1. Représentations linéaires

Dans cette partie et la suivante, G désigne un groupe et k un corps, tous deux quelconques.

DÉFINITION 1.1. *Une représentation k-linéaire de G est la donnée d'un k-espace vectoriel V et d'un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$.*

On parle aussi de représentation de G *sur* l'espace vectoriel V. L'inclusion $\mathrm{S}_V \subset \mathrm{GL}(V)$ montre qu'il est équivalent de se donner une représentation ρ de G sur V, et une action de G sur V, disons $(g, v) \mapsto g.v$, telle que pour tout $g \in G$ la bijection $\mathrm{L}_g : v \mapsto g.v$ est k-linéaire. Le lien entre les deux points de vue est bien sûr la formule $\mathrm{L}_g = \rho(g)$ pour $g \in G$.

On note souvent (V, ρ), ou même simplement V ou ρ, une représentation de G. La *dimension*, ou le *degré*, de (V, ρ) est la dimension du k-espace vectoriel V. Dans ce cours on considérera surtout des représentations de dimension finie.

EXEMPLE 1.2. *Si G est un sous-groupe de $\mathrm{GL}_n(k)$, son action naturelle sur k^n définit une représentation k-linéaire de G.* Par exemple, tout sous-groupe de $\mathrm{SO}(3)$ admet une représentation $\mathbb{R}$-linéaire naturelle sur $\mathbb{R}^3$, et tout sous-groupe de $\mathrm{Sp}(1)$ possède une représentation naturelle $\mathbb{C}$-linéaire sur $\mathbb{C}^2$.

Si (V, ρ) est une représentation k-linéaire de dimension n de G, le choix d'une base e de V définit un morphisme de groupes

$$\rho^e : G \to \mathrm{GL}_n(k),\ g \mapsto \mathrm{Mat}_e \rho(g).$$

Changer de base e revient simplement a conjuguer ρ^e par un élément de $\mathrm{GL}_n(k)$ (matrice de changement de base).

DÉFINITION 1.3. *Deux représentations k-linéaires (V_1, ρ_1) et (V_2, ρ_2) de G de même dimension finie seront dites isomorphes, ou équivalentes, s'il existe des bases e_1 et e_2 de V_1 et V_2, avec $\rho_1^{e_1} = \rho_2^{e_2}$.*

Ainsi, *on s'intéresse essentiellement aux classes de conjugaison de morphismes* $G \to \mathrm{GL}_n(k)$.

EXEMPLE 1.4. *(i) Une représentation k-linéaire de G de dimension 1 est la donnée d'un morphisme $G \to k^\times$.* Pour $k = \mathbb{C}$, c'est donc un élément de $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$.

(ii) L'action triviale de G sur $V = k$ est une représentation linéaire de dimension 1 appelée *représentation triviale de G.*

(iii) Se donner une représentation ρ de $G = \mathbb{Z}$ sur V est la même chose que se donner l'image de $\rho(1)$, qui est un élément arbitraire de $\mathrm{GL}(V)$. Classifier à isomorphisme près les représentations k-linéaires de $\mathbb{Z}$ de dimension n revient donc à déterminer les classes de conjugaison d'éléments de $\mathrm{GL}_n(k)$.

En guise d'autre exemple, supposons donnée une action du groupe G sur un ensemble X. Notons kX le k-espace vectoriel *libre sur l'ensemble* X, c'est-à-dire l'espace $k^{(X)}$ muni de sa base canonique des e_x avec $x \in X$. On a donc une somme directe $kX = \bigoplus_{x \in X} k\,\mathrm{e}_x$. On dispose d'un morphisme naturel $\rho : G \to \mathrm{GL}(kX)$ défini par $\rho(g)(\mathrm{e}_x) = \mathrm{e}_{gx}$ pour tout $g \in G$ et tout $x \in X$.

Définition 1.5. *Si G agit sur X, la représentation ci-dessus de G sur $k\,X$ est appelée* représentation de permutation *associée.*

Ces représentations sont très particulières : dans la base $\{\mathrm{e}_x\}$ de kX, la matrice de chaque $\rho(g)$ avec $g \in G$ a un unique coefficient non nul, égal à 1, sur chaque colonne et sur chaque ligne.

Exemple 1.6. Considérons l'action naturelle de $G = \mathrm{S}_n$ sur $X = \{1, \ldots, n\}$. Elle définit une représentation de permutation de S_n sur $kX = k^n = \oplus_{i=1}^n k\mathrm{e}_i$ vérifiant $\sigma(\mathrm{e}_i) = \mathrm{e}_{\sigma(i)}$ pour $\sigma \in \mathrm{S}_n$ et $i \in \{1, \ldots, n\}$, soit encore $\sigma(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$ pour $x \in k^n$. Dans la base des e_i, c'est le morphisme $\mathrm{S}_n \to \mathrm{GL}_n(k)$ déjà rencontré dans la démonstration du Théorème 2.1 Chap. 6.

2. Le point de vue $k[G]$-modules

Nous verrons de nombreux autres exemples un peu plus tard. Expliquons d'abord comment les représentations k-linéaires de G peuvent être vue alternativement, et avec profit, comme des modules sur un anneau adéquat, appelée *k-algèbre du groupe G*. Rappelons d'abord la définition d'une k-algèbre.

Définition 2.1. *Une k-algèbre est un anneau A muni d'un morphisme d'anneau $k \to A$.*

Par exemple, l'anneau $\mathrm{M}_n(k)$ est une k-algèbre via $k \to \mathrm{M}_n(k)$, $\lambda \mapsto \lambda \mathrm{I}_n$. De même, l'anneau $k[X]$ est une k-algèbre via l'inclusion évidente ("les constantes"). Comme tout morphisme d'anneau d'un corps vers un anneau non nul est injectif, le morphisme $k \to A$ est souvent simplement vu comme une inclusion. Il permet de voir A comme un k-espace vectoriel, ainsi que tout A-module par restriction des scalaires.

Construction de $k[G]$: La donnée de k et G permet de construire une structure de k-algèbre sur le k-espace vectoriel $A =: k\,G$. En effet, on munit A de l'unique loi de composition k-bilinéaire $\mu : A \times A \to A, (x, y) \mapsto xy$, qui dans la base des $\{\mathrm{e}_g\}_{g \in G}$ est donnée par la formule $\mathrm{e}_g\,\mathrm{e}_h := \mathrm{e}_{gh}$. Elle est associative par associativité de la loi de groupe de G (voir l'Exercice 9.33) et de neutre e_1. Elle est distributive vis-à-vis de $(A, +)$, par bilinéarité. Autrement dit, $(A, +, \mu)$ est un anneau. Par construction, $\lambda \mapsto \lambda \mathrm{e}_1$ est un morphisme d'anneaux $k \to A$, faisant donc de A une k-algèbre. On notera presque toujours g l'élément e_g de A pour alléger les écritures.

Définition 2.2. *Soient k un corps et G un groupe. La k-algèbre d'espace sous-jacent $k\,G$ construite ci-dessus s'appelle* l'algèbre du groupe G à coefficients dans k *et est notée $k[G]$. Sa dimension comme k-espace vectoriel est $|G|$.*

Exemple 2.3. L'anneau $k[G]$ est commutatif si, et seulement si, G l'est. Il n'est pas difficile de montrer que l'on a $k[\mathbb{Z}] \simeq k[T, T^{-1}]$ et, pour tout entier $n \geqslant 1$, on a $k[\mathbb{Z}/n\mathbb{Z}] \simeq k[T]/(T^n - 1)$. La structure de $\mathbb{C}[G]$ pour G fini sera élucidée plus loin dans le cours : voir la Remarque 7.7.

Qu'est-ce qu'un $k[G]$-module ? D'abord, tout $k[G]$-module V est *a fortiori* un k-espace vectoriel, par restriction des scalaires au sous-corps $k1$ de $k[G]$, que l'on identifie à k via $x \mapsto x1$. De plus, il induit une application $G \times V \to V$, $(g, v) \mapsto gv$ qui est manifestement une action de G sur V. Enfin, cette action est par automorphismes k-linéaires : on a

$$g(\lambda v) = g(\lambda 1\, v) = (g\lambda 1)v = (\lambda 1 g)v = (\lambda 1)(gv) = \lambda gv$$

(car g et $\lambda 1$ commutent par construction dans $k[G]$). Ainsi, *à tout $k[G]$-module V est associé une représentation k-linéaire ρ_V de G sur V*, vérifiant $\rho_V(g)(v) = gv$. Réciproquement, toute action de G sur un k-espace vectoriel V par automorphismes k-linéaires s'étend de manière unique en une structure de $k[G]$-module sur V. En effet, comme $\{g\}_{g\in G}$ est une k-base de $k[G]$ il y a un sens à considérer

$$\nu : k[G] \times V \to V, (\sum_{g\in G} \lambda_g\, g, v) \mapsto \sum_{g\in G} \lambda_g \rho(g)v.$$

C'est trivialement une structure de $k[G]$-module sur V ![1] On a montré :

Proposition-Définition 2.4. (Propriété universelle de l'algèbre du groupe) *Il est équivalent de se donner une représentation k-linéaire du groupe G et un $k[G]$-module. Plus précisément :*

(i) Si V est un $k[G]$-module, il existe une unique représentation k-linéaire de G sur le k-espace vectoriel sous-jacent à V, notée $\rho_V : G \to \mathrm{GL}(V)$, vérifiant $\rho_V(g)(v) = g.v$ pour tout $g \in G$ et $v \in V$. On l'appelle la représentation associée à V.

(ii) Reciproquement, si (V, ρ) est une repésentation k-linéaire de G, il existe une unique structure de $k[G]$-module sur V étendant celle de k-espace vectoriel, et vérifiant $g.v = \rho(g)(v)$ pour tout $g \in G$ et $v \in V$. On l'appelle $k[G]$-module associé à (V, ρ), et on le note en général simplement V.

Ces deux constructions sont inverses l'une de l'autre.

Dans la suite, nous jonglerons souvent entre les points de vue « représentation » et « $k[G]$-module » sans commentaire, via la proposition ci-dessus. Ainsi, étudier les représentations de G est la même chose qu'étudier l'algèbre $k[G]$-linéaire ! Toutes les notions s'appliquant aux modules s'appliquent en particulier aux représentations, ce qui nous évite en particulier de les redéfinir (même si nous en retraduirons certaines ci-dessous) : sous-modules, produits, sommes, sommes directes ... ainsi que la notion de morphisme et d'isomorphisme. Par exemple, un *morphisme* entre deux représentations k-linéaires (V_1, ρ_1) et (V_2, ρ_2) de G est par définition une application $k[G]$-linéaire entre les $k[G]$-modules V_1 et V_2 associés.

Définition 2.5. *Si V_1 et V_2 sont des $k[G]$-modules, on note* $\mathrm{Hom}_{k[G]}(V_1, V_2)$ *le k-espace vectoriel des applications $k[G]$-linéaires de V_1 vers V_2.*

Une application k-linéaire $u : V_1 \to V_2$ est $k[G]$-linéaire si, et seulement si, on a

$$u \circ \rho_1(g) = \rho_2(g) \circ u, \ \ \forall\ g \in G,$$

(on parle aussi d'*opérateur d'entrelacement*). C'est un isomorphisme si, et seulement si, elle est bijective. On retrouve bien la notion d'isomorphisme de représentations déjà introduite plus haut :

1. En effet, ν est k-bilinéaire, donc (M1) et (M2) sont satisfaits et il suffit de vérifier (M3) pour $a, a' \in G$, mais c'est la définition d'une action de G sur V.

PROPOSITION 2.6. *Deux $k[G]$-modules de dimension finie U et V sont isomorphes, si et seulement si, les représentations associées (U, ρ_U) et (V, ρ_V) le sont.*

DÉMONSTRATION — Soient $e = (e_1, \ldots, e_n)$ et $f = (f_1, \ldots, f_n)$ des k-bases de U et V respectivement, et $u : U \to V$ la bijection k-linéaire définie par $u(e_i) = f_i$ pour tout i. Pour $g \in G$ on a clairement $\mathrm{Mat}_f\, u \circ \rho_U(g) \circ u^{-1} = \mathrm{Mat}_e\, \rho_U(g)$. On a donc $\mathrm{Mat}_e\, \rho_U(g) = \mathrm{Mat}_f\, \rho_V(g) \iff u \circ \rho_U(g) \circ u^{-1} = \rho_V(g)$. □

3. Décomposition en irréductibles

Soit V un $k[G]$-module. Un sous-k-espace vectoriel $W \subset V$ est dit *G-invariant* (ou *G-stable*, ou une *sous-représentation de V*) si on a $g.w \in W$ pour tout $w \in W$ et tout $g \in G$, *i.e.* si c'est un *sous-module* de V. Soient $e = (e_1, \ldots, e_{p+q})$ une base de V telle que $e_1, \ldots, e_p$ est une base de W. Alors W est G-invariant si, et seulement si, on a

$$\mathrm{Mat}_e\, \rho_V(g) = \begin{bmatrix} \star_p & \star \\ 0 & \star_q \end{bmatrix}, \quad \forall\, g \in G.$$

DÉFINITION 3.1. *Soit V un $k[G]$-module, ou ce qui revient au même, une représentation k-linéaire de G. On dit que V est* irréductible (*ou* simple), *si on a $V \neq \{0\}$ et si les seuls sous-modules de V sont $\{0\}$ et V.*

Une représentation de dimension 1 (comme la triviale) est irréductible.

PROPOSITION 3.2. *Supposons k algébriquement clos, G abélien et V un $k[G]$-module irréductible de dimension finie. Alors V est de dimension* 1.

DÉMONSTRATION — En effet, les $\rho_V(g)$ sont trigonalisables car k est algébriquement clos et V de k-dimension finie. Ils commutent entre eux car G est abélien. Ils possèdent donc une droite G-stable commune (cotrigonalisabilité) $D \subset V$. Par irréductibilité de V, on a $D = V$. □

PROPOSITION 3.3. *Un $k[G]$-module V non nul est irréductible si, et seulement si, on a $k[G]v = V$ pour tout $v \neq 0$ dans V.*

DÉMONSTRATION — En effet, si V est irréductible, et $v \in V$ est non nul, alors $k[G]v$ est un sous-module de V, nécessairement égal à V. Réciproquement, si W est un sous-module non nul de V, et si $v \in W$ est non nul, on a $V = k[G]v \subset W$, et donc $W = V$. □

En particulier, un $k[G]$-module irréductible est monogène. Attention, la réciproque est fausse : voir l'Exercice 9.10. Développons maintenant un exemple instructif. Considérons, pour $n \geqslant 2$, la représentation de permutation de S_n sur $k^n = \oplus_{i=1}^n k e_i$ de l'Exemple 1.6. Elle n'est pas irréductible. En effet, la droite D engendrée par le vecteur $(1, 1, \ldots, 1) = \sum_{i=1}^n e_i$ est fixée, donc G-stable, et définit donc une représentation de S_n isomorphe à k (la triviale). De plus, l'hyperplan $H \subset k^n$ défini par $\sum_i x_i = 0$ est également manifestement G-stable.

PROPOSITION 3.4. *Les seuls sous-modules de la représentation de permutation naturelle de* S_n *sur* k^n *sont* $\{0\}, D, H$ *et* V. *En outre, on a*

$$V = H \oplus D \iff n \in k^\times.$$

DÉMONSTRATION — Il est clair que l'on a $D \subset H \iff \sum_{i=1}^n e_i \in H \iff n.1 = 0$ dans k, d'où la seconde assertion. Montrons la première. Soit W un sous $k[\mathrm{S}_n]$-module de k^n non inclus dans la droite D. Il existe donc $x \in W$ et $i \neq j$ tels que $x_i \neq x_j$. Mais alors l'élément $x - (i\,j)\,x$ est dans W, et il est égal à

$$(x_i - x_j)(e_i - e_j).$$

Quitte à diviser par $x_i - x_j$ (non nul), on a donc $e_i - e_j \in W$. Quitte à appliquer encore des éléments de S_n, on a aussi $e_i - e_l$ dans W pour tout $l \neq i$, puis $H = \mathrm{vect}_k(e_i - e_l) \subset W$. Comme H est un hyperplan, on a $W = H$ ou $W = V$. □

DÉFINITION 3.5. *Un* $k[G]$*-module* V *est dit* semi-simple *s'il existe une décomposition en somme directe* $V = \oplus_{i \in I} V_i$ *où les* V_i *sont des sous-modules irréductibles.*

On trouve aussi la terminologie *complètement réductible* pour *semi-simple.* Il est clair que irréductible (ou nul) implique semi-simple.

PROPOSITION 3.6. (Caractérisation de la semi-simplicité) *Soit* V *un* $k[G]$*-module de dimension finie. Il y a équivalence entre :*

(a) V *est semi-simple.*

(b) V *est somme (pas forcément directe) de sous-modules irréductibles.*

(c) Pour tout sous-module W *de* V*, il existe un sous-module* S *de* V *vérifiant* $V = W \oplus S$ *(« existence d'un supplémentaire stable »).*

(d) tout sous-module de V *est semi-simple.*

DÉMONSTRATION — Les implication (a) $\Longrightarrow$ (b) et (d) $\Longrightarrow$ (a) sont triviales.

Montrons (b) $\Longrightarrow$ (c). Supposons $V = \sum_{i \in I} V_i$ avec les V_i irréductibles. Soit W un sous-module de V. Si W contient tous les V_i, on a $W = V$ et $S = \{0\}$ convient. Sinon, il existe $i \in I$ avec V_i non inclus dans W. Dans ce cas, $V_i \cap W$ est un sous-module de V_i distinct de V_i. Par irréductibilité de V_i, on a $V_i \cap W = \{0\}$. Ainsi, V_i et W sont en somme directe dans V, et $W' := V_i \oplus W$ est un sous-module de V. Par récurrence descendante sur $\dim W$, il existe un sous-module $S' \subset V$ avec $W' \oplus S' = V$. On conclut en posant $S = S' \oplus V_i$.

Montrons (c) $\Longrightarrow$ (d) par récurrence sur la dimension du sous-module $W \subset V$ en question. Le cas $W = \{0\}$ est trivial par convention, donc on suppose W non nul. Soit U un sous-module non nul de W de dimension minimale. Alors U est nécessairement irréductible. Par (c), il existe un suppémentaire G-stable S de U dans V. Tout élément de $w \in W$ s'écrit de manière unique $u + s$ avec $u \in U$ et $s \in S$, et donc $s = w - u \in S \cap W$. On a donc $W = U \oplus (S \cap W)$ avec $S \cap W$ un sous-module de V de dimension $< \dim W$, et on conclut par récurrence. □