INTRODUCTION À LA THÉORIE DE LA REPRÉSENTATION MAT 6609

ABRAHAM BROER

Références

[1] Ya. G. Berkovich and E.M. Zhmud', *Characters of finite groups. Part 1 and Part 2.* Translations of Mathematical Monographs Vol. 172 and Vol. 181, Amer. Math. Soc., 1997.

[2] C.W. Curtis et I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience Publishers, New York, 1962.

[3] D.S. Dummit et R.M. Foote, *Abstract algebra. Third edition,* 2003.

[4] W. Fulton et J. Harris, *Representation theory. A first course*, G.T.M. **129**, Springer-Verlag, New York, 1991.

[5] I.M. Martin, *Character theory of finite groups,* Dover Publ., New York, 1994.

[6] N. Jacobson, *Basic algebra. I*, W. H. Freeman and Co., San Francisco, Calif., 1974.

[7] N. Jacobson, *Basic algebra. II*, W. H. Freeman and Co., San Francisco, Calif., 1980.

[8] G. James et M. Liebeck, *Representations and characters of groupes. Second edition*, Cambridge University Press, Cambridge, United Kingdom, 2001.

[9] J.-P. Serre, *Représentations linéaires des groupes finis. Deuxième édition*, Hermann, Paris, 1971.

1. Introduction

Chaque matrice complexe $n \times n$ est conjuguée à une matrice de la forme normale de Jordan. Si un groupe agit linéairement sur $\mathbb{C}^n$, chaque élément du groupe est représenté par une matrice. La théorie de la représentation cherche des formes normales pour toutes ces matrices simultanément.

La théorie est particulièrement bien développée pour les groupes finis. Pour les groupes infinis la théorie générale est *trop générale* pour obtenir des résultats intéressant; il faut se restreindre sur certaines sous-catégories de représentations pour obtenir des théories satisfaisantes.

Par exemple pour les groupes de Lie compacts et leurs représentations continues la théorie s'est aussi aussi bien développée comme la théorie des représentations des groupes finis. Dans ce cours il s'agit principalement de ce deux théories de représentations. Ces deux théories sont à la base de toute autre théorie de la représentations. Il faut mentionner qu'aussi autres catégories de groupes (et algèbres) et de classes de représentations sont bien étudiées et appliquées dans les domaines diverses comme la théorie des nombres, l'analyse harmonique ou la physique quantique.

1.1. **Un exemple.** Pour un exemple, considérons le groupe S_3 des permutations de $\{1, 2, 3\}$. Dans le tableau suivant on donne trois représentations; ρ_1 de dimension 1 (la représentation triviale), ρ_2

Date: January 11, 2007.

de dimension 2 (la représentation signe) et ρ_3 de dimension 2 (la représentation dihédrale).

S_3	(1)	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
ρ_1	(1)	(1)	(1)	(1)	(1)	(1)
ρ_2	(1)	(-1)	(-1)	(-1)	(1)	(1)
ρ_3	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}-1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&-1\\-1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&-1\end{pmatrix}$	$\begin{pmatrix}0&-1\\1&-1\end{pmatrix}$	$\begin{pmatrix}-1&1\\-1&0\end{pmatrix}$

L'analogue du théorème de Jordan pour le groupe S_3 est le résultat suivant. Soit μ une représentation de S_3 par des matrices complexes $n \times n$. Alors (possiblement après conjugaison) pour chaque permutation $\pi \in S_3$ la matrice associée à π est une matrice block-diagonale de la forme

$$\operatorname{diag}(\mu_1(\pi), \mu_2(\pi), \ldots, \mu_s(\pi))$$

où chaque block μ_i est soit ρ_1, ou ρ_2, ou ρ_3.

Par exemple, considérons la représentation par matrices de permutation

S_3	(1)	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
μ	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$	$\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$	$\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$	$\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$	$\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$

Soit

$$P := \begin{pmatrix}1&1&0\\1&-1&1\\1&0&-1\end{pmatrix}.$$

Si on remplace chaque matrice M par $P^{-1}MP$ on obtient la représentation matricielle

S_3	(1)	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
$P^{-1}\mu P$	$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&-1&1\\0&0&1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&0&-1\\0&-1&0\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&1&0\\0&1&-1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&0&-1\\0&1&-1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&-1&1\\0&-1&0\end{pmatrix}$

Alors

$$P^{-1}\mu P = \operatorname{diag}(\rho_1, \rho_3).$$

Soit $\mu = \operatorname{diag}(\rho_1, \rho_2, \rho_3)$ de dimension 4. Considérons R, la collection de toutes les matrices de la forme

$$\begin{pmatrix}*&0&0&0\\0&*&0&0\\0&0&*&*\\0&0&*&*\end{pmatrix}.$$

C'est une algèbre complexe de dimension 6, c'est à dire, R est un anneau et simultanément un espace vectoriel complexe de dimension 6. On voit que les six matrices $\mu(\pi)$, $\pi \in S_3$, font une base de R. C'est à dire, si $M \in R$, alors ils existent 6 uniques scalaires $c_\pi \in \mathbb{C}$, $\pi \in S_3$, tels que

$M = \sum_{\pi\in S_3} c_\pi \mu(\pi)$. Soit $M' = \sum_{\pi\in S_3} c'_\pi \mu(\pi)$ un autre élément de R. Alors

$$\begin{aligned} MM' &= \sum_{\pi\in S_3} c_\pi \mu(\pi) \sum_{\pi\in S_3} c'_\pi \mu(\pi) \\ &= \sum_{\pi_1,\pi_2\in S_3} c_{\pi_1} c'_{\pi_2} \mu(\pi_1)\mu(\pi_2) \\ &= \sum_{\pi_1,\pi_2\in S_3} c_{\pi_1} c'_{\pi_2} \mu(\pi_1\pi_2) \\ &= \sum_{\pi\in S_3} \left(\sum_{\pi_1\in S_3} c_{\pi_1} c'_{\pi_1^{-1}\pi} \right) \mu(\pi) \end{aligned}$$

Donc on peut effectuer le produit matriciel MM' par un calcul avec *l'algèbre de groupe*, comme on vient de faire. Inversement, on peut effectuer un calcul dans l'algèbre de groupe, par un calcul matriciel.

Chaque représentation de dimension finie de S_3 contient un certain nombre de copies de ρ_1, ρ_2 et ρ_2, disons n_1, n_2 et respectivement n_3. Il y a une méthode simple et explicite pour calculer le nombre de copies avant de connaître la forme normale. Cette méthode utilise seulement la trace (et pas toute la matrice), qui ne change pas après une conjugaison. Et aussi $\mathrm{tr}(\mathrm{diag}(\mu_1, \mu_2) = \mathrm{tr}(\mu_1)+\mathrm{tr}(\mu_2)$ pour les matrices block-diagonales.

Remarquons d'abord que la somme des matrices de ρ_2 est 0, et aussi que la somme des matrices de ρ_3 est la matrice 0. Mais la somme des matrices de ρ_1 est (6). Il suit que n_1 est la trace de la matrice $\frac{1}{6}\sum_{\pi\in S_3} \rho(\pi)$, ou

$$n_1 = \frac{1}{6} \sum_{\pi\in S_3} \mathrm{tr}(\rho(\pi)).$$

Puis, remarquons que si on multiplie les matrices $\rho_3(\pi)$ par le signe de $\pi \in S_3$ et après on prend la somme, on obtient encore une fois la matrice 0; la même chose pour ρ_1, mais cette fois on obtient la somme (6) pour ρ_2. Il suit que

$$n_2 = \frac{1}{6} \sum_{\pi\in S_3} \rho_1(\pi)\mathrm{tr}(\rho(\pi)).$$

Si $n \times n$ est la taille des matrices de ρ, alors $n = n_1 + n_2 + 2n_3$, donc

$$n_3 = \frac{n - n_1 - n_2}{2}.$$

Alternativement, remarquons que si on multiplie les $\rho_1(\pi)$ par $\mathrm{tr}(\rho_3(\pi))$ pour $\pi \in S_3$ et après on prend la somme, on obtient (0); la même chose pour ρ_2, mais cette fois on obtient la somme $\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$ pour ρ_3. Et donc on obtient la formule

$$n_3 = \frac{1}{6} \sum_{\pi\in S_3} \mathrm{tr}(\rho_3(\pi))\mathrm{tr}(\rho(\pi)).$$

Soit $V = \mathbb{C}[X_1, X_2, X_3]$ l'anneau de polynômes complexes dans les variables X_1, X_2, X_3. En particulier, V est un espace vectoriel complexe. On a une décomposition comme espace vectoriel

$$V = V_0 \oplus V_1 \oplus V_2 \oplus V_3 \oplus \ldots \oplus V_n \oplus \ldots,$$

où V_n est la collection des polynômes homogènes de degré n. Une base est par exemple

$$1, X_1, X_2, X_3, X_1^2, X_2^2, X_3^2, X_1X_2, X_1X_3, X_2X_3, X_1^3, \ldots$$

Comparer avec l'expansion de

$$\frac{1}{(1-X_1t)(1-X_2t)(1-X_3t)}$$

en $t = 0$

$$1 + (X_1 + X_2 + X_3)t + (X_1^2 + X_2^2 + X_3^2 + X_1X_2 + X_1X_3 + X_2X_3)t^2 + (X_1^3 + \ldots)t^3 + \ldots.$$

On voit que le coefficient de t^n est une somme de monômes, et ces monômes forment une base de V_n. Si on met toutes les variables égales à 1 on obtient que le coefficient de t^n dans l'expansion à $t = 0$ de $\frac{1}{(1-t)^3}$ est exactement la dimension de n.

Le groupe S_3 agit linéairement sur V et chaque V_n en permutant les variables. Donc chaque permutation π de S_3 donne pour chaque n une application linéaire de V_n dans V_n; cette application est représentée par une matrice $\mu_n(\pi)$. Par exemple si $\pi = (1, 3, 2)$ et $n = 2$, alors

$$\pi X_1^2 = X_{\pi(1)}^2 = X_3^2, \pi X_2^2 = X_1^2, \pi X_3^2 = X_2^2, \pi X_1X_2 = X_3X_1, \pi X_1X_3 = X_3X_2, \pi X_2X_3 = X_1X_2$$

et la matrice

$$\mu_2((1,3,2)) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

De façon analogue on obtient pour $(1, 2), (1, 3), (2, 3), (1, 2, 3)$ les matrices

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}; \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}; \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}; \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

La matrice identité est associée à $(1) \in S_3$. Nous pouvons calculer $n_1 = \frac{1}{6}(6+2+2+2+0+0) = 2$, $n_2 = \frac{1}{6}(6-2-2-2+0+0) = 0$ et $n_3 = (6-2)/4 = 2 = \frac{1}{6}(12+0+0+0-0-0)$. Donc il existe une matrice P tel que $P^{-1}\mu_2 P = \mathrm{diag}(\rho_1, \rho_1, \rho_3, \rho_3)$.

La trace de $(1, 3, 2)$ de la matrice associée à V_n est le coefficient de $\frac{1}{(1-t^3)}$ (vous voyez pourquoi? changer la base X_1, X_2, X_3 vers une base de vecteurs propre), pour les autres permutations:

S_3	(1)	$(1,2)$	$(1,3)$	$(2,3)$	$(1,2,3)$	$(1,3,2)$
tr	$\frac{1}{(1-t)^3}$	$\frac{1}{(1-t)(1-t^2)}$	$\frac{1}{(1-t)(1-t^2)}$	$\frac{1}{(1-t)(1-t^2)}$	$\frac{1}{(1-t^3)}$	$\frac{1}{(1-t^3)}$

On a

$$\frac{1}{6}\left(\frac{1}{(1-t)^3} + \frac{1}{(1-t)(1-t^2)} + \frac{1}{(1-t)(1-t^2)} + \frac{1}{(1-t)(1-t^2)} + \frac{1}{(1-t^3)} + \frac{1}{(1-t^3)}\right)$$

est égale à

$$\frac{1}{(1-t)(1-t^2)(1-t^3)}$$

Donc le coefficient de t^n dans l'expansion de $\frac{1}{(1-t)(1-t^2)(1-t^3)}$ est le nombre de fois que ρ_1 apparaît dans V_n.

2. Rappel de quelques résultats de l'algèbre

Travailler uniquement avec des matrices n'est pas suffisamment flexible, il sera nécessaire d'abstraire et de travailler avec des espaces vectoriels et les applications linéaires et même avec des modules sur des anneaux et ses morphismes.

Dans cette section on rappelle quelques constructions algébriques et on donne quelques résultats préliminairs.

Pour nous les anneaux seront toujours supposés d'être associatifs et unitairs. Si M est un module à gauche d'un anneau R d'unité $\mathbf{1}$, on supposera aussi toujours que $\mathbf{1} \cdot m = m$, pour chaque $m \in M$.

Pour un anneau R on dénote le sous-ensemble de ses unité par $R^\times$, donc $R^\times$ est la collection des éléments qui admettent un inverse multiplicativement. En fait, $R^\times$ est un groupe. Un *corps gauche* est un anneau dont chaque élément non-zéro admet un inverse multiplicatif, alors si $R^\times = R\backslash\{0\}$. Un corps gauche est un corps si la multiplication est commutative.

Pour un R-module à gauche M on dénote

$$\mathrm{End}_R(M) : Ł : M \to M; L \text{ est endomorphisme de } M \text{ comme } R\text{-module à gauche}\}$$

pour l'anneau des endomorphismes de M. Et puis on écrit $\mathrm{GL}(M) := (\mathrm{End}_R(M))^\times$, alors

$$\mathrm{GL}(M) := \{L : M \to M;\ L \text{ est automorphisme de } M \text{ comme } R\text{-module à gauche}\}.$$

Soit M un R-module. On rappelle que le R-module *dual* M^* est défini par

$$M^* := \mathrm{Hom}_R(M, R),$$

c'est l'ensemble des fonctionnelles sur M.

On dit qu'un sous-ensemble $B \subseteq M$ d'un R-module à gauche M est *indépendant* si pour chaque equation linéaire

$$r_1 b_1 + r_2 b_2 + \ldots + r_n b_n = 0,$$

avec $r_i \in R$, et $b_i \in B$ (tous différents), on a automatiquement que les scalaires r_i sont 0. On dit que $B \subseteq M$ est un *ensemble générateur*, si M coincide avec le sous R-module de M engendré par B, noté par $< B >_R$. On dit que $B \subseteq M$ est une *base* si B est un ensemble générateur indépendant. Pas chaque R-module à gauche contient une base. Par exemple, le $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ n'admet pas de base.

2.1. **Modules libres et bases.**

Soit R un anneau. Les modules à gauche *libres* ressemblent le plus les espaces vectoriels. Ce sont par définition les modules qui admettent une base. Explicitement, $\mathcal{B} \subset M$ est une base de M si pour chaque non-zero $m \in M$ il existe une unique expression finie

$$m = c_1 b_1 + c_2 b_2 + \ldots + c_r b_r,$$

où les $b_i \in B$ et où les $c_i \in R$ sont tous non-zéro. Une base n'est pas nécessairement finie.

Si R est un anneau commutatif et M un R-module admettant deux bases finies $\mathcal{B}_1$ et $\mathcal{B}_2$, alors $|\mathcal{B}_1| = |\mathcal{B}_2|$, pour une preuve voir [6, Theorem 3.4]. La même chose est vraie si R est un corps gauche, par exemple les quaternions de Hamilton $\mathbb{H}$ (la preuve est analogue au cas des espace vectoriels usuels sur des corps) ou n'importe quel corps. Dans ces cas $r := |\mathcal{B}_1|$ est appelé *le rang* de M (ou la *dimension* de M).

Si $\mathcal{B} \subset M$ est une base et N un autre R-module (pas nécessairement libre) alors chaque application $\phi : \mathcal{B} \to N$ a une unique extension $\tilde{\phi} : M \to N$ qui est R-linéaire et $\tilde{\phi}(b) = \phi(b)$, pour chaque $b \in \mathcal{B}$. Elle est définie par

$$\tilde{\phi}(m) := c_1\phi(b_1) + c_2\phi(b_2) + \ldots + c_r\phi(b_r),$$

si $m = c_1b_1 + c_2b_2 + \ldots + c_rb_r$.

2.2. **Le module libre sur un ensemble.** Le R-module libre RX sur un ensemble X, où X un ensemble quelconque et R un anneau, est défini comme l'ensemble des applications $f : X \to R$ telles que $f(x) \neq 0$ pour seulement un nombre fini de $x \in X$:

$$RX := \{f : X \to R; |\{x \in X;\ f(x) \neq 0\}| < \infty\}.$$

On définit $f_1 + f_2$ et cf par

$$(f_1 + f_2)(x) := f_1(x) + f_2(x),\ (cf)(x) := c(f(x))$$

où l'addition et la multiplication de R sont utilisés. Ici $f, f_1, f_2 \in RX$ et $c \in R$. RX est appelé le *R-module à gauche libre sur l'ensemble X*.

Chaque $x \in X$ donne un élément $\delta_x \in RX$ défini par

$$\delta_x(x) = 1 \ \text{ et } \ \delta_x(y) = 0 \ \text{ si } y \neq x.$$

Chaque $f \in RX$ s'écrit uniquement comme une somme finie

$$f = \sum_{x \in X} f(x)\delta_x,$$

parce que $f(x)$ est parr définition presque toujours 0. Souvent on simplifie l'écriture, et on écrit simplement $f = \sum_x f(x)x$, c-à-d, δ_x est remplacé par x. Et puis on peut identifier X avec un sous-ensemble de RX; ce sous-ensemble est la base naturelle de RX comme R-module à gauche libre.

Chaque application (ensembliste) $\phi : X \to M$ vers un R-module M donne un R-module homomorphisme $\tilde{\phi} : RX \to M$ par

$$\tilde{\phi}(f) = \sum_{x \in X} f(x)\phi(x).$$

C'est l'unique R-homomorphisme $\tilde{\phi}$ tel que

$$\tilde{\phi}(\delta_x = \tilde{\phi}(x)) = \phi(x).$$

Cette construction nous sera souvent très utile.

2.3. **Coordonnés.** Soit M est un R-module à gauche libre avec la base finie ordonnée

$$\mathcal{B} = \{e_1, e_2, \ldots, e_r\}.$$

Alors pour chaque $m \in M$ il existe un unique *vecteur de coordonnés*

$$[m]_{\mathcal{B}} = (m_1, m_2, \ldots, m_r) \in R^r,$$

tels que $m = \sum_{i=1}^{r} m_i e_i$. On a

$$[cm + c'm']_{\mathcal{B}} = c[m]_{\mathcal{B}} + c'[m']_{\mathcal{B}},$$

alors l'application de $M \to \mathbb{R}^n$ qui associe à chaque $m \in M$ son vecteur de coordonnés est un isomorphisme de R-modules à gauche. Si la base ordonnée est fixée on écrit simplement $[m] = [m]_{\mathcal{B}}$.

Soit maintenant M' un autre R-module libre avec base ordonnée finie $\mathcal{B}' = \{f_1, \ldots f_s\}$ et soit $\phi : M \to M'$ un R-module homomorphisme, c-à-d, $\phi(cm + c'm') = c\phi(m) + c'\phi(m')$. Définissons comme en algèbre linéaire la matrice $s \times r$

$$[\phi]^{\mathcal{B}}_{\mathcal{B}'} = [\phi] = (c_{ij})_{1 \le i \le s, 1 \le j \le r} \in \mathrm{Mat}(s \times r, R)$$

par

$$\phi(e_j) = \sum_{i=1}^{s} c_{ij} f_i.$$

On a pour $m = \sum_i m_i e_i$:

$$\begin{aligned}
\phi(m) &= \phi(\sum_{j=1}^{r} m_j e_j) \\
&= \sum_{j=1}^{r} m_j \phi(e_j) \\
&= \sum_{j=1}^{r} \sum_{i=1}^{s} m_j c_{ij} f_i \\
&= \sum_{i=1}^{s} \left(\sum_{j=1}^{r} m_j c_{ij} \right) f_i
\end{aligned}$$

Considérons premièrement le cas que où R est un anneau commutatif. Alors on a

$$\phi(m) = \sum_{i=1}^{s} \left(\sum_{j=1}^{r} c_{ij} m_j \right) f_j$$

et donc si on considère un vecteur de coordonnés comme un vecteur colonne

$$[\phi(m)]_{\mathcal{B}'} = [\phi]^{\mathcal{B}}_{\mathcal{B}'} \cdot [m]_{\mathcal{B}},$$

où à droite on a utilisé la multiplication matricielle entre une matrice et un vecteur colonne. Pour $c \in R$ on a

$$[\phi(cm)] = [\phi][cm] = [\phi]c[m] = c[\phi][m]$$

(encore une fois, parce que R est supposé d'être commutatif).

Si M'' est un troisème module avec base $\mathcal{B}''$ et $\phi_2 : M' \to M''$ est aussi un R-morphisme on a

$$[\phi_1 \circ \phi_2][m] = [(\phi_1 \circ \phi_2)(m)] = [\phi_1(\phi_2(m)] = [\phi_1][\phi_2(m)] = [\phi_1][\phi_2][m],$$

donc $[\phi_1 \circ \phi_2] = [\phi_1][\phi_2]$.

En particulier si $M = M'$, $\mathcal{B} = \mathcal{B}'$ on obtient un homomorphisme de groupe $\phi \mapsto [\phi]$ de $\mathrm{GL}(M) \to \mathrm{GL}(r, R)$, qui est en fait un isomorphisme.

Lemme 2.1. *Supposons R est un anneau commutatif. Le choix d'une base d'un R-module libre de dimension r induit un isomorphisme de groupe:*

$$\mathrm{GL}(M) \simeq \mathrm{GL}(r, R) : \phi \mapsto [\phi]$$

Mais si R n'est pas commutatif, les matrices scalaires ne commutent plus avec toutes les matrices, alors la multiplication par une matrice n'est plus une application R-linéaire, et on doit modifier cette méthode un peu. Pour une matrice M, soit M^t la matrice transpose $M^t_{ij} := M_{ji}$. Remarquons que maintenant on n'a plus que $(M_1 M_2)^t = M_2^t M_1^t$ pour deux matrices.

Si on considère cette fois un vecteur de coordononnés comme un vecteur *ligne* on a

$$[\phi(m)]_{\mathcal{B}'} = [m]_{\mathcal{B}} \left([\phi]^{\mathcal{B}}_{\mathcal{B}'}\right)^t,$$

où à droite on a utilisé la multiplication matricielle entre un vecteur ligne et une matrice. Pour $c \in R$ on a

$$[\phi(cm)] = [cm][\phi]^t = c[m][\phi]^t.$$

Si M'' est un troisème module avec base $\mathcal{B}''$ et $\phi_2 : M' \to M''$ est aussi un R-morphisme on a

$$[m][\phi_1 \circ \phi_2]^t = [(\phi_1 \circ \phi_2)(m)] = [\phi_1(\phi_2(m))] = [\phi_2(m)][\phi_1]^t = [m][\phi_2]^t[\phi_1]^t,$$

donc $[\phi_1 \circ \phi_2]^t = [\phi_2]^t[\phi_1]^t$.

L'application $\phi \mapsto \left([\phi]^t\right)^{-1}$ de $\mathrm{GL}(M)$ vers $\mathrm{GL}(r, R)$ est un homomorphisme de groupe, parce que

$$\left([\phi_1]^t\right)^{-1} \left([\phi_2]^t\right)^{-1} = \left([\phi_2]^t[\phi_1]^t\right)^{-1} = \left([\phi_1 \circ \phi_2]^t\right)^{-1}$$

C'est même un isomorphisme de groupe.

Lemme 2.2. *Le choix d'une base d'un R-module libre de dimension r induit un isomorphisme de groupe:*

$$\mathrm{GL}(M) \simeq \mathrm{GL}(r, R) : \phi \mapsto \left([\phi]^t\right)^{-1}]$$

Si R est commutatif on va toujours utiliser la première isomorphisme.

Un petit exemple. Soit $R = M = \mathbb{H}$, le corps gauche de quaternions. Soit $\phi : \mathbb{H} \to \mathbb{H}$ une application $\mathbb{H}$-linéaire pour le module à gauche $\mathbb{H}$. Alors $\phi(h) = \phi(h \cdot 1) = h \cdot \phi(1)$, alors ϕ est la multiplication *à droite* par $\phi(1) \in \mathbb{H}$. L'application ϕ est inversible, si et seulement si $\phi(1) \neq 0$. L'isomorphisme $\mathrm{GL}(V) \to \mathrm{GL}(1, \mathbb{H}) = \mathbb{H}^\times$ est donné par $\phi \mapsto (\phi(1))^{-1}$.

Il y a d'autres différences entre la théorie classique où R est commutatif, et le cas général. Par exemple, si R est commutatif, une matrice carrée avec coefficients dans R est inversible (i.e., cette matrice est dans $\mathrm{GL}(r, R)$) si et seulement si son déterminant est inversible dans R. Par contre si R n'est pas commutatif, on n'a même pas une bonne définition de déterminant en général.

2.4. **Module dual et base duale.** Soit M un R-module. On rappelle que le module dual M^* est défini par

$$M^* := \mathrm{Hom}_R(M, R).$$

Supposons M est libre avec base $\mathcal{B}$. Pour un vecteur de base $b \in \mathcal{B}$, on définit *le vecteur de base dual* (ou la fonction coordonné associé à $b \in \mathcal{B}$) $b^* \in M^* = \mathrm{Hom}_R(M, R)$ comme l'application R-lineaire telle que $b^*(v)$ est le coefficient v_b de b dans l'écriture $v = \sum_{b' \in \mathcal{B}} v_{b'} b'$. La *base duale* est la collection

$$\mathcal{B}^* := \{b^*; b \in \mathcal{B}\} \subset V^*.$$

Mais il faut faire attention, c'est une définition confusante : en général $\mathcal{B}^*$ *n'est pas une base* de l'espace dual M^*, sauf si $\mathcal{B}$ est finie ! Par exemple, l'application

$$H : v = \sum_{b \in \mathcal{B}} c_b(v) b \mapsto \sum_{b \in \mathcal{B}} c_b(v)$$

est dans M^*, mais n'est pas une combinaison *finie* des vecteurs de base duale $\mathcal{B}^*$, sauf si $\mathcal{B}$ est finie. On pourrait écrire $H = \sum_{b \in \mathcal{B}} b^*$, mais cette somme n'est pas finie ! En fait, M^* est le *produit direct* (et pas la somme directe) de ses sous-espaces Rb^*, $b \in \mathcal{B}$: chaque $\eta \in \mathrm{Hom}_R(M, R)$ s'écrit uniquement comme une expression formelle (possiblement infinie)

$$\eta = \sum_{b \in \mathcal{B}} c_b b^*,$$

où chaque coefficient c_b est dans R. Pour chaque $v \in V$ il y a seulement un nombre fini d'́léments de base duale b^* tel que $b^*(v) \neq 0$, donc

$$\eta(v) = \sum_{b \in \mathcal{B}} c_b b^*(v)$$

devient une somme finie. Donc chaque fonctionnelle est quand-même une combinaison linéaire (mais possiblement infinie !) des vecteurs de base duals.

Supposons $\phi : M \to M$ est un endomorphisme de R-module. Alors on obtient un endomorphisme duale $\phi^* : M^* \to M^*$, par $\phi^*(\eta) := \eta \circ \phi$. Supposons que la base fixée est finie, disons $\mathcal{B} = \{e_1, \ldots, e_r\}$ et $[\phi]$ est la matrice associée. Alors $\phi(e_j) = \sum_i [\phi]_{i,j} e_i$ et

$$[\phi]_{i,j} = e_i^*(\phi(e_j)).$$

On a

$$\left(\phi^*(e_j^*)\right)(e_i) = (e_j^* \circ \phi)(e_i) = e_j^*(\sum_r [\phi]_{j,r} e_r = [\phi]_{j,i}.$$

Donc la matrice de ϕ^* par rapport à la base duale est $[\phi]^t$, la matrice transposée.

2.5. **Existence de bases et lemme de Zorn.** Soit V un espace vectoriel sur un corps k (ou un module sur un corps gauche). L'existence d'une base est une conséquence du "lemme de Zorn" des fondements des mathématiques. C'est une hypothèse fondamentale des mathématiques équivalente à l'axiome de choix. On peut la voir comme une type d'induction transcendante.

Soit Ω un ensemble muni d'un ordre partiel $\leq$. Une *chaîne* C de Ω est un sous-ensemble totalement ordonné, c-à-d, pour chaque pair $x, y \in C$ soit $x \leq y$, soit $y \leq x$. Une *borne supérieure* d'un sous-ensemble $A \subset \Omega$ est un $x \in \Omega$ tel que $y \leq x$ pour chaque $y \in A$. Un *élément maximal* de Ω est un élément $x \in \Omega$ tel que $x \leq y$ est seulement possible si $x = y$.

Hypothèse 2.1 (Lemme de Zorn)**.** *Soit Ω un ensemble non-vide muni d'un ordre partiel. Supposons que chaque chaîne de Ω a une borne supérieure. Alors Ω contient au moins un élément maximal.*

En acceptant cette hypothèse on déduit l'existence d'une base.

Corollaire 2.1. *Soit V un espace vectoriel sur un corps k et supposons $V \neq 0$.*

Si A est un sous-ensemble linéairement indépendant de V et B un sous-ensemble générateur de V et $A \subseteq B$, alors il existe une base $\mathcal{B}$ contenant A et contenue dans B :

$$A \subseteq \mathcal{B} \subseteq B.$$

Le résultat reste vrai si on remplace V par un module non-zero sur un corps gauche.

Preuve. Posons Ω pour l'ensemble de tous les sous-ensembles linéairement indépendant contenant A et contenu dans B. Alors Ω n'est pas vide, parce que $V \neq 0$ et donc B n'est pas vide, et Ω est partiellement ordonné par $\subseteq$. Soit $\Sigma \subset \Omega$ une chaîne. Alors la réunion $U := \cup_{Y \in \Sigma} Y$ contient A et est contenue dans B. Soit $\sum_{i=1}^{n} c_i u_i = 0$ une relation linéaire entre n éléments de U. Comme Σ est totalement ordonné, il existe un $C \in \Sigma$ contenant tous les u_i's. Mais C est linéairement indépendant, donc la relation est triviale. Donc $U \in \Omega$ et U est une borne supérieure pour la chaine Σ.

Par le lemme de Zorn on conclut que Ω contient un élément maximal $\mathcal{B}$, en particulier $A \subseteq \mathcal{B} \subseteq B$ et $\mathcal{B}$ est un ensemble indépendant. Montrons que $\mathcal{B}$ est aussi un ensemble générateur. Soit $v \in B - \mathcal{B}$, par la maximalité de $\mathcal{B}$ l'ensemble $\mathcal{B} \cup \{v\}$ n'est plus linéairement indépendant, donc il existe une relation non-triviale $cv + \sum_{i=1}^{n} c_i b_i = 0$ pour un nombre fini de b_i's dans $\mathcal{B}$ et des scalaires c, c_i. Si $c = 0$, alors nécessairement les autres constants sont aussi 0, parce que $\mathcal{B}$ est indépendant; une contradiction. Donc $c \neq 0$ et v est une combinaison linéaire des $b_1, \ldots, b_n$. Mais B est un ensemble générateur, donc $\mathcal{B}$ est aussi un ensemble générateur. □

Corollaire 2.2. *Soit $U \subset V$ un sous-espace vectoriel. Alors il existe un complément, c-à-d, il existe un sous-espace vectoriel $U' \subset V$ tel que $V = U \oplus U'$.*

Preuve. Soit $e_i, i \in I$ une base de U. Par le résultat précédent on peut trouver $f_j; j \in J$ tel que $\{e_i; i \in I\} \cup \{f_j; j \in J\}$ est une base de V. On définit maintenant U' comme l'espace engendré par les $f_j, j \in J$. □

3. L'algèbre de groupe et ses modules

Fixons un groupe G et un anneau R, typiquement R sera $\mathbb{C}$ ou un autre corps. On va donner le R-module à gauche sur G, RG, la structure d'un anneau. La multiplication sur RG est induite par la multiplication de G :

$$\delta_g * \delta_k := \delta_{gk},$$

où gk est le produit de g et k dans le groupe G. Donc (avec la notation simplifiée) $g * k := gk$ et

$$f * h = \sum_{g \in G} f(g) g \ * \ \sum_{k \in G} h(k) k = \sum_{g,k \in G} f(g) h(k) gk = \sum_{g \in G} \left(\sum_{k} f(k) h(k^{-1} g \right) g.$$

Ou le produit $f * h$ est la fonction sur G définie par

$$(f * h)(g) := \sum_{k \in G} f(k)h(k^{-1}g),$$

le *produit de convolution*. Les sommes sont tous finies, à cause de la restriction sur les fonctions sur G permises dans RG. L'unité de cet anneau est $\mathbf{1} = \delta_{\mathbf{1}_G}$; l'associativité de la multiplication de RG est une conséquence de l'associativité de la multiplication du groupe et de l'associativité de la multiplication de l'anneau R. Il est facile de vérifier les autres axiomes d'anneau (associatif et unitaire). Nous pouvons identifier R avec le sous-anneau $R\mathbf{1}$ de RG; ainsi par restriction chaque RG-module est aussi un R-module.

La méme construction fonctionne aussi si on remplace G par un monoïde.

3.1. **Actions linéaires de groupes.** Soit M un RG-module, alors par restriction M est aussi un R-module. Chaque $g \in G$ peut être considéré comme un élément de la base naturelle de RG, et donc la multiplication $g \cdot m \in M$ satisfait

$$(i)\ \mathbf{1}_G \cdot m = m;\ (ii)\ (g_1 g_2) \cdot m = g_1 \cdot (g_2 \cdot m);\ (iii)\ g \cdot (c_1 m_1 + c_2 m_2) = c_1(g \cdot m_1) + c_2(g \cdot m_2),$$

pour chaques $m, m_1, m_2 \in V$, $g, g_1, g_2 \in G$ et $c_1, c_2 \in k$.

Inversement, si M est un R-module et $G \times M \to M : g, \mapsto g \cdot m$ satisfait les trois règles (i), (ii) et (iii), alors M est un RG-module. Un tel action de G sur M est appelé une *action R-linéaire*. Donc les actions R-linéaires de G sont exactement les RG-modules.

Ce qu'on vient de définir sont les actions linéaires à gauche. On pourrait aussi définir les actions à droites, comme on fait dans les livres sur la thèorie de la représentations de la provenance de l'Angletère, par exemple [8]. La théorie ne change pas essentiellement, sauf dans les détails, et il faut faire attention si on lit ces livres que "gauche" est remplacé par "droite", et vice versa (par exemple la définition du groupe symétrique y est un peu différente).

Dans ce cours le plus souvent le corps $\mathbb{C}$ des nombres complexes sera utilisé pour R, mais on utilisera aussi les nombres réels $\mathbb{R}$ et des corps fini de temps en temps. On est aussi intéressé à utiliser les quaternions $\mathbb{H}$, des espaces vectoriels sur $\mathbb{H}$ et des matrices avec des coefficients dans $\mathbb{H}$. On rappelle que l'anneau $\mathbb{H}$ est presque un corps, le seul axiom des corps qui n'est pas satisfait est l'axiom de la commutativité de la multiplication, en particulier n'importe quelle quaternion non-zero a un inverse (unique). On dit que c'est un *corps gauche*. Pour être capable de travailler aussi avec $\mathbb{H}$ (et d'autres corps gauches) il faut modifier les faits standard de l'algèbre linéaire un peu. Mais il est aussi facile de travailler avec un anneau, qui sera ici toujours supposé d'être associatif et unitair, et ses modules. Aussi $R = \mathbb{Z}$ est utilisé de temps en temps.

Une variation sur le théorème de Cayley généralisé des actions sur un ensemble est le suivant, la preuve est analogue.

Lemme 3.1. *Soit M un R-module à gauche, où R est un anneau (associatif et unitaire), et G un groupe.*

(i) Supposons $g \cdot m$ est une action R-linéaire de G sur M. Définissons $\rho : G \to \mathrm{GL}(M)$ par $\rho(g)(m) := g \cdot m$. Alors ρ est un homomorphisme de groupes.

(ii) Supposons $\rho : G \to \mathrm{GL}(M)$ est un homomorphisme de groupe. Alors $g \cdot m := \rho(g)(m)$ définit une action R-linéaire de G sur M.

Preuve. (i) Soit $G \times M \to M : \ (g, m) \mapsto g \cdot m$ une action linéaire. On définit l'application $\rho(g) : \ M \to M$ par

$$\rho(g)(m) := g \cdot m.$$

Alors $\rho(g)$ est un R-module homomorphisme :

$$\rho(g)(\lambda v + \mu w) = g \cdot (\lambda v + \mu w) = \lambda(g \cdot v) + \mu(g \cdot w) = \lambda\rho(g)(v) + \mu\rho(g)(w).$$

Et $\rho(g)$ est inversible avec l'inverse $\rho(g^{-1})$:

$$(\rho(g) \circ \rho(g^{-1}))(m) = \rho(g)(\rho(g^{-1})(m)) = g \cdot (g^{-1} \cdot m) = (gg^{-1}) \cdot m = \mathbf{1}_G \cdot m = m$$

et d'une manière analogue $\rho(g^{-1}) \circ \rho(g) = \mathbf{1}$.

Donc on a une application

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

C'est un homomorphisme de groupes :

$$\rho(g_1 g_2)(m) = (g_1 g_2) \cdot m = g_1 \cdot (g_2 \cdot m) = \rho(g_1)\left(\rho(g_2)(m)\right) = \left(\rho(g_1) \circ \rho(g_2)\right)(m)$$

(ii) Par contre, supposons $\rho : \ G \to \mathrm{GL}(M)$ est un homomorphisme de groupe. On définit une action

$$G \times M \to M : \ (g, m) \mapsto g \cdot m := \rho(g)(m).$$

On vérifie :

$$\mathbf{1}_G \cdot m = \rho(\mathbf{1}_G)(m) = \mathbf{1}(m) = m;$$

et

$$(g_1 g_2) \circ m = \rho(g_1 g_2)(m) = \left(\rho(g_1) \circ \rho(g_2)\right)(m) = \rho(g_1)\left(\rho(g_2)(m)\right) = g_1 \cdot (g_2 \cdot m).$$

L'action est linéaire :

$$g \cdot (\lambda v + \mu w) = \rho(g)(\lambda v + \mu w) = \lambda\rho(g)(v) + \mu\rho(g)(w) = \lambda(g \cdot v) + \mu(g \cdot w).$$

□

On dira que deux représentations $f_1 : \ G \to \mathrm{GL}(M_1)$ et $f_2 : \ G \to \mathrm{GL}(M_2)$, où M_1 et M_2 sont tous les deux R-modules, sont *équivalentes*, s'il existe un R-module isomorphisme

$$\omega : \ V_1 \to V_2,$$

tel que

$$f_2(g) \circ \omega = \omega \circ f_1(g)$$

pour chaque $g \in G$, où

$$g \cdot \omega(m) = \omega(g \cdot m),$$

pour les action linéaires correspondantes.

Lemme 3.2. *Soit R un anneau, M un R-module à gauche et G un groupe.*

(i) Si $g \cdot m$ est une action linéaire de G sur M alors M est un RG-module à gauche par

$$fm := \sum_{g \in G} f(g)(g \cdot m).$$

(ii) Si M est un RG module, alors G agit linéairement sur M par l'action $g \cdot m := \delta_g m$.

3.2. **Morphismes de kG-modules.** Le langage de modules est utile.

Soit $\phi:\ M \to M'$ un morphisme de RG-modules. Alors c'est un R-module homomorphisme tel que $\phi:\ M \to M'$ qui respecte les deux opérations de G :

$$g \cdot \phi(m) = \phi(g \cdot m),$$

pour chaque $g \in G$ et $v \in M$.

Le noyaux et l'image d'un RG-morphisme sont des RG-modules. Si W_1, W_2 sont deux sous RG-modules de V, alors $W_1 \cap W_2$ et $W_1 + W_2 = \{w_1 + w_2; w_1 \in W_1, w_2 \in W_2\}$ sont aussi des sous RG-modules. Pour chaque sous RG-module $W \subset V$, le quotient V/W a une structure de RG module avec l'action linéaire $g \cdot (v + W) := g \cdot v + W$.

On a aussi comme d'habitude deux notions de somme directe. Si W_1, W_2 sont deux sous RG-modules à gauche de V, on écrit $V = W_1 \oplus W_2$ si $V_1 + V_2 = V$ et $V_1 \cap V_2 = 0$. Si V_1 et V_2 sont deux RG-modules on écrit $V_1 \oplus V_2$ pour le produit cartésien des deux R-modeles à gauche avec l'action $g \cdot (v_1, v_2) := (g \cdot v_1, g \cdot v_2)$.

On dit qu'un RG-module V est *décomposable* si $V = W_1 \oplus W_2$ pour deux sous RG-modules non-zéro; sinon V est *indécomposable*. On dit qu'un RG-module V est *simple* si V ne contient aucun RG-sous-module non-trivial. Un module simple est indécomposable, mais un module indécomposable n'est pas nécessairement simple.

Si $\rho : G \to \mathrm{GL}(M)$ est une représentation, alors M est un RG-module. Si $U \subset V$ est un sous RG-module, par la correspondance on aura une représentation $\rho_U : G \to \mathrm{GL}(U)$. Cette représentation est appelé *sous-représentation* de ρ.

3.3. **Actions et actions linéaires.** Soit X un G-ensemble, c'est à dire, il y une multiplication externe fixé $(g, x) \mapsto g \cdot x$ satisfaisant

$$(i)\mathbf{1}_G \cdot x = x,\ (ii)(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x).$$

Alors RX devient un RG-module à gauche défini par :

$$\sum_{c_g} g \cdot \sum_x n_x x := \sum_{g \in G, x \in X} c_g n_x (g \cdot x) = \sum_x \left(\sum_{g \in G} c_g n_{g^{-1} \cdot x} \right) x.$$

Ou RX est un RG-module par

$$[f * h](x) := \sum_{g \in G} f(g) h(g^{-1} \cdot x).$$

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA