mathrm{i}}{n}}$. Ainsi $\mathbb{C}$ est un caractère multiplicatif de C_n mais en regardant $\mathbb{C}$ comme $\mathbb{R}^2$ aussi une $\mathbb{R}$-représentation de degré 2. Ensuite, regardant les coefficients des matrices de taille 2 pour r^k comme des nombres complexes, aussi une $\mathbb{C}$-représentation de degré 2. Puisque les points $e^{\frac{2\pi k \mathrm{i}}{n}}$ sont les a sommets d'un polygone régulier P_n d'ordre n on peut voir C_n aussi comme le groupe des symétries directes de P_n.
2) Le groupe **diédral** D_n des toutes les symétries de P_n est engendré par r et une symétrie s, l'application $(x, y) \mapsto (x, -y)$. Le plan $\mathbb{R}^2$ est une représentation de D_n de degré 2. Il n'est pas vrai que $\mathbb{C}$ est une représentation car s est la conjugaison complexe qui n'est pas $\mathbb{C}$–linéaire.

1.3 Représentations équivalentes

Deux représentations (V, ρ) et (V', ρ') (sur un corps K) sont équivalentes s'il y existe un isomorphisme K-linéaire $\tau : V \to V'$ telle que $\rho'_g = \tau \circ \rho_g \circ \tau^{-1}$, c.à.d. il existe $\tau \in \mathrm{Hom}^G(V, V')$, un isomorphisme équivariant.

Exemple 1.3.1. Si V est une représentation de G de dimension n un choix de base donne une action sur K^n. Un autre choix choix de base donne une représentation équivalente.

1.4 Sous-représentations

Soit V une représentation. Un sous-espace stable par G est appellé une **sous-représentation**. Il y a toujours les sous-représentations dites **triviales** $\{0\}$ et V. Si V n'admet aucun autre sous-représentation, on dit que V est **irréductible**.

Exemple 1.4.1. Supposons que $K = \mathbb{C}$. On va montrer que si G est fini et abélien, une représentation est somme directe de représentations de degré 1, nécessairement irréductibles. D'abord on note que $g^m = e$, alors $\rho_g^m = \mathrm{id}_V$ et donc le polynôme minimale de ρ_g divise $X^m - 1$, un polynôme à racines différentes. Donc ρ_g est diagonalisable avec valeurs propres des racines d'unité. Si de plus G est fini et abélien, les ρ_g commutent et donc il y a une base $\{e_1, \ldots, e_n\}$ des vecteurs propres communes à toutes les ρ_g. Il suit que $V = \bigoplus_{j=1}^n \mathbb{C}e_j$ est la décomposition souhaité.

Théorème 1.4.2. *Soit V une représentation d'un groupe fini G et W une sous-représentation. Alors W admet une supplémentaire W^0 stable par G.*

Démonstration : Soit W' n'importe que supplémentaire et $p : V \to V$ la projection sur W ayant W' pour noyau. Rappelons que $p_g = \rho_g \circ p \circ \rho_g^{-1}$. L'application

$$p^0 := \frac{1}{\#G} \cdot \sum p_g : V \to V$$

a W pour image et $p^0|W = \mathrm{id}_W$. Donc p^0 est une projection sur W. Le noyau W^0 est une supplémentaire. Puisque p^0 est G-équivariant par construction, W^0 est G-stable. □

Clairement on a : V est irréductible si et seulement si V n'est pas somme directe de sous-représentations non-triviales et donc le théorème implique (par récurrence sur la dimension de V) :

Corollaire 1.4.3. *Chaque représentation de dimension finie se décompose en représentations irréductibles.*

Un mot d'avertissement : cette décomposition n'est pas unique !

Remarque. Soit $K = \mathbb{C}$ ou $\mathbb{R}$ et V une K-espace muni d'une métrique provenant d'une forme sequilinéaire $\langle , \rangle$. Alors si V est représentation d'une groupe fini G on peut remplacer cette forme par

$$\langle x, y \rangle^0 = \frac{1}{\#G} \cdot \sum \langle \rho_g x, \rho_g y \rangle, \quad x, y \in V.$$

Cela donne une métrique G-invariante sur V et si W est G-stable, aussi $W^\perp$ l'est.

Chapitre 2

Caractères

On suppose que V est un $\mathbb{C}$-espace de dimension finie. A partir du § 2.2 on supposera G est un groupe fini.

2.1 Définition

Soit f un endomorphisme de V.

Soit (F_{ij}) la matrice de f par rapport à une base de V. On sait que $\operatorname{Tr} f = \sum_i F_{ii}$. Lorsque $\mathbb{C}$ est algébriquement clos, $\operatorname{Tr} f = \sum$(valeurs propres de f).

Définition 2.1.1. Le **caractère** $\chi : G \to \mathbb{C}$ associé à une représentation (V, ρ) est défini par $\chi(g) := \operatorname{Tr}(\rho_g)$. On dit que χ est un caractère **irréductible** si ρ l'est.

Si $f^n = \mathrm{id}_V$, les valeurs propres sont des n-ième racines d'unité. Dans ce cas $\operatorname{Tr} f$ est somme de racines d'unité. Cela applique à $f = \rho_g$, (V, ρ) une représentation de groupe fini G.

Pour $f = \chi$ un caractère d'un groupe *fini* on a

$$\chi(g^{-1}) = \overline{\chi(g)}. \tag{2.1}$$

En effet, $\chi(g^{-1}) = \operatorname{Tr}(\rho_{g^{-1}}) = \operatorname{Tr}(\rho_g)^{-1} = \sum \lambda^{-1}$ somme sur les valeurs propres λ de g. Mais λ étant une racine d'unité, on a $\lambda^{-1} = \bar{\lambda}$ et $\sum \bar{\lambda} = \overline{\sum \lambda} = \overline{\operatorname{Tr} \rho_g}$.

2.2 Lemme de Schur

Lemme 2.2.1 (Schur)**.** *Soient $\rho^i : G \to \mathrm{GL}(V_i)$, $i = 1, 2$ deux représentations irréductibles et soit $f : V_1 \to V_2$ équivariante. Alors,*

1. *soit $f = 0$, soit f est un isomorphisme ;*
2. *de plus, si $(V, \rho) = (V_1, \rho^1) = (V_2, \rho^2)$, alors $f = \lambda \cdot \mathrm{id}_V$.*

La preuve découle immédiatement du fait que les V_i, $i = 1, 2$ sont irréductibles.

Remarque. Le point i) reste vrai pour n'importe quel corps K, pour ii) on doit supposer que K est algébriquement clos. On n'utilise pas que G est fini.

Pour le résultat suivant G doit être fini. C'est une conséquence immédiat du lemme de Schur.

Corollaire 2.2.2. *Soient $\rho^i : G \to \mathrm{GL}(V_i)$, $i = 1, 2$ deux représentations irréductibles d'un groupe fini G, et soit f linéaire (mais pas forcément équivariante). On pose*

$$f^0 = \frac{1}{|G|} \sum_{g \in G} (\rho_g^2)^{-1} \circ f \circ \rho_g^1.$$

Alors f^0 est G-équivariante et donc :

1. *$f^0 = 0$ si V_1 et V_2 ne sont pas équivalentes ;*
2. *si $(V, \rho) = (V_1, \rho^1) = (V_2, \rho^2)$, alors*

$$f^0 = \frac{\mathrm{Tr}\, f}{\dim V} \cdot \mathrm{id}_V \,.$$

On a besoin de la forme matricielle des deux assertions de la Corollaire précendente. On suppose que ρ_g^1 correspond à $(R_{ij}(g)$ et ρ_g^2 à $(S_{k\ell}(g)$. On trouve dans les 2 cas de la Corollaire précédente :

$$1) \iff \sum_{g \in G} S_{ij}(g^{-1}) \circ R_{k\ell}(g) = 0 \quad \forall i, j, k, \ell \tag{2.2}$$

$$2) \iff \sum_{g \in G} R_{ij}(g^{-1}) \circ R_{k\ell}(g) = \frac{|G|}{\dim V} \delta_{ik} \cdot \delta_{j\ell} \quad \forall i, j, k, \ell. \tag{2.3}$$

2.3 Produit scalaire et applications

On considère $\mathbb{C}[G]$, la représentation régulière de G avec base $\{e_g\}_{g \in G}$. A noter que $f \in \mathbb{C}[G]$ est une somme $f = \sum_{g \in G} f(g) e_g$ et donc on peut la voir comme fonction $f : G \to \mathbb{C}$.

L'ensemble $\mathbb{C}[G]$ n'est pas seulement un $\mathbb{C}$-espace vectoriel mais admet un produit scalaire G-invariant :

$$\langle f \mid f' \rangle = \frac{1}{|G|} \sum_{g \in G} f(g) \overline{f'(g)}.$$

Dans le cas spécial où $f = \chi$, le caractère d'une représentation, par (2.1) on a $\overline{\chi(g)} = \chi(g^{-1})$ et donc

$$\langle f \mid \chi \rangle = \frac{1}{|G|} \sum_{g \in G} f(g) \chi(g^{-1}) = \frac{1}{|G|} \sum_{g \in G} f(g^{-1}) \chi(g) \tag{2.4}$$

Les formules (2.2), (2.3) et (2.4) impliquent :

Proposition 2.3.1. *Soient χ, χ' les deux caractères irréductibles de ρ, ρ' respectivement. Alors,*

1. *$\langle \chi \mid \chi \rangle = 1 = \langle \chi' \mid \chi' \rangle$;*
2. *ρ et ρ' inéquivalente implique $\langle \chi \mid \chi' \rangle = 0$.*

Soient $V_1, \ldots V_h$ les représentations irréductibles de G qui correspondent aux caractères distincts [1] $\{\chi_1 = 1, \ldots, \chi_h\}$.

1. On a utilisé ici que pour $|G| = n$ fini, il n'y a qu'un nombre fini de classes d'équivalence de représentations irréductibles car il n'y a qu'un nombre fini de caractères $\chi : G \to \mathbb{C}$ ($\chi(g)$ est un des n-ième racines d'unité et donc en total au plus n^2 possibilités pour χ).

Théorème 2.3.2. *Soit V une représentation avec caractère χ et soit*

$$V = V_1' \oplus \cdots \oplus V_k'$$

une décomposition en irréductibles. Alors

$$n_i := \langle \chi \mid \chi_i \rangle = \textit{nombre de } j \textit{ telle que } V_j' \simeq V_i.$$

Si V' est une autre G–représentation, alors V et V' sont équivalentes si et seulement si leurs caractères sont égaux.

Le théorème est une conséquence directe de la Prop. 2.3.1.

Définition 2.3.3. La décomposition

$$V = W_1 \oplus \cdots W_h, \quad W_i = \oplus_{\{j; V_j' \simeq V_i\}} V_j' \simeq \oplus V_i^{n_i}. \tag{2.5}$$

s'appelle la *décomposition isotypique*

Proposition 2.3.4. *Soient $V_1, \ldots V_h$ les représentations irréductibles de G qui correspondent aux caractères distinctes $\{\chi_1 = 1, \ldots, \chi_h\}$. Soit (V, ρ) une G-représentation avec décomposition isotypique* (2.5) *Alors*

$$\frac{n_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \rho_g$$

est la projection sur la sommande W_i suivant la décomposition isotypique de V. En particulier, la décomposition isotypique est unique.

Démonstration : Soit $q_i = \frac{n_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \rho_g$. Alors q_i est G-équivariant. Soit $V' \subset V$ un sous-représentation irréductible avec caractère χ'. Alors $q_i | V' = \lambda \, \mathrm{id}$, un multiple de l'identité. En comparant les traces on trouve

$$\lambda = \frac{n_i}{\dim V} \langle \chi_i \mid \chi' \rangle = \begin{cases} 0 \text{ si } V' \not\simeq V_i \\ 1 \text{ si } V' \simeq V_i. \end{cases}$$

et donc $q_i | W_i = \mathrm{id}$ et $q_i | W_j = 0$ si $j \neq i$. □

On regarde la représentation régulière $(\mathbb{C}[G], R)$ (avec caractère χ_R). Puisque G agit par permutation des éléments $\{e_g\}$, $g \in G$ d'une base, la matrice $R(g)$ a trace 0 sauf si $g = e$. Donc si W est une représentation irréductible de G avec caractère χ, on a :

$$\langle \chi_R \mid \chi \rangle = \frac{1}{|G|} \sum_g \chi_R(g^{-1}) \chi(g) = \chi(e) = \dim W.$$

Donc $(\mathbb{C}[G], R) \simeq \sum \dim(W) W$ où la somme est prise sur les irréductibles de G. Cela montre :

Proposition 2.3.5. *Soient V_i les classes de représentations inéquivalentes V_i avec caractères χ_i, $i = 1, \ldots, h$. On pose $n_i = \dim V_i$. On a des restrictions suivantes*

1. $\sum_{i=1}^h n_i^2 = |G|$,
2. *Si $g \neq e$ on a $\sum_{i=1}^h n_i \chi_i(g) = 0$.*

Démonstration : Puisque $\chi_R(g) = \sum n_i \chi_i(g)$, le résultat suit car $\chi_i(e) = n_i$ et $\chi_i(g) = 0$ sinon. □

Chapitre 3

L'algèbre $\mathbb{C}[G]$.

3.1 Le produit de convolution

On a $\mathbb{C}[G] = \bigoplus_{g\in G} \mathbb{C}\cdot e_g$. On obtient une multiplication $*$ sur $\mathbb{C}[G]$ si on pose $e_g * e_h := e_{gh}$ que l'on étend par bilinéarité :

$$(\sum_{g\in G} a_g e_g) * (\sum_{h\in G} a_h e_h) = (\sum_{g,h\in G} a_g b_h e_{gh}) \in \mathbb{C}[G].$$

L'unité dans cet algèbre est $\mathbf{1} := e_e$. Pour montrer que $(\mathbb{C}[G], +, *, \mathbf{1})$ est une algèbre unitaire, on remarque que la distributivité de $(+, *)$ est automatique, que $eg = g = ge$ entraîne que $\mathbf{1}$ est un unité, que – finalement – l'associativité de la multiplication de G entraîne l'associativité de $*$.

Une représentation

$$\rho : G \to \mathrm{GL}(V)$$

induit un homomorphisme de $\mathbb{C}$-espace vectorielles

$$\begin{array}{ccc} \tilde{\rho} : \mathbb{C}[G] & \longrightarrow & \mathrm{End}\, V, \\ \sum_g a_g e_g & \longmapsto & \sum a_g \rho_g. \end{array}$$

On verifie aisément que $\tilde{\rho}$ est un morphisme d'algèbres et on a :

Proposition 3.1.1. *La donnée d'une représentation ρ est équivalente à donner son morphisme d'algèbres induite $\tilde{\rho}$.*

Rappelons qu'on peut considérer $f \in \mathbb{C}[G]$ comme fonction $f : G \to \mathbb{C}$. L'élément de base e_g correspond à la fonction de *Dirac* δ_g qui prend la valeur 1 sur g et vaut 0 sinon.

Lemme 3.1.2. *Le produit $*$ s'identifie à la convolution parmi les fonctions :*

$$f_1 * f_2(h) = \sum_{g_1 g_2 = h} f_1(g_1) f_2(g_2) = \sum_{g\in G} f_1(g) f_2(g^{-1}h).$$

En effet

$$\begin{aligned}\left(\sum_{g_1\in G} f_1(g_1)e_{g_1}\right) * \left(\sum_{g_2\in G} f_2(g_2)e_{g_2}\right) &= \sum_{g_1,g_2\in G} f_1(g_1)f_2(g_2)e_{g_1g_2} \\ &= \sum_{h}\left(\sum_{g_1g_2=h} f_1(g_1)f_2(g_2)\right)e_h.\end{aligned}$$

Exemple 3.1.3. Soit G le groupe C_n cyclique d'ordre n avec générateur r. L'algèbre $\mathbb{C}[C_n]$ s'identifie avec l'algèbre $P_n := \mathbb{C}[X]/(X^n-1)$ des polynômes "modulo X^n-1" : On envoie r à $\bar{X}$, la classe de X dans P_n. Le produit de convolution donne le produit de P_n induit par multiplication des polynômes :

$$\left(\sum_{k=0}^{n-1} a_k\bar{X}^k\right) * \left(\sum_{m=0}^{n-1} b_m\bar{X}^m\right) = \sum_{k=0}^{n-1}\sum_{\ell=0}^{n-1} a_\ell b_{[k-\ell]}\bar{X}^k,$$

ou $[s]$ est l'unique entier égal à s modulo n tel que $0 \le [s] < n$. On note que ce produit n'est pas égal au produit "usuel" sur G où $(f\cdot g)(s) = f(s)\cdot g(s)$. En effet, ce produit consiste à multiplier a_k et b_k :

$$\left(\sum_{k=0}^{n-1} a_k\bar{X}^k\right) \cdot \left(\sum_{m=0}^{n-1} b_m\bar{X}^m\right) = \sum_{k=0}^{n-1} a_kb_k\bar{X}^k,$$

donc, cette algèbre est isomorphe à l'algèbre $\mathbb{C}^n$, somme directe de n copies de $\mathbb{C}$.

Plus tard on a besoin de la transformation de Fourier qui compare ces deux produits :

Exemple 3.1.4 (Transformation de Fourier). Un caractère multiplicatif $\chi : G \to \mathbb{C}^\times$ correspond à une représentation de degré 1 avec une extension :

$$\tilde{\chi} : \mathbb{C}[G] \to \mathbb{C}.$$

Les caractères multiplicatifs de G forment le groupe dual $\widehat{G}$. Le $\mathbb{C}$-espace vectoriel $\mathbb{C}[\widehat{G}]$ est une algèbre pour $*$ mais aussi pour le produit donné par

$$(f_1\cdot f_2)(\chi) = f_1(\chi)f_2(\chi).$$

Pour $f \in \mathbb{C}[G]$ considérons la fonction $\hat{f}$ sur le groupe dual $\widehat{G}$ définie par :

$$\begin{aligned}&\widehat{G} \xrightarrow{\hat{f}} \mathbb{C} \\ &\chi \mapsto \hat{f}(\chi) = \tilde{\chi}(f).\end{aligned}$$

On obtient ainsi le **morphisme de Fourier**

$$\begin{array}{lcl}(\mathbb{C}[G],\ \text{produit convolution } *) & \to & (\mathbb{C}[\widehat{G}],\ \text{produit "usuel" } \cdot) \\ f & \mapsto & \hat{f}\,,\end{array}$$

un morphisme de $\mathbb{C}$–algèbres.
Cas spécial : $G = C_n$, le groupe cyclique d'ordre n avec générateur r. On pose

$$\omega := \exp\left(-\frac{2\pi\mathrm{i}}{n}\right).$$

Les caractères multiplicatifs sont les χ_j définis par $\chi_j(r^k) = \omega^{jk}$. Si on identifie $(\mathbb{C}[\widehat{G}], \cdot)$ avec l'algèbre $\mathbb{C} \oplus \mathbb{C}X \oplus \mathbb{C}X^2 \oplus \cdots \oplus \mathbb{C}X^{n-1} \simeq \mathbb{C}^n$, l'application de Fourier devient :

$$f \mapsto \hat{f} = \sum_{j=0}^{n} f(\omega^j) X^j. \tag{3.1}$$

3.2 Le cas abélien.

On applique l'exemple 3.1.4 au cas où est G abélien. Soient $\chi_1, \ldots, \chi_n$ les $n = |G|$ caractères multiplicatifs de G. Ils donnent une base orthonormée de $\mathbb{C}[G]$ et donc pour tout $f \in \mathbb{C}[G]$ on a :

$$f = \sum_{i=1}^{n} \langle f \mid \chi_i \rangle \chi_i = \sum_{i=1}^{n} \langle f \mid \bar{\chi}_i \rangle \chi_i^{-1}.$$

D'autre part, par la définition du produit $\langle - \mid - \rangle$ on a

$$\hat{f}(\chi_i) = \tilde{\chi}_i(f) = \sum_g f(g)\chi_i(g) = |G| \langle f \mid \bar{\chi}_i \rangle.$$

On a donc la **formule d'inversion** :

Lemme 3.2.1.

$$f = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\chi^{-1} = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi^{-1})\chi.$$

Ce lemme implique que $f \mapsto \hat{f}$ est injective et donc

Proposition 3.2.2. *Pour un groupe abélien G, la transformation de Fourier est un isomorphisme $\mathbb{C}[G] \xrightarrow{\sim} \mathbb{C}[\hat{G}]$.*

Exemple 3.2.3 (Le groupe cyclique C_n). Revenons à l'équation (3.1). L'isomorphisme dit que f est déterminé uniquement par ses valeurs au points $1, \omega, \ldots, \omega^{n-1}$. En effet, la formule d'inversion n'est rien autre que la formule d'interpolation de Lagrange : par la formule d'inversion, on a

$$\begin{aligned} f &= \frac{1}{n} \sum_{k=0}^{n-1} \hat{f}(\chi_k^{-1}) X^k \\ &= \sum_{k=0}^{n-1} \Big[\frac{1}{n} \sum_{j=0}^{n-1} f(\omega^j) \omega^{-kj} \Big] X^k \\ &= \sum_{j=0}^{n-1} f(\omega^j) \underbrace{\Big[\frac{1}{n} \sum_{k=0}^{n-1} \omega^{-kj} X^k \Big]}_{p_j(X)} \end{aligned}$$

et $p_j(X)$ est le polynôme de Lagrange degré $n-1$ tel que $p_j(\omega^\ell) = \delta_{j\ell}$, $\ell = 0, \ldots, n-1$.

3.3 Application : Transformée de Fourier rapide

On se place dans l'anneau $(P_n, *)$. Le calcul direct du produit de convolution $f * g$ comporte n^2 multiplications. Mais, puisque $\widehat{f * g} = \hat{f} \cdot \hat{g}$ on peut d'abord calculer les valeurs $f(\omega^j)$, $g(\omega^j)$, pour $j = 0, \ldots, n-1$ (donc $2n$ opérations), ensuite multiplier $f(\omega^j)$ et $g(\omega^j)$ (donc n opérations) et ensuite, il faut faire la transformée de Fourier. Ceci explique l'intérêt de trouver un calcul rapide.

Le calcul de Cooley et Tukey (1965), abrégé **FFT** ("Fast Fourier Transform") donne une réponse. Pour expliquer ce calcul, supposons que $n = 2^k = 2n'$. Rappelons que $\omega = \exp\left(-\frac{2\pi \mathrm{i}}{n}\right)$. Soit F la transformée de Fourier associée à (n, ω) et F' la transformée associée à $(n', \omega' = \omega^2)$. On a :

$$f = \underbrace{a_0 + a_2 X^2 + \cdots + a_{2(n'-1)}(X^2)^{n'-1}}_{f^+(X^2)} + X \cdot \underbrace{\left(a_1 + a_3 X^2 + \cdots a_{2n'-1}(X^2)^{n'-1}\right)}_{f^-(X^2)}.$$

Les degrés de f^+ et f^- sont $\leq n' - 1$. Si on écrit $F(f) = \sum F_i(f) X^i$ on a :

$$\begin{aligned} F(f) = \quad & \textstyle\sum_{j=0}^{n'-1} \left[F'_j(f^+) + \omega^j F'_j(f^-)\right] X^j + \\ & \textstyle\sum_{j=n'}^{2n'-1} \left[F'_j(f^+) - \omega^j F'_j(f^-)\right] X^j. \end{aligned}$$

On a donc remplacé le calcul de $F(f)$ par le calcul des $F'(f^+)$, $F'(f^-)$ et $(n'-1) = \frac{1}{2}n - 1$ multiplications et $2n' = n$ additions/soustractions. Si $C(n)$ est le coût du calcul de $F(f)$. On a donc :

$$C(n) = 2C(\frac{1}{2}n) + \frac{3}{2}n.$$

On trouve facilement que $C(n) = n \cdot \frac{3}{2}\log_2(n)$. Il suit que le coût du calcul de $f * g$ utilisant ce FFT est $n(3 + \frac{3}{2}\log_2(n)) \sim \frac{3}{2} n \log n + O(n)$, beaucoup moins que le coût n^2 du calcul direct.

3.4 Le Centre de $\mathbb{C}[G]$ et les Fonctions Centrales

Définition 3.4.1. Une fonction $f : G \to \mathbb{C}$ est dite **centrale** si $f(hgh^{-1}) = f(g)$ pour tout $h, g \in G$.

Lemme 3.4.2. *Les fonctions centrales forment le centre Z_G de l'algèbre $\mathbb{C}[G]$.*

Démonstration : Soit $f = \sum f(g) e_g$. On a

$$(\sum_{g \in G} f(g) e_g) e_h = \sum_{g \in G} f(g) e_{gh} = \sum_{g \in G} f(gh^{-1}) e_g$$

et

$$e_h (\sum_{g \in G} f(g) e_g) = \sum_{g \in G} f(g) e_{hg} = \sum_{g \in G} f(h^{-1}g) e_g.$$

Donc f est dans le centre de $\mathbb{C}[G]$ si et seulement si $f(gh^{-1}) = f(h^{-1}g)$ pour tout $g, h \in G$, i.e. $f(g) = f(hgh^{-1})$ pour tout $g, h \in G$. □

Pour trouver une base de Z_G on introduit $\mathcal{C} :=$ classes de conjugaisons de G. Donc un élément $c \in \mathcal{C}$ est une classe d'équivalence $c = [x]$ où x et x' sont équivalents si et seulement si x et x' sont conjugués dans G, i.e. $x' = gxg^{-1}$ pour un $g \in G$. On introduit

$$e_c := \sum_{x \in c} x \in \mathbb{C}[G].$$

Lemme 3.4.3. *Les e_c, $c \in \mathcal{C}$ forment une base de Z_G. En particulier,* $\dim_{\mathbb{C}} Z_G = |\mathcal{C}|$*, le nombre des classes de conjugaison de G.*

Démonstration : On a :

$$\sum f(x)e_x \in Z_G \iff f(x) = f([x]) \quad \forall x \in G$$

et donc en particulier $e_c \in Z_G$ et on peut écrire

$$f \in Z_G \iff f = \sum_{c \in \mathcal{C}} f(c) \left(\sum_{x \in c} e_x \right) = \sum_{c \in \mathcal{C}} f(c) e_c$$

et donc les e_c forment une base de Z_G. □

3.5 Application aux représentations irréductibles

Rappelons (Prop. 3.1.1) qu'une représentation (V, ρ) de G n'est rien autre qu'un homomorphisme $\tilde{\rho} : \mathbb{C}[G] \to \mathrm{End}(V)$. On vérifie aisément :

Lemme 3.5.1. *$\tilde{\rho}(f)$ est G–équivariante $\iff$ $f \in Z_G$.*

Le lemme de Schur (§ 2.2) implique :

Corollaire 3.5.2. *Si $\rho : G \to \mathrm{GL}(V)$ est irréductible avec caractère χ, et $f \in Z_G$, alors*

$$\tilde{\rho}(f) = \lambda \,\mathrm{id}_V, \quad \lambda = \frac{|G|}{\dim V} \langle f \mid \bar{\chi} \rangle.$$

Démonstration : On a

$$\lambda \dim V = \mathrm{Tr}\, \tilde{\rho}(f) = \sum f(g)\chi(g) = |G| \langle f \mid \bar{\chi} \rangle.$$

□

On utilise ces résultats pour prouver le théorème central :

Théorème 3.5.3. *Les caractères $\chi_1, \ldots, \chi_h$ des représentations irréductibles de G forment une base orthonormée de Z_G. En particulier $h = |\mathcal{C}|$, le nombre des classes de conjugaison de G.*

Démonstration : On sait déjà que les χ_j forment un système orthonormé. Il suffit de prouver que si $f \in Z_G$, alors les h relations $\langle f \mid \bar{\chi}_j \rangle = 0$, $j = 1, \ldots, h$ impliquent que $f = 0$. Par le corollaire, si ρ est irréductible, $\tilde{\rho}(f) = 0$. Donc, c'est vrai pour *toute* représentation de G, en particulier pour R, la représentation régulière :

$$0 = \tilde{R}(f)(e_1) = \sum_{g \in G} f(g) R_g(e_1) = \sum_{g \in G} f(g) e_g = f. \quad \square$$

Il y a des relations supplémentaires parmi les χ_j :

Proposition 3.5.4. *Soit $g \in G$ et $c(g)$ la classe de conjugaison de g. Alors*

1.
$$\sum_{i=1}^{h} \overline{\chi_i(g)} \cdot \chi_i(g) = \frac{|G|}{|c(g)|}.$$

2. Si h et g ne sont pas conjugués :

$$\sum_{i=1}^{h} \overline{\chi_i(h)} \cdot \chi_i(g) = 0.$$

Démonstration : Soit $e_{c(g)} = \sum_{x \in c(g)} e_x$ alors

$$e_{c(g)} = \sum_{i=1}^{h} \lambda_i \chi_i, \quad \lambda_i = \langle e_{c(g)} \mid \chi_i \rangle = \frac{|c(g)|}{|G|} \overline{\chi_i(g)}$$

et donc

$$\delta_{gh} = e_{c(g)}(h) = \sum_{i=1}^{h} \frac{|c(g)|}{|G|} \overline{\chi_i(g)} \cdot \chi_i(h). \qquad \square$$

Chapitre 4

Exemples

4.1 Table des caractères

Soit G un groupe d'ordre n, $c_1 = \{1\}$, c_2, .. , c_h les classes de conjugaison de G. Soit χ_1 la représentation triviale (de dimension 1) et $\chi_2, \ldots, \chi_h$ les caractères des autres classes de représentations irréductibles de G. Le table des caractères de G est un table où on met $\chi_i(c_k)$ dans la i-ème ligne et K-ième colonne. La matrice qu'on définit a partir de ce table en multipliant les colonnes par $\sqrt{\frac{|c_k|}{n}}$,

$$U = (u_{ij})_{i,j=1}^{h}, \quad u_{ij} = \sqrt{\frac{|c_k|}{n}}\chi_i(c_k),$$

est unitaire, une conséquence immédiate des relations d'orthogonalité, Proposition 2.3.1. En particulier *les colonnes sont orthogonales entre elles,* mais pas les lignes. En plus : dans la première colonne on voit les degrés des représentations.

Exemple 4.1.1. 1) Le groupe cyclique C_n avec générateur r . On a les n classes de conjugaison $\left\{1, r, r^2, \ldots, r^{n-1}\right\}$ et les n caractères χ^k, $k = 0, \ldots n-1$ donné par $\chi^k(r^j) = \omega^{kj}$, $\omega = \exp(\frac{-2\pi \mathrm{i}}{n})$. Le table est

TABLE 4.1 – Table pour C_n

	1	$\cdots$	r^j	$\cdots$	r^{n-1}
1	1	$\cdots$	1	$\cdots$	1
χ	1	$\cdots$	ω^j	$\cdots$	ω^{n-1}
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$
χ^i	1	$\cdots$	ω^{ij}	$\cdots$	$\omega^{i(n-1)}$
$\vdots$	$\vdots$		$\vdots$	$\vdots$	$\vdots$
χ^{n-1}	1	$\cdots$	$\omega^{(n-1)j}$	$\cdots$	$\omega^{(n-1)^2}$

2) Le groupe diédral D_n, groupe se symétries du polygone réguliere P_n est engendré par la r r d'ordre n et une réflexion s ; on a $srs = r^{-1}$. On voit que r

et r^{-1} sont conjugués. Si $n = 2m$ ou $n = 2m+1$ on a $m+1$ classes de conjugaison parmi les rotations (lesquels ?). Si $n = 2m$ on a deux types de reflexions : celles dont l'axe de symétrie passe par les sommets de P_n, e.g. s et celles dont l'axe passe par les centres de deux arrêtes opposés, e.g. sr. Si $n = 2m + 1$ il n'y a qu'un seul type de symétrie. En total on trouve $m + 3$, respectivement $m + 2$ classes de conjugaison.

Soit χ un caractère multiplicatif. On doit avoir $\chi(r)^n = 1$ et $\chi(s)^2 = 1$. Puisque $srs = r^{-1}$ on a $\chi(r)^2 = 1$. On doit donc avoir $\chi(r) = \pm 1$ et $\chi(s) = \pm 1$. Mais, si n est impair $\chi(r)^n = 1$ force $\chi(r) = 1$. On a donc 4 caractères si n est paire et 2 si n est impaire.

Soit ρ la représentation naturelle dans $\mathbb{R}^2$. La représentation ρ a pour caractère $\chi_\rho(r) = 2\cos(\frac{2\pi}{n})$ et $\chi_\rho(s) = 0$. De ρ on trouve une représentation $\rho^j(r) = \rho(r^j)$, $\rho^j(s) = 0$. Pour $j = 1, \ldots, m-1$ (si $n = 2m$) respectivement $j = 1, \ldots, m$ (si $n = 2m + 1$) elles sont différentes, car la valeur sur r de la caractère correspondante est $2\cos(\frac{2\pi j}{n})$. Cela donne en total $m - 1 + 4 = m + 3$ représentations si $n = 2m$ et $m + 2$ représentations si $n = 2m$. Il n'y a donc pas plus de représentations irréductibles. Avec $c_r := \cos(\frac{2\pi r}{n})$ on a

TABLE 4.2 – Table pour D_{2m}

	1	r	$\cdots$	r^j	$\cdots$	r^m	s	sr
1	1	1	$\cdots$	1	$\cdots$	1	1	1
χ	1	-1	$\cdots$	$(-1)^j$	$\cdots$	$(-1)^m$	-1	-1
χ'	1	1	$\cdots$	1	$\cdots$	1	1	-1
$\chi \cdot \chi'$	1	-1	$\cdots$	$(-1)^j$	$\cdots$	$(-1)^m$	-1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
ρ^i	2	$2c_i$	$\cdots$	$2c_{ij}$	$\cdots$	$2c_{im}$	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

4.2 Autres Exemples

On peut trouver des représentations d'un groupe G à partir de celles d'un sous-groupe H si on peut trouver un sous-groupe normale N de G telle que $G = HN$ et $H \cap N = 1$. Alors, soit $\rho : H \to \mathrm{GL}(V)$ une représentation. On définit $\tilde{\rho} : G \to \mathrm{GL}(V)$ par $\tilde{\rho}_{hn} = \rho_h$. Soit $g = hn$ et $g' = r'h'$. Puisque $hnh'n' = hh'(\underbrace{h'^{-1}nh'n}_{\in N})$, on a $\tilde{\rho}_{gg'} = \rho_{hh'} = \tilde{\rho}_g \circ \tilde{\rho}_{g'}$ et donc $\tilde{\rho}$ est une représentation. On va utiliser cela pour les groupes $\mathfrak{S}_4$ et $\mathfrak{A}_4$ à partir de $\mathfrak{S}_3 = D_3$ et C_3.

$\mathfrak{S}_3$

Ce groupe est le groupe D_3 car le groupe $\mathfrak{S}_3$ opérant sur les sommets $\{a, b, c\}$ d'une triangle équilatère P_3 est le groupe de ses symétries. On a $r = (abc)$ et $s = (ab)$. Le table est

TABLE 4.3 – Table pour $\mathfrak{S}_3$

	1	(abc)	(ab)
χ_0	1	1	1
χ_1	1	1	-1
ρ	2	-1	0

$\mathfrak{A}_4$

Soit T le tétraèdre régulier à sommets $\{a, b, c, d\}$. Le groupe $\mathfrak{A}_4$ est le groupe des symétries directe de T. En effet ce groupe comprend les classes de conjugaison

1. $\{1\}$;
2. les 3 rotations $x = (ab)(cd)$, $y = (ac)(bd)$, $z = (ad)(bc)$ sur π avec axe les diagonaux d_x, d_y, d_z respectivement ;
3. les 4 rotations d'angle $\frac{2\pi}{3}$ donné par $t = (abc), tx = (bdc), ty = (adb), tz = (acd)$;
4. les 4 rotations d'angle $\frac{4\pi}{3}$ donné par $t^2 = (acb), t^2x = (adc), t^2y = (bcd), t^2z = (abd)$;

D'autre part, si g est une telle isométrie, elle fixe le barycentre de T, permute les sommets de façon fidèle. Soit g fixe un seul sommet (rotation d'ordre 3, soit aucune (rotation d'ordre 2). Donc on a toutes les permutations paires de $\{a, b, c, d\}$.

Le groupe $\mathfrak{A}_4$ permute les diagonaux $\{d_x, d_y, d_z\}$ et donc le groupe $N = \{1, x, y, z\}$ est un sous-groupe normal. Le groupe $H = \{1, t, t^2\}$ a la propriété que $\mathfrak{A}_4 = HN$. On obtient de cette façon 3 caractères provenant des 3 caractères du groupe cyclique $H = C_3$. Il reste la représentation *naturelle* ρ_T sur $\mathbb{R}^3$. On trouve le table

TABLE 4.4 – Table pour $\mathfrak{A}_4$

	1	x	t	t^2
χ_0	1	1	1	1
χ_1	1	1	ζ_3^2	ζ_3
χ_2	1	1	ζ_3	ζ_3^2
ρ_T	3	-1	0	0

$\mathfrak{S}_4$

Soit T comme dans le paragraphe précédent. Le groupe $\mathfrak{S}_4$ est le groupe des symétries de T. On a les classes de conjugaisons suivantes :

1. $\{1\}$;
2. les 3 rotations x, y, z ;

3. les 8 rotations d'ordre 3, représenté par les cycles d'ordre 3, par example (abc) ;
4. les 3 anti-rotations d'angle $\frac{\pi}{2}$ représentées par les cycles d'ordre 4, par example $(abcd)$;

Pour montrer que $u = (abcd)$ représente une anti-rotation on note que les 3 axes $\{d_x, d_y, d_z\}$ sont orthogonaux et que u tourne d_x en d_z et d_z dans d_z avec orientation opposée. Par rapport à une base orthogonale adaptée à $\{d_x, d_y, d_z\}$ la matrice de u devient : $U := \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, une rotation avec angle $\pi/2$ suivi d'une réflexion par rapport à un plan orthogonal à l'axe.

Soit $N = \{1, x, y, z\}$ et H le sous-groupe $\mathfrak{S}_3$ des permutations de $\{a, b, c\}$ laissant fixe le sommet d. Donc $\mathfrak{S}_4 = N\mathfrak{S}_3$ et on peut relever les représentations χ_1 et ρ de $\mathfrak{S}_3$.

TABLE 4.5 – Table pour $\mathfrak{S}_4$

	1	x	(ab)	abc	$(abcd)$
$\tilde{\chi}_0$	1	1	1	1	1
$\epsilon = \tilde{\chi}_1$	1	1	-1	1	-1
$\tilde{\rho}$	2	2	0	-1	0
ρ_T	3	-1	1	0	-1
$\epsilon\rho_T$	3	-1	-1	0	1

Explication : ρ_T est la représentation de $\mathfrak{S}_4$ comme groupe des symétries de T. Les traces sont calculées à partir de la description géométrique. Le caractère $\tilde{\rho}$ doit être le même que ϵ le caractère de parité. La représentation $\epsilon\rho_T$ est définie comme $(\epsilon\rho_T)_g = \epsilon(g)\rho_g$, $g \in \mathfrak{S}_4$.

4.3 Table de caractères et la structure de groupe

Soit G un groupe fini et $\widehat{G}$ son groupe de caractères. On rappelle que le **groupe dérivé** $D(G) = [G, G]$ est le sous-groupe distingué des commutateurs de G et que son quotient $G_{\mathrm{ab}} = G/[G, G]$ est **l'abélianisé** de G. Chaque caractère multiplicatif $\chi : G \to \mathbb{C}^\times$ étant 1 sur $[G, G]$, se factorise par $\bar{\chi} : G_{\mathrm{ab}} \to \mathbb{C}^\times$. Chaque caractère de G_{ab} s'étend en un caractère multiplicatif de G. Par l'inversion de Fourier (Prop. 3.2.2), si $\bar{\chi}(\bar{g}) = 1$ pour tout $\bar{\chi} \in \widehat{G_{\mathrm{ab}}}$, alors $\bar{g} = 1$, c.à.d. $g \in D(G)$. On peut donc retrouver $D(G)$ en lisant le table de caractères :

$$D(G) = \{g \in G; \chi(g) = 1 \text{ pour tout caractère multiplicatif } \chi\}.$$

On peut également retrouver le **centre** $Z = Z_G$ de façon suivante. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation irréductible avec caractère χ_V. Par le Cor. 3.5.2 $\rho(z)$ est une homothétie pour $z \in Z$, i.e. $\rho(z) = \chi(z)\,\mathrm{id}_V$ où χ est un caractère multiplicatif de Z. Clairement $\chi(z) \cdot \dim(V) = \chi_V(z)$ et donc $|\chi_V(z)| = \dim(V) = \chi(1)$. Réciproquement, si $|\chi_V(z)| = \dim(V) = \chi(1)$ pour tout caractère χ d'une

représentation irréductible de G, alors $z \in Z$. On laisse cet assertion en exercice. On on a donc

$$Z_G = \{s \in G; |\chi_V(s)| = \chi(1) \text{ pour tout caractère irréductible } \chi\}.$$

De façon similaire on peut retrouver les **sous-groupes distingués** de G utilisant la notion de **noyau** d'un caractère χ associé à la représentation $\rho : G \to \mathrm{GL}(V)$.

$$\ker(\chi) := \{g \in G; \chi(g) = \chi(1)\}.$$

Les assertions suivantes sont laissées en exercice ; la proposition explique comment retrouver les sous-groupes distingués de G :

Proposition 4.3.1. *1.* $\ker(\chi)$ *est le noyau de l'homomorphisme* ρ *et donc un sous-groupe distingué de* G*.*

2. Chaque sous-groupe distingué H *est intersection d'un nombre fini des noyaux de caractères irréductibles.*

Corollaire 4.3.2. *Un groupe* G *est* ***simple*** *(c'est-à-dire que* G *ne possède aucun sous-groupe distingué autre que* $\{1\}$ *et* G*) si et seulement si pour tout* $g \in G$*,* $g \neq 1$ *et et tout caractère irréductible* $\chi \neq 1$ *on a* $\chi(g) \neq \chi(1)$*.*

Chapitre 5

Retour sur le centre de $\mathbb{C}[G]$

5.1 Décomposition du centre de $\mathbb{C}[G]$

Soient $\rho^i : G \to \mathrm{GL}(W_i)$, $i = 1, \ldots, h$ les représentations irréductibles de G à isomorphisme près. On pose $d_i = \dim W_i$. Soit $\tilde{\rho}^{(i)} : \mathbb{C}[G] \to \mathrm{End}\, W_i$ l'homomorphisme d'algèbres associé.

Théorème 5.1.1. *On a un isomorphisme de $\mathbb{C}$-algèbres*

$$\tilde{\rho} := \tilde{\rho}^{(1)} \times \cdots \times \tilde{\rho}^{(h)} : \mathbb{C}[G] \xrightarrow{\sim} \prod_{i=1}^{h} \mathrm{End}\, W_i.$$

Démonstration : Vu l'égalité $|G| = \sum_i n_i^2$, les dimensions du but et source de $\tilde{\rho}$ sont égales. Il suffit de montrer que $\tilde{\rho}$ est surjectif. Sinon, les élément de l'image obéissent une relation linéaire non-triviale. En termes de matrices $R_{ij}^{\alpha}(g)$ pour les $\rho_g^{(k)}$ on obtient alors une relation de la forme

$$\sum_{k=1}^{h} a_k R_{ij}^{(k)}(g) = 0, \quad \forall g \in G.$$

On multiplie cette relation avec $R_{\ell m}^{(\alpha)}(g^{-1})$ et on somme sur $g \in G$. On utilisera l'équation (2.2) en ensuite (2.3) :

$$\begin{aligned} 0 &= \sum_k \sum_g a_k R_{ij}^{(k)}(g) R_{\ell m}^{(\alpha)}(g^{-1}) \\ &= \sum_g a_\alpha R_{ij}^{(\alpha)}(g) R_{\ell m}^{(\alpha)}(g^{-1}) \\ &= \frac{|G|}{d_\alpha} a_\alpha \end{aligned}$$

et donc $a_\alpha = 0$ pour $\alpha = 1, \ldots, h$. Contradiction.

□

Corollaire 5.1.2. *Le centre $Z(G)$ de $\mathbb{C}[G]$ est isomorphe au produit directe $\mathbb{C}^h$ de h copies de l'algèbre $\mathbb{C}$. Plus précisément, soit p_α la projection sur le α-ème*

facteur de $\mathbb{C}^h$, χ_α *le caractère associé à* $\rho^{(\alpha)}$ *les fonctions linéaires*

$$Z(G) \ni f \mapsto p_\alpha \circ \tilde{\rho}(f) = \frac{|G|}{d_\alpha} \langle f \mid \bar{\chi}^\alpha \rangle = \frac{1}{d_\alpha} \sum_g f(g) \overline{\chi_\alpha(g)}$$

se combinent en un isomorphisme

$$\prod_{\alpha=1}^{h} p_\alpha \circ \tilde{\rho} : Z(G) \xrightarrow{\sim} \mathbb{C}^h.$$

Démonstration : C'est une conséquence directe du Corr. 3.5.2. □

5.2 Intermède : les entiers algébriques

Soit B un anneau *commutatif* et $A \subset B$ un sous-anneau.

Définition 5.2.1. On dit que $\xi \in B$ est A-**entier** s'il existe un polynôme *unitaire* $P \in A[X]$ tel que $P(\xi) = 0$.

Exemples 5.2.2. 1) Si $B|A$ est une extension de corps $\xi \in B$ est A-entier si et seulement si ξ est A-algébrique. Un tel élément satisfait une équation $Q(X) = 0$ irréductible et on peut toujours choisir Q unitaire. Dans le cas spécial $A = \mathbb{Q}$ et $B = \mathbb{C}$ on parle s'un **nombre algébrique**. Notation $\bar{\mathbb{Q}}$.
2) Si $A = \mathbb{Z}$ et $B = \mathbb{C}$ on parle d'un **entier algébrique**. Notation : $\bar{\mathbb{Z}}$. Clairement, un entier algébrique est un nombre algébrique. Une racine d'unité est un entier algébrique (car elle satisfait $X^n - 1 = 0$ pour n convenable).

Si $Q(X) \in \mathbb{Q}[X]$ est le polynôme minimal irréductible pour un entier algébrique ξ pour lequel $P(\xi) = 0$ on a Q divise P dans $\mathbb{Q}[X]$ et on peut choisir $Q \in \mathbb{Z}[X]$ (conséquence du lemme de Gauss). Les conjugués de ξ sont les autres racines de $Q(X) = 0$ et donc :
Si $\xi \in \mathbb{C}$ *est un* $\mathbb{Z}$*-entier, tout ses conjugués sont des* $\mathbb{Z}$*-entiers.*

Une relation utile entre les rationnels et les entiers algébriques :

Lemme 5.2.3. *Un nombre rationnel qui est entier algébrique est entier.*

Démonstration : Soit $\xi = p/q \in \mathbb{Q}$ et $(p, q) = 1$. On suppose que $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, $a_j \in \mathbb{Z}$, est telle que $P(\xi) = 0$. Alors $p^n + q(a_{n-1}p^{n-1} + \cdots a_0 q^{n-1}) = 0$. Cela implique que p divise q contrairement au choix $(p, q) = 1$. □

La propriété principale des entiers est qu'ils forment un sous-anneau :

Proposition 5.2.4. *l'ensemble* $\{\xi \in B; \xi$ *est* A*-entier*$\}$ *est un sous-anneau de* B *contenant* A.

On déduit cette propriété du lemme suivant :

Lemme 5.2.5. $\xi \in B$ *est* A*-entier si et seulement s'il y a un sous-module* M *de type fini de* B *tel que* $\xi M \subset M$.

Lemme $\implies$ *Proposition :* Soient $\xi_\alpha \in B$, $\alpha = 1, 2$ deux A-entiers et $M_\alpha \subset B$ un sousmodule de type fini de B tel que $\xi_\alpha M_\alpha \subset M_\alpha$. Alors on a :

$$(\xi_1 \pm \xi_2)M_1M_2 \subset M_1M_2, \quad \xi_1\xi_2 M_1M_2 \subset M_1M_2.$$

Puisque M_1M_2 est un sous-module de type fini de B on peut encore appliquer le lemme. □.

Preuve du Lemme :

$\implies$ Si $\xi^n + a_1\xi^{n-1} + \cdots + a_n = 0$, $a_j \in A$, le module $M = A + \xi A + \cdots \xi^{n-1}A$ a la propriété $\xi M \subset M$.

$\impliedby$ Soit $M = Ae_1 + \cdots Ae_n$. On peut écrire

$$\xi e_j = \sum_{i=1}^{n} A_{ij}e_i, \quad A_{ij} \in A$$

et donc, par algèbre linéaire dans B^n, on a $\det(A_{ij} - \xi I_n) = 0$ ce qui donne le polynôme unitaire $P(X) = \det((A_{ij}) - XI_n) \in A[X]$ tel que $P(\xi) = 0$. □

Les entiers algébriques qu'on utilise le plus souvent sont les **racines unités** : Une N-ième racine d'unité satisfait $X^N = 1$ et est donc un entier algébrique.

Exemple 5.2.6. Soit G un groupe fini et $\chi : G \to \mathbb{C}^\times$ le caractère d'une représentation. Alors pour tout $g \in G$ le nombre $\chi(g)$ est un entier algébrique.

Un moyenne de racines d'unités peut aussi figurer comme entier algébrique, mais on a :

Lemme 5.2.7 (Kronecker)**.** *Un moyenne de racines d'unités ne peut être un entier algébrique que si c'est* 0 *ou bien si tout les racines sont égales.*

Démonstration : La moyenne μ de racines d'unité satisfait $|\mu| \leq 1$ avec égalité si et seulement si les racines sont égales. Dans l'exemple 5.2.2 2) on a vu que les conjugués de μ sont des entiers algébriques. Le produit b de toutes les conjuguées de μ est le coefficient constant du polynôme minimal $Q \in \mathbb{Q}[X]$ de μ et donc b est un nombre rationnel. D'autre part, en tant que produit d'entiers algébriques, c'est un entier algébrique. Donc, par le Lemme 5.2.3, $b \in \mathbb{Z}$. Mais $|b| \leq 1$ et donc $b = 0$ ou bien $b = \pm 1$. Dans le premier cas un des conjuguées de μ est nulle, donc $\mu = 0$; dans dernier cas $|\mu| = 1$ et donc tout les racines doivent être égales. □

Exemple 5.2.8. Soit V un $\mathbb{C}$-espace vectoriel $f \in \mathrm{GL}(V)$ d'ordre fini tel que $\frac{\mathrm{Tr}\, f}{\dim V} \in \overline{\mathbb{Z}}$, i.e. un entier algébrique. Alors f est une homothétie. En effet, les valeurs propres de f sont des racines d'unité et $\frac{\mathrm{Tr}\, f}{\dim V}$ est leur moyenne. Par Kronecker les valeurs propres sont tous égales, i.e. $f = \mu\, \mathrm{id}_V$.

On revient à $Z(G)$. C'est un anneau commutatif contenant $\mathbb{Z} \cdot e_1 \simeq \mathbb{Z}$. Les membres de la base canonique $\{e_c; c \in \mathcal{C}\}$ sont tous des entiers (sur $\mathbb{Z}$) :

Lemme 5.2.9. *Soit G un groupe fini et c une classe de conjugaison, alors $e_c = \sum_{x \in c} x$ est $\mathbb{Z}$–entier.*

Démonstration : Soient $c, d \in \mathcal{C}$. Alors $e_c \cdot e_d$ est une combinaison entière de la base canonique :

$$e_c \cdot e_d = \sum_{x \in \mathcal{C}} n_x^{(e,d)} e_x, \quad n_x^{(e,d)} \in \mathbb{N}.$$

Soit $M = \sum_{x \in \mathcal{C}} \mathbb{Z}e_x$, alors $e_c M \subset M$ et le résultat est une conséquence du Lemme 5.2.5. □

Corollaire 5.2.10. *Soit*

$$c = \sum_{g \in G} \gamma(g) e_g \in Z(G), \quad \text{telle que pour tout } g \in G,\ \gamma(g) \in \bar{\mathbb{Z}},$$

alors c est entier (sur $\mathbb{Z}$).

Démonstration : Puisque $c \in Z(G)$, on a que $c = \sum_{c \in \mathcal{C}} \gamma(g) e_c$ et donc $\mathbb{Z}$–entier. □

5.3 Application

Le but est de montrer :

Théorème 5.3.1. *Soit V une représentation irréductible de G, alors* $\dim V$ *divise l'ordre de G.*

On le déduira de la proposition suivante :

Proposition 5.3.2. *Soit $\rho : G \to \mathrm{GL}(V)$ irréductible et soit χ son caractère et soit*

$$c = \sum_{g \in G} \gamma(g) e_g \in Z(G), \quad \text{avec pour tout } g \in G,\ \gamma(g) \in \bar{\mathbb{Z}}.$$

Alors

$$\frac{1}{\dim V} \sum_{g \in G} \gamma(g) \chi(g) \in \bar{\mathbb{Z}}.$$

Démonstration : Par le Corr. 5.2.10 l'élément c est $\mathbb{Z}$-entier et donc aussi l'image de c sous l'homomorphisme $Z(G) \to \mathbb{C}$ du Corr. 5.1.2 qui est $\frac{1}{\dim V} \sum_{g \in G} \gamma(g)\chi(g)$. □

Preuve du Théorème 5.3.1.. On pose $n = \dim V$. On applique la Proposition avec

$$c := \sum \chi(g^{-1}) e_g \in Z(G)$$

où χ est le caractère de la représentation. Donc

$$\frac{1}{n} \sum_{g \in G} \chi(g^{-1})\chi(g) = \frac{|G|}{n} \in \overline{\mathbb{Z}}.$$

Puisqu'un nombre rationnel et algébriquement entier est entier (Lemme 5.2.3), on a que $\frac{|G|}{n} \in \mathbb{Z}$, i.e. n divise l'ordre du groupe G. □

Corollaire 5.3.3. *Soit $s \in G$ et c_s sa classe de congugaison. On pose $c = \sum_{x \in c_s} x$. Alors pour tout G–représentation irréductible de degré n et de caractère χ, on a*

$$\frac{|c_s|}{n} \chi(s) \in \bar{\mathbb{Z}}.$$

Chapitre 6

Application : le théorème pq de Burnside

6.1 Groupes résolubles et nilpotents

Soit G un groupe. Une **série normale** est une filtration

$$G = G_1 \supset G_2 \supset \cdots G_k \supset G_{k+1} \supset \cdots ,$$

telle que les G_i sont des sous-groupes de G tels que $G_{i+1} \lhd G_i$. On appelle G_i/G_{i+1} les **facteurs** de la série.

Définition 6.1.1. Un groupe G est **résoluble** si G admet une série normale telle que ses facteurs sont abéliens.

On laisse la preuve du résultat suivant au lecteur :

Lemme 6.1.2. *1. Un sous-groupe et un groupe quotient d'un groupe résoluble est résoluble ;*

2. Soit $K \lhd G$ résoluble ainsi que G/K. Alors G est résoluble.

On peut aussi travailler avec la **série dérivée** :

$$G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \cdots , \quad G^{(k+1)} = [G^{(k)}, G^{(k)}].$$

En effet, on a :

Lemme 6.1.3. *G est résoluble si et seulement si la série dérivée se termine.*

Démonstration : $\Longleftarrow$ Les facteurs de la série dérivée sont les abélianisés des $G^{(k)}$.
$\Longrightarrow$: Par récurrence on montre facilement l'inclusion $G^{(i)} \subset G_{i+1}$ et donc si la série normal se termine avec $G_n = \{1\}$, on a $G^{(n-1)} \subset G_n = \{1\}$ et la série dérivée se termine. □

La **série centrale** d'un groupe est construite par récurrence. On pose $Z_0 = \{1\}$, $Z_1 = Z_G$, le centre du groupe G et avec $\pi : G \to G/Z_k$ l'application canonique, on pose

$$Z_{k+1} := \pi^{-1}(Z_{G/Z_k}).$$

Cela donne une filtration de G par des sous-groupes distingués Z_k :

$$1 \subset Z_1 \subset Z_2 \subset \cdots \subset Z_k \subset Z_{k+1} \cdots$$

telle que

$$Z_{k+1}/Z_k = Z_{G/Z_k}.$$

Définition 6.1.4. G est **nilpotent** si la série centrale est finie :

$$\{1\} \subset Z_1 \subset Z_2 \subset \cdots \subset Z_{m-1} \subset Z_m = G.$$

En particulier, G/Z_{m-1} est abélien et donc $G^{(1)} = [G, G] \subset Z_{m-1}$.

Par récurrence on montre que $G^{(k)} \subset Z_{m-k}$ et donc $G^{(m)} \subset Z_0 = \{1\}$. Il suit que :

Lemme 6.1.5. *Un groupe nilpotent est résoluble.*

Exemple 6.1.6. Soit G un p–groupe, i.e. $|G|$ est une puissance d'un premier p. Un tel groupe est nilpotent et donc résoluble. Pour le montrer, on note d'abord que si G est abélien, on a une série centrale simple : $\{1\} \subset Z_G = G$

Sinon, soit c_x la classe de conjugaison de x. On note que $x \in Z_G$ si et seulement si $c_x = \{x\}$. Soit $s \notin Z_G$. Le centralisateur $Z(s)$ de s est distinct de G. Puisque $|C_s| = \frac{|G|}{|Z(s)|}$ on déduit que $|C_s|$ est divisible par p. Puisque

$$|G| = |Z_G| + \sum_{s \notin Z_G} |c_s|,$$

on en déduit que $|Z_G|$ est divisible par p et donc n'est pas trivial. Donc on peut appliquer récurrence à Z_G.

6.2 Le théorème de Burnside

Théorème 6.2.1. *Soit G un groupe d'ordre $p^a q^b$. Alors, G est résoluble.*

Démonstration : D'abord, par l'exemple 6.1.6 on peut supposer que $a, b \geq 1$. Il suffit de montrer qu'un tel G n'est pas simple : un sous-groupe distingué N propre de G est résoluble par récurrence ainsi que G/N et on appliquera le Lemme 6.1.2.

Supposons donc que G simple. On arivera à une contradiction. Par Sylow il existe un sous-groupe $H \subset G$ d'ordre q^b. Par l'exemple 6.1.6 c'est un groupe nilpotent et en particulier $Z_H \neq \{1\}$. Soit $s \in Z_H$, $s \neq 1$. Par définition de s, $Z_G(s)$ contient H et donc

$$|c_s| = \frac{|G|}{|Z_G(s)|} = p^\gamma, \quad 1 \leq \gamma \leq a.$$

Le fait que $\gamma = 0$ est exclu vient du fait qu'alors $Z_G(s) = G$ et donc le groupe cyclique N engendré par s serait un sous-groupe propre et distingué dans G, contrairement à l'hypothèse que G soit simple.
Conclusion : $|c_s|$ est divisible par p.

On considère les caractères des représentations irréductibles de G. Puisque G est simple, seulement le caractère identité est un caractère multiplicatif et donc pour les autres $\chi(1) = n \geq 2$.
Si $\chi(s) \neq 0$, on a $\gcd(|c_s|, n) \neq 1$, i.e. p divise n le degré de la représentation.
Démonstration : Si $\gcd(|c_s|, n) = 1$ du fait que par la Cor. 5.3.3 on a

$$\frac{|c_s|}{n}\chi(s) \in \bar{\mathbb{Z}}$$

aussi $\frac{1}{n}\chi(s) \in \bar{\mathbb{Z}}$; en fait $\exists x, y \in \mathbb{Z}$ tels que $x|c_s| + yn = 1$ et donc $\frac{1}{n}\chi(s) = x\frac{|c_s|}{n}\chi(s) + y\chi(s) \in \bar{\mathbb{Z}}$. Donc, si $\rho : G \to \mathrm{GL}(V)$ est la représentation irréductible associée à χ, par l' Exemple 5.2.8, on a que ρ_s est une homothétie $\neq \mathrm{id}_V$ (car ρ est fidèle – sinon $\ker \rho$ était un sous-groupe distingué non-triviale) et donc $s \in Z_G = \{1\}$, contradiction. □

Maintenant on peut finir la preuve que l'hypothèse G simple donne une contradiction : On applique nos considérations à la représentation régulière avec caractère χ_R :

$$0 = \chi_R(s) = 1 + \sum_{\chi \neq 1} n\chi(s) = 1 + p(\text{entier algébrique } \xi)$$

où on somme sur les caractères *irréductibles* $\chi \neq 1$. On déduit que $\xi = -1/p \in \overline{\mathbb{Z}}$ et donc on obtient la contradiction par le Lemme 5.2.3. □