Algèbre 1

Cours de Sandra Rozensztajn
Notes de Alexis Marchand

ENS de Lyon
S1 2017-2018
Niveau L3

Table des matières

1 Relations d'équivalence et quotients

1.1 Généralités

Définition 1.1.1 (Relation)**.** *Une* relation *sur un ensemble X est une partie $\mathcal{R}$ de $X \times X$. On notera $x\mathcal{R}y$ plutôt que $(x, y) \in \mathcal{R}$.*

Définition 1.1.2 (Relation d'équivalence)**.** *On dit qu'une relation $\mathcal{R}$ sur un ensemble X est* d'équivalence *lorsque les trois conditions suivantes sont vérifiées :*

(i) Réflexivité *:* $\forall x \in X,\ x\mathcal{R}x$.

(ii) Symétrie *:* $\forall (x, y) \in E^2,\ (x\mathcal{R}y \Longrightarrow y\mathcal{R}x)$.

(iii) Transitivité : $\forall (x,y,z) \in E^3,\ (x\mathcal{R}y \text{ et } y\mathcal{R}z \Longrightarrow x\mathcal{R}z)$.

Définition 1.1.3 (Classe d'équivalence)**.** *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble X et $x \in X$. On appelle* classe d'équivalence *de x l'ensemble noté* $\mathrm{Cl}(x)$ *et défini par* $\mathrm{Cl}(x) = \{y \in X,\ y\mathcal{R}x\}$. *On a :*

$$\forall (x,y) \in X^2,\ x\mathcal{R}y \Longleftrightarrow \mathrm{Cl}(x) = \mathrm{Cl}(y).$$

Pour $C \subset X$, on dit que C est une classe d'équivalence *pour $\mathcal{R}$ lorsque $\exists x \in X,\ C = \mathrm{Cl}(x)$. Tout élément $x \in C$ est alors appelé* représentant *de la classe C.*

Définition 1.1.4 (Partition)**.** *Si X est un ensemble, une* partition *de X est un ensemble de sous-ensembles de X non vides, deux à deux disjoints, et de réunion égale à X.*

Proposition 1.1.5. *Soit X un ensemble.*

(i) *Soit $\mathcal{R}$ une relation d'équivalence sur X. Alors $\{\mathrm{Cl}(x),\ x \in X\}$ est une partition de X.*

(ii) *Réciproquement, si $\mathfrak{P} \subset \mathcal{P}(X)$ est une partition de X, alors la relation $\mathcal{R}$ définie par*

$$\forall (x,y) \in X^2,\ x\mathcal{R}y \Longleftrightarrow (\exists C \in \mathfrak{P},\ x \in C \text{ et } y \in C)$$

est une relation d'équivalence dont les éléments de $\mathfrak{P}$ sont exactement les classes d'équivalence.

Définition 1.1.6 (Quotient)**.** *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble X. On appelle* quotient *de X par $\mathcal{R}$, noté $X/\mathcal{R}$, l'ensemble des classes d'équivalence pour $\mathcal{R}$. On appelle* projection canonique *l'application surjective*

$$\pi : \left| \begin{array}{l} X \longrightarrow X/\mathcal{R} \\ x \longmapsto \mathrm{Cl}(x) \end{array} \right. .$$

Théorème 1.1.7 (Théorème de factorisation ensembliste)**.** *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble X, $\pi : X \to X/\mathcal{R}$ la projection canonique. Soit Y un ensemble et $f : X \to Y$ une application. S'équivalent :*

(i) $\forall (x,y) \in X^2,\ x\mathcal{R}y \Longrightarrow f(x) = f(y)$.

(ii) *f se factorise par π, i.e. il existe $g : X/\mathcal{R} \to Y$ t.q. $f = g \circ \pi$.*

Si ces conditions sont vérifiées, alors la factorisation est unique.

1.2 Quotients d'espaces vectoriels

Notation 1.2.1. *Dans toute la suite, k est un corps fixé et E, V, W sont des k-espaces vectoriels.*

Définition 1.2.2 (Quotient d'espaces vectoriels)**.** *Soit F un sous-espace vectoriel de E. On définit une relation $\mathcal{R}_F$ sur E par :*

$$\forall (x,y) \in E^2,\ x\mathcal{R}_F y \Longleftrightarrow (x-y) \in F.$$

Alors $\mathcal{R}_F$ est d'équivalence et vérifie les propriétés suivantes :

(i) $\forall\, (x,x',y,y') \in E^4,\ (x\mathcal{R}_F y \text{ et } x'\mathcal{R}_F y') \Longrightarrow (x+x')\,\mathcal{R}_F\,(y+y')$,

(ii) $\forall (x,y) \in E^2,\ \forall \lambda \in k,\ x\mathcal{R}_F y \Longrightarrow (\lambda x)\,\mathcal{R}_F\,(\lambda y)$.

Le quotient $E/\mathcal{R}_F$ est noté E/F.

Théorème 1.2.3. *Soit F un sous-espace vectoriel de E. Alors il existe une unique structure de k-espace vectoriel sur E/F t.q. la projection canonique $\pi : E \to E/F$ est une application linéaire. Dans la suite, E/F sera muni de cette structure.*

Proposition 1.2.4. *Soit F un sous-espace vectoriel de E. Soit $\pi : E \to E/F$ la projection canonique.*

(i) *π est surjective et* $\mathrm{Ker}\,\pi = F$.

(ii) *Si S est un supplémentaire de F dans E (i.e. $E = F \oplus S$), alors $\pi_{|S} : S \to E/F$ est un isomorphisme d'espaces vectoriels.*

Corollaire 1.2.5. *Si E est de dimension finie et F est un sous-espace vectoriel de E alors E/F est de dimension finie, et* $\dim(E/F) = \dim E - \dim F$.

Proposition 1.2.6. *Soit F un sous-espace vectoriel de E. On note $\mathcal{G}(E/F)$ l'ensemble des sous-espaces vectoriels de E/F et $\mathcal{G}_F(E)$ l'ensemble des sous-espaces vectoriels de E contenant F. Alors l'application*

$$\Psi : \left| \begin{array}{c} \mathcal{G}(E/F) \longrightarrow \mathcal{G}_F(E) \\ H \longmapsto \pi^{-1}(H) \end{array} \right.$$

est une bijection, où $\pi : E \to E/F$ est la projection canonique.

Théorème 1.2.7 (Théorème de factorisation linéaire)**.** *Soit F un sous-espace vectoriel de E, $\pi : E \to E/F$ la projection canonique. Soit $f : E \to V$ une application linéaire. S'équivalent :*

(i) $F \subset \operatorname{Ker} f$.

(ii) *f se factorise linéairement par π, i.e. il existe $g : E/F \to V$ linéaire t.q. $f = g \circ \pi$.*

Si ces conditions sont vérifiées, alors la factorisation est unique.

2 Formes linéaires et dualité

Notation 2.0.1. *Dans toute la suite, E, V, W sont des k-espaces vectoriels.*

2.1 Formes linéaires et hyperplans

Définition 2.1.1 (Forme linéaire, hyperplan)**.**

(i) *On appelle* forme linéaire *sur E toute application linéaire de E dans k.*

(ii) *On appelle* hyperplan *de E tout sous-espace vectoriel H de E t.q. il existe $x \in E \backslash \{0\}$ avec $E = H \oplus kx$.*

Proposition 2.1.2. *Soit H un sous-espace vectoriel de E. S'équivalent :*

(i) *H est un hyperplan.*

(ii) *Il existe une forme linéaire non nulle μ sur E t.q. $H = \operatorname{Ker} \mu$.*

De plus, toutes les formes linéaires de noyau H sont colinéaires.

2.2 Espace dual et bidual

Définition 2.2.1 (Espace dual)**.** *On appelle* espace dual *de E, noté E^*, l'espace vectoriel des formes linéaires sur E.*

Proposition 2.2.2. *Soit $(e_i)_{i \in I}$ une base de E. Alors pour toute famille $(a_i)_{i \in I}$ d'éléments de k, il existe un unique $\mu_a \in E^*$ t.q. $\forall i \in I$, $\mu_a(e_i) = a_i$. On définit ainsi un isomorphisme d'espaces vectoriels entre E^* et k^I.*

Remarque 2.2.3. *Dans le cas où E est l'espace $k^{(I)}$ des familles presque nulles indexées par I, on obtient l'isomorphisme suivant :*

$$\left(k^{(I)}\right)^* \simeq k^I.$$

Corollaire 2.2.4. *Si E est de dimension finie, alors E^* est aussi de dimension finie, et on a :*

$$\dim E^* = \dim E.$$

Remarque 2.2.5. *Désormais, E, V et W sont de dimension finie.*

Définition 2.2.6 (Base duale)**.** *Soit $e = (e_1, \dots, e_n)$ une base de E. On pose $e^* = (e_1^*, \dots, e_n^*)$, avec :*

$$\forall\, (i,j) \in [\![1,n]\!]^2,\ e_i^*\,(e_j) = \delta_{ij}.$$

Alors e^* est une base de E^*, dite base duale *de e.*

Définition 2.2.7 (Espace bidual)**.** *On appelle* espace bidual *de E l'espace $E^{**} = (E^*)^*$.*

Proposition 2.2.8. *On considère :*

$$\iota : \left| \begin{array}{l} E \longrightarrow E^{**} \\ x \longmapsto \mathrm{ev}_x : \left| \begin{array}{l} E^* \longrightarrow k \\ \mu \longmapsto \mu(x) \end{array} \right. \end{array} \right. .$$

Alors ι est un isomorphisme d'espaces vectoriels (car E est de dimension finie). Cet isomorphisme sera dit canonique*.*

Proposition 2.2.9. *Soit β une base de E. On appelle β^* la base duale de β (c'est une base de E^*) et β^{**} la base duale de β^* (c'est une base de E^{**}). Alors, $\beta^{**} = \iota(\beta)$, où $\iota : E \to E^{**}$ est l'isomorphisme canonique.*

2.3 Transposée d'une application linéaire

Définition 2.3.1 (Transposée)**.** *Soit $u : E \to V$ une application linéaire. On définit la* transposée de *u par :*

$${}^t u : \left| \begin{array}{l} V^* \longrightarrow E^* \\ \mu \longmapsto \mu \circ u \end{array} \right. .$$

C'est une application linéaire.

Proposition 2.3.2. *Soit $u : E \to V$ et $v : V \to W$ deux applications linéaires. Alors :*

$${}^t(v \circ u) = {}^t u \circ {}^t v.$$

Proposition 2.3.3. *Soit β_E et β_V des bases respectives de E et V. Soit $u : E \to V$ une application linéaire. Alors :*

$$\mathcal{M}_{\beta_V^*, \beta_E^*}\left({}^t u\right) = {}^t\left(\mathcal{M}_{\beta_E, \beta_V}(u)\right).$$

Proposition 2.3.4. *Soit $u : E \to V$ une application linéaire. Alors u et ${}^t({}^t u)$ coïncident* via *les isomorphismes canoniques entre E et E^{**} et entre V et V^{**}.*

2.4 Sommes directes

Proposition 2.4.1. *Soit $E_1, \dots, E_n$ des k-espaces vectoriels. Alors l'application*

$$\left| \begin{array}{l} \left(\bigoplus_{i=1}^n E_i\right)^* \longrightarrow \bigoplus_{i=1}^n E_i^* \\ \lambda \longmapsto \left(\lambda_{|E_i}\right)_{1 \leqslant i \leqslant n} \end{array} \right.$$

est un isomorphisme, dit canonique.

2.5 Orthogonalité

Définition 2.5.1 (Orthogonal)**.** *Si $A \subset E$, on pose :*

$$A^\perp = \{\mu \in E^*,\ \forall x \in A,\ \mu(x) = 0\} = \{\mu \in E^*,\ A \subset \operatorname{Ker} \mu\}.$$

*On dit que $A^\perp$ est l'*orthogonal *de A.*

Proposition 2.5.2. *Soit F un sous-espace vectoriel de E. Alors l'application*

$$\left| \begin{array}{c} (E/F)^* \longrightarrow F^\perp \\ x \longmapsto {}^t\pi(x) \end{array} \right.,$$

où $\pi : E \to E/F$ est la projection canonique, est un isomorphisme, dit canonique.

Corollaire 2.5.3. *Soit F un sous-espace vectoriel de E. Alors :*

$$\dim F + \dim F^\perp = \dim E.$$

Proposition 2.5.4.

(i) *Si $A \subset B \subset E$, alors $B^\perp \subset A^\perp \subset E^*$.*

(ii) *Pour tout $A \subset E$, $A^\perp = \operatorname{Vect}(A)^\perp$.*

Proposition 2.5.5. *Soit F et G deux sous-espaces vectoriels de E.*

(i) $(F+G)^\perp = F^\perp \cap G^\perp$ *(et cette égalité reste vraie en dimension infinie).*

(ii) $(F \cap G)^\perp = F^\perp + G^\perp$ *(mais cette égalité est fausse en dimension infinie).*

Définition 2.5.6. *Soit $A \subset E^*$. On définit :*

$$A^\top = \{x \in E,\ \forall \mu \in A,\ \mu(x) = 0\} = \{x \in E,\ A \subset \operatorname{Ker} \mathrm{ev}_x\}.$$

Proposition 2.5.7. *Soit $A \subset E^*$. En notant $\iota : E \to E^{**}$ l'isomorphisme canonique, on a $\iota\left(A^\top\right) = A^\perp$. Par la suite, on oubliera donc la notation $A^\top$ et on identifiera $A^\perp$ à un sous-espace vectoriel de E.*

Proposition 2.5.8.

(i) *Si F est un sous-espace vectoriel de E, alors $F^{\perp\perp} = F$.*

(ii) *Si $A \subset E$, alors $A^{\perp\perp} = \operatorname{Vect}(A)$.*

Théorème 2.5.9. *On note $\mathcal{G}(E)$ (resp. $\mathcal{G}(E^*)$) l'ensemble des sous-espaces vectoriels de E (resp. de E^*). Alors l'application*

$$\left| \begin{array}{c} \mathcal{G}(E) \longrightarrow \mathcal{G}(E^*) \\ F \longmapsto F^\perp \end{array} \right.$$

est une bijection qui envoie les sous-espaces vectoriels de E de dimension d sur les sous-espaces vectoriels de E^* de dimension $(\dim E - d)$.

Théorème 2.5.10. *Soit $u : E \to V$ une application linéaire. Alors :*

$$\operatorname{Ker}\left({}^t u\right) = (\operatorname{Im} u)^\perp \qquad \text{et} \qquad \operatorname{Im}\left({}^t u\right) = (\operatorname{Ker} u)^\perp.$$

Corollaire 2.5.11. *Soit $u : E \to V$ une application linéaire. Alors :*

$$\operatorname{rg} u = \operatorname{rg}\left({}^t u\right).$$

Corollaire 2.5.12. *Soit $(n,p) \in (\mathbb{N}^*)^2$. Alors $\forall A \in \mathbb{M}_{n,p}(k)$, $\operatorname{rg} A = \operatorname{rg}({}^t A)$.*

3 Formes bilinéaires

Notation 3.0.1. *On fixe $n \in \mathbb{N}^*$, $E, F, G, E_1, \ldots, E_n$ des k-espaces vectoriels de dimension finie.*

3.1 Applications multilinéaires

Définition 3.1.1 (Application multilinéaire)**.** *On dit qu'une application $f : E_1 \times \cdots \times E_n \to F$ est* n-linéaire *lorsque pour tout $i \in [\![1, n]\!]$ et pour tout $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in E_1 \times \cdots \times E_{i-1} \times E_{i+1} \times \cdots \times E_n$, l'application $x \in E_i \longmapsto f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n) \in F$ est linéaire. On note $n\text{-Lin}(E_1, \ldots, E_n, F)$ l'espace vectoriel des applications n-linéaires $E_1 \times \cdots \times E_n \to F$. Si $n = 2$, on parle d'*applications bilinéaires*, et on note* $\text{Bil}(E_1, E_2, F) = 2\text{-Lin}(E_1, E_2, F)$. *Si $F = k$, on parle de* formes n-linéaires *ou* bilinéaires*. On pourra noter $n\text{-Lin}(E_1, \ldots, E_n) = n\text{-Lin}(E_1, \ldots, E_n, k)$ et $\text{Bil}(E_1, E_2) = \text{Bil}(E_1, E_2, k)$.*

Exemple 3.1.2.

(i) *Soit $(\mu_1, \ldots, \mu_n) \in E_1^* \times \cdots \times E_n^*$. Alors l'application* $\left|\begin{array}{l} E_1 \times \cdots \times E_n \longrightarrow k \\ (x_1, \ldots, x_n) \longmapsto \mu_1(x_1) \cdots \mu_n(x_n) \end{array}\right.$ *est une forme n-linéaire.*

(ii) *Si $\mathcal{A}$ est une k-algèbre, alors l'application* $\left|\begin{array}{l} \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A} \\ (a, b) \longmapsto ab \end{array}\right.$ *est bilinéaire.*

(iii) *L'application* $\left|\begin{array}{l} E \times E^* \longrightarrow k \\ (x, \mu) \longmapsto \mu(x) \end{array}\right.$ *est une forme bilinéaire appelée* crochet de dualité.

(iv) *Si $E = k^n$, alors* $\det : E^n \to k$ *est n-linéaire.*

3.2 Formes bilinéaires

Proposition 3.2.1. *Soit $(e_i)_{i \in I}$, $(f_j)_{j \in J}$ des bases respectives de E et F. Alors l'application*

$$\Phi : \left|\begin{array}{l} \text{Bil}(E, F, G) \longrightarrow G^{I \times J} \\ \qquad\qquad u \longmapsto (u(e_i, f_j))_{(i,j) \in I \times J} \end{array}\right.$$

est un isomorphisme d'espaces vectoriels. En particulier :

$$\dim \text{Bil}(E, F, G) = (\dim E)(\dim F)(\dim G).$$

Corollaire 3.2.2. $\dim \text{Bil}(E, F) = (\dim E)(\dim F)$.

Définition 3.2.3 (Matrice d'une forme bilinéaire)**.** *Soit $\beta_E = (e_i)_{1 \leqslant i \leqslant n}, \beta_F = (f_j)_{1 \leqslant j \leqslant p}$ des bases respectives de E et F. Pour $\phi \in \text{Bil}(E, F)$, on appelle* matrice de ϕ *dans les bases β_E, β_F la matrice suivante :*

$$\mathcal{M}_{\beta_E, \beta_F}(\phi) = (\phi(e_i, e_j))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} \in \mathbb{M}_{n,p}(k).$$

Si $E = F$ et $\beta_E = \beta_F$, on notera $\mathcal{M}_{\beta_E}(\phi) = \mathcal{M}_{\beta_E, \beta_E}(\phi)$.

Proposition 3.2.4. *Soit $\beta_E = (e_i)_{1 \leqslant i \leqslant n}, \beta_F = (f_j)_{1 \leqslant j \leqslant p}$ des bases respectives de E et F. Soit $\phi \in \text{Bil}(E, F)$. Alors $\mathcal{M}_{\beta_E, \beta_F}(\phi)$ est l'unique matrice $A \in \mathbb{M}_{n,p}(k)$ t.q.*

$$\forall (x, y) \in E \times F,\ \phi(x, y) = {}^tXAY \qquad \text{avec} \begin{cases} X = \mathcal{M}_{\beta_E}(x) \\ Y = \mathcal{M}_{\beta_F}(y) \end{cases}.$$

Proposition 3.2.5. *Soit β_E, β'_E deux bases de E, β_F, β'_F deux bases de F. Soit $P_E \in GL_n(k)$ la matrice de passage de β_E à β'_E, soit $P_F \in GL_p(k)$ la matrice de passage de β_F à β'_F. Alors :*

$$\mathcal{M}_{\beta'_E, \beta'_F}(\phi) = {}^tP_E \mathcal{M}_{\beta_E, \beta_F}(\phi) P_F.$$

Définition 3.2.6 (Rang d'une forme bilinéaire)**.** *Soit $\phi \in \text{Bil}(E, F)$. On appelle* rang de ϕ *le rang de la matrice $\mathcal{M}_{\beta_E, \beta_F}(\phi)$, où β_E, β_F sont des bases quelconques de E et F. D'après la proposition 3.2.5, cette définition ne dépend pas du choix de β_E, β_F.*

3.3 Formes bilinéaires et dualité

Définition 3.3.1. *Soit $\phi \in \mathrm{Bil}(E,F)$. On définit deux applications linéaires $\ell_\phi \in \mathcal{L}(E,F^*)$ et $r_\phi \in \mathcal{L}(F,E^*)$ par :*

$$\ell_\phi : \left| \begin{array}{c} E \longrightarrow F^* \\ x \longmapsto \phi(x,\cdot) \end{array} \right. \qquad et \qquad r_\phi : \left| \begin{array}{c} F \longrightarrow E^* \\ y \longmapsto \phi(\cdot,y) \end{array} \right. .$$

Proposition 3.3.2. *Les applications suivantes sont des isomorphismes d'espaces vectoriels :*

$$L : \left| \begin{array}{c} \mathrm{Bil}(E,F) \longrightarrow \mathcal{L}(E,F^*) \\ \phi \longmapsto \ell_\phi \end{array} \right. \qquad et \qquad R : \left| \begin{array}{c} \mathrm{Bil}(E,F) \longrightarrow \mathcal{L}(F,E^*) \\ \phi \longmapsto r_\phi \end{array} \right. .$$

Remarque 3.3.3. *On a $\forall u \in \mathcal{L}(E,F^*)$, $R \circ L^{-1}(u) = {}^t u$.*

Proposition 3.3.4. *Soit β_E, β_F des bases respectives de E et F. Soit $\phi \in \mathrm{Bil}(E,F)$. Alors :*

$$\mathcal{M}_{\beta_E,\beta_F}(\phi) = \mathcal{M}_{\beta_E,\beta_F^*}(\ell_\phi) \qquad et \qquad {}^t(\mathcal{M}_{\beta_E,\beta_F}(\phi)) = \mathcal{M}_{\beta_F,\beta_E^*}(r_\phi).$$

Corollaire 3.3.5. *Pour $\phi \in \mathrm{Bil}(E,F)$, $\operatorname{rg}\phi = \operatorname{rg}\ell_\phi = \operatorname{rg} r_\phi$.*

Exemple 3.3.6. *Si $\phi \in \mathrm{Bil}(E,E^*)$ est le crochet de dualité, alors $\ell_\phi \in \mathcal{L}(E,E^{**})$ est l'isomorphisme canonique et $r_\phi = id_{E^*}$.*

Définition 3.3.7 (Forme bilinéaire non dégénérée)**.** *Soit $\phi \in \mathrm{Bil}(E,F)$. S'équivalent :*

(i) *Il existe β_E, β_F bases de E, F t.q. $\mathcal{M}_{\beta_E,\beta_F}(\phi)$ est inversible.*

(ii) *Pour tous β_E, β_F bases de E, F, $\mathcal{M}_{\beta_E,\beta_F}(\phi)$ est inversible.*

(iii) *ℓ_ϕ est un isomorphisme.*

(iv) *r_ϕ est un isomorphisme.*

Si ces conditions sont vérifiées, on dit que ϕ est une forme bilinéaire non dégénérée*.*

Remarque 3.3.8. *Pour que $\phi \in \mathrm{Bil}(E,F)$ soit non dégénérée, il est nécessaire que $\dim E = \dim F$.*

Exemple 3.3.9. *Le crochet de dualité est une forme bilinéaire non dégénérée.*

Proposition 3.3.10. *Soit $\phi \in \mathrm{Bil}(E,F)$. On note $E' = E/\operatorname{Ker}\ell_\phi$ et $F' = F/\operatorname{Ker} r_\phi$, et on pose π_E et π_F les projections canoniques respectives associées à ces deux quotients. Alors il existe une unique $\phi' \in \mathrm{Bil}(E',F')$ vérifiant :*

$$\forall (x,y) \in E \times F,\ \phi'(\pi_E(x), \pi_F(y)) = \phi(x,y).$$

De plus, ϕ' est non dégénérée.

Notation 3.3.11. *On notera $\mathrm{Bil}(E) = \mathrm{Bil}(E,E) = \mathrm{Bil}(E,E,k)$.*

Proposition 3.3.12. *L'isomorphisme* $\left| \begin{array}{c} \mathrm{Bil}(E) \longrightarrow \mathcal{L}(E,E^*) \\ \phi \longmapsto \ell_\phi \end{array} \right.$ *fait correspondre les formes bilinéaires non dégénérées avec les isomorphismes de E dans E^*.*

3.4 Orthogonalité

Définition 3.4.1 (Orthogonal)**.** *Soit $\phi \in \mathrm{Bil}(E,F)$.*

(i) *Pour $V \subset E$, on note $V^\perp = \{y \in F,\ \forall x \in V,\ \phi(x,y) = 0\}$.*

(ii) *Pour $W \subset F$, on note $W^\perp = \{x \in E,\ \forall y \in W,\ \phi(x,y) = 0\}$.*

Remarque 3.4.2. *Si $\phi \in \mathrm{Bil}(E,E^*)$ est le crochet de dualité, on retrouve la notion d'orthogonalité de la définition 2.5.1.*

Proposition 3.4.3. *Soit $\phi \in \mathrm{Bil}(E,F)$.*

(i) *Pour $V \subset E$, on a $V^\perp = \ell_\phi(V)^\perp$, où $V^\perp$ est compris au sens de la définition 3.4.1 et $\ell_\phi(V)^\perp$ est compris au sens de la définition 2.5.1.*

(ii) *Pour $W \subset F$, on a $W^\perp = r_\phi(W)^\perp$, où $W^\perp$ est compris au sens de la définition 3.4.1 et $r_\phi(W)^\perp$ est compris au sens de la définition 2.5.1.*

Proposition 3.4.4. *Soit $\phi \in \mathrm{Bil}(E,F)$.*

(i) *Pour V sous-espace vectoriel de E, on a $\dim V + \dim V^\perp \geqslant \dim F$, avec égalité dès que ϕ est non dégénérée.*

(ii) *Pour W sous-espace vectoriel de F, on a $\dim W + \dim W^\perp \geqslant \dim E$, avec égalité dès que ϕ est non dégénérée.*

Corollaire 3.4.5. *Soit $\phi \in \mathrm{Bil}(E,F)$. On suppose ϕ non dégénérée. Alors, pour V sous-espace vectoriel de E, on a $V = E \iff V^\perp = \{0_F\}$ et $V = \{0_E\} \iff V^\perp = F$.*

3.5 Formes symétriques, alternées et antisymétriques

Définition 3.5.1 (Formes symétriques, alternées et antisymétriques)**.** *Soit $\phi \in \mathrm{Bil}(E)$.*

(i) *On dit que ϕ est* symétrique *lorsque $\forall (x,y) \in E^2$, $\phi(x,y) = \phi(y,x)$.*

(ii) *On dit que ϕ est* antisymétrique *lorsque $\forall (x,y) \in E^2$, $\phi(x,y) = -\phi(y,x)$.*

(iii) *On dit que ϕ est* alternée *lorsque $\forall x \in E$, $\phi(x,x) = 0$.*

Proposition 3.5.2. *Soit $\phi \in \mathrm{Bil}(E)$.*

(i) *ϕ est symétrique $\iff \ell_\phi = r_\phi \iff {}^t\ell_\phi = \ell_\phi \iff {}^tr_\phi = r_\phi$.*

(ii) *ϕ est antisymétrique $\iff \ell_\phi = -r_\phi \iff {}^t\ell_\phi = -\ell_\phi \iff {}^tr_\phi = -r_\phi$.*

Corollaire 3.5.3. *Soit $\phi \in \mathrm{Bil}(E)$. Si ϕ est symétrique ou antisymétrique, la notation $V^\perp$, pour $V \subset E$, n'est pas ambiguë : elle ne dépend pas du fait de voir V comme partie du "premier" ou du "second" E.*

Proposition 3.5.4. *Toute forme bilinéaire alternée est antisymétrique. De plus, si $\operatorname{car} k \neq 2$, alors la réciproque est vraie.*

Proposition 3.5.5. *Soit $\phi \in \mathrm{Bil}(E)$, β_E une base de E.*

(i) *ϕ est symétrique $\iff \mathcal{M}_{\beta_E}(\phi)$ est symétrique.*

(ii) *ϕ est antisymétrique $\iff \mathcal{M}_{\beta_E}(\phi)$ est antisymétrique.*

(iii) *ϕ est alternée $\iff \mathcal{M}_{\beta_E}(\phi)$ est antisymétrique avec des zéros sur la diagonale.*

Définition 3.5.6.

(i) *On note $S(E) \subset \mathrm{Bil}(E)$ l'espace des formes bilinéaires symétriques.*

(ii) *On note $A(E) \subset \mathrm{Bil}(E)$ l'espace des formes bilinéaires alternées.*

Proposition 3.5.7. *On note $n = \dim E$.*

(i) *$\dim S(E) = \frac{n(n+1)}{2}$ et $\dim A(E) = \frac{n(n-1)}{2}$.*

(ii) *Si $\operatorname{car} k \neq 2$, alors $\mathrm{Bil}(E) = S(E) \oplus A(E)$.*

4 Formes quadratiques

Notation 4.0.1. *Dans la suite, on suppose que $\operatorname{car} k \neq 2$, et on note E, E' deux k-espaces vectoriels de dimension finie.*

4.1 Généralités

Définition 4.1.1 (Forme quadratique)**.** *On appelle* forme quadratique *sur E toute application $q : E \to k$ t.q. il existe $\phi \in \mathrm{Bil}(E)$ t.q.*

$$\forall x \in E,\ q(x) = \phi(x, x).$$

On dit alors que q est la forme quadratique associée à ϕ. On note $Q(E)$ l'espace vectoriel des formes quadratiques sur E.

Proposition 4.1.2. *On considère :*

$$p : \left| \begin{array}{l} \mathrm{Bil}(E) \longrightarrow Q(E) \\ \qquad \phi \longmapsto \left| \begin{array}{l} E \longrightarrow k \\ x \longmapsto \phi(x, x) \end{array} \right. \end{array} \right. .$$

Alors p est linéaire, surjective et $\operatorname{Ker} p = A(E)$.

Corollaire 4.1.3. $Q(E) \simeq \mathrm{Bil}(E)/A(E) \simeq S(E)$.

Définition 4.1.4 (Forme polaire)**.** *On appelle* forme polaire *de $q \in Q(E)$ l'unique forme bilinéaire symétrique ϕ t.q. q est associée à ϕ. On a :*

$$\forall (x, y) \in E^2,\ \phi(x, y) = \frac{1}{4}\left(q(x + y) - q(x - y)\right).$$

Définition 4.1.5 (Rang d'une forme quadratique)**.** *Étant donné une forme quadratique $q \in Q(E)$, on appelle* rang *de q le rang de la forme polaire de q. On dit que q est* non dégénérée *si sa forme polaire est non dégénérée.*

Proposition 4.1.6. *Soit F un sous-espace vectoriel de E et $q \in Q(E)$. Alors $q_{|F}$ est une forme quadratique, dont la forme polaire est $\phi_{|F \times F}$, où ϕ est la forme polaire de q.*

Proposition 4.1.7. *Soit $\beta = (e_1, \ldots, e_n)$ une base de E. Soit $q : E \to k$. On considère :*

$$f_q : \left| \begin{array}{l} k^n \longrightarrow k \\ (x_1, \ldots, x_n) \longmapsto q\left(\displaystyle\sum_{i=1}^{n} x_i e_i\right) \end{array} \right. .$$

Alors q est une forme quadratique ssi *f_q est un polynôme homogène (i.e. dont tous les monômes sont de même degré) de degré* 2.

4.2 Matrice d'une forme quadratique

Définition 4.2.1 (Isomorphisme de formes quadratiques)**.** *Soit $q \in Q(E)$, $q' \in Q(E')$. On dit que q et q' sont* isomorphes *s'il existe un isomorphisme d'espaces vectoriels $u : E \to E'$ tel que $q = q' \circ u$.*

Définition 4.2.2 (Matrice d'une forme quadratique)**.** *Soit $q \in Q(E)$, β une base de E. On appelle matrice de q dans la base β, notée $\mathcal{M}_\beta(q)$, la matrice de la forme polaire de q dans la base β.*

Remarque 4.2.3. *Soit $q \in Q(E)$, β une base de E. Alors $\mathcal{M}_\beta(q)$ est symétrique.*

Proposition 4.2.4. *Soit $q \in Q(E)$, β et β' deux bases de E, P la matrice de passage de β à β'. Alors :*

$$\mathcal{M}_{\beta'}(q) = {}^tP \mathcal{M}_\beta(q) P.$$

Définition 4.2.5 (Matrices congruentes)**.** *On dit que deux matrices $A, A' \in \mathbb{M}_n(k)$ sont* congruentes *lorsque :*

$$\exists P \in GL_n(k),\ A' = {}^tPAP.$$

Proposition 4.2.6. *Soit $q, q' \in Q(E)$, β une base de E. Alors q et q' sont isomorphes* ssi *$\mathcal{M}_\beta(q)$ et $\mathcal{M}_\beta(q')$ sont congruentes.*

4.3 Discriminant d'une forme quadratique

Définition 4.3.1 (Discriminant d'une forme quadratique dans une base)**.** *Pour $q \in Q(E)$ et β base de E, on définit le* discriminant *de q dans la base β par :*

$$\operatorname{disc}_\beta(q) = \det \mathcal{M}_\beta(q).$$

Définition 4.3.2 (Discriminant d'une forme quadratique)**.** *Pour $q \in Q(E)$, on appelle* discriminant *de q, noté* $\operatorname{disc} q$*, la classe de* $\operatorname{disc}_\beta(q)$ *dans $k/\sim$ (où $\sim$ est définie par : $\forall (x,y) \in k^2,\ x \sim y \iff \exists c \in k^*,\ x = c^2 y$), où β est n'importe quelle base de E.*

Proposition 4.3.3.

(i) *Une forme quadratique est non dégénérée* ssi *son discriminant est non nul.*

(ii) *Deux formes quadratiques isomorphes ont le même discriminant.*

4.4 Orthogonalité

Définition 4.4.1 (Orthogonal)**.** *Soit $q \in Q(E)$, ϕ sa forme polaire. Pour $A \subset E$, on note $A^\perp$ l'orthogonal de A au sens des formes bilinéaires :*

$$A^\perp = \{x \in E,\ \forall a \in A,\ \phi(x,a) = 0\}.$$

Définition 4.4.2 (Noyau d'une forme quadratique)**.** *Soit $q \in Q(E)$, ϕ sa forme polaire. On appelle* noyau *de q le noyau de ϕ :*

$$\operatorname{Ker} q = \operatorname{Ker} \ell_\phi = \operatorname{Ker} r_\phi = E^\perp.$$

Proposition 4.4.3. *Une forme quadratique est non dégénérée* ssi *son noyau est nul.*

Remarque 4.4.4. *Soit q une forme quadratique et F un sous-espace vectoriel de E. Alors $F \cap \operatorname{Ker} q \subset \operatorname{Ker} q_{|F}$, mais ce n'est pas forcément une égalité.*

Proposition 4.4.5. *Soit $q \in Q(E)$ et F un sous-espace vectoriel de E. Alors :*

$$\dim F + \dim F^\perp \geqslant \dim E,$$

avec égalité ssi *q est non dégénérée.*

Remarque 4.4.6. *Soit $q \in Q(E)$ et F un sous-espace vectoriel de E. On peut avoir $E \supsetneq F + F^\perp$ même si q est non dégénérée.*

Proposition 4.4.7. *Soit $q \in Q(E)$. On note $E' = E/\operatorname{Ker} q$, et π la projection canonique associée. Alors il existe une unique forme quadratique $q' \in Q(E')$ t.q. $q = q' \circ \pi$. De plus, q' est non dégénérée.*

Remarque 4.4.8. *Soit $q \in Q(E)$, $E' = E/\operatorname{Ker} q$ et $q' \in Q(E')$ définie comme ci-dessus. Alors, si S est un supplémentaire de* $\operatorname{Ker} q$ *dans E, $q_{|S}$ et q' sont isomorphes.*

4.5 Adjoint d'un endomorphisme

Définition 4.5.1 (Adjoint d'un endomorphisme)**.** *Soit $q \in Q(E)$, ϕ sa forme polaire. Soit $u \in \mathcal{L}(E)$. Alors il existe un unique endomorphisme $u^* \in \mathcal{L}(E)$ t.q.*

$$\forall (x,y) \in E^2,\ \phi(u(x), y) = \phi(x, u^*(y)).$$

*On dit que u^* est l'*adjoint *de u.*

Proposition 4.5.2. *Soit $q \in Q(E)$. L'application* $\left| \begin{array}{c} \mathcal{L}(E) \longrightarrow \mathcal{L}(E) \\ u \longmapsto u^* \end{array} \right.$ *est linéaire, bijective et involutive. De plus $\forall (u,v) \in \mathcal{L}(E)^2,\ (v \circ u)^* = u^* \circ v^*$.*

Proposition 4.5.3. *Soit $q \in Q(E)$, $u \in \mathcal{L}(E)$ et β une base de E. Alors :*

$$\mathcal{M}_\beta(u^*) = {}^t\!\left(\mathcal{M}_\beta(q)\mathcal{M}_\beta(u)\mathcal{M}_\beta(q)^{-1}\right).$$

4.6 Cône isotrope d'une forme quadratique

Définition 4.6.1 (Cône isotrope)**.** *Soit $q \in Q(E)$. On définit le* cône isotrope *de q par :*

$$\mathcal{C}(q) = \{x \in E,\ q(x) = 0\}.$$

Les éléments de $\mathcal{C}(q)$ sont appelés vecteurs isotropes*. Si $\mathcal{C}(q) = \{0\}$, on dit que q est* anisotrope*.*

Proposition 4.6.2. *Soit $q \in Q(E)$.*

(i) $\forall x \in \mathcal{C}(q),\ \forall \lambda \in k,\ (\lambda x) \in \mathcal{C}(q)$.

(ii) $\operatorname{Ker} q \subset \mathcal{C}(q)$ *mais on n'a pas nécessairement égalité (et $\mathcal{C}(q)$ n'est pas forcément un sous-espace vectoriel de E).*

4.7 Bases orthogonales

Définition 4.7.1 (Famille orthogonale)**.** *Soit $q \in Q(E)$, ϕ sa forme polaire. On dit qu'une famille $(x_i)_{i\in I} \in E^I$ est* orthogonale *lorsque :*

$$\forall (i,j) \in I^2,\ i \neq j \Longrightarrow \phi(x_i, x_j) = 0.$$

On appelle base orthogonale *toute base de E qui est orthogonale.*

Proposition 4.7.2. *Soit $q \in Q(E)$, β une base de E. Alors β est une base orthogonale* ssi *$\mathcal{M}_\beta(q)$ est diagonale.*

Théorème 4.7.3. *Toute forme quadratique admet une base orthogonale.*

Démonstration. Par récurrence sur $n = \dim E$. Clair pour $n = 1$. Supposons le résultat vrai jusqu'à $(n-1)$ et soit E un espace vectoriel de dimension n. Si $q = 0$, toute base est orthogonale. Sinon, soit $e_1 \in E$ t.q. $q(e_1) \neq 0$. On note $H = \{e_1\}^\perp$. Alors $H \cap (ke_1) = \{0\}$. Et on a $\dim H + \dim(ke_1) \geqslant \dim E$, d'où $E = H \oplus (ke_1)$. On conclut alors en appliquant l'hypothèse de récurrence à H. □

Proposition 4.7.4. *Soit $q \in Q(E)$. Se donner une base orthogonale de E revient à se donner une famille $(\mu_1, \ldots, \mu_r) \in (E^*)^r$ de formes linéaires sur E linéairement indépendantes et une famille $(a_1, \ldots, a_r) \in k^r$ t.q.*

$$\forall x \in E,\ q(x) = \sum_{i=1}^{r} a_i \mu_i(x)^2.$$

Proposition 4.7.5. *Soit $q \in Q(E)$. Soit $(\mu_1, \ldots, \mu_n) \in (E^*)^n$ une base de E^* et $(a_1, \ldots, a_n) \in k^n$ t.q. $\forall x \in E,\ q(x) = \sum_{i=1}^n a_i \mu_i(x)^2$. Alors :*

(i) *q est non dégénérée* ssi *$\forall i \in [\![1, n]\!],\ a_i \neq 0$.*

(ii) *$\operatorname{disc} q$ est la classe de $\prod_{i=1}^n a_i$.*

(iii) $\operatorname{Ker} q = \bigcap_{\substack{1 \leqslant i \leqslant n \\ a_i \neq 0}} \{\mu_i\}^\perp$.

(iv) $\operatorname{rg} q = |\{i \in [\![1, n]\!],\ a_i \neq 0\}|$.

Remarque 4.7.6. *Soit $q, q' \in Q(E)$, $(\mu_1, \ldots, \mu_n)$, $(\lambda_1, \ldots, \lambda_n)$ deux bases de E^* et $(a_1, \ldots, a_n) \in k^n$, $(b_1, \ldots, b_n) \in k^n$ t.q. $\forall x \in E,\ q(x) = \sum_{i=1}^n a_i \mu_i(x)^2$ et $q'(x) = \sum_{i=1}^n b_i \lambda_i(x)^2$. Si $\forall i \in [\![1, n]\!],\ a_i = b_i$ alors q et q' sont isomorphes. Réciproquement, si q et q' sont isomorphes, on peut trouver des bases $(\mu_1, \ldots, \mu_n)$ et $(\lambda_1, \ldots, \lambda_n)$ de E^* t.q. on ait les écritures ci-dessus avec $\forall i \in [\![1, n]\!],\ a_i = b_i$. Mais l'isomorphisme de formes quadratiques n'est pas toujours aussi facile à vérifier.*

4.8 Méthode de Gauß

Théorème 4.8.1 (Méthode de Gauß)**.** *La* méthode de Gauß *est un algorithme permettant, à partir de $q \in Q(E)$, de déterminer une base $(\mu_1, \dots, \mu_n) \in (E^*)^n$ et une famille $(a_1, \dots, a_n) \in k^n$ t.q. $\forall x \in E,\ q(x) = \sum_{i=1}^n a_i \mu_i(x)^2$.*

Démonstration. On se ramène au cas où $E = k^n$, quitte à se donner une base de E. On procède ensuite par récurrence sur n. Le résultat est clair pour $n = 1$. En supposant le résultat vrai jusqu'à $(n-1)$, soit $q \in Q(k^n)$. On se donne $(\alpha_i)_{1 \leqslant i \leqslant n}$, $(\beta_{ij})_{1 \leqslant i < j \leqslant n}$ t.q.

$$\forall x \in k^n,\ q(x) = \sum_{1 \leqslant i \leqslant n} \alpha_i x_i^2 + \sum_{1 \leqslant i < j \leqslant n} \beta_{ij} x_i x_j.$$

On distingue deux cas. *Premier cas* : $\exists i \in [\![1, n]\!],\ \alpha_i \neq 0$. Par exemple, supposons $\alpha_1 \neq 0$. Alors :

$$\forall x \in k^n,\ q(x) = \alpha_1 \left(\underbrace{x_1 + \frac{1}{2\alpha_1} \sum_{2 \leqslant j \leqslant n} \beta_{1j} x_j}_{\mu_1(x)} \right)^2 + \underbrace{\sum_{2 \leqslant i < j \leqslant n} \beta_{ij} x_i x_j - \frac{1}{4\alpha_1} \left(\sum_{2 \leqslant j \leqslant n} \beta_{1j} x_j \right)^2}_{q'(x_2, \dots, x_n)}.$$

Ainsi, $\mu_1 \in (k^n)^*$ et $q' \in Q(k^{n-1})$. On applique l'hypothèse de récurrence à q', puis on conclut. *Second cas* : $\forall i \in [\![1, n]\!],\ \alpha_i = 0$. On peut supposer $q \neq 0$. Dans ce cas, il existe $1 \leqslant i < j \leqslant n$ t.q. $\beta_{ij} \neq 0$. Par exemple, supposons que $\beta_{12} \neq 0$. Alors :

$$\begin{aligned}
\forall x \in k^n,\ q(x) &= \beta_{12} x_1 x_2 + x_1 \underbrace{\sum_{3 \leqslant j \leqslant n} \beta_{1j} x_j}_{L_1(x_3, \dots, x_n)} + x_2 \underbrace{\sum_{3 \leqslant j \leqslant n} \beta_{2j} x_j}_{L_2(x_3, \dots, x_n)} + \sum_{3 \leqslant i < j \leqslant n} \beta_{ij} x_i x_j \\
&= \beta_{12} \left(\overbrace{x_1 + \frac{1}{\beta_{12}} L_2(x_3, \dots, x_n)}^{\lambda_1(x)} \right) \left(\overbrace{x_2 + \frac{1}{\beta_{12}} L_1(x_3, \dots, x_n)}^{\lambda_2(x)} \right) \\
&\qquad + \underbrace{\sum_{3 \leqslant i < j \leqslant n} \beta_{ij} x_i x_j - \frac{1}{\beta_{12}} L_1(x_3, \dots, x_n) L_2(x_3, \dots, x_n)}_{q''(x_3, \dots, x_n)} \\
&= \beta_{12} \left(\underbrace{\frac{\lambda_1(x) + \lambda_2(x)}{2}}_{\mu_1'(x)} \right)^2 - \beta_{12} \left(\underbrace{\frac{\lambda_1(x) - \lambda_2(x)}{2}}_{\mu_2'(x)} \right)^2 + q''(x_3, \dots, x_n).
\end{aligned}$$

Ainsi, $\mu_1', \mu_2' \in (k^n)^*$ et $q'' \in Q(k^{n-2})$. On applique l'hypothèse de récurrence à q'', et on conclut. □

4.9 Classification des formes quadratiques sur $\mathbb{R}$ et $\mathbb{C}$

Théorème 4.9.1. *Soit $q \in Q(\mathbb{C}^n)$. On note $r = \operatorname{rg} q$. Alors il existe des formes linéaires $\mu_1, \dots, \mu_r$ linéairement indépendantes t.q.*

$$q = \sum_{i=1}^r \mu_i(x)^2.$$

De plus, deux formes quadratiques sur $\mathbb{C}^n$ sont isomorphes ssi *elles ont le même rang.*

Définition 4.9.2 (Formes positives, négatives)**.** *Soit $q \in Q(\mathbb{R}^n)$.*

(i) *On dit que q est* positive *lorsque $\forall x \in \mathbb{R}^n,\ q(x) \geqslant 0$.*

(ii) *On dit que q est* définie positive *lorsque $\forall x \in \mathbb{R}^n \backslash \{0\},\ q(x) > 0$.*

(iii) *On dit que q est* négative *lorsque* $\forall x \in \mathbb{R}^n,\ q(x) \leqslant 0$.

(iv) *On dit que q est* définie négative *lorsque* $\forall x \in \mathbb{R}^n \backslash \{0\},\ q(x) < 0$.

Remarque 4.9.3. *Si $q \in Q(\mathbb{R}^n)$ est définie (positive ou négative) alors $\mathcal{C}(q) = \{0\}$. En particulier,* $\operatorname{Ker} q = \{0\}$ *donc q est non dégénérée.*

Théorème 4.9.4 (Loi d'inertie de Sylvester)**.** *Soit $q \in Q(\mathbb{R}^n)$. Soit $(r, s) \in \mathbb{N}^2$ t.q. il existe des formes linéaires $\mu_1, \ldots, \mu_{r+s}$ linéairement indépendantes t.q.*

$$\forall x \in \mathbb{R}^n,\ q(x) = \sum_{i=1}^{r} \mu_i(x)^2 - \sum_{i=r+1}^{r+s} \mu_i(x)^2.$$

Alors :

(i) $r = \max\Big\{\rho \in \mathbb{N},\ \exists F$ *sous-espace vectoriel de* $\mathbb{R}^n,\ \dim F = \rho$ et $q_{|F}$ *est définie positive*$\Big\}$.

(ii) $s = \max\Big\{\sigma \in \mathbb{N},\ \exists F$ *sous-espace vectoriel de* $\mathbb{R}^n,\ \dim F = \sigma$ et $q_{|F}$ *est définie négative*$\Big\}$.

Démonstration. On complète $(\mu_1, \ldots, \mu_{r+s})$ en une base $(\mu_1, \ldots, \mu_n)$ de $(\mathbb{R}^n)^*$. On note $(e_1, \ldots, e_n)$ la base préduale de $(\mu_1, \ldots, \mu_n)$ et on pose $F^+ = \operatorname{Vect}(e_1, \ldots, e_r)$, $F^- = \operatorname{Vect}(e_{r+1}, \ldots, e_{r+s})$ et $F^0 = \operatorname{Vect}(e_{r+s+1}, \ldots, e_n)$. Alors $\mathbb{R}^n = F^+ \oplus F^- \oplus F^0$. De plus, $q_{|F^+}$ est définie positive et $q_{|F^-}$ est définie négative, ce qui prouve les inégalités $(\leqslant)$. Réciproquement, soit F, F' des sous-espaces vectoriels de $\mathbb{R}^n$ t.q. $q_{|F}$ et $q_{|F'}$ sont respectivement définie positive et définie négative. Alors :

$$F \cap \left(F^- \oplus F^0\right) = F' \cap \left(F^+ \oplus F^0\right) = \{0\}.$$

Ceci prouve que $\dim F \leqslant r$ et $\dim F' \leqslant s$. D'où les inégalités $(\geqslant)$. □

Théorème 4.9.5. *Soit $q \in Q(\mathbb{R}^n)$. Alors il existe un couple $(r, s) \in \mathbb{N}^2$ et des formes linéaires $\mu_1, \ldots, \mu_{r+s}$ linéairement indépendantes t.q.*

$$\forall x \in \mathbb{R}^n,\ q(x) = \sum_{i=1}^{r} \mu_i(x)^2 - \sum_{i=r+1}^{r+s} \mu_i(x)^2.$$

Le couple (r, s) est uniquement déterminé par q ; il est appelé signature *de q. Et deux formes quadratiques sont isomorphes* ssi *elles ont la même signature.*

Proposition 4.9.6. *Soit $q \in Q(\mathbb{R}^n)$ une forme quadratique de signature (r, s). Alors :*

(i) *q est positive* ssi $s = 0$.

(ii) *q est définie positive* ssi $r = n$.

(iii) *q est négative* ssi $r = 0$.

(iv) *q est définie négative* ssi $s = n$.

(v) $\operatorname{rg} q = r + s$.

(vi) *q est non dégénérée* ssi $r + s = n$.

Corollaire 4.9.7. *Soit $q \in \mathcal{Q}(\mathbb{R}^n)$. Alors $\mathcal{C}(q) = \{0\}$* ssi *q est définie (positive ou négative).*

5 Produit tensoriel d'espaces vectoriels de dimension finie

Notation 5.0.1. *Dans la suite, k est un corps et tous les espaces vectoriels considérés sont sur k et de dimension finie.*

5.1 Généralités

Définition 5.1.1 (Produit tensoriel d'espaces vectoriels)**.** *Soit E, F deux k-espaces vectoriels de dimension finie. Soit $(e_1, \dots, e_n)$ une base de E, $(f_1, \dots, f_m)$ une base de F. On définit le* produit tensoriel *de E et F comme le couple $(E \otimes F, b_{E,F})$, où $E \otimes F$ est un k-espace vectoriel de dimension nm et $b_{E,F} : E \times F \to E \otimes F$ est une application bilinéaire t.q. $(b_{E,F}(e_i, f_j))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant m}}$ est une base de $E \otimes F$.*

Théorème 5.1.2. *Soit E, F deux k-espaces vectoriels de dimension finie. Alors pour tout espace-vectoriel G de dimension finie sur k, l'application*

$$u_G : \left| \begin{array}{c} \mathcal{L}(E \otimes F, G) \longrightarrow \mathrm{Bil}(E, F, G) \\ f \longmapsto f \circ b_{E,F} \end{array} \right.$$

est un isomorphisme d'espaces vectoriels.

Corollaire 5.1.3. *Soit E, F deux k-espaces vectoriels de dimension finie. Soit M un k-espace vectoriel de dimension finie et $\beta \in \mathrm{Bil}(E, F, M)$ t.q. le théorème 5.1.2 reste vrai en remplaçant $(E \otimes F, b_{E,F})$ par (M, β). Alors il existe un unique isomorphisme $\varphi : E \otimes F \to M$ t.q. $\beta = \varphi \circ b_{E,F}$. Ainsi, on peut identifier tous les couples $(E \otimes F, b_{E,F})$ construits avec différentes bases de E et F.*

Corollaire 5.1.4. *Soit E, F deux k-espaces vectoriels de dimension finie. Alors :*

$$\dim(E \otimes F) = (\dim E)(\dim F).$$

Corollaire 5.1.5. *Soit E, F deux k-espaces vectoriels de dimension finie. Alors les espaces $(E \otimes F)^*$ et $\mathrm{Bil}(E, F)$ sont canoniquement isomorphes.*

Définition 5.1.6 (Tenseurs simples)**.** *Soit E, F deux k-espaces vectoriels de dimension finie. Pour $(x, y) \in E \times F$, on notera $x \otimes y = b_{E,F}(x, y) \in E \otimes F$. Les éléments de $E \otimes F$ de la forme $x \otimes y$ seront appelés* tenseurs simples.

Remarque 5.1.7. *Soit E, F deux k-espaces vectoriels de dimension finie. $E \otimes F$ est engendré par les tenseurs simples mais peut contenir d'autres éléments que les tenseurs simples.*

Proposition 5.1.8. *Soit E, F deux k-espaces vectoriels de dimension finie. Alors $\mathcal{L}(E, F)$ et $E^* \otimes F$ sont canoniquement isomorphes.*

Démonstration. On pose d'abord :

$$\psi : \left| \begin{array}{c} E^* \times F \longrightarrow \mathcal{L}(E, F) \\ (\mu, y) \longmapsto \left| \begin{array}{c} E \longrightarrow F \\ x \longmapsto \mu(x) y \end{array} \right. \end{array} \right. .$$

Alors $\psi \in \mathrm{Bil}(E^*, F, \mathcal{L}(E, F))$. Soit donc $u \in \mathcal{L}(E^* \otimes F, \mathcal{L}(E, F))$ t.q. $\psi = u \circ b_{E,F}$. Montrons que u est surjective. Soit $(f_1, \dots, f_n)$ une base de F. Soit $h \in \mathcal{L}(E, F)$. Pour $i \in [\![1, n]\!]$, soit $\mu_i = {}^t h(f_i^*) \in E^*$. Alors $\forall x \in E$, $h(x) = \sum_{i=1}^n \mu_i(x) f_i$ donc $h = u(\sum_{i=1}^n \mu_i \otimes f_i)$. Donc u est surjective. Et $\dim \mathcal{L}(E, F) = \dim(E^* \otimes F)$ donc u est un isomorphisme. □

Remarque 5.1.9. *Soit E, F deux k-espaces vectoriels de dimension finie, et soit $u : E^* \otimes F \to \mathcal{L}(E, F)$ l'isomorphisme canonique. Alors pour tout $t \in E^* \otimes F$, $\mathrm{rg}\, u(t)$ est le nombre minimal de tenseurs simples nécessaires dans une écriture de t comme somme de tenseurs simples.*

5.2 Morphismes

Proposition 5.2.1. *Soit E, E', F, F' des k-espaces vectoriels de dimension finie, $u \in \mathcal{L}(E, E')$, $v \in \mathcal{L}(F, F')$. Alors il existe un unique élément noté $(u \otimes v) \in \mathcal{L}(E \otimes F, E' \otimes F')$ vérifiant :*

$$\forall (x, y) \in E \times F,\ (u \otimes v)(x \otimes y) = u(x) \otimes v(y).$$

Proposition 5.2.2. *Soit E, E', E'', F, F', F'' des k-espaces vectoriels de dimension finie. On considère $u \in \mathcal{L}(E, E')$, $v \in \mathcal{L}(F, F')$, $u' \in \mathcal{L}(E', E'')$, $v' \in \mathcal{L}(F', F'')$. Alors :*

$$(u' \otimes v') \circ (u \otimes v) = (u' \circ u) \otimes (v' \circ v).$$

Corollaire 5.2.3. *Soit E, E', F, F' des k-espaces vectoriels de dimension finie, $u \in \mathcal{L}(E, E')$, $v \in \mathcal{L}(F, F')$. Si u et v sont des isomorphismes, alors $(u \otimes v)$ est aussi un isomorphisme.*

5.3 Quelques isomorphismes canoniques

Proposition 5.3.1. *Soit E, F, G trois k-espaces vectoriels de dimension finie. Alors il existe un unique isomorphisme (dit canonique) $u : (E \oplus F) \otimes G \to (E \otimes G) \oplus (F \otimes G)$ vérifiant :*

$$\forall (x, y, z) \in E \times F \times G,\ u((x, y) \otimes z) = (x \otimes z, y \otimes z).$$

Proposition 5.3.2. *Soit E, F deux k-espaces vectoriels de dimension finie. Alors il existe un unique isomorphisme (dit canonique) $u : E \otimes F \to F \otimes E$ vérifiant :*

$$\forall (x, y) \in E \times F,\ u(x \otimes y) = y \otimes x.$$

Proposition 5.3.3. *Soit E, F, G trois k-espaces vectoriels de dimension finie. Alors il existe un unique isomorphisme (dit canonique) $u : (E \otimes F) \otimes G \to E \otimes (F \otimes G)$ vérifiant :*

$$\forall (x, y, z) \in E \times F \times G,\ u((x \otimes y) \otimes z) = x \otimes (y \otimes z).$$

On pourra donc noter $E \otimes F \otimes G$ pour $(E \otimes F) \otimes G$ ou $E \otimes (F \otimes G)$.

6 Groupes

6.1 Généralités

Définition 6.1.1 (Groupe)**.** *Un* groupe *est la donnée de $(G, *, e)$, où G est un ensemble, $* : G \times G \to G$ est une loi de composition interne, $e \in G$, vérifiant :*

(i) *$*$ est associative : $\forall (a, b, c) \in G^3,\ (a * b) * c = a * (b * c)$.*

(ii) *e est un élément neutre pour $*$: $\forall a \in G,\ a * e = e * a = a$.*

(iii) *Tout élément de G est inversible : $\forall a \in G,\ \exists b \in G,\ a * b = b * a = e$.*

Proposition 6.1.2. *Soit G un groupe.*

(i) *L'élément neutre de G est unique.*

(ii) *L'inverse d'un élément $a \in G$ est unique ; on le note a^{-1}.*

Définition 6.1.3 (Groupe abélien)**.** *On dit qu'un groupe G est* abélien *(ou* commutatif*) lorsque $\forall (a, b) \in G^2,\ a * b = b * a$.*

Définition 6.1.4 (Ordre d'un groupe)**.** *Soit G un groupe. On appelle* ordre *de G le cardinal de G (qui peut être infini).*

Définition 6.1.5 (Sous-groupe)**.** *Soit G un groupe et $H \subset G$. On dit que H est un* sous-groupe *de G lorsque les propriétés suivantes sont vérifiées :*

(i) $e \in H$.

(ii) $\forall (a,b) \in H^2,\ (a * b) \in H$.

(iii) $\forall a \in H,\ a^{-1} \in H$.

Proposition 6.1.6. *Soit G un groupe et $H \subset G$. Alors H est un sous-groupe de G* ssi *les conditions suivantes sont vérifiées :*

(i) $H \neq \varnothing$.

(ii) $\forall (a,b) \in H^2,\ (a * b^{-1}) \in H$.

Définition 6.1.7 (Sous-groupe engendré)**.** *Soit G un groupe et $X \subset G$. On appelle* sous-groupe engendré *par X, et on note $\langle X \rangle$, le plus petit sous-groupe de G contenant X (il existe car une intersection de sous-groupes de G est un sous-groupe de G). On a :*

$$\langle X \rangle = \{a_1^{\varepsilon_1} * \cdots * a_n^{\varepsilon_n},\ n \in \mathbb{N},\ (a_1, \ldots, a_n) \in X^n,\ (\varepsilon_1, \ldots, \varepsilon_n) \in \{-1,1\}^n\}\,.$$

Définition 6.1.8 (Groupe monogène)**.** *On dit qu'un groupe G est* monogène *(ou* cyclique*) lorsque $\exists x \in G,\ G = \langle x \rangle$.*

Définition 6.1.9 (Ordre d'un élément)**.** *Soit G un groupe. Étant donné $x \in G$, on appelle* ordre *de x l'ordre de $\langle x \rangle$ (qui peut être infini).*

Définition 6.1.10 (Morphisme de groupes)**.** *Soit G, G' deux groupes. On appelle* morphisme de groupes *toute application $f : G \to G'$ vérifiant :*

(i) $f(e) = e'$.

(ii) $\forall (a,b) \in G^2,\ f\,(a * b) = f(a) *' f(b)$.

Définition 6.1.11 (Isomorphisme de groupes)**.** *Soit G, G' deux groupes, $f : G \to G'$ un morphisme de groupes. On dit que f est un* isomorphisme *lorsque f est bijectif. Si tel est le cas, alors f^{-1} est aussi un morphisme de groupes (donc un isomorphisme). On dit alors que G et G' sont* isomorphes *et on note $G \simeq G'$.*

Définition 6.1.12 (Noyau et image)**.** *Soit G, G' deux groupes, $f : G \to G'$ un morphisme de groupes. On définit :*

$$\operatorname{Im} f = f(G) \qquad \text{et} \qquad \operatorname{Ker} f = f^{-1}\left(\{e'\}\right).$$

Proposition 6.1.13. *Soit G, G' deux groupes, $f : G \to G'$ un morphisme de groupes. Alors* $\operatorname{Im} f$ *et* $\operatorname{Ker} f$ *sont des sous-groupes de respectivement G' et G. Et :*

(i) *f est surjective* ssi $\operatorname{Im} f = G'$.

(ii) *f est injective* ssi $\operatorname{Ker} f = \{e\}$.

6.2 Classes définies par un sous-groupe

Définition 6.2.1 (Classes à gauche)**.** *Soit G un groupe et H un sous-groupe de G. On définit une relation $\sim_H$ sur G par :*

$$\forall (x,y) \in G^2,\ x \sim_H y \iff y^{-1}x \in H.$$

Alors $\sim_H$ est une relation d'équivalence. Et on pose $G/H = G/\sim_H$. Les éléments de G/H sont appelés classes à gauche *de G pour H. Étant donné $x \in G$, la classe de x dans G/H est notée xH.*

Remarque 6.2.2. *On peut définir de même les* classes à droite *pour un sous-groupe H de G, en considérant la relation d'équivalence $x \sim_H y \iff xy^{-1} \in H$. L'ensemble quotient est alors noté $H\backslash G$, ses éléments sont appelés* classes à droite*, et la classe d'un $x \in G$ est notée Hx.*

Définition 6.2.3 (Indice d'un sous-groupe)**.** *Soit G un groupe et H un sous-groupe de G. On appelle* indice *de H dans G, et on note $[G : H]$, le cardinal de G/H (qui peut être infini).*

Remarque 6.2.4. *Soit G un groupe et H un sous-groupe de G. Alors G/H est fini* ssi *$H\backslash G$ est fini. Si tel est le cas, alors $|G/H| = |H\backslash G|$.*

Théorème 6.2.5. *Soit G un groupe et H un sous-groupe de G. Alors toutes les classes à gauche de G pour H ont le même cardinal.*

Corollaire 6.2.6. *Soit G un groupe et H un sous-groupe de G. Si G est fini, alors :*

$$|G| = |H| \cdot [G : H] .$$

Corollaire 6.2.7 (Théorème de Lagrange)**.** *Soit G un groupe et H un sous-groupe de G. Si G est fini, alors $|H|$ divise $|G|$.*

Corollaire 6.2.8. *Soit G un groupe. Alors pour tout $x \in G$, l'ordre de x divise l'ordre de G.*

6.3 Sous-groupes distingués

Définition 6.3.1 (Sous-groupe distingué)**.** *Soit G un groupe et H un sous-groupe de G. S'équivalent :*

(i) $\forall a \in G,\ aH = Ha$.

(ii) $\forall a \in G,\ aHa^{-1} \subset H$.

(iii) $G/H = H\backslash G$.

On dit alors que H est un sous-groupe distingué *(ou* normal*) de G.*

Exemple 6.3.2. *Si G est un groupe abélien, alors tout sous-groupe de G est distingué.*

Notation 6.3.3 (Commutateur)**.** *Soit G un groupe. Pour $(x, y) \in G^2$, on note $[x, y] = xyx^{-1}y^{-1}$.*

Définition 6.3.4 (Groupe dérivé et centre)**.** *Soit G un groupe. On définit :*

(i) *Le* groupe dérivé *de G : $D(G) = \langle \{[x, y] ,\ (x, y) \in G^2\} \rangle$,*

(ii) *Le* centre *de G : $Z(G) = \{x \in G,\ \forall y \in G,\ xy = yx\}$.*

Proposition 6.3.5. *Soit G un groupe. Alors $D(G)$ et $Z(G)$ sont des sous-groupes distingués de G. De plus, tout sous-groupe de $Z(G)$ est distingué dans G.*

Proposition 6.3.6. *Soit G, G' deux groupes, $f : G \to G'$ un morphisme de groupes. Alors* $\operatorname{Ker} f$ *est un sous-groupe distingué de G.*

Définition 6.3.7 (Normalisateur d'un sous-groupe)**.** *Soit G un groupe et H un sous-groupe de G. On appelle* normalisateur *de H dans G l'ensemble :*

$$N_G(H) = \{x \in G,\ xH = Hx\} .$$

Proposition 6.3.8. *Soit G un groupe et H un sous-groupe de G. Alors $N_G(H)$ est le plus grand sous-groupe de G t.q. H est un sous-groupe distingué de $N_G(H)$. En particulier, H est distingué dans G* ssi *$G = N_G(H)$.*

Définition 6.3.9 (Groupe simple)**.** *On dit qu'un groupe G est simple s'il n'a pas de sous-groupe distingué non trivial (i.e. différent de $\{e\}$ et G).*

6.4 Groupes quotients

Théorème 6.4.1. *Soit G un groupe et H un sous-groupe distingué de G. Alors il existe une unique structure de groupe sur G/H t.q. la projection canonique $\pi : G \to G/H$ est un morphisme de groupes. On a alors $H = \operatorname{Ker} \pi$.*

Corollaire 6.4.2. *Soit G un groupe et H un sous-groupe de G. Alors H est distingué* ssi *il existe un groupe G' et un morphisme $f : G \to G'$ t.q. $H = \operatorname{Ker} f$.*

Proposition 6.4.3. *Soit G un groupe. Alors $G/D(G)$ est un groupe abélien, et $D(G)$ est le plus petit sous-groupe distingué de G vérifiant cette propriété.*

Proposition 6.4.4. *Soit G un groupe et H un sous-groupe distingué de G. On note $\Gamma(G/H)$ l'ensemble des sous-groupes de G/H et $\Gamma_H(G)$ l'ensemble des sous-groupes de G contenant H. Alors l'application*

$$\Psi : \left| \begin{array}{rcl} \Gamma(G/H) & \longrightarrow & \Gamma_H(G) \\ K & \longmapsto & \pi^{-1}(K) \end{array} \right.$$

est une bijection, où $\pi : G \to G/H$ est la projection canonique.

Théorème 6.4.5 (Théorème de factorisation pour les groupes)**.** *Soit G, G' deux groupes, $f : G \to G'$ un morphisme de groupes, H un sous-groupe distingué de G et $\pi : G \to G/H$ la projection canonique. S'équivalent :*

(i) *$H \subset \operatorname{Ker} f$.*

(ii) *Il existe un morphisme de groupes $u : G/H \to G'$ t.q. $f = u \circ \pi$.*

Si ces conditions sont vérifiées, alors la factorisation est unique.

Corollaire 6.4.6. *Soit G, G' deux groupes, $f : G \to G'$ un morphisme de groupes. Alors :*

$$G/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

6.5 Actions de groupes

Définition 6.5.1 (Action de groupe)**.** *Soit G un groupe et X un ensemble. Une* action *de G sur X est la donnée d'une application* $\left| \begin{array}{rcl} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array} \right.$ *vérifiant :*

(i) *$\forall (a, b) \in G^2$, $\forall x \in X$, $a \cdot (b \cdot x) = (ab) \cdot x$.*

(ii) *$\forall x \in X$, $e \cdot x = x$.*

Notation 6.5.2. *Si X est un ensemble, on note $\operatorname{Bij}(X)$ le groupe des bijections de X dans X.*

Proposition 6.5.3. *Soit G un groupe et X un ensemble. Alors une application $\cdot : G \times X \to X$ est une action de groupe* ssi *l'application*

$$\left| \begin{array}{rcl} G & \longrightarrow & \operatorname{Bij}(X) \\ a & \longmapsto & \left| \begin{array}{rcl} X & \longrightarrow & X \\ x & \longmapsto & a \cdot x \end{array} \right. \end{array} \right.$$

est un morphisme de groupes.

Exemple 6.5.4.

(i) *$GL_n(\mathbb{C})$ agit sur $\mathbb{C}^n$.*

(ii) *Si X est un ensemble, $\operatorname{Bij}(X)$ agit sur X.*

(iii) *$GL_n(\mathbb{C})$ agit sur $\mathbb{M}_n(\mathbb{C})$ par conjugaison.*

(iv) *Un groupe G agit sur lui-même par translation ou par conjugaison.*

Proposition 6.5.5. *Soit G un groupe.*

(i) *Si G agit sur un ensemble X et H est un sous-groupe de G, alors* $\left|\begin{array}{l} H \times X \longrightarrow X \\ (h,x) \longmapsto h \cdot x \end{array}\right.$ *est une action de H sur X.*

(ii) *Si G agit sur deux ensembles X et Y, alors* $\left|\begin{array}{l} G \times (X \times Y) \longrightarrow X \times Y \\ (g,(x,y)) \longmapsto (g \cdot x, g \cdot y) \end{array}\right.$ *est une action de G sur $X \times Y$.*

(iii) *Si G agit sur un ensemble X, alors* $\left|\begin{array}{l} G \times \mathcal{P}(X) \longrightarrow \mathcal{P}(X) \\ (g,E) \longmapsto \{g \cdot x,\ x \in E\} \end{array}\right.$ *est une action de G sur $\mathcal{P}(X)$.*

(iv) *Si G agit sur un ensemble X et Y est une partie de X vérifiant $\forall g \in G,\ \forall y \in Y,\ g \cdot y \in Y$, alors* $\left|\begin{array}{l} G \times Y \longrightarrow Y \\ (g,y) \longmapsto g \cdot y \end{array}\right.$ *est une action de G sur Y.*

Définition 6.5.6 (Action fidèle)**.** *On dit qu'une action d'un groupe G sur un ensemble X est* fidèle *lorsque le morphisme associé $\phi : G \to \mathrm{Bij}(X)$ est injectif.*

Proposition 6.5.7. *Soit G un groupe agissant sur un ensemble X, $\phi : G \to \mathrm{Bij}(X)$ le morphisme associé. Alors $G/\operatorname{Ker}\phi$ agit sur X, et cette action est fidèle.*

Définition 6.5.8 (Stabilisateurs)**.** *Soit G un groupe agissant sur un ensemble X. Pour $x \in X$, on définit le* stabilisateur *de x par :*

$$\mathrm{Stab}_G(x) = \{g \in G,\ g \cdot x = x\}.$$

Ainsi $\mathrm{Stab}_G(x)$ est un sous-groupe de G et si $\phi : G \to \mathrm{Bij}(X)$ est le morphisme associé à l'action de G sur X, alors $\operatorname{Ker}\phi = \bigcap_{x \in X} \mathrm{Stab}_G(x)$.

Définition 6.5.9 (Orbites)**.** *Soit G un groupe agissant sur un ensemble X. Pour $x \in X$, on définit l'*orbite *de x par :*

$$G \cdot x = \{g \cdot x,\ g \in G\}.$$

On peut de plus définir une relation $\sim$ sur X par $\forall (x,y) \in X^2,\ x \sim y \iff y \in G \cdot x$. Alors $\sim$ est une relation d'équivalence dont les classes d'équivalence sont les orbites.

Définition 6.5.10 (Action transitive)**.** *On dit qu'une action est* transitive *lorsqu'il n'y a qu'une seule orbite.*

Définition 6.5.11. *Si G est un groupe agissant sur un ensemble X, on note :*

$$X^G = \{x \in X,\ \forall g \in G,\ g \cdot x = x\}.$$

Exemple 6.5.12. *Soit G un groupe. Alors G agit sur lui-même par conjugaison et $G^G = Z(G)$.*

Théorème 6.5.13 (Théorème de Cayley)**.** *Soit G un groupe fini de cardinal n. Alors il existe un morphisme injectif de groupes de G dans $\mathfrak{S}_n$. Autrement dit, G s'identifie à un sous-groupe de $\mathfrak{S}_n$.*

Démonstration. Considérer l'action de G sur lui-même par translation à gauche. □

6.6 Formule des classes

Proposition 6.6.1. *Soit G un groupe agissant sur un ensemble X. Soit $x \in X$. Alors :*

(i) *$G/\operatorname{Stab}_G(x)$ est en bijection avec $G \cdot x$.*

(ii) *Pour tout $g \in G$, on a $\operatorname{Stab}_G(g \cdot x) = g \operatorname{Stab}_G(x) g^{-1}$.*

(iii) *Pour tout $g \in G$, on a $\{h \in G,\ h \cdot x = g \cdot x\} = g \operatorname{Stab}_G(x)$.*

Corollaire 6.6.2. *Soit G un groupe agissant sur un ensemble X. Soit $x \in X$. Alors $G \cdot x$ est finie* ssi $\operatorname{Stab}_G(x)$ *est d'indice fini dans G. Si tel est le cas, alors :*

$$\begin{aligned} |G \cdot x| &= [G : \operatorname{Stab}_G(x)] \\ &= \frac{|G|}{|\operatorname{Stab}_G(x)|} \qquad \textit{si } G \textit{ est fini.} \end{aligned}$$

En particulier, si G est fini, alors $|G \cdot x|$ divise $|G|$.

Théorème 6.6.3 (Formule des classes)**.** *Soit G un groupe agissant sur un ensemble fini X. Soit $\Omega \subset X$ un ensemble de représentants des orbites de X sous l'action de G. Alors :*

$$\begin{aligned} |X| &= \sum_{x \in \Omega} [G : \operatorname{Stab}_G(x)] \\ &= \sum_{x \in \Omega} \frac{|G|}{|\operatorname{Stab}_G(x)|} \qquad \textit{si } G \textit{ est fini.} \end{aligned}$$

6.7 Le cas des p-groupes

Définition 6.7.1 (p-groupe)**.** *Si p est un nombre premier, on appelle p-*groupe *tout groupe fini dont le cardinal est une puissance de p.*

Théorème 6.7.2. *Soit G un p-groupe agissant sur un ensemble fini X. Alors :*

$$|X| \equiv \left|X^G\right| \quad [p]\,.$$

Démonstration. Soit Ω un ensemble de représentants des orbites de X. Selon la formule des classes (théorème 6.6.3), on a :

$$|X| = \sum_{x \in \Omega} [G : \operatorname{Stab}_G(x)] = \left|X^G\right| + \sum_{x \in \Omega \setminus X^G} [G : \operatorname{Stab}_G(x)]\,.$$

Or, pour $x \in \Omega \setminus X^G$, $[G : \operatorname{Stab}_G(x)]$ est un entier strictement supérieur à 1 et divisant $|G|$, qui est une puissance de p. Donc $\forall x \in \Omega \setminus X^G$, $p \mid [G : \operatorname{Stab}_G(x)]$. □

Théorème 6.7.3 (Lemme de Cauchy)**.** *Soit G un groupe fini et p un nombre premier divisant $|G|$. Alors il existe un élément $x \in G$ d'ordre exactement p.*

Démonstration. On note $X = \{(x_1, \ldots, x_p) \in G^p,\ x_1 \cdots x_p = e\}$. On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par $i \cdot (x_1, \ldots, x_p) = (x_{i+1}, \ldots, x_{i+p})$. On note $S = \{(x, \ldots, x)\,,\ x \in G \text{ est d'ordre exactement } p\}$. Il suffit de prouver que $S \neq \varnothing$. Or on a $X^{\mathbb{Z}/p\mathbb{Z}} = \{(e, \ldots, e)\} \cup S$. Ainsi, selon le théorème 6.7.2 :

$$|S| = \left|X^{\mathbb{Z}/p\mathbb{Z}}\right| - 1 \equiv |X| - 1 = |G|^{p-1} - 1 \equiv -1 \not\equiv 0 \quad [p]\,.$$

Donc $|S| \neq 0$ et $S \neq \varnothing$. □

Théorème 6.7.4. *Soit G un p-groupe non trivial. Alors $Z(G) \supsetneq \{e\}$.*

Démonstration. On considère l'action de G sur lui-même par conjugaison. On a $G^G = Z(G)$. Donc $|Z(G)| = \left|G^G\right| \equiv |G| \equiv 0 \quad [p]$. Donc $p \mid |Z(G)|$, et $|Z(G)| \geqslant 1$ (car $e \in Z(G)$), donc $|Z(G)| \geqslant p$. □

Corollaire 6.7.5. *Si p est un nombre premier et G est un p-groupe d'ordre p^2, alors G est abélien.*

6.8 Les théorèmes de Sylow

Définition 6.8.1 (p-Sylow)**.** *Soit G un groupe fini et p un nombre premier. On appelle* p-Sylow *de G tout sous-groupe H de G qui est un p-groupe et t.q. $p \nmid [G : H]$. Autrement dit, H est un p-Sylow* ssi $|H| = p^{v_p(|G|)}$*, où $v_p(|G|)$ est la valuation p-adique de $|G|$.*

Proposition 6.8.2. *Pour tout groupe fini G, il existe un morphisme injectif de groupes de G dans un groupe admettant un p-Sylow.*

Démonstration. Si $n = |G|$, le théorème de Cayley (théorème 6.5.13) fournit un morphisme injectif $\varphi : G \to \mathfrak{S}_n$. Si k est un corps fixé, on considère alors :

$$u : \left| \begin{array}{l} \mathfrak{S}_n \longrightarrow GL_n(k) \\ \quad \sigma \longmapsto \left(\delta_{i,\sigma(j)}\right)_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} \end{array} \right. .$$

Alors u est un morphisme injectif de groupes. On fixe $k = \mathbb{Z}/p\mathbb{Z}$. Ainsi, $u \circ \varphi : G \to GL_n(\mathbb{Z}/p\mathbb{Z})$ est un morphisme injectif de groupes. Or :

$$|GL_n(\mathbb{Z}/p\mathbb{Z})| = \prod_{k=0}^{n-1} \left(p^n - p^k\right) = p^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} \left(p^k - 1\right).$$

Ainsi, les p-Sylow de $GL_n(\mathbb{Z}/p\mathbb{Z})$ sont les sous-groupes de $GL_n(\mathbb{Z}/p\mathbb{Z})$ de cardinal $p^{\frac{n(n-1)}{2}}$. Si on note $T \subset GL_n(\mathbb{Z}/p\mathbb{Z})$ l'ensemble des matrices triangulaires supérieures avec des 1 sur la diagonale, alors T est un sous-groupe de $GL_n(\mathbb{Z}/p\mathbb{Z})$ de cardinal $p^{\frac{n(n-1)}{2}}$; c'est donc un p-Sylow. □

Proposition 6.8.3. *Soit G un groupe fini, H un sous-groupe de G et P un p-Sylow de G. Alors il existe $a \in G$ t.q. $(aPa^{-1}) \cap H$ est un p-Sylow de H.*

Démonstration. On considère l'action de H par translation à gauche sur G/P. Comme $p \nmid |G/P|$, il existe une orbite de cardinal non divisible par p (d'après la formule des classes). Soit donc $a \in G$ t.q. $|H \cdot (aP)|$ n'est pas divisible par p. Notons que :

$$\mathrm{Stab}_H(aP) = \mathrm{Stab}_G(aP) \cap H = \left(aPa^{-1}\right) \cap H.$$

Ainsi $|H \cdot (aP)| = [H : (aPa^{-1}) \cap H]$. Donc $p \nmid [H : (aPa^{-1}) \cap H]$, et $(aPa^{-1}) \cap H$ est un p-groupe comme sous-groupe de aPa^{-1} (qui est un p-groupe car $|aPa^{-1}| = |P|$). Donc $(aPa^{-1}) \cap H$ est un p-Sylow de H. □

Corollaire 6.8.4. *Si un groupe admet un p-Sylow, alors tous ses sous-groupes aussi.*

Théorème 6.8.5 (Théorèmes de Sylow)**.** *Soit G un groupe fini et p un nombre premier. Alors :*

(i) *G admet au moins un p-Sylow.*

(ii) *Tous les p-Sylow de G sont conjugués.*

(iii) *Si $n_p(G)$ est le nombre de p-Sylow de G, alors $n_p(G) \mid |G|$ et $n_p(G) \equiv 1 \quad [p]$.*

Démonstration. (i) C'est une conséquence de la proposition 6.8.2 et du corollaire 6.8.4. (ii) Soit H et P deux p-Sylow de G. Selon la proposition 6.8.3, il existe $a \in G$ t.q. $(aPa^{-1}) \cap H$ est un p-Sylow de H. Comme H est un p-groupe, on a donc $(aPa^{-1}) \cap H = H$, i.e. $H \subset aPa^{-1}$. Par ailleurs $|H| = |P| = |aPa^{-1}|$, donc $H = aPa^{-1}$. (iii) On note X l'ensemble des p-Sylow de G. Selon (i), $X \neq \varnothing$. On considère l'action de G sur X par conjugaison. Selon (ii), cette action est transitive. Donc X est une orbite, d'où $|X|$ divise $|G|$, i.e. $n_p(G)$ divise $|G|$. Soit maintenant $P \in X$ (car $X \neq \varnothing$). On considère dorénavant l'action de P sur X par conjugaison. Comme P est un p-groupe, le théorème 6.7.2 fournit $n_p(G) = |X| \equiv \left|X^P\right| \quad [p]$. Montrons alors que $X^P = \{P\}$, ce qui fournira bien $n_p(G) \equiv 1 \quad [p]$. Soit $Q \in X^P$. On a $\forall x \in P$, $xQx^{-1} = Q$, donc $P \subset N_G(Q)$. De plus, $Q \subset N_G(Q)$. Donc P et Q sont des p-Sylow de $N_G(Q)$. Selon (ii), il existe $a \in N_G(Q)$ t.q. $P = aQa^{-1}$. Or Q est distingué dans $N_G(Q)$, donc $aQa^{-1} = Q$, d'où $Q = P$. Donc $X^P = \{P\}$ et $n_p(G) \equiv 1 \quad [p]$. □

Corollaire 6.8.6. *Soit G un groupe fini, H un sous-groupe de G qui est un p-groupe. Alors H est contenu dans un p-Sylow de G.*

Démonstration. Soit P un p-Sylow de G, qui existe selon le premier théorème de Sylow (théorème 6.8.5). Selon la proposition 6.8.3, soit $a \in G$ t.q. $(aPa^{-1}) \cap H$ est un p-Sylow de H. Alors $(aPa^{-1}) \cap H = H$ car H est un p-groupe, d'où $H \subset aPa^{-1}$, et aPa^{-1} est un p-Sylow de G. □

6.9 Le groupe symétrique

6.9.1 Généralités

Définition 6.9.1 (Groupe symétrique)**.** *On note $\mathfrak{S}_n = \mathrm{Bij}\left(\llbracket 1, n \rrbracket\right)$, pour $n \in \mathbb{N}^*$.*

Définition 6.9.2 (Cycle)**.** *Soit $r > 1$. On appelle* r-cycle *de $\mathfrak{S}_n$ tout $\sigma \in \mathfrak{S}_n$ t.q. il existe $i_1, \ldots, i_r \in \llbracket 1, n \rrbracket$ deux à deux distincts t.q.*

$$\forall j \in \llbracket 1, r \llbracket,\ \sigma\left(i_j\right) = i_{j+1} \quad \text{et} \quad \sigma\left(i_r\right) = i_1 \quad \text{et} \quad \forall i \in \llbracket 1, n \rrbracket \backslash \left\{i_1, \ldots, i_r\right\},\ \sigma(i) = i.$$

On note alors $\sigma = (i_1 \ \cdots \ i_r)$. On appelle support *de σ l'ensemble $\{i_1, \ldots, i_r\}$. Un r-cycle est d'ordre exactement r dans le groupe $\mathfrak{S}_n$. Les 2-cycles sont appelés* transpositions*.*

Proposition 6.9.3. *Deux cycles à supports disjoints commutent.*

Théorème 6.9.4. *Tout élément de $\mathfrak{S}_n$ s'écrit de manière unique à l'ordre près comme produit de cycles à supports disjoints.*

Corollaire 6.9.5. *$\mathfrak{S}_n$ est engendré par les transpositions. Plus précisément, tout $\sigma \in \mathfrak{S}_n$ s'écrit comme produit d'au plus $(n-1)$ transpositions.*

Proposition 6.9.6. *Si $c_1, \ldots, c_t$ sont des cycles de $\mathfrak{S}_n$ à supports disjoints de longueurs respectives $\ell_1, \ldots, \ell_t$, alors l'ordre de $\prod_{i=1}^{t} c_i$ est le* PPCM *des $(\ell_i)_{1 \leqslant i \leqslant t}$.*

6.9.2 Conjugaison dans $\mathfrak{S}_n$

Lemme 6.9.7. *Soit $(i_1 \ \cdots \ i_r)$ un r-cycle de $\mathfrak{S}_n$. Alors :*

$$\forall \tau \in \mathfrak{S}_n,\ \tau\left(i_1 \ \cdots \ i_r\right)\tau^{-1} = \left(\tau\left(i_1\right) \ \cdots \ \tau\left(i_r\right)\right).$$

Théorème 6.9.8. *À une permutation $\sigma \in \mathfrak{S}_n$, on associe une partition de n (i.e. une suite d'entiers $k_1 \geqslant \cdots \geqslant k_s \geqslant 1$ avec $\sum_{i=1}^{s} k_i = n$) donnée par les longueurs des cycles dans la décomposition de σ en produit de cycles à supports disjoints. Alors deux éléments de $\mathfrak{S}_n$ sont conjugués* ssi *ils ont la même partition associée.*

Théorème 6.9.9. *Si $n \geqslant 3$, alors $Z\left(\mathfrak{S}_n\right) = \{id\}$.*

6.9.3 Signature

Théorème 6.9.10. *Si $n \geqslant 2$, alors il existe un unique morphisme de groupes non trivial $\mathfrak{S}_n \to \mathbb{C}^*$. Ce morphisme est appelé* signature *et noté ε. Il est à valeurs dans $\{-1, 1\}$.*

Démonstration. *Unicité.* Si $\varphi : \mathfrak{S}_n \to \mathbb{C}^*$ est un morphisme de groupes, alors toutes les transpositions sont conjuguées deux à deux donc ont la même image (car $\mathbb{C}^*$ est abélien), et cette image est dans $\{-1, 1\}$ (car les transpositions sont d'ordre 2). De plus, les transpositions engendrent $\mathfrak{S}_n$ donc φ est uniquement déterminé par l'image des transpositions. Donc il y a au plus deux morphismes de groupes $\mathfrak{S}_n \to \mathbb{C}^*$, dont un est trivial. *Existence.* On définit :

$$\varepsilon : \sigma \in \mathfrak{S}_n \longmapsto \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \mathbb{C}^*.$$

On montre que ε est un morphisme de groupes. Et $\varepsilon\left((1\,2)\right) < 0$ donc ε est non trivial. □

Corollaire 6.9.11.

(i) *Si $\sigma \in \mathfrak{S}_n$ est un produit de k transpositions, alors $\varepsilon(\sigma) = (-1)^k$. En particulier, la parité de k ne dépend que de σ et pas du choix des transpositions.*

(ii) *Si $c \in \mathfrak{S}_n$ est un ℓ-cycle, alors $\varepsilon(c) = (-1)^{\ell+1}$.*

Définition 6.9.12 (Parité d'une permutation)**.** *On dit qu'une permutation $\sigma \in \mathfrak{S}_n$ est* paire *lorsque $\varepsilon(\sigma) = 1$. Dans le cas contraire (i.e. $\varepsilon(\sigma) = -1$), on dit que σ est* impaire*.*

6.9.4 Le groupe alterné

Définition 6.9.13 (Groupe alterné)**.** *On appelle* groupe alterné *le groupe :*

$$\mathfrak{A}_n = \operatorname{Ker} \varepsilon = \{\sigma \in \mathfrak{S}_n,\ \varepsilon(\sigma) = 1\}\,.$$

Proposition 6.9.14. *$\mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{S}_n$ d'indice 2. De plus, c'est l'unique sous-groupe d'indice 2 de $\mathfrak{S}_n$.*

Proposition 6.9.15. *$\mathfrak{A}_n$ est engendré par les 3-cycles.*

Démonstration. Comme tout élément de $\mathfrak{A}_n$ s'écrit comme produit d'un nombre pair de transpositions, il suffit de prouver que le produit de deux transpositions peut s'écrire comme produit de 3-cycles. □

Proposition 6.9.16. *Si $n \geqslant 5$, alors les 3-cycles sont conjugués dans $\mathfrak{A}_n$.*

Démonstration. Soit σ, σ' deux 3-cycles. Selon le théorème 6.9.8, il existe $\tau \in \mathfrak{S}_n$ t.q. $\sigma' = \tau\sigma\tau^{-1}$. Si $\tau \in \mathfrak{A}_n$, cela prouve que σ et σ' sont conjugués dans $\mathfrak{A}_n$. Sinon, soit a, b deux éléments distincts de $[\![1, n]\!]$ hors du support de σ (car $n \geqslant 5$). Alors la transpositions $(a\,b)$ commute avec σ. Ainsi, en notant $\tau' = \tau\,(a\,b)$, on a $\sigma' = \tau'\sigma\tau'^{-1}$, et $\tau' \in \mathfrak{A}_n$. □

Corollaire 6.9.17. *Si H est un sous-groupe distingué de $\mathfrak{A}_n$ contenant un 3-cycle, alors $H = \mathfrak{A}_n$.*

Lemme 6.9.18. *Si H est un sous-groupe distingué de $\mathfrak{A}_5$ contenant un 5-cycle, alors H contient tous les 5-cycles.*

Démonstration. Soit $c \in H$ un 5-cycle. Alors $\langle c \rangle$ est un 5-Sylow de $\mathfrak{A}_5$ (car $|\mathfrak{A}_5| = \frac{1}{2}\,|\mathfrak{S}_5| = 60$). Selon le deuxième théorème de Sylow (théorème 6.8.5), les 5-Sylow de $\mathfrak{A}_5$ sont exactement les conjugués de $\langle c \rangle$, qui sont inclus dans H car H est distingué. Donc H contient tous les 5-Sylow de $\mathfrak{A}_5$, donc tous les 5-cycles de $\mathfrak{A}_5$. □

Proposition 6.9.19. *$\mathfrak{A}_5$ est simple.*

Démonstration. Soit $H \subsetneq \mathfrak{A}_5$ un sous-groupe distingué. On énumère les éléments de $\mathfrak{A}_5$:

— L'identité (1 élément).
— Les 3-cycles (20 éléments) : si H en contient un, alors $H = \mathfrak{A}_5$.
— Les produits de deux transpositions à supports disjoints (15 éléments) : si H en contient un, alors H les contient tous.
— Les 5-cycles (24 éléments) : si H en contient un, alors H les contient tous.

L'identité est dans H, et aucun 3-cycle n'est dans H (car $H \neq \mathfrak{A}_5$). Ainsi $|H|$ est égal à 1, $1 + 15$, $1 + 24$ ou $1 + 15 + 24$. Mais $|H| \mid 60$ donc $|H| = 1$, i.e. $H = \{id\}$. □

Théorème 6.9.20. *Si $n \geqslant 5$, alors $\mathfrak{A}_n$ est simple.*

Démonstration. Soit $H \subset \mathfrak{A}_n$ un sous-groupe distingué, $H \neq \{id\}$. Soit $\sigma \in H \backslash \{id\}$. Soit $a \in [\![1,n]\!]$ t.q. $\sigma(a) \neq a$. On note $b = \sigma(a)$, et on se donne $c \in [\![1,n]\!] \backslash \{a, b, \sigma(b)\}$. On note $\tau = (a\,c\,b) \in \mathfrak{A}_n$. On considère $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$. Comme $\sigma \in H$ et H est distingué, $\tau\sigma\tau^{-1} \in H$, donc $\rho \in H$. Et on a :

$$\rho = \tau\left(\sigma\tau^{-1}\sigma^{-1}\right) = (a\,c\,b)\,(b\,\sigma(b)\,\sigma(c))\,.$$

Soit $X = \{a, b, c, \sigma(b), \sigma(c)\}$ le support de ρ. On a $|X| \leqslant 5$. Soit donc Y un ensemble de cardinal 5 t.q. $X \subset Y \subset [\![1,n]\!]$. On pose :

$$G = \{\tau \in \mathfrak{A}_n,\ \tau(Y) \subset Y \text{ et } \forall x \in [\![1,n]\!] \backslash Y,\ \tau(x) = x\}\,.$$

On a $G \simeq \mathfrak{A}_5$, donc G est simple selon la proposition 6.9.19. Soit alors $H' = H \cap G$. H' est distingué dans G, et $\rho \in H'$. Comme $\rho \neq id$, il vient $H' = G$, i.e. $G \subset H$. En particulier, H contient un 3-cycle donc $H = \mathfrak{A}_n$. □

7 Représentations linéaires des groupes finis

7.1 Généralités

Définition 7.1.1 (Représentation linéaire)**.** *Soit G un groupe. On appelle* représentation linéaire *de G la donnée d'un $\mathbb{C}$-espace vectoriel V de dimension finie et d'un morphisme de groupes $\rho : G \to GL(V)$. On dit que V est l'*espace sous-jacent *de la représentation. La représentation est notée (ρ, V) ; on abrège parfois en omettant ρ ou V. Pour $g \in G$ et $v \in V$, on pourra noter $g \cdot v = \rho(g)v$. On appelle* degré *de la représentation la dimension de V. On dit que la représentation est* fidèle *lorsque ρ est injectif.*

Remarque 7.1.2. *Une représentation linéaire de G peut être vue comme la donnée d'un $\mathbb{C}$-espace vectoriel V de dimension finie et d'une action de G sur V t.q. pour tout $g \in G$, l'application* $\begin{vmatrix} V \longrightarrow V \\ v \longmapsto g \cdot v \end{vmatrix}$ *est linéaire.*

7.2 Constructions de représentations

Proposition 7.2.1. *Si G est un groupe, et $\varphi : G \to \mathbb{C}^*$ est un morphisme, alors φ peut être vu comme une représentation de degré 1 de G. Une telle représentation est appelée* caractère linéaire *de G.*

Proposition 7.2.2 (Somme de deux représentations)**.** *Soit G un groupe. Soit (ρ, V) et (ρ', V') deux représentations de G. On note $i : GL(V) \times GL(V') \to GL(V \oplus V')$ l'injection canonique. On considère $r = i \circ (\rho, \rho')$. Alors $(r, V \oplus V')$ est une représentation de G.*

Proposition 7.2.3 (Produit tensoriel de deux représentations)**.** *Soit G un groupe. Soit (ρ, V) et (ρ', V') deux représentations de G. On considère $r : g \in G \longmapsto \rho(g) \otimes \rho'(g) \in GL(V \otimes V')$. Alors $(r, V \otimes V')$ est une représentation de G.*

Proposition 7.2.4 (Torsion d'une représentation par un caractère)**.** *Soit G un groupe, (ρ, V) une représentation de G et ψ un caractère de G. On considère $r : g \in G \longmapsto \psi(g)\rho(g) \in GL(V)$. Alors (r, V) est une représentation de G. C'est en fait le produit tensoriel des représentations (ρ, V) et $(\psi, \mathbb{C})$.*

Proposition 7.2.5. *Soit G un groupe. Soit (ρ, V) et (ρ', V') deux représentations de G. On considère :*

$$r : \begin{vmatrix} G \longrightarrow GL(\mathcal{L}(V, V')) \\ g \longmapsto \begin{vmatrix} \mathcal{L}(V, V') \longrightarrow \mathcal{L}(V, V') \\ f \longmapsto \rho'(g) \circ f \circ \rho(g)^{-1} \end{vmatrix} \end{vmatrix}.$$

Alors $(r, \mathcal{L}(V, V'))$ est une représentation de G.

Proposition 7.2.6. *Soit G un groupe. Soit (ρ, V) une représentation de G. On considère $r : g \in G \longmapsto {}^t\rho(g)^{-1} \in GL(V^*)$. Alors (r, V^*) est une représentation de G.*

Proposition 7.2.7. *Soit G un groupe, H un sous-groupe de G. Soit (ρ, V) une représentation de G.*

(i) $\left(\rho_{|H}, V\right)$ *est une représentation de H.*

(ii) *On suppose que H est distingué dans G et que $H \subset \operatorname{Ker}\rho$. Soit $\pi : G \to G/H$ la projection canonique. Alors il existe une représentation $(\overline{\rho}, V)$ de G/H t.q. $\rho = \overline{\rho} \circ \pi$.*

Proposition 7.2.8 (Représentation de permutation associée à une action)**.** *Soit G un groupe agissant sur un ensemble fini X. On note $V_X = \bigoplus_{x\in X} \mathbb{C}e_x$ et on définit $\rho_X : G \to GL(V_X)$ par $\forall g \in G,\ \forall x \in X,\ \rho_X(g)e_x = e_{g\cdot x}$. Alors (ρ_X, V_X) est une représentation de G.*

Exemple 7.2.9. *$\mathfrak{S}_n$ agit de manière naturelle sur $[\![1, n]\!]$. Et la représentation de permutation $(\rho, \mathbb{C}^n)$ associée à cette action vérifie $\forall \sigma \in \mathfrak{S}_n, \forall i \in [\![1, n]\!]$, $\rho(\sigma)e_i = e_{\sigma(i)}$, où $(e_1, \ldots, e_n)$ est la base canonique de $\mathbb{C}^n$.*

7.3 Sous-espaces stables

Définition 7.3.1 (Sous-espaces stables)**.** *Soit (ρ, V) une représentation d'un groupe G. Soit W un sous-espace vectoriel de V. On dit que W est un* sous-espace stable *lorsque :*

$$\forall g \in G,\ \rho(g)W \subset W.$$

Supposons maintenant que W est stable.

(i) *On a une représentation de G notée $\left(\rho_{|W}, W\right)$ définie par $\forall g \in G,\ \rho_{|W}(g) = \rho(g)_{|W}$. On dit que c'est une* sous-représentation *de (ρ, V).*

(ii) *On a une représentation de G notée $\left(\rho_{V/W}, V/W\right)$ définie par $\forall g \in G,\ \rho_{V/W}(g) \circ \pi = \pi \circ \rho(g)$, où $\pi : V \to V/W$ est la projection canonique. On dit que c'est une* représentation quotient *de (ρ, V).*

Définition 7.3.2. *Si (ρ, V) est une représentation d'un groupe G, on note :*

$$V^G = \{x \in V,\ \forall g \in G,\ g \cdot x = x\}.$$

Alors V^G est un sous-espace stable de V.

Exemple 7.3.3 (Représentation standard de $\mathfrak{S}_n$)**.** *On considère la représentation $(\rho, \mathbb{C}^n)$ de $\mathfrak{S}_n$ définie dans l'exemple 7.2.9. On note $\mu : x \in \mathbb{C}^n \longmapsto \sum_{i=1}^n x_i$ et $D = \mathbb{C}(e_1 + \cdots + e_n)$. Alors $D = (\mathbb{C}^n)^{\mathfrak{S}_n}$. Ainsi $\mathbb{C}^n = D \oplus \operatorname{Ker}\mu$, et D et $\operatorname{Ker}\mu$ sont des sous-espaces stables. De plus, la sous-représentation $\left(\rho_{|D}, D\right)$ est triviale. Et on appelle* représentation standard *de $\mathfrak{S}_n$ la sous-représentation $\left(\rho_{|\operatorname{Ker}\mu}, \operatorname{Ker}\mu\right)$, qui sera notée H_n.*

7.4 Morphismes de représentations

Définition 7.4.1 (Morphisme de représentations)**.** *Soit (ρ, V) et (ρ', V') deux représentations d'un groupe G. On appelle* morphisme de représentations *de (ρ, V) vers (ρ', V') toute application linéaire $u : V \to V'$ t.q.*

$$\forall g \in G,\ u \circ \rho(g) = \rho'(g) \circ u.$$

*On dit aussi que u est G-*équivariante*. On note $\operatorname{Hom}_G(V, V')$ l'ensemble des morphismes de représentations de (ρ, V) vers (ρ', V'). C'est un sous-espace vectoriel de $\mathcal{L}(V, V')$.*

Définition 7.4.2 (Isomorphisme de représentations)**.** *Soit (ρ, V) et (ρ', V') deux représentations d'un groupe G. On appelle* isomorphisme de représentations *tout morphisme de représentations bijectif. Autrement dit, un isomorphisme de représentations est une application linéaire bijective $u : V \to V'$ vérifiant :*

$$\forall g \in G,\ \rho'(g) = u \circ \rho(g) \circ u^{-1}.$$

Proposition 7.4.3. *Soit (ρ, V) et (ρ', V') deux représentations d'un groupe G. Si $u : V \to V'$ est un isomorphisme de représentations, alors $u^{-1} : V' \to V$ est aussi un isomorphisme de représentations.*

Proposition 7.4.4. *Soit (ρ, V) et (ρ', V') deux représentations d'un groupe G. En considérant la représentation canonique de G sur $\mathcal{L}(V, V')$ (c.f. proposition 7.2.5), on a :*

$$\mathrm{Hom}_G(V, V') = \mathcal{L}(V, V')^G.$$

Proposition 7.4.5. *Soit (ρ, V) et (ρ', V') deux représentations d'un groupe G. Alors l'isomorphisme canonique $V^* \otimes V' \to \mathcal{L}(V, V')$ est un isomorphisme de représentations.*

7.5 Sous-espaces stables et supplémentaires

Théorème 7.5.1. *Soit (ρ, V) une représentation d'un groupe fini G. Soit $W \subset V$ un sous-espace stable. Alors W admet un supplémentaire stable par G.*

Démonstration. On va construire $\pi \in \mathcal{L}(V)$ un projecteur G-équivariant d'image W. Ainsi, $\mathrm{Ker}\,\pi$ sera un supplémentaire de W, stable par G. Pour cela, soit d'abord p un projecteur quelconque d'image W. On pose :

$$\pi = \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ p \circ \rho(g)^{-1}.$$

Montrer que $\forall g \in G,\ \pi \circ \rho(g) = \rho(g) \circ \pi$, i.e. π est G-équivariant. De plus, comme W est stable, $(\pi \circ p)$ et p coïncident sur W. Et ils coïncident clairement sur $\mathrm{Ker}\,p$. Comme $V = W \oplus \mathrm{Ker}\,p$, on a donc $\pi \circ p = p$. On en déduit que $\pi \circ \pi = \pi$. Ainsi, π est un projecteur, $W \supset \mathrm{Im}\,\pi$; et $\mathrm{tr}\,p = \mathrm{tr}\,\pi$, d'où $\mathrm{rg}\,p = \mathrm{rg}\,\pi$, ce qui fournit $W = \mathrm{Im}\,\pi$. Donc π convient. □

Remarque 7.5.2. *Soit (ρ, V) une représentation d'un groupe fini G. Soit U, W deux sous-espaces stables de V t.q. $V = U \oplus W$. Alors (ρ, V) est la somme des représentations $\left(\rho_{|U}, U\right)$ et $\left(\rho_{|W}, W\right)$ (c.f. proposition 7.2.2). De plus, la représentation $\left(\rho_{|U}, U\right)$ est isomorphe à $\left(\rho_{V/W}, V/W\right)$.*

Proposition 7.5.3. *Soit (ρ, V) une représentation d'un groupe fini G. On pose :*

$$\pi_G = \frac{1}{|G|} \sum_{g \in G} \rho(g).$$

Alors π_G est un projecteur G-équivariant d'image V^G.

Démonstration. Montrer que $\forall g \in G,\ \pi_G \circ \rho(g) = \pi_G = \rho(g) \circ \pi_G$. Ceci prouve que π_G est G-équivariant et permet de montrer que $\pi_G \circ \pi_G = \pi_G$. En déduire de plus que $V^G = \mathrm{Im}\,\pi_G$. □

Corollaire 7.5.4. *Soit (ρ, V) une représentation d'un groupe fini G. Alors :*

$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\,\rho(g).$$

7.6 Représentations irréductibles

Définition 7.6.1 (Représentation irréductible)**.** *Soit (ρ, V) une représentation d'un groupe G. On dit que (ρ, V) est* irréductible *lorsque $V \neq \{0\}$ et les seuls sous-espaces de V stables par G sont $\{0\}$ et V.*

Notation 7.6.2. *Si G est un groupe, on note I_G l'ensemble des classes d'isomorphisme des représentations irréductibles de G. Les éléments de I_G (qui sont des classes d'équivalence de représentations) seront assimilés à des représentations.*

Théorème 7.6.3 (Lemme de Maschke)**.** *Soit (ρ, V) une représentation non nulle d'un groupe fini G. Alors V s'écrit comme somme directe de sous-espaces stables qui sont des représentations irréductibles.*

Remarque 7.6.4. *La décomposition fournie par le lemme de Maschke n'est pas nécessairement unique.*

Exemple 7.6.5. *On reprend les notations de l'exemple 7.3.3. Alors la décomposition $\mathbb{C}^n = D \oplus \operatorname{Ker} \mu$ est une décomposition de $\mathbb{C}^n$ en représentations irréductibles.*

Théorème 7.6.6 (Lemme de Schur)**.** *Soit (ρ, V) et (r, W) deux représentations irréductibles d'un groupe fini G. Alors on est dans l'un des deux cas suivants :*

(i) $\operatorname{Hom}_G(V, W) = \{0\}$.

(ii) *(ρ, V) et (r, W) sont isomorphes et* $\dim \operatorname{Hom}_G(V, W) = 1$.

En particulier, $\operatorname{Hom}_G(V, V) = \mathbb{C} id_V$.

Démonstration. Soit $u \in \operatorname{Hom}_G(V, W)$. Notons que $\operatorname{Ker} u$ et $\operatorname{Im} u$ sont des sous-espaces stables respectifs de V et W. Comme V et W sont irréductibles, on a $\operatorname{Ker} u = \{0\}$ ou $\operatorname{Ker} u = V$, et $\operatorname{Im} u = \{0\}$ ou $\operatorname{Im} u = W$. Donc $u = 0$ ou u est un isomorphisme. Supposons maintenant que $\operatorname{Hom}_G(V, W) \neq \{0\}$. Alors (ρ, V) et (r, W) sont isomorphes. Reste à prouver que $\dim \operatorname{Hom}_G(V, W) = 1$. Soit donc $(u, v) \in (\operatorname{Hom}_G(V, W) \backslash \{0\})^2$. On note $f = u^{-1} \circ v \in \operatorname{Hom}_G(V, V) \backslash \{0\}$. Il suffit de prouver que $f \in \mathbb{C} id_V$. Pour cela, soit $\lambda \in \mathbb{C}$ une valeur propre de f (car $\mathbb{C}$ est algébriquement clos). L'espace $\operatorname{Ker}(f - \lambda id_V)$ est stable par G, non réduit à $\{0\}$, donc il est égal à V (car V est irréductible). Ainsi, $f = \lambda id_V$. □

Notation 7.6.7. *Soit (ρ, V) une représentation d'un groupe fini G. À l'aide du lemme de Maschke (théorème 7.6.3), on écrit :*

$$V = \bigoplus_{i=1}^{n} V_i,$$

où V_i est une représentation irréductible de G pour tout $i \in [\![1, n]\!]$. Pour $W \in I_G$, on pose alors :

$$n_W = \left| \{ i \in [\![1, n]\!],\ V_i \simeq W \} \right|.$$

Proposition 7.6.8. *Deux représentations (ρ, V) et (ρ', V') d'un groupe fini G sont isomorphes* ssi

$$\forall W \in I_G,\ n_W = n'_W.$$

En particulier, pour $W \in I_G$, n_W ne dépend pas du choix de la décomposition de V en sous-espaces irréductibles.

Démonstration. Pour $W \in I_G$, on notera :

$$V_W = \bigoplus_{\substack{1 \leqslant i \leqslant n \\ V_i \simeq W}} V_i \qquad \text{et} \qquad V'_W = \bigoplus_{\substack{1 \leqslant i \leqslant n' \\ V'_i \simeq W}} V'_i$$

Ainsi :

$$V = \bigoplus_{W \in I_G} V_W \qquad \text{et} \qquad V' = \bigoplus_{W \in I_G} V'_W.$$

($\Rightarrow$) Soit $f : V \to V'$ un isomorphisme de représentations. Montrons que $f(V_W) \subset V'_W$ pour tout $W \in I_G$. Soit pour cela $U \in I_G$, avec $U \not\simeq W$ (si $\forall U \in I_G, U \simeq W$, alors $V'_W = V'$, donc $f(V_W) \subset V'_W$). On note π_U la projection sur V'_U parallèlement à $\bigoplus_{U' \in I_G \setminus \{U\}} V'_{U'}$. Soit de plus $i' \in [\![1, n']\!]$ t.q. $V'_{i'} \simeq U$. On note $\pi_{i'}$ la projection dans V'_U sur $V'_{i'}$ associée à la somme directe $V'_U = \bigoplus_{\substack{1 \leqslant i \leqslant n' \\ V'_i \simeq U}} V'_i$. On considère donc, pour $i \in [\![1, n]\!]$ t.q. $V_i \simeq W$:

$$W \simeq V_i \xrightarrow{f_{|V_i}} V' \xrightarrow{\pi_U} V'_U \xrightarrow{\pi_{i'}} V'_{i'} \simeq U.$$

Ainsi $\pi_{i'} \circ \pi_U \circ f_{|V_i}$ est un morphisme entre deux représentations irréductibles non isomorphes ; selon le lemme de Schur (théorème 7.6.6), ce morphisme est nul. Or :

$$\pi_U \circ f_{|V_i} = \sum_{\substack{1 \leqslant i' \leqslant n \\ V'_{i'} \simeq U}} \pi_{i'} \circ \pi_U \circ f_{|V_i} = 0.$$

Autrement dit $\operatorname{Im} f_{|V_i} \subset \operatorname{Ker} \pi_U$. Et ceci est vrai pour tout U t.q. $U \not\simeq W$, donc $\operatorname{Im} f_{|V_i} \subset V'_W$. Ceci étant vrai pour tout $i \in [\![1, n]\!]$ t.q. $V_i \simeq W$, il vient $f(V_W) \subset V'_W$. Et f est un isomorphisme de représentations, ce qui fournit :

$$\forall W \in I_G,\ f(V_W) = V'_W.$$

Donc :

$$\forall W \in I_G,\ n_W = \frac{\dim V_W}{\dim W} = \frac{\dim V'_W}{\dim W} = n'_W.$$

($\Leftarrow$) Si $\forall w \in I_G,\ n_W = n'_W$, alors $\forall W \in I_G,\ V_W \simeq V'_W$ donc :

$$V = \bigoplus_{W \in I_G} V_W \simeq \bigoplus_{W \in I_G} V'_W = V'.$$

□

Proposition 7.6.9. *Soit G un groupe abélien fini. Alors toutes les représentations irréductibles de G sont de dimension* 1.

Démonstration. Soit (ρ, V) une représentation irréductible de G. Soit $g \in G$. Soit λ une valeur propre de $\rho(g)$ (car $\mathbb{C}$ est algébriquement clos). On considère $V_\lambda = \operatorname{Ker}(\rho(g) - \lambda id_V)$. Alors V_λ est stable par G (car G est abélien), et $V_\lambda \neq \{0\}$. Comme (ρ, V) est irréductible, $V_\lambda = V$. Donc $\rho(g) = \lambda id_V$. Ainsi, $\forall g \in G,\ \rho(g) \in \mathbb{C} id_V$. Donc tout sous-espace de V est stable par G. Donc V est de dimension 1. □

7.7 Caractère d'une représentation

Définition 7.7.1 (Caractère)**.** *Soit (ρ, V) une représentation d'un groupe fini G. Le* caractère *de (ρ, V) est l'application suivante :*

$$\chi_V : \begin{vmatrix} G \longrightarrow \mathbb{C} \\ g \longmapsto \operatorname{tr} \rho(g) \end{vmatrix}.$$

Si (ρ, V) est irréductible, on dit que χ_V est un caractère irréductible. *Si $\dim V = 1$, on dit que χ_V est un* caractère linéaire.

Proposition 7.7.2. *Soit (ρ, V) et (ρ', V') deux représentations d'un groupe fini G. Si (ρ, V) et (ρ', V') sont isomorphes, alors :*

$$\chi_V = \chi_{V'}.$$

Proposition 7.7.3. *Soit (ρ, V) une représentation d'un groupe fini G. Alors :*

$$\forall g \in G,\ \chi_V\left(g^{-1}\right) = \overline{\chi_V(g)}.$$

Démonstration. Soit $g \in G$, $n = \dim V$. On note $\lambda_1, \dots, \lambda_n$ les valeurs propres de $\rho(g)$. Comme G est un groupe fini, on a $\rho(g)^{|G|} = \rho\left(g^{|G|}\right) = 1$. Donc $\forall i \in [\![1, n]\!]$, $|\lambda_i| = 1$. Donc :

$$\chi_V\left(g^{-1}\right) = \operatorname{tr}\rho(g)^{-1} = \sum_{i=1}^{n} \lambda_i^{-1} = \sum_{i=1}^{n} \overline{\lambda_i} = \overline{\sum_{i=1}^{n} \lambda_i} = \overline{\operatorname{tr}\rho(g)} = \overline{\chi_V(g)}.$$

□

Remarque 7.7.4. *Soit (ρ, V) une représentation d'un groupe fini G. Pour tout $g \in G$, le polynôme $\left(X^{|G|} - 1\right)$ est simplement scindé et annule $\rho(g)$, donc $\rho(g)$ est diagonalisable.*

Proposition 7.7.5. *Soit (ρ, V) une représentation d'un groupe fini G. Alors :*

$$\forall g \in G,\ \rho(g) = id_V \iff \chi_V(g) = \dim V.$$

Corollaire 7.7.6. *Soit (ρ, V) une représentation d'un groupe fini G. Alors (ρ, V) est fidèle* ssi $\forall g \in G\backslash\{e\},\ \chi_V(g) \neq \dim V$.

Proposition 7.7.7. *Soit (ρ, V) et (r, W) deux représentations d'un groupe fini G. Alors :*

(i) $\chi_{V\oplus W} = \chi_V + \chi_W$.

(ii) $\chi_{\mathcal{L}(V,W)} = \overline{\chi_V}\chi_W$.

(iii) $\chi_{V\otimes W} = \chi_V\chi_W$.

(iv) $\chi_{V^*} = \overline{\chi_V}$.

Proposition 7.7.8. *Soit (ρ, V) une représentation d'un groupe fini G. Alors :*

$$\dim V^G = \frac{1}{|G|}\sum_{g\in G} \chi_V(g).$$

Démonstration. Voir corollaire 7.5.4. □

Exemple 7.7.9. *Soit G un groupe fini agissant sur un ensemble fini X. Soit (ρ_X, V_X) la représentation de permutation associée à cette action (c.f. proposition 7.2.8). Alors :*

$$\forall g \in G,\ \chi_{V_X}(g) = \left|\{x \in X,\ g \cdot x = x\}\right|.$$

7.8 Interlude – Espaces hermitiens

Définition 7.8.1 (Espace hermitien)**.** *Soit E un $\mathbb{C}$-espace vectoriel de dimension finie. On appelle* produit scalaire hermitien *sur E toute application $\langle\cdot \mid \cdot\rangle : E \times E \to \mathbb{C}$ vérifiant les trois conditions suivantes :*

(i) $\langle\cdot \mid \cdot\rangle$ *est* sesquilinéaire *: $\forall x \in E,\ \forall (y, y') \in E^2,\ \forall \alpha \in \mathbb{C},\ \langle x \mid y + \alpha y'\rangle = \langle x \mid y\rangle + \alpha \langle x \mid y'\rangle$ et $\forall y \in E,\ \forall (x, x') \in E^2,\ \forall \alpha \in \mathbb{C},\ \langle x + \alpha x' \mid y\rangle = \langle x \mid y\rangle + \overline{\alpha}\langle x' \mid y\rangle$.*

(ii) $\langle\cdot \mid \cdot\rangle$ *est* hermitienne *: $\forall (x, y) \in E^2,\ \langle y \mid x\rangle = \overline{\langle x \mid y\rangle}$.*

(iii) $\langle\cdot \mid \cdot\rangle$ *est* définie positive *: $\forall x \in E\backslash\{0\},\ \langle x \mid x\rangle \in \mathbb{R}_+^*$.*

On dit alors que $(E, \langle\cdot \mid \cdot\rangle)$ est un espace hermitien*.*

Définition 7.8.2 (Orthogonal)**.** *Soit E un espace hermitien. Pour $X \subset E$, on définit :*

$$X^\perp = \{y \in E,\ \forall x \in X,\ \langle x \mid y\rangle = 0\} = \{y \in E,\ \forall x \in X,\ \langle y \mid x\rangle = 0\}.$$

Proposition 7.8.3. *Soit E un espace hermitien.*

(i) *Pour $X \subset E$, $X^\perp$ est un sous-espace vectoriel de E.*

(ii) *Pour $X \subset E$, $X^\perp = \mathrm{Vect}(X)^\perp$.*

(iii) *Si V est un sous-espace vectoriel de E, $E = V \oplus V^\perp$.*

Corollaire 7.8.4. *Soit E un espace hermitien et V un sous-espace vectoriel de E. Alors :*

(i) *$V = E \iff V^\perp = \{0\}$ et $V = \{0\} \iff V^\perp = E$.*

(ii) *$V^{\perp\perp} = V$.*

Définition 7.8.5 (Famille orthogonale, orthonormale)**.** *Soit E un espace hermitien, $(e_i)_{i\in I}$ une famille d'éléments de E.*

(i) *On dit que $(e_i)_{i\in I}$ est* orthogonale *lorsque $\forall (i,j) \in I^2,\ i \neq j \Longrightarrow \langle e_i \mid e_j\rangle = 0$.*

(ii) *On dit que $(e_i)_{i\in I}$ est* orthonormale *lorsqu'elle est orthogonale et que $\forall i \in I,\ \langle e_i \mid e_i\rangle = 1$.*

Remarque 7.8.6. *Toute famille orthonormale d'un espace hermitien est libre.*

Exemple 7.8.7. *On peut redémontrer le théorème 7.5.1 en utilisant des notions d'espaces hermitiens. Pour cela, soit (ρ, V) une représentation d'un groupe fini G et soit $W \subset V$ un sous-espace stable. On se donne d'abord $\langle \cdot \mid \cdot \rangle$ un produit scalaire hermitien quelconque sur V. On va utiliser $\langle \cdot \mid \cdot \rangle$ pour construire sur V un produit scalaire hermitien $[\cdot \mid \cdot]$ vérifiant :*

$$\forall g \in G,\ \forall (x,y) \in V^2,\ [g\cdot x \mid g \cdot y] = [x \mid y]\,.$$

On définit pour cela :

$$[\cdot \mid \cdot] : (x,y) \in V^2 \longmapsto \sum_{g\in G} \langle g\cdot x \mid g\cdot y\rangle\,.$$

Alors $[\cdot \mid \cdot]$ convient. On considère $W^\perp$ l'orthogonal de W au sens de $[\cdot \mid \cdot]$. Alors $V = W \oplus W^\perp$, et on vérifie que $W^\perp$ est stable par G.

7.9 Fonctions centrales

Définition 7.9.1 (Fonction centrale)**.** *Soit G un groupe fini. On appelle* fonction centrale *sur G toute application $f : G \to \mathbb{C}$ qui vérifie :*

$$\forall (g,h) \in G^2,\ f(gh) = f(hg).$$

Autrement dit, une fonction centrale est une fonction constante sur les classes de conjugaison. On note $R(G)$ le $\mathbb{C}$-espace vectoriel des fonctions centrales sur G.

Proposition 7.9.2. *Soit G un groupe fini. Alors* $\dim R(G)$ *est le nombre de classes de conjugaison dans G.*

Exemple 7.9.3. *Soit (ρ, V) une représentation d'un groupe fini G. Alors $\chi_V \in R(G)$.*

Définition 7.9.4 (Structure hermitienne de $R(G)$)**.** *On munit $R(G)$ d'un produit scalaire hermitien en posant :*

$$\forall (u,v) \in R(G)^2,\ \langle u \mid v\rangle = \frac{1}{|G|}\sum_{g\in G} \overline{u(g)}v(g).$$

Proposition 7.9.5. *Soit (ρ, V) et (r, W) deux représentations d'un groupe fini G. Alors, dans $R(G)$:*

$$\langle \chi_W \mid \chi_V\rangle = \dim \mathrm{Hom}_G\,(W,V)\,.$$

Démonstration. On considère la représentation de G sur $\mathcal{L}(W,V)$ obtenue à partir des représentations sur V et W (c.f. proposition 7.2.5). Alors, avec les propositions 7.4.4, 7.7.8 et 7.7.7, on a :

$$\dim \mathrm{Hom}_G(W,V) = \dim \mathcal{L}(W,V)^G = \frac{1}{|G|}\sum_{g\in G}\chi_{\mathcal{L}(W,V)}(g) = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_W}(g)\chi_V(g) = \langle \chi_W \mid \chi_V\rangle .$$

□

Corollaire 7.9.6. *Soit (ρ,V) et (r,W) deux représentations d'un groupe fini G. Alors :*

$$\dim \mathrm{Hom}_G(W,V) = \dim \mathrm{Hom}_G(V,W).$$

Corollaire 7.9.7. *Soit G un groupe fini. Alors la famille $(\chi_V)_{V\in I_G}$ est orthonormale.*

Démonstration. Utiliser le lemme de Schur (théorème 7.6.6). □

Proposition 7.9.8. *Soit (ρ,V) une représentation d'un groupe fini G. Étant donné $W\in I_G$, on définit n_W comme dans la notation 7.6.7. Alors :*

$$\forall W\in I_G,\ n_W = \langle \chi_W \mid \chi_V\rangle .$$

Corollaire 7.9.9. *Soit (ρ,V) et (ρ',V') deux représentations d'un groupe fini G. Alors :*

$$\chi_V = \chi_{V'} \iff (\rho,V)\simeq(\rho',V').$$

Définition 7.9.10 (Représentation régulière gauche)**.** *Soit G un groupe fini. Alors G agit sur lui-même par translation à gauche. Comme dans la proposition 7.2.8, on en déduit une action de G sur $V_G=\mathbb{C}^{|G|}$, appelée* représentation régulière gauche *de G.*

Proposition 7.9.11. *Soit G un groupe fini et V_G sa représentation régulière gauche. Alors :*

$$\chi_{V_G} = |G|\,\mathbb{1}_{\{e\}}.$$

Proposition 7.9.12. *Soit G un groupe fini et $W\in I_G$. Alors, pour la représentation régulière gauche de G, on a $n_W=\dim W$.*

Démonstration. On a :

$$n_W = \langle \chi_W \mid \chi_{V_G}\rangle = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_W(g)}\chi_{V_G}(g) = \overline{\chi_W(e)} = \overline{\mathrm{tr}\, id_W} = \dim W.$$

□

Corollaire 7.9.13. *Soit G un groupe fini. Alors :*

$$|G| = \sum_{W\in I_G}(\dim W)^2 .$$

Démonstration. Utiliser le fait que $|G|=\dim V_G$ et la proposition 7.9.12. □

Proposition 7.9.14. *Soit G un groupe fini. Alors $(\chi_W)_{W\in I_G}$ est une base orthonormale de $R(G)$.*

Démonstration. On a déjà vu (c.f. corollaire 7.9.7) que la famille $(\chi_W)_{W\in I_G}$ est orthonormale (donc libre). Montrons que $\mathrm{Vect}(\chi_W,\ W\in I_G) = R(G)$, i.e. $\{\chi_W,\ W\in I_G\}^\perp = \{0\}$. Soit donc $\alpha\in\{\chi_W,\ W\in I_G\}^\perp$. Étant donnée une représentation (ρ,V) de G, on définit :

$$f_{V,\alpha} = \sum_{g\in G}\overline{\alpha(g)}\rho(g)\in\mathcal{L}(V).$$

Alors $f_{V,\alpha} \in \mathrm{Hom}_G(V,V)$. Ainsi, si V est irréductible, $f_{V,\alpha}$ est une homothétie : il existe $\lambda \in \mathbb{C}$ t.q. $f_{V,\alpha} = \lambda id_V$. On a alors :

$$\lambda(\dim V) = \mathrm{tr}\, f_{V,\alpha} = \sum_{g\in G} \overline{\alpha(g)}\chi_V(g) = |G|\,\langle \alpha \mid \chi_V\rangle = 0,$$

donc $\lambda = 0$ et $f_{V,\alpha} = 0$. Remarquons maintenant que si (ρ, V) est une représentation quelconque de G, $V = U \oplus W$, avec U et W stables, alors U et W sont stables par $f_{V,\alpha}$ et $f_{V,\alpha|U} = f_{U,\alpha}$ et $f_{V,\alpha|W} = f_{W,\alpha}$. En décomposant une représentation quelconque (ρ, V) de G en somme de décompositions irréductibles (c.f. lemme de Maschke, théorème 7.6.3), on en déduit que $f_{V,\alpha} = 0$. On applique cela à la représentation régulière gauche (ρ_G, V_G) (c.f. définition 7.9.10) de G. Ainsi, en notant e_1 le vecteur de base de V_G indexé par le neutre de G :

$$0 = f_{V_G,\alpha}(e_1) = \sum_{g\in G} \overline{\alpha(g)}\,(g\cdot e_1) = \sum_{g\in G} \overline{\alpha(g)} e_g.$$

Comme $(e_g)_{g\in G}$ est une base de V_G, il vient $\forall g \in G,\ \alpha(g) = 0$, i.e. $\alpha = 0$. □

Corollaire 7.9.15. *Soit G un groupe fini. Alors G a autant de représentations irréductibles que de classes de conjugaison.*

Corollaire 7.9.16. *Soit G un groupe fini. Alors :*

$$\forall \alpha \in R(G),\ \alpha = \sum_{W\in I_G} \langle \chi_W \mid \alpha\rangle\, \chi_W.$$

7.10 Table des caractères

Définition 7.10.1 (Table des caractères)**.** *Soit G un groupe fini. On appelle* table de caractères *de G le tableau dont les colonnes sont indexées par les classes de conjugaison $\gamma_1, \ldots, \gamma_s$ (il est aussi utile d'indiquer le nombre d'éléments de chaque classe de conjugaison) de G et les lignes sont indexées par les représentations irréductibles $W_1, \ldots, W_s$ de G. Dans la case (i,j) est indiquée la valeur de $\chi_{W_i}(g_j)$, où g_j est un élément quelconque de γ_j.*

Exemple 7.10.2 (Table des caractères de $\mathfrak{S}_3$)**.** *On note $\mathbb{1}$ la représentation triviale de $\mathfrak{S}_3$, ε la signature, et H_3 la représentation standard de $\mathfrak{S}_3$ (c.f. exemple 7.3.3). Alors la table des caractères de $\mathfrak{S}_3$ est donnée par :*

	(1) *1 élément*	(1 2) *3 éléments*	(1 2 3) *2 éléments*
$\mathbb{1}$	1	1	1
ε	1	-1	1
H_3	2	0	-1

Proposition 7.10.3. *Soit G un groupe fini. On considère la table des caractères de G, vue comme une matrice $X \in \mathbb{M}_s(\mathbb{C})$. On note $K \in \mathbb{M}_s(\mathbb{C})$ la matrice diagonale dont le i-ième coefficient est le cardinal de la i-ième classe de conjugaison de G.*

(i) *Dans la colonne correspondant à la classe de e (habituellement la première colonne), le coefficient de la i-ième ligne est la dimension de la i-ième représentation irréductible de G. Donc le somme des carrés des coefficients présents dans cette colonne est égale à $|G|$ (c.f. corollaire 7.9.13).*

(ii) $\overline{X} K\,({}^tX) = |G|\, I_s$.

(iii) ${}^t\big(\overline{X}\big) X = |G|\, K^{-1}$.

(iv) *Les colonnes de X sont deux à deux orthogonales pour le produit scalaire hermitien usuel.*

Exemple 7.10.4 (Table des caractères de $\mathfrak{S}_4$)**.** *On note $\mathbb{1}$ la représentation triviale de $\mathfrak{S}_4$, ε la signature, H_4 la représentation standard de $\mathfrak{S}_4$, $H_4(\varepsilon)$ la torsion de H_4 par ε (c.f. proposition 7.2.4) et W la cinquième représentation irréductible de $\mathfrak{S}_4$. Alors la table des caractères de $\mathfrak{S}_4$ est donnée par :*

	(1) *1 élément*	$(1\,2)$ *6 éléments*	$(1\,2\,3)$ *8 éléments*	$(1\,2\,3\,4)$ *6 éléments*	$(1\,2)(3\,4)$ *3 éléments*
$\mathbb{1}$	1	1	1	1	1
ε	1	-1	1	-1	1
H_4	3	1	0	-1	-1
$H_4(\varepsilon)$	3	-1	0	1	-1
W	2	0	-1	0	2

8 Groupes linéaires

8.1 Généralités

Définition 8.1.1 (Groupes linéaires)**.** *Soit k un corps, $n \in \mathbb{N}^*$.*

(i) *On note $GL_n(k)$ le groupe des matrices inversibles de $\mathbb{M}_n(k)$ et $SL_n(k) = \operatorname{Ker}\det \subset GL_n(k)$.*

(ii) *Si E est un k-espace vectoriel de dimension n, on note $GL(E)$ le groupe des endomorphismes inversibles de $\mathcal{L}(E)$ et $SL(E) = \operatorname{Ker}\det \subset GL(E)$.*

On a $GL(E) \simeq GL_n(k)$ et $SL(E) \simeq SL_n(k)$.

Proposition 8.1.2. *Soit k un corps fini de cardinal q, $n \in \mathbb{N}^*$. Alors :*

$$|GL_n(k)| = \prod_{i=0}^{n-1} \left(q^n - q^k\right) \qquad \text{et} \qquad |SL_n(k)| = \frac{1}{q-1} \prod_{i=0}^{n-1} \left(q^n - q^k\right).$$

8.2 Transvections

Définition 8.2.1 (Transvection)**.** *Soit k un corps, E un k-espace vectoriel de dimension n. On dit que $u \in GL(E)$ est une* transvection *lorsque :*

(i) $\dim \operatorname{Ker}(u - id_E) = n - 1$.

(ii) $\det u = 1$.

Proposition 8.2.2. *Soit k un corps, E un k-espace vectoriel de dimension n. Pour $u \in GL(E)$, les propriétés suivantes sont équivalentes :*

(i) *u est une transvection.*

(ii) *Il existe $\mu \in E^*\backslash\{0\}$ et $v \in \operatorname{Ker}\mu\backslash\{0\}$ t.q.*

$$\forall x \in E,\ u(x) = x + \mu(x)v.$$

On dit alors que u est une transvection d'hyperplan $H = \operatorname{Ker}\mu$ et de droite $D = kv$. H et D sont entièrement déterminés par u car $H = \operatorname{Ker}(u - id_E)$ et $D = \operatorname{Im}(u - id_E)$.

(iii) *Il existe une base $\mathcal{B}$ de E et un $\lambda \in k^*$ t.q. $\mathcal{M}_{\mathcal{B}}(u) = I_n + \lambda E^{n-1,n}$.*

(iv) *Il existe une base $\mathcal{B}$ de E t.q. $\mathcal{M}_{\mathcal{B}}(u) = I_n + E^{n-1,n}$.*

Proposition 8.2.3. *Soit k un corps, E un k-espace vectoriel de dimension n. Soit $u \in GL(E)$ une transvection d'hyperplan H et de droite D. Alors pour tout $g \in GL(E)$, gug^{-1} est une transvection d'hyperplan $g(H)$ et de droite $g(D)$.*

Proposition 8.2.4. *Soit k un corps, E un k-espace vectoriel de dimension n. Alors toutes les transvections sont conjuguées dans $GL(E)$.*

Démonstration. Selon la proposition 8.2.2, pour toute transvection u, il existe une base $\mathcal{B}$ de E t.q. $\mathcal{M}_{\mathcal{B}}(u) = I_n + E^{n-1,n}$. □

Proposition 8.2.5. *Soit k un corps, E un k-espace vectoriel de dimension n. Si $n \geqslant 3$, alors toutes les transvections sont conjuguées dans $SL(E)$.*

Démonstration. Soit u, v deux transvections (donc $(u, v) \in SL(E)^2$). Soit $g \in GL(E)$ t.q. $v = gug^{-1}$. On note $a = \det g$. Soit $\mathcal{B}$ une base de E t.q. $\mathcal{M}_{\mathcal{B}}(u) = I_n + E^{n-1,n}$. Si on pose $h \in GL(E)$ défini par $\mathcal{M}_{\mathcal{B}}(h) = \operatorname{diag}(a, 1, \ldots, 1)$, on a $uh = hu$ (car $n \geqslant 3$). Ainsi, $v = (gh^{-1})\, u\, (gh^{-1})^{-1}$, et $(gh^{-1}) \in SL(E)$. □

Proposition 8.2.6. *Soit k un corps. Dans $SL_2(k)$, toute matrice de transvection est conjuguée à une matrice de la forme $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, avec $x \in k^*$. De plus, pour $(x, y) \in (k^*)^2$, les matrices $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ sont conjuguées* ssi *il existe $t \in k^*$ t.q. $\frac{x}{y} = t^2$.*

8.3 Dilatations

Définition 8.3.1 (Dilatation)**.** *Soit k un corps, E un k-espace vectoriel de dimension n. On dit que $u \in GL(E)$ est une* dilatation *lorsque :*

(i) $\dim \operatorname{Ker}(u - id_E) = n - 1$.

(ii) $\det u \neq 1$.

Proposition 8.3.2. *Soit k un corps, E un k-espace vectoriel de dimension n. Pour $u \in GL(E)$, les propriétés suivantes sont équivalentes :*

(i) *u est une dilatation.*

(ii) *Il existe un hyperplan H, une droite D et un $a \in k^* \backslash \{1\}$ avec $E = H \oplus D$ t.q.*

$$\forall x \in H,\ u(x) = x \qquad \text{et} \qquad \forall x \in D,\ u(x) = ax.$$

On dit alors que u est la dilatation d'hyperplan H, de droite D et de rapport a. u est caractérisée par H, D, a, et réciproquement.

(iii) *Il existe une base $\mathcal{B}$ de E et un $a \in k^* \backslash \{1\}$ t.q. $\mathcal{M}_{\mathcal{B}}(u) = \operatorname{diag}(1, \ldots, 1, a)$.*

Proposition 8.3.3. *Soit k un corps, E un k-espace vectoriel de dimension n. Soit $u \in GL(E)$ la dilatation d'hyperplan H, de droite D et de rapport a. Alors pour tout $g \in GL(E)$, gug^{-1} est la dilatation d'hyperplan $g(H)$, de droite $g(D)$ et de rapport a.*

Proposition 8.3.4. *Soit k un corps, E un k-espace vectoriel de dimension n. Alors deux dilatations u, v sont conjuguées dans $GL(E)$* ssi *elles on le même rapport (i.e. $\det u = \det v$).*

8.4 Opérations élémentaires sur les lignes et les colonnes

Définition 8.4.1 (Matrices élémentaires)**.** *Soit k un corps, $\lambda \in k^*$, $(i, j) \in [\![1, n]\!]^2$ avec $i \neq j$.*

(i) *La* matrice de transvection *$T_{ij}(\lambda)$ est définie par $T_{ij}(\lambda) = I_n + \lambda E_{ij}$.*

(ii) *La* matrice de transposition *P_{ij} est définie par $P_{ij} = I_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$.*

Remarque 8.4.2. *Soit k un corps, $\lambda \in k^*$, $(i, j) \in [\![1, n]\!]^2$ avec $i \neq j$. Alors $T_{ij}(\lambda)$ est la matrice d'une transvection : il existe une transvection $u \in GL(k^n)$ et une base $\mathcal{B}$ de k^n t.q. $T_{ij}(\lambda) = \mathcal{M}_{\mathcal{B}}(u)$.*

Proposition 8.4.3. *Soit k un corps, $A \in \mathbb{M}_n(k)$, $\lambda \in k^*$, $(i, j) \in [\![1, n]\!]^2$ avec $i \neq j$. On note $\mathfrak{L}_1, \ldots, \mathfrak{L}_n$ les n vecteurs lignes de A, $\mathfrak{C}_1, \ldots, \mathfrak{C}_n$ les n vecteurs colonnes de A. On a alors une correspondance entre les matrices élémentaires et les opérations élémentaires sur les lignes et les colonnes de A :*

Lignes	Transvection	$\mathfrak{L}_i \longleftarrow \mathfrak{L}_i + \lambda\mathfrak{L}_j$	$A \longmapsto T_{ij}(\lambda)A$
	Transposition	$\mathfrak{L}_i \longleftrightarrow \mathfrak{L}_j$	$A \longmapsto P_{ij}A$
Colonnes	Transvection	$\mathfrak{C}_i \longleftarrow \mathfrak{C}_i + \lambda\mathfrak{C}_j$	$A \longmapsto AT_{ji}(\lambda)$
	Transposition	$\mathfrak{C}_i \longleftrightarrow \mathfrak{C}_j$	$A \longmapsto AP_{ij}$

Remarque 8.4.4. *Les opérations de transvection ne changent pas le déterminant, mais les opérations de transposition le multiplient par* (-1).

Théorème 8.4.5 (Algorithme du pivot de Gauß)**.** *Soit* k *un corps,* $A \in \mathbb{M}_n(k)$*. Alors on peut transformer* A *en une matrice diagonale* D *par des opérations élémentaires sur les lignes et les colonnes. De plus,* $\det A = (-1)^m \det D$*, où* m *est le nombre de transpositions effectuées.*

8.5 Générateurs des groupes linéaires

Lemme 8.5.1. *Soit* k *un corps et* $a \in k^*$*. Alors :*

(i) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(ii) $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & a^{-1} \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$.

Théorème 8.5.2. *Soit* k *un corps et* $n \in \mathbb{N}^*$*. Alors* $SL_n(k) = \langle \{T_{ij}(\lambda),\ i \neq j,\ \lambda \in k^*\} \rangle$

Démonstration. Pour $i \neq j$, on pose $\widetilde{P}_{ij} = I_n - E_{ii} - E_{jj} + E_{ij} - E_{ji} \in SL_n(k)$. Pour $i \leqslant n-1$ et $a \in k^*$, on pose $\delta_i(a) = \operatorname{diag}(1, \ldots, 1, a, a^{-1}, 1, \ldots, 1) \in SL_n(k)$, où le a est en position i. On note $G_1 = \langle \{T_{ij}(\lambda),\ i \neq j,\ \lambda \in k^*\} \rangle$, $G_2 = \left\langle G_1 \cup \left\{\widetilde{P}_{ij},\ i \neq j\right\}\right\rangle$ et $G_3 = \langle G_2 \cup \{\delta_i(a),\ i \leqslant n-1,\ a \in k^*\} \rangle$. Notons que G_3 contient toutes les matrices diagonales de $SL_n(k)$. Or, avec le théorème 8.4.5, on voit que toute matrice $A \in SL_n(k)$ s'écrit $A = PDQ$, avec $(P, Q) \in G_2^2$, D diagonale. Ainsi, $SL_n(k) = G_3$. De plus, avec le lemme 8.5.1, on voit que $G_2 = G_1$ puis que $G_3 = G_2$. Ainsi, $G_1 = SL_n(k)$. □

Théorème 8.5.3. *Soit* k *un corps et* E *un* k*-espace vectoriel de dimension* n*.*

(i) $SL(E)$ *est engendré par les transvections.*

(ii) $GL(E)$ *est engendré par les transvections et les dilatations.*

8.6 Sous-groupes et quotients des groupes linéaires

Proposition 8.6.1. *Soit* k *un corps et* $n \in \mathbb{N}^*$*. Alors :*

(i) $Z(SL_n(k)) = \mu_n(k) I_n \simeq \mu_n(k)$*, où* $\mu_n(k) = \{\lambda \in k^*,\ k^n = 1\}$.

(ii) $Z(GL_n(k)) = k^* I_n \simeq k^*$.

Proposition 8.6.2. *Soit* k *un corps et* $n \in \mathbb{N}^*$*. Alors :*

(i) $D(SL_n(k)) = SL_n(k)$*, sauf si* $n = 2$ et $(k \simeq \mathbb{Z}/2\mathbb{Z}$ ou $k \simeq \mathbb{Z}/3\mathbb{Z})$.

(ii) $D(GL_n(k)) = SL_n(k)$*, sauf si* $n = 2$ et $k \simeq \mathbb{Z}/2\mathbb{Z}$.

Corollaire 8.6.3. *Soit* k *un corps et* $n \in \mathbb{N}^*$*. Soit* A *un groupe abélien*

(i) *On suppose que* $n \neq 2$ ou $(k \not\simeq \mathbb{Z}/2\mathbb{Z}$ et $k \not\simeq \mathbb{Z}/3\mathbb{Z})$*. Alors tout morphisme* $\varphi : SL_n(k) \to A$ *est trivial.*

(ii) *On suppose que* $n \neq 2$ ou $k \not\simeq \mathbb{Z}/2\mathbb{Z}$*. Alors pour tout morphisme* $\varphi : GL_n(k) \to A$*, il existe un morphisme* $\psi : k^* \to A$ *t.q.* $\varphi = \psi \circ \det$.

8.7 Groupes projectifs linéaires

Définition 8.7.1 (Groupes projectifs linéaires)**.** *Soit k un corps, $n \in \mathbb{N}^*$.*

(i) *On note $PGL_n(k) = GL_n(k)/Z(GL_n(k))$ et $PSL_n(k) = SL_n(k)/Z(SL_n(k))$.*

(ii) *Si E est un k-espace vectoriel de dimension n, on note $PGL(E) = GL(E)/Z(GL(E))$ et $PSL(E) = SL(E)/Z(SL(E))$.*

On a $PGL(E) \simeq PGL_n(k)$ et $PSL(E) \simeq PSL_n(k)$.

Théorème 8.7.2. *Soit k un corps, $n \in \mathbb{N}^*$. Alors $PSL_n(k)$ est simple, sauf si $n = 2$ et ($k \simeq \mathbb{Z}/2\mathbb{Z}$ ou $k \simeq \mathbb{Z}/3\mathbb{Z}$).*

Remarque 8.7.3. *$PSL_2(\mathbb{Z}/2\mathbb{Z}) \simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \simeq \mathfrak{S}_3$ et $PSL_2(\mathbb{Z}/3\mathbb{Z}) \simeq \mathfrak{A}_4$.*

Remarque 8.7.4. *Soit k un corps et E un k-espace vectoriel de dimension n. On note $\mathbb{P}(E)$ l'ensemble des droites vectorielles de E, appelé* espace projectif *de E. Alors $GL(E)$ agit sur $\mathbb{P}(E)$, mais cette action n'est pas fidèle, son noyau est $Z(GL(E))$. Ainsi, $PGL(E) = GL(E)/Z(GL(E))$ agit de manière fidèle sur $\mathbb{P}(E)$. De même, $PSL(E)$ agit de manière fidèle sur $\mathbb{P}(E)$.*

9 Groupes orthogonaux

9.1 Généralités

Définition 9.1.1 (Groupes orthogonaux)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. On pose :*

$$O(q) = \{u \in GL(E),\ \forall x \in E,\ q(u(x)) = q(x)\},$$

et $SO(q) = O(q) \cap SL(E)$. Les éléments de $O(q)$ sont appelés isométries *; ceux de $SO(q)$ sont appelés* isométries directes*.*

Proposition 9.1.2. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Soit $u \in GL(E)$.*

(i) *Soit β une base orthonormée de E. Alors $u \in O(q)$* ssi *$u(\beta)$ est une base orthonormée de E.*

(ii) *$u \in O(q)$* ssi *$u^* = u^{-1}$.*

(iii) *Si $u \in O(q)$, alors $(\det u) \in \{-1, +1\}$.*

Proposition 9.1.3. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Si n est impair, alors $O(q) \simeq SO(q) \times \{-1, +1\}$ (car $(-id_E) \in O(q) \backslash SO(q)$).*

9.2 Aspect matriciel

Définition 9.2.1 (Groupes orthogonaux)**.** *Soit $n \in \mathbb{N}^*$. On définit :*

$$O_n(\mathbb{R}) = \left\{A \in GL_n(\mathbb{R}),\ {}^tAA = I_n\right\},$$

et $SO_n(\mathbb{R}) = O_n(\mathbb{R}) \cap SL_n(\mathbb{R})$.

Proposition 9.2.2. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Soit β une base orthonormale de E et $u \in GL(E)$. Alors :*

(i) *$u \in O(q) \iff \mathcal{M}_\beta(u) \in O_n(\mathbb{R})$.*

(ii) *$u \in SO(q) \iff \mathcal{M}_\beta(u) \in SO_n(\mathbb{R})$.*

Ainsi, $O(q) \simeq O_n(\mathbb{R})$ et $SO(q) \simeq SO_n(\mathbb{R})$.

Proposition 9.2.3. *Soit $n \in \mathbb{N}^*$. Alors $O_n(\mathbb{R})$ est une partie compacte de $\mathbb{M}_n(\mathbb{R})$.*

9.3 Décomposition polaire

Définition 9.3.1 (Endomorphisme symétrique)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Un endomorphisme $u \in \mathcal{L}(E)$ est dit* symétrique *lorsque $u^* = u$. On note $S(E)$ l'ensemble des endomorphismes symétriques de $\mathcal{L}(E)$.*

Théorème 9.3.2 (Théorème spectral)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Alors tout endomorphisme symétrique sur E est diagonalisable en base orthonormée, à valeurs propres réelles.*

Définition 9.3.3 (Endomorphismes positifs et définis positifs)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Soit $u \in S(E)$.*

(i) *On dit que u est* positif*, et on note $u \in S^+(E)$, lorsque les valeurs propres de u sont positives.*

(ii) *On dit que u est* défini positif*, et on note $u \in S^{++}(E)$, lorsque les valeurs propres de u sont strictement positives.*

Remarque 9.3.4. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Soit $u \in S(E)$. Alors u est défini positif* ssi $(x, y) \longmapsto \langle u(x) \mid y\rangle$ *est un produit scalaire, où $\langle \cdot \mid \cdot \rangle$ est la forme polaire de q.*

Proposition 9.3.5. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Alors pour tout $g \in S^{++}(E)$, il existe un unique $h \in S^{++}(E)$ t.q. $g = h^2$. De plus, h est un polynôme en g.*

Théorème 9.3.6 (Décomposition polaire)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Soit $g \in GL(E)$. Alors il existe un unique couple $(u, s) \in O(q) \times S^{++}(E)$ t.q. $g = us$. De plus, s est un polynôme en (g^*g).*

Remarque 9.3.7. *La décomposition polaire définit une bijection $O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R}) \to GL_n(\mathbb{R})$. On peut en fait montrer que cette bijection est un difféomorphisme.*

Remarque 9.3.8. *$O_n(\mathbb{R})$ est un sous-groupe compact maximal de $GL_n(\mathbb{R})$.*

Remarque 9.3.9. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Soit $f \in \mathcal{L}(E)$. Alors f admet une décomposition polaire (i.e. $\exists (u, s) \in O(q) \times S^+(E)$, $f = us$), mais elle n'est pas nécessairement unique.*

9.4 Symétries, réflexions et renversements

Définition 9.4.1 (Symétries, réflexions, renversements)**.** *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E.*

(i) *Si V est un sous-espace vectoriel de E, on a $E = V \oplus V^\perp$, et on définit la* symétrie orthogonale *s_V par rapport à $V^\perp$ comme la symétrie par rapport à $V^\perp$ parallèlement à V. On a $s_V \in O(q)$.*

(ii) *Si D est une droite vectorielle de E, on définit la* réflexion *τ_D de droite D par $\tau_D = s_D$.*

(iii) *Si P est un plan vectoriel de E, on définit le* renversement *σ_P de plan P par $\sigma_P = s_P$.*

Proposition 9.4.2. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E.*

(i) *Soit V, V' deux sous-espaces vectoriels de E de même dimension. Alors s_V et $s_{V'}$ sont conjuguées par un élément de $SO(q)$.*

(ii) *Si V est un sous-espace vectoriel de E et $u \in O(q)$, alors $us_Vu^{-1} = s_{u(V)}$.*

Proposition 9.4.3. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Alors $O(q)$ agit transitivement sur $\{x \in E,\ \|x\| = r\}$ pour tout $r \geqslant 0$.*

9.5 Générateurs des groupes orthogonaux

Théorème 9.5.1. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Alors $O(q)$ est engendré par les réflexions. Plus précisément, toute isométrie $u \in O(q)$ s'écrit comme produit d'au plus* $\operatorname{codim} \operatorname{Ker}(u - id_E)$ *réflexions.*

Lemme 9.5.2. *Soit E un $\mathbb{R}$-espace vectoriel de dimension $n \geqslant 3$ et q une forme quadratique définie positive sur E. Si D et D' sont deux droites vectorielles de E, alors il existe deux plans vectoriels P et P' t.q.*

$$\tau_D \tau_{D'} = \sigma_P \sigma_{P'}.$$

Théorème 9.5.3. *Soit E un $\mathbb{R}$-espace vectoriel de dimension n et q une forme quadratique définie positive sur E. Si $n \geqslant 3$, $SO(q)$ est engendré par les renversements. Plus précisément, toute isométrie directe $u \in SO(q)$ s'écrit comme produit d'au plus* $\operatorname{codim} \operatorname{Ker}(u - id_E)$ *renversements.*

9.6 Sous-groupes des groupes orthogonaux

Proposition 9.6.1. *Soit $n \in \mathbb{N}^*$.*

(i) $Z(O_n(\mathbb{R})) = \{-I_n, +I_n\}$.

(ii) *Si $n \geqslant 3$, $Z(SO_n(\mathbb{R})) = \{-I_n, +I_n\} \cap SO_n(\mathbb{R})$.*

(iii) *Si $n \leqslant 2$, $Z(SO_n(\mathbb{R})) = SO_n(\mathbb{R})$.*

Proposition 9.6.2. *Soit $n \in \mathbb{N}^*$.*

(i) $D(O_n(\mathbb{R})) = SO_n(\mathbb{R})$.

(ii) *Si $n \geqslant 3$, $D(SO_n(\mathbb{R})) = SO_n(\mathbb{R})$.*

(iii) *Si $n \leqslant 2$, $D(SO_n(\mathbb{R})) = \{I_n\}$.*

9.7 Groupes projectifs orthogonaux

Définition 9.7.1 (Groupes projectifs orthogonaux)**.** *Soit $n \in \mathbb{N}^*$.*

(i) *On note $PO_n(\mathbb{R}) = O_n(\mathbb{R})/Z(O_n(\mathbb{R}))$ et $PSO_n(\mathbb{R}) = SO_n(\mathbb{R})/Z(SO_n(\mathbb{R}))$.*

(ii) *Si E est un $\mathbb{R}$-espace vectoriel de dimension n et q est une forme quadratique définie positive sur E, on note $PO(q) = O(q)/Z(O(q))$ et $PSO(q) = SO(q)/Z(SO(q))$.*

On a $PO(q) \simeq PO_n(\mathbb{R})$ et $PSO(q) \simeq PSO_n(\mathbb{R})$.

Théorème 9.7.2. $PSO_4(\mathbb{R}) \simeq SO_3(\mathbb{R}) \times SO_3(\mathbb{R})$.

Notation 9.7.3. *Pour $\theta \in \mathbb{R}$, on note :*

$$R_\theta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \in SO_3(\mathbb{R}).$$

Proposition 9.7.4. *Tout élément de $SO_3(\mathbb{R})$ est conjugué dans $SO_3(\mathbb{R})$ à un R_θ, $\theta \in \mathbb{R}$.*

Corollaire 9.7.5. *$SO_3(\mathbb{R})$ est connexe par arcs.*

Proposition 9.7.6. *Pour $\theta \in \mathbb{R}$, R_θ est conjugué à $R_{-\theta}$ dans $SO_3(\mathbb{R})$.*

Démonstration. Montrer que $R_{-\theta} = S R_\theta S^{-1}$, avec $S = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. □

Proposition 9.7.7. *Soit $(A, B) \in SO_3(\mathbb{R})^2$. Alors A et B sont conjugués dans $SO_3(\mathbb{R})$* ssi $\operatorname{tr} A = \operatorname{tr} B$.

Théorème 9.7.8. *$SO_3(\mathbb{R})$ est simple.*

Démonstration. Soit N un sous-groupe distingué non trivial de $SO_3(\mathbb{R})$. On va montrer que N contient un renversement. Comme tous les renversements sont conjugués dans $SO_3(\mathbb{R})$, on en déduira que N contient tous les renversements, donc $N = SO_3(\mathbb{R})$ car les renversements engendrent $SO_3(\mathbb{R})$. Soit donc $A \in N \backslash \{I_n\}$. Si A est un renversement, on a terminé. Sinon, quitte à conjuguer, on peut supposer que $A = R_\theta$, $\theta \in \mathbb{R}$. Alors :

$$R_{2\theta} = [R_\theta, S] \in N,$$

où S est définie dans la démonstration de la proposition 9.7.6. Comme R_θ n'est pas un renversement, $R_{2\theta} \neq I_n$. Donc $\operatorname{tr} R_{2\theta} = 1 + 2\cos(2\theta) < 3$. Pour $x \in [0, \pi]$, on note $U(x) = \begin{pmatrix} \cos x & \sin x & 0 \\ -\sin x & \cos x & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Et on considère :

$$\gamma : x \in [0, \pi] \longmapsto \operatorname{tr}[R_\theta, U(x)] \in \mathbb{R}.$$

On a $\gamma(0) = \operatorname{tr} I_n = 3$, $\gamma(\pi) = \operatorname{tr}[R_\theta, S] = \operatorname{tr} R_{2\theta} = 3 - \varepsilon$, avec $\varepsilon > 0$. Comme γ est continue, $\gamma([0, \pi]) \supset [3 - \varepsilon, 3]$. En particulier, il existe $m \in \mathbb{N}^*$ et $x \in [0, \pi]$ t.q. $\gamma(x) = 1 + 2\cos\left(\frac{\pi}{m}\right)$. D'après la proposition 9.7.7, $[R_\theta, U(x)]$ est alors conjugué à $R_{\frac{\pi}{m}}$. Donc $R_{\frac{\pi}{m}} \in N$, d'où $R_\pi = \left(R_{\frac{\pi}{m}}\right)^m \in N$. Donc N contient un renversement et $N = SO_3(\mathbb{R})$. □

Théorème 9.7.9. *$PSO_n(\mathbb{R})$ est simple si $n = 3$ ou $n \geqslant 5$.*