Algèbre M1 Cours 13

Centre de l'algèbre de groupe

14 décembre 2010

Programme

Aujourd'hui, G désigne un groupe fini.
Dans un premier temps, on va poursuivre l'étude des caractères sur les corps algébriquement clos de caractéristique nulle. Le but étant de démontrer que dans ce cas les dimensions des représentations irréductibles divise l'ordre du groupe. On commence pour cela par généraliser la notion d'élément algébrique au cas des anneaux : c'est la notion d'élément entier.
La deuxième partie est consacré à la démonstration des résultats de la semaine dernière dans le cas d'un corps de caractéristique finie ne divisant pas l'ordre du groupe.
Le point commun entre ces deux parties repose sur l'étude des propriétés du centre de l'algèbre de groupe.

Élément entier

Définition – Élément entier sur un anneau. Soient A et B deux anneaux commutatifs unitaires et $\rho : A \to B$ un morphisme d'anneaux (unitaires). On dit que $b \in B$ est entier sur A s'il existe $P \in A[X]$ unitaire tel que $P(b) = 0$ c'est-à-dire si

$$P = \sum_{i=0}^{n} a_i X^i ,$$

on a

$$\sum_{i=0}^{n} \rho(a_i) b^i = 0.$$

Exemple – Le cas des corps. Si $A = k$ et $B = K$ sont des corps, un élément entier de K n'est rien d'autre qu'un élément algébrique de K puisque le coefficient dominant de P est inversible.

Exemple – Le cas de $\mathbb{Z}$. Pour tout entier n, tout élément de $\mathbb{Z}/n\mathbb{Z}$ est entier sur $\mathbb{Z}$: $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est racine de $X - k \in Z[X]$ unitaire.

Élément entier sur $\mathbb{Z}$

Exemple Les éléments de $\mathbb{Q}$ qui sont entiers sur $\mathbb{Z}$ sont les éléments de $\mathbb{Z}$.

Tout élément de $\mathbb{Z}$ est évidemment entier sur $\mathbb{Z}$ ($n \in \mathbb{Z}$ est racine de $X - n$).
Inversement, soit $x = p/q \in \mathbb{Q}$ avec $p, q \in \mathbb{Z}$ et $p \wedge q = 1$ et $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ un polynôme unitaire annulant x. En réduisant au même dénominateur, on obtient

$$p^n + a_{n-1}p^{n-1}q + \cdots + a_0 q^n = 0$$

Ainsi
$$p^n = -q(a_{n-1}p^{n-1} + \cdots + a_0 q^{n-1})$$

et donc $q \mid p^n$ ce qui est absurde sauf si $q = \pm 1$ et donc $x \in \mathbb{Z}$.

Structure des éléments algébriques

Proposition Soient A et B deux anneaux commutatifs unitaires et $\rho : A \to B$ un morphisme d'anneaux. Alors, on a équivalence

(i) $b \in B$ est entier sur A

(ii) Il existe un sous-anneau C de B contenant b et des éléments $c_1, \ldots, c_n \in A$ tel que tout élément de $c \in C$ puisse s'écrire comme combinaison linéaire à coefficients dans A des c_i (on a $c = \sum_{i=1}^{n} a_i c_i$).

Preuve

$(i) \Rightarrow (ii)$. Soit $P \in A[X]$ un polynôme unitaire de degré n annulant b. On pose alors $C = A[b] := \{Q(b),\ Q \in A[b]\}$ et $c_i = b^i$ pour $0 \leqslant i \leqslant n-1$. Il suffit alors de montrer que pour $k \geqslant n$, on a b^k est combinaison linéaire à coefficients dans A de b^i pour $0 \leqslant i \leqslant n-1$.
On raisonne par récurrence sur k. Pour $k = n$, le résultat est évident grâce à la relation $P(b) = 0$. À présent si $k > n$, en multipliant la relation $P(b) = 0$ par b^{k-n}, on obtient que b^k est combinaison linéaire à coefficient dans A de $b^{k-1}, \ldots, b^{k-n}$ qui d'après l'hypothèse de récurrence sont eux mêmes des combinaisons des b^i pour $0 \leqslant i \leqslant n-1$.

Preuve (suite)

$(ii) \Rightarrow (i)$. Pour tout $i \in \{1, \ldots, n\}$, on peut écrire $bc_i = \sum_{i=1}^{n} a_{ij} c_j$. Ce qu'on peut encore écrire matriciellement

$$\underbrace{\begin{bmatrix} a_{1,1} - b & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ a_{n,1} & \cdots & a_{n,n-1} & a_{n,n} - b \end{bmatrix}}_{U} \begin{bmatrix} c_1 \\ \vdots \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

En multipliant à gauche par le transposée de la comatrice de U, on obtient l'égalité $\det(U)c_i = 0$ pour tout $i \in \{1, \ldots, n\}$. En écrivant $1_B = 1_C = \sum_{i=1}^{n} a_i c_i$, on en déduit que $\det(U) = 0$. En développant le déterminant, on obtient un polynôme annulateur de b unitaire à coefficients dans A (le polynôme caractéristique de la matrice $(a_{ij})_{1 \leqslant i,j \leqslant n}$).

Fermeture intégrale

Proposition Soient A et B deux anneaux commutatifs unitaires et $\rho : A \to B$ un morphisme d'anneaux. L'ensemble des éléments de B entiers sur A forme un sous-anneau de B appelé la fermeture intégrale de A dans B.

Preuve. Soient $x, y \in B$ entiers sur A, $P \in A[X]$ un polynôme unitaire annulant x de degré m et $Q \in A[X]$ un polynôme unitaire annulant y de degré n.
On considère le sous-anneau $C = A[x, y] = \{R(x, y),\ R \in A[X, Y]\}$ de B. On va montrer que tout élément de C est combinaison linéaire à coefficients dans A des $x^i y^j$ pour $i \in \{1, \ldots, m\}$ et $j \in \{1, \ldots, n\}$.
On a $A[x, y] = A[x][y]$ et y est entier sur $A[x]$. Ainsi, tout élément de $A[x, y]$ s'écrit comme combinaison linéaire à coefficients dans $A[x]$ de $1, y, \ldots, y^{m-1}$. Comme tout élément de $A[x]$ s'écrit comme combinaison linéaire à coefficients dans A de $1, x, \ldots, x^{n-1}$, on obtient le résultat.

Une application

On en déduit que $x - y \in A[x, y]$ et $xy \in A[x, y]$ sont entiers sur A. Par ailleurs, 1_B est racine du polynôme unitaire $X - 1_A \in A[X]$. ■

Corollaire – Un exemple important. Soit V un G-module de dimension finie sur k algébriquement clos et χ_V le caractère associé. Alors, pour tout $g \in G$, $\chi_V(g) \in k$ est entier sur $\mathbb{Z}$.

Preuve. On est sur un corps algébriquement clos donc $\rho_V(g)$ est trigonalisable et $\chi_V(g)$ est la somme des valeurs propres de G (comptées avec multiplicité). Par ailleurs, on a $g^{|G|} = 1$ et donc les valeurs propres de $\rho_V(g)$ sont des racines $|G|^{\mathrm{e}}$ de l'unité.
Or une racine $|G|^{\mathrm{e}}$ de l'unité est racine de $X^{|G|} - 1$ et donc entière sur k. Ainsi $\chi_V(g)$ est une somme d'éléments entiers sur k et donc entier sur k.

Morphisme d'anneaux

Remarque Soient A, B et C trois anneaux commutatifs unitaires, $\rho : A \to B$ et $\varphi : B \to C$ deux morphismes d'anneaux si $b \in B$ est entier sur A alors $\varphi(b) \in C$ est entier sur A.
En effet, si $P \in A[X]$ annule b alors P annule $\varphi(b)$.

Centre de l'algèbre de groupe

Proposition – Centre. Soit $x = \sum_{g \in G} \lambda_g g \in k[G]$. Alors $x \in Zk[G]$ si et seulement si $\lambda : g \mapsto \lambda_g$ est une fonction centrale.

Preuve. On a $x \in Zk[G]$ si et seulement si $hx = xh$ pour tout $h \in G$ si et seulement si $hxh^{-1} = x$ pour tout $h \in G$.
Or $hxh^{-1} = \sum_{g \in G} \lambda_g hgh^{-1}$. Comme $g \mapsto hgh^{-1}$ est une bijection de G, l'égalité $hxh^{-1} = h$ devient $\lambda_{hgh^{-1}} = \lambda_g$ pour tout $g \in G$.
Ainsi $\lambda_{hgh^{-1}} = \lambda_g$ pour tous $g, h \in G$ ce qui est précisément dire que λ est une fonction centrale.

Notation – Classe de conjugaison. On note $\mathscr{C}$ l'ensemble des classes de conjugaison de G.

Base du centre

Corollaire – Base du centre. Le centre $Zk[G]$ de $k[G]$ est un sous-espace vectoriel de dimension $r = |\mathscr{C}|$ de $k[G]$.
Une base de $Zk[G]$ est donnée par les fonctions indicatrices $\mathbf{1}_C = \sum_{g \in C} g$ où C parcourent les classes de conjugaison de G.

Preuve. D'après la proposition précédente, un élément du centre s'écrit

$$x = \sum_{C \in \mathscr{C}} \lambda_C \mathbf{1}_C$$

où λ_C désigne la valeur commune de λ sur la classe de conjugaison C. Les fonctions $\mathbf{1}_C$ forment donc une partie génératrice de $Zk[G]$.
Comme les classes de conjugaison forment une partition de G, si $\sum_{C \in \mathscr{C}} \lambda_C \mathbf{1}_C = 0$ alors $\lambda_C = 0$ pour tout C (l'élément g apparaît une seule fois dans la somme avec comme coefficient λ_C où C désigne la classe de conjugaison de g).

Un sous-anneau de type fini

Lemme Si C et C' sont deux classes de conjugaison de G, on peut écrire

$$\mathbf{1}_C\mathbf{1}_{C'} = \sum_{C''\in\mathscr{C}} n_{C''}\mathbf{1}_{C''} \quad \text{avec} \quad n_{C''} \in \mathbb{Z}$$

Preuve. Comme $Zk[G]$ est un sous-anneau de $k[G]$, on a

$$\mathbf{1}_C\mathbf{1}_{C'} = \sum_{C''\in\mathscr{C}} n_{C''}\mathbf{1}_{C''} \quad \text{avec} \quad n_{C''} \in k$$

Par ailleurs, pour $g \in C''$, $n_{C''}$ est le coefficient de g dans le produit $\mathbf{1}_C\mathbf{1}_{C'}$. Mais

$$\mathbf{1}_C\mathbf{1}_{C'} = \left(\sum_{g\in C} g\right)\left(\sum_{g\in C'} g\right) = \sum_{g\in C, h\in C'} gh = \sum_{g\in G} n_g g$$

où n_g est le nombre de façon d'écrire g comme produit d'un élément de C par un élément de C'.

Un sous-anneau de type fini

Corollaire L'ensemble

$$\left\{ \sum_{C \in \mathscr{C}} n_C \mathbf{1}_C, \quad n_C \in \mathbb{Z} \right\}$$

est un sous-anneau de $Zk[G]$. C'est le sous-anneau de $Zk[G]$ engendré par les $\mathbf{1}_C$ pour $C \in \mathscr{C}$.

Application Les éléments $\mathbf{1}_C$ sont des éléments entiers sur $\mathbb{Z}$ de $Zk[G]$.

Application Soit $x = \sum_{g \in G} \lambda_g g \in Zk[G]$ tel que pour tout g, λ_g soit entier sur $\mathbb{Z}$. Alors x est un élément entier sur $\mathbb{Z}$ de $Zk[G]$. En effet, on a $x = \sum_{C \in \mathscr{C}} (\lambda_C 1_G) \mathbf{1}_C$ avec $\lambda_C = \lambda_g$ si $g \in C$ et λ_C est entier sur $\mathbb{Z}$.

Applications

Proposition – Dimension des représentations irréductibles. Soit k un corps algébriquement clos de caractéristique nulle et V une représentation irréductible de G. On a $\dim V \mid |G|$.

Preuve. Soit $x \in Zk[G]$, $\rho_V(x)$ est alors un G-morphisme de V. Comme V est irréductible, $\rho_V(x)$ est une homothétie (lemme de Schur). On note $\lambda(x)$ le rapport de l'homothétie $\rho_V(x)$.
On définit ainsi un morphisme d'anneaux unitaires

$$\lambda : \begin{cases} Zk[G] \longrightarrow k \\ \quad x \quad \longmapsto \lambda(x) \end{cases}$$

De plus, on a $\lambda(x) = \dim(V)^{-1}\mathrm{tr}\,(\rho_V(x)) = \dim(V)^{-1}\chi_V(x)$.
On considère alors $x = \sum_{g \in G} \chi_V(g^{-1})g \in Zk[G]$ qui est entier sur $\mathbb{Z}$.
Comme $\chi_V(x) = |G|\langle \chi_V, \chi_V \rangle = |G| \dim_k \mathrm{End}_G(V) = |G|$, on obtient $\lambda(x) = |G|/\dim V$ est entier sur $\mathbb{Z}$ (puisque λ est un morphisme d'anneau). Finalement $|G|/\dim V \in \mathbb{Q}$ est entier sur $\mathbb{Z}$ et donc c'est un élément de $\mathbb{Z}$.

G-morphismes et algèbre de groupes

Proposition Soit V un G-module sur k. Les applications k-linéaires

$$\Delta : \begin{cases} \mathrm{Hom}_G(k[G], V) \longrightarrow V \\ \qquad f \qquad\qquad \longmapsto f(1) \end{cases}$$

et

$$\nabla : \begin{cases} V \longrightarrow \mathrm{Hom}_G(k[G], V) \\ v \longmapsto (x \mapsto xv = \rho_V(x)(v)) \end{cases}$$

sont des bijections réciproques l'une de l'autre.

Preuve. Δ est évidemment k-linéaire. Par ailleurs, l'application $f_v : x \mapsto xv$ est un G-morphisme. En effet, f_v est bien k-linéaire et $f_v(gx) = (gx)v = g(xv)$ (car ρ_V est un morphisme d'algèbres). Ainsi ∇ est bien définie.
Pour finir, $\Delta\nabla(v) = \rho_V(1)(v) = v$ pour tout $v \in V$ et, pour $x \in k[G]$, $\nabla\Delta(f)(x) = \rho_V(x)(f(1))$. Mais comme f est un G-morphisme, on a $\rho_V(x)f(1) = f(x)$. Ainsi $\nabla\Delta(f)(x) = f(x)$ pour tout $x \in k[G]$.

G-endomorphisme de l'algèbre de groupe

Proposition L'application

$$\Delta : \begin{cases} \mathrm{End}_G(k[G]) & \longrightarrow k[G] \\ f & \longmapsto f(1) \end{cases}$$

est un anti-isomorphisme de k-algèbres.

Preuve. On a vu que Δ est un isomorphisme de k-espace vectoriels. On calcule alors

$$\Delta(f \circ f') = (f \circ f')(1) = f(f'(1)) = f(f'(1)1) = f'(1)f(1) = \Delta(f')\Delta(f).$$

La quatrième égalité résulte du fait que f est un G-morphisme.

Remarque La bijection réciproque ∇ montre que les G-endomorphismes de $k[G]$ sont les multiplications à droites par les éléments de $k[G]$.

Anneau opposé

Définition – Anneau opposé. Soit $(A, +, \cdot)$ un anneau unitaire. On définit sur A un nouveau produit par noté $*$ par $a * b := b \cdot a$. On vérifie que $(A, +, *)$ est encore un anneau unitaire. On le note A^{op} et on dit que c'est l'anneau opposé de A.

Exemple Pour un anneau commutatif, on a $A = A^{\mathrm{op}}$.

Remarque Un anti-morphisme d'anneaux de A dans B est simplement un morphisme d'anneaux de A dans B^{op} ou un morphisme d'anneaux de A^{op} dans B.

Remarque – Algèbre de groupes. L'unique application k-linéaire qui envoie g sur g^{-1} pour tout $g \in G$ est un isomorphisme d'anneaux entre $k[G]$ et $k[G]^{\mathrm{op}}$.

Remarque – Algèbre de matrices. Soit A un anneau **commutatif** unitaire. L'application $M \mapsto {}^tM$ est un isomorphisme d'anneaux entre $\mathrm{M}_n(A)$ et $\mathrm{M}_n(A)^{\mathrm{op}}$.

Retour sur la semisimplicité

On suppose à présent que k est un corps algébriquement clos de caractéristique nulle ou de caractéristique première à l'ordre de G. Dans ce cas, on a vu que dans ce cas $k[G]$ est un G-module semisimple. De plus, il est de type fini (engendré par 1). On peut donc écrire une décomposition en tant que G-module

$$k[G] = {V_1}^{n_1} \oplus \cdots \oplus {V_s}^{n_s}$$

où V_i et V_j sont des G-modules simples, non isomorphes si $i \neq j$. On a alors

$$k[G]^{\mathrm{op}} \simeq \mathrm{End}_G(k[G]) = \mathrm{M}_{n_1}(\mathrm{End}_G(V_1)) \times \cdots \times \mathrm{M}_{n_s}(\mathrm{End}_G(V_s)).$$

Mais d'après le lemme de Schur, comme k est algébriquement clos, on a $\mathrm{End}_G(V_i) = k\mathrm{id}$. Ainsi

$$k[G] \simeq k[G]^{\mathrm{op}} \simeq \mathrm{M}_{n_1}(k) \times \cdots \times \mathrm{M}_{n_s}(k).$$

Comme $Z\mathrm{M}_n(k) = k\mathrm{id}$ et que le centre d'un produit d'anneaux est le produit des centres, on en déduit que s est le nombre de classes de conjugaison de G.

Retour sur la semisimplicité

En calculant la dimension de $k[G]$, on obtient

$$|G| = \sum_{i=1}^{s} n_i \dim V_i = \sum_{i=1}^{s} {n_i}^2.$$

Par ailleurs, on a

$$V_i \overset{\nabla}{\simeq} \mathrm{Hom}_G(k[G], V_i) = \bigoplus_{j=1}^{s} \mathrm{Hom}_G(V_j, V_i)^{n_j} = \mathrm{End}_G(V_i)^{n_i} = k^{n_i}$$

(la dernière égalité résultant du lemme de Schur).
Ainsi $n_i = \dim(V_i)$ et

$$|G| = \sum_{i=1}^{s} \dim {V_i}^2 \quad \text{et} \quad k[G] \overset{G\text{-mod.}}{\simeq} {V_1}^{\dim V_1} \oplus \cdots \oplus {V_s}^{\dim V_s}$$

Enfin, si V est un G-module simple, on obtient par le même calcul que ci-dessus (en remplaçant V_i par V) $V \simeq \bigoplus_{j=1}^{s} \mathrm{Hom}_G(V_j, V)^{n_j}$.

En particulier, comme $\dim V \neq 0$, V est isomorphe à l'un des V_i (lemme de Schur) et il y a donc exactement s classes d'isomorphisme de G-modules simples.

Bilan

Soit G un groupe fini et k est un corps algébriquement clos de caractéristique nulle ou de caractéristique première à l'ordre de G.

Le nombre de G-modules simples est égal au nombre de classes de conjugaison de G.

Tout G-module simple apparaît dans la représentation régulière $k[G]$ un nombre de fois égal à sa dimension : on a

$$k[G] = {V_1}^{\dim V_1} \oplus \cdots \oplus {V_s}^{\dim V_s}$$

où les V_i forment un système de représentants des classes d'isomorphisme de G-modules simples.

On a $|G| = \sum_{i=1}^{s} \dim {V_i}^2$.

Idempotents

On a vu que

$$k[G]^{op} \overset{k\text{-alg}}{\simeq} \mathrm{M}_{n_1}(k) \times \cdots \times \mathrm{M}_{n_s}(k).$$

Dans le membre de droite, les éléments $f_i = (0, \ldots, 0, \mathrm{Id}_{n_i}, 0, \ldots, 0)$ sont des idempotents centraux. On cherche alors à décrire leur correspondant e_i dans $k[G]$ c'est-à-dire donner explicitement les coordonnées dans la base canonique de $k[G]$.

On écrit donc $e_i = \sum_{g \in G} a_g g$ et on cherche les a_g.

Le calcul va reposer sur la connaissance de χ le caractère de la représentation régulière $k[G]$. On désigne par $\chi_1, \ldots, \chi_s$ les caractères irréductibles de G.

On a vu que $\chi(e_i g^{-1}) = \sum_{h \in G} a_h \chi(hg^{-1}) = |G| a_g$ pour tout $g \in G$.

Par ailleurs, on a aussi

$$\chi(e_i g^{-1}) = \sum_{j=1}^{s} n_j \chi_j(e_i g^{-1}) = \sum_{j=1}^{s} \dim V_j \chi_j(e_i g^{-1}).$$

Idempotents (suite)

Mais par définition de e_i, e_i agit comme l'identité sur V_i et comme 0 sur V_j avec $j \neq i$. Ainsi

$$\rho_{V_j}(e_i g^{-1}) = \rho_{V_j}(e_i)\rho_{V_j}(g^{-1}) = \delta_{i,j}\rho_{V_j}(g^{-1}).$$

Finalement, on trouve $|G|a_g = \dim V_i \chi_{V_i}(g^{-1})$.

Ainsi
$$e_i = \frac{\dim V_i}{|G|} \sum_{g \in G} \chi_{V_i}(g^{-1})g.$$

Application Si V est une représentation quelconque de G alors $\rho_V(e_i)$ est le projecteur sur la composante V_i-isotypique de V parallèlement aux autres composantes isotypiques.
Par exemple, si V_i est la représentation triviale alors on retrouve

$$\frac{1}{|G|} \sum_{g \in G} g.$$

Conséquences

Corollaire – Dimensions. Si $\mathrm{car} k = p$ est un nombre premier (qui ne divise pas l'ordre de G) alors les dimensions des représentations irréductibles ne sont pas divisibles par p (sinon, on aurait $e_i = 0$).

Corollaire – Indépendance des caractères. Les caractères irréductibles de G sont linéairement indépendants. En effet, si $\sum_{i=1}^{s} \lambda_i \chi_i = 0$ alors en évaluant en e_j, on obtient

$$0 = \sum_{i=1}^{s} \lambda_i \chi_i(e_j) = \lambda_j \chi_j(e_j) = \dim V_j \lambda_j$$

et donc $\lambda_j = 0$.

D'autres questions

1. Changement de groupes : comment comparer les représentations d'un groupe avec celles d'un de ces sous-groupes ?
2. Les problèmes de « rationalité » : comment comparer les représentations irréductibles sur $\mathbb{C}$ avec celles sur $\mathbb{R}$, ou sur $\mathbb{Q}$?
3. Représentations « mdulaire » : que se passe-t-il si $\mathrm{car} k \mid |G|$?

Références

1. Jean-Pierre Serre, *Représentations linéaires des groupes finis*
2. William Fulton & Joe Harris, *Representation Theory*
3. Serge Lang, *Algebra*