6. Propriétés d'intégralité des caractères

DÉFINITION 6.1. *(Dedekind) Un entier algébrique est un nombre complexe annulé par un polynôme* unitaire *à coefficients entiers. On note* $\overline{\mathbb{Z}} \subset \mathbb{C}$ *l'ensemble des entiers algébriques.*

En particulier, un entier algébrique est un nombre algébrique. Par exemple, les complexes $\sqrt{N}$ et $e^{2i\pi/N}$ pour $N \in \mathbb{Z}$, les entiers usuels, ou encore tout $x \in \mathbb{C}$ tel que $x^3 = x + 1$, sont des entiers algébriques. On peut dire que les entiers algébriques sont aux nombres algébriques ce que les entiers sont aux nombres rationnels. La proposition suivante, classique à sa formulation près, en est un premier indicateur.

PROPOSITION 6.2. *Les entiers algébriques qui sont rationnels sont dans* $\mathbb{Z}$*. Autrement dit, on a* $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$*.*

DÉMONSTRATION — C'est le fait bien connu que si le rationnel p/q, avec $(p, q) = 1$, est racine d'un polynôme $P \in \mathbb{Z}[X]$, alors q divise le coefficient dominant de P, comme on le voit en regardant l'égalité $q^n P(p/q) = 0$ avec $n = \deg(P)$. Si P est unitaire, on a donc $q = \pm 1$, puis $p/q \in \mathbb{Z}$. □

PROPOSITION 6.3. $\overline{\mathbb{Z}}$ *est un sous-anneau de* $\mathbb{C}$*.*

Observons cependant que $\overline{\mathbb{Z}}$ n'est pas un sous-corps de $\mathbb{C}$. En effet, on a $1/N \notin \overline{\mathbb{Z}}$ pour $N \geqslant 2$ d'après la proposition précédente. Pour démontrer la Proposition 6.3, nous aurons besoin du critère d'intégralité suivant.

PROPOSITION 6.4. *Soit* R *un anneau de groupe additif (abélien) de type fini et sans torsion.*[5] *Alors pour tout* $x \in R$ *il existe* $P \in \mathbb{Z}[X]$ *unitaire tel que* $P(x) = 0$*.*

DÉMONSTRATION — Un groupe abélien de type fini sans torsion est libre. Pour $x \in R$, on considère l'application $\mathbb{Z}$-linéaire $\mathrm{m}_x : R \to R, r \mapsto xr$, de multiplication par x. Comme R est un $\mathbb{Z}$-module libre de rang fini, on sait que la donnée d'une $\mathbb{Z}$-base à n éléments $e_1, \ldots, e_n$ de R identifie l'anneau $\mathrm{End}_{\mathbb{Z}}(R)$ à $\mathrm{M}_n(\mathbb{Z})$. Concrètement, on a $xe_j = \sum_{i=1}^n m_{i,j} e_i$ pour des uniques $m_{i,j} \in \mathbb{Z}$, et on a

$$\mathrm{Mat}_e \mathrm{m}_x = (m_{i,j}) \in \mathrm{M}_n(\mathbb{Z}).$$

Mais toute matrice dans $\mathrm{M}_n(\mathbb{Z})$ est annulée par un polynôme unitaire à coefficients entiers : son polynôme caractéristique. Si P est celui de $\mathrm{Mat}_e \mathrm{m}_x$, on a donc $P(\mathrm{m}_x) = 0 = \mathrm{m}_{P(x)}$ et donc $P(x)1 = P(x) = 0$ dans R. □

DÉMONSTRATION — (de la Proposition 6.3) Soient $x, y \in \overline{\mathbb{Z}}$. Supposons x et y annulés par des polynômes dans $\mathbb{Z}[X]$ unitaires de degrés respectifs m et n. On a donc $x^m \in X := \sum_{i=0}^{m-1} \mathbb{Z} x^i$ et $y^n \in Y := \sum_{j=0}^{n-1} \mathbb{Z} y^j$. On en déduit $x^a \in X$ et $y^b \in Y$ pour tout $a, b \geqslant 0$. Il en résulte que $R := \sum_{0 \leqslant i < m, 0 \leqslant j < n} \mathbb{Z} x^i y^j$ est un sous-anneau de $\mathbb{C}$. Mais le groupe additif de R de type fini, et sans torsion car $R \subset \mathbb{C}$. La Proposition 6.4 entraîne $R \subset \overline{\mathbb{Z}}$. On conclut car on a xy et $x \pm y \in R$. □

5. L'hypothèse « sans torsion » n'est pas nécessaire mais simplifie quelque peu l'argument.

La proposition 6.3 permet de vérifier que certains nombres algébriques ne sont pas des entiers algébriques. Par exemple $x = \frac{1+\sqrt{3}}{2}$ est un nombre algébrique, satisfaisant $x^2 - x - 1/2 = 0$. Si x était entier algébrique, il en serait de même de $x^2 - x = 1/2$, ce qui n'est pas. Mentionnons tout de même qu'il ne faut pas toujours se fier aux apparences : le nombre d'or $\phi = \frac{1+\sqrt{5}}{2}$ est un entier algébrique, car on a $\phi^2 = \phi + 1$.

Retournons aux caractères des groupes finis. On fixe désormais G un groupe fini. La première observation est la suivante.

PROPOSITION 6.5. *Pour tout caractère χ de G, et tout $g \in G$, on a $\chi(g) \in \overline{\mathbb{Z}}$.*

DÉMONSTRATION — En effet, on sait que $\chi(g)$ est une somme finie de racines de l'unité (Proposition 4.8). Mais toute racine n-ème de l'unité est dans $\overline{\mathbb{Z}}$, car annulée par $X^n - 1$. On conclut par la Proposition 6.3. □

Le résultat clé est le suivant, car un quotient n'a pas tendance à être entier :

PROPOSITION 6.6. (Frobenius) *Pour tout $\chi \in \operatorname{Irr} G$, de dimension $n = \chi(1)$, et tout $g \in G$, on a*

$$\frac{1}{n} \, |\mathrm{Conj}(g)| \, \chi(g) \in \overline{\mathbb{Z}}.$$

DÉMONSTRATION — (Démonstration de Burnside) En effet notons $\mathbb{Z}[G] \subset \mathbb{C}[G]$ le sous-groupe $\oplus_{g \in G} \mathbb{Z} g$. C'est clairement un sous-anneau, et il est libre de rang $|G|$ comme $\mathbb{Z}$-module, avec pour base les $g \in G$. D'après la Proposition 6.4, tout élément de $\mathbb{Z}[G]$ est donc annulé par un polynôme unitaire à coefficients entiers.

Soit $C \subset G$ la classe de conjugaison de g. L'élément $z = \sum_{h \in C} h$ est dans $\mathbb{Z}[G] \cap \mathrm{Z}(\mathbb{C}[G])$ par le Lemme 4.22 (i). Par le paragraphe précédent, il est annulé par un polynôme unitaire $P \in \mathbb{Z}[X]$. Mais par le Lemme 4.22 (i), on sait aussi que z agit sur tout $\mathbb{C}[G]$-module irréductible S par l'homothétie de rapport

$$\lambda_S(z) \; = \; \frac{1}{\dim S} \, |C| \, \chi_S(g).$$

Mais on a clairement $\lambda_S(Q(z)) = Q(\lambda_S(z))$ pour tout $Q \in \mathbb{C}[X]$, car $\lambda_S : \mathrm{Z}(\mathbb{C}[G]) \to \mathbb{C}$ est un morphisme de $\mathbb{C}$-algèbres. De $P(z) = 0$ on déduit donc $P(\lambda_S(z)) = 0$, c'est-à-dire $\lambda_S(z) \in \overline{\mathbb{Z}}$. On conclut en posant $\chi = \chi_V$. □

En guise d'application de cette propriété, montrons le théorème suivant.

THÉORÈME 6.7. (Frobenius) Soit V un $\mathbb{C}[G]$-module irréductible de dimension finie. Alors $\dim V$ divise $|G|$.

DÉMONSTRATION — Si $g_1, \ldots, g_h$ sont des représentants des classes de conjugaison de G, la relation d'orthogonalité $\langle \chi_V, \chi_V \rangle = 1$ montre

$$\frac{|G|}{\dim V} = \frac{|G|}{\dim V} \langle \chi_V, \chi_V \rangle = \sum_{i=1}^{h} \left(\frac{1}{\dim V} \, |\mathrm{Conj}(g_i)| \, \chi_V(g_i) \right) \, \overline{\chi_V(g_i)}.$$

D'après les Propositions 6.3, 6.5 et 6.6, cet élément est dans $\overline{\mathbb{Z}}$. (Il est clair que $\overline{\mathbb{Z}}$ est stable par conjugaison complexe). On conclut par la Proposition 6.2. □

EXEMPLE 6.8. Si G est d'ordre pq avec p, q premiers et $p \leqslant q$. Les représentations irréductibles de G sont de degré 1 ou p. En effet, celles de degré $n > 1$ vérifient $n^2 < |G| = pq$ et $n \mid pq$.

EXEMPLE 6.9. Soit G un p-groupe non abélien d'ordre p^3, par exemple le groupe de Heisenberg $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$. Alors les représentations irréductibles de G sont de dimension p^n avec $n \leqslant 3$. Mais $p^{2n} \leqslant |G| = p^3$ implique $n \leqslant 1$. Donc les seules dimensions possibles sont 1 et p. En fait, le centre Z de G est nécessairement cyclique d'ordre p (il est non trivial, et G/Z n'est pas cyclique), donc G/Z est d'ordre p^2, et donc abélien. On en déduit $\mathrm{D}(G) = Z$, puis que G a exactement $|G/Z| = p^2$ caractères de degré 1. La formule $p^3 = p^2 + p^2(p-1)$ montre qu'il y a exactement $p-1$ caractères irréductibles de degré p.

Comme nous le verrons dans le Complément § 9, Burnside a donné d'autres applications frappantes de ces idées !

7. Complément I : Retour sur le déterminant d'un groupe

Revenons, comme promis, sur la question de Dedekind consistant à factoriser le déterminant

$$\det G \;=\; \det(X_{gh^{-1}})_{g,h\in G}$$

d'un groupe fini G, introduit au §2 Chap. 3. C'est manifestement un polynôme homogène de degré $|G|$ à coefficients dans $\mathbb{Z}$ en les indéterminées X_g indexées par les éléments de G. Notons $\mathbb{C}[X_G]$ l'anneau de polynômes $\mathbb{C}[\{X_g\}_{g\in G}]$ en ces $|G|$ variables et à coefficients *complexes*.

THÉORÈME 7.1. (Frobenius) *Si G est un groupe fini, et si $n_1,\dots,n_h$ sont les dimensions des h caractères irréductibles de G, alors on a une décomposition*

$$\det G = \prod_{i=1}^{h} F_i^{n_i}$$

où les F_i sont des polynômes irréductibles, homogènes de degré n_i, en les X_g, et 2 à 2 non associés.

Pour cela, associons à chaque $\mathbb{C}[G]$-module de dimension finie V un polynôme $\mathrm{D}_V \in \mathbb{C}[X_G]$ en posant, pour tout $|G|$-uple $x_G = (x_1,\dots,x_g,\dots)\in\mathbb{C}^G$,

$$\mathrm{D}_V(x_G) \;:=\; \det\Big(\sum_{g\in G} x_g\,\rho_V(g)\Big).$$

Ce polynôme D_V est manifestement homogène de degré $\dim V$, et ne dépend que de la classe d'isomorphisme de V. De plus, on a

$$\mathrm{D}_{V\oplus U} = \mathrm{D}_V\mathrm{D}_U.$$

EXEMPLE 7.2. Si V est de dimension 1, de caractère de degré 1 associé $\chi : G\to\mathbb{C}^\times$, on a clairement $\mathrm{D}_V = \sum_{g\in G}\chi(g)\mathrm{X}_g$.

EXEMPLE 7.3. Considérons $V=\mathbb{C}^3$ la représentation de permutation standard de $G=\mathrm{S}_3$. On a vu $V=\mathbb{C}\oplus H$ avec H irréductible. Posant $E=X_1$, $T_1=X_{(23)}$, $T_2=X_{(13)}$, $T_3=X_{(12)}$, $C_1=X_{(1\,2\,3)}$ et $C_2=X_{(1\,3\,2)}$ on constate

$$\det\begin{bmatrix} E+T_1 & T_3+C_2 & T_2+C_1\\ T_3+C_1 & E+T_2 & T_1+C_3\\ T_2+C_2 & T_1+C_1 & E+T_3\end{bmatrix} = \mathrm{D}_V = (E+T_1+T_2+T_3+C_1+C_2)\,\mathrm{D}_H.$$

En se plaçant dans la base e_1-e_2, e_2-e_3 de H, on vérifierait (exercice !)

$$\mathrm{D}_H = \det\begin{bmatrix} E+T_1-T_3+C_2 & -T_2+T_3-C_1+C_2\\ T_1-T_2+C_1-C_2 & E-T_1+T_3-C_1\end{bmatrix}.$$

On a donc $\det\mathrm{S}_3 = \mathrm{D}_1\mathrm{D}_\varepsilon\mathrm{D}_H^2$ (Théorème 7.1 et Table 2).

EXEMPLE 7.4. Pour $V=\mathbb{C}\,G$ (représentation régulière), on constate

$$\mathrm{D}_{\mathbb{C}G} = \det G. \tag{72}$$

En effet, soit $z=\sum_{g\in G}x_g g\in\mathbb{C}[G]$. Pout $h\in G\subset\mathbb{C}\,G$ on constate $zh=\sum_{g\in G}x_g\,gh = \sum_{g\in G}x_{gh^{-1}}g$, de sorte que la matrice de la multiplication par z dans la base canonique de $\mathbb{C}\,G$, est $(x_{gh^{-1}})_{g,h\in G}$.

L'exemple précédent indique clairement la marche à suivre pour démontrer le théorème. D'après le Corollaire 4.18, on a aussi une décomposition

$$\mathbb{C}\,G \simeq \oplus_{i=1}^{h} S_i^{\oplus n_i}$$

où S_i est un $\mathbb{C}[G]$-module irréductible de dimension n_i, non isomorphe à S_j pour $j \neq i$. On en déduit

$$\det G = \prod_{i=1}^{h} \mathrm{D}_{S_i}^{n_i}.$$

Posant $F_i = \mathrm{D}_{S_i}$, le Théorème 7.1 découle du lemme suivant.

LEMME 7.5. *Soient U et V deux $\mathbb{C}[G]$-modules irréductibles.*

(i) Le polynôme D_U est irréductible dans $\mathbb{C}[X_G]$.

(ii) Si U est V sont non isomorphes, alors D_U et D_V sont non proportionnels.

L'ingrédient restant pour prouver ce lemme est le théorème important suivant. Si V est un $\mathbb{C}[G]$-module, on dispose d'un morphisme de $\mathbb{C}$-algèbres naturel

$$\pi_U : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V),\ x \mapsto (v \mapsto x.v).$$

THÉORÈME 7.6. *Soit G un groupe fini.*

(i) (Burnside) *Si V est un $\mathbb{C}[G]$-module irréductible, alors π_V est surjectif. Autrement dit, les $\rho_V(g)$ avec $g \in G$ engendrent $\mathbb{C}$-linéairement $\mathrm{End}_{\mathbb{C}}(V)$.*

(ii) (Maschke) *Si $S_1, \ldots, S_h$ sont "les" $\mathbb{C}[G]$-modules irréductibles de G, deux à deux non isomorphes, alors le morphisme de $\mathbb{C}$-algèbres*

$$\pi : \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(S_1) \times \mathrm{End}_{\mathbb{C}}(S_2) \times \cdots \times \mathrm{End}_{\mathbb{C}}(S_h),$$

$$x \mapsto (\pi_{S_1}(x), \pi_{S_2}(x), \ldots, \pi_{S_h}(x)),$$

est un isomorphisme.

DÉMONSTRATION — Le morphisme π est injectif ! En effet, si on a $z \in \mathbb{C}[G]$ avec $\pi(z) = 0$, alors l'élément z agit par 0 dans tout $\mathbb{C}[G]$-module irréductible, puis donc par Maschke dans tout $\mathbb{C}[G]$-module de dimension finie. Dans le cas de la représentation régulière, on a $z.1 = z$ et donc $z = 0$. (On a déjà rencontré cet argument dans la démonstration du Théorème 4.20). Mais on a

$$\dim \mathbb{C}G = \sum_{i=1}^{h} (\dim S_i)^2 = \dim \prod_{i=1}^{h} \mathrm{End}_{\mathbb{C}}(V_i),$$

de sorte que l'injectivité de π implique sa bijectivité, d'où le (ii). En particulier, pour tout $i = 1, \ldots, h$ on a $\mathrm{Im}\,\pi_i = \mathrm{End}_{\mathbb{C}}(S_i)$, ce qui démontre le (i). □

REMARQUE 7.7. En particulier, on a montré qu'il existe un isomorphisme de $\mathbb{C}$-algèbres $\mathbb{C}[G] \xrightarrow{\sim} \prod_{i=1}^{h} \mathrm{M}_{n_i}(\mathbb{C})$, où les n_i sont les dimensions des représentations irréductibles de G. Mentionnons aussi que le Théorème de Burnside vaut encore (par une preuve différente) si G est quelconque (pas forcément fini) et si $\mathbb{C}$ est remplacé par un corps algébriquement clos quelconque.

Nous pouvons enfin démontrer le Lemme 7.5 (et donc le Théorème 7.1).

DÉMONSTRATION — (Preuve du Lemme 7.5). Montrons d'abord l'assertion (ii). Soient U et V deux $\mathbb{C}[G]$-modules irréductibles non isomorphes. D'après le Théorème 7.6 (ii), il existe $z \in \mathbb{C}[G]$ tel que $\pi_U(z) = \mathrm{Id}_U$ et $\pi_V(z) = 0$. Écrivons $z = \sum_{g\in G} x_g g$ et posons $x = (x_g)_{g\in G} \in \mathbb{C}^G$. Alors on a $\mathrm{D}_U(x) = \det \pi_U(x) = 1$ et $\mathrm{D}_V(x) = \det \pi_V(x) = 0$. Cela montre le (ii).

Montrons mainenant le (i). On fixe une base $e = (e_1, \dots, e_n)$ de V et on pose $\mathrm{Mat}_e \rho_V(g) = (m_{i,j}(g))_{1\leqslant i,j\leqslant n}$. Les n^2 formes linéaires

$$\mathrm{L}_{i,j} : \mathbb{C}^G \to \mathbb{C}, (x_g)_{g\in G} \mapsto \sum_{g\in G} x_g\, m_{i,j}(g),$$

sont linéairement indépendantes d'après le Théorème 7.6 (i). On les complète arbitrairement en une base du dual de $\mathbb{C}^G$, en ajoutant $\mathrm{L}_1, \dots, \mathrm{L}_r$ (avec $r = |G| - n^2$). Dans ces nouvelles variables linéaires, on a donc $\mathbb{C}[X_G] = \mathbb{C}[\{\mathrm{L}_{i,j}\}_{i,j}][\mathrm{L}_1, \dots, \mathrm{L}_r]$. Mais par définition, on a aussi

$$\mathrm{D}_V = \det((\mathrm{L}_{i,j})_{1\leqslant i,j\leqslant n}).$$

On conclut par le fait, classique !, que le déterminant de la matrice $(\mathrm{T}_{i,j})_{1\leqslant i,j\leqslant n}$ (à coefficients indéterminées) est irréductible dans $\mathbb{C}[\{\mathrm{T}_{i,j}\}_{1\leqslant i,j\leqslant n}]$: voir l'Exercice 9.32. □

8. Complément II : Décomposition à la Fourier de $\mathrm{L}^2(G)$

Soit G un groupe fini. Le groupe G admet une représentation $\mathbb{C}$-linéaire naturelle sur $\mathrm{L}^2(G)$ par translations à droite, que nous avions noté $(g, f) \mapsto \mathrm{R}_g(f)$ au Chapitre 3. Nous avions aussi vu que cette représentation est *unitaire* relativement au produit scalaire $\langle -, - \rangle$ de $\mathrm{L}^2(G)$, c'est à dire que l'on a

$$\langle \mathrm{R}_g(f), \mathrm{R}_g(f') \rangle = \langle f, f' \rangle \tag{73}$$

pour tout $g \in G$ et tout $f, f' \in \mathrm{L}^2(G)$. On se propose dans cette partie d'étudier la décomposition en irréductibles de la représentation $\mathrm{L}^2(G)$.

LEMME 8.1. *L'application* $\mathrm{L}^2(G) \to \mathbb{C}[G]$, $f \mapsto \sum_{g\in G} f(g^{-1})g$ *et un isomorphisme de* $\mathbb{C}[G]$*-modules.*

DÉMONSTRATION — L'application ψ de l'énoncé est clairement un isomorphisme de $\mathbb{C}$-espace vectoriel. Il ne reste qu'à voir que pour $h \in G$ et $f \in \mathrm{L}^2(G)$ on a $\psi(\mathrm{R}_h(f)) = h\psi(f)$. On conclut car par changement de variables $g \mapsto hg$ on a

$$\psi(\mathrm{R}_h(f)) = \sum_{g\in G} \mathrm{R}_h(f)(g^{-1})g = \sum_{g\in G} f(g^{-1}h)g = \sum_{g\in G} f(g^{-1})hg = h\psi(f).$$

□

D'après le Corollaire 4.18, on en déduit que toute représentation irréductible U de G intervient dans $\mathrm{L}^2(G)$ avec une multiplicité $\dim U$. Nous allons raffiner ce résultat en identifiant concrètement les composantes isotypiques de $\mathrm{L}^2(G)$. La notion clé est celle de *coefficient matriciel*.

DÉFINITION 8.2. *Soit U un $\mathbb{C}[G]$-module de dimension finie. Pour $u \in U$ et $\varphi \in U^*$, on pose $\mathrm{c}_{u,\varphi} : G \to \mathbb{C}, g \mapsto \varphi(g.u)$. Une application $G \to \mathbb{C}$ de cette forme s'appelle un* coefficient matriciel *de U. On note* $\mathrm{Coeff}(U) \subset \mathrm{L}^2(G)$ *le sous-espace vectoriel engendré par les coefficients matriciels de U.*

Par exemple, si l'on choisit une base $e = (e_1, \ldots, e_n)$ de U, et si l'on pose

$$\mathrm{Mat}_e\, \rho_U(g) \;=\; (\, m_{i,j}(g)\,)_{1 \leqslant i,j \leqslant n} \in \mathrm{GL}_n(\mathbb{C}),$$

alors pour tout $1 \leqslant i, j \leqslant n$ l'application $G \mapsto \mathbb{C}, g \mapsto m_{i,j}(g)$, est un coefficient matriciel de U. En effet, on a $m_{i,j} = \mathrm{c}_{e_i, e_j^\star}$ où les $e_i^\star \in U^\star$ désignent la base duale de e_i. Cela explique la terminologie. Comme l'application

$$U \times U^\vee \to \mathrm{L}^2(G), (u, \varphi) \mapsto \mathrm{c}_{u,\varphi}, \tag{74}$$

est manifestement $\mathbb{C}$-bilinéaire, on en déduit

$$\mathrm{Coeff}(U) \;=\; \sum_{1 \leqslant i,j \leqslant n} \mathbb{C}\, m_{i,j}. \tag{75}$$

Par exemple, le caractère $\chi_U = \sum_{i=1}^n m_{i,i}$ est une somme de coefficients matriciels, et on a $\chi_U \in \mathrm{Coeff}(U)$. Comme deux représentation isomorphes ont même représentations matricielles associés dans des bases convenables, on en déduit aussi que *le sous-espace* $\mathrm{Coeff}(U)$ *de* $\mathrm{L}^2(G)$ *ne dépend que de la classe d'isomorphisme de U.*

LEMME 8.3. *Soit U un $\mathbb{C}[G]$-module de dimension finie. Le sous-espace* $\mathrm{Coeff}(U)$ *de* $\mathrm{L}^2(G)$ *est un sous-$\mathbb{C}[G]$ module stable par les translations à gauche par G.*

La translation à gauche par $g \in G$ est définie par $\mathrm{L}_g(f)(h) = f(g^{-1}h)$.

DÉMONSTRATION — Pour $g, h \in H$, $u \in U$ et $\varphi \in U^\vee$ on constate

$$\mathrm{R}_h(\mathrm{c}_{u,\varphi})(g) = \varphi(ghu) = \mathrm{c}_{hu,\varphi}(g) \tag{76}$$

et donc $\mathrm{R}_h(\mathrm{c}_{u,\varphi}) = \mathrm{c}_{hu,\varphi}$. Un calcul similaire montre $\mathrm{L}_h(\mathrm{c}_{u,\varphi}) = \mathrm{c}_{u,h.\varphi}$. Cela montre que $\mathrm{Coeff}(U)$ est G-stable dans $\mathrm{L}^2(G)$, stable également par les translations à gauche. □

LEMME 8.4. *Si U est un $\mathbb{C}[G]$-module irréductible, alors* $\mathrm{Coeff}(U)$ *coïncide avec la composante U-isotypique de* $\mathrm{L}^2(G)$.

DÉMONSTRATION — À $\varphi \in V^*$ fixé, l'application $U \to \mathrm{L}^2(G)$, $u \mapsto \mathrm{c}_{u,\varphi}$, qui est $\mathbb{C}$-linéaire par bilinéarité de (74), est $\mathbb{C}[G]$-linéaire par la Formule (76). En particulier, si U est irréductible, chaque $\mathrm{c}_{u,\varphi}$ non nul engendre une sous-représentation de $\mathrm{L}^2(G)$ isomorphe à U. Cela implique que $\mathrm{Coeff}(U)$ est inclus dans la composante isotypique de U dans $\mathrm{L}^2(G)$.

Réciproquement, soit $V \subset \mathrm{L}^2(G)$ une sous-représentation (irréductible) isomorphe à U. Montrons qu'elle est incluse dans $\mathrm{Coeff}(U)$. Soit $\phi \in V$ non nulle. Il existe $x \in G$ tel que $\phi(x) \neq 0$. Considérons la forme linéaire $\varphi : \mathrm{L}^2(G) \to \mathbb{C}, f \mapsto f(x)$. Alors $\mathrm{c}_{\phi,\varphi} : G \mapsto \mathbb{C}, g \mapsto \phi(xg)$ est dans $\mathrm{Coeff}(S)$. Mais on a

$\mathrm{Coeff}(S) = \mathrm{Coeff}(U)$ car U et S sont isomorphes. Ainsi $\mathrm{L}_x \mathrm{c}_{\phi,x.\varphi} = \phi$ est aussi dans $\mathrm{Coeff}(U)$, puis $S = \mathbb{C}[G].\phi \subset \mathrm{Coeff}(U)$, par le Lemme 8.4. □

Le résultat principal est alors le suivant :

THÉORÈME 8.5. *Soient $S_1, \ldots, S_h$ des représentants des classes d'isomorphisme de $\mathbb{C}[G]$-modules irréductibles. On a une décomposition orthogonale*

$$\mathrm{L}^2(G) = \bigoplus_{1 \leqslant i \leqslant h}^{\perp} \mathrm{Coeff}(S_i),$$

ainsi que l'égalité $\dim \mathrm{Coeff}(S_i) = (\dim S_i)^2$ *pour tout* $i = 1, \ldots, h$.

DÉMONSTRATION — Par unitarité (73), on peut écrire $\mathrm{L}^2(G)$ comme somme directe *orthogonale* de sous-représentations irréductibles. En regroupant entre eux les facteurs isomorphes, on en déduit une décomposition

$$\mathrm{L}^2(G) = \bigoplus_{1 \leqslant i \leqslant h}^{\perp} U_i.$$

où U_i est une somme directe de sous-représentations irréductibles isomorphes à S_i. D'après la Proposition 3.14, U_i est la composante isotypique de S_i dans $\mathrm{L}^2(G)$. D'après le Lemme 8.4, on a donc $U_i = \mathrm{Coeff}(S_i)$. D'après le Lemme 8.1 et le Corollaire 4.18, on a $U_i \simeq S_i^{\oplus \dim S_i}$, et en particulier, $\dim U_i = (\dim S_i)^2$. □

REMARQUE 8.6. La Formule montre que l'égalité $\dim \mathrm{Coeff}(U) = (\dim U)^2$ est équivalente à dire que les n^2 fonctions $m_{i,j} : G \to \mathbb{C}$ *loc. cit.* sont $\mathbb{C}$-linéairement indépendantes, ou encore que les $\rho_U(g)$ avec $g \in G$ engendrent linéairement $\mathrm{End}_{\mathbb{C}}(U)$. Cela donne une autre démonstration du Théorème 7.6.

9. Complément III : Des théorèmes de Burnside et P. Hall

Le résultat suivant est connu pour être l'une des premières applications spectaculaires de la théorie des caractères à la structure des groupes finis.

THÉORÈME 9.1. (Burnside, 1904) *Soit G un groupe fini d'ordre $p^a\, q^b$ avec p, q des nombres premiers et $a, b \in \mathbb{Z}_{\geqslant 0}$. Alors G est résoluble.*

La démonstration qui suit est celle de Burnside. Il a fallu attendre 1972 pour que H. Bender [6] en donne une seconde démonstration (pas franchement plus simple) n'utilisant pas la théorie des caractères. La démonstration de Burnside repose sur le résultat suivant, aussi dû à Burnside.

THÉORÈME 9.2. (Burnside) *Soit G un groupe fini possédant une classe de conjugaison de cardinal p^n avec p premier et $n \geqslant 1$. Alors G n'est pas simple.*

DÉMONSTRATION — (Théorème 9.2 $\Longrightarrow$ Théorème 9.1) On raisonne par récurrence sur $|G|$. Il suffit de montrer que G n'est pas simple. En effet, si H est un sous-groupe distingué de G distinct de 1 et G, alors H et G/H sont d'ordre $p^{a'} q^{b'} < |G|$, et donc résolubles par récurrence, ainsi donc que G par la Proposition 8.7 Chap. 4.

6. *A group theoretic proof of Bunside's $p^a q^b$ theorem*, Math. Z. (1972).

On peut supposer $p \neq q$, ainsi que $a, b \geqslant 1$, car un p-groupe non abélien n'est pas simple (par exemple, son centre est non trivial). Soit $g \in G$ non central. On sait que $|\mathrm{Conj}\, g| > 1$ est un diviseur de $|G|$. Par le Théorème 9.2, on peut supposer que $|\mathrm{Conj}\, g|$ est multiple de pq pour tout $g \neq 1$, car sinon G est simple.

Écrivons alors l'équation aux classes pour l'action de conjugaison de G sur lui-même. On a $|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{s} |\mathrm{Conj}\, g_i|$, où $g_1, \ldots, g_s$ sont des représentants des classes de conjugaisons non centrales de G. Alors pq divise $|\mathrm{Conj}\, g_i|$ pour tout $i = 1, \ldots, s$, et donc pq divise $\mathrm{Z}(G)$, et $\mathrm{Z}(G) \neq \{1\}$: G n'est pas simple. □

Pour démontrer le Théorème 9.2, nous aurons besoin du lemme d'arithmétique suivant.

LEMME 9.3. *Soient $\lambda_1, \ldots, \lambda_n \in \mathbb{C}^\times$ des racines de l'unité. On suppose que $\frac{1}{n}(\lambda_1 + \cdots + \lambda_n)$ est non nul et dans $\overline{\mathbb{Z}}$. Alors tous les λ_i sont égaux.*

DÉMONSTRATION — Ce lemme admet une démonstration assez limpide lorsqu'on dispose d'un peu de théorie des corps (voir le cours d'Algèbre 2 !). Pour être complet nous en donnerons une démonstration directe, mais un peu technique, à la fin de cette section. □

DÉMONSTRATION — (du Théorème 9.2) Soit g avec $|\mathrm{Conj}(g)| = p^n$ comme dans l'énoncé. La seconde relation d'orthogonalité (entre 1 et g) s'écrit

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

Comme $1/p$ n'est pas dans $\overline{\mathbb{Z}}$, on en déduit qu'il existe $\chi \neq 1$ tel que

$$\frac{1}{p}\chi(1)\chi(g) \notin \overline{\mathbb{Z}}.$$

En particulier, p ne divise par $\chi(1)$, et $\chi(g)$ est non nul. Mais d'autre part, on sait que $\frac{1}{\chi(1)}|\mathrm{Conj}(g)|\,\chi(g)$ est dans $\overline{\mathbb{Z}}$. Comme $\chi(1)$ est premier à $p^n = |\mathrm{Conj}(g)|$, on a

$$\frac{\chi(g)}{\chi(1)} \in \overline{\mathbb{Z}}. \tag{77}$$

En effet, soient $a, b \in \mathbb{Z}$ avec $a\chi(1) + b|\mathrm{Conj}(g)| = 1$ (Bezout). On a alors $\frac{\chi(g)}{\chi(1)} = a\chi(g) + b\frac{1}{\chi(1)}|\mathrm{Conj}(g)|\,\chi(g) \in \overline{\mathbb{Z}}$ par les Propositions 6.5 et 6.6.

Soit $\rho : G \to \mathrm{GL}(V)$ une représentation irréductible de caractère χ. D'après le Lemme 9.3 (et la Proposition 4.8), la relation (77) implique que $\rho(g)$ a toutes ses valeurs propres égales : c'est une homothétie. Comme les homothéties forment un sous-groupe distingué de $\mathrm{GL}(V)$, $H := \rho^{-1}(\mathbb{C}^\times \mathrm{id}_V)$ est un sous-groupe distingué de G contenant g, donc non trivial. Si G est simple, on a $H = G$, *i.e.* $\rho(H) \subset \mathbb{C}^\times \mathrm{id}_V$, puis $\dim V = 1$ par irréductibilité de V. Ainsi χ est un caractère non trivial de degré 1. Si G est simple, le morphisme $\chi : G \to \mathbb{C}^\times$ est injectif, et donc G est abélien, ce qui contredit l'existence d'une classe de conjugaison à > 1 éléments. □

Le théorème de Burnside admet la généralisation suivante, que nous avions simplement énoncé au Chapitre 6 (Théorème 4.4).

THÉORÈME 9.4. (P. Hall) *Soit G un groupe fini. On suppose que pour tout diviseur n de $|G|$ tel que n et $|G|/n$ sont premiers entre eux, G possède un sous-groupe d'ordre n. Alors G est résoluble*

Reformulons l'hypothèse. Notons $\Pi(G)$ l'ensemble des diviseurs premiers distincts de $|G|$, de sorte que l'on a $|G| = \prod_{p\in\Pi(G)} p^{v_p}$. L'hypothèse du Théorème ci-dessus est que pour tout sous ensemble fini $\pi \subset \Pi(G)$, le groupe G possède un sous-groupe d'ordre $\prod_{p\in\pi} p^{v_p}$. Un tel sous-groupe s'appelle un *π-sous groupe (de Hall)*. On a déjà démontré au Chapitre 6 que si G est résoluble, alors il possède des π-sous groupes pour tout $\pi \subset \Pi(G)$, de sorte que le résultat ci-dessus est l'assertion réciproque. Pour $\pi = \{p\}$ un singleton, un π-sous groupe de G est simplement un p-Sylow. On sait qu'ils exisent toujours, par Sylow. Ainsi, si $|\Pi(G)| = 2$, les hypothèses sont automatiquement satisfaites, et dans ce cas la conclusion (G résoluble) est simplement le théorème de Burnside. Noter aussi que dans le cas $|\Pi(G)| = 1$, *i.e.* G est un p-groupe, l'hypothèse est vide, et la conclusion vaut car les p-groupes sont résolubles (Corollaire 1.9 Chap. 6).

Nous suivons la présentation du cours de Serre de la démonstration du théorème de Hall. Nous aurons besoin du lemme suivant :

LEMME 9.5. *Soient G un groupe fini, et A et B deux sous-groupes de G d'indices premiers entre eux. On a $G = AB$ et $[A : A \cap B] = [G : B]$.*

DÉMONSTRATION — En effet, par Lagrange l'indice $[G : A \cap B]$ est divisible par $[G : A]$ et $[G : B]$, et donc par leur produit $[G : A][G : B]$ sous l'hypothèse de l'énoncé. Regardons l'action naturelle de A par translations à gauche sur G/B. Le stabilisateur de $\{B\} \in G/B$ est $A \cap B$. Mais toujours par Lagrange on a

$$|A/A \cap B| = |A|/|A \cap B| = [G : A \cap B]/[G : A] = |G/B|.$$

Cela démontre d'abord la formule de l'énoncé, et aussi que la A-orbite de $\{B\}$ est tout G/B, *i.e.* $G = AB$. □

Nous aurons aussi besoin du critère suivant de résolubilité.

PROPOSITION 9.6. (Wielandt) *Soit G un groupe fini. On suppose que G possède trois sous-groupes résolubles d'indices 2 à 2 premiers entre eux. Alors G est résoluble.*

DÉMONSTRATION — On raisonne par récurrence sur $|G|$. Soient H_1, H_2, H_3 les trois sous-groupes de l'énoncé. On peut supposer $H_1 \neq \{1\}$, car sinon $H_2 = H_3 = G$ est résoluble. Par un argument déjà vu dans le premier paragraphe de la démonstration du Théorème 4.1 Chap. 6, comme H_1 est résoluble il existe un nombre premier p tel que H_1 possède un sous-groupe abélien p-élementaire non trivial et distingué A. Comme H_2 et H_3 ont des indices premiers entre eux, on peut supposer quitte à les échanger que p ne divise par $[G : H_2]$. Ainsi, H_2 contient un p-Sylow S de G.

Par Sylow, il existe $g \in G$ tel que $g^{-1}Ag \subset S$. Par le Lemme 9.5 on a $G = H_1H_2$. Comme A est distingué dans H_1, tout conjugué de A (par un élément de G) est donc de la forme $h^{-1}Ah$ avec $h \in H_2$. On a vu qu'il existe un tel conjugué dans S, donc dans H_2. Tous les conjugés de A sont donc inclus dans H_2. Soit B le sous-groupe

de G engendré par les gAg^{-1} avec $g \in G$. Il est non trivial, distingué dans G, et inclus dans H_2, donc résoluble. Pour des raisons générales, l'image H_i' de H_i dans le groupe quotient G/B est d'indice divisant $[G : H_i]$, et les H_i' sont résolubles. Par récurrence, G/B est résoluble, ainsi donc que G. □

Démonstration — (du Théorème de Hall) Pour $p \in \Pi(G)$, appelons *p-complément* de G un π-sous groupe avec $\pi = \Pi(G) \smallsetminus \{p\}$. Démontrons, par récurrence sur $|G|$, que si G possède un p-complément pour tout $p \in \Pi(G)$ alors G est résoluble. Cet énoncé entraîne manifestement le Théorème de Hall. Pour la même raison que ci-dessus, il est clair pour $|\Pi(G)| = 1$, et résulte du théorème de Burnside pour $|\Pi(G)| = 2$.

On suppose donc que $\Pi(G)$ possède au moins 3 éléments distincts p_1, p_2, p_3, et on choisit H_1, H_2 et H_3 des p_i-compléments de G (ils existent par hypothèse). On a en particulier $|H_i| < |G|$ pour tout i. D'après Wieldandt (Prop. 9.6), il suffit de voir que chacun des H_i satisfait l'hypothèse de récurrence. Soient $p \in \Pi(H_i)$ et soit H un p-complément de G. On a $p \neq p_i$ par définition de H_i. Comme $[G : H_i]$ (une puissance de p_i) et $[G : H]$ (une puissance de p) sont premiers entre eux, on a $[H_i : H \cap H_i] = [G : H]$ par le Lemme 9.5, et $H \cap H_i$ est un p-complément de H_i. □

Terminons, comme promis, par une démonstration relativement élémentaire du Lemme 9.3. Il sera commode de dégager d'abord les deux énoncés suivants.

Lemme 9.7. *Soient $x_1, \dots, x_n$ et $y_1, \dots, y_m$ dans $\mathbb{C}$. On suppose que les polynômes $\prod_{i=1}^n (X - x_i)$ et $\prod_{j=1}^m (X - y_j)$ sont dans $\mathbb{Q}[X]$. Alors on a aussi*

$$\prod_{1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m} (X - x_i - y_j) \ \in \ \mathbb{Q}[X].$$

Démonstration — Pour tout $P \in \mathbb{Q}[X]$, on a $\prod_{i=1}^n P(X - x_i) \in \mathbb{Q}[X]$. En effet, le polynôme $\prod_{i=1}^n P(X - X_i) \in \mathbb{Q}[X][X_1, \dots, X_n]$ est symétrique en les X_i, et donc ses coefficients en X sont des polynômes à coefficients rationnels en les polynômes symétriques élémentaires en les X_k. Mais les polynômes symétriques élémentaires en les x_i sont dans $\mathbb{Q}$ par hypothèse. On conclut en posant $P = \prod_{j=1}^m (X - y_j)$. □

Soit $x \in \mathbb{C}$. On dit que x est *algébrique* s'il existe $P \in \mathbb{Q}[X]$ non nul avec $P(x) = 0$, ou autrement si $\mathrm{I}_x := \{P \in \mathbb{Q}[X] \mid P(x) = 0\}$ est $\neq \{0\}$. Observons que I_x est un idéal de $\mathbb{Q}[X]$ (*idéal annulateur de x*), de sorte que s'il est non nul il est principal de la forme (Π_x) pour un unique polynôme unitaire $\Pi_x \in \mathbb{Q}[X]$, appelé *polynôme minimal* du nombre algébrique x. C'est donc aussi le polynôme unitaire de plus petit degré de $\mathbb{Q}[X]$ annulant x.

Lemme 9.8. *Soit $x \in \mathbb{C}$ algébrique. On a $x \in \overline{\mathbb{Z}}$ si, et seulement si, $\Pi_x \in \mathbb{Z}[X]$.*

Démonstration — La condition est trivialement suffisante. Supposons donc $x \in \overline{\mathbb{Z}}$. Par hypothèse, il existe $P \in \mathbb{Z}[X]$ unitaire avec $P(x) = 0$. On a donc $P \in \mathrm{I}_x$, puis $\Pi_x \,|\, P$ dans $\mathbb{Q}[X]$. En particulier, toute y de Π_x dans $\mathbb{C}$ est racine de P, et donc dans $\overline{\mathbb{Z}}$. Comme $\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$ par la Proposition 6.3, on en déduit $\Pi_x \in \overline{\mathbb{Z}}[X]$, et on conclut car on a $\overline{\mathbb{Z}}[X] \cap \mathbb{Q}[X] = \mathbb{Z}[X]$ par la Proposition 6.2. □

Démonstration — (du Lemme 9.3) Choisissons $N \geqslant 1$ assez grand de sorte que l'on ait $\lambda_i^N = 1$ pour tout $1 \leqslant i \leqslant n$. Posons $z = \frac{1}{n}(\lambda_1 + \cdots + \lambda_n)$. Chaque λ_i/n est algébrique, car annulé par $(nX)^N - 1$. Par le Lemme 9.7, le polynôme

$$P(X) = \prod_{\zeta_1,\zeta_2,\ldots,\zeta_n \in \mu_N} (X - \frac{\zeta_1 + \zeta_2 + \cdots + \zeta_n}{n}) \tag{78}$$

est dans $\mathbb{Q}[X]$ et annule z. En particulier, z est algébrique. Comme on a $z \neq 0$ par hypothèse, on a $\Pi_z(0) \neq 0$ sinon Π_z/X serait dans I_z et de degré $< \deg \Pi_z$. Mais comme z est dans $\overline{\mathbb{Z}}$, on a aussi $\Pi_z \in \mathbb{Z}[X]$ d'après le Lemme 9.8, et donc au final

$$\Pi_z(0) \ \in \ \mathbb{Z} \smallsetminus \{0\}. \tag{79}$$

On vu $P \in \mathrm{I}_z = (\Pi_z)$ et donc toute racine z' de Π_z dans $\mathbb{C}$ est de la forme $\frac{1}{n}(\sum_{i=1}^n \lambda_i')$ avec les $\lambda_i' \in \mu_N$ pour tout $i = 1, \ldots, n$. Toute racine de Π_z dans $\mathbb{C}$ est donc de module $\leqslant \frac{1+\cdots+1}{n} = 1$. Mais le produit de ces racines est de norme $\geqslant 1$ par (79), de sorte que chacune est de norme 1, et en particulier $|z| = 1$. Le cas d'égalité de l'inégalité triangulaire dans $\mathbb{C}$ implique que les λ_i sont tous positivement proportionnels, et donc égaux car ils sont de même module 1, ce que l'on voulait démontrer. □