COURS DE MASTER 1 : MODULES, ESPACES QUADRATIQUES

OLIVIER BRINON

Version du 17 novembre 2017.

Table des matières

Rappel. Si A est un anneau et $I \subsetneq A$ un idéal strict, alors il existe un idéal maximal $\mathfrak{m} \subset A$ tel que $I \subset \mathfrak{m}$ (théorème de Krull).

1. Rudiments de théorie des modules sur un anneau

1.1. Notions de module sur un anneau.

Soit A un anneau unitaire (pas commutatif *a priori*).

Définition 1.1.1. Un **A-module à gauche** est la donnée d'un triplet $(M, +, \cdot)$ où $(M, +)$ est un groupe abélien et $\cdot : A \times M \to M$ une loi de composition externe vérifiant les propriétés suivantes :

(1) $(\forall a, b \in A)\ (\forall m \in M)\ (a + b) \cdot m = a \cdot m + b \cdot m$;
(2) $(\forall a, b \in A)\ (\forall m \in M)\ (ab) \cdot m = a \cdot (b \cdot m)$;
(3) $(\forall a \in A)\ (\forall m_1, m_2 \in M)\ a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$;
(4) $(\forall m \in M)\ 1 \cdot m = m$

(cela revient à se donner un morphisme d'anneaux $A \to \mathsf{End}(M)$). Les éléments de A s'appellent les **scalaires**. Comme d'habitude, on commettera quasi systématiquement l'abus consistant à désigner un module par l'ensemble sous-jacent, en parlant du A-module M. En outre, on notera souvent am au lieu de $a \cdot m$.

Remarque 1.1.2.
(1) Bien sûr, on a une notion analogue de A-module à droite, dont on ne va pas se servir : désormais, quand on parlera de modules, il s'agira toujours de modules à gauche.
(2) On peut voir la notion de module comme une généralisation de celle d'espace vectoriel. Il faut prendre garde toutefois que bon nombre de propriétés agréables des espaces vectoriels (l'existence de bases en particulier) sont compétement fausses pour les modules sur un anneau qui n'est pas un corps.

Exemples 1.1.3. (0) L'anneau A lui-même est un A-module, la loi externe étant donnée par le produit de A.
(1) Si A est un corps, un A-module n'est autre qu'un A espace vectoriel.
(2) Un $\mathbf{Z}$-module n'est rien d'autre qu'un groupe abélien.
(3) Si K est un corps, un $K[X]$-module est un K-espace vectoriel muni d'un endomorphisme (qui correspond à la multiplication par X). On reviendra sur cette situation plus tard.
(4) Si $I \subseteq A$ est un idéal, alors I et A/I sont des A-modules.

Définition 1.1.4. Soient Λ un ensemble et $(M_\lambda)_{\lambda\in\Lambda}$ une famille de A-modules.
(1) On note $\prod_{\lambda\in\Lambda} M_\lambda$ l'ensemble produit. C'est l'ensemble des applications $f\colon \Lambda \to \bigcup_{\lambda\in\Lambda} M_\lambda$ telles que $f(\lambda) \in M_\lambda$ pour tout $\lambda \in \Lambda$. C'est un A-module, qu'on appelle le A-module **produit** des $(M_\lambda)_{\lambda\in\Lambda}$.
(2) On note $\bigoplus_{\lambda\in\Lambda} M_\lambda$ le sous-ensemble de $\prod_{\lambda\in\Lambda} M_\lambda$ constitué des fonctions $f\colon \Lambda \to \bigcup_{\lambda\in\Lambda} M_\lambda$ telles que $\{\lambda \in \Lambda,\ f(\lambda) \neq 0\}$ est *fini*. C'est un A-module, qu'on appelle la **somme** des $(M_\lambda)_{\lambda\in\Lambda}$.
(3) Si tous de M_λ sont égaux à M, on note M^Λ et $M^{(\Lambda)}$ au lieu de $\prod_{\lambda\in\Lambda} M$ et $\bigoplus_{\lambda\in\Lambda} M$.

Remarque 1.1.5. Si l'ensemble Λ est fini, les A-modules $\prod_{\lambda\in\Lambda} M_\lambda$ et $\bigoplus_{\lambda\in\Lambda} M_\lambda$ coïncident. C'est faux lorsque Λ est infini.

Si $n \in \mathbf{N}$, on note M^n au lieu de $M^{\{1,\dots,n\}}$.

Définition 1.1.6. Soit M un A-module. Un **sous-module** de M est une partie $N \subseteq M$ stable par $+$ et par multiplication par les scalaires, *i.e.* telle que

$$(\forall a \in A)\ (\forall n_1, n_2 \in N)\ n_1 + an_2 \in N.$$

Exemples 1.1.7. Les sous-modules de A ne sont autres que ses idéaux (à gauche). Si $(M_\lambda)_{\lambda\in\Lambda}$ une famille de A-modules, $\bigoplus_{\lambda\in\Lambda} M_\lambda$ est un sous-A-module de $\prod_{\lambda\in\Lambda} M_\lambda$.

Opérations sur les sous-modules d'un A-module. Soient M un A-module et $(M_\lambda)_{\lambda\in\Lambda}$ une famille de sous-A-modules de M. Alors l'intersection $\bigcap_{\lambda\in\Lambda} M_\lambda$ est un sous-module de M. Par ailleurs, on pose

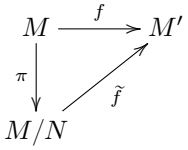
$$\sum_{\lambda\in\Lambda} M_\lambda = \Big\{ \sum_{\lambda\in\Lambda} m_\lambda \,\Big|\, (m_\lambda)_{\lambda\in\Lambda} \in \bigoplus_{\lambda\in\Lambda} M_\lambda \Big\}$$

(l'ensemble des sommes *finies* d'éléments de $\bigcup_{\lambda\in\Lambda} M_\lambda$). C'est un sous-$A$-module de M, qu'on appelle la **somme** de $(M_\lambda)_{\lambda\in\Lambda}$.

Définition 1.1.8. Soit M un A-module.
(1) Soit $X \subseteq M$. Il existe un plus petit (au sens de l'inclusion) sous-A-module N de M tel que $X \subseteq N$. On l'appelle le sous-A-module de M **engendré** par X. Ce n'est autre que l'intersection des sous-A-modules de M qui contiennent X. C'est aussi la somme $\sum_{x\in X} Ax$ (où $Ax = \{ax,\ a \in A\}$).
(2) On dit qu'une partie $X \subseteq M$ **engendre** M, ou que c'est une **partie génératrice** de M si le sous-A-module de M engendré par X est M en entier.
(3) Le A-module M est dit **type fini** s'il contient une partie génératrice finie.
(4) Le A-module M est dit **noethérien** si tous ses sous-A-modules sont de type fini.

Définition 1.1.9. • Soient M et N deux A-modules à gauche. Un **morphisme de A-modules** ou encore une **application A-linéaire** de M vers N est un morphisme de groupes $f\colon M \to N$ qui vérifie en outre $f(am) = af(m)$ pour tout $a \in A$ et $m \in M$. On note $\mathsf{Hom}_A(M, N)$ l'ensemble des applications A-linéaires de M dans N. C'est un groupe abélien, et un A-module à gauche si A est commutatif.
• Le **noyau** de f est $\mathsf{Ker}(f) = f^{-1}(0)$, c'est un sous-$A$-module de M, et l'**image** de f est $\mathsf{Im}(f) = f(M)$, c'est un sous-A-module de N. Le **conoyau** de f est $\mathsf{Coker}(f) := N/\mathsf{Im}(f)$.
• On dit que f et un **isomorphisme** si f est bijective (l'application f^{-1} est alors A-linéaire). Cela équivaut à $\mathsf{Ker}(f) = \{0\}$ (*i.e.* f injective) et $\mathsf{Im}(f) = N$ (c'est-à-dire $\mathsf{Coker}(f) = \{0\}$, *i.e.* f surjective).

Définition 1.1.10. Soient M un A-module et N un sous-A-module. On dispose du groupe quotient M/N. Il est naturellement muni d'une structure de A-module (parce que si $m \in M$ et $a \in A$, on a $a(m+N) = am + aN \subseteq am + N$). Le A-module M/N s'appelle de A-module **quotient** de M par N. L'application canonique $\pi\colon M \to M/N; m \mapsto m+N$ est A-linéaire, et jouit de la propriété universelle suivante : pour toute application A-linéaire $f\colon M \to M'$ telle que $N \subseteq \mathsf{Ker}(f)$, il existe une unique application A-linéaire $\widetilde{f}\colon M/N \to M'$ telle que $f = \widetilde{f} \circ \pi$.



En particulier, si $f\colon M \to M'$ est un morphisme de A-modules, on dispose de la **décomposition canonique** $f = \iota \circ \widetilde{f} \circ \pi$ où $\iota\colon \mathsf{Im}(f) \to M'$ est l'inclusion, $\widetilde{f}$ un isomorphisme et $\pi\colon M \to M/\mathsf{Ker}(f)$ la projection canonique.

Définition 1.1.11. (1) Un A-module **libre** est un A-module isomorphe au A-module $A^{(\Lambda)}$ pour un ensemble Λ convenable.

(2) Soit Λ un ensemble. Pour $\lambda \in \Lambda$, on définit $e_\lambda \in A^{(\Lambda)}$ par $e_\lambda(\eta) = \delta_{\lambda,\eta}$ (symbole de Kronecker, qui vaut 1 si $\lambda = \eta$ et 0 sinon). La famille $(e_\lambda)_{\lambda\in\Lambda}$ s'appelle la **base canonique** de $A^{(\Lambda)}$.

Proposition 1.1.12. (1) Si $a \in A^{(\Lambda)}$, on a l'égalité $a = \sum_{\lambda\in\Lambda} a(\lambda)e_\lambda$ (la somme est finie).

(2) Si M est un A-module, l'application A-linéaire

$$\begin{aligned}\mathsf{Hom}_A(A^{(\Lambda)}, M) &\to M^\Lambda \\ f &\mapsto (f(e_\lambda))_{\lambda\in\Lambda}\end{aligned}$$

est un isomorphisme. En d'autres termes, la donnée d'une application A-linéaire $f\colon A^{(\Lambda)} \to M$ équivaut à la donnée de la famille $(f(e_\lambda))_{\lambda\in\Lambda}$.

Démonstration. (1) Pour $\eta \in \Lambda$, on a $\Big(\sum_{\lambda\in\Lambda} a(\lambda)e_\lambda\Big)(\eta) = a(\eta)$.

(2) Cela résulte de $f(a) = \sum_{\lambda\in\Lambda} a(\lambda)f(e_\lambda)$ pour tout $f \in \mathsf{Hom}_A(A^{(\Lambda)}, M)$ et $a \in A^{(\Lambda)}$ (égalité qui s'obtient par A-linéarité).

□

Définition 1.1.13. D'après la proposition 1.1.12, un A-module M est libre si et seulement s'il existe une famille $(m_\lambda)_{\lambda\in\Lambda}$ d'éléments de M telle que tout élément $m \in M$ s'écrit de façon unique $m = \sum_{\lambda\in\Lambda} a_\lambda m_\lambda$ avec $(a_\lambda)_{\lambda\in\Lambda} \in A^{(\Lambda)}$. Un telle famille $(m_\lambda)_{\lambda\in\Lambda}$ s'appelle une **base** de M (dans le cas où A est un corps, on retrouve la définition habituelle de base).

Remarque 1.1.14. Lorsque A est un corps, tout A-module est libre (tout espace vectoriel admet une base). Ce n'est plus du tout le cas pour un anneau quelconque. Par exemple, si $I \subseteq A$ est un idéal de A distinct de $\{0\}$ et de A, le A-module A/I n'est pas libre (si $e \in A/I$ et $a \in I\backslash\{0\}$, on a $ae = 0$). Par exemple, $\mathbf{Z}/2\,\mathbf{Z}$ est un $\mathbf{Z}/4\,\mathbf{Z}$ module, mais il n'est pas libre. On peut montrer (mais ça n'est pas évident, *cf* proposition 1.4.16) que $\mathbf{Z}^{\mathbf{N}}$ n'est pas libre sur $\mathbf{Z}$.

Proposition 1.1.15. Les bases d'un module libre ont toutes même cardinal.

Démonstration. Il s'agit de montrer que si Λ et Λ' sont des ensembles tels que les A-modules $A^{(\Lambda)}$ et $A^{(\Lambda')}$ sont isomorphes, alors Λ et Λ' ont même cardinal. Soit $f\colon A^{(\Lambda)} \to A^{(\Lambda')}$ un isomorphisme, et $I \subseteq A$ un idéal maximal de A (il en existe en vertu du théorème de Krull). Comme f est A-linéaire, il induit un isomorphisme $\overline{f}\colon (A/I)^{(\Lambda)} \to (A/I)^{(\Lambda')}$. Comme I est maximal, A/I est un corps : les A/I espaces vectoriels $(A/I)^{(\Lambda)}$ et $(A/I)^{(\Lambda')}$ sont isomorphes, on a donc $\mathsf{Card}(\Lambda) = \mathsf{Card}(\Lambda')$. □

Définition 1.1.16. D'après la proposition précédente, si M est isomorphe à A^n avec $n \in \mathbf{N}$, l'entier n est un invariant de M, qu'on appelle le **rang** de M.

Remarque 1.1.17. (1) Si M et N sont deux A-modules libres de rangs respectifs m et n, il résulte de la proposition 1.1.12 (2), après le choix de bases dans M et dans N, que

$$\mathsf{Hom}_A(M,N) \simeq \mathsf{Hom}_A(A^m,A^n) = \mathsf{M}_{n\times m}(A).$$

Comme pour les espaces vectoriels de dimension finie, après le choix de bases, la donnée d'une application A-linéaire entre deux A-modules libres de rang fini équivaut à celle de sa matrice dans ces bases.

(2) Soient M un A-module et $\{m_\lambda\}_{\lambda\in\Lambda}$ une famille d'éléments de M. D'après la proposition 1.1.12 (2), il existe une unique application A-linéaire $f\colon A^{(\Lambda)} \to M$ telle que $f(e_\lambda) = m_\lambda$ pour tout $\lambda \in \Lambda$.

Le A-module $\mathsf{Im}(f)$ est le sous-module de M engendré par $\{m_\lambda\}_{\lambda\in\Lambda}$. En particulier, la famille $\{m_\lambda\}_{\lambda\in\Lambda}$ est génératrice si f est surjective, et c'est une base si f est un isomorphisme. Lorsque f est injective, on dit que $\{m_\lambda\}_{\lambda\in\Lambda}$ est **libre**.

Proposition 1.1.18. (1) Soit M un A-module. Alors M est noethérien si et seulement si toute suite croissante de sous-A-modules de M est stationnaire.

(2) Soient M un A-module et N un sous-A-module de M. Alors M est noethérien si et seulement si les A-modules N et M/N sont noethériens.

Démonstration. (1) Supposons M noethérien, et soit $(M_n)_{\in\mathbf{N}}$ une suite croissante de sous-A-modules de M. Comme le sous-A-module $\sum\limits_{n\in\mathbf{N}} M_n$ est de type fini, il est engendré par $\{m_1,\dots,m_r\}$. Comme la réunion est croissante, il existe $N \in \mathbf{N}$ tel que $\{m_1,\dots,m_r\} \subseteq M_N$. On a alors $M_N \subseteq \sum\limits_{n\in\mathbf{N}} M_n \subseteq M_N$ et donc $\sum\limits_{n\in\mathbf{N}} M_n = M_N$, et $M_n = M_n$ pour tout $n \geqslant N$: la suite $(M_n)_{\in\mathbf{N}}$ est stationnaire.

Supposons M non noethérien : il existe un sous-A-module M' qui n'est pas de type fini. On construit par récurrence une suite *strictement* croissante de sous-A-modules de type fini de M' de la façon suivante : on pose $M'_0 = \{0\}$, et si M'_n est construit, il est distinct de M' (puisque M'_n est de type fini et M' ne l'est pas) : soient $m_n \in M'\backslash M'_n$ et $M'_{n+1} = M'_n + Am_{n+1}$. On a $M'_n \subsetneq M'_{n+1} \subset M'$.

(2) Si M est noethérien, alors N est de type fini. Par ailleurs, si N' est un sous-A-module de M/N, on a $N' = \widetilde{N}/N$ avec $\widetilde{N} = \pi^{-1}(N')$ (où $\pi\colon M \to M/N$ est la projection canonique). Comme M est noethérien, $\widetilde{N}$ est de type fini, c'est *a fortiori* de cas de $N' = \widetilde{N}/N$, et M/N est noethérien.

Supposons N et M/N noethériens. Soit $(M_n)_{n\in\mathbf{N}}$ une suite croissante de sous-A-modules de M. On dispose des suites croissantes $(M_n \cap N)_{n\in\mathbf{N}}$ et $((N+M_n)/N)_{n\in\mathbf{N}}$ de sous-A-modules de N et de M/N respectivement. Comme ces derniers sont noethériens, ces suites sont stationnaires : il existe $n_0 \in \mathbf{N}$ tel que pour $n \geqslant n_0$, on a $M_n \cap N = M_{n_0} \cap N$ et $(N+M_n)/N = (N+M_{n_0})/N$ *i.e.* $N + M_n = N + M_{n_0}$. Si $m \in M_n$, il existe donc $x \in N$ et $y \in M_{n_0} \subseteq M_n$ tels que $m = x + y$. Comme $x = y - m \in N \cap M_n = N \cap M_{n_0}$, on a $m \in M_{n_0}$, d'où $M_n \subseteq M_{n_0}$ *i.e.* $M_n = M_{n_0}$. Le A-module M est donc noethérien.

□

Corollaire 1.1.19. Si M_1 et M_2 sont deux A-modules noethériens, le A-module produit $M_1 \times M_2$ est noethérien.

Démonstration. Les modules $M_1 \simeq M_1 \times \{0\}$ et $M_2 \simeq (M_1 \times M_2)/(M_1 \times \{0\})$, étant noethériens, cela résulte de la proposition 1.1.18 (2). □

Définition 1.1.20. L'anneau A est dit **noethérien** s'il est noethérien vu comme A-module. Par définition, cela signifie que tout idéal de A est de type fini. En vertu de la proposition 1.1.18, cela équivaut au fait que toute suite croissante d'idéaux de A est stationnaire.

Proposition 1.1.21. Si A est noethérien, tout A-module de type fini est noethérien.

Démonstration. Soit M un A-module de type fini. Alors il existe $n \in \mathbf{N}$ et une application A-linéaire surjective $f\colon A^n \to M$. Comme A est noethérien, il en est de même de A^n (corollaire 1.1.19), et donc de $M = A^n/\mathsf{Ker}(f)$ (proposition 1.1.18 (2)). □

Théorème 1.1.22. (Hilbert) Si A est un anneau noethérien, alors $A[X]$ est noethérien.

Démonstration. Soit $I \subseteq A[X]$ un idéal. Pour $n \in \mathbf{N}$, notons J_n l'ensemble des coefficients dominants des éléments de I qui sont de degré n. Comme I est un idéal de $A[X]$, l'ensemble J_n est un idéal de A. En outre, si $n \leqslant m$ et $a \in J_n$ (de sorte qu'il existe $P \in I$ de degré n de coefficient dominant égal à a), alors $a \in J_m$ (car a est le coefficient dominant du polynôme $X^{m-n}P$). La suite d'idéaux $(J_n)_{n\in\mathbf{N}}$ est donc croissante.

Comme A est noethérien, cette suite est stationnaire : soit $d \in \mathbf{N}$ tel que $n \geqslant d \Rightarrow J_n = J_d$. Comme A est noethérien, l'idéal J_d est de type fini : choisissons $\alpha_1, \dots, \alpha_r$ des générateurs de J_d, ce sont les coefficients dominants de $P_1, \dots, P_r \in J_d$ respectivement. Par ailleurs, si $A[X]_{<d}$ désigne le sous-A-module de $A[X]$ constitué du polynôme nul et des polynômes de degré $< d$, posons $M = I \cap A[X]_{<d}$. Comme $A[X]_{<d}$ est un A module de type fini, il est noethérien (*cf* proposition 1.1.21), de sorte que M est de type fini : soient $Q_1, \dots, Q_s$ des générateurs de M. On a bien sûr

$$\alpha_1 A[X] + \cdots + \alpha_r A[X] + Q_1 A[X] + \cdots + Q_s A[X] \subseteq I$$

Montrons l'inclusion réciproque. Si $P \in I$ est de degré $n \geqslant d$, son coefficient dominant a appartient à J_d, de sorte qu'il existe $a_1, \dots, a_r \in A$ tels que $a = a_a\alpha_1 + \cdots + a_r\alpha_r$. Le polynôme $P - \sum_{i=1}^{r} a_i X^{n-d} P_i \in I$ est de degré $< n$: quitte à soustraire à P un élément de $\alpha_1 A[X] + \cdots + \alpha_r A[X]$, on peut supposer que $\deg(P) < d$. Mais alors $P \in M = I \cap A[X]_{<d}$, et $P \in Q_1 A[X] + \cdots + Q_s A[X]$, ce qui prouve que $P \in \alpha_1 A[X] + \cdots + \alpha_r A[X] + Q_1 A[X] + \cdots + Q_s A[X]$. Ainsi, l'idéal I est de type fini, et $A[X]$ est noethérien. □

Corollaire 1.1.23. Soient A un anneau noethérien et B une A-algèbre de type fini. Alors B est un anneau noethérien.

Démonstration. Comme B est de type fini, il existe $b_1, \dots, b_r \in B$ tels que $B = A[b_1, \dots, b_r]$, si bien qu'on dispose du morphisme de A-algèbres $f\colon A[X_1, \dots, X_r] \to B$ défini par $f(X_i) = b_i$ pour $i \in \{1, \dots, r\}$. Il est surjectif : si $I = \mathsf{Ker}(f)$, on a $B \simeq A[X_1, \dots, X_r]/I$. Comme A est noethérien, il en est de même de $A[X_1, \dots, X_r]$ (en appliquant r fois le théorème 1.1.22), de sorte que B est une $A[X_1, \dots, X_r]$-algèbre noethérienne : c'est donc un anneau noethérien. □

Définition 1.1.24. Soient M un A-module et $m \in M$. On pose $\mathsf{ann}_A(m) = \{a \in A,\ am = 0\}$. C'est un idéal (à gauche) de A, appelé **idéal annulateur** de m. On dit que m est de **torsion** si $\mathsf{ann}_A(m) \neq \{0\}$, *i.e.* s'il existe $a \in A\backslash\{0\}$ tel que $am = 0$. On note M_{tors} l'ensemble des éléments de M qui sont de torsion. On dit que M est **sans torsion** (resp. *de torsion*) si $M_{\mathsf{tors}} = \{0\}$ (resp. $M_{\mathsf{tors}} = M$).
On pose $\mathsf{ann}_A(M) = \{a \in A \,|\, (\forall m \in M)\ am = 0\} = \bigcap_{m \in M} \mathsf{ann}_A(m)$. C'est un idéal de A, appelé **idéal annulateur** de M. Si A est commutatif, on en déduit une structure de $A/\mathsf{ann}_A(M)$-module sur M. Remarquons que M peut-être de torsion même si $\mathsf{ann}_A(M) = \{0\}$: pa exemple, on a $\mathsf{ann}_{\mathbf{Z}}(\mathbf{Q}/\mathbf{Z}) = \{0\}$.

Exemple 1.1.25. Si $I \subseteq A$ est un idéal non nul, A/I est de torsion. Par exemple, $\mathbf{Z}/2\mathbf{Z}$ est un $\mathbf{Z}/6\mathbf{Z}$ de torsion. De même, $\mathbf{Q}/\mathbf{Z}$ est un $\mathbf{Z}$-module de torsion.

Proposition 1.1.26. Supposons A commutatif, intègre et soit M un A-module. Alors M_{tors} est un sous-A-module de M et le A-module quotient M/M_{tors} est sans torsion.

Démonstration. Si $m_1, m_2 \in M_{\mathsf{tors}}$ et $\alpha \in A$, il existe $a_1, a_2 \in A\backslash\{0\}$ tels que $a_1 m_1 = 0$ et $a_2 m_2 = 0$. Comme A est intègre, on a $a_1 a_2 \neq 0$ et $a_1 a_2(m_1 + \alpha m_2) = 0$ implique $m_1 + \alpha m_2 \in M_{\mathsf{tors}}$.

Soit $m \in M$ dont l'image $m + M_{\mathsf{tors}}$ est de torsion dans M/M_{tors} : il existe $a \in A\backslash\{0\}$ tel que $am + M_{\mathsf{tors}} = M_{\mathsf{tors}}$ *i.e.* $am \in M_{\mathsf{tors}}$. Il existe donc $b \in A\backslash\{0\}$ tel que $b(am) = 0$. Comme A est intègre, on a $ab \neq 0$, et $m \in M_{\mathsf{tors}}$. □

Remarque 1.1.27. (1) Ce qui précède tombe en défaut si A n'est pas supposé intègre. Par exemple, si $A = M = \mathbf{Z} \times \mathbf{Z}$, alors $M_{\mathsf{tors}} = (\mathbf{Z} \times \{0\}) \cup (\{0\} \times \mathbf{Z})$ n'est pas un sous-module de M.
(2) Un A-module libre est sans torsion, mais la réciproque est fausse en général (elle est valide dans le cas des modules de type fini sur un anneau principal, *cf* corollaire 1.4.13).

1.2. Le produit tensoriel.

1.2.1. *Cas d'un anneau de base commutatif.* Dans cette partie, on suppose A commutatif. Soient M et N deux A-modules.

Définition 1.2.2. Soit L un A-module. Une application $f\colon M \times N \to L$ est dite **bilinéaire** si elle vérifie les conditions suivantes :
(i) f est linéaire à gauche, *i.e.* $(\forall a \in A)\,(\forall m_1, m_2 \in M)\,(\forall n \in N)\, f(am_1 + m_2, n) = af(m_1, n) + f(m_2, n)$;
(ii) f est linéaire à droite, *i.e.* $(\forall a \in A)\,(\forall m \in M)\,(\forall n_1, n_2 \in N)\, f(m, an_1 + n_2) = af(m, n_1) + f(m, n_2)$.
L'ensemble $\mathsf{Bil}_A(M, N, L)$ des applications bilinéaires $M \times N \to L$ est un A-module.

Proposition 1.2.3. Il existe un couple $(M\otimes_A N, \varphi)$ où $M\otimes_A N$ est un A-module et $\varphi\colon M\times N\to M\otimes_A N$ une application bilinéaire, ayant la propriété universelle suivante : si $f\colon M\times N\to L$ est une application bilinéaire, il existe une unique application A-linéaire $\widetilde{f}\colon M\otimes_A N\to L$ telle que $f=\widetilde{f}\circ\varphi$.

$$\begin{array}{ccc} M\times N & \xrightarrow{\quad f\quad} & L \\ & {\scriptstyle\varphi}\searrow \quad \nearrow{\scriptstyle\widetilde{f}} & \\ & M\otimes_A N & \end{array}$$

Remarque 1.2.4. La propriété universelle du couple $(M\otimes_A N,\varphi)$ implique qu'il est unique à unique isomorphisme près.

Démonstration. Considérons le A-module $A^{(M\times N)}$ des fonctions $M\times N\to A$ à support fini. On dispose de la base canonique $\big(e_{(m,n)}\big)_{(m,n)\in M\times N}$. Notons K le sous-module de $A^{(M\times N)}$ engendré par les éléments suivants :

- $e_{(m_1+m_2,n)}-e_{(m_1,n)}-e_{(m_2,n)}$ pour $m_1,m_2\in M$ et $n\in N$;
- $e_{(m,n_1+n_2)}-e_{(m,n_1)}-e_{(m,n_2)}$ pour $m\in M$ et $n_1,n_2\in N$;
- $e_{(am,n)}-ae_{(m,n)}$ et $e_{(m,an)}-ae_{(m,n)}$ pour $a\in A$, $m\in M$ et $n\in N$.

Posons $M\otimes_A N=A^{(M\times N)}/K$. C'est un A-module. Soient $i\colon M\times N\to A^{(M\times N)};(m,n)\mapsto e_{(m,n)}$ et $\pi\colon A^{(M\times N)}\to M\otimes_A N$ la surjection canonique. On pose $\varphi=\pi\circ i$: par définition de K, l'application φ est bilinéaire. Si maintenant $f\colon M\times N\to L$ est bilinéaire, on définit l'application A-linéaire $\widehat{f}\colon A^{(M\times N)}\to L$ en posant $\widehat{f}(e_{(m,n)})=f(m,n)$ pour tout $m\in M$ et $n\in N$. Comme f est bilinéaire, on a $K\subset\mathsf{Ker}(\widehat{f})$: l'application $\widehat{f}$ se factorise par une application $\widetilde{f}\colon M\otimes_A N\to L$, de sorte que $f=\widetilde{f}\circ\varphi$ (on a $\widetilde{f}(\pi(e_{(m,n)}))=f(m,n)$ pour tout $m\in M$ et $n\in N$).

$$\begin{array}{ccccc} M\times N & & \xrightarrow{\quad f\quad} & & \\ & {\scriptstyle\varphi}\searrow & & & \\ {\scriptstyle i}\downarrow & & M\otimes_A N & \xrightarrow{\ \widetilde{f}\ } & L \\ & {\scriptstyle\pi}\nearrow & & & \\ A^{(M\times N)} & & \xrightarrow[\quad\widehat{f}\quad]{} & & \end{array}$$

□

Remarque 1.2.5. (1) Une reformulation de la propriété universelle du produit tensoriel est

$$\mathsf{Bil}(M,N,L)\simeq\mathsf{Hom}_A(M,\mathsf{Hom}_A(N,L))\simeq\mathsf{Hom}_A(M\otimes_A N,L)$$

(2) Si M est un A-module et B une A-algèbre (*i.e.* on a un morphisme d'anneaux $A\to B$, qui fait de B un A-module), alors $B\otimes_A M$ est muni d'une structure de B-module (changement de base).

Notation. Avec les notations de la preuve de la proposition 1.2.3, on pose $m\otimes n=\pi(e_{(m,n)})\in M\otimes_A N$ pour tout $m\in M$ et $n\in N$. Les éléments de $M\otimes_A N$ de cette forme s'appellent les **tenseurs simples**. Ils engendrent $M\otimes_A N$, mais en général, les éléments de $M\otimes_A N$ ne sont pas tous des tenseurs simples.

Proposition 1.2.6. Si M et N sont libres, de bases $(e_\lambda)_{\lambda\in\Lambda}$ et $(f_\delta)_{\delta\in\Delta}$ respectivement, alors $M\otimes_A N$ est libre, de base $(e_\lambda\otimes f_\delta)_{(\lambda,\delta)\in\Lambda\times\Delta}$.

Démonstration. Si L est un A-module, on a

$$\begin{aligned}\mathsf{Bil}(M,N,L)&\simeq\mathsf{Hom}_A(M,\mathsf{Hom}_A(N,L))\\&\simeq\mathsf{Hom}_A(A^{(\Lambda)},\mathsf{Hom}_A(A^{(\Delta)},L))\\&\simeq\mathsf{Hom}_A(A^{(\Lambda)},L^\Delta)\\&\simeq L^{\Lambda\times\Delta}\\&\simeq\mathsf{Hom}_A(A^{(\Lambda\times\Delta)},L)\end{aligned}$$

(*cf* proposition 1.1.12 (2)), ce qui prouve que $A^{(\Lambda\times\Delta)}$ a la propriété universelle de $M\otimes_A N$: ils sont isomorphes, la base canonique de $A^{(\Lambda\times\Delta)}$ correspondant à $(e_\lambda\otimes f_\delta)_{(\lambda,\delta)\in\Lambda\times\Delta}$. □

Fonctorialité du produit tensoriel. Soient $f\colon M\to M'$ et $g\colon N\to N'$ deux applications A-linéaires. Elles induisent l'application $M\times N\to M'\otimes_A N';(m,n)\mapsto f(m)\otimes g(n)$. Cette dernière est bilinéaire : elle se factorise de façon unique par une application A-linéaire

$$f\otimes g\colon M\otimes_A N\to M'\otimes_A N'$$

En particulier, si $f\colon M \to M'$ est A-linéaire et N un A-module, on a une application $M \otimes_A N \xrightarrow{f\otimes 1} M' \otimes_A N$. Un cas particulier important est le changement de base : si B est une A-algèbre, f induit une application B-linéaire $B \otimes_A M \to B \otimes_A M'$.

Remarque 1.2.7. Bien entendu, si $f\colon M \to M'$ est un isomorphisme, alors $M \otimes_A N \xrightarrow{f\otimes 1} M' \otimes_A N$ est un isomorphisme. Par contre, si f est seulement supposé injectif, alors $M \otimes_A N \xrightarrow{f\otimes 1} M' \otimes_A N$ n'est pas injectif en général (trouver des exemples). Par contre, la surjectivité est conservée, mieux, on a $\mathsf{Coker}(f\otimes 1) \simeq \mathsf{Coker}(f) \otimes_A N$ (exercice).

Exercice 1.2.8. (1) Montrer que $M \otimes_A N \simeq N \otimes_A M$.
(2) Montrer que $(\mathbf{Z}/a\,\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/b\,\mathbf{Z}) \simeq \mathbf{Z}/\,\mathsf{pgcd}(a,b)\,\mathbf{Z}$.
(3) Montrer que $\mathbf{C} \otimes_{\mathbf{C}} \mathbf{C} \to \mathbf{C}$; $z_1 \otimes z_2 \mapsto z_1 z_2$ et $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \to \mathbf{C}^2$; $z_1 \otimes z_2 \mapsto (z_1 z_2, z_1 \overline{z}_2)$ sont des isomorphismes.
(4) Soient K un corps et V un K-espace vectoriel, $V^\vee = \mathsf{Hom}_K(V,K)$ son dual. Alors l'application $V \otimes_K V^\vee \to \mathsf{End}_K(V)$ qui à $v \otimes \alpha$ (avec $v \in V$ et $\alpha \in V^\vee$) associe l'endomorphisme (de rang 1) donné par $x \mapsto \alpha(x)v$ est un isomorphisme. De plus, l'application $V \otimes_K V^\vee \to K$; $v \otimes \alpha \mapsto \alpha(v)$ correspond, *via* cet isomorphisme, à la trace $\mathsf{Tr}\colon \mathsf{End}_K(V) \to K$.

1.2.9. *Cas général.* Dans ce numéro, on ne suppose pas A commutatif *a priori*. Soient M un A-module à droite et N un A-module à gauche.

Définition 1.2.10. Soit L un groupe abélien. On dira qu'une application $f\colon M \times N \to L$ est *A-linéaire au centre* lorsque $(\forall a \in A)\,(\forall m \in M)\,(\forall n \in N)\, f(ma,n) = f(m,an)$. On note $\mathsf{Bil}^A_{\mathbf{Z}}(M,N,L)$ l'ensemble des applications $\mathbf{Z}$-bilinéaires $M \times N \to L$ qui sont A-linéaires au centre. C'est un groupe abélien.

Remarque 1.2.11. Le groupe $\mathsf{Hom}_{\mathbf{Z}}(N,L)$ est naturellement muni d'une structure de A-module à droite : si $a \in A$, $\varphi \in \mathsf{Hom}_{\mathbf{Z}}(N,L)$ et $n \in N$, on a $(\varphi a)(n) = \varphi(an)$. On a alors l'isomorphisme naturel

$$\mathsf{Bil}^A_{\mathbf{Z}}(M,N,L) \xrightarrow{\sim} \mathsf{Hom}_A(M, \mathsf{Hom}_{\mathbf{Z}}(N,L))$$

Proposition 1.2.12. Il existe un couple $(M \otimes_A N, \varphi)$ où $M \otimes_A N$ est un groupe abélien et $\varphi\colon M \times N \to M \otimes_A N$ une application $\mathbf{Z}$-bilinéaire et A-linéaire au centre, ayant la propriété universelle suivante : si $f\colon M \times N \to L$ est une application $\mathbf{Z}$-bilinéaire et A-linéaire au centre, il existe un unique morphisme de groupes abéliens $\widetilde{f}\colon M \otimes_A N \to L$ tel que $f = \widetilde{f} \circ \varphi$.

Remarque 1.2.13. Là encore, la propriété universelle du couple $(M \otimes_A N, \varphi)$ implique qu'il est unique à unique isomorphisme près.

La preuve est essentiellement identique à celle de la proposition 1.2.3 : on considère le $\mathbf{Z}$-module $\mathbf{Z}^{(M\times N)}$, sa base canonique $\big(e_{(m,n)}\big)_{(m,n)\in M\times N}$ et K le sous-groupe engendré par les éléments suivants :

- $e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)}$ pour $m_1, m_2 \in M$ et $n \in N$;
- $e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)}$ pour $m \in M$ et $n_1, n_2 \in N$;
- $e_{(ma,n)} - e_{(m,an)}$ pour $a \in A$, $m \in M$ et $n \in N$.

Le groupe quotient $M \otimes_A N = \mathbf{Z}^{(M\times N)}/K$ muni de l'application naturelle φ a la propriété universelle requise.

Remarque 1.2.14. (1) Soit B un anneau. Supposons M muni d'une structure de B-module à gauche. Alors la groupe abélien $M \otimes_A N$ est muni d'une structure de B-module à gauche, donnée sur les tenseurs simples par $b(m \otimes n) = (bm) \otimes n$ pour $b \in B$, $m \in M$ et $n \in N$.
(2) Supposons A commutatif. Munissons M de la structure de A-module à gauche donnée par $am = ma$ pour tout $a \in A$ et $m \in M$. Il en résulte que $M \otimes_A N$ est muni d'une structure de A-module, qui n'est autre que le produit tensoriel défini au numéro précédent dans le cas commutatif. C'est bien normal : l'application φ est alors A-bilinéaire, et si L est un A-module, $f \in \mathsf{Bil}_A(M,N,L) \subset \mathsf{Bil}^A_{\mathbf{Z}}(M,N,L)$, le morphisme de groupes $\widetilde{f}\colon M \otimes_A N \to L$ tel que $f = \widetilde{f} \circ \varphi$ est A-linéaire par unicité (si $a \in A$, les applications $x \mapsto a\widetilde{f}(x)$ et $x \mapsto \widetilde{f}(ax)$ factorisent toutes les deux af).
(3) Comme dans le cas commutatif, si $f\colon M_1 \to M_2$ (resp. $g\colon N_1 \to N_2$) est une application A-linéaire entre deux A-modules à droite (resp. à gauche), on dispose du morphisme de groupes $f \otimes g\colon M_1 \otimes_A N_1 \to M_2 \otimes_A N_2$.
(4) Mise en garde : si M et N sont des A-modules à droite et à gauche, mais que les structures à droite et à gauche ne sont pas compatibles, on n'a pas d'isomorphisme $M \otimes_A N \simeq N \otimes_A M$ (même dans le cas où A est commutatif).

1.3. **Puissances symétriques et extérieures.** Soient K un corps et V un K-espace vectoriel.

Définition 1.3.1. Soient W un K-espace vectoriel, $n \in \mathbf{N}_{>0}$ et $f\colon V^n \to W$ une application n-linéaire (*i.e.* linéaire par rapport à chacune des variables). On dit que f est **symétrique** (resp. **alternée**) si $f(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = f(v_1, \dots, v_n)$ pour tous $v_1, \dots, v_n \in V$ et $\sigma \in \mathfrak{S}_n$ (resp. $f(v_1, \dots, v_n) = 0$ dès qu'il existe $1 \leqslant i < j \leqslant n$ tels que $v_i = v_j$).

Remarque 1.3.2. Si $f\colon V^n \to W$ est une application n-linéaire alternée, alors f est antisymétrique, *i.e.* $f(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = \varepsilon(\sigma) f(v_1, \dots, v_n)$ pour tous $v_1, \dots, v_n \in V$ et $\sigma \in \mathfrak{S}_n$ (cela se vérifie sur les transpositions, auquel cas cela résulte de la polarisation). Lorsque $\mathsf{car}(K) \neq 2$, une application antisymétrique est alternée (c'est faux en général quand $\mathsf{car}(K) = 2$).

Théorème 1.3.3. Il existe un couple $(\mathsf{Sym}^n(V), s)$ (resp. $(\mathsf{Alt}^n(V), a)$) ayant la propriété universelle suivante : si $f\colon V^n \to W$ est une application n-linéaire symétrique (resp. alternée), alors il existe une unique application linéaire $\widetilde{f}\colon \mathsf{Sym}^n(V) \to W$ (resp. $\widetilde{f}\colon \mathsf{Alt}^n(V) \to W$) telle que $f = \widetilde{f} \circ s$ (resp. $f = \widetilde{f} \circ a$), *i.e.* telle que le diagramme

$$\begin{array}{ccc} V^n & \xrightarrow{\quad f \quad} & W \\ & {\scriptstyle s}\searrow \quad \nearrow{\scriptstyle \widetilde{f}} & \\ & \mathsf{Sym}^n(V) & \end{array} \qquad \left(\text{resp. } \begin{array}{ccc} V^n & \xrightarrow{\quad f \quad} & W \\ & {\scriptstyle a}\searrow \quad \nearrow{\scriptstyle \widetilde{f}} & \\ & \mathsf{Alt}^n(V) & \end{array}\right)$$

soit commutatif.

Démonstration. Soit S_n (resp. A_n) le sous-K-espace vectoriel de $V^{\otimes n} := \underbrace{V \otimes \cdots \otimes V}_{n \text{ fois}}$ engendré par les éléments $v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$ pour tous $v_1, \dots, v_n \in V$ et $\sigma \in \mathfrak{S}_n$ (resp. par les éléments $v_1 \otimes \cdots \otimes v_n$ pour tous $v_1, \dots, v_n \in V$ tels qu'il existe $1 \leqslant i < j \leqslant n$ avec $v_i = v_j$). D'après la propriété universelle du produit tensoriel, il existe une unique application K-linéaire $\breve{f}\colon V^{\otimes n} \to W$ telle que $f = \breve{f} \circ \pi$ (où $\pi\colon V^n \to V^{\otimes n}$ est l'application naturelle). Par définition, f est symétrique (resp. alternée) si et seulement si $S_n \subset \mathsf{Ker}(\breve{f})$ (resp. $A_n \subset \mathsf{Ker}(\breve{f})$). L'application $\breve{f}$ se factorise alors en une application K-linéaire $\widetilde{f}\colon V^{\otimes n}/S_n \to W$ (resp. $\widetilde{f}\colon V^{\otimes n}/A_n \to W$). Cela montre que $\mathsf{Sym}^n(V) := V^{\otimes n}/S_n$, muni du composé $s\colon V^n \to V^{\otimes n} \to V^{\otimes n}/S_n$ (resp. $\mathsf{Alt}^n(V) := V^{\otimes n}/A_n$, muni du composé $a\colon V^n \to V^{\otimes n} \to V^{\otimes n}/A_n$) a la propriété universelle requise. □

Définition 1.3.4. $\mathsf{Sym}^n(V)$ (resp. $\mathsf{Alt}^n(V)$) s'appelle la **puissance symétrique** (resp. **puissance exterieure**) n-ième de V.

Notation. Très souvent, on note $\bigwedge^n V$ au lieu de $\mathsf{Alt}^n(V)$. Par ailleurs, on écrit $v_1 \cdot v_2 \cdots v_n$ au lieu de $s(v_1, \dots, v_n)$ et $v_1 \wedge \cdots \wedge v_n$ au lieu de $a(v_1, \dots, v_n)$. On pose $\mathsf{Sym}^0(V) = \mathsf{Alt}^0(V) = K$.

Lemme 1.3.5. Supposons V de dimension finie et choisissons une base $\mathfrak{B} = (e_1, \dots, e_d)$ de V sur K. Alors $(e_{i_1} \cdot e_{i_2} \cdots e_{i_n})_{1 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_n \leqslant d}$ (resp. $(e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n})_{1 \leqslant i_1 < i_2 < \cdots < i_n \leqslant d}$) est une base de $\mathsf{Sym}^n(V)$ (resp. $\mathsf{Alt}^n(V)$).

Corollaire 1.3.6. On a $\dim_K(\mathsf{Sym}^n(V)) = \binom{n+d-1}{n}$ et $\dim_K(\mathsf{Alt}^n(V)) = \binom{d}{n}$.

Remarque 1.3.7. Le choix d'une base de V sur K fournit un isomorphisme $\mathsf{Sym}^n(V) \xrightarrow{\sim} K_n[X_1, \dots, X_d]$ où $K_n[X_1, \dots, X_d]$ désigne l'espace des polynômes homogènes de degré n dans $K[X_1, \dots, X_d]$.

Soient V_1 et V_2 deux K-espaces vectoriels de dimension finie. Si $i \in \{0, \dots, n\}$ et $v_1^{(1)}, \dots, v_i^{(1)} \in V_1$, $v_{i+1}^{(2)}, \dots, v_n^{(2)} \in V_2$, alors $v_1^{(1)} \cdots v_i^{(1)} \cdot v_{i+1}^{(2)} \cdots v_n^{(2)} \in \mathsf{Sym}^n(V_1 \oplus V_2)$ et $v_1^{(1)} \wedge \cdots \wedge v_i^{(1)} \wedge v_{i+1}^{(2)} \wedge \cdots \wedge v_n^{(2)} \in \mathsf{Alt}^n(V_1 \oplus V_2)$. D'après la propriété universelle des puissances symétriques et exterieures, on en déduit des applications K-linéaires $\mathsf{Sym}^i(V_1) \otimes \mathsf{Sym}^{n-i}(V_2) \to \mathsf{Sym}^n(V_1 \oplus V_2)$ et $\mathsf{Alt}^i(V_1) \otimes \mathsf{Alt}^{n-i}(V_2) \to \mathsf{Alt}^n(V_1 \oplus V_2)$.

Corollaire 1.3.8. Les application qui précèdent induisent des isomorphismes

$$\bigoplus_{i=0}^{n} \mathsf{Sym}^i(V_1) \otimes \mathsf{Sym}^{n-i}(V_2) \xrightarrow{\sim} \mathsf{Sym}^n(V_1 \oplus V_2)$$

$$\bigoplus_{i=0}^{n} \mathsf{Alt}^i(V_1) \otimes \mathsf{Alt}^{n-i}(V_2) \xrightarrow{\sim} \mathsf{Alt}^n(V_1 \oplus V_2)$$

Remarque 1.3.9. On peut démontrer le corollaire en utilisant la propriété universelle des puissances symétriques et exterieures, puis en déduire le lemme 1.3.5 par récurrence sur d.

Supposons désormais $\mathsf{car}(K) > n$. Si $v_1, \dots, v_n \in V^n$, posons $f_s(v_1, \dots, v_n) = \sum_{\sigma \in \mathfrak{S}_n} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$. Cela définit une application $f_s \colon V^n \to V^{\otimes n}$ qui est n-linéaire et symétrique : elle se factorise donc de façcon unique en une application $\iota_s \colon \mathsf{Sym}^n(V) \to V^{\otimes n}$ (il s'agit d'un opérateur de symétrisation). De même, posons $f_a(v_1, \dots, v_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$. Cela définit une application $f_a \colon V^n \to V^{\otimes n}$ qui est n-linéaire et antisymétrique (donc alternée vu l'hypothèse) : elle se factorise donc de façcon unique en une application $\iota_a \colon \mathsf{Alt}^n(V) \to V^{\otimes n}$ (il s'agit d'un opérateur d'antisymétrisation).
On munit $V^{\otimes n}$ de l'action de $\mathfrak{S}_n$ donnée par $\sigma(v_1 \otimes \cdots \otimes v_n) = v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$. Alors $\frac{1}{n!} \iota \circ \pi_s$ (où $\pi_s \colon V^{\otimes n} \to \mathsf{Sym}^n(V)$ est la projection canonique) n'est autre que le projecteur sur le sous-espace $\left(V^{\otimes n}\right)^{\mathfrak{S}_n}$ des invariants sous l'action de $\mathfrak{S}_n$, parallèlement au sous-espace des anti-invariants, *i.e.* des éléments $x \in V^{\otimes n}$ tels que $\sigma(x) = \varepsilon(\sigma) x$ pour tout $\sigma \in \mathfrak{S}_n$. De plus, $\frac{1}{n!} \iota \circ \pi_a$ (où $\pi_a \colon V^{\otimes n} \to \mathsf{Alt}^n(V)$ est la projection canonique) est le projecteur orthogonal.

Remarque 1.3.10. Dans le cas $n = 2$, le projecteurs qui précèdent fournissent une décomposition $V^{\otimes 2}(V) = \mathsf{Sym}^2(V) \oplus \mathsf{Alt}^2(V)$. En effet, avec les notations de la preuve du théorème 1.3.3, ils fournissent des identifications $\mathsf{Sym}^2(V) = A_2$ et $\mathsf{Alt}^2(V) = S_2$ et $S_2 \oplus A_2 = V^{\otimes 2}$.

Définition 1.3.11. L'**algèbre tensorielle** (resp. **symétrique**, resp. **extérieure**) de V est

$$\mathsf{T}^\bullet(V) := \bigoplus_{n=0}^{\infty} V^{\otimes n} \quad (\text{resp. } \mathsf{Sym}^\bullet(V) := \bigoplus_{n=0}^{\infty} \mathsf{Sym}^n(V) \quad \text{resp. } \mathsf{Alt}^\bullet(V) := \bigoplus_{n=0}^{\infty} \mathsf{Alt}^n(V))$$

munis du produit induit par l'isomorphisme $V^{\otimes n} \otimes V^{\otimes m} \xrightarrow{\sim} V^{\otimes (n+m)}$.

Proposition 1.3.12. $\mathsf{Sym}^\bullet(V)$ est le quotient de l'algèbre $\mathsf{T}^\bullet(V)$ par l'idéal bilatère engendré par les éléments de la forme $v_1 \otimes v_2 - v_2 \otimes v_1$ pour $v_1, v_2 \in V$. De même, $\mathsf{Alt}^\bullet(V)$ est le quotient de l'algèbre $\mathsf{T}^\bullet(V)$ par l'idéal bilatère engendré par les éléments de la forme $v \otimes v$ pour $v \in V$.

Remarque 1.3.13. (1) Si $\dim_K(V) = d$, le choix d'une base de V fournit un isomorphisme de K-algèbres $\mathsf{Sym}^\bullet(V) \xrightarrow{\sim} K[X_1, \dots, X_d]$.
(2) Les algèbres $\mathsf{Sym}^\bullet(V)$ et $\mathsf{Alt}^\bullet(V)$ ont des propriétés universelles (qui se déduisent facilement de celles des $\mathsf{Sym}^n(V)$ et des $\mathsf{Alt}^n(V)$), et qui permettent de retrouver facilement le corollaire 1.3.8.

1.4. **Modules de type fini sur les anneaux principaux.** On suppose désormais A principal. Par définition, A est intègre : on note K son corps des fractions. Rappelons que A est factoriel : on dispose du pgcd et du ppcm. En outre, comme les idéaux de A sont engendrés par un élément, ils sont de type fini, *i.e.* A est noethérien.

Dans ce qui suit, quand on écrit une matrice, les coefficients vides correspondent à des zéros. Si $n \in \mathbf{N}_{>0}$ et $a_1, \dots, a_n \in A$, on pose

$$\mathsf{diag}(a_1, \dots, a_n) = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \in \mathsf{M}_n(A).$$

Définition 1.4.1. Si $n \in \mathbf{N}_{>0}$ on pose $\mathsf{GL}_n(A) = \{M \in \mathsf{M}_n(A) \mid \det(M) \in A^\times\}$. D'après les formules de Cramer, c'est le groupe des éléments inversibles de $\mathsf{M}_n(A)$ (prendre garde que $\det(A) \neq 0$ est insuffisant). On pose $\mathsf{SL}_n(A) = \{M \in \mathsf{M}_n(A) \mid \det(M) = 1\}$. C'est un sous-groupe de $\mathsf{GL}_n(A)$.

Proposition 1.4.2. Soient $n \in \mathbf{N}_{\geqslant 2}$ et $a_1, \dots, a_n$ des éléments de A qui engendrent l'idéal unité. Alors il existe une matrice dans $\mathsf{SL}_n(A)$ dont la première ligne est $(a_1, \dots, a_n)$.

Démonstration. Posons $X = (a_1, \dots, a_n)$. Il s'agit de prouver l'existence d'une matrice $M \in \mathsf{SL}_n(A)$ telle que $XM^{-1} = (1, 0, \dots, 0)$. On procède par récurrence sur $n \geqslant 2$.

Cas $n = 2$. Comme $A = Aa_1 + Aa_2$, il existe $u, v \in A$ tels que $va_1 - ua_2 = 1$. La matrice $M = \begin{pmatrix} a_1 & a_2 \\ u & v \end{pmatrix}$ répond alors à la question.

Cas $n > 2$. Soit $dA = \mathsf{pgcd}(a_2, \dots, a_n)$ et $b_2, \dots, b_n \in A$ tels que $db_i = a_i$ pour $i \in \{2, \dots, n\}$. On a $\mathsf{pgcd}(b_2, \dots, b_n) = A$: par hypothèse de récurence, il existe $M_1' \in \mathsf{SL}_{n-1}(A)$ telle que $YM_1'^{-1} = (1, 0, \dots, 0)$ où $Y = (b_2, \dots, b_n)$. Soit alors

$$M_1 = \begin{pmatrix} 1 & \\ & M_1' \end{pmatrix}$$

On a $\det(M_1) = \det(M_1') = 1$ et $XM_1^{-1} = (a_1, d, 0, \dots, 0)$. On utilise le cas $n = 2$: comme $\mathsf{pgcd}(a_1, d) = A$, il existe $M_2' \in \mathsf{SL}_2(A)$ avec $(a_1, d)M_2^{-1} = (1, 0)$. Soit alors

$$M_2 = \begin{pmatrix} M_2' & \\ & \mathrm{I}_{n-2} \end{pmatrix}$$

où $\mathrm{I}_{n-2} \in \mathsf{SL}_{n-2}(A)$ désigne la matrice identité. On a $\det(M_2) = \det(M_2') = 1$ et $XM_1^{-1}M_2^{-1} = (1, 0, \dots, 0)$, *i.e.* $XM^{-1} = (1, 0, \dots, 0)$ avec $M = M_2M_1 \in \mathsf{SL}_n(A)$. □

Remarque 1.4.3. Cette preuve fournit une procédure effective pour construire la matrice si on sait traiter le cas $n = 2$ (par exemple lorsque A est un anneau euclidien).

Définition 1.4.4. Si $n, m \in \mathbf{N}_{>0}$, on fait agir $\mathsf{SL}_n(A) \times \mathsf{SL}_m(A)$ sur le A-module $\mathsf{M}_{n\times m}(A)$ par

$$(P, Q) \cdot M = P^{-1}MQ.$$

Deux matrices $M_1, M_2 \in \mathsf{M}_{n\times m}(A)$ sont dites **équivalentes** si elles sont dans la même orbite pour cette action. On écrit alors $M_1 \sim M_2$ (cela définit une relation d'équivalence). Remarquons qu'on peut aussi faire agir $\mathsf{GL}_n(A) \times \mathsf{GL}_m(A)$ de la même façon.

Remarque 1.4.5. Lorsque $n = m$, on prendra garde à ne pas confondre cette notion avec celle, plus fine, de matrices **semblables** : si $M_1, M_2 \in \mathsf{M}_n(A)$, on dit que M_1 et M_2 sont semblables s'il existe $P \in \mathsf{GL}_n(A)$ tel que $M_2 = P^{-1}M_1P$.

Définition 1.4.6. Un matrice **réduite** est une matrice de la forme

$$\begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_r \\ & & \end{pmatrix} \in \mathsf{M}_{n\times m}(A)$$

avec $r \in \{0, \dots, \min\{m, n\}\}$ et $\alpha_1, \dots, \alpha_r \in A\backslash\{0\}$ tels que $\alpha_i | \alpha_{i+1}$ pour tout $i \in \{0, \dots r-1\}$.

Notation. (1) Fixons une famille $(p_\lambda)_{\lambda\in\Lambda}$ de représentants des éléments irréductibles de A. Tout élément $a \in A\backslash\{0\}$ admet une décomposition unique en facteurs irréductibles :

$$a = u \prod_{\lambda\in\Lambda} p_\lambda^{n_\lambda}$$

où $u \in A^\times$ et $(n_\lambda)_{\lambda\in\Lambda}$ est une famille d'entiers presque tous nuls (*i.e.* tous nuls sauf un nombre fini). On pose alors

$$\ell(a) = \sum_{\lambda\in\Lambda} n_\lambda \in \mathbf{N}$$

qu'on appelle **longueur** de a. Ce n'est autre que le nombre de facteurs irréductibles de a (par exemple, on a $\ell(a) = 0 \Leftrightarrow a \in A^\times$ et $\ell(a) = 1$ si et seulement si A est irréductible). Si $M = [m_{i,j}]_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} \in \mathsf{M}_{n\times m}(A)\backslash\{0\}$, on pose

$$\ell(M) = \min\big\{\ell(m_{i,j}) \,\big|\, 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m,\ m_{i,j} \neq 0\big\}.$$

(2) Si $\sigma \in \mathfrak{S}_n$ est une permutation, on pose $P_\sigma = \big(\delta_{\sigma(i),j}\big)_{1\leqslant i,j\leqslant n} \in \mathsf{M}_n(A)$ (où $\delta_{i,j}$ est le symbole de Kronecker). On a $\det(P_\sigma) = \varepsilon(\sigma)$ (où $\varepsilon(\sigma)$ désigne la signature de σ), de sorte que $P_\sigma \in \mathsf{GL}_n(A)$. Posons $\widetilde{P}_\sigma = \mathsf{diag}\big(1, \dots, 1, \varepsilon(\sigma)\big)P_\sigma \in \mathsf{SL}_n(A)$.
Si $M \in \mathsf{M}_{n\times m}(A)$, la matrice $P_\sigma M$ est l'élément de $\mathsf{M}_{n\times m}(A)$ dont la i-ième ligne est la $\sigma(i)$-ième ligne de M. De même, si $\gamma \in \mathfrak{S}_m$ est une permutation, la matrice MP_γ est déduite de M en permutant les colonnes suivant γ. En multipliant M par $\widetilde{P}_\sigma$ à gauche (resp. par $\widetilde{P}_\gamma$ à droite), on permute les lignes suivant σ (resp. les colonnes suivant γ) et on multiplie la dernière ligne (resp. colonne) par $\varepsilon(\sigma)$ (resp. $\varepsilon(\gamma)$).

Théorème 1.4.7. Tout matrice $M \in \mathsf{M}_{n\times m}(A)$ est équivalente à une matrice réduite.

Démonstration. On peut supposer $M \neq 0$. On procède par récurrence sur $d = \min\{m, n\}$.
Supposons $d = 1$. Quitte à transposer, on peut supposer $n = 1$, de sorte que M est un vecteur ligne. Si $m = 1$, il n'y a rien à faire : supposons $m \geqslant 2$. Notons α_1 le pgcd des coefficients de M : on a $M = \alpha_1 X$ où X est un vecteur ligne dont les composantes engendrent l'idéal unité. D'après la proposition 1.4.2, il existe une matrice $Q \in \mathsf{SL}_n(A)$ telle que la première ligne de Q^{-1} soit égale à X. On a alors $XQ = (1, 0, \dots, 0)$ et donc $MQ = (\alpha_1, 0, \dots, 0)$.
Supposons désormais $d > 1$. Rappelons que $M \neq 0$. Soit $\delta = \min\big\{\ell(M') \,\big|\, M' \sim M\big\} \in \mathbf{N}$. Quitte à remplacer M par une matrice équivalente convenable, on peut supposer que $\ell(M) = \delta$. Il existe $i_0 \in \{1, \dots, n\}$ et

$j_0 \in \{1,\dots,m\}$ tels que $\ell(m_{i_0,j_0}) = \delta$. Notons $\tau_{1,i_0} \in \mathfrak{S}_n$ (resp. $\tau_{1,j_0} \in \mathfrak{S}_m$) la transposition de $\{1,\dots,n\}$ (resp. $\{1,\dots,m\}$) échangeant 1 et i_0 (resp. j_0), et posons $M' = \widetilde{P}_{\tau_{1,i_0}}^{-1} M \widetilde{P}_{\tau_{1,j_0}} \in \mathsf{M}_{n\times m}(A)$ (où $\widetilde{P}_{\tau_{1,i_0}} \in \mathsf{SL}_n(A)$ et $\widetilde{P}_{\tau_{1,j_0}} \in \mathsf{SL}_m(A)$ sont les matrices de permutation modifiées, *cf* définition 1.4.1 (2)). On a $M' \sim M$ et $m'_{1,1} = m_{i_0,j_0}$: quitte à remplacer M par M', on peut supposer que $\ell(m_{1,1}) = \delta$. Posons $\alpha_1 := m_{1,1}$.

• Commençons par montrer que α_1 divise les coefficients de la première ligne et de la première colonne. Quitte à transposer, il suffit de traiter le cas de la première colonne. Raisonnons par l'absurde : supposons qu'il existe $i \in \{2,\dots,n\}$ tel que $\alpha_1 \nmid m_{i,1}$. Quitte à permuter la deuxième et la i-ème ligne, on peut supposer $i = 2$. Soit $\widetilde{\alpha}_1 = \mathsf{pgcd}(\alpha_1, m_{2,1})$. Comme $\widetilde{\alpha}_1$ divise strictement α_1, on a $\ell(\widetilde{\alpha}_1) < \delta$. Par ailleurs, il existe $a, b \in A$ tels que $\widetilde{\alpha}_1 = am_{1,1} + bm_{2,1}$. Posons alors

$$P = \begin{pmatrix} a & b & & & \\ -m_{2,1}/\widetilde{\alpha}_1 & m_{1,1}/\widetilde{\alpha}_1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

On a $\det(P) = 1$ et le coefficient d'indice $(1,1)$ de $M' = PM$ est $\widetilde{\alpha}_1$. On a $M' \sim M$ et $\ell(M') \leqslant \ell(\widetilde{\alpha}_1) < \delta$, ce qui contredit la définition de δ.

• Quitte à multiplier M à gauche par la matrice

$$\begin{pmatrix} 1 & & & \\ -m_{2,1}/\alpha_1 & 1 & & \\ \vdots & & \ddots & \\ -m_{n,1}/\alpha_1 & & & 1 \end{pmatrix} \in \mathsf{SL}_n(A)$$

et à droite par la matrice

$$\begin{pmatrix} 1 & -m_{1,2}/\alpha_1 & \cdots & -m_{1,m}/\alpha_1 \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \in \mathsf{SL}_m(A)$$

on peut supposer que $m_{i,1} = 0$ pour $\in \{2,\dots,n\}$ et $m_{1,j} = 0$ pour $j \in \{2,\dots,m\}$. En effet, cela donne une matrice équivalente, et de même longueur (puisqu'on a pas changé le coefficient d'indice $(1,1)$).

• La matrice M est donc de la forme

$$\begin{pmatrix} \alpha_1 & \\ & M_1 \end{pmatrix}$$

avec $M_1 \in \mathsf{M}_{(n-1)\times(m-1)}(A)$. Par hypothèse de récurrence, il existe $P_1 \in \mathsf{SL}_{n-1}(A)$, $Q_1 \in \mathsf{SL}_{m-1}(A)$, $r \in \mathbf{N}$, et des éléments $\alpha_2,\dots,\alpha_r \in A\backslash\{0\}$ tels que $\alpha_i | \alpha_{i+1}$ pour tout $i \in \{2,\dots,r-1\}$ et

$$P_1^{-1} M_1 Q_1 = \begin{pmatrix} \alpha_2 & & \\ & \ddots & \\ & & \alpha_r \end{pmatrix}$$

Quitte à multiplier M par $\begin{pmatrix} 1 & \\ & P_1^{-1} \end{pmatrix} \in \mathsf{SL}_n(A)$ à gauche et par $\begin{pmatrix} 1 & \\ & Q_1 \end{pmatrix} \in \mathsf{SL}_m(A)$ à droite, on peut supposer que

$$M = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_r \end{pmatrix}$$

Reste à voir que $\alpha_1 \mid \alpha_2$, et on aura fini. Supposons le contraire. Soit $\alpha'_1 = \mathsf{pgcd}(\alpha_1, \alpha_2)$. Comme $\alpha_1 \nmid \alpha_2$, on a $\ell(\alpha'_1) < \ell(\alpha_1) = \delta$. Il existe $a, b \in A$ tels que $a\alpha_1 + b\alpha_2 = \alpha'_1$. L'égalité

$$\begin{pmatrix} 1 & \\ a & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 & \\ & \alpha_2 \end{pmatrix} \begin{pmatrix} 1 & \\ b & 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \\ \alpha'_1 & \alpha_2 \end{pmatrix}$$

montre qu'il existe $M' = (m_{i,j})_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}} \in \mathsf{M}_{n\times m}(A)$ équivalente à M et telle que $m'_{2,1} = \alpha'_1$. On a alors $\ell(M') \leqslant \ell(\alpha'_1) < \delta$, ce qui contredit la définition de δ. On a fini. □

Remarque 1.4.8. (1) Dans le cas où A est *euclidien*, il est possible de rendre cet énoncé constructif, à l'aide d'opérations élémentaires.

(2) Dans le cas où A est un corps, on retrouve le fait bien connu que les orbites pour la relation d'équivalence sont caractérisées par le rang : toute matrice M est équivalente à $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$ (où le nombre de 1 est $\mathrm{rg}(M)$).

Théorème 1.4.9. (Théorème de la base adaptée). Soit M un sous-A-module d'un A-module L libre de rang n fini. Alors M est libre, et il existe une base $(e_1, \dots, e_n)$ de L, un entier $r \leqslant n$ et $\alpha_1, \dots, \alpha_r \in A\backslash\{0\}$ tels que

$$\begin{cases} \alpha_i | \alpha_{i+1} & \text{pour tout } i \in \{0, \dots r-1\} \\ (\alpha_1 e_1, \dots, \alpha_r e_r) & \text{soit une base de } M. \end{cases}$$

Démonstration. Comme A est principal, il est noethérien. Comme L est libre de rang fini, le A-module L est noethérien (proposition 1.1.21) : son sous-A-module M est donc lui aussi de type fini. Choisissons $x_1, \dots, x_m \in M$ une famille génératrice. On dispose donc d'une application A-linéaire

$$f \colon A^m \to L$$
$$(a_1, \dots, a_m) \mapsto \sum_{j=1}^{m} a_j x_j$$

dont l'image n'est autre que M. Après le choix d'une base $\mathfrak{B}$ de L, cette application est donnée par une matrice $n \times m$ (dont la j-ième colonne consiste en les coordonnées de x_j dans la base $\mathfrak{B}$). D'après le théorème 1.4.7, cette dernière est équivalente à une matrice réduite : quitte à effectuer un changement de base de A^m et de L, elle s'écrit

$$\begin{pmatrix} \alpha_1 & & & \\ & \ddots & & \\ & & \alpha_r & \\ & & & \end{pmatrix}$$

avec $r \in \{0, \dots, \min\{m, n\}\}$ et $\alpha_1, \dots, \alpha_r \in A\backslash\{0\}$ tels que $\alpha_i | \alpha_{i+1}$ pour tout $i \in \{0, \dots r-1\}$. Si on note $(e_1, \dots, e_n)$ la nouvelle base de L, l'image de f est donc le sous-A-module libre de base $(\alpha_1 e_1, \dots, \alpha_r e_r)$. □

Remarque 1.4.10. Le résultat qui précède est faux lorsque A n'est pas principal. Par exemple $\mathbf{Z}/2\mathbf{Z}$ est un sous-$\mathbf{Z}/4\mathbf{Z}$-module non libre de $\mathbf{Z}/4\mathbf{Z}$. De même, le sous-$\mathbf{Z} \times \mathbf{Z}$-module $\mathbf{Z} \times \{0\}$ de $\mathbf{Z} \times \mathbf{Z}$ n'est pas libre.

Théorème 1.4.11. (Théorème des facteurs invariants). Soit M un A-module de type fini. Alors il existe des entiers $d, r \in \mathbf{N}$ et $a_1, \dots, a_d \in A\backslash\big(\{0\} \cup A^\times\big)$ tels que

$$\begin{cases} a_i | a_{i+1} & \text{pour tout } i \in \{0, \dots d-1\} \\ M \simeq (A/a_1A) \times \cdots \times (A/a_dA) \times A^r \end{cases}$$

En outre, les entiers d, r et les idéaux $a_1A, \dots, a_dA$ sont uniques. L'entier r s'appelle le **rang** de M et si $r = 0$, les éléments $(a_1, \dots, a_d)$ « les » **facteurs invariants** de M.

Démonstration. • Commençons par montrer l'existence. Comme M est de type fini, choisissons une famile génératrice $m_1, \dots, m_n$: on dispose d'une application surjective

$$f \colon A^n \to M$$
$$(\lambda_1, \dots, \lambda_n) \mapsto \sum_{i=1}^{n} \lambda_i m_i.$$

Comme A^n est libre, il admet une base $(e_1, \dots, e_n)$ telle que

$$\mathsf{Ker}(f) = \bigoplus_{i=1}^{s} A\alpha_i e_i$$

avec $s \in \{1, \dots, n\}$ et $\alpha_1, \dots, \alpha_s \in A\backslash\{0\}$ tels que $\alpha_i | \alpha_{i+1}$ pour tout $i \in \{0, \dots s-1\}$ (théorème de la base adaptée). En passant au quotient, f induit un isomorphisme A-linéaire

$$M \simeq A^n/\mathsf{Ker}(f) = \Big(\bigoplus_{i=1}^{s} (A/\alpha_i A)e_i\Big) \oplus \Big(\bigoplus_{i=s+1}^{n} Ae_i\Big)$$

Soit $t = \max\big(i \in \{1,\dots,s\},\ \alpha_i \in A^\times\big)$ (on a $t = 0$ si $\alpha_1 \notin A^\times$). Posons $d = s-t$, $r = n-s$ et $a_i = \alpha_{t+i}$ pour $i \in \{1,\dots,d\}$. On a $a_1,\dots,a_d \in A\backslash\big(\{0\} \cup A^\times\big)$ et $a_i | a_{i+1}$ pour tout $i \in \{0,\dots d-1\}$. En outre, comme

$$A/\alpha_i A = \begin{cases} 0 & \text{si } i \leqslant t \\ A/a_{i-t}A & \text{si } t < i \leqslant s \end{cases}$$

on a bien

$$M \simeq (A/a_1A) \times \cdots \times (A/a_dA) \times A^r.$$

• Montrons maintenant l'unicité. On a déjà $M_{\mathsf{tors}} = (A/a_1A) \times \cdots \times (A/a_dA)$ et donc $M/M_{\mathsf{tors}} \simeq A^r$. L'entier r ne dépend donc que de M (proposition 1.1.15). Il suffit donc de traiter le cas où M est de torsion. On a $M \simeq \prod_{i=1}^{d}(A/a_iA)$ avec $a_1 \mid a_2 \mid \cdots \mid a_d$ dans $A\backslash\{0\}$. Notons $\mathscr{P}$ l'ensemble des éléments irréductibles de A. Si $p \in \mathscr{P}$, l'idéal pA est premier non nul donc maximal [1] : le A-module M/pM est un A/pA-espace vectoriel de dimension finie $d_p(M)$ (on a donc $d_p(M) = \#\{i \in \{1,\dots,d\} \mid p \mid a_i\}$). On en déduit déjà que $d = d(M) := \max_{p\in\mathscr{P}} d_p(M)$ ne dépend que de M.

Pour tout $n \in \mathbf{N}$, on a $d_p(p^nM/p^{n+1}M) = \#\{i \in \{1,\dots,d\} \,|\, v_p(a_i) \geqslant n+1\}$. Il en résulte que pour tout $n \in \mathbf{N}_{>0}$, l'entier

$$\#\{i \in \{1,\dots,d\} \,|\, v_p(a_i) = n\} = d_p(p^{n-1}M/p^nM) - d_p(p^nM/p^{n+1}M)$$

ne dépend que de M et de p. Comme on a $v_p(a_1) \leqslant v_p(a_2) \leqslant \cdots \leqslant v_p(a_d)$, cela implique que pour tout $p \in \mathscr{P}$ et tout $i \in \{1,\dots,d\}$, l'entier $v_p(a_i)$ ne dépend que de M et de p. Cela signifie que les idéaux a_iA ne dépendent que de M.

Remarque : autre façon de finir.

Lemme 1.4.12. Si $a, b \in A\backslash\{0\}$, on a $a(A/bA) \simeq A/\frac{b}{\mathsf{pgcd}(a,b)}A$.

Démonstration. Écrivons $a = \alpha\,\mathsf{pgcd}(a,b)$ et $b = \beta\,\mathsf{pgcd}(a,b)$: on a $\mathsf{pgcd}(\alpha,\beta) = 1$. Soit $\pi\colon A \to A/bA$ la projection canonique. Alors $a(A/bA)$ est l'image du composé $\pi \circ m_a$, où $m_a\colon A \to A$ est la multiplication par a. On a $x \in \mathsf{Ker}(\pi \circ m_a) \Leftrightarrow ax \in bA \Leftrightarrow \alpha x \in \beta A \Leftrightarrow x \in \beta A$ (parce que $\mathsf{pgcd}(\alpha,\beta) = 1$). Le morphisme surjectif $\pi \circ m_a\colon A \to a(A/ba)$ induit donc un isomorphisme $A/\beta A \xrightarrow{\sim} a(A/bA)$. □

On montre alors l'unicité des idéaux a_iA par récurrence sur d, le cas $d = 0$ étant vide. Supposons donc $M \simeq \prod_{i=1}^{d}(A/a_iA) \simeq \prod_{i=1}^{d}(A/b_iA)$ avec $a_1 \mid a_2 \mid \cdots \mid a_d$ et $b_1 \mid b_2 \mid \cdots \mid b_d$. Soit $s = \max\{i \in \{1,\dots,d\} \,|\, a_iA = a_1A\}$. On a alors $a_1M \simeq \prod_{i=s+1}^{d} a_1(A/a_iA) \simeq \prod_{i=1}^{d} a_1(A/b_iA)$. D'après le lemme 1.4.12, cela signifie que $a_1M \simeq \prod_{i=s+1}^{d} A/\frac{a_i}{a_1}A \simeq \prod_{i=1}^{d} A/\frac{b_i}{\mathsf{pgcd}(a_1,b_i)}A$. Par unicité de $d(a_1M)$, cela implique que $A/\frac{b_i}{\mathsf{pgcd}(a_1,b_i)}A = \{0\}$, *i.e.* $b_iA = \mathsf{pgcd}(a_1,b_i)A$ soit $a_1A \subset b_iA$ pour tout $i \in \{1,\dots,s\}$. Symétriquement, on a aussi $b_iA \subset a_1A$, et donc $a_iA = b_iA$ pour tout $i \in \{1,\dots,s\}$. En outre, on a $a_1M \simeq \prod_{i=s+1}^{d} A/\frac{a_i}{a_1}A \simeq \prod_{i=s+1}^{d} A/\frac{b_i}{a_1}A$: l'hypothèse de récurrence implique que $\frac{a_i}{a_1}A = \frac{b_i}{a_1}A$ et donc $a_iA = b_iA$ pour tout $i \in \{s+1,\dots,d\}$, ce qui achève la preuve. □

Corollaire 1.4.13. Un A-module de type fini sans torsion est libre.

Corollaire 1.4.14. Les idéaux $\alpha_1A,\dots,\alpha_rA$ des théorèmes 1.4.7 et 1.4.9 sont uniques.

Démonstration. Si $M = \bigoplus_{i=1}^{r} A\alpha_ie_i \subseteq \bigoplus_{i=1}^{n} Ae_i = L$, on a $L/M \simeq \bigoplus_{i=1}^{r}(A/\alpha_iA)e_i \times A^{n-r}$. Soit s le nombre d'indices $i \in \{1,\dots,r\}$ tels que $\alpha_iA = A$ (*i.e.* $\alpha_i \in A^\times$). On a $L/M \simeq (A/\alpha_{s+1}A) \times \cdots \times (A/\alpha_rA) \times A^{n-r}$. D'après le théorème 1.4.11, les entiers $r-s$ et $n-r$ et donc s ne dépendent que de L et M, ainsi que les idéaux $\alpha_{s+1}A,\dots,\alpha_rA$, ce qui implique l'unicité pour le théorème 1.4.9. Cela implique l'unicité dans le théorème 1.4.7. On a fini. □

Les deux résultats suivants, bien qu'assez intuitifs, sont plus difficiles que ce qui précède.

Proposition 1.4.15. Soit M un A-module libre. Alors tout sous-A-module de M est libre.

Démonstration. Lorsque M est de rang fini, c'est le théorème de la base adaptée (théorème 1.4.9). Traitons le cas général. Soit N un sous-A-module de M. Soient $\mathbf{x} = \{x_i\}_{i\in I}$ une base de M et $\mathbf{y} = \{y_j\}_{j\in J}$ une famille libre de N. On pose $T = \sum_{j\in J} Ay_j$ le sous-A-module de N engendré par $\mathbf{y}$. Notons S le sous-A-module de M engendré par les x_i qui interviennent dans l'écriture des y_j dans la base $\mathbf{x}$. On se restreint aux familles $\mathbf{y}$ telles que $S \cap N = T$. De telles familles existent. Par exemple, si $\mathbf{y}_0$ est une famille libre de N qui est finie (à un élément par exemple), alors S_0 est de type fini donc libre de rang fini. Le sous-A-module $S_0 \cap N$ est donc libre de rang fini d'après le théorème de la base adaptée : si $\mathbf{y}$ est une base de $S_0 \cap N$ sur A, alors $S = S_0$ (avec des notations évidentes) et $S \cap N = T$. L'ensemble des tels $\mathbf{y}$ est donc non vide. Comme il est clairement inductif (pour l'inclusion), il admet un élément maximal d'après le théorème de Zorn : on peut supposer la famille $\mathbf{y}$ maximale. Montrons que cette dernière engendre N (*i.e.* $T = N$).

Supposons le contraire et soit $v \in N\backslash T$. Comme $S \cap N = T$, l'élément v fait intervenir des x_i qui n'appartiennent pas à S. Considérons l'ensemble $\mathcal{M}$ de ces v tels que le nombre de nouveaux x_i est minimal. Dans $\mathcal{M}$, choisissons un v ayant un coefficient de nouveau x_i qui a un nombre minimal de facteurs irréductibles. Soient x_{i_0} le nouveau x_i et α le coefficient en question. Montrons que $\mathbf{y}' = \mathbf{y} \cup \{v\}$ contredit la maximalité de $\mathbf{y}$. Comme

1. Si A est un anneau principal et $\mathfrak{p} \subset A$ est premier non nul, alors $\mathfrak{p}$ est maximal. En effet, soit $\mathfrak{m} \supseteq \mathfrak{p}$ un idéal maximal (*cf* théorème de Krull). Comme A est principal, il existe $a, b \in A\backslash\{0\}$ tels que $\mathfrak{p} = aA$ et $\mathfrak{m} = bA$. Comme $\mathfrak{p} \subseteq \mathfrak{m}$, on a $b|a$: il existe $c \in A$ tel que $a = bc$. Mais comme $\mathfrak{p}$ est premier, on a $b \in \mathfrak{p}$ ou $c \in \mathfrak{p}$. Dans le dernier cas, il existerait $d \in A$ tel que $c = ad$, et donc $a = abd$ d'où $bd = 1$ vu que A est intègre et $a \neq 0$. Cela imliquerait $b \in A^\times$ et donc $\mathfrak{m} = A$ ce qui n'est pas. On a donc en fait $b \in \mathfrak{p}$, d'où $\mathfrak{m} \subseteq \mathfrak{p}$ *i.e.* $\mathfrak{p} = \mathfrak{m}$ est maximal.

v fait intervenir $x_{i_0} \notin S$, la famille $\mathbf{y}'$ est libre dans N. Reste à montrer, avec des notations évidentes, que $S' \cap N = T'$, sachant que l'inclusion $T' \subseteq S' \cap N$ est triviale. Soit $w \in S' \cap N$.
Supposons $w \notin T$. Comme $w \in S'$, l'ensemble des nouveaux x_i intervenant dans w est inclus dans S' et donc dans celui des nouveaux x_i intervenant dans v. Par minimalité de ce dernier, on a $w \in \mathcal{M}$ et w fait intervenir tous les nouveaux x_i qui interviennent dans v. C'est en particulier le cas pour x_{i_0} : on a $w = \beta x_{i_0} + \cdots$ avec $\beta \in A\backslash\{0\}$. Par minimalité de α, le nombre de facteurs irréductibles de $\mathsf{pgcd}(\alpha, \beta)$ est supérieur ou égal au nombre de facteurs irréductibles de α *i.e.* $\alpha|\beta$ (en effet, il existe $a, b \in A$ tels que $a\alpha + b\beta = \delta = \mathsf{pgcd}(\alpha, \beta)$, on a alors $av + bw \in (S' \cap N)\backslash T'$) : on a $\beta = \lambda\alpha$. L'élément $w - \lambda v$ appartient à $S' \cap N$ et ne fait pas intervenir x_{i_0}. Comme l'ensemble des nouveaux x_i qu'il fait intervenir est inclus dans S', donc dans l'ensemble des nouveaux x_i intervenant dans v, il n'en fait intervenir aucun nouveau (par minimalité du nombre de nouveaux x_i qui interviennent dans v). On a donc $w - \lambda v \in S \cap N = T$ d'où $w \in T + Av = T'$, ce qu'on voulait. □

Proposition 1.4.16. Supposons que A n'est pas un corps. Alors le A-module $A^{\mathbf{N}}$ n'est pas libre.

Démonstration. Supposons que $M = A^{\mathbf{N}}$ est libre. Remarquons tout d'abord que M n'est pas dénombrablement engendré. Si A est dénombrable, c'est évident pour des raisons de cardinalité, et si A n'est pas dénombrable, un argument à la Vandermonde montre que la famille $\{(1, \alpha, \alpha^2, \ldots)\}_{\alpha \in A}$ est libre dans M. Soit $p \in A$ premier (A n'est pas un corps). Soit S le sous-A-module de M engendré par les éléments $(a_0, a_1, a_2, \ldots)$ tels qu'il existe une suite $(r_n)_{n\in\mathbf{N}}$ tel que $a_n \in p^{r_n}A$ et $\lim\limits_{n\to\infty} r_n = +\infty$. Comme M est libre et A principal, le sous-module S est libre (*cf* proposition précédente). Par ailleurs, si $x = (1, p, p^2, \ldots)$, on a $xM \subseteq S$: le A-module S n'est pas de type dénombrable d'après ce qui précède. Le A/pA-espace vectoriel S/pS est donc de dimension non dénombrable. Ceci est absurde, car $S/pS \simeq (A/pA)^{(\mathbf{N})}$ est le A/pA-espace vectoriel des suites à support fini, qui est de dimension dénombrable. L'hypothèse M libre est donc absurde. □

1.5. **Application à la réduction des endomorphismes.** Soient K un corps commutatif, V un K-espace vectoriel. Rappelons que $\mathsf{End}_K(V)$ est une K-algèbre (la multiplication étant donnée par la composition des endomorphismes). Elle est non commutative si $\dim_K(V) > 1$. Si $f \in \mathsf{End}_K(V)$ et $P \in K[X]$, on dispose donc de $P(f) \in \mathsf{End}_K(V)$. Cela fournit un morphisme d'anneaux $\alpha_f \colon K[X] \to \mathsf{End}_K(V)$; $P \mapsto P(f)$, et munit donc V d'une structure de $K[X]$-module : on note V_f le $K[X]$-module ainsi obtenu. Réciproquement, si M est un $K[X]$-module, alors M est en particulier un K-espace vectoriel, et l'action de X sur M est donnée par un endomorphisme f_M. On a bien sûr $f_M = f$ si $M = V_f$. Ainsi $(V, f) \mapsto V_f$ est une bijection de « l'ensemble » des couples constitués d'un K-espace vectoriel V et d'un endomorphisme f de V sur « l'ensemble » des $K[X]$-modules.

Proposition 1.5.1. Le K-espace vectoriel V est de dimension finie si et seulement si V_f est de type fini et de torsion.

Démonstration. Comme V est de type fini comme K-espace vectoriel, il l'est *a fortiori* en tant que $K[X]$-module. Par ailleurs, si $v \in V$, la famille $\big(f^n(v)\big)_{n\in\mathbf{N}}$ est liée : il existe $N \in \mathbf{N}_{>0}$ et $(\lambda_0, \ldots, \lambda_N) \in K^{N+1}\backslash\{0\}$ tels que $\sum\limits_{n=0}^{N} \lambda_n f^n(V)$, de sorte que si $P = \sum\limits_{n=0}^{N} \lambda_n X^n$, on a $P(f)(v) = 0$: le $K[X]$-module V est de torsion. Réciproquement, soit $v_1, \ldots, v_d$ une famille génératrice du $K[X]$-module V. Pour tout $i \in \{1, \ldots, d\}$, il existe $P_i \in K[X]\backslash\{0\}$ tel que $P_i(f)(v_i) = 0$. On a donc un morphisme K-linéaire surjectif $\bigoplus\limits_{i=1}^{d}(K[X]/(P_i)) \to V$, d'où $\dim_K(V) \leqslant \dim_K\left(\bigoplus_{i=1}^{d}(K[X]/(P_i))\right) = \sum_{i=1}^{d} \deg(P_i) < \infty$. □

Exemple 1.5.2. Soit $V = K^{(\mathbf{N})}$. Soit $(e_n)_{n\in\mathbf{N}}$ la base de V définie par $e_n = (\delta_{m,n})_{m\in\mathbf{N}}$, et $f \in \mathsf{End}_K(V)$ défini par $f(e_n) = e_{n+1}$. Alors V_f est le $K[X]$-module libre de rang 1 engendré par e_0.

Définition 1.5.3. Supposons V de dimension finie d sur K et soit $f \in \mathsf{End}_K(V)$.
(1) L'endomorphisme f est dit **cyclique** s'il existe $v \in V$ tel que V est engendré par la famille $\big(f^n(v)\big)_{n\in\mathbf{N}}$. Cela signifie que le $K[X]$-module V_f est mongène (engendré par un élément).
(2) On note $\chi_f(X) = \det\big(X\,\mathrm{Id}_V - f\big)$ le **polynôme caractéristique** de f. C'est un polynôme de degré d à coefficients dans K.
(3) Comme $\dim_K\big(\mathsf{End}_K(V)\big) = d^2$, l'homorphisme $\alpha_f \colon K[X] \to \mathsf{End}_K(V)$ n'est pas injectif : il existe un unique polynôme unitaire $\mu_f \in K[X]$ tel que $\mathsf{Ker}(\alpha_f) = \mu_f K[X]$. On l'appelle le **polynôme minimal** de f.

Proposition 1.5.4. Soit $f \in \mathsf{End}_K(V)$ cyclique. Alors il existe $v \in V$ tel que la famille
$$\big(v, f(v), \ldots, f^{d-1}(v)\big)$$
soit une K-base de V, où $d = \dim_K(V)$. Dans ce cas, on a $\mu_f = \chi_f$ et $V_f \simeq K[X]/\mu_f K[X]$.

Démonstration. Soit $v \in V$ tel que $\big(f^n(v)\big)_{n\in\mathbf{N}}$ engendre le K-espace vectoriel V, et
$$\begin{aligned} \alpha_v \colon K[X] &\to V \\ P &\mapsto P(f)(v) \end{aligned}$$
C'est une application K-linéaire surjective. Comme V est de dimension finie sur K, on a $\mathsf{Ker}(\alpha_v) = P_v K[X]$ avec $P_v \in K[X]$ unitaire. En passant au quotient, on en déduit un isomorphisme de $K[X]$-modules

$K[X]/P_vK[X] \xrightarrow{\sim} V_f$. En particulier, on a $\deg(P_v) = d = \dim_K(V)$. Écrivons $P_v = X^d - \sum_{n=1}^{d} \lambda_n X^{d-n}$: on a $d = \dim_K(V)$ et $\big(v, f(v), \dots, f^{d-1}(v)\big)$ est une K-base de V.
Si $k \in \mathbf{N}$, on a $P_v(f)(f^k(v)) = f^k(P_v(f)(v)) = 0$: par K-linéarité on a $P_v(f) = 0$ et donc $\mu_f \mid P_v$. Réciproquement, comme $\mu_f(f) = 0$, on a $\mu_f \in \mathsf{Ker}(\alpha_v)$ donc $P_v \mid \mu_f$. Les polynômes P_v et μ_f étant unitaires, on a $\mu_f = P_v$.
La matrice de f dans la base $\big(v, f(v), \dots, f^{d-1}(v)\big)$ est donnée par

$$C(\lambda_1, \dots, \lambda_d) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & \lambda_d \\ 1 & \ddots & & \vdots & \lambda_{d-1} \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & 1 & 0 & \lambda_2 \\ 0 & \cdots & 0 & 1 & \lambda_1 \end{pmatrix}$$

(une matrice de cette forme s'appelle une **matrice compagnon**). On a

$$\det\big(X\,\mathrm{I}_n - C(\lambda_1, \dots, \lambda_d)\big) = \begin{vmatrix} X & \cdots & \cdots & 0 & -\lambda_d \\ -1 & \ddots & & \vdots & -\lambda_{d-1} \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & -1 & X & -\lambda_2 \\ 0 & \cdots & 0 & -1 & X-\lambda_1 \end{vmatrix} = X \begin{vmatrix} X & \cdots & \cdots & 0 & -\lambda_{d-1} \\ -1 & \ddots & & \vdots & -\lambda_{d-2} \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & -1 & X & -\lambda_2 \\ 0 & \cdots & 0 & -1 & X-\lambda_1 \end{vmatrix} + (-1)^d \lambda_d \underbrace{\begin{vmatrix} -1 & X & & 0 \\ 0 & \ddots & \ddots & \\ \vdots & \ddots & -1 & X \\ 0 & \cdots & 0 & -1 \end{vmatrix}}_{=(-1)^{d-1}}$$

$$= X \det\big(X\,\mathrm{I}_n - C(\lambda_1, \dots, \lambda_{d-1})\big) - \lambda_d = \cdots = X^d - \sum_{n=1}^{d} \lambda_n X^{d-n} = P_v$$

et donc $\chi_f = P_v = \mu_f$. □

Exemple 1.5.5. Si f est cyclique et $\mu_f = X^d$, alors f est nilpotent, d'indice de nilpotence d (*i.e.* $f^d = 0$ mais $f^{d-1} = 0$). Dans une base convenable, la matrice de f est de la forme

$$J_d := C(0, \dots, 0) = \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

On l'appelle **matrice nilpotente élémentaire d'ordre** d.

Théorème 1.5.6. Soient V un K-espace vectoriel et $f \in \mathsf{End}_K(V)$. Alors il existe $r \in \mathbf{N}_{>0}$ et $V_1, \dots, V_r$ des sous-K-espaces vectoriels de V tels que
(1) $V = \bigoplus_{i=1}^{r} V_i$;
(2) $f_i := f_{|V_i}$ est cyclique ;
(3) $P_1 \mid P_2 \mid \cdots \mid P_r$ où P_i est le polynôme minimal de f_i.
En outre, l'entier r et les polynômes $P_1, \dots, P_r$ sont uniques.

Démonstration. Le $K[X]$-module V_f est de type fini de torsion : on peut lui appliquer le théorème des facteurs invariants (théorème 1.4.11). Il existe $r \in \mathbf{N}_{>0}$ et $P_1, \dots, P_r \in K[X]$ unitaires uniques tels que

$$V_f \simeq \big(K[X]/P_1K[X]\big) \times \cdots \times \big(K[X]/P_rK[X]\big).$$

En termes de K-espaces vectoriels, cela correspond à une décomposition $V = \bigoplus_{i=1}^{r} V_i$ telle que si $f_i = f_{|V_i}$, on a $V_{f_i} = V_i \simeq K[X]/P_iK[X]$. L'endomorphisme f_i est alors cyclique, et $\mu_{f_i} = P_i = \chi_{f_i}$ en vertu de la proposition 1.5.4. □

Remarque 1.5.7. (1) Il n'est pas très difficile (mais un peu long) de démontrer ce résultat directement.
(2) En termes matriciels, le théorème précédent se traduit ainsi : si $A \in \mathsf{M}_d(K)$, il existe $r \in \mathbf{N}_{>0}$, $C_1, \dots, C_r$ des matrices compagnons telles que $\chi_{C_1} | \cdots | \chi_{C_r}$ et $P \in \mathsf{GL}_d(K)$ tels que

$$P^{-1}AP = \begin{pmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & C_r \end{pmatrix}$$

Définition 1.5.8. (1) Les polynômes $P_1, \dots, P_r$ du théorème 1.5.6 s'appellent les **invariants de similitude** de f.
(2) Soient V_1, V_2 deux K-espaces vectoriels de dimension finie, $f_1 \in \mathsf{End}_K(V_1)$ et $f_2 \in \mathsf{End}_K(V_2)$. On dit que (V_1, f_1) et (V_2, f_2) sont **semblables** lorsqu'il existe un isomorphisme $\varphi\colon V_2 \xrightarrow{\sim} V_1$ tel que $f_2 = \varphi^{-1} \circ f_1 \circ \varphi$. Bien sûr, traduit en termes matriciels, on retrouve la notion habituelle de similitude.

Remarque 1.5.9. (V_1, f_1) et (V_2, f_2) sont semblables si et seulement si les $K[X]$-modules V_{1,f_1} et V_{2,f_2} sont isomorphes (si $\varphi\colon V_2 \to V_1$ est une application K-linéaire, l'application $\varphi\colon V_{2,f_2} \to V_{1,f_1}$ est $K[X]$-linéaire si et seulement si $X \cdot \varphi(v) = \varphi(X \cdot v)$ pour tout $v \in V_2$, ce qui équivaut à $\varphi \circ f_2 = f_1 \circ \varphi$).

Proposition 1.5.10. Soient V un K-espace vectoriel de dimension finie et $f \in \mathsf{End}_K(V)$. Notons $P_1, \dots, P_r$ ses invariants de similitude.
(1) L'endomorphisme f est cyclique si et seulement si $r = 1$. On a alors $\mu_f = \chi_f = P_1$.
(2) On a $\chi_f = \prod_{i=1}^{r} P_i$ (en particulier, $\dim_K(V) = \sum_{i=1}^{r} \deg(P_i)$).
(3) On a $\mu_f = P_r$.

Démonstration. (1) Si f est cyclique, on a $r = 1$ par unicité de r, et donc $\mu_f = \chi_f = P_1$ en vertu de la proposition 1.5.4. La réciproque est évidente.
(2) Avec les notations du théorème 1.5.6, on a $\chi_f = \prod_{i=1}^{r} \chi_{f_i}$ vu que $V = \bigoplus_{i=1}^{r} V_i$. Mais f_i est cyclique : on a $\chi_{f_i} = \mu_{f_i} = P_i$, et on a bien $\chi_f = \prod_{i=1}^{r} P_i$.
(3) Si $P \in K[X]$, on a $P(f) = 0 \Leftrightarrow (\forall i \in \{1, \dots, r\})\ P(f_i) = 0$ (car $V = \bigoplus_{i=1}^{r} V_i$). On a donc $\mu_f = \mathop{\mathsf{ppcm}}_{1 \leqslant i \leqslant r}(\mu_{f_i}) = \mathop{\mathsf{ppcm}}_{1 \leqslant i \leqslant r}(P_i) = P_r$ vu que $P_1 \mid P_2 \mid \cdots \mid P_r$. □

Corollaire 1.5.11. (Théorème de Cayley-Hamilton). On a $\mu_f \mid \chi_f$, *i.e.* $\chi_f(f) = 0$.

Proposition 1.5.12. Soient V_1, V_2 deux K-espaces vectoriels de dimension finie, $f_1 \in \mathsf{End}_K(V_1)$ et $f_2 \in \mathsf{End}_K(V_2)$, $P_1, \dots, P_r$ et $Q_1, \dots, Q_s$ leurs invariants de similitude respectifs. Alors (V_1, f_1) et (V_2, f_2) sont semblables si et seulement si $r = s$ et $P_i = Q_i$ pour $i \in \{1, \dots, r\}$.

Démonstration. Supposons (V_1, f_1) et (V_2, f_2) semblables. Cela signifie qu'on a un isomorphisme $\varphi\colon V_2 \xrightarrow{\sim} V_1$ tel que $f_2 = \varphi^{-1} \circ f_1 \circ \varphi$, *i.e.* un isomorphisme de $K[X]$-modules $\varphi\colon V_{f_2} \xrightarrow{\sim} V_{f_1}$. Cela implique que

$$\big(K[X]/Q_1K[X]\big) \times \cdots \times \big(K[X]/Q_sK[X]\big) \simeq V_{f_2} \xrightarrow{\sim} V_{f_1} \simeq \big(K[X]/P_1K[X]\big) \times \cdots \times \big(K[X]/P_rK[X]\big).$$

Par unicité dans le théorème 1.4.11, on a $r = s$ et $P_i = Q_i$ pour $i \in \{1, \dots, r\}$.

Réciproquement, supposons $r = s$ et $P_i = Q_i$ pour $i \in \{1, \dots, r\}$. Cela implique qu'on a des isomorphismes de $K[X]$-modules :

$$V_{f_2} \simeq \big(K[X]/Q_1K[X]\big) \times \cdots \times \big(K[X]/Q_sK[X]\big) = \big(K[X]/P_1K[X]\big) \times \cdots \times \big(K[X]/P_rK[X]\big) \simeq V_{f_1}$$

notons φ leur composé. C'est en particulier un isomorphisme de K-espaces vectoriels. Comme c'est en fait un isomorphisme de $K[X]$-modules, on a $\varphi(X \cdot v) = X \cdot \varphi(v)$ *i.e.* $\varphi(f_2(v)) = f_1(\varphi(v))$ pour tout $v \in V_2$, soit $f_2 = \varphi^{-1} \circ f_1 \circ \varphi$. □

Corollaire 1.5.13. (Décomposition de Jordan). Soit $N \in \mathsf{M}_d(K)$ une matrice nilpotente. Alors il existe une unique suite d'entiers $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_r$ et $P \in \mathsf{GL}_d(K)$ tels que

$$P^{-1}NP = \begin{pmatrix} J_{d_1} & 0 & \cdots & 0 \\ 0 & J_{d_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & J_{d_r} \end{pmatrix}$$

(où J_d désigne la matrice nilpotente élémentaire d'ordre d).

Démonstration. Si N est nilpotente, son polynôme minimal est une puissance de X : il en est de même de ses invariants de similitude. Avec les notations du théorème 1.5.6, on a donc $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_r$ tels que $P_i = X^{d_i}$. Il suffit alors d'appliquer le théorème 1.5.6. □

Soient V un K-espace vectoriel et $f \in \mathsf{End}_K(V)$. On dispose du dual de V :

$$V^\vee = \mathsf{Hom}_K(V, K)$$

(le K-espace vectoriel des formes linéaires sur V). L'endomorphisme f induit un endomorphisme

$$\begin{aligned} f^\vee : V^\vee &\to V^\vee \\ \eta &\mapsto \eta \circ f \end{aligned}$$

appelé **transposée** de f.

Corollaire 1.5.14. Supposons V de dimension finie. Alors (V, f) et $(V^\vee, f^\vee)$ sont semblables.

Démonstration. D'après le théorème 1.4.11, on a $V = \bigoplus_{i=1}^{r} V_i$ avec $f_i := f_{|V_i}$ cyclique. Comme $V^\vee = \bigoplus_{i=1}^{r} V_i^\vee$, il suffit donc de traiter le cas où f est cyclique. Soit alors $v \in V$ tel que $\big(v, f(v), \dots, f^{d-1}(v)\big)$ est une K-base de V et notons $\big(e_0, e_1, \dots, e_{d_i-1}\big)$ la base duale. Écrivons $\chi_f = \mu_f = X^d - \sum_{j=0}^{d-1} \lambda_{d-j} X^j$, de sorte que $f^d(v) = \sum_{j=0}^{d-1} \lambda_{d-j} f^j(v)$.

Pour $i, n \in \{0, \dots, d-1\}$, on a

$$f^\vee(e_i)(f^n(v)) = e_i(f^{n+1}(v)) = \begin{cases} \delta_{n,i-1} & \text{si } n < d-1 \\ e_i\Big(\sum_{j=1}^{d} \lambda_{d-j} f^j(v)\Big) = \lambda_{d-i} & \text{si } n = d-1 \end{cases}$$

On a donc $f^\vee(e_0) = \lambda_d e_{d-1}$ et $f^\vee(e_i) = e_{i-1} + \lambda_{d-i} e_d$ si $i \in \{0, \dots, d-1\}$. La matrice de $f^\vee$ dans la base $\big(e_0, e_1, \dots, e_{d_i-1}\big)$ est donc

$${}^{\mathrm{t}}C(\lambda_1, \dots, \lambda_d) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ \lambda_d & \cdots & \cdots & \lambda_2 & \lambda_1 \end{pmatrix}$$

la transposée de la matrice compagnon $C(\lambda_1, \dots, \lambda_d)$. Comme les polynômes caractéristiques (resp. minimaux) d'une matrice et de sa transposée sont les mêmes, on a $\chi_{f^\vee} = \chi_f = \mu_f = \mu_{f^\vee}$ et donc $f^\vee$ est cyclique, de même invariants de similitude que f : les endomorphismes f et $f^\vee$ sont donc semblables d'après la proposition 1.5.12. □

Remarque 1.5.15. Bien sûr, cela implique que pour tout $A \in \mathsf{M}_d(K)$, les matrices A et ${}^{\mathrm{t}}A$ sont semblables. Notons que lorsque K est algébriquement clos, cela peut se démontrer directement en utilisant le théorème 1.5.23. Pour traiter le cas général, on peut alors invoquer le résultat de « descente » classique suivant : si L/K est une extension de corps et si $A_1, A_2 \in \mathsf{M}_d(K)$ sont semblables dans $\mathsf{M}_d(L)$, alors elles sont déjà semblables dans $\mathsf{M}_d(K)$.

Notation. Soient V un K-espace vectoriel et $f \in \mathsf{End}_K(V)$. On pose

$$\mathcal{C}(f) = \{g \in \mathsf{End}_K(V) \mid fg = gf\}.$$

On l'appelle le **commutant** de f. Remarquons qu'on a toujours l'inclusion $K[f] \subseteq \mathcal{C}(f)$, où $K[f]$ désigne la sous-K-algèbre de $\mathsf{End}_K(V)$ engendrée par f.

Proposition 1.5.16. Si f est cyclique, on a $\mathcal{C}(f) = K[f]$ et $\dim_K\big(\mathcal{C}(f)\big) = \dim_K(V)$.

Démonstration. Posons $d = \dim_K(V)$ et soit $v \in V$ tel que $\big(v, f(v), \dots, f^{d-1}(v)\big)$ soit une base de V. Posons

$$\begin{aligned} \beta : \mathcal{C}(f) &\to V \\ g &\mapsto g(v) \end{aligned}$$

C'est une application K-linéaire. Si $g \in \mathcal{C}(f)$, on a $\beta(g) = g(v) = \sum_{i=0}^{d-1} \lambda_i f^i(v)$. Posons $P = \sum_{i=0}^{d-1} \lambda_i X^i \in K[X]$. On a donc $g(v) = P(f)(v)$. Si $n \in \mathbf{N}$, on

$$g(f^n(v)) = f^n(g(v)) = f^n(P(f)(v)) = (X^n P)(f)(v) = (PX^n)(f)(v) = P(f)(f^n(v)).$$

Les endomorphismes g et $P(f)$ coïncident donc sur la base $\big(v, f(v), \dots, f^{d-1}(v)\big)$: ils sont donc égaux. Cela montre que $\mathcal{C}(f) = K[f]$ et que l'application β est injective (car l'endomorphisme g ne dépend que de P donc de $g(v)$).

Si $P = \sum_{i=0}^{d-1} \lambda_i X^i \in K[X]$ est de degré $< d$, alors $g = P(f)$ vérifie $g(v) = \sum_{i=0}^{d-1} \lambda_i f^i(v)$: l'application β est donc surjective. C'est donc un isomorphisme et $\dim_K\big(\mathcal{C}(f)\big) = \dim_K(V)$. □

Lemme 1.5.17. Soient A un anneau principal, α et β deux éléments de A tels que α divise β. Alors les A-modules $\mathsf{Hom}_A(A/\alpha A, A/\beta A)$ et $\mathsf{Hom}_A(A/\beta A, A/\alpha A)$ sont isomorphes à $A/\alpha A$.

Démonstration. Écrivons $\beta = \alpha\beta'$. On a $\{\lambda \in A,\ \lambda\alpha \in \beta A\} = \beta' A$: on a un homomorphisme surjectif de A-modules :

$$\begin{aligned} \varphi : A &\longrightarrow \mathsf{Hom}_A(A/\alpha A, A/\beta A) \\ \lambda &\longmapsto (\varphi(\lambda) : a \mod \alpha A \mapsto \beta'\lambda a \mod \beta A) \end{aligned}$$

et $\lambda \in \mathsf{Ker}(\varphi)$ équivaut à $\beta'\lambda \in \beta A$ *i.e.* $\lambda \in \alpha A$. L'homomorphisme φ induit donc un isomorphisme $\tilde{\varphi} : A/\alpha A \xrightarrow{\sim} \mathsf{Hom}_A(A/\alpha A, A/\beta A)$. De même, on a un homomorphisme surjectif de A-modules :

$$\begin{aligned} \psi : A &\longrightarrow \mathsf{Hom}_A(A/\beta A, A/\alpha A) \\ \lambda &\longmapsto (\psi(\lambda) : a \mod \beta A \mapsto \lambda a \mod \alpha A) \end{aligned}$$

avec $\mathsf{Ker}(\psi) = \alpha A$. L'homomorphisme ψ induit donc un isomorphisme

$$\tilde{\psi} : A/\alpha A \xrightarrow{\sim} \mathsf{Hom}_A(A/\beta A, A/\alpha A).$$

□

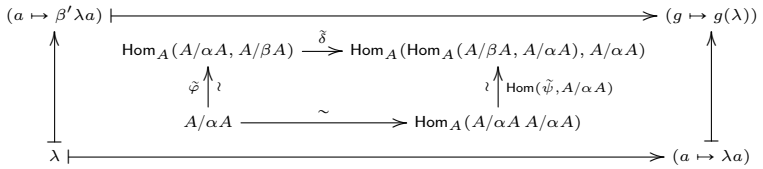
Remarque 1.5.18. On a en fait un accouplement :

$$\begin{aligned} \delta : \mathsf{Hom}_A(A/\alpha A, A/\beta A) \otimes_A \mathsf{Hom}_A(A/\beta A, A/\alpha A) &\to \beta' A/\beta A \xrightarrow[\theta]{\sim} A/\alpha A \\ f \otimes g &\mapsto f \circ g \end{aligned}$$

d'où un homomorphisme de A-modules :

$$\begin{aligned} \tilde{\delta} : \mathsf{Hom}_A(A/\alpha A, A/\beta A) &\to \mathsf{Hom}_A(\mathsf{Hom}_A(A/\beta A, A/\alpha A), A/\alpha A) \\ f &\mapsto (f \circ - : g \mapsto f \circ g). \end{aligned}$$

On a le diagramme commutatif :



qui montre que $\tilde{\delta}$ est un isomorphisme.

Proposition 1.5.19. Soient A un anneau principal et M un A-module de torsion et de type fini. Alors le A-module $\mathsf{End}_A(M)$ admet un sous-module facteur direct M' isomorphe à M. On a $M' = \mathsf{End}_A(M)$ si et seulement si M est cyclique (*i.e.* engendré par un élément).

Démonstration. Comme A est principal, le théorème des diviseurs élémentaires (*cf* théorème 1.4.11) affirme qu'il existe $r \in \mathbf{N}$ et $\alpha_1, \dots, \alpha_r \in A$ avec $\alpha_1 | \alpha_2 | \dots | \alpha_r$ tels que $M \simeq \bigoplus_{i=1}^{r} M_i$ avec $M_i \simeq A/\alpha_i A$. On a alors

$$\mathsf{End}_A(M) \simeq \bigoplus_{1 \leqslant i,j \leqslant r} \mathsf{Hom}_A(M_i, M_j).$$

Soit $M' = \bigoplus_{i=1}^{r} \mathsf{Hom}_A(M_i, M_i)$ le sous-A-module de $\mathsf{End}_A(M)$ constitué des endomorphismes qui respectent la décomposition $M \simeq \bigoplus_{i=1}^{r} M_i$. C'est un facteur direct de $\mathsf{End}_A(M)$. Par ailleurs, d'après le lemme 1.5.17, comme $M_i \simeq A/\alpha_i A$, on a $\mathsf{Hom}_A(M_i, M_i) \simeq M_i$ pour tout $i \in \{1, \dots, r\}$, et donc $M' \simeq M$. Le A-module $\mathsf{End}_A(M)$ admet donc un sous-module facteur direct M' isomorphe à M. Si $r = 1$, alors $\mathsf{End}_A(M) = \mathsf{Hom}_A(M_1, M_1) = M'$. Si $r > 1$, alors $\mathsf{Hom}_A(M_1, M_2) \hookrightarrow \mathsf{End}_A(M)/M'$. Comme $\alpha_1 | \alpha_2$, on a $\mathsf{Hom}_A(M_1, M_2) \simeq M_1$ (lemme 1.5.17). Comme $M_1 \neq 0$, on a $M' \neq \mathsf{End}_A(M)$ si $r > 1$. Ainsi $M' = \mathsf{End}_A(M)$ si et seulement si $r \leqslant 1$ *i.e.* si et seulement si M est cyclique. □

Proposition 1.5.20. Soient V un K-espace vectoriel et $f \in \mathsf{End}_K(V)$. Alors $\mathcal{C}(f) \simeq \mathsf{End}_{K[X]}(V_f)$. Si V est de dimension finie, on a $\dim_K(\mathcal{C}(f)) \geqslant \dim_K(V)$, avec égalité si et seulement si f est cyclique.

Démonstration. Posons $A = K[X]$ et $M = V_f$ (rappelons qu'il s'agit du A-module dont le groupe sous-jacent est V, et tel que $X \cdot v = f(v)$ pour $v \in V$). On a

$$\begin{aligned}
\mathsf{End}_A(M) = \mathsf{End}_{K[X]}(V_f) &= \{g \in \mathsf{End}_K(V) \,|\, (\forall P \in K[X])\,(\forall v \in V)\, f(P \cdot v) = P \cdot f(v)\} \\
&= \{g \in \mathsf{End}_K(V) \,|\, (\forall v \in V)\, g(X \cdot v) = X \cdot g(v)\} \\
&= \{g \in \mathsf{End}_K(E) \,|\, (\forall v \in V)\, g(f(v)) = f(g(v))\} \\
&= \mathcal{C}(f).
\end{aligned}$$

Si en outre V est de dimension finie sur K, le $K[X]$-module V_f est de type fini et de torsion. D'après la proposition 1.5.19, le $K[X]$-module $\mathsf{End}_{K[X]}(V_f)$ admet alors un sous-module M' facteur direct isomorphe à $M = V_f$. En particulier, on a $\dim_K(V) \leqslant \dim_K(\mathsf{End}_{K[X]}(V_f)) = \dim_K(\mathcal{C}(f))$.
L'inégalité qui précède est un égalité si et seulement si on a $M' = \mathsf{End}_A(M)$, *i.e.* si et seulement si M est cyclique (d'après la proposition 1.5.19) soit encore si et seulement si f est cyclique. □

On fixe V un K-espace vectoriel de dimension finie et $f \in \mathsf{End}_K(V)$.

Lemme 1.5.21. (Lemme des noyaux). Si $P_1, P_2 \in K[X]$ sont premiers entre eux, alors

$$\mathsf{Ker}\left((P_1 P_2)(f)\right) = \mathsf{Ker}\left(P_1(f)\right) \oplus \mathsf{Ker}\left(P_2(f)\right).$$

Démonstration. On a bien sûr $\mathsf{Ker}\left(P_1(f)\right) + \mathsf{Ker}\left(P_2(f)\right) \subseteq \mathsf{Ker}\left((P_1 P_2)(f)\right)$. Comme P_1 et P_2 sont premiers entre eux, il existe $U, V \in K[X]$ tels que $UP_1 + VP_2 = 1$. Si $v \in \mathsf{Ker}\left(P_1(f)\right) \cap \mathsf{Ker}\left(P_2(f)\right)$, on a $v = (UP_1 + VP_2)(f)(v) = 0$ et donc $\mathsf{Ker}\left(P_1(f)\right) \cap \mathsf{Ker}\left(P_2(f)\right) = \{0\}$. Par ailleurs, si $v \in \mathsf{Ker}\left((P_1 P_2)(f)\right)$ on a $v = (UP_1 + VP_2)(f)(v) = v_1 + v_2$ avec $v_1 = (V(f) \circ P_2(f))(v)$ et $v_2 = (U(f) \circ P_1(f))(v)$. Mais $P_1(f)(v_1) = (V(f) \circ (P_1 P_2)(f))(v) = 0$ vu que $v \in \mathsf{Ker}\left((P_1 P_2)(f)\right)$, *i.e.* $v_1 \in \mathsf{Ker}\left(P_1(f)\right)$. De même, on a $v_2 \in \mathsf{Ker}\left(P_2(f)\right)$. □

Proposition 1.5.22. L'endomorphisme f est diagonalisable si et seulement si il est annulé par un polynôme scindé à racines simples (*i.e.* si et seulement si μ_f est scindé à racines simples).

Démonstration. Si f est diagonalisable, alors f est annulé par le polynôme $\prod_{i=1}^{n} (X - \lambda_i)$. Réciproquement, si f est annulé par un polynôme $P = \prod_{i=1}^{m} (X - \ell_i)$ (où les ℓ_i sont deux à deux distincts), alors $\mathsf{Ker}\left(P(f)\right) = \bigoplus_{i=1}^{m} \mathsf{Ker}\left(P_i(f)\right)$ où $P_i = X - \ell_i$, de sorte que $V = \bigoplus_{i=1}^{m} V_{(i)}$ avec $f_{|V_{(i)}} = \ell_i \operatorname{Id}_{V_{(i)}}$ et f est diagonalisable. □

On suppose désormais que le corps K contient les valeurs propres de f (c'est le cas lorsque K est algébriquement clos). Le polynôme χ_f est scindé : écrivons $\chi_f(X) = \prod_{i=1}^{n} (X - \lambda_i)^{d_i}$. On pose

$$V(\lambda_i) = \mathsf{Ker}\left((f - \lambda_i \operatorname{Id}_V)^{d_i}\right)$$

qu'on appelle le **sous-espace caractéristique** de f pour la valeur propre λ_i. Il est stable par tout endomorphisme de V qui commute à f (en effet, si $fg = gf$ et $v \in V(\lambda_i)$, on a $(f - \lambda_i \operatorname{Id}_{V(\lambda_i)})^{d_i}(g(v)) = g((f - \lambda_i \operatorname{Id}_{V(\lambda_i)})^{d_i}(v)) = 0$ et donc $g(v) \in V(\lambda_i)$).

Théorème 1.5.23. (Décomposition de Dunford). On a $V = \bigoplus_{i=1}^{n} V(\lambda_i)$ et il existe $\delta, \nu \in \mathsf{End}_K(V)$ uniques tels que
(1) $f = \delta + \nu$;
(2) δ est diagonalisable et ν est nilpotent ;
(3) $\delta\nu = \nu\delta$.
Pour tout $i \in \{1, \dots, n\}$, on a $\dim_K(V(\lambda_i)) = d_i$ et la restriction de δ à $V(\lambda_i)$ est $\lambda_i \operatorname{Id}_{V(\lambda_i)}$.

Démonstration. Pour $i \in \{1, \dots, n\}$, posons $P_i = (X - \lambda_i)^{d_i}$. Comme $\chi_f = \prod_{i=1}^{n} P_i$ et comme les P_i sont deux à deux premiers entre eux, le lemme des noyaux (lemme 1.5.21) implique que $\mathsf{Ker}\left(\chi_f(f)\right) = \bigoplus_{i=1}^{n} \mathsf{Ker}\left(P_i(f)\right)$. Mais $\mathsf{Ker}\left(\chi_f(f)\right) = V$ en vertu du théorème de Cayley-Hamilton (corollaire 1.5.11), et $\mathsf{Ker}\left(P_i(f)\right) = V(\lambda_i)$ pour $i \in \{1, \dots, n\}$: on a bien $V = \bigoplus_{i=1}^{n} V(\lambda_i)$.
Existence de la décomposition : Soit δ l'unique endomorphisme de V dont la restriction à $V(\lambda_i)$ est $\lambda_i \operatorname{Id}_{V(\lambda_i)}$ pour $i \in \{1, \dots, n\}$. L'endomorphisme δ est diagonalisable par construction. Posons $\nu = f - \delta$.

Le sous-espace $V(\lambda_i)$ est stable par f, et les endomorphismes $\delta_{|V(\lambda_i)} = \lambda_i \operatorname{Id}_{V(\lambda_i)}$ et $f_{|V(\lambda_i)}$ commutent *i.e.* f et δ commutent sur $V(\lambda_i)$. Comme $V = \bigoplus_{i=1}^{n} V(\lambda_i)$, les endomorphismes f et δ commutent. Il en résulte que δ et $\nu = f - \delta$ commutent. Par ailleurs, on a $\nu_{|V(\lambda_i)} = f_{|V(\lambda_i)} - \delta_{|V(\lambda_i)} = f_{|V(\lambda_i)} - \lambda_i \operatorname{Id}_{V(\lambda_i)}$, de sorte que $\nu_{V(\lambda_i)}^{d_i} = (f_{V(\lambda_i)} - \lambda_i \operatorname{Id}_{V(\lambda_i)})^{d_i} = (f - \lambda_i \operatorname{Id}_V)_{V(\lambda_i)}^{d_i} = 0$ par définition de $V(\lambda_i)$. Il en résulte que $\nu_{V(\lambda_i)}$ est nilpotent pour $i \in \{1, \dots, n\}$, et donc que ν est nilpotent.

Unicité de la décomposition : Soient $\delta', \nu' \in \mathsf{End}_K(V)$ avec δ' diagonalisable, ν' nilpotent, tels que $f = \delta' + \nu'$ et $\delta'\nu' = \nu'\delta'$. Comme δ' commute à $f = \delta' + \nu'$, il laisse stable $V_{(\lambda_i)}$ pour tout $i \in \{1, \dots, n\}$. Mais comme $\delta_{|V(\lambda_i)} = \lambda_i \operatorname{Id}_{V(\lambda_i)}$, les endomorphismes $\delta'_{|V(\lambda_i)}$ et $\delta_{|V(\lambda_i)}$ commutent *i.e.* δ' et δ commutent sur $V(\lambda_i)$. Comme $V = \bigoplus_{i=1}^{n} V(\lambda_i)$, les endomorphismes δ' et δ commutent. Il en résulte que δ' commute aussi à $\nu = f - \delta$. Mais comme f commute à δ et à ν, il en est de même de $\nu' = f - \delta'$: bref, les endomorphismes $f, \delta, \delta', \nu, \nu'$ commutent deux à deux. On a alors $\delta' - \delta = \nu - \nu'$. Comme ν et ν' commutent et sont nilpotents, l'endomorphisme $\nu - \nu'$ est nilpotent. Il en est donc de même de $\delta' - \delta$. Soit $i \in \{1, \dots, n\}$. Comme δ' est diagonalisable, il est annulé par un polynôme à racines simples : il en est de même de $\delta'_{|V(\lambda_i)}$ (rappelons que $V(\lambda_i)$ est stable par δ'). On a donc $V(\lambda_i) = \bigoplus_{j=1}^{n_i} V_{i,j}$ avec $\delta_{|V_{i,j}} = \lambda'_{i,j} \operatorname{Id}_{V_{i,j}}$. Mézalor $(\delta' - \delta)_{V_{i,j}} = \lambda'_{i,j} \operatorname{Id}_{V_{i,j}} - \lambda_i \operatorname{Id}_{V_{i,j}}$ est nilpotent : on a nécessairement $\lambda'_{i,j} = \lambda_i$ (et donc $n_i = 1$), de sorte que $\delta'_{V(\lambda_i)} = \delta_{V(\lambda_i)}$. Comme $V = \bigoplus_{i=1}^{n} V(\lambda_i)$, on a donc$\delta' = \delta$, et donc $\nu' = f = \delta' = \nu$.

Comme $V = \bigoplus_{i=1}^{n} V(\lambda_i)$ est respectée par f, on a $\chi_f = \prod_{i=1}^{n} \chi_{f_{|V(\lambda_i)}}$. Mais $f_{|V(\lambda_i)} = \lambda_i \operatorname{Id}_{V(\lambda_i)} + \nu_{|V(\lambda_i)}$ avec $\nu_{|V(\lambda_i)}$ nilpotent, de sorte que $\chi_{f_{|V(\lambda_i)}} = (X - \lambda_i)^{\dim_K(V(\lambda_i))}$. On a donc $\dim_K(V(\lambda_i)) = d_i$ pour tout $i \in \{1, \dots, n\}$. □

Proposition 1.5.24. Pour $i \in \{1, \dots, n\}$, notons π_i désigne le projecteur de V sur $V(\lambda_i)$ parallèlement à $\bigoplus_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} V(\lambda_j)$. Alors

(1) $\bigoplus_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} V(\lambda_j) = \mathsf{Ker}(\pi_i) = \mathsf{Im}\left((f - \lambda_i \operatorname{Id}_V)^{d_i}\right)$;

(2) $\delta, \nu, \pi_i \in K[f]$, *i.e.* δ, ν et les π_i peuvent s'exprimer comme des polynômes en f.

Démonstration. Comme les polynômes $(X - \lambda_i)^{d_i}$ et $\prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (X - \lambda_j)^{d_j}$ sont premiers entre eux, il existe $U_i, V_i \in K[X]$ tels que $(X - \lambda_i)^{d_i} U_i + V_i \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (X - \lambda_j)^{d_j} = 1$. Posons $P_i = V_i \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} (X - \lambda_j)^{d_j}$. On a $\chi_f | (X - \lambda_i)^{d_i} P_i$, de sorte que $(f - \lambda_i \operatorname{Id}_V)^{d_i} P_i(f) = 0$ (en vertu du théorème de Cayley-Hamilton, *cf* corollaire 1.5.11) : pour tout $v \in V$, on a $P_i(f)(v) \in \mathsf{Ker}\left((f - \lambda_i)^{d_i}\right) = V(\lambda_i) = \mathsf{Im}(\pi_i)$. De même, on a $(f - \lambda_i \operatorname{Id}_V)^{d_i} U_i(f)(v) \in \mathsf{Ker}(\pi_i)$. Mais comme $v = P_i(f)(v) + (f - \lambda_i \operatorname{Id}_V)^{d_i} U_i(f)(v)$, on a donc $P_i(f)(v) = \pi_i(v)$ et $(f - \lambda_i \operatorname{Id}_V)^{d_i} U_i(f)(v) = v - \pi_i(v)$. Ainsi $\pi_i = P_i(f) \in K[f]$ et $\mathsf{Ker}(\pi_i) \subseteq \mathsf{Im}\left((f - \lambda_i \operatorname{Id}_V)^{d_i}\right)$. Mais comme

$$\begin{aligned} \dim_K\left(\mathsf{Ker}(\pi_i)\right) = \dim_K(V) - \dim_K\left(\mathsf{Im}(\pi_i)\right) &= \dim_K(V) - \dim_K\left(\mathsf{Ker}\left((f - \lambda_i \operatorname{Id}_V)^{d_i}\right)\right) \\ &= \dim_K\left(\mathsf{Im}\left((f - \lambda_i \operatorname{Id}_V)^{d_i}\right)\right) \end{aligned}$$

on a en fait $\mathsf{Ker}(\pi_i) = \mathsf{Im}\left((f - \lambda_i \operatorname{Id}_V)^{d_i}\right)$.

Enfin, on a $\delta = \sum_{i=1}^{n} \lambda_i \pi_i$ et $\nu = f = \delta$, de sorte que $\delta, \nu \in K[f]$. □

Pour $i \in \{1, \dots, n\}$, soit $V(\lambda_i) = \bigoplus_{j=1}^{m_i} V_{i,j}$ une décomposition de Jordan de l'endomorphisme $\nu_{|V(\lambda_i)}$ (*cf* corollaire 1.5.13). Posons $d_{i,j} = \dim_K(V_{i,j})$.

Proposition 1.5.25. On a $\dim_K\left(\mathcal{C}(f)\right) = \dim_K(V) + 2 \sum_{i=1}^{n} \sum_{j=1}^{m_i} (m_i - j) d_{i,j}$.

Démonstration. Si $g \in \mathsf{End}_K(V)$ commute à f, alors les sous-espaces caractéristiques de f sont stables par g : on a $\mathcal{C}(f) = \mathsf{End}_{K[X]}(V_f) \simeq \bigoplus_{i=1}^{n} \mathsf{End}_{K[X]}(V(\lambda_i)) = \bigoplus_{i=1}^{n} \mathcal{C}(f_{|V(\lambda_i)})$. Pour $i \in \{1, \dots, n\}$, on a $\mathcal{C}(f_{|V(\lambda_i)}) = \mathsf{End}_{K[X]}(V_{f_{V(\lambda_i)}}) \simeq \bigoplus_{1 \leqslant j_1, j_2 \leqslant m_i} \mathsf{Hom}_{K[X]}(V_{i,j_1}, V_{i,j_2})$. Comme

$$\dim_K(\mathsf{Hom}_{K[X]}(V_{i,j_1}, V_{i,j_2})) = \min(d_{i,j_1}, d_{i,j_2})$$

d'après le lemme 1.5.17, on a

$$\dim_K\left(\mathcal{C}(f)\right) = \sum_{i=1}^{n} \sum_{j=1}^{m_i} (2(m_i - j) + 1) d_{i,j} = \dim_K(V) + 2 \sum_{i=1}^{n} \sum_{j=1}^{m_i} (m_i - j) d_{i,j}$$

vu que $\sum_{i=1}^{n} \sum_{j=1}^{m_i} d_{i,j} = \sum_{i=1}^{n} d_i = \dim_K(V)$. □

Remarque 1.5.26. On retrouve le fait que $\dim_K\left(\mathcal{C}(f)\right) \geqslant \dim_K(V)$ (proposition 1.5.20). Par ailleurs, on a égalité si et seulement si pour tout $i \in \{1, \dots, n\}$ on a $m_i = 1$, c'est-à-dire si et seulement si tous les sous-espaces propres de f sont de dimension 1, c'est une nouvelle caractérisation des endomorphismes cycliques (*cf* proposition 1.5.20).

2. Représentations linéaires des groupes finis

Dans tout ce qui suit, G est un groupe fini et K un corps (souvent $\mathbf{C}$ dans la pratique).

2.1. Définitions, premières propriétés.

Définition 2.1.1. Une **représentation linéaire** de G (sur K) est un K-espace espace vectoriel V muni d'une action linéaire de G. Cela équivaut à la donnée d'un morphisme de groupes $\rho\colon G \to \mathsf{GL}(V)$. Le **degré** de V est $\dim_K(V) \in \mathbf{N} \cup \{\infty\}$.

Exemple 2.1.2. Soit X un ensemble muni d'une action de G. La **représentation de permutation** associée est $V_X := \bigoplus_{x\in X} Ke_x$ où l'action de G sur V_X est donnée par $g(e_x) = e_{g.x}$. Le morphisme de groupes associé est le composé $G \to \mathfrak{S}_X \to \mathsf{GL}(V_X)$ où $\mathfrak{S}_X \to \mathsf{GL}(V_X)$ est le morphisme naturel (permutation des vecteurs de base).
Lorsque $X = \{*\}$, on obtient le **caractère trivial** $\rho_0 \colon G \to K^\times$; $g \mapsto 1$.
Lorsque $X = G$ muni de l'action de G par translation à gauche, on obtient la **représentation régulière** $K[G] = \bigoplus_{g\in G} Ke_g$.

Remarque 2.1.3. • Comme souvent, on désignera souvent une représentation (V, ρ) par le K-espace vectoriel sous-jacent V.
• La représentation régulière $K[G]$ est naturellement un anneau (commutatif si et seulement si G l'est). La multiplication est donnée par $\left(\sum_{g\in G} \lambda_g e_g\right)\left(\sum_{\gamma\in G} \mu_\gamma e_\gamma\right) = \sum_{g\in G}\left(\sum_{\gamma\in G} \lambda_{g\gamma^{-1}}\mu_\gamma\right) e_g$.
• La donnée d'une représentation (V, ρ) équivaut à celle d'un $K[G]$-module. En effet, si M est un $K[G]$-module, l'application $\rho\colon G \to \mathsf{End}(M)$ qui envoie $g \in G$ sur la multiplication à gauche par g est à valeurs dans $\mathsf{GL}(M)$ (car tout $g \in G$ est inversible) et c'est un morphisme de groupes, *i.e.* une représentation. Réciproquement, si $a = \sum_{g\in G} \lambda_g e_g \in K[G]$ et $v \in V$, la loi $(a, v) \mapsto av = \sum_{g\in G} \lambda_g g.v$ munit V d'une structure de $K[G]$-module.

Exercice 2.1.4. Montrer que que $K[\mathbf{Z}/n\,\mathbf{Z}] \simeq K[X]/X^nK[X]$, décrire $K[\mathfrak{S}_3]$.

Dans tout ce qui suit, on se restreint aux représentations de degré *fini*.

Remarque 2.1.5. Si $\#G = n$ et $\rho\colon G \to \mathsf{GL}(V)$ est une représentation, on a $\rho(g)^n = \rho(g^n) = \mathrm{Id}_V$ pour tout $g \in G$. Il en résulte que $\rho(g)$ admet $X^n - 1$ comme polynôme annulateur. Si K est algébriquement clos et n est premier à la caractéristique de K (c'est le cas lorsque $K = \mathbf{C}$), alors $X^n - 1$ est scindé à racines simples dans K, et $\rho(g)$ est diagonalisable, à valeurs propres des racines n-ièmes de l'unité.

Opérations sur les représentations. Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations. Alors on dispose des représentations suivantes :
- la somme directe $(V_1 \oplus V_2, \rho_1 \oplus \rho_2)$: l'action est donnée par $g.(v_1, v_2) = (g.v_1, g.v_2)$;
- le produit tensoriel $(V_1 \otimes V_2, \rho_1 \otimes \rho_2)$: l'action est donnée par $g.(v_1 \otimes v_2) = g.v_1 \otimes g.v_2$;
- $(\mathsf{Hom}_K(V_1, V_2), \rho)$ où $\rho(g)(f) = \rho_2(g) \circ f \circ \rho_1(g)^{-1}$, *i.e.* $(g.f)(v) = g.f(g^{-1}.v)$ pour $f \in \mathsf{Hom}_K(V_1, V_2)$ et $g \in G$;
- la représentation duale $V^\vee = \mathsf{Hom}_K(V, K)$: c'est un cas particulier du précédent, avec $V_2 = K$ la représentation triviale (la représentation ainsi obtenue s'appelle aussi **contragrédiente**).

Remarque 2.1.6. Soit (V, ρ) une représentation et $n \in \mathbf{N}_{>0}$: on dispose de la représentation $V^{\otimes n}$ (donnée par l'action diagonale comme expliqué ci-dessus). Si $\mathsf{car}(K) = 0$, les puissances symétrique et extérieure $\mathsf{Sym}^n(V)$ et $\mathsf{Alt}^n(V)$ s'identifient aux sous-K-espaces vectoriels de $V^{\otimes n}$ constitués des invariants et des anti-invariants de $V^{\otimes n}$ sous l'action naturelle du groupe $\mathfrak{S}_n$. Ils sont stables sous l'action de G, ce qui fournit deux nouvelles représentations, encore notées $\mathsf{Sym}^n(V)$ et $\mathsf{Alt}^n(V)$.
On a un isomorphisme de représentations $V^{\otimes 2} = \mathsf{Sym}^2(V) \oplus \mathsf{Alt}^2(V)$.

Définition 2.1.7. Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations. Une application $f \in \mathsf{Hom}_K(V_1, V_2)$ est (G-)**équivariante** si $f \circ \rho_1(g) = \rho_2(g) \circ f$ pour tout $g \in G$. L'ensemble des applications équivariantes $V_1 \to V_2$ n'est autre que le K-espace vectoriel $\mathsf{Hom}_G(V_1, V_2) := \mathsf{Hom}_K(V_1, V_2)^G = \mathsf{Hom}_{K[G]}(V_1, V_2)$.

Exercice 2.1.8. Montrer que $\mathsf{Hom}_K(V_1, V_2) \simeq V_1^\vee \otimes_K V_2$.

Définition 2.1.9. • Une **sous-représentation** d'une représentation V est un sous-K-espace vectoriel $W \subset V$ stable sous l'action de G, *i.e.* tel que $(\forall w \in W)\,(\forall g \in G)\, g.w \in W$.
• Une représentation V est **irréductible** si $V \neq \{0\}$ et ses seules sous-représentations sont $\{0\}$ et V.

Théorème 2.1.10. (Maschke) Supposons $\mathsf{pgcd}(\#G, \mathsf{car}(K)) = 1$. Soient V une représentation et $W \subset V$ une sous-représentation. Alors W admet un supplémentaire stable par G.

Démonstration. Soit p_0 n'importe quel projecteur de V tel que $\mathsf{Im}(p_0) = W$ (le choix d'un tel p_0 équivaut à celui d'un supplémentaire de W dans V). Posons $p = \frac{1}{\#G}\sum_{g\in G} \rho(g) \circ p_0 \circ \rho(g)^{-1} \in \mathsf{End}(V)$ (c'est licite puisque $\mathsf{pgcd}(\#G, \mathsf{car}(K)) = 1$). Par construction $\rho(g) \circ p = p \circ \rho(g)$ pour tout $g \in G$. Comme $\mathsf{Im}(p_0) = W$ est stable par G, on a $\mathsf{Im}(p) \subset W$. Enfin, si $w \in W$, on a $\rho(g)^{-1}(w) \in W$ (car W est stable par G), donc $p_0(\rho(g)^{-1}(w)) = \rho(g)^{-1}(w)$ et $(\rho(g) \circ p_0 \circ \rho(g)^{-1})(w) = w$, d'où $p(w) = w$ et $\mathsf{Im}(p) = W$. Cela implique que $p^2 = p$, de sorte que p est un projecteur. Ainsi, p est un projecteur G-équivariant de V d'image W : on a $V = W \oplus \mathsf{Ker}(p)$ et $\mathsf{Ker}(p)$ est un supplémentaire de W stable par G. □

Corollaire 2.1.11. (Complète réductibilité des représentations). Si $\mathsf{pgcd}(\#G, \mathsf{car}(K)) = 1$, toute représentation est somme directe de représentations irréductibles.

Remarque 2.1.12. (1) Il n'y a pas unicité dans la décomposition (exemple : V représentation triviale de dimension > 1).
(2) C'est faux si $\mathsf{pgcd}(\#G, \mathsf{car}(K)) \neq 1$. Par exemple, si $K = \mathbf{F}_p$, $G = \mathbf{Z}/p\,\mathbf{Z}$, $V = K[G]$ est la représentation régulière et $W = \big\{ \sum_{g\in G} \lambda_g e_g \,\big|\, \sum_{g\in G} \lambda_g = 0 \big\}$.
(3) En termes de $K[G]$-modules, le théorème 2.1.10 signifie que lorsque $\mathsf{pgcd}(\#G, \mathsf{car}(K)) = 1$ (en particulier quand $\mathsf{car}(K) = 0$), tout sous-$K[G]$-module d'un $K[G]$-module est **facteur direct**, *i.e.* admet un supplémentaire (comme $K[G]$-module). C'est totalement faux en général si $K[G]$ est remplacé par un anneau quelconque, par exemple dans le cas élémentaire des $\mathbf{Z}$-modules ($2\,\mathbf{Z} \subset \mathbf{Z}$ n'a pas de supplémentaire).

Théorème 2.1.13. (Lemme de Schur) Supposons K algébriquement clos. Soient (V_1, ρ_1) et (V_2, ρ_2) deux représentations *irréductibles* et $f \in \mathsf{Hom}_G(V_1, V_2)$. On a l'alternative suivante :
- si V_1 et V_2 ne sont pas isomorphes, alors $f = 0$;
- si $V_1 = V_2$ (comme représentations), alors f est une homothétie.

Démonstration. • Supposons $f \neq 0$. Comme $\mathsf{Ker}(f)$ est un sous-espace de V_1 stable par G, on a $\mathsf{Ker}(f) = \{0\}$ ou $\mathsf{Ker}(f) = V_1$ (parce que V_1 est irréductible) : comme $f \neq 0$, on a $\mathsf{Ker}(f) = \{0\}$. De même, $\mathsf{Im}(f)$ est un sous-espace de V_2 stable par G, on a $\mathsf{Im}(f) = \{0\}$ ou $\mathsf{Im}(f) = V_2$ (parce que V_2 est irréductible) : comme $f \neq 0$, on a $\mathsf{Im}(f) = V_2$. Ainsi f est un isomorphisme (de représentations de G).
• Supposons maintenant $V_1 = V_2$. Comme K est algébriquement clos, f admet au moins une valeur propre λ. Alors le sous-espace propre associé $W = \mathsf{Ker}(f - \lambda \operatorname{Id}_{V_1}) \neq \{0\}$ est stable par G. Comme V_1 est irréductible, on a nécessairement $W = V_1$ et $f = \lambda \operatorname{Id}_{V_1}$ est une homothétie. □

Remarque 2.1.14. Les théorèmes 2.1.10 et 2.1.13 impliquent que la « catégorie » des représentations d'un groupe fini sur un corps algébriquement clos de caractéristique 0 est particulièrement simple, et que les représentations irréductibles sont en quelque sorte ses « atomes ». Ceci sera grandement précisé dans le numéro suivant.

2.2. **Théorie des caractères.** On suppose désormais que $K = \mathbf{C}$ (la théorie marcherait de façon essentiellement identique sur n'importe quel corps algébriquement clos de caractéristique 0).

Définition 2.2.1. Soit (V, ρ) une représentation. Son **caractère** est l'application

$$\chi_V : G \to \mathbf{C}$$
$$g \mapsto \mathsf{Tr}(\rho(g))$$

Comme son nom l'indique, elle caractérise la représentation, comme nous allons le voir.

Proposition 2.2.2. (1) Si (V, ρ) est une représentation, on a $\chi_V(1) = \dim_{\mathbf{C}}(V)$, $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ et $\chi_V(g^{-1}hg) = \chi_V(h)$ pour tout $g, h \in G$.
(2) Si (V_1, ρ_1) et (V_2, ρ_2) sont deux représentations, on a $\chi_{V_1 \oplus V_2} = \chi_{V_1} + \chi_{V_2}$, $\chi_{V_1 \otimes V_2} = \chi_{V_1} \cdot \chi_{V_2}$ et $\chi_{\mathsf{Hom}(V_1, V_2)} = \overline{\chi}_{V_1} \cdot \chi_{V_2}$.
(3) Si (V, ρ) est une représentation, on a $\chi_{\mathsf{Sym}^2(V)}(g) = \frac{1}{2}\big(\chi_V(g)^2 + \chi_V(g^2)\big)$ et $\chi_{\mathsf{Alt}^2(V)}(g) = \frac{1}{2}\big(\chi_V(g)^2 - \chi_V(g^2)\big)$ pour tout $g \in G$.

Démonstration. (1) On a $\rho(1) = \operatorname{Id}_V$, donc $\chi_V(1) = \mathsf{Tr}(\operatorname{Id}_V) = \dim_{\mathbf{C}}(V)$. D'après la remarque 2.1.5, si $g \in G$, l'endormorphisme $\rho(g)$ est diagonalisable à valeurs propres des racines de l'unité, donc $\mathsf{Tr}(\rho(g)^{-1}) = \overline{\mathsf{Tr}(\rho(g))}$. Enfin, on a $\rho(g^{-1}hg) = \rho(g)^{-1}\rho(h)\rho(g)$ est semblable à $\rho(h)$: ils ont même trace, *i.e.* $\chi_V(g^{-1}hg) = \chi_V(h)$.
(2) D'après la remarque 2.1.5 encore, si $g \in G$, il existe une base $\mathfrak{B}_1 = (e_i)_{1\leqslant i\leqslant n}$ (resp. $\mathfrak{B}_2 = (f_j)_{1\leqslant j\leqslant m}$) de V_1 (resp. V_2) dans laquelle la matrice de $\rho_1(g)$ (resp. $\rho_2(g)$) est $\mathsf{diag}(\lambda_1, \dots, \lambda_n)$ (resp. $\mathsf{diag}(\mu_1, \dots, \mu_m)$). La matrice de $\rho_1(g) \oplus \rho_2(g)$ dans la base $\mathfrak{B}_1 \cup \mathfrak{B}_2$ est alors $\mathsf{diag}(\lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_m)$, dont la trace est $\lambda_1 + \cdots + \lambda_n + \mu_1 + \cdots + \mu_m = \mathsf{Tr}(\rho_1(g)) + \mathsf{Tr}(\rho_2(g))$. De même, la matrice de $\rho_1(g) \otimes \rho_2(g)$ dans la base $\mathfrak{B}_1 \otimes \mathfrak{B}_2$ est $\mathsf{diag}(\lambda_i\mu_j)_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}}$, ce qui implique que $\mathsf{Tr}(\rho_1(g) \otimes \rho_2(g)) = \sum_{i=1}^n \sum_{j=1}^m \lambda_i\mu_j = \mathsf{Tr}(\rho_1(g))\,\mathsf{Tr}(\rho_2(g))$.
Enfin, la matrice de l'action de g dans la base $(e_i^* \otimes f_j)$ est $\mathsf{diag}(\lambda_i^{-1}\mu_j = \overline{\lambda}_i\mu_j)_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}}$, dont la trace est $\sum_{i=1}^n \sum_{j=1}^m \overline{\lambda}_i\mu_j = \overline{\mathsf{Tr}(\rho_1(g))}\,\mathsf{Tr}(\rho_2(g))$.
(3) Plaçons-nous dans une base $(e_1, \dots, e_n)$ de V dans laquelle la matrice de $\rho(g)$ est $\mathsf{diag}(\lambda_1, \dots, \lambda_n)$. Alors $(e_i \cdot e_j)_{1\leqslant i\leqslant j\leqslant n}$ (resp. $(e_i \wedge e_j)_{1\leqslant i<j\leqslant n}$) est une base de $\mathsf{Sym}^2(V)$ (resp. $\mathsf{Alt}^2(V)$) dans laquelle l'action de

$\mathsf{Sym}^2(\rho)$ (resp. $\mathsf{Alt}^2(\rho)$) est diagonale, à coefficients diagonaux $(\lambda_i\lambda_j)_{1\leqslant i\leqslant j\leqslant n}$ (resp. $(\lambda_i\lambda_j)_{1\leqslant i<j\leqslant n}$). On a donc $\chi_{\mathsf{Sym}^2(V)}(g) = \sum_{1\leqslant i\leqslant j\leqslant n}\lambda_i\lambda_j = \frac{1}{2}\big(\chi_V(g)^2 + \chi_V(g^2)\big)$ et $\chi_{\mathsf{Alt}^2(V)}(g) = \sum_{1\leqslant i<j\leqslant n}\lambda_i\lambda_j = \frac{1}{2}\big(\chi_V(g)^2 - \chi_V(g^2)\big)$, puisque $\chi_V(g)^2 = (\lambda_1+\cdots+\lambda_n)^2$ et $\chi_V(g^2) = \lambda_1^2+\cdots+\lambda_n^2$. □

2.2.3. *Relations d'othogonalité.*

Notation. Si $f_1, f_2 \in \mathscr{F}(G,\mathbf{C})$, on pose

$$\langle f_1|f_2\rangle = \tfrac{1}{\#G}\sum_{g\in G}\overline{f_1(g)}f_2(g) \in \mathbf{C}$$

Cela munit $\mathscr{F}(G,\mathbf{C})$ d'un produit scalaire hermitien.

Lemme 2.2.4. Soient (V,ρ) une représentation et χ son caractère. Alors $p_V := \frac{1}{\#G}\sum_{g\in G}\rho(g)$ est un projecteur G-équivariant dont l'image est V^G. En particulier, on a $\dim_{\mathbf{C}}(V^G) = \mathsf{Tr}(p_V) = \langle 1|\chi\rangle$.

Démonstration. Si $g\in G$, on a $\rho(g)\circ p_V = p_V\circ\rho(g) = p_V$, ce qui prouve l'équivariance et $\mathsf{Im}(p_V)\subset V^G$. De plus, si $v\in V^G$, on a $p_V(v) = v$, ce qui montre que $\mathsf{Im}(p_V) = V^G$ et que p_V est un projecteur. □

Théorème 2.2.5. Les caractères des représentations irréductibles de G forment une famille orthonormale de $\mathscr{F}(G,\mathbf{C})$: si V_1 et V_2 sont deux représentations irréductibles, on a

$$\langle\chi_{V_1}|\chi_{V_2}\rangle = \begin{cases}1 & \text{si } V_1\simeq V_2\\ 0 & \text{sinon}\end{cases}$$

Démonstration. On considère la représentation $V = \mathsf{Hom}_{\mathbf{C}}(V_1,V_2)$: son caractère est $\overline{\chi}_{V_1}\chi_{V_2}$. D'après le lemme 2.2.4, on a $\dim_{\mathbf{C}}(V^G) = \langle 1|\overline{\chi}_{V_1}\chi_{V_2}\rangle = \langle\chi_{V_1}|\chi_{V_2}\rangle$. Le théorème résulte donc du lemme de Schur (*cf* théorème 2.1.13). □

Définition 2.2.6. (1) On appelle **caractère irréductible** le caractère d'un représentation irréductible de G.
(2) Une fonction $f\colon G\to\mathbf{C}$ est dite **centrale** si elle est constante sur les classes de conjugaison de G. Les fonctions centrales forment un sous-espace vectoriel $\mathscr{F}_c(G,\mathbf{C})$ de $\mathscr{F}(G,\mathbf{C})$, de dimension le nombre n_G de classes de conjugaison dans G. D'après la proposition 2.2.2 (1), si (V,ρ) est une représentation, on a $\chi_V\in\mathscr{F}_c(G,\mathbf{C})$.

Corollaire 2.2.7. (1) Le nombre de (classes d'isomorphisme de) représentations irréductibles de G est fini, inférieur à n_G.
(2) Toute représentation V est déterminée à isomorphisme près par son caractère χ_V : si $V_1,\dots,V_k$ forment une famille complète de représentants des classes d'isomorphisme des représentations irréductibles de G, on a $V\simeq\bigoplus_{i=1}^k V_i^{\langle\chi_V|\chi_{V_i}\rangle}$.
(3) Un caractère χ est irréductible si et seulement si $\langle\chi|\chi\rangle = 1$.

Démonstration. (1) Résulte du théorème 2.2.5 et de $\dim_{\mathbf{C}}(\mathscr{F}_c(G,\mathbf{C})) = n_G$.
(2) D'après le théorème de Maschke (*cf* théorème 2.1.10), on a $V\simeq\bigoplus_{i=1}^k V_i^{m_i}$: on a alors $\chi_V = \sum_{i=1}^k m_i\chi_{V_i}$, de sorte que $m_i = \langle\chi_V|\chi_{V_i}\rangle$: les multiplicités ne dépendent que de χ_V.
(3) Résulte de (2). □

2.2.8. *Décomposition de la représentation régulière et conséquences.* Dans ce qui suit on note χ le caractère de la représentation régulière $\mathbf{C}[G]$. Si $g\in G\backslash\{1\}$, alors g agit sans point fixe sur G : on a

$$\chi(g) = \begin{cases}\#G & \text{si } g = 1\\ 0 & \text{si } g\neq 1\end{cases}$$

Proposition 2.2.9. On a $\mathbf{C}[G]\simeq\bigoplus_{i=1}^k V_i^{\dim_{\mathbf{C}}(V_i)}$ où $V_1,\dots,V_k$ sont « les » représentations irréductibles de G.

Démonstration. Pour $i\in\{1,\dots,k\}$, la multiplicité de V_i dans $\mathbf{C}[G]$ est $\langle\chi|\chi_{V_i}\rangle = \frac{1}{\#G}\sum_{g\in G}\overline{\chi(g)}\chi_{V_i}(g) = \chi_{V_i}(1) = \dim_{\mathbf{C}}(V_i)$. □

Corollaire 2.2.10. On a $\#G = \sum_{i=1}^k(\dim_{\mathbf{C}}(V_i))^2$ et $\sum_{i=1}^k\dim_{\mathbf{C}}(V_i)\chi_{V_i}(g) = 0$ si $g\neq 1$.

Démonstration. D'après la proposition 2.2.9, on a $\chi = \sum_{i=1}^{k} \dim_{\mathbf{C}}(V_i)\chi_{V_i}$. Appliqué à $g = 1$, on en déduit $\#G = \sum_{i=1}^{k}(\dim_{\mathbf{C}}(V_i))^2$, appliqué à $g \neq 1$, on a $\sum_{i=1}^{k} \dim_{\mathbf{C}}(V_i)\chi_{V_i}(g) = 0$. □

Lemme 2.2.11. Soient $\alpha\colon G \to \mathbf{C}$ et (V,ρ) une représentation. Posons $\varphi_\alpha = \sum_{g\in G} \alpha(g)\rho(g)$. Alors α est centrale si et seulement si pour toute représentation, l'application φ_α est G-équivariante.

Démonstration. L'application φ_α est équivariante si et seulement si

$$(\forall h \in G)\, \rho(h)^{-1} \circ \varphi_\alpha \circ \rho(h) = \varphi_\alpha \Leftrightarrow (\forall h \in G) \sum_{g\in G} \alpha(g)\rho(h^{-1}gh) = \sum_{g\in G} \alpha(g)\rho(g)$$
$$\Leftrightarrow (\forall h \in G) \sum_{g\in G} \alpha(hgh^{-1})\rho(g) = \sum_{g\in G} \alpha(g)\rho(g) \quad (*)$$

C'est donc le cas lorsque α est centrale. Réciproquement, supposons que φ_α soit G-équivariante pour toute représentation (V,ρ). Appliquons l'égalité $(*)$ à la représentation régulière : on a $\sum_{g\in G} \alpha(hgh^{-1})e_g = \sum_{g\in G} \alpha(g)e_g \in \mathbf{C}[G]$ et donc $\alpha(hgh^{-1}) = \alpha(g)$ pour tout $g, h \in G$, *i.e.* α est centrale. □

Théorème 2.2.12. Soient $V_1, \ldots, V_k$ « les » représentations irréductibles de G. Alors $\{\chi_{V_1}, \ldots, \chi_{V_k}\}$ est une base orthonormale de $\mathscr{F}_c(G, \mathbf{C})$. En particulier, le nombre de (classes d'isomorphisme de) représentations irréductibles est égal au nombre de classes de conjugaison de G, soit encore $k = n_G$.

Démonstration. On sait déjà que $\{\chi_{V_1}, \ldots, \chi_{V_k}\}$ forment une famille orthogonale de $\mathscr{F}_c(G, \mathbf{C})$ (théorème 2.2.5). Il suffit de montrer que si $\alpha \in \mathscr{F}_c(G, \mathbf{C})$ est orthogonale à $\{\chi_{V_1}, \ldots, \chi_{V_k}\}$, alors $\alpha = 0$. D'après le lemme 2.2.11, l'application φ_α est G-équivariante pour toute représentation V. Lorsque V est irréductible, c'est une homothétie d'après le lemme de Schur (théorème 2.1.13) : on a $\varphi_\alpha = \lambda \operatorname{Id}_V$. On a alors $\lambda \dim_{\mathbf{C}}(V) = \mathsf{Tr}(\varphi_\alpha) = \sum_{g\in G} \alpha(g)\chi(g) = \#G\overline{\langle \alpha | \overline{\chi} \rangle} = 0$ par hypothèse sur α, ce qui implique $\lambda = 0$. Comme c'est vrai pour toute représentation irréductible, c'est vrai pour toute représentation en vertu du théorème de Maschke (*cf* théorème 2.1.10 et son corollaire). Appliqué à la représentation régulière, on en déduit que $\sum_{g\in G} \alpha(g)e_g = 0 \in \mathbf{C}[G]$, et donc $\alpha = 0$. □

Il en résulte que la théorie des représentations de G est entièrement décrite par sa **table des caractères** : soit $\{\chi_1, \ldots, \chi_k\}$ les caractères irréductibles et $\{C_1, \ldots, C_k\}$ ses classes de conjugaison.

	C_1	C_2	$\cdots$	C_k
χ_1	$\chi_1(C_1)$	$\chi_1(C_2)$	$\cdots$	$\chi_1(C_k)$
χ_2	$\chi_2(C_1)$	$\chi_2(C_2)$	$\cdots$	$\chi_2(C_k)$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$
χ_k	$\chi_k(C_1)$	$\chi_k(C_2)$	$\cdots$	$\chi_k(C_k)$

Proposition 2.2.13. La matrice $\left(\sqrt{\frac{\#C}{\#G}}\chi(C)\right)_{C,\chi}$ (où C parcourt les classes de conjugaison et χ les caractères irréductibles de G) est unitaire. En particulier, on a

$$\sum_{\chi} \overline{\chi(g)}\chi(h) = \begin{cases} 0 & \text{si } g \text{ et } h \text{ ne sont pas conjugués} \\ \frac{\#G}{\#C} & \text{si } g \text{ et } h \text{ ont même classe de conjugaison } C \end{cases}$$

Démonstration. Si χ_1 et χ_2 sont des caractères irréductibles, on a $\frac{1}{\#G}\sum_{g\in G} \overline{\chi_1(g)}\chi_2(g) = \delta_{\chi_1,\chi_2}$ (relations d'orthogonalité, *cf* théorème 2.2.5). Comme les caractères sont des fonctions centrales, cela signifie que $\frac{1}{\#G}\sum_C \#C\overline{\chi_1(C)}\chi_2(C) = \begin{cases} 1 & \text{si } \chi_1 = \chi_2 \\ 0 & \text{sinon} \end{cases}$, *i.e.* que la matrice $\left(\sqrt{\frac{\#C}{\#G}}\chi(C)\right)_{C,\chi}$ est unitaire. On a donc aussi $\sum_\chi \sqrt{\frac{\#C_1}{\#G}}\overline{\chi(C_1)}\sqrt{\frac{\#C_2}{\#G}}\chi(C_2) = \delta_{C_1,C_2}$, soit encore $\sum_\chi \overline{\chi(g)}\chi(h) = 0$ si g et h ne sont pas conjugués, et $\sum_\chi \overline{\chi(g)}\chi(h) = \frac{\#G}{\#C}$ si g et h ont même classe de conjugaison C. □

Corollaire 2.2.14. G est commutatif si et seulement si ses représentations irréductibles sont toutes de dimension 1.

Démonstration. Si G est commutatif, on a $n_G = \#G$, et donc $\#G = \sum_{i=1}^{\#G}(\dim_{\mathbf{C}}(V_i))^2$ (théorème 2.2.12 et corollaire 2.2.10). La réciproque est immédiate. □

Corollaire 2.2.15. Si H est un sous-groupe commutatif de G, alors toute représentation irréductible de G est de dimension $\leqslant [G : H]$.

Démonstration. Soient (V,ρ) une représentation irréductible de G, et W une sous-représentation irréductible de $\rho_{|H}$. On a $\dim_{\mathbf{C}}(W)=1$ d'après le corollaire 2.2.14. Soit $V'=\mathsf{Vect}_{\mathbf{C}}\{\rho(g)(W)\}_{g\in G}$. Comme V' est stable par G et V irréductible, on a $V'=V$. Par ailleurs, on a $g'\in gH\Rightarrow\rho(g')(W)=\rho(g)(W)$, de sorte que $V'=\mathsf{Vect}_{\mathbf{C}}\{\rho(g)(W)\}_{gH\in G/H}$: on a $\dim_{\mathbf{C}}(V)\leqslant\#(G/H)=[G:H]$. □

Exemple 2.2.16. Si $n\in\mathbf{N}_{\geqslant 3}$, le groupe diédral D_n est engendré par deux éléments r et s assujetis aux relations $r^n=s^2=e$ et $srs=r^{-1}$. Il n'est pas commutatif. Le sous-groupe $\langle r\rangle\subset D_n$ est cyclique (donc commutatif) d'indice 2 : les représentations irréductibles de D_n sont de dimension 1 ou 2.

Remarque 2.2.17. On peut montrer que $\dim_{\mathbf{C}}(V)^2\leqslant[G:\mathsf{Z}(G)]$ pour toute représentation irréductible V de G.

Proposition 2.2.18. Si (V,ρ) est une représentation irréductible de G, alors $\dim_{\mathbf{C}}(V)\mid\#G$.

Si $g\in G$, on note $C(g)$ la classe de conjugaison de g, et on pose $P(g)=\sum\limits_{h\in C(g)}e_h\in\mathbf{Z}[G]\subset\mathbf{C}[G]$ et $P_V(g)=\rho(P(g))=\sum\limits_{h\in C(g)}\rho(h)\in\mathsf{End}(V)$.

Lemme 2.2.19. On a $P_V(g)=\frac{\#C(g)}{\dim_{\mathbf{C}}(V)}\chi_V(g)\,\mathrm{Id}_V$.

Démonstration. Si $\gamma\in G$, on a $\rho(\gamma)^{-1}P_V(g)\rho(\gamma)=\sum\limits_{h\in C(g)}\rho(\gamma^{-1}h\gamma)=P_v(g)$, donc $P_V(g)\colon V\to V$ est G-équivariante. Comme V est irréductible, le lemme de Schur (*cf* théorème 2.1.13) implique qu'il existe $\lambda_g\in\mathbf{C}$ tel que $P_V(g)=\lambda_g\,\mathrm{Id}_V$. Il vient $\lambda_g\dim_{\mathbf{C}}(V)=\sum\limits_{h\in C(g)}(\mathsf{Tr}\circ\rho)(h)=\sum\limits_{h\in C(g)}\chi_V(h)=\#C(g)\chi_V(g)$ en prenant la trace. □

Lemme 2.2.20. Soit $X\in\mathbf{Q}$. Si x est racine d'un polynôme unitaire à coefficients entiers, alors $x\in\mathbf{Z}$.

Démonstration. Écrivons $x=\frac{a}{b}$ avec $a\in\mathbf{Z}$, $b\in\mathbf{N}_{>0}$ et $\mathsf{pgcd}(a,b)=1$. Par hypothèse, il existe $n\in\mathbf{N}$ et $a_1,\dots,a_n\in\mathbf{Z}$ tels que $x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$. Il vient $a^n+a_1a^{n-1}b+a_2a^{n-2}b^2+\cdots+a_nb^n=0$ (en multipliant par b^n), ce qui montre que $b\mid a^n$. Comme $\mathsf{pgcd}(a,b)=1$, on a nécessairement $b=1$, et donc $x=a\in\mathbf{Z}$. □

Démonstration de la proposition 2.2.18. Fixons $\{g_1,\dots,g_k\}\subset G$ un système complet de représentants des classes de conjugaison de G. Posons aussi $\widetilde{P}=\sum\limits_{i=1}^{k}\frac{\#G}{\#C(g_i)}P(g_i)P(g_i^{-1})$. Comme $\#C(g_i)\mid\#G$ (parce que la classe $C(g_i)$ est un G-ensemble transitif) et $P(g_i),P(g_i^{-1})\in\mathbf{Z}[G]$, on a $\widetilde{P}\in\mathbf{Z}[G]$.

De façon analogue, on pose aussi $\widetilde{P}_V=\rho(\widetilde{P})=\sum\limits_{i=1}^{k}\frac{\#G}{\#C(g_i)}P_V(g_i)P_V(g_i^{-1})$. Le lemme 2.2.19 appliqué à g_i et g_i^{-1} implique que $\widetilde{P}_V=\sum\limits_{i=1}^{k}\frac{\#G}{\#C(g_i)}\frac{\#C(g_i)}{\dim_{\mathbf{C}}(V)}\chi_V(g_i)\frac{\#C(g_i^{-1})}{\dim_{\mathbf{C}}(V)}\chi_V(g_i^{-1})\,\mathrm{Id}_V=\frac{\#G}{(\dim_{\mathbf{C}}(V))^2}\sum\limits_{i=1}^{k}\#C(g_i)\,|\chi_V(g_i)|^2\,\mathrm{Id}_V$ car $\#C(g_i^{-1})=\#C(g_i)$ et $\chi_V(g_i^{-1})=\overline{\chi_V(g_i)}$. On a $\sum\limits_{i=1}^{k}\#C(g_i)\,|\chi_V(g_i)|^2=\sum\limits_{g\in G}|\chi_V(g)|^2=\#G\langle\chi_V|\chi_V\rangle$ (parce que χ_V est une fonction centrale). Comme V est irréductible, on a $\langle\chi_V|\chi_V\rangle=1$ (*cf* théorème 2.2.5), ce qui montre que $\widetilde{P}_V=\left(\frac{\#G}{\dim_{\mathbf{C}}(V)}\right)^2\mathrm{Id}_V$.

Notons $R=\mathbf{C}[G]$ la représentation régulière, et posons $\widetilde{P}_R=\rho_R(\widetilde{P})$ (c'est l'endomorphisme de R induit par la multiplication par $\widetilde{P}$). Comme $\widetilde{P}\in\mathbf{Z}[G]$, la matrice de $\widetilde{P}_R$ dans la base $(e_g)_{g\in G}$ est à coefficients entiers : son polynôme caractéristique $f(X)$ est à coefficients entiers. Par ailleurs, la représentation R contient la représentation V. Cette dernière est stable par $\widetilde{P}_R$, qui induit $\widetilde{P}_V=\left(\frac{\#G}{\dim_{\mathbf{C}}(V)}\right)^2\mathrm{Id}_V$. Cela implique en particulier que $\left(\frac{\#G}{\dim_{\mathbf{C}}(V)}\right)^2$ est une valeur propre de $\widetilde{P}_R$: on a $f\left(\left(\frac{\#G}{\dim_{\mathbf{C}}(V)}\right)^2\right)=0$. Comme $f(X)$ est unitaire et $\left(\frac{\#G}{\dim_{\mathbf{C}}(V)}\right)^2\in\mathbf{Q}$, le lemme 2.2.20 implique que $\left(\frac{\#G}{\dim_{\mathbf{C}}(V)}\right)^2\in\mathbf{Z}$, et donc $\frac{\#G}{\dim_{\mathbf{C}}(V)}\in\mathbf{Z}$, *i.e.* $\dim(V)\mid\#G$. □

Corollaire 2.2.21. Si (V,ρ) est une représentation irréductible de G, alors $\dim_{\mathbf{C}}(V)\mid[G:\mathsf{Z}(G)]$.

Démonstration. Si $z\in\mathsf{Z}(G)$, alors $\rho(Z)\in\mathsf{End}_G(V)$: d'après le lemme de Schur (*cf* théorème 2.1.13), il existe $\lambda_z\in\mathbf{C}^\times$ tel que $\rho(z)=\lambda_z\,\mathrm{Id}_V$. L'application $\mathsf{Z}(G)\to\mathbf{C}^\times$; $z\mapsto\lambda_z$ est un morphisme de groupes. Si $k\in\mathbf{N}_{>0}$, on dispose de la représentation $V^{\boxtimes k}$ de G^k (*cf* 2.4.2). D'après la proposition 2.4.3, cette dernière est irréductible. Par ailleurs, le sous-groupe $H_k=\{(z_1,\dots,z_k)\in\mathsf{Z}(G)^k\mid z_1\cdots z_k=e\}\subset G^k$ agit trivialement : on en déduit une représentation irréductible de dimension $\dim_{\mathbf{C}}(V^{\boxtimes k})=(\dim_{\mathbf{C}}(V))^k$ de G^k/H_k. D'après

la proposition 2.2.18, l'entier $(\dim_{\mathbf{C}}(V))^k$ divise $\#(G^k/H_k) = \frac{\#G^k}{\#\,\mathsf{Z}(g)^{k-1}} = [G : \mathsf{Z}(G)]^k \#Z(G)$. Pour tout nombre premier p, on a donc $kv_p(\dim_{\mathbf{C}}(V)) \leqslant kv_p([G : \mathsf{Z}(G)]) + v_p(\#\,\mathsf{Z}(G))$. Comme c'est vrai pour tout $k \in \mathbf{N}_{>0}$, on a donc $v_p(\dim_{\mathbf{C}}(V)) \leqslant v_p([G : \mathsf{Z}(G)])$, et donc $\dim_{\mathbf{C}}(V) \mid [G : \mathsf{Z}(G)]$. □

2.3. **Restriction et induction.**

2.3.1. *Définition et premières propriétés.* Soit H un sous-groupe de G.

Définition 2.3.2. Si (V, ρ) est une représentation de G, alors $(V, \rho_{|H})$ est une représentation de H, appelée *restriction* de V à H. On la note $\mathsf{Res}^G_H(V)$.

Remarque 2.3.3. En général, la restriction d'une représentation irréductible de G n'est pas une représentation irréductible de H.

Réciroquement, soit W une représentation de H. D'après la remarque 2.1.3, cela équivaut à la donnée d'une structure de $\mathbf{C}[H]$-module sur W.

Définition 2.3.4. La représentation de G *induite* par W est

$$\mathsf{Ind}^G_H(W) := \mathbf{C}[G] \otimes_{\mathbf{C}[H]} W$$

(où on voit $\mathbf{C}[G]$ comme un $\mathbf{C}[H]$-module à gauche de la façon naturelle). C'est un $\mathbf{C}[G]$-module donc une représentation de G. L'action de G sur $\mathsf{Ind}^G_H(W)$ est donnée sur les tenseurs simples par $g \cdot (e_{g'} \otimes w) = e_{gg'} \otimes w$ pour $g, g' \in G$ et $w \in W$.

Remarque 2.3.5. L'irréductibilité de W n'entraine pas celle de $\mathsf{Ind}^G_H(W)$.

Proposition 2.3.6. Soient V une représentation de G, W une représentation de H et K un sous-groupe de G contenant H. On a :
(1) $\mathsf{Res}^G_H(V) = \mathsf{Res}^K_H(\mathsf{Res}^G_K(V))$;
(2) $\mathsf{Ind}^G_H(W) = \mathsf{Res}^G_K(\mathsf{Ind}^K_H(W))$;
(3) $\mathsf{Hom}_G(\mathsf{Ind}^G_H(W), V) \simeq \mathsf{Hom}_H(W, \mathsf{Res}^G_H(V))$;
(4) $\mathsf{Ind}^G_H(W) \otimes_{\mathbf{C}} V \simeq \mathsf{Ind}^G_H(W \otimes_{\mathbf{C}} \mathsf{Res}^G_H(V))$.

Démonstration. La propriété (1) est triviale. La propriété (2) n'est autre que l'isomorphisme évident

$$\mathbf{C}[G] \otimes_{\mathbf{C}[K]} (\mathbf{C}[K] \otimes_{\mathbf{C}[H]} W) \xrightarrow{\sim} \mathbf{C}[G] \otimes_{\mathbf{C}[H]} W$$

La propriété (3) est l'isomorphisme

$$\mathsf{Hom}_G(\mathsf{Ind}^G_H(W), V) = \mathsf{Hom}_{\mathbf{C}[G]}(\mathbf{C}[G] \otimes_{\mathbf{C}[H]} W, V) \simeq \mathsf{Hom}_{\mathbf{C}[H]}(W, V) = \mathsf{Hom}_H(W, \mathsf{Res}^G_H(V))$$

Pour la propriété (4), on part du morphisme H-équivariant $W \to \mathsf{Ind}^G_H(W)$ qui induit le morphisme H-équivariant $W \otimes_{\mathbf{C}} \mathsf{Res}^G_H(V) \to \mathsf{Ind}^G_H(W) \otimes_{\mathbf{C}} V$. Comme $\mathsf{Ind}^G_H(W) \otimes_{\mathbf{C}} V$ est en fait un $\mathbf{C}[G]$-module, ce dernier induit un morphisme G-équivariant $\mathsf{Ind}^G_H(W \otimes_{\mathbf{C}} \mathsf{Res}^G_H(V)) \to \mathsf{Ind}^G_H(W) \otimes_{\mathbf{C}} V$, qui n'est autre que l'isomorphisme naturel $\mathbf{C}[G] \otimes (W \otimes_{\mathbf{C}} V) \xrightarrow{\sim} (\mathbf{C}[G] \otimes_{\mathbf{C}[H]} W) \otimes_{\mathbf{C}} V$. □

2.3.7. *Description explicite de l'induite.* Fixons $T \subset G$ un système complet de représentants des classes à gauche modulo H. On a $G = \bigsqcup_{\tau \in T} \tau H$, ce qui implique que

$$\mathbf{C}[G] = \bigoplus_{\tau \in T} e_\tau \, \mathbf{C}[H]$$

est un $\mathbf{C}[H]$-module libre de rang $[G : H]$. On a donc

$$\mathsf{Ind}^G_H(W) = \bigoplus_{\tau \in T} e_\tau \otimes W$$

ce qui implique :

Proposition 2.3.8. $\dim_{\mathbf{C}}(\mathsf{Ind}^G_H(W)) = [G : H] \dim_{\mathbf{C}}(W)$.

Décrivons l'action de G sur chacun des facteurs $e_\tau \otimes W$. Si $g \in G$, $\tau \in T$ et $w \in W$, il existe $t_{(g,\tau)} \in T$ et $h_{(g,\tau)} \in H$ uniques tels que

$$g\tau = t_{(g,\tau)} h_{(g,\tau)}$$

On a alors

$$g \cdot (e_\tau \otimes w) = e_{t_{(g,\tau)} h_{(g,\tau)}} \otimes w = e_{t_{(g,\tau)}} \otimes h_{(g,\tau)} \cdot w \in e_{t_{(g,\tau)}} \otimes W$$

Une autre façon commode (et intrinsèque) de décrire l'induite est la suivante :

Proposition 2.3.9. $\mathsf{Ind}_H^G(W) \simeq \mathsf{Hom}_H(\mathbf{C}[G], W) := \{f\colon G \to W \mid (\forall g \in G)\,(\forall h \in H)\, f(hg) = hf(g)\}$ (où l'action de G sur $f \in \mathsf{Hom}_H(\mathbf{C}[G], W)$ est donnée par $(g' \cdot f)(g) = f(gg')$ pour tous $g, g' \in G$).

Démonstration. Si $w \in W$, posons

$$i(w)\colon G \to W$$
$$g \mapsto \begin{cases} g \cdot w & \text{si } g \in H \\ 0 & \text{si } g \notin H \end{cases}$$

Cela définit une application $i\colon W \to \mathsf{Hom}_H(\mathbf{C}[G], W)$. Elle est H-équivariante. Elle induit donc une application G-équivariante $1 \otimes i\colon \mathsf{Ind}_H^G(W) \to \mathsf{Hom}_H(\mathbf{C}[G], W)$. Soit

$$j\colon \mathsf{Hom}_H(\mathbf{C}[G], W) \to \mathsf{Ind}_H^G(W)$$
$$f \mapsto \sum_{\tau \in T} e_\tau \otimes f(\tau^{-1})$$

Si $f \in \mathsf{Hom}_H(\mathbf{C}[G], W)$, on a $((1 \otimes i) \circ j)(f) = \sum_{\tau \in T} \tau \cdot i(f(\tau^{-1}))$. Pour $g \in G$, on a

$$(\tau \cdot i(f(\tau^{-1})))(g) = i(f(\tau^{-1}))(g\tau) = \begin{cases} g\tau \cdot f(\tau^{-1}) = f(g) & \text{si } g\tau \in H \\ 0 & \text{sinon} \end{cases}$$

ce qui montre que $(1 \otimes i) \circ j = \mathrm{Id}_{\mathsf{Hom}_H(\mathbf{C}[G], W)}$. Si $w \in W$, on a $(j \circ (1 \otimes i))(1 \otimes w) = j(i(w)) = \sum_{\tau \in T} e_\tau \otimes i(w)(\tau^{-1})$. Comme $i(w)(\tau^{-1}) = 0$ si $w \notin H$ et $e_\tau \otimes i(w)(\tau^{-1}) = 1 \otimes e_\tau i(w)(\tau^{-1}) = 1 \otimes w$ si $\tau \in H$, on a $(j \circ (1 \otimes i))(1 \otimes w)$. On en déduit que $j \circ (1 \otimes i) = \mathrm{Id}_{\mathsf{Ind}_H^G(W)}$, ce qui montre que $1 \otimes i$ et j sont des isomorphismes inverses l'un de l'autre. □

2.3.10. *Caractère d'une représentation induite.*

Proposition 2.3.11. (1) Si $g \in G$, on a $\chi_{\mathsf{Ind}_H^G(W)}(g) = \sum_{\substack{\tau \in T \\ \tau^{-1} g \tau \in H}} \chi_W(\tau^{-1} g \tau)$.

(2) Soit C est une classe de conjugaison de G. L'intersection $H \cap C = \bigsqcup_{i=1}^r \Gamma_i$ se décompose en une union de classes de conjugaison de H. On a $\chi_{\mathsf{Ind}_H^G(W)}(C) = [G : H] \sum_{i=1}^r \frac{\#\Gamma_i}{\#C} \chi_W(\Gamma_i)$.

Démonstration. (1) On a vu que $\mathsf{Ind}_H^G(W) = \bigoplus_{\tau \in T} e_\tau \otimes W$, et que $g \in G$ envoie $e_\tau \otimes W$ sur $e_{t_{(g,\tau)}} \otimes W$ où $t_{(g,\tau)} \in T$ est tel que $g\tau H = t_{(g,\tau)} H$. Il en résulte que les facteurs $e_\tau \otimes W$ ne contribuent à la trace de g agissant sur $\mathsf{Ind}_H^G(W)$ que si $g\tau H = \tau H$, *i.e.* $\tau^{-1} g \tau \in H$, l'action de g sur $e_\tau \otimes W \simeq W$ est alors donnée par celle que $\tau^{-1} g \tau$ sur W.

(2) On a $\#C \chi_{\mathsf{Ind}_H^G(W)}(C) = \sum_{g \in C} \chi_{\mathsf{Ind}_H^G(W)}(g) = \sum_{g \in C} \sum_{\substack{\tau \in T \\ \tau^{-1} g \tau \in H}} \chi_W(\tau^{-1} g \tau) = \sum_{\tau \in T} \sum_{i=1}^r \sum_{\substack{g \in C \\ \tau^{-1} g \tau \in \Gamma_i}} \chi_W(\tau^{-1} g \tau) = \sum_{\tau \in T} \sum_{i=1}^r \sum_{\tau^{-1} g \tau \in \tau^{-1} C \tau \cap \Gamma_i} \chi_W(\Gamma_i)$. Comme C est une classe de conjugaison, on a $\tau^{-1} C \tau \cap \Gamma_i = \Gamma_i$, ce qui implique que $\sum_{\tau^{-1} g \tau \in \tau^{-1} C \tau \cap \Gamma_i} \chi_W(\Gamma_i) = \#\Gamma_i \chi_W(\Gamma_i)$, et $\#C \chi_{\mathsf{Ind}_H^G(W)}(C) = [G : H] \sum_{i=1}^r \#\Gamma_i \chi_W(\Gamma_i)$. □

Proposition 2.3.12. (Réciprocité de Frobenius) Soient W une représentation de H et V une représentation de G, on a

$$\langle \chi_{\mathsf{Ind}_H^G(W)} | \chi_V \rangle_G = \langle \chi_W | \chi_{\mathsf{Res}_H^G(V)} \rangle_H$$

Démonstration. Par bilinéarité des produits scalaires sur $\mathscr{F}(G, \mathbf{C})$ et $\mathscr{F}(H, \mathbf{C})$, il suffit de traiter le cas où W et V sont irréductibles. On a alors

$$\langle \chi_{\mathsf{Ind}_H^G(W)} | \chi_V \rangle_G = \dim_{\mathbf{C}}(\mathsf{Hom}_G(\mathsf{Ind}_H^G(W), V)) = \dim_{\mathbf{C}}(\mathsf{Hom}_H(W, \mathsf{Res}_H^G(V))) = \langle \chi_W | \chi_{\mathsf{Res}_H^G(V)} \rangle_H$$

(*cf* proposition 2.3.6 (3)). □

2.4. **Exemples.**

2.4.1. *Cas d'un groupe cyclique.* Soient $n \in \mathbf{N}_{>1}$ et $G = \mathbf{Z}/n\,\mathbf{Z}$. Comme G est abélien, ses représentations irréductibles sont de dimension 1, il y en a n (à isomorphisme près). Soit $\zeta \in \mathbf{C}$ une racine primitive n-ième de l'unité. Pour $k \in \mathbf{Z}/n\,\mathbf{Z}$, soit $\chi_k \colon G \to \mathbf{C}^\times; 1 \mapsto \zeta^k$ (de sorte que $\chi_k = \chi_1^{\otimes k}$). Ce sont des (caractères de) représentations irréductibles. La table des caractères est alors

	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\cdots$	$\overline{n-1}$
χ_0	1	1	1	$\cdots$	1
χ_1	1	ζ	ζ^2	$\cdots$	ζ^{n-1}
χ_2	1	ζ^2	ζ^4	$\cdots$	$\zeta^{2(n-1)}$
$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\cdots$	$\vdots$
χ_{n-1}	1	ζ^{n-1}	$\zeta^{2(n-1)}$	$\cdots$	$\zeta^{(n-1)^2}$

2.4.2. *Cas d'un groupe produit.* Soient G_1 et G_2 deux groupes, et (V_1, ρ_1) (resp. (V_2, ρ_2)) une représentation de G_1 (resp. G_2). On dispose alors de la représentation **produit tensoriel externe** $\rho_1 \boxtimes \rho_2 \colon G_1 \times G_2 \to \mathsf{GL}(V_1 \otimes_K V_2)$ définie par

$$(g_1, g_2)(v \otimes w) = g_1(v) \otimes g_2(w)$$

On la note $V_1 \boxtimes V_2$.

Proposition 2.4.3. (1) On a $\chi_{V_1 \boxtimes V_2}(g_1, g_2) = \chi_{V_1}(g_1)\chi_{V_2}(g_2)$.
(2) Si V_1 et V_2 sont irréductibles, il en est de même de $V_1 \boxtimes V_2$.
(3) Les représentations irréductibles de $G_1 \times G_2$ sont les $V_1 \boxtimes V_2$ avec V_1 et V_2 irréductibles.

Démonstration. (1) est évident.
(2) On a $\langle \chi_{V_1 \boxtimes V_2} | \chi_{V_1 \boxtimes V_2} \rangle = \frac{1}{\#G_1 \#G_2} \sum_{(g_1,g_2) \in G_1 \times G_2} |\chi_{V_1}(g_1)\chi_{V_2}(g_2)|^2 = \langle \chi_{V_1} | \chi_{V_1} \rangle \langle \chi_{V_2} | \chi_{V_2} \rangle = 1$, de sorte que $V_1 \boxtimes V_2$ est irréductible.
(3) Soient $V_1, \ldots, V_k$ (resp. $W_1, \ldots, W_\ell$) « les »représentations irréductibles de G_1 (resp. G_2). D'après le corollaire 2.2.10, on a $\#G_1 = \sum_{i=1}^k (\dim_{\mathbf{C}}(V_i))^2$ et $\#G_2 = \sum_{j=1}^\ell (\dim_{\mathbf{C}}(W_j))^2$: le produit de ces égalités donne $\#(G_1 \times G_2) = \sum_{\substack{1 \leqslant i \leqslant k \\ 1 \leqslant j \leqslant \ell}} (\dim_{\mathbf{C}}(V_i \boxtimes W_j))^2$. D'après (2), les représentations $V_i \boxtimes W_j$ de $G_1 \times G_2$ sont irréductibles pour $i \in \{1, \ldots, k\}$ et $j \in \{1, \ldots, \ell\}$: le corollaire 2.2.10 implique qu'il n'y en a pas d'autres. □

Exemple 2.4.4. La table des caractères de $\mathbf{Z}/2\,\mathbf{Z}$ est

	$\overline{0}$	$\overline{1}$
χ_+	1	1
χ_-	1	-1

Celle du groupe de Klein $(\mathbf{Z}/2\,\mathbf{Z})^2$ est donc

	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$
$\chi_{+,+}$	1	1	1	1
$\chi_{+,-}$	1	1	-1	-1
$\chi_{-,+}$	1	-1	1	-1
$\chi_{-,-}$	1	-1	-1	1

3. Espaces quadratiques

Dans tout ce qui suit, K désigne un corps.

3.1. **Formes quadratiques.**

3.1.1. *Définitions, représentation matricielle.*

Définition 3.1.2. Soient V et W deux K-espaces vectoriels. Une **forme bilinéaire** sur $V \times W$ est une application $\varphi \colon V \times W \to K$ telle que

$$(\forall w \in W) \;\; \varphi(.,w) \colon v \mapsto \varphi(v,w) \text{ est une forme linéaire sur } V$$
$$(\forall v \in V) \;\; \varphi(v,.) \colon w \mapsto \varphi(v,w) \text{ est une forme linéaire sur } W$$

(*i.e.* $\varphi(v,w)$ est linéaire en v et en w). L'ensemble des formes bilinéaires sur $V \times W$ est un K-espace vectoriel, noté $\mathscr{L}_2(V,W)$.
Une forme bilinéaire sur V est une forme bilinéaire sur $V \times V$, et on note $\mathscr{L}_2(V)$ le K-espace vectoriel des formes bilinéaires sur V.

Remarque 3.1.3. Par définition, on a $\mathscr{L}_2(V,W) = \mathsf{Bil}(V,W,K) \simeq \mathsf{Hom}_K(V \otimes_K W, K) = (V \otimes_K W)^\vee$.

Exemples 3.1.4. (1) Soit $n \in \mathbf{N}_{>0}$. L'application

$$K^n \times K^n \to K$$
$$\big((x_1,\dots,x_n),(y_1,\dots,y_n)\big) \mapsto x_1y_1 + \cdots + x_ny_n$$

(2) Soient V un K-espace vectoriel et V^* son dual. L'application

$$\langle .|. \rangle \colon V^* \times V \to K$$
$$(f,v) \mapsto \langle f|v\rangle = f(v)$$

(c'est le **crochet de la dualité**).

(3) Soient $a < b$ deux réels, $K\colon [a,b] \to \mathbf{R}$ une application continue, l'application

$$\mathscr{C}^0([a,b],\mathbf{R}) \times \mathscr{C}^0([a,b],\mathbf{R}) \to \mathbf{R}$$
$$(f,g) \mapsto \int_a^b (Kfg)(x)\,\mathrm{d}x$$

Définition 3.1.5. Soit $\varphi \in \mathscr{L}_2(V,W)$.

(1) Si $v \in V$ et $w \in W$, on dit que v et w sont *orthogonaux* (pour φ) lorsque $\varphi(v,w) = 0$.

(2) Plus généralement, $A \subset V$ et $B \subset W$ sont dits orthogonaux lorsque $(\forall (v,w) \in A \times B)\ \varphi(v,w) = 0$.

(3) Si $A \subset E$ (resp. $B \subset F$), l'**orthogonal** de A (resp. B) est

$$A^\perp = \{w \in W \mid (\forall v \in A)\ \varphi(v,w) = 0\} \quad (\text{resp. } B^\perp = \{v \in V \mid (\forall w \in W)\ \varphi(v,w) = 0\})$$

C'est un sous-espace vectoriel de W (resp. V).

(4) Soient $W_1, W_2 \subseteq V$ deux sous-espaces vectoriels. On dit que W_1 et W_2 sont en **somme directe orthogonale** s'ils sont orthogonaux et $V = W_1 \oplus W_2$. On note alors $V = W_1 \overset{\perp}{\oplus} W_2$.

Définition 3.1.6. Matrice d'une forme bilinéaire. Soient V, W deux K-espaces vectoriels de *dimension finie*, $\mathfrak{B} = (e_1,\dots,e_n)$ (resp. $\mathfrak{B}' = (f_1,\dots,f_p)$) une base de V (resp. de W). Si $\varphi \in \mathscr{L}_2(V,W)$, la matrice de φ dans les bases $\mathfrak{B}$ et $\mathfrak{B}'$ est

$$\mathrm{Mat}_{\mathfrak{B},\mathfrak{B}'}(\varphi) = \big(\varphi(e_i,f_j)\big)_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant p}} \in \mathsf{M}_{n,p}(K)$$

Si $V = W$ et $\mathfrak{B} = \mathfrak{B}'$, la matrice de $\varphi \in \mathscr{L}_2(V)$ dans $\mathfrak{B}$ est $\mathrm{Mat}_{\mathfrak{B}}(\varphi) := \mathsf{M}_{\mathfrak{B},\mathfrak{B}}(\varphi) \in \mathsf{M}_n(K)$.

Si $v \in V$ et $w \in W$, on a $v = \sum_{i=1}^n x_ie_i$ et $w = \sum_{j=1}^p y_jf_j$. Matriciellement, v et w sont représentés par les vecteurs colonnes $X = (x_i)_{1\leqslant i\leqslant n} \in K^n$ et $Y = (y_j)_{1\leqslant j\leqslant p} \in K^p$ respectivement. Si $A = \mathsf{M}_{\mathfrak{B},\mathfrak{B}'}(\varphi)$, on a

$$\begin{aligned}\varphi(v,w) &= \varphi\Big(\sum_{i=1}^n x_ie_i, y\Big)\\ &= \sum_{i=1}^n x_i\varphi(e_i,y) = \sum_{i=1}^n x_i\varphi\Big(e_i, \sum_{j=1}^p y_jf_j\Big)\\ &= \sum_{i=1}^n\sum_{j=1}^p x_iy_j\varphi(e_i,f_j)\end{aligned}$$

c'est la composante de la matrice ${}^tXAY$ (matrice 1×1).

Remarque 3.1.7. $\varphi \in \mathscr{L}_2(V,W)$ définit l'application linéaire

$$\mathsf{L}_\varphi \colon W \to V^\vee$$
$$w \mapsto \varphi(.,w)$$

La matrice $\mathrm{Mat}_{\mathfrak{B},\mathfrak{B}'}(\varphi)$ n'est autre que la matrice de L_φ dans les bases $\mathfrak{B}'$ et $\mathfrak{B}^*$ (la base duale de $\mathfrak{B}$).

Formules de changement de base. Reprenons les notations de la définition, et soient $\mathfrak{B}_1, \mathfrak{B}_2$ deux bases de V (resp. $\mathfrak{B}'_1, \mathfrak{B}'_2$ deux bases de W). Notons P (resp. Q) la matrice de changement de base de $\mathfrak{B}_1$ à $\mathfrak{B}_2$ (resp. de $\mathfrak{B}'_1$ à $\mathfrak{B}'_2$). Si $v \in V$ est représenté par le vecteur colonne X_1 (resp. X_2) dans la base $\mathfrak{B}_1$ (resp. $\mathfrak{B}_2$), on a $X_1 = PX_2$. Avec des notations évidentes, on a de même $Y_1 = QY_2$. Notons A_1 (resp. A_2) la matrice de φ dans les bases $\mathfrak{B}_1$ et $\mathfrak{B}'_1$ (resp. $\mathfrak{B}_2$ et $\mathfrak{B}'_2$). On a

$$\big(\varphi(v,w)\big) = {}^tX_1A_1Y_1 = {}^t(PX_2)A_1QY_2 = {}^tX_2\big({}^tPA_1Q\big)Y_2$$

ceci étant vrai pour tout v et tout w, on a donc

Proposition 3.1.8. $A_2 = {}^tPA_1Q$.

Dans tout ce qui suit, V désigne un K-espace vectoriel.

Définition 3.1.9. Soit $\varphi \in \mathscr{L}_2(V)$. On dit que φ est **symétrique** (resp. **antisymétrique**) lorsque

$$(\forall v, w \in V) \quad \varphi(w,v) = \varphi(v,w) \quad (\text{resp. } \varphi(w,v) = -\varphi(v,w))$$

On note $\mathscr{S}_2(V)$ (resp. $\mathscr{A}_2(V)$) le sous-K-espace vectoriel de $\mathscr{L}_2(V)$ constitué des formes bilinéaires symétriques (resp. antisymétriques).

Exercice 3.1.10. Supposons $\mathsf{car}(K) \neq 2$.
(1) Montrer que $\mathscr{L}_2(V) = \mathscr{S}_2(V) \oplus \mathscr{A}_2(V)$.
(2) Montrer que $\varphi \in \mathscr{L}_2(V)$ est antisymétrique si et seulement si $\varphi(v,v) = 0$ pour tout $v \in V$.

Remarque 3.1.11. Si $\mathsf{car}(K) = 2$, on a $\mathscr{S}_2(V) = \mathscr{A}_2(V)$.

Proposition 3.1.12. $\varphi \in \mathscr{L}_2(V)$ est symétrique (resp. antisymétrique) si et seulement si sa matrice dans toute base de V est symétrique (resp. antisymétrique).

Démonstration. Si $\mathfrak{B}$ est une base de V et A la matrice de φ dans $\mathfrak{B}$, on a

$${}^tXAY = {}^t\big({}^tXAY\big) = {}^tY{}^tAX$$

pour tout $X, Y \in K^n$. □

Définition 3.1.13. Deux matrices $A, B \in \mathsf{M}_n(K)$ sont **congruentes** s'il existe $P \in \mathsf{GL}_n(K)$ telle que $B = {}^tPAP$. C'est une relation d'équivalence. Deux matrices congruentes ont même rang.

Proposition 3.1.14. Si $\varphi \in \mathscr{L}_2(V)$, $\mathfrak{B}, \mathfrak{B}'$ sont deux bases de V et P la matrice de changement de base de $\mathfrak{B}$ à $\mathfrak{B}'$, on a $\mathrm{Mat}_{\mathfrak{B}'}(\varphi) = {}^tP\,\mathrm{Mat}_{\mathfrak{B}}(\varphi)P$. En particulier, on a $\det(\mathrm{Mat}_{\mathfrak{B}'}(\varphi)) = \det(\mathrm{Mat}_{\mathfrak{B}}(\varphi))\det(P)^2$.

Définition 3.1.15. Si $\varphi \in \mathscr{L}_2(V)$ et $\mathfrak{B}$ est une base de V, l'image de $\det(\mathrm{Mat}_{\mathfrak{B}}(\varphi))$ dans $\{0\} \cup (K^\times/K^{\times 2})$ ne dépend pas de la base $\mathfrak{B}$. On l'appelle le **discriminant** de φ et on le note $\mathsf{disc}(\varphi) \in \{0\} \cup (K^\times/K^{\times 2})$.

Définition 3.1.16. Une **forme quadratique** sur V est une application $q\colon V \to K$ telle qu'il existe $\varphi \in \mathscr{L}_2(V)$ telle que $q(v) = \varphi(v,v)$ pour tout $v \in V$. L'ensemble des formes quadratiques sur V forme un K-espace vectoriel noté $\mathscr{Q}(V)$.

Remarque 3.1.17.
(1) Il n'y a pas unicité pour φ dans la définition précédente : si $\mathsf{car}(K) \neq 2$, toutes les formes bilinéaires antisymétriques donnent la forme quadratique nulle.
(2) Si V est de dimension finie, $\mathfrak{B} = (e_1, \ldots, e_n)$ une base de V et $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$, on a

$$q(x) = \varphi(x,x) = {}^tXAX = \sum_{1 \leqslant i,j \leqslant n} a_{i,j}x_ix_j$$

pour tout $x = \sum_{i=1}^n x_ie_i \in V$: une forme quadratique n'est rien d'autre qu'une fonction polynômiale homogène de degré 2. En particulier, on a $q(\lambda v) = \lambda^2 q(v)$ pour tout $v \in V$ et $\lambda \in K$.

3.1.18. *Polarisation, non dégénérescence, isotropie.* **On suppose désormais** $\mathsf{car}(K) \neq 2$.

Proposition 3.1.19. (Polarisation). Soit $q \in \mathscr{Q}(V)$. Il existe une unique forme bilinéaire *symétrique* φ telle que $q(v) = \varphi(v,v)$ pour tout $v \in V$. C'est la **forme polaire** de q. Pour $v, w \in V$, on a

$$\begin{aligned}\varphi(v,w) &= \tfrac{1}{2}\big(q(v+w) - q(v) - q(w)\big)\\ &= \tfrac{1}{4}\big(q(v+w) - q(v-w)\big)\end{aligned}$$

(identités de polarisation).

Corollaire 3.1.20. On a un isomorphisme de K-espaces vectoriels $\mathscr{S}_2(V) \xrightarrow{\sim} \mathscr{Q}(V)$.

Remarque 3.1.21. Grâce à la correspondance entre formes bilinéaires symétriques et formes quadratiques qui précède, la terminologie que nous allons mettre en place pour les formes bilinéaires symétriques s'applique également aux formes quadratiques associées. Par exemple, le discriminant d'une forme quadratique q, noté $\mathsf{disc}(q)$ est le discriminant de sa forme polaire.

Définition 3.1.22. Un **espace quadratique** (sur K) est un couple (V, φ) où V est un K-espace vectoriel et $\varphi \in \mathscr{S}_2(V)$ une forme bilinéaire symétrique sur V. D'après ce qui précède, cela équivaut à la donnée du couple (V, q) où q est la forme quadratique associée à φ.

Rappelons qu'on a défini l'application linéaire associée à φ :

$$\begin{aligned} \mathsf{L}_\varphi \colon V &\to V^\vee \\ v &\mapsto \varphi(.,v) \end{aligned}$$

Définition 3.1.23. Soient (V,φ) un espace quadratique sur K. Si $\dim_K(V) < +\infty$, soient $\mathfrak{B}$ une base de V et $A = \mathrm{Mat}_{\mathfrak{B}}(\varphi)$.

(1) On dit que φ est **non dégénérée** si L_φ est injective, *i.e.* si $V^\perp = \{0\}$. Lorsque $\dim_K(V) < +\infty$, cela équivaut à $A \in \mathsf{GL}_n(K)$.

(2) Le **rang** de φ est le rang de l'application K-linéaire L_φ. Lorsque $\dim_K(V) < +\infty$, c'est le rang de la matrice A.

Proposition 3.1.24. Supposons $\dim_K(V) < +\infty$ et $\varphi \in \mathscr{S}_2(V)$. Les conditions suivantes sont équivalentes :

- φ est non dégénérée ;
- φ est de rang $\dim_K(V)$;
- $\mathsf{disc}(\varphi) \neq 0$ (soit encore $\mathsf{disc}(\varphi) \in K^\times/K^{\times 2}$) ;
- l'application linéaire associée $\mathsf{L}_\varphi \colon V \to V^\vee$ est un isomorphisme.

Remarque 3.1.25.

(1) La dimension de V, le rang et le discriminant de φ sont des invariants attachés à sa classe d'isomorphisme.

(2) Conformément à la remarque 3.1.21, le rang (resp. la matrice $\mathrm{Mat}_{\mathfrak{B}}(q)$ dans la base $\mathfrak{B}$) d'une forme quadratique q sur V est le rang (resp. la matrice dans la base $\mathfrak{B}$) de sa forme polaire associée.

(3) Soient $n \in \mathbf{N}_{>0}$ et $q \colon K^n \to K$; $(x_1,\dots,x_n) \mapsto \sum_{i=1}^{n} a_i x_i^2 + \sum_{1\leqslant i<j\leqslant n} b_{i,j} x_i x_j$. Alors la matrice de q dans la base canonique de K^n est

$$\begin{pmatrix} a_1 & \frac{b_{1,2}}{2} & \cdots & \frac{b_{1,n}}{2} \\ \frac{b_{1,2}}{2} & a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \frac{b_{n-1,n}}{2} \\ \frac{b_{1,n}}{2} & \cdots & \frac{b_{n-1,n}}{2} & a_n \end{pmatrix}$$

Proposition 3.1.26. Supposons V de dimension finie. Soient $q \in \mathscr{Q}(V)$ et φ la forme polaire associée. Si W est un sous-espace vectoriel de V, alors

$$\dim_K(W) + \dim_K(W^\perp) \geqslant \dim_K(V) \quad \text{et} \quad W \subset (W^\perp)^\perp$$

Si φ est non dégénérée, ce sont des égalités.

Démonstration. • Notons $f \colon V \to W^\vee$ le composé de $\mathsf{L}_\varphi \colon V \to V^\vee$ et de $r \colon V^\vee \to W^\vee$ (la restriction à W). On a $\mathsf{Ker}(f) = \{v \in V,\ (\forall w \in W)\ \varphi(v,w) = \mathsf{L}_\varphi(v)(w) = 0\} = W^\perp$. L'application K-linéaire induit donc un morphisme K-linéaire injectif $\widetilde{f} \colon V/W^\perp \to W^\vee$. On a donc $\dim_K(V/W^\perp) \leqslant \dim_K(W^\vee) = \dim_K(W)$, et donc $\dim_K(V) \leqslant \dim_K(W) + \dim_K(W^\perp)$.

• Supposons maintenant φ non dégénérée : l'application L_φ est bijective. Comme r est surjective, l'application f est surjective : il en est de même de $\widetilde{f}$, qui est donc un isomorphisme, et on a $\dim_K(V) = \dim_K(W) + \dim_K(W^\perp)$.

• On a bien sûr $W \subset (W^\perp)^\perp$. Lorsque φ est non dégénérée, c'est une égalité par égalité des dimensions. □

Exercice 3.1.27. On a plus précisément [2], on a $\dim_K(W) + \dim_K(W^\perp) = \dim_K(V) + \dim_K(W \cap V^\perp)$.

Corollaire 3.1.28. Si la restriction de φ à $W \subset V$ est non dégénérée, alors $W \oplus W^\perp = V$.

Démonstration. Le sous-espace W est non dégénérée si et seulement si on a $W \cap W^\perp = \{0\}$. Comme $\dim_K(W) + \dim_K(W^\perp) \geqslant \dim_K(V)$ d'après la proposition 3.1.26, cela implique $W \oplus W^\perp = V$. □

Remarque 3.1.29. Il est faux en général que $W \cap W^\perp = \{0\}$, même lorsque φ est non dégénérée. Par exemple, si $V = K^2$ et $q(x_1,x_2) = x_1^2 - x_2^2$ (on a alors $\varphi\big((x_1,x_2),(y_1,y_2)\big) = x_1y_1 - x_2y_2$), alors $w = (1,1)$ vérifie $q(w) = 0$, de sorte que si $W = \mathsf{Vect}(w)$, on a $W \subseteq W^\perp$. En fait, dans cet exemple, φ est non dégénérée, et $W = W^\perp$.

2. Le noyau de la restriction $\mathsf{L}_{\varphi|W} \colon W \to V^\vee$ est $W \cap V^\perp$, ce qui induit un isomorphisme $W/(W \cap V^\perp) \simeq \mathsf{L}_\varphi(W) \subset V^\vee$. L'orthogonal, au sens de la dualité, de $\mathsf{L}_\varphi(W)$ est $\{v \in V \mid (\forall w \in W)\ \varphi(v,w) = 0\} = W^\perp$. On a donc un isomorphisme $\mathsf{L}_\varphi(W) \simeq (V/W^\perp)^\vee$ (cela résulte de la non dégénérescence du crochet de la dualité). Finalement, on a $W/(W \cap V^\perp) \simeq (V/W^\perp)^\vee$ et donc $\dim_K(W) - \dim_K(W \cap V^\perp) = \dim_K(V) - \dim_K(W^\perp)$.

Définition 3.1.30. Soient (V,q) un espace quadratique et $v \in V$.
(1) On dit que v est **isotrope** lorsque $q(v)=0$. Si v est isotrope et $\lambda \in K$, alors λv est aussi isotrope : l'ensemble des vecteurs isotropes forme un cône appelé le **cône isotrope**.
(2) Un **sous-espace totalement isotope** (SETI) est un sous-espace $W \subset V$ sur lequel la restriction de q est nulle, *i.e.* tel que $W \subset W^\perp$. Un **sous-espace totalement isotope maximal** (SETIM) est un SETI maximal (au sens de l'inclusion).
(3) On dit que (V,q) (ou simplement q) est **anisotrope** si 0 est le seul vecteur isotrope.

Remarque 3.1.31. (1) D'après la remarque qui précède, une forme quadratique peut parfaitement être non dégénérée et avoir des vecteurs isotropes non nuls. Par contre, une forme quadratique anisotrope est *a fortiori* non dégénérée.
(2) Si q est non dégénérée et W est un SETI, on a $\dim_K(V) = \dim_K(W) + \dim_K(W^\perp) \geqslant 2\dim_K(W)$, de sorte que $\dim_K(W) \leqslant \left\lfloor \frac{\dim_K(V)}{2} \right\rfloor$. On verra plus tard (*cf* corollaire 3.3.27) que les SETIM ont tous même dimension.

Définition 3.1.32. (1) Un **plan hyperbolique** est un espace quadratique (H,q) de dimension 2 ayant pour base deux vecteurs isotropes v_1, v_2 tels que $\varphi(v_1,v_2) \neq 0$. Quitte à diviser v_1 par $\varphi(v_1,v_2)$, on peut supposer que $\varphi(v_1,v_2)=1$. La matrice de q dans la base (v_1,v_2) de H est alors $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.
(2) Un **espace hyperbolique** est un espace quadratique (V,q) qui est somme directe orthogonale de plans hyperboliques. Après permutation de vecteurs de base, il existe alors une base $(e_1,\dots,e_{2n})$ de V dans laquelle la matrice de q s'écrit par blocs $\left(\begin{smallmatrix} 0 & \mathrm{I}_n \\ \mathrm{I}_n & 0 \end{smallmatrix}\right)$. Un sous-espace totalement isotrope de dimension $\frac{\dim_K(V)}{2}$ dans V s'appelle un **lagrangien** (c'est alors un SETIM de (V,q)).

Exercice 3.1.33. Si (H,q) est un plan hyperbolique, alors $q\colon H \to K$ est surjective [3].

Lemme 3.1.34. (Lemme de gonflement hyperbolique) Soient (V,q) un espace quadratique non dégénéré, W un sous-espace vectoriel, $U = \mathsf{Ker}(q_{|W}) = W \cap W^\perp$ et W' un supplémentaire de U dans W. Si $(u_1,\dots,u_r)$ est une base de U, alors il existe une famille $(v_1,\dots,v_r)$ de V telle que si $H_i = \mathsf{Vect}(u_i,v_i)$, on a :
(1) H_i est un plan hyperbolique pour tout $i \in \{1,\dots,r\}$;
(2) les sous-espaces $W', H_1, \dots, H_r$ sont en somme directe orthogonale dans V.

Démonstration. La forme quadratique $q_{|W'}$ est non dégénérée. On procède par récurrence sur $r = \dim_K(U)$ (le cas $r=0$ étant vide). Supposons $r>0$. Posons $U_1 = \mathsf{Vect}(u_2,\dots,u_r)$ et $W_1 = U_1 \oplus W'$: on a $W_1 \subsetneq W$, donc $W^\perp \subsetneq W_1^\perp$ (car q est non dégénérée) : soit $v_1 \in W_1^\perp \backslash W^\perp$. On a $\varphi(u_1,v_1) \neq 0$ (sinon v_1 serait orthogonal à $W = W_1 \oplus Ku_1$). Quitte à diviser v_1 par $\varphi(u_1,v_1)$, on peut supposer que $\varphi(u_1,v_1)=1$. Quitte ensuite à remplacer v_1 par $v_1 - q(v_1)u_1$, on peut en outre supposer que $q(v_1)=0$. Le plan $H_1 = \mathsf{Vect}(u_1,v_1)$ est alors hyperbolique, et $H_1 \subset W_1^\perp$. Considérons l'espace $\widetilde{W}_1 = Kv_1 \oplus W = U_1 \oplus H_1 \oplus W'$. La restriction de q à $H_1 \oplus W'$ est non dégénérée. Comme $H_1 \subset W_1^\perp$, on a $U_1 \subset (H_1 \oplus W')^\perp$. Il en résulte que $\mathsf{Ker}(q_{|\widetilde{W}_1}) = U_1$. Comme $\widetilde{W}_1 = U_1 \oplus (H_1 \oplus W')$, l'hypothèse de récurrence implique l'existence de vecteurs $v_2,\dots,v_r \in V$ tels que les plans $H_i = \mathsf{Vect}(u_i,v_i)$ soient hyperboliques pour $i \in \{2,\dots,r\}$ et $H_1 \oplus W', H_2, \dots, H_r$ en somme directe orthogonale, ce qui achève la preuve. □

Exemple 3.1.35. Si un espace quadratique non dégénéré contient un vecteur isotrope non nul, alors il contient un plan hyperbolique. Plus généralement, un SETI est un lagrangien d'un sous-espace hyperbolique de V.

Corollaire 3.1.36. Si (V,q) est un espace quadratique non dégénéré de dimension finie, il existe une décomposition en somme directe orthogonale $V = H_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} H_d \overset{\perp}{\oplus} W$ telle que
(1) $(H_i, q_{|H_i})$ est un plan hyperbolique pour tout $i \in \{1,\dots,d\}$;
(2) $q_{|W}$ est anisotrope.

Démonstration. On procède par récurrence sur la dimension de V, le cas $\dim_K(V)=0$ étant trivial. Supposons $\dim_K(V)>0$. Si q est anisotrope, il n'y a rien à faire : on a $V=W$. Si V contient un vecteur isotrope non nul, il existe un plan $H_1 \subset V$ tel que $(H_1, q_{|H_1})$ soit hyperbolique (*cf* lemme 3.1.34). Comme $q_{|H_1}$ est non dégénérée, on a $V = H_1 \overset{\perp}{\oplus} H_1^\perp$ il suffit d'appliquer l'hypothèse de récurrence à $H_1^\perp$. □

3. On a $q\left(\frac{x}{2}e_1 + e_2\right) = 2\varphi\left(\frac{x}{2}e_1, e_2\right) = x$ pour tout $x \in K$.

Remarque 3.1.37. On verra plus tard (*cf* corollaire 3.3.30) que l'entier d est la dimension commune à tous les SETIM de (V,q), et que la classe d'isomorphisme de $(W, q_{|W})$ ne dépend que de (V,q) et pas de la décomposition.

3.1.38. *Bases orthogonales, orthogonalisation.* Comme précédemment, (V,φ) est un espace quadratique sur K, et q désigne la forme quadratique associée.

Définition 3.1.39. Une famille de vecteurs $(e_i)_{i\in I}$ de V est **orthogonale** si

$$(\forall i,j\in I)\ \ i\neq j \Rightarrow \varphi(e_i,e_j)=0$$

Une **base orthogonale** est une base de V qui est orthogonale.

Remarque 3.1.40. Une base $\mathfrak{B}$ de V est orthogonale si et seulement si $\mathrm{Mat}_{\mathfrak{B}}(\varphi)$ est diagonale.

Théorème 3.1.41. Si V est de dimension finie, l'espace quadratique (V,φ) admet une base orthogonale.

Démonstration. On procède par récurrence sur $n=\dim_K(V)$, le cas $n=0$ étant évident : supposons $n>0$. Si $q=0$, il n'y a rien à faire : on peut supposer qu'il existe un vecteur non isotrope e_1. D'après le corollaire 3.1.28, on a $V = Ke_1\oplus H$ avec $e_1^\perp = H\subset V$. Par hypothèse de récurrence, la restriction de φ à $H\times H$ admet une base orthogonale $(e_2,\dots,e_n)$. La famille $(e_1,e_2,\dots,e_n)$ est alors une base orthogonale de V. □

Corollaire 3.1.42. Toute forme quadratique sur un K-espace vectoriel de dimension finie est combinaison linéaire de carrés de formes linéaires linéairement indépendantes.

Démonstration. Soit $\mathbf{e}=(e_1,e_2,\dots,e_n)$ est une base orthogonale de V pour q. Pour $i\in\{1,\dots,n\}$, posons $a_i=\varphi(e_i,e_i)$. Pour $v=\sum_{i=1}^n x_ie_i$, on a $q(x)=\sum_{1\leqslant i,j\leqslant n}x_ix_j\varphi(e_i,e_j)=\sum_{i=1}^n a_ix_i^2$, ce qui implique que $q=\sum_{i=1}^n a_ie_i^{*2}$, où $(e_i^*)_{1\leqslant i\leqslant n}$ désigne la base duale de $\mathbf{e}$. □

Notation. Si $a_1,\dots,a_n\in K$, on notera $\langle a_1,\dots,a_n\rangle$ la forme quadratique q sur K^n dont la matrice dans la base canonique est $\mathsf{diag}(a_1,\dots,a_n)$: en coordonnées, on a $q(x_1,\dots,x_n)=a_1x_1^2+\cdots+a_nx_n^2$.

Remarque 3.1.43. (1) Un plan hyperbolique est isomorphe à $\langle 1,-1\rangle$.
(2) On a bien sûr $\mathsf{disc}(\langle a_1,\dots,a_n\rangle)=a_1\cdots a_n \mod K^{\times 2}$ et $\langle a_1,\dots,a_n\rangle=\langle a_1\rangle\oplus\cdots\oplus\langle a_n\rangle$.

Corollaire 3.1.44. On a une décomposition $V=V^\perp\oplus W$ avec $q_{|W}$ non dégénérée.

Démonstration. Soit $(e_1,\dots,e_n)$ une base orthogonale de V pour q. Quitte à permuter ses vecteurs, on peut supposer que $q(e_i)\neq 0$ pour $i\in\{1,\dots,r\}$ et $q(e_i)=0$ pour $i\in\{r+1,\dots,n\}$ (de sorte que $r=\mathrm{rg}(q)$). On a alors $V^\perp=\mathsf{Vect}(e_{r+1},\dots,e_n)$ et $V=V^\perp\oplus W$ avec $W=\mathsf{Vect}(e_1,\dots,e_r)$. Comme $\mathrm{rg}(q_{|W})=r=\dim_K(W)$, la forme quadratique $q_{|W}$ est non dégénérée. □

3.1.45. *Réduction de Gauss.* Soient $n\in\mathbf{N}_{>0}$, $V=K^n$ et $q\colon V\to K$ une forme quadratique. Écrivons

$$q(x_1,\dots,x_n)=\sum_{i=1}^n a_{i,i}x_i^2+2\sum_{1\leqslant i<j\leqslant n}a_{i,j}x_ix_j$$

On veut construire $f_1,\dots,f_r\in V^\vee$ linéairement indépendantes est $\alpha_1,\dots,\alpha_r\in K$ tels que $q=\sum_{i=1}^r\alpha_if_i^2$. On peut bien sûr supposer $q\neq 0$.
Premier cas : Il existe $i\in\{1,\dots,n\}$ tel que $a_{i,i}\neq 0$ (« q contient un carré »).
Quitte à permuter les indices, on peut supposer que $i=1$. On écrit alors

$$q(x_1,\dots,x_n)=a_{1,1}x_1^2+2a_{1,1}x_1f(x_2,\dots,x_n)+r(x_2,\cdots,x_n)$$

avec $f(x_2,\dots,x_n)=\sum_{j=2}^n\frac{a_{1,j}}{a_{1,1}}x_j$ et $r(x_2,\cdots,x_n)=\sum_{i=2}^n a_{i,i}x_i^2+2\sum_{2\leqslant i<j\leqslant n}a_{i,j}x_ix_j$, si bien que

$$q(x_1,\dots,x_n)=a_{1,1}\big(x_1+f(x_2,\dots,x_n)\big)^2+q_2(x_2,\cdots,x_n)$$

où $q_2(x_2,\cdots,x_n)=r(x_2,\cdots,x_n)-a_{1,1}f(x_2,\dots,x_n)^2$. Il suffit d'appliquer l'algorithme à la forme quadratique q_2 (les formes linéaires obtenues sont linéairement indépendantes de $f_1\colon(x_1,\dots,x_n)\mapsto x_1+f(x_2,\dots,x_n)$).
Deuxième cas : Pour tout $i\in\{1,\dots,n\}$, on a $a_{i,i}=0$ (« q ne contient pas de carré »).
Quitte à permuter les indices, on peut supposer que $a_{1,2}\neq 0$ (rappelons qu'on a supposé $q\neq 0$). On écrit alors

$$q(x_1,\dots,x_n)=2\Big(a_{1,2}x_1x_2+x_1u(x_3,\dots,x_n)+x_2v(x_3,\dots,x_n)+r(x_3,\cdots,x_n)\Big)$$

avec

$$\begin{cases} u(x_3,\dots,x_n) = \sum_{j=3}^n a_{1,j}x_j \\ v(x_3,\dots,x_n) = \sum_{j=3}^n a_{2,j}x_j \\ r(x_3,\cdots,x_n) = \sum_{3\leqslant i<j\leqslant n} a_{i,j}x_ix_j \end{cases}$$

si bien que

$$q(x_1,\dots,x_n) = 2a_{1,1}\ell_1(x_1,\dots,x_n)\ell_2(x_1,\dots,x_n) + q_2(x_3,\cdots,x_n)$$

où

$$\begin{cases} \ell_1(x_1,\dots,x_n) = x_1 + \frac{1}{a_{1,2}}v(x_3,\dots,x_n) \\ \ell_2(x_1,\dots,x_n) = x_2 + \frac{1}{a_{1,2}}u(x_3,\dots,x_n) \\ q_2(x_3,\cdots,x_n) = 2r(x_3,\cdots,x_n) - \frac{2}{a_{1,2}}u(x_3,\dots,x_n)v(x_3,\dots,x_n) \end{cases}$$

On a

$$4\ell_1\ell_2 = (\ell_1+\ell_2)^2 - (\ell_1-\ell_2)^2$$

Il suffit donc de poser $f_1 = \ell_1+\ell_2$, $f_2 = \ell_1-\ell_2$ et d'appliquer l'algorithme à la forme quadratique q_2 (les formes linéaires obtenues ne font intervenir que les variables $x_3,\dots,x_n$: elles sont linéairement indépendantes de $f_1\colon (x_1,\dots,x_n)\mapsto x_1+x_2+\cdots$ et $f_2\colon (x_1,\dots,x_n)\mapsto x_1-x_2+\cdots$).

Exercice 3.1.46. Appliquer l'algorithme à la forme quadratique $q(x,y,z) = xy+yz+xz$ (réponse : $q(x,y,z) = (x+z)(y+z)-z^2 = \frac{1}{4}(x+y+2z)^2 - \frac{1}{4}(x-y)^2 - z^2$).

3.2. **Isométries, adjonction.**

Définition 3.2.1. Soient (V_1,q_1) et (V_2,q_2) deux espaces quadratiques sur K. Une **isométrie** de (V_1,q_1) dans (V_2,q_2) est une application K-linéaire $f\colon V_1\to V_2$ telle que $(\forall v\in V_1)\, q_2(f(v)) = q_1(v)$, *i.e.* qui préserve les formes quadratiques. On dit que (V_1,q_1) et (V_2,q_2) sont **isomorphes** s'il existe une isométrie $f\colon V_1\to V_2$ qui est un isomorphisme (l'application f^{-1} est alors une isométrie).

Remarque 3.2.2. Soient φ_1 et φ_2 les formes polaires de q_1 et q_2 respectivement. Alors $f\colon V_1\to V_2$ est une isométrie si et seulement si $\varphi_2(f(v),f(v')) = \varphi_1(v,v')$ pour tout $v,v'\in V_1$ (cela résulte immédiatement des formules de polarisation).

On fixe désormais (V,q) un espace quadratique de dimension finie sur K avec q *non dégénérée*. On note φ sa forme polaire.

Lemme 3.2.3. L'ensemble des isométries de (V,q) dans lui-même est un sous-groupe de $\mathsf{GL}(V)$.

Démonstration. Si $f\colon V\to V$ est une isométrie, on a $\varphi(f(v),f(v')) = \varphi(v,v')$ pour tout $v,v'\in V$. Si $v\in\mathsf{Ker}(f)$, on a donc $\varphi(v,v') = 0$ pour tout $v'\in V$, *i.e.* $v\in V^\perp = \{0\}$ (car q est non dégénérée). On a donc $\mathsf{Ker}(f) = \{0\}$, de sorte que $f\in\mathsf{GL}(V)$ (rappelons qu'on a supposé $\dim_K(V) < +\infty$). L'ensemble des isométries est évidemment stable par composition et inverse. C'est donc un sous-groupe de $\mathsf{GL}(V)$. □

Définition 3.2.4. Le groupe des isométries $\mathsf{O}(q) = \{f\in\mathsf{GL}(V)\,|\,q\circ f = q\} = \{f\in\mathsf{GL}(V)\,|\,\varphi\circ f = \varphi\}$ de (V,q) dans lui-même, s'appelle le **groupe orthogonal** de (V,q).

3.2.5. *Interprétation matricielle.* Fixons une base $\mathfrak{B}$ de V, et posons $A = \mathrm{Mat}_{\mathfrak{B}}(q)$. Si $f\in\mathsf{GL}(V)$ et $M = \mathrm{Mat}_{\mathfrak{B}}(f)$, la matrice de $q\circ f$ dans $\mathfrak{B}$ est ${}^tMAM$, de sorte que $f\in\mathsf{O}(q)$ si et seulement si ${}^tMAM = A$.

Proposition 3.2.6. Si $f\in\mathsf{O}(q)$, on a $\det(f)\in\{\pm1\}$.

Démonstration. Avec les notations qui précèdent, on a ${}^tMAM = A$, donc $\det({}^tMAM) = \det(A)$, *i.e.* $\det(M)^2\det(A) = \det(A)$. Comme q est non dégénérée, on a $\det(A)\neq 0$, de sorte que $\det(M)^2 = 1$, *i.e.* $\det(f) = \det(M)\in\{\pm1\}$. □

Définition 3.2.7. Le **groupe spécial orthogonal** de q est $\mathsf{SO}(q) = \{f\in\mathsf{O}(q)\,|\,\det(f) = 1\}$. C'est un sous-groupe de $\mathsf{O}(q)$, d'indice 2 lorsque $V\neq\{0\}$.

3.2.8. *Adjoint d'un endomorphisme.*

Proposition 3.2.9. Soit $f \in \mathsf{End}_K(V)$. Il existe un unique élément $f^* \in \mathsf{End}_K(V)$ tel que
$$(\forall v, v' \in V)\ \ \varphi(f(v), v') = \varphi(v, f^*(v'))$$

Démonstration. Si $v' \in V$, on dispose de la forme linéaire $\varphi(f(.), v') \colon v \mapsto \varphi(f(v), v')$. Comme q est non dégénérée, l'application $\mathsf{L}_\varphi \colon V \to V^\vee$ est un isomorphisme (*cf* proposition 3.1.24) : il existe donc $f^*(v') \in V$ unique tel que $\mathsf{L}_\varphi(v') \circ f = \varphi(f(.), v') = \mathsf{L}_\varphi(f^*(v'))$. On a alors $\varphi(f(v), v') = \varphi(v, f^*(v'))$ pour tout $v \in V$. La formule qui précède se réécrit $({}^{\mathrm{t}}f \circ \mathsf{L}_\varphi)(v') = (\mathsf{L}_\varphi \circ f^*)(v')$ pour tout $v' \in V$, et donc ${}^{\mathrm{t}}f \circ \mathsf{L}_\varphi = \mathsf{L}_\varphi \circ f^*$, soit encore
$$f^* = \mathsf{L}_\varphi^{-1} \circ {}^{\mathrm{t}}f \circ \mathsf{L}_\varphi$$
ce qui prouve [4] que $f^* \in \mathsf{End}_K(V)$. □

Définition 3.2.10. L'endomorphisme f^* s'appelle l'**adjoint** de f (pour la forme non-dégénérée q).

Remarque 3.2.11. (1) La formule $f^* = \mathsf{L}_\varphi^{-1} \circ f \circ \mathsf{L}_\varphi$ montre que f^* et f sont semblables. Fixons une base $\mathfrak{B}$ de V, posons $A = \mathrm{Mat}_{\mathfrak{B}}(q)$, $M = \mathrm{Mat}_{\mathfrak{B}}(f)$ et $M^* = \mathrm{Mat}_{\mathfrak{B}}(f^*)$. On a alors $M^* = A^{-1}{}^{\mathrm{t}}MA$ (rappelons que A, qui est aussi la matrice de L_φ dans $\mathfrak{B}$ et $\mathfrak{B}^*$, est inversible parce que q est non dégénérée).

(2) Reformulation de la définition de $\mathsf{O}(q)$. Soit $f \in \mathsf{End}_K(V)$. On a $f \in \mathsf{O}(q)$ si et seulement si $\varphi(f(v), f(v')) = \varphi(v, v')$ pour tout $v, v' \in V$. Comme $\varphi(f(v), f(v')) = \varphi(v, f^* \circ f(v'))$, et φ est non-dégénérée, cela équivaut donc à $f^* \circ f = \mathrm{Id}_V$, *i.e.* $f^* = f^{-1}$. On a donc
$$\mathsf{O}(q) = \{f \in \mathsf{GL}(V) \mid f^* \circ f = \mathrm{Id}_V\}$$

(3) Si $f \in \mathsf{End}_K(V)$, alors on a le diagramme commutatif
$$\begin{array}{ccc} V & \xrightarrow{\mathsf{L}_\varphi} & V^\vee \\ {\scriptstyle f^*}\downarrow & & \downarrow{\scriptstyle {}^{\mathrm{t}}f} \\ V & \xrightarrow{\mathsf{L}_\varphi} & V^\vee \end{array}$$
C'est bien logique : l'isomorphisme L_φ permet d'identifier $V \times V$ muni de φ à $V \times V^\vee$ muni du crochet de la dualité, pour lequel l'adjonction n'est autre que la transposition.

Proposition 3.2.12. Si $f, g \in \mathsf{End}_K(V)$ et $\lambda \in K$, on a $(f^*)^* = f$, $(f \circ g)^* = g^* \circ f^*$ et $(f + \lambda g)^* = f^* + \lambda g^*$.

3.3. **Théorèmes de Cartan-Dieudonné et de Witt.** Dans tout ce numéro, (V, q) est un espace quadratique non dégénéré, et φ la forme polaire de q.

Définition 3.3.1. Soit $W \subset V$ un sous-K-espace vectoriel tel que $W \oplus W^\perp = V$ (comme q est non dégénérée, cela équivaut à $W \cap W^\perp = \{0\}$, soit encore $q_{|W}$ non dégénérée). La **symétrie orthogonale** par rapport à W est la symétrie σ de $V = W \oplus W^\perp$ par rapport à W parallèlement à $W^\perp$: on a $\sigma(w + w') = w - w'$ pour $w \in W$ et $w' \in W^\perp$. Lorsque W est un hyperplan (resp. un sous-espace de codimension 2), on parle de **réflexion** (resp. **renversement**).

Remarque 3.3.2. (1) Si σ est une symétrie orthogonale, on a $\sigma \in \mathsf{O}(q)$. En effet, si $w \in W$ et $w' \in W^\perp$, on a $q(\sigma(w + w')) = q(w - w') = q(w) + q(w') = q(w + w')$ (parce que $\varphi(w, w') = 0$).

(2) Si σ est une réflexion (resp. un reversement), on a $\det(\sigma) = -1$ (resp. $\det(\sigma) = 1$).

Lemme 3.3.3. Si $v_1, v_2 \in V$ sont tels que $q(v_1) = q(v_2) \neq 0$, il existe $\sigma \in \mathsf{O}(q)$, produit d'une ou deux réflexions de V, telle que $\sigma(v_1) = v_2$.

Démonstration. Posons $u = \frac{v_1 + v_2}{2}$ et $v = \frac{v_1 - v_2}{2}$: on a $v_1 = u + v$ et $v_2 = u - v$ et $\varphi(u, v) = \frac{q(v_1) - q(v_2)}{4} = 0$. On a $q(u) = \frac{q(v_1) + 2\varphi(v_1, v_2) + q(v_2)}{4}$ et $q(v) = \frac{q(v_1) - 2\varphi(v_1, v_2) + q(v_2)}{4}$, de sorte que $q(u) + q(v) = q(v_1) \neq 0$: on a $q(u) \neq 0$ ou $q(v) \neq 0$.

• Si $q(u) \neq 0$, soit σ_1 la réflexion par rapport à l'hyperplan $u^\perp$ (cela a un sens car $q(u) \neq 0 \Rightarrow u^\perp \cap Ku = \{0\}$). On a $\sigma_1(u) = -u$ et $\sigma_1(v) = v$ (parce que $v \in u^\perp$), de sorte que $\sigma_1(v_1) = \sigma_1(u + v) = -u + v = -v_2$. Soit σ_2 la réflexion par rapport à l'hyperplan $v_2^\perp$ (rappelons que $q(v_2) \neq 0$) : on a $\sigma_2(v_2) = -v_2$, donc $\sigma = \sigma_2 \circ \sigma_1 \in \mathsf{O}(q)$ vérifie $\sigma(v_1) = v_2$.

• Si $q(v) \neq 0$, soit σ la réflexion par rapport à $v^\perp$. On a $\sigma(u) = u$ et $\sigma(v) = -v$ (parce que u et v sont orthogonaux), de sorte que $\sigma(v_1) = \sigma(u + v) = u - v = v_2$. □

4. On peut démontrer que $f^* \in \mathsf{End}_K(V)$ de façon pédestre : si $v, v', v'' \in V$ et $\lambda \in K$, on a $\varphi(v, f^*(v' + \lambda v'')) = \varphi(f(v), v' + \lambda v'') = \varphi(f(v), v') + \lambda\varphi(f(v), v'') = \varphi(v, f^*(v')) + \lambda\varphi(v, f^*(v'')) = \varphi(v, f^*(v') + \lambda f^*(v''))$, *i.e.* $\varphi(v, f^*(v') + \lambda f^*(v'') - f^*(v' + \lambda v'')) = 0$. Comme φ est non dégénérée, cela implique $f^*(v' + \lambda v'') = f^*(v') + \lambda f^*(v'')$, *i.e.* $f^* \in \mathsf{End}_K(V)$.

Remarque 3.3.4. Reprenons les notations du lemme 3.3.3. Dans le cas où $q(u) \neq 0$, on peut aussi considérer la symétrie orthogonale par rapport à Ku (ce n'est autre que $-\sigma_1$). On a alors $\sigma(u) = u$ et $\sigma(v) = -v$ (parce que u et v sont orthogonaux), de sorte que $\sigma(v_1) = v_2$. Cela montre que sous les hypothèses du lemme 3.3.3, il existe une symétrie orthogonale σ de V telle que $\sigma(v_1) = v_2$.

3.3.5. *Théorème de Cartan-Dieudonné.*

Proposition 3.3.6. (Cartan-Dieudonné, version faible) Tout élément de $\mathsf{O}(q)$ s'écrit comme produit d'au plus $2\dim_K(V)$ réflexions. En particulier, les réflexions engendrent $\mathsf{O}(q)$.

Démonstration. Soit $f \in \mathsf{O}(q)$. On procède par récurrence sur $n = \dim_K(V)$, le cas $n = 1$ étant trivial car alors $f \in \{\pm \mathrm{Id}_V\}$. Si $n > 1$, il existe une base orthogonale $(e_1, \dots, e_n)$ de V pour q (*cf* théorème 3.1.41). Comme $f \in \mathsf{O}(q)$, on a $q(f(e_1)) = q(e_1)$: d'après le lemme 3.3.3, il existe $\sigma \in \mathsf{O}(q)$ produit d'une ou deux réflexions, telle que $\sigma(e_1) = f(e_1)$. Cela implique que $f_1 := \sigma^{-1} \circ f$ vérifie $f_1(e_1) = e_1$. Comme $f_1 \in \mathsf{O}(q)$, on a $f_1(e_1^\perp) = e_1^\perp$: par hypothèse de récurrence, la restriction de f_1 à $e_1^\perp$ (qui est de dimension $n-1$) s'écrit comme un produit de $r \leqslant 2(n-1)$ réflexions $\sigma_1 \circ \cdots \sigma_r$ de $e_1^\perp$. Pour $i \in \{1, \dots, r\}$, on prolonge σ_i à V en posant $\sigma_i(e_1) = e_1$: l'application σ_i ainsi obtenue est une réflexion de V, et $f_1 = \sigma_1 \circ \cdots \sigma_r$, si bien que $f = \sigma \circ \sigma_1 \circ \cdots \circ \sigma_r$ est produit d'au plus $r + 2 \leqslant 2n$ réflexions. □

Lemme 3.3.7. Si $\dim_K(V) \geqslant 3$ et σ_1, σ_2 sont des réflexions, alors il existe des renversements τ_1 et τ_2 tels que $\sigma_1 \circ \sigma_2 = \tau_1 \circ \tau_2$.

Démonstration. • Si $\dim_K(V) = 3$, alors $\tau_i = -\sigma_i$ est un reversement pour $i \in \{1, 2\}$, et $\sigma_1 \circ \sigma_2 = \tau_1 \circ \tau_2$.
• Supposons désormais $\dim_K(V) > 3$. Soient H_1 et H_2 les hyperplans de σ_1 et σ_2 respectivement. On peut supposer $H_1 \neq H_2$ (sinon $\sigma_1 \circ \sigma_2 = \mathrm{Id}_V$ et on prend $\tau_1 = \tau_2$ un renversement quelconque). On a $H_1 = v_1^\perp$ et $H_2 = v_2^\perp$ avec v_1 et v_2 non isotropes. Le plan $P = \mathsf{Vect}(v_1, v_2)$ n'est pas totalement isotrope, et $P^\perp = H_1 \cap H_2$ est de dimension $\dim_K(V) - 2$. En particulier, on n'a pas $P \subset P^\perp = H_1 \cap H_2$, *i.e.* $\dim_K(P \cap P^\perp) \leqslant 1$. Comme $P^\perp = (P \cap P^\perp) \oplus W$ avec W non dégénérée (corollaire 3.1.44), il existe $W' \subset P^\perp$ non dégénéré et de dimension $\dim_K(V) - 3$. D'après le corollaire 3.1.28, on a $V = W' \oplus W'^\perp$. La restriction de $\sigma_1 \circ \sigma_2$ à W' est l'identité, et sa restriction à $W'^\perp$ est un produit de deux réflexions. Comme $\dim_K(W'^\perp) = 3$, le premier cas montre que cette restriction est le produit de deux renversements τ_1' et τ_2', qu'on prolonge à V par l'identité sur W' en τ_1 et τ_2 respectivement. On a alors $\sigma_1 \circ \sigma_2 = \tau_1 \circ \tau_2$. □

Corollaire 3.3.8. Si $\dim_K(V) \geqslant 3$, le groupe $\mathsf{SO}(q)$ est engendré par les renversements.

Démonstration. D'après la proposition 3.3.6, un élément de $\mathsf{SO}(q)$ est le produit d'un nombre *pair* de réflexions, et donc aussi le produit d'un nombre (pair) de renversements (*cf* lemme 3.3.7). □

Théorème 3.3.9. (Cartan-Dieudonné) Tout élément de $\mathsf{O}(q)$ s'écrit comme produit d'au plus $\dim_K(V)$ réflexions.

Démonstration. Soit $f \in \mathsf{O}(q)$. On procède par récurrence sur $n = \dim_K(V)$. Si $\dim_K(V) = 1$, on a $\mathsf{O}(q) = \{\pm \mathrm{Id}_V\}$. Supposons $\dim_K(V) = 2$. Soit $v \in V$ non isotrope. On a $q(v) = q(f(v)) \neq 0$: d'après la remarque 3.3.4, il existe une réflexion σ telle que $f(v) = \sigma(v)$ (la remarque fournit une réflexion parce que $\dim_K(V) = 2$). On a alors $\sigma^{-1} \circ f(v) = v$, et $\sigma^{-1} \circ f$ laisse stable la droite $v^\perp$. La restriction à cette droite est donc soit l'identité, soit la multiplication par -1, de sorte que $\sigma^{-1} \circ f = \mathrm{Id}_V$ ou $\sigma^{-1} \circ f = \sigma'$ ou σ' est la réflexion d'axe Kv. On a donc $f \in \{\sigma, \sigma \circ \sigma'\}$, ce qui prouve le théorème dans ce cas. Supposons maintenant $\dim_K(V) > 2$.
Premier cas : il existe $v \in \mathsf{Ker}(f - \mathrm{Id}_V)$ non isotrope. On a $V = Kv \oplus v^\perp$ et $f(v) = v$: le sous-espace $v^\perp$ est stable par f. Par récurrence, f est produit d'au plus $n-1$ réflexions (étendues par l'identité sur Kv).
Deuxième cas : il existe $v \in V$ non isotrope tel que $f(v) - v$ soit non isotrope. Notons σ la réflexion d'hyperplan $(f(v) - v)^\perp$. On a $\sigma(f(v) - v) = v - f(v)$. En outre, $\sigma(f(v) + v) = f(v) + v$ (parce que $\varphi(f(v) - v, f(v) + v) = q(f(v)) - q(v) = 0$, *i.e.* $f(v) + v \in (f(v) - v)^\perp$). En sommant, il vient $\sigma(f(v)) = v$: comme dans le premier cas, $\sigma \circ f$ est alors produit d'au plus $n-1$ réflexions, et donc f d'au plus n réflexions.
Troisième cas : $\mathsf{Ker}(f - \mathrm{Id}_V)$ est un SETI et pour tout $v \in V$ non isotrope, le vecteur $f(v) - v$ est isotrope.
• Montrons que dans ce cas $\mathsf{Im}(f - \mathrm{Id}_V)$ est un SETI. Vu l'hypothèse, il suffit de montrer que si $v \in V$ isotrope, alors $(f - \mathrm{Id}_V)(v)$ aussi. On a $\dim_K(V^\perp) = n - 1 > \frac{n}{2}$: l'espace $v^\perp$ n'est pas totalement isotrope. Soit $w \in v^\perp$ non isotrope. Les vecteurs w, $v + w$ et $v - w$ sont alors non isotropes. D'après l'hypothèse, leurs image par $f - \mathrm{Id}_V$ est isotrope. On a donc

$$0 = q((f - \mathrm{Id}_V)(v + w)) + q((f - \mathrm{Id}_V)(v - w)) - 2q((f - \mathrm{Id}_V)(w)) = 2q((f - \mathrm{Id}_V)(v))$$

• On a $\dim_K(\mathsf{Ker}(f-\mathrm{Id}_V)) \leqslant \frac{n}{2}$ et $\dim_K(\mathsf{Im}(f-\mathrm{Id}_V)) \leqslant \frac{n}{2}$. D'après le théorème du rang, on a $\dim_K(\mathsf{Ker}(f-\mathrm{Id}_V))+\dim_K(\mathsf{Im}(f-\mathrm{Id}_V)) = n$: cela implique que $\mathsf{Ker}(f-\mathrm{Id}_V)$ et $\mathsf{Im}(f-\mathrm{Id}_V)$ sont des SETI de dimension $\frac{n}{2}$. Cela prouve que V est hyperbolique, et donc de dimension paire $n = 2d$. Soit $(e_1,\dots,e_d)$ une base de $\mathsf{Ker}(f-\mathrm{Id}_V)$: il existe une famille $(e_{d+1},\dots,e_n)$ telle que $H_i = \mathsf{Vect}(e_i, e_{d+i})$ soit un plan hyperbolique et V somme directe orthogonale des H_i (*cf* lemme 3.1.34). Pour tout $i \in \{1,\dots,d\}$, on a $f(e_i) = e_i$. Écrivons $f(e_{d+i}) = \sum_{j=1}^n a_{i,j}e_j$. On a $\delta_{i,k} = \varphi(e_i, e_{d+k}) = \varphi(f(e_i), f(e_{d+k})) = \sum_{j=1}^n a_{k,j}\varphi(e_i,e_j) = a_{k,i}$. Cela implique que la matrice de f dans la base $\mathfrak{B} = (e_1,\dots,e_n)$ est de la forme $\left(\begin{smallmatrix} \mathrm{I}_d & A \\ 0 & \mathrm{I}_d \end{smallmatrix}\right)$, et $\det(f) = 1$. Cela prouve que ce cas ne se produit pas et donc que que le théorème est vrai lorsque $\det(f) = -1$. Si $\det(f) = 1$, et si σ est une réflexion, alors $\det(\sigma\circ f) = -1$: cela implique que $\sigma\circ f$ est produit d'au plus n réflexions d'après ce qui précède. Comme n est pair et $\det(\sigma\circ f) = -1$, le nombre de réflexions est impair : $\sigma\circ f$ est produit d'au plus $n-1$ réflexions, et donc f d'au plus n réflexions. □

Corollaire 3.3.10. Si $\dim_K(V) \geqslant 3$, tout élément de $\mathsf{SO}(q)$ est produit d'au plus $\dim_K(V)$ renversements.

Démonstration. Résulte du théorème 3.3.9 et du lemme 3.3.7. □

Proposition 3.3.11. Soit $f \in \mathsf{O}(q)$.
(1) Si f est un produit de r réflexions, alors $\dim_K(\mathsf{Ker}(f-\mathrm{Id}_V)) \geqslant \dim_K(V) - r$.
(2) Si $\mathsf{Ker}(f-\mathrm{Id}_V) = \{0\}$, alors f ne peut pas s'écrire comme un produit de moins de n réflexions.

Démonstration. (1) Écrivons $f = \sigma_1\circ\cdots\circ\sigma_r$ comme un produit de r réflexions. Si $W_i = \mathsf{Ker}(\sigma_i - \mathrm{Id}_V)$ est l'hyperplan fixé par σ_i, alors $W_1\cap\cdots\cap W_r$ est fixe par f. On a donc $\dim_K(\mathsf{Ker}(f-\mathrm{Id}_V)) \geqslant \dim_K(W_1\cap\cdots\cap W_r) \geqslant \dim_K(V) - r$. (2) est une conséquence immédiate de (1). □

3.3.12. *Le centre de* $\mathsf{O}(q)$ *et de* $\mathsf{SO}(q)$ (*cas où* $\dim_K(V) \geqslant 3$). Dans ce numéro, on suppose que $\dim_K(V) \geqslant 3$.

Lemme 3.3.13. Toute droite de V est intersection de deux plans non dégénérés.

Démonstration. Soit $v \in V\backslash\{0\}$. Supposons v non isotrope. Soit $w, w' \in v^\perp$ non isotropes et orthogonaux (premiers vecteurs d'une base orthogonale de $v^\perp$) : on a $Kv = P\cap P'$ avec $P = \mathsf{Vect}(v,w)$ et $P' = \mathsf{Vect}(v,w')$ des plans non dégénérés.
Si v est isotrope, il existe $w \in V$ tel que $P = \mathsf{Vect}(v,w)$ soit un plan hyperbolique. Comme $\dim_K(V) \geqslant 3$, on a $P \neq V$. Comme $v^\perp \neq V$ (c'est un hyperplan), on a $P\cup v^\perp \neq V$ (une réunion de sous-espaces vectoriels est un sous-espace vectoriel si et seulement si l'un est inclus dans l'autre) : soient $w' \in V\backslash(v^\perp\cup P)$ et $P' = \mathsf{Vect}(v,w')$. Le plan P' est hyperbolique (parce que $\varphi(v,w') \neq 0$), et $Kv = P\cap P'$ (parce que $w' \notin P$). □

Proposition 3.3.14. Le centre de $\mathsf{O}(q)$ est $\{\pm\mathrm{Id}_V\}$. Le centre de $\mathsf{SO}(q)$ et $\{\pm\mathrm{Id}_V\}$ si $\dim_K(V)$ est paire, $\{\mathrm{Id}_V\}$ si $\dim_K(V)$ est impaire.

Démonstration. Soit $f \in \mathsf{O}(q)$ qui commute à tous les éléments de $\mathsf{SO}(q)$. Soit $v \in V\backslash\{0\}$: d'après le lemme 3.3.13, il existe des plans non dégénérés P et P' tels que $Kv = P\cap P'$. Alors f commute aux symétries orthogonales σ et σ' par rapport aux plans $P^\perp$ et $P'^\perp$ (car $\sigma,\sigma' \in \mathsf{SO}(q)$). Cela implique que $f(P) = P$ et $f(P') = P'$, de sorte que $f(Kv) = Kv$. Comme c'est vrai pour tout $v \in V\backslash\{0\}$, cela implique que f est une homothétie. Écrivons $f = \lambda\,\mathrm{Id}_V$: comme $f^* = \lambda\,\mathrm{Id}_V$ et $f^*\circ f = \mathrm{Id}_V$, on a $\lambda^2 = 1$ et donc $f \in \{\pm\mathrm{Id}_V\}$. □

Remarque 3.3.15. L'hypothèse $\dim_K(V) \geqslant 3$ n'est pas superflue, comme on va le voir dans le prochain paragraphe.

3.3.16. *Les groupes* $\mathsf{O}(q)$ *et* $\mathsf{SO}(q)$ (*cas où* $\dim_K(V) = 2$). Dans ce numéro, on suppose que $\dim_K(V) = 2$. D'après le corollaire 3.1.36, on a deux cas : (V,q) est un plan hyperbolique ou (V,q) est anisotrope.

Proposition 3.3.17. Si (V,q) est un plan hyperbolique, alors $\mathsf{SO}(q)$ est abélien et $\mathsf{Z}(\mathsf{O}(q)) = \{\pm\mathrm{Id}_V\}$ sauf si V est un plan hyperbolique et $K = \mathbf{F}_3$ (cas dans lequel $\mathsf{O}(q) \simeq (\mathbf{Z}/2\,\mathbf{Z})^2$).

Démonstration. Comme (V,q) est hyperbolique, il existe une base dans laquelle la matrice de q est $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Si $f \in \mathsf{O}(q)$ a pour matrice $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, la relation $A = {}^tMAM$ équivaut à $2ac = 2bd = 0$ et $ad + bc = 1$. Si $a = 0$, on a $bc = 1$ donc $d = 0$ et $\left(\begin{smallmatrix} 0 & b \\ b^{-1} & 0 \end{smallmatrix}\right)$ avec $b \in K^\times$. Si $c = 0$, on a $ad = 1$ donc $b = 0$ et $M = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ avec $a \in K^\times$. Cela implique que $\mathsf{SO}(q) \simeq \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right) \,\middle|\, a \in K^\times \right\} \simeq K^\times$ est abélien. Par ailleurs, si $f \in \mathsf{Z}(\mathsf{O}(q))$, alors M commute à $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ ce qui implique que $M \in \{\pm\mathrm{I}_2, \pm A\}$. Le groupe $\mathsf{O}(q)$ est alors abélien si et seulement si $K = \mathbf{F}_3$. Si $K \neq \mathbf{F}_3$, il existe $x \in K^\times$ tel que $x^2 \neq 1$, et A ne commute pas à $\left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right)$, ce qui montre que $M \in \{\pm\mathrm{I}_2\}$, et donc $\mathsf{Z}(\mathsf{O}(q)) = \{\pm\mathrm{Id}_V\}$. □

Lemme 3.3.18. Supposons (V,q) anisotrope. Si $f \in \mathsf{SO}(q)$ et $\mathsf{Ker}(f - \mathrm{Id}_V) \neq \{0\}$, alors $f = \mathrm{Id}_V$. Les éléments de $\mathsf{O}(q)\backslash\mathsf{SO}(q)$ sont les réflexions, et tout élément de $\mathsf{SO}(q)$ peut s'écrire comme produit de deux réflexions, l'une des deux pouvant être choisie arbitrairement.

Démonstration. • Soient $f \in \mathsf{SO}(q)$ et $v \in V\backslash\{0\}$ tels que $f(v) = v$. Comme f est une isométrie, on a $f(v^\perp) = v^\perp$, et $f_{|v^\perp} \in \mathsf{O}(q_{|v^\perp}) = \{\pm \mathrm{Id}_{v^\perp}\}$. Comme $\det(f) = 1$, on a nécessairement $f_{|v^\perp} = \mathrm{Id}_{v^\perp}$, et donc $f = \mathrm{Id}_V$.
• Soit $f \in \mathsf{O}(q)\backslash\mathsf{SO}(q)$. Fixons $v \in V\backslash\{0\}$. On a $q(f(v)) = q(v) \neq 0$ (car q est anisotrope) : d'après le lemme 3.3.3 (ou même la remarque 3.3.4), il existe une réflexion σ telle que $f(v) = \sigma(v)$. Alors $f_1 = \sigma^{-1} \circ f \in \mathsf{SO}(q)$ et $f_1(v) = v$. D'après ce qu'on vient de voir, on a $f_1 = \mathrm{Id}_V$, *i.e.* $f = \sigma$.
• Soient $f \in \mathsf{SO}(q)$ et σ_0 une réflexion quelconque. Alors $\sigma = f \circ \sigma_0^{-1} \in \mathsf{O}(q)\backslash\mathsf{SO}(q)$, ce qui implique que σ est une réflexion d'après ce qui précède. Il en résulte que $f = \sigma \circ \sigma_0$ est produit de deux réflexions (la réflexion σ_0 ayant été fixée à l'avance). □

Proposition 3.3.19. Si (V,q) est anisotrope, alors $\mathsf{SO}(q)$ est abélien et $\mathsf{Z}(\mathsf{O}(q)) = \{\pm \mathrm{Id}_V\}$.

Démonstration. • Si $f \in \mathsf{Z}(\mathsf{O}(q))$ et $v \in V\backslash\{0\}$, alors f commute à la réflexion par rapport à Kv (qui existe vu que $q(v) \neq 0$), ce qui montre que la famille $\{v, f(v)\}$ est liée : l'argument habituel montre que f est une homothétie, et donc $f \in \{\pm \mathrm{Id}_V\}$, de sorte que $\mathsf{Z}(\mathsf{O}(q)) = \{\pm \mathrm{Id}_V\}$.
• Soient $f_1, f_2 \in \mathsf{SO}(q)$. Choisissons une réflexion σ_0. D'après le lemme 3.3.18, il existe une réflexion σ_1 telle que $f_1 = \sigma_1 \circ \sigma_0$. De même, il existe une réflexion σ_2 telle que $f_2 = \sigma_2 \circ \sigma_1$. Comme $\sigma := \sigma_2 \circ \sigma_0 \circ \sigma_1 \in \mathsf{O}(q)\backslash\mathsf{SO}(q)$, c'est une réflexion. C'est donc une involution : on a $\sigma = \sigma^{-1} = \sigma_1^{-1} \circ \sigma_0^{-1} \circ \sigma_2^{-1}$ et donc $\sigma_2 \circ \sigma_0 \circ \sigma_1 = \sigma_1 \circ \sigma_0 \circ \sigma_2$. En composant par σ_1 à droite, on a donc $\sigma_2 \circ \sigma_0 = \sigma_1 \circ \sigma_0 \circ \sigma_2 \circ \sigma_1$, *i.e.* $f_2 \circ f_1 = f_1 \circ f_2$. Cela montre que $\mathsf{SO}(q)$ est abélien. □

Exemple 3.3.20. On a $\mathsf{SO}_2(\mathbf{R}) = \left\{ \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \,\middle|\, \theta \in \mathbf{R} \right\} \simeq \mathbf{R}/2\pi\,\mathbf{Z}$.

Remarque 3.3.21. On a montré que $\mathsf{SO}(q)$ est abélien dans tous les cas lorsque $\dim_K(V) = 2$.

3.3.22. *Théorèmes de Witt applications.*

Théorème 3.3.23. (Witt, simplification des espaces quadratiques) Soient (V_1,q_1), (V_2,q_2) et (W,q) trois espaces quadratiques *non-dégénérés* tels que $(V_1 \oplus W, q_1 \oplus q) \simeq (V_2 \oplus W, q_2 \oplus q)$. Alors $(V_1,q_1) \simeq (V_2,q_2)$.

Démonstration. Comme W admet des bases orthogonales (*cf* théorème 3.1.41), il suffit de traiter le cas où $\dim_K(W) = 1$. Écrivons $W = Ke$, et fixons $f : V_1 \oplus W \to V_2 \oplus W$ une isométrie. On a $(q_2 \oplus q)(f(0_{V_1} \oplus e)) = (q_1 \oplus q)(0_{V_1} \oplus e) = q(e) = (q_2 \oplus q)(0_{V_2} \oplus e)$: d'après le lemme 3.3.3, il existe $\sigma \in \mathsf{O}(q_2 \oplus q)$ telle que $\sigma(f(0_{V_1} \oplus e)) = 0_{V_2} \oplus e$, de sorte que l'isométrie $\sigma \circ f$ envoie $\{0_{V_1}\} \oplus W$ sur $\{0_{V_2}\} \oplus W$. Elle induit donc une isométrie entre les orthogonaux $V_1 \otimes \{0_W\} \simeq V_1$ et $V_2 \otimes \{0_W\} \simeq V_2$. □

Théorème 3.3.24. (Witt, prolongement des isomorphismes) Soient (V,q) un espace quadratique *non-dégénéré*, W un sous-K-espace vectoriel de V et $f : W \to V$ une application injective et isométrique (*i.e.* telle que $q \circ f = q_{|W}$). Alors il existe $\widetilde{f} \in \mathsf{O}(q)$ telle que $\widetilde{f}_{|W} = f$, *i.e.* f se prolonge en une isométrie de V.

Démonstration. Commençons par observer que grâce aux formules de polarisation, l'hypothèse implique que f préserve φ, *i.e.* que $(\forall w_1, w_2 \in W)\, \varphi(f(w_1), f(w_2)) = \varphi(w_1, w_2)$. On procède par récurrence sur $\dim_K(V)$. Le cas $\dim_K(W) = 0$ est trivial : supposons que $W \neq \{0\}$.
Premier cas : W n'est pas totalement isotrope : soit $w \in W$ tel que $q(w) \neq 0$. On a $V = Kw \oplus w^\perp$ donc $W = Kw \oplus (W \cap w^\perp)$. Par ailleurs, comme $q(f(w)) = q(w) \neq 0$, il existe $\sigma \in \mathsf{O}(q)$ telle que $\sigma(w) = f(w)$ (*cf* lemme 3.3.3), de sorte que $f_1 := \sigma^{-1} \circ f$ vérifie $f_1(w) = w$. Comme $\sigma \in \mathsf{O}(q)$, on a en outre $(\forall w_1, w_2 \in W)\, \varphi(f_1(w_1), f_1(w_2)) = \varphi(w_1, w_2)$. Cela implique que $f_1(W \cap w^\perp) \subset w^\perp$. On applique l'hypothèse de récurrence à $f_{1|w^\perp}$ (qui est une application injective et isométrique $W \cap w^\perp \to w^\perp$) : il existe $\widetilde{f}_{1|w^\perp} \in \mathsf{O}(w^\perp)$ qui la prolonge. On étend $\widetilde{f}_{1|w^\perp}$ à V en posant $\widetilde{f}_1(w) = w$: on a $\widetilde{f}_1 \in \mathsf{O}(q)$ et $\widetilde{f}_{1|W} = f_1 = \sigma^{-1} \circ f$, de sorte que $f = \widetilde{f}_{|W}$ avec $\widetilde{f} = \sigma \circ \widetilde{f}_1 \in \mathsf{O}(q)$.
Deuxième cas : W est totalement isotrope. Soit $(u_1, \ldots, u_d)$ une base de W. D'après le lemme 3.1.34, il existe une famille $(v_1, \ldots, v_d)$ de V telle que $H_i = \mathsf{Vect}(u_i, v_i)$ soit un plan hyperbolique pour tout $i \in \{1, \ldots, d\}$ et $H_1, \ldots, H_d$ sont deux à deux orthogonaux. Comme f est injective, la famille $(f(u_1), \ldots, f(u_d))$ est une base de $f(W)$, qui est lui aussi totalement isotrope (parce que $q \circ f = q_{|W}$). D'après le lemme 3.1.34, il existe une famille $(v'_1, \ldots, v'_d)$ de V telle que $H'_i = \mathsf{Vect}(f(u_i), v'_i)$ soit un plan hyperbolique pour tout

$i \in \{1, \dots, d\}$ et $H'_1, \dots, H'_d$ sont deux à deux orthogonaux. Posons alors $W' = \mathsf{Vect}(u_1, \dots, u_d, v_1, \dots, v_d)$ et définissons $f' \colon W' \to V$ en posant $f'(u_i) = f(u_i)$ et $f'(v_i) = v'_i$ pour $i \in \{1, \dots, d\}$. On a bien sûr $f'_{|W} = f$, et $q \circ f' = q_{|W'}$. Comme W' est non dégénéré, cela nous ramène au premier cas : il existe $\widetilde{f} \in \mathsf{O}(q)$ tel que $\widetilde{f}_{|W'} = f'$, et donc $\widetilde{f}_{|W} = f$. □

Remarque 3.3.25. On peut déduire le théorème 3.3.23 du théorème 3.3.24. Soit $h \colon V_1 \oplus W \to V_2 \oplus W$ une isométrie. Posons $V = V_1 \oplus W$. On part de l'application $f \colon \{0_{V_1}\} \oplus W \to V$ définie par $f(w) = h^{-1}(0_{V_2} \oplus w)$. Elle est certainement injective et isométrique pour $q_1 \oplus q$: d'après le théorème 3.3.24, elle se prolonge en $\widetilde{f} \in \mathsf{O}(q_1 \oplus q)$. L'isométrie $h \circ \widetilde{f}$ envoie donc $\{0_{V_1}\} \oplus W$ dans $\{0_{V_2}\} \oplus W$: elle induit une isométrie entre les orthogonaux $V_1 \oplus \{0_W\} \simeq V_1$ et $V_2 \oplus \{0_W\} \simeq V_2$.

Soit $d \in \mathbf{N}$. Si $f \in \mathsf{O}(q)$ et W est un SETI de dimension d de V, il en est de même de $f(W)$: on en déduit une action du groupe $\mathsf{O}(q)$ sur l'ensemble des SETI de dimension d de V.

Corollaire 3.3.26. Cette action est transitive.

Démonstration. Soient W et W' deux SETI de dimension d. Soient $\iota \colon W \to W'$ un isomorphisme K-linéaire (il en existe puisque $\dim_K(W) = \dim_K(W')$) et f le composé de ι et de l'inclusion de W' dans V. On a $q \circ f = 0 = q_{|W}$: d'après le théorème 3.3.24, f se prolonge en $\widetilde{f} \in \mathsf{O}(q)$, et $\widetilde{f}(W) = W'$. □

Corollaire 3.3.27. Tous les SETIM ont tous même dimension.

Démonstration. Soient W et W' deux SETIM de V. Quitte à les échanger, on peut supposer que $\dim_K(W) \leqslant \dim_K(W')$. Soit W'' un sous-K-espace vectoriel de W' de dimension $\dim_K(W)$. Alors W'' est un SETI, et d'après le corollaire 3.3.26, il existe $f \in \mathsf{O}(q)$ tel que $f(W'') = W$. On a alors $W \subset f(W')$: comme $f(W')$ est un SETI et W un SETIM, on a nécessairement $W = f(W')$, de sorte que $\dim_K(W) = \dim_K(W')$. □

Définition 3.3.28. L'**indice d'isotropie** de V est la dimension δ commune à tous les SETIM de V.

Remarque 3.3.29. Il résulte de ce qui précède que l'action de $\mathsf{O}(q)$ sur l'ensemble des SETI a $\delta + 1$ orbites.

Corollaire 3.3.30. L'entier d du corollaire 3.1.36 est égal à l'indice d'isotropie de V.

Démonstration. Soit $V = H_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} H_d \overset{\perp}{\oplus} W$ une décomposition de V comme dans le corollaire 3.1.36. Si L est un lagrangien de l'espace hyperbolique $H_1 \oplus \cdots \oplus H_d$, alors $\dim_K(L) = d$ et L est un SETI de V : on a $d \leqslant \delta$. Supposons $d < \delta$: le SETI L est strictement inclus dans un SETIM. Il existe donc $v \in L^\perp \backslash L$ isotrope. Mais $L^\perp = L \oplus W$: cela contredit le fait que W est anisotrope. On a donc $d = \delta$. □

Corollaire 3.3.31. La classe d'isomorphisme du module quadratique anisotrope $(W, q_{|W})$ du corollaire 3.1.36 ne dépend que de la classe d'isomorphisme de (V, q), et pas de la décomposition.

Démonstration. Soient $V = H_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} H_d \overset{\perp}{\oplus} W$ et $V = H'_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} H'_{d'} \overset{\perp}{\oplus} W'$ deux décompositions comme dans le 3.1.36. D'après le corollaire 3.3.30, on a $d = d' = \delta$ (l'indice d'isotropie de (V, q)). Le théorème 3.3.23 appliqué d fois permet de montrer que $H_k \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} H_d \overset{\perp}{\oplus} W \simeq H'_k \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} H'_{d'} \overset{\perp}{\oplus} W'$ pour tout $k \in \{1, \dots, d+1\}$ (en simplifiant successivement par $H_1 \simeq H'_1$, $H_2 \simeq H'_2$, *etc*), ce qui montre que $W \simeq W'$ (comme modules quadratiques). □

L'énoncé suivant précise les corollaires 3.1.36 et 3.3.30.

Corollaire 3.3.32. Soit L un SETIM de V. Alors il existe un espace hyperbolique H de V dont L est un lagrangien, $V = H \oplus H^\perp$ et $H^\perp$ est anisotrope.

Démonstration. Soit $(e_1, \dots, e_\delta)$ une base de L. D'après le lemme 3.1.34, il existe une famille $(e_{\delta+1}, \dots, e_{2\delta})$ telle que $H = \mathsf{Vect}(e_1, \dots, e_{2\delta})$ soit un espace hyperbolique, dont L est un lagrangien. Comme H est non dégénéré, on a $V = H \oplus H^\perp$. Si $v \in H^\perp$ est isotrope et non nul, alors $L \oplus Kv$ est un SETI, ce qui contredit la fait que L est un SETIM : l'espace $H^\perp$ est anisotrope. □

3.4. **Classification des espaces quadratiques.** Soit V un K espace vectoriel de dimension finie.

Définition 3.4.1. Deux formes quadratiques q_1 et q_2 sur V sont **équivalentes** lorsque les modules quadratiques (V, q_1) et (V, q_2) sont isomorphes, *i.e.* lorsqu'il existe $u \in \mathsf{GL}(V)$ tel que $q_2 = q_1 \circ u$. Si $\mathfrak{B}$ est une base de V, cela signifie que les matrices de q_2 et q_1 dans $\mathfrak{B}$ sont congruentes. C'est une relation d'équivalence.

Classifier les formes quadratiques sur K signifie décrire les classes d'isomorphismes de modules quadratiques sur K.
Dans ce qui suit, on se donne une forme quadratique q sur V.

3.4.2. *Cas d'un corps algébriquement clos.* Dans ce numéro, on suppose K algébriquement clos.

Proposition 3.4.3. Il existe une base de V dans laquelle la matrice de q est

$$\mathsf{diag}(\underbrace{1,\dots,1}_{r \text{ fois}},0,\dots,0) = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \end{pmatrix}$$

où r est le rang de q.

Démonstration. D'après le théorème 3.1.41, il existe une base orthogonale $(e_1, \dots, e_n)$. Quitte à permuter les vecteurs de base, on peut supposer que $q(e_i) \neq 0$ pour $i \in \{1, \dots, r\}$ et $q(e_i) = 0$ pour $i \in \{r+1, \dots, n\}$. Comme K est algébriquement clos, il existe $\alpha_i \in K^\times$ tel que $\alpha_i^2 = q(e_i)$ pour $i \in \{1, \dots, r\}$. La famille $(\alpha_1^{-1}e_1, \dots \alpha_r^{-1}e_r, e_{r+1}, \dots, e_n)$ est une base de V, dans laquelle la matrice de q est $\mathsf{diag}(\underbrace{1,\dots,1}_{r \text{ fois}},0,\dots,0)$. □

Théorème 3.4.4. Un espace quadratique sur K algébriquement clos est entièrement déterminé, à isomorphisme près, par sa dimension et son rang.

Démonstration. On sait déjà que deux modules quadratiques isomorphes ont même dimension et même rang (*cf* remarque 3.1.25 (1)). Réciproquement, si (V, q) et (V', q') ont même dimension n et même rang r, ils sont tous les deux isomorphes à $r\langle 1\rangle + (n-r)\langle 0\rangle$. □

Corollaire 3.4.5. En dimension n, il y a une seule classe d'isomorphisme de formes quadratiques non dégénérées sur $\mathbf{C}$.

3.4.6. *Cas du corps* $\mathbf{R}$. Dans ce numéro, on suppose $K = \mathbf{R}$.

Définition 3.4.7. On dit que q est **positive** (resp. **définie positive**) si

$$(\forall v \in V)\ \ q(v) \geqslant 0 \quad (\text{resp. } (\forall v \in V\backslash\{0\})\ \ q(v) > 0)$$

On définit de même les notions de forme quadratique **négative** ou **définie négative**.

Exemples 3.4.8. On se place dans $V = \mathbf{R}^2$.
(1) $q_1(x, y) = x^2 + y^2$ est définie positive.
(2) $q_2(x, y) = x^2$ est positive, mais pas définie positive.
(3) $q_3(x, y) = x^2 - y^2$ n'est ni positive, ni négative.

Théorème 3.4.9. (Cauchy-Schwarz). Supposons q positive. Pour tout $v_1, v_2 \in V$, on a

$$\varphi(v_1, v_2)^2 \leqslant q(v_1)q(v_2)$$

Il y a égalité si v_1 et v_2 sont colinéaires. Si q est définie positive, il y a égalité si et seulement si v_1 et v_2 sont colinéaires.

Démonstration. Pour tout $t \in \mathbf{R}$, on a $0 \leqslant q(tv_1 + v_2) = t^2 q(v_1) + 2t\varphi(v_1, v_2) + q(v_2)$. Si $q(v_1) = 0$, cela implique que $\varphi(v_1, v_2) = 0$ et donc l'inégalité. Si $q(v_1) \neq 0$, cela implique que le discriminant du trinôme du second degré $q(v_1)T^2 + 2\varphi(v_1, v_2)T + q(v_2)$ est négatif : on a $\varphi(v_1, v_2)^2 - q(v_1)q(v_2) \leqslant 0$.
Si q est définie positive et $\varphi(v_1, v_2)^2 = q(v_1)q(v_2)$, on a $q(tv_1 + v_2) = 0$ soit encore $tv_1 + v_2 = 0$ où $t = -2\frac{\varphi(v_1,v_2)}{q(v_1)} \in \mathbf{R}$ est l'unique racine du trinôme introduit plus haut. □

Corollaire 3.4.10. Supposons q positive. Alors q est définie positive si et seulement si q est non dégénérée.

Démonstration. Si q est définie positive, pour tout $v \in V\backslash\{0\}$, on a $q(v) > 0$ donc $v \notin V^\perp$ d'où $V^\perp = \{0\}$. Réciproquement, si q n'est pas définie positive, il existe $v \in V\backslash\{0\}$ tel que $q(v) = 0$. L'inégalité de Cauchy-Schwarz implique alors que $\varphi(v, w) = 0$ pour tout $w \in V$, et donc que q est dégénérée. □

Corollaire 3.4.11. Si q est positive et $v_1, v_2 \in V$, on a
$$\sqrt{q(v_1+v_2)} \leqslant \sqrt{q(v_1)} + \sqrt{q(v_2)}$$
avec égalité si $v_2 = 0$ ou $(\exists \lambda \in \mathbf{R}_{\geqslant 0})\ \ v_1 = \lambda v_2$, et seulement dans ce cas lorsque q est définie positive.

Démonstration. D'après l'inégalité de Cauchy-Schwarz, on a $\varphi(v_1, v_2) \leqslant \sqrt{q(v_1)q(v_2)}$. Comme $q(v_1+v_2) = q(v_1) + q(v_2) + 2\varphi(v_1, v_2)$, on a bien
$$q(v_1+v_2) \leqslant q(v_1) + q(v_2) + 2\sqrt{q(v_1)q(v_2)} = \big(\sqrt{q(v_1)} + \sqrt{q(v_2)}\big)^2$$
Supposons $\sqrt{q(v_1+v_2)} = \sqrt{q(v_1)} + \sqrt{q(v_2)}$. D'après ce qui précède, cela équivaut à $\varphi(v_1, v_2) = \sqrt{q(v_1)q(v_2)}$. Si q est définie positive, cela implique que v_1 et v_2 sont colinéaires. Si $v_2 \neq 0$, on peut écrire $v_1 = \lambda v_2$ avec $\lambda \in \mathbf{R}$. On a alors $\sqrt{q((1+\lambda)v_2)} = \sqrt{q(\lambda v_2)} + \sqrt{q(v_2)}$, *i.e.* $|1+\lambda|\sqrt{q(v_2)} = (1+|\lambda|)\sqrt{q(v_2)}$, et donc $|1+\lambda| = 1+|\lambda|$ vu que $q(v_2) \neq 0$. On a donc $(1+\lambda)^2 = (1+|\lambda|)^2$, *i.e.* $2\lambda = 2|\lambda|$ soit $\lambda \geqslant 0$. □

Remarque 3.4.12. Lorsque q est définie positive, l'application $\sqrt{q}\colon V \to \mathbf{R}_{\geqslant 0}$ est donc une **norme**.

Définition 3.4.13. La **signature** de q est le couple (s,t) où s (resp. t) est la plus grande des dimensions des sous-espaces V de E tels que la restriction $q_{|V}$ de q à V soit définie positive (resp. définie négative).

Théorème 3.4.14. (Inertie de Sylvester). Si q a signature (s,t) et $\mathfrak{B} = (e_1, \dots, e_n)$ est une base orthogonale de V pour q, alors s (resp. t) est le nombre d'indices $i \in \{1, \dots, n\}$ tels que $q(e_i) > 0$ (resp. $q(e_i) < 0$). En particulier, le rang de q est $s+t$, et la signature de q est un invariant d'isomorphisme.

Démonstration. Dans la base $\mathfrak{B}$, la matrice A de q est de la forme
$$A = \begin{pmatrix} q(e_1) & & \\ & \ddots & \\ & & q(e_n) \end{pmatrix}$$
Quitte à permuter les vecteurs de $\mathfrak{B}$, on peut supposer que $q(e_i) > 0$ pour $i \in \{1, \dots, s_0\}$, $q(e_i) < 0$ pour $i \in \{s_0+1, \dots, s_0+t_0\}$ et $q(e_i) = 0$ pour $i > s_0 + t_0$. Par définition de la signature, on a $s_0 \leqslant s$ et $t_0 \leqslant t$. Soient $W \subseteq E$ un sous-espace de dimension s tel que $q_{|W}$ soit définie positive, et $W' = \mathsf{Vect}(e_{s_0+1}, \dots, e_n)$. Si $v \in W \cap W'$, on a $q(v) \leqslant 0$ (car $v \in W'$). Comme $v \in W$, on a $q(v) \geqslant 0$, et donc $q(v) = 0$, d'où $v = 0$ vu que $q_{|W}$ est définie positive. Ainsi, on a $W \cap W' = \{0\}$, de sorte que $\dim_{\mathbf{R}}(W) + \dim_{\mathbf{R}}(W') \leqslant \dim_{\mathbf{R}}(V) = n$. Comme $\dim_{\mathbf{R}}(W') = n - s_0$, on a donc $s \leqslant s_0$, et donc $s = s_0$. On montre de même que $t = t_0$. □

Corollaire 3.4.15. Si q a pour signature (s,t), il existe un base de V dans laquelle la matrice de q est
$$\mathsf{diag}(\underbrace{1, \dots, 1}_{s \text{ fois}}, \underbrace{-1, \dots, -1}_{t \text{ fois}}, 0, \dots, 0)$$
En particulier, deux espaces quadratiques sont isomorphes si et seulement si ils ont même dimension et même signature.

Démonstration. Si $(e_1, \dots, e_n)$ est une base orthonormée, on peut supposer, quitte à permuter les vecteurs de base, que $q(e_i) > 0$ pour $i \in \{1, \dots, s\}$, $q(e_i) < 0$ pour $i \in \{s+1, \dots, s+t\}$ et $q(e_i) = 0$ pour $i \in \{s+t+1, \dots, n\}$. La famille $\big(\frac{e_1}{\sqrt{q(e_1)}}, \dots, \frac{e_s}{\sqrt{q(e_s)}}, \frac{e_{s+1}}{\sqrt{-q(e_{s+1})}}, \dots, \frac{e_{s+t}}{\sqrt{-q(e_{s+t})}}, e_{s+t+1}, \dots, e_n\big)$ est une base de V, dans laquelle la matrice de q est $\mathsf{diag}(\underbrace{1, \dots, 1}_{s \text{ fois}}, \underbrace{-1, \dots, -1}_{t \text{ fois}}, 0, \dots, 0)$. Le module quadratique (V, q) est donc isomorphe à $s\langle 1\rangle + t\langle -1\rangle + (n-s-t)\langle 0\rangle$. □

Corollaire 3.4.16. En dimension n, il y a $n+1$ classes d'isomorphisme de formes quadratiques non dégénérées sur $\mathbf{R}$.

Notation. On note $\mathsf{O}(s,t)$ (resp. $\mathsf{O}(n)$, ou parfois $\mathsf{O}_n(\mathbf{R})$) le groupe orthogonal de $(\mathbf{R}^{s+t}, s\langle 1\rangle + t\langle -1\rangle)$ (resp. $(\mathbf{R}^n, n\langle 1\rangle)$). On définit de même leurs sous-groupes $\mathsf{SO}(s,t)$ et $\mathsf{SO}(n)$.

3.4.17. *Cas d'un corps fini.* Dans ce numéro, on suppose que K est fini. Rappelons que $q := \#K = p^d$ où $p = \mathsf{car}(K)$ et $d = \dim_{\mathbf{F}_p}(K)$. En outre, nous avons supposé $\mathsf{car}(K) \neq 2$, de sorte que q est impair. On pose $c\colon K^\times \to K^\times; x \mapsto x^2$ et $\ell\colon K^\times \to K^\times; x \mapsto x^{\frac{q-1}{2}}$. Ce sont des morphismes de groupes.

Proposition 3.4.18. On a $\mathsf{Im}(\ell) = \mathsf{Ker}(c) = \{\pm 1\}$ et $\mathsf{Ker}(\ell) = \mathsf{Im}(c)$. En particulier, le sous-groupe des carrés de $K^\times$ est d'ordre $\frac{q-1}{2}$, *i.e.* $\#\big(K^\times/K^{\times 2}\big) = 2$. En outre, il y a $\frac{q+1}{2}$ carrés dans K.

Démonstration. $\mathsf{Ker}(c)$ est l'ensemble des racines du polynôme $X^2-1=(X-1)(X+1)$: comme $p\neq 2$, on a $\mathsf{Ker}(c)=\{\pm 1\}$ de cardinal 2. Cela implique que $\#\,\mathsf{Im}(c)=\frac{q-1}{2}$. On a $\ell\circ c=1$, de sorte que $\mathsf{Im}(c)\subset \mathsf{Ker}(\ell)$. Comme $\mathsf{Ker}(\ell)$, ensemble des racines du polynôme $X^{\frac{q-1}{2}}-1$, a au plus $\frac{q-1}{2}$ éléments, on a l'égalité $\mathsf{Im}(c)=\mathsf{Ker}(\ell)$, donc $\#\,\mathsf{Im}(\ell)=2$, et donc $\mathsf{Im}(\ell)=\{\pm 1\}=\mathsf{Ker}(c)$. □

Corollaire 3.4.19. Si q est de rang $\geqslant 2$, alors $q\colon V\to K$ est surjective, en particulier il existe $v\in V$ tel que $q(v)=1$.

Démonstration. Le module quadratique (V,q) est isomorphe à $\langle a_1,\dots,a_r,0,\dots,0\rangle$ avec $a_1\cdots a_r\neq 0$: il suffit de montrer que la forme quadratique $\langle a_1,a_2\rangle$ sur K^2 est surjective. Soit $y\in K$. Les ensembles $\{a_1x_1^2\,|\,x_1\in K\}\subset K$ et $\{y-a_2x_2^2\,|\,x_2\in K\}\subset K$ sont de cardinal $\frac{q+1}{2}$: leur intersection n'est pas vide. Il existe donc $x_1,x_2\in K$ tels que $a_1x_1^2=y-a_2x_2^2$, *i.e.* $y=a_1x_1^2+x_2^2$, ce qui achève la preuve. □

Théorème 3.4.20. Il existe une base de V dans laquelle la matrice de q est $\mathsf{diag}(\underbrace{1,\dots,1}_{r-1\text{ fois}},a,0,\dots,0)$. En particulier, deux formes quadratiques non dégénérées sur K sont isomorphes si et seulement si elles ont même rang et même discriminant.

Démonstration. Soit r le rang de q. On peut supposer $r=n$ *i.e.* q non dégénérée. On procède par récurrence sur r. Si $r=1$, alors $q=\langle a\rangle$, et on a fini. Supposons $r>1$. D'après le corollaire 3.4.19, il existe $e_1\in V$ tel que $q(e_1)=1$. Par hypothèse de récurrence, il existe une base $(e_2,\dots,e_r)$ de $e_1^\perp$ dans laquelle la matrice de $q_{|e_1^\perp}$ est $\mathsf{diag}(1,\dots,1,a)$. La matrice de q dans la base $(e_1,\dots,e_r)$ est donc $\mathsf{diag}(1,\dots,1,a)$, et on a bien sûr $\mathsf{disc}(q)=aK^{\times 2}$ dans ce cas.
Deux modules quadratiques isomorphes ont toujours même même rang et même discriminant. Réciproquement, deux modules quadratiques non dégénérés de rang r et discriminant $aK^{\times 2}$ sont isomorphes à $\langle\underbrace{1,\dots,1}_{r-1\text{ fois}},a\rangle$ d'après ce qui précède : ils sont isomorphes. □

Corollaire 3.4.21. En dimension n, il y a deux classes d'isomorphisme de formes quadratiques non dégénérées sur K.

Exemple 3.4.22. Cas où $\dim_K(V)=2$. Soit $a\in K^\times$. Alors $\langle 1,a\rangle$ est un plan hyperbolique si $-a$ est un carré dans K, et anisotrope sinon. Par exemple, la norme $\mathsf{N}\colon \mathbf{F}_{q^2}\to\mathbf{F}_q; x\mapsto x^{q+1}$ fournit une forme quadratique anisotrope sur $\mathbf{F}_{q^2}$ (vu comme espace vectoriel de dimension 2 sur $\mathbf{F}_q$). En effet, soit $\alpha\in\mathbf{F}_{q^2}$ tel que $\mathbf{F}_{q^2}=\mathbf{F}_q(\alpha)$: le polynôme minimal de α sur $\mathbf{F}_q$ est de la forme $P(X)=X^2-aX+b\in\mathbf{F}_q[X]$. On a $P(X)=(X-\alpha)(X-\alpha^q)$ *i.e.* $a=\alpha+\alpha^q$ et $b=\alpha^{q+1}=\mathsf{N}(\alpha)$. Une base de $\mathbf{F}_{q^2}$ sur $\mathbf{F}_q$ est donnée par $(1,\alpha)$. Si $x=u+\alpha v\in\mathbf{F}_{q^2}$ (avec $u,v\in\mathbf{F}_q$), on a $\mathsf{N}(x)=(u+\alpha v)(u+\alpha^q v)$ et donc $\mathsf{N}(x)=u^2+auv+bv^2$, ce qui montre que N est une forme quadratique sur $\mathbf{F}_{q^2}$. Elle est anisotrope car $\mathsf{N}(x)=0\Rightarrow x^{q+1}=0\Rightarrow x=0$.

3.4.23. *Une remarque sur le cas du corps* $\mathbf{Q}$. Comme on l'a vu, la classification des modules quadratiques sur un corps K dépend de ses carrés, *i.e.* de son arithmétique. Le cas du corps des rationnels (et plus généralement des corps de nombres) est donc nettement plus subtil que les cas qui précèdent. On se contentera de la remarque suivante.

Proposition 3.4.24. Si $0<r\leqslant n$ sont des entiers, il y a une infinité de classes d'isomorphisme de modules quadratiques de dimension n et de rang r.

Démonstration. Il suffit de le voir pour $r=n=1$. La décomposition en produit de facteurs premiers fournit un isomorphisme de groupes $\mathbf{Z}^{(\mathbb{P})}\xrightarrow{\sim}\mathbf{Q}^\times$ (où $\mathbb{P}$ désigne l'ensemble des nombres premiers). Il induit un isomorphisme $\mathbf{F}_2^{(\mathbb{P})}\xrightarrow{\sim}\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$: l'ensembles des valeurs possibles pour le discriminant est infini. Par exemple, si p et q sont deux nombres premiers distincts, les formes quadratiques $\langle p\rangle$ et $\langle q\rangle$ ne sont pas isomorphes (cela équivaudrait au fait que $\frac{p}{q}$ est un carré dans $\mathbf{Q}^\times$, ce qui n'est pas). □

3.5. **Algèbres de quaternions et formes quadratiques.** Dans tout ce qui suit, K est un corps de caractéristique différente de 2.

Définition 3.5.1. Soient $a,b\in K^\times$. L'**algèbre de quaternions (généralisée)** $(a,b)_K$ est le K espace vectoriel de base $(1,i,j,k)$ muni de la multiplication déterminée par les conditions suivantes :
(1) la multiplication est bilinéaire et associative ;
(2) 1 est neutre pour la multiplication ;
(3) $i^2=a1$, $j^2=b1$, $ij=-ji=k$.

Dans ce qui suit, si $x \in K$, on écrira x au lieu de $x1$ dans $(a,b)_K$.

Remarque 3.5.2. On a $k^2 = ijij = -i^2j^2 = -ab$, $ik = i^2j = aj$, $ki = -ji^2 = -aj$, $jk = -j^2i = -bi$ et $kj = ij^2 = bi$, donc la table de multiplication :

	1	i	j	k
1	1	i	j	k
i	i	a	k	aj
j	j	$-k$	b	$-bi$
k	k	$-aj$	bi	$-ab$

Lemme 3.5.3. (1) On a $(1,b)_K \simeq \mathsf{M}_2(K)$:
(2) Si $\lambda \neq 0$, on a $(a,b)_K \simeq (\lambda^2 a, b)_K \simeq (b,a)_K \simeq (a,-ab)_K$.

Démonstration. (1) Un isomorphisme est donné par $(i,j) \mapsto \left(\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & 1\\ b & 0\end{smallmatrix}\right)\right)$.
(2) L'isomorphisme $(a,b)_K \simeq (\lambda^2 a, b)_K$ est donné par $(i,j) \mapsto (\lambda^{-1}i, j)$, $(a,b)_K \simeq (b,a)_K$ par $(i,j) \mapsto (j,i)$ et $(a,b)_K \simeq (a,-ab)_K$ par $(i,j) \mapsto (i,k)$. □

Exemple 3.5.4. (1) Lorsque K est algébriquement clos, tout élément est un carré : on a $(a,b)_K \simeq \mathsf{M}_2(K)$ pour tout $a, b \in K^\times$.
(2) Lorsque $K = \mathbf{R}$ et $a = b = -1$, on retrouve le corps de quaternions de Hammilton.

Définition 3.5.5. Soit A une K-algèbre.
(1) On dit que A est simple si ses seuls idéaux bilatères sont $\{0\}$ et A.
(2) On dit que A est centrale si son centre est $K1_A$.

Proposition 3.5.6. Soit A une K-algèbre de dimension 4. Les propriétés suivantes sont équivalentes :
(i) A est une algèbre de quaternions ;
(ii) $A \otimes_K \overline{K} \simeq \mathsf{M}_2(\overline{K})$;
(iii) A est centrale simple sur K.
Lorsqu'elles sont remplies, A est corps (non commutatif) ou isomorphe à $\mathsf{M}_2(K)$.

Démonstration. Supposons (i) : il existe $a, b \in K^\times$ tels que $A \simeq (a,b)_K$. On a donc $A \otimes_K \overline{K} \simeq (a,b)_{\overline{K}}$. Dans $\overline{K}$, tout élément est un carré, ce qui implique $(a,b)_{\overline{K}} \simeq \mathsf{M}_2(\overline{K})$ (*cf* lemme 3.5.3), et donc (ii).
Supposons (ii). Si $x \in \mathsf{Z}(A)$, alors $x \otimes 1 \in \mathsf{Z}(A \otimes_K \overline{K}) \simeq \mathsf{Z}(\mathsf{M}_2(\overline{K})) = \overline{K}\,\mathrm{I}_2$, et donc $x \otimes 1 \in (K1_A) \otimes_K \overline{K}$, ce qui implique $x \in K$. Si $I \subset A$ est un idéal bilatère, alors $I \otimes_K \overline{K}$ est un idéal bilatère de $A \otimes_K \overline{K} \simeq \mathsf{M}_2(\overline{K})$: comme $\mathsf{M}_2(\overline{K})$ est simple, on a $I \otimes_K \overline{K} = \{0\}$ ou $I \otimes_K \overline{K} = A \otimes_K \overline{K}$, *i.e.* $I = \{0\}$ ou $I = A$ (on peut le voir en utilisant $\dim_K(I)$). Cela montre (iii).
Supposons (iii). Premier cas : supposons qu'il existe $x \in A \backslash \{0\}$ tel que $Ax \neq A$: l'ensemble des idéaux à gauche propres (*i.e.* distincts de $\{0\}$ et de A) est non vide. Soit I un idéal à gauche de dimension minimale. L'action de A sur I par translation à gauche fournit un morphisme K-linéaire $f\colon A \to \mathsf{End}_K(I)$. Comme A est simple et $\mathsf{Ker}(f)$ est un idéal bilatère, on a $\mathsf{Ker}(f) = \{0\}$ (on a $\mathsf{Ker}(f) \neq A$ parce que $f(1) = \mathrm{Id}_I$), de sorte que f est injective. Comme $\dim_K(A) = 4$, cela implique $\dim_K(I) \in \{2,3\}$. Supposons $\dim_K(I) = 3$: l'idéal I est unique (sinon on pourrait construire un idéal à gauche plus petit en considérant l'intersection de deux tels idéaux). Cela implique que I est aussi stable par multiplication à droite : c'est un idéal bilatère, contredisant la simplicité de A. On a donc nécessairement $\dim_K(I) = 2$, et donc $A \simeq \mathsf{M}_2(K) \simeq (1,1)_K$ est une algèbre de quaternions.
Deuxième cas : A est un corps (non commutatif). Si $x \in A \backslash K$, l'anneau $K(x)$ est un sous-corps commutatif de A : on a nécessairement $[K(x) : K] = 2$, et $K(x)$ est son propre centralisateur dans A. Comme $\mathsf{car}(K) \neq 2$, il existe $i \in K(x) \backslash K$ tel que $i^2 = a \in K^\times \backslash (K^\times)^2$. La conjugaison $c_i\colon A \to A$, $y \mapsto iyi^{-1}$ par i sur A est donc une involution. Comme $K(x)$ est son propre centralisateur dans A, on a $\mathsf{Ker}(c_i - \mathrm{Id}_A) = K(i)$, de sorte que $\dim_K(\mathsf{Ker}(c_i + \mathrm{Id}_A)) = 2$: soit $j \in A$ tel que $c_i(j) = -j$. On a alors $ij = -ji$, donc aussi $ij^2 = j^2 i$, *i.e.* $j^2 \in K(i)$: il existe $b, c \in K$ tels que $j^2 = b + ci$. Si on avait $c \neq 0$, alors $i \in K(j)$, donc $K(i) \subsetneq K(j)$ d'où $K(j) = A$, contredisant la non commutativité de A : on a nécessairement $j^2 = b \in K^\times$, et donc $A \simeq (a,b)_K$.
Les deux cas qui précèdent montrent la dichotomie $A \simeq \mathsf{M}_2(K)$ et A est un corps non commutatif. □

Définition 3.5.7. Une algèbre de quaternions isomorphe à $\mathsf{M}_2(K)$ est dite **déployée**, et **non déployée** dans le cas contraire.

Définition 3.5.8. Dans l'algèbre $(a,b)_K$, le **conjugué** de $x = \alpha + \beta i + \gamma j + \delta k$ est $x^* = \alpha - \beta i - \gamma j - \delta k$. Sa **trace** est $\mathsf{T}(x) = x + x^* = 2\alpha \in K$, et sa **norme** est $\mathsf{N}(x) = xx^* = x^*x = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2$. Le sous-espace des **quaternions purs** est $\mathsf{Ker}(T) = Ki \oplus Kj \oplus Kk$.

Remarque 3.5.9. Si $A \simeq (a,b)_K$ est une algèbre de quaternions, on a $(a,b)_K \otimes_K \overline{K} \simeq \mathsf{M}_2(\overline{K})$, et $\mathsf{T}\otimes\overline{K}$ et $\mathsf{N}\otimes\overline{K}$ sont la trace et le déterminant sur $\mathsf{M}_2(\overline{K})$. Comme les automorphismes de $\mathsf{M}_2(\overline{K})$ sont donnés par la conjugaison par un élément de $\mathsf{GL}_2(\overline{K})$, les applications T et N ne dépendent que de la K-algèbre $A = (a,b)_K$ et pas de a et b. Notons que si $x \in A$, on a l'identité de Cayley-Hammilton $x^2 - \mathsf{T}(x)x + \mathsf{N}(x) = 0$ (qui n'est autre que $(x-x)(x-x^*)=0$).

Soit $A \simeq (a,b)_K$ une algèbre de quaternions. La norme d'une algèbre de quaternions est une forme quadratique non dégénérée : plus précisément, on a $(A,\mathsf{N}) \simeq \langle 1,-a,-b,ab\rangle$. Notons au passage que la forme quadratique N est multiplicative, *i.e.* que $\mathsf{N}(xy) = \mathsf{N}(x)\,\mathsf{N}(y)$ pour tout $x,y \in A$. De plus, son discriminant vaut $1 \in K^\times/(K^\times)^2$. Si $x,y \in (a,b)_K$, on a $\mathsf{N}(x+y) = (x+y)(x+y)^* = (x+y)(x^*+y^*) = \mathsf{N}(x) + xy^* + yx^* + \mathsf{N}(y) = \mathsf{N}(x) + \mathsf{N}(y) + \mathsf{T}(xy^*)$: la forme polaire de la forme quadratique N est $(x,y) \mapsto \frac{1}{2}\mathsf{T}(xy^*)$. On a la décomposition en somme orthogonale $A = K \oplus A_0$ où $A_0 = \mathsf{Ker}(T)$ est le sous-espace des quaternions purs.

Proposition 3.5.10. L'application $A \mapsto (A_0, \mathsf{N}_{|A_0})$ définit une bijection entre les classes d'isomorphisme d'algèbres de quaternions sur K et les classes d'isomorphisme d'espaces quadratiques non dégénérés de dimension 3 et de discriminant 1. Dans cette bijection, les corps correspondent aux espaces quadratiques anisotropes, et $\mathsf{M}_2(K)$ à l'unique forme isotrope $\langle -1,-1,1\rangle$.

Démonstration. D'après ce qui précède, l'application est bien définie. Si (V,q) est un espace quadratique non dégénéré de dimension 3 et de discriminant 1. On a $(V,q) \simeq \langle -a,-b,ab\rangle$ (*cf* théorème 3.1.41), ce qui montre que l'application est surjective. Si A est une algèbre de quaternions telle que $(A_0, \mathsf{N}_{|A_0}) \simeq \langle -a,-b,ab\rangle$, il existe $i,j \in A_0$ orthogonaux tel que $\mathsf{N}(i) = i^* = -i^2 = -a$ et $\mathsf{N}(j) = -j^2 = -b$. Comme i et j sont orthogonaux, on a $0 = \mathsf{T}(ij^*) = -ij - ji$ donc $ji = -ij$. On a donc $A \simeq (a,b)_K$, et l'application est injective.

Si A est un corps et $x \in A_0$, on a $\mathsf{N}(x) = 0 \Rightarrow xx^* = 0 \Rightarrow x = 0$, de sorte que $\mathsf{N}_{|A_0}$ est anisotrope. Si $A \simeq \mathsf{M}_2(K)$, on a $A \simeq (1,1)_K$, donc $(A_0, \mathsf{N}_{|A_0}) \simeq \langle -1,-1,1\rangle$ est isotrope, ce qui prouve la dernière assertion. □

Exemple 3.5.11. Lorsque K est fini et $a,b \in K^\times$, l'espace quadratique $\langle -a,-b,ab\rangle$ a des vecteurs isotropes non nuls (car elle est de rang 3 *cf* corollaire 3.4.19) : on a $(a,b)_K \simeq \mathsf{M}_2(K)$, et à isomorphisme près, il y a une seule algèbre de quaternion sur K (c'est relié au fait que tout corps fini est commutatif).

4. Espaces symplectiques

4.1. **Formes alternées.** Soit K un corps.

Définition 4.1.1. Un **espace symplectique** (sur K) est un couple (V,ψ) où V est un K-espace vectoriel de dimension finie et $\psi\colon V \times V \to K$ une forme **symplectique**, c'est-à-dire bilinéaire, non-dégénérée, et **alternée** *i.e.* telle que

$$(*) \qquad (\forall v \in V)\, \psi(v,v) = 0$$

Remarque 4.1.2.
(1) Si (V,ψ) est un espace symplectique et $v,w \in V$, on a $\psi(w,v) = -\psi(v,w)$ (en développant $\psi(v+w,v+w)=0$), de sorte que ψ est **antisymétrique**. Lorsque $\mathsf{car}(K) \neq 2$, cela équivaut à $(*)$. Lorsque $\mathsf{car}(K) = 2$, ψ est symétrique, mais la symétrie n'implique pas $(*)$.
(2) Dans une base de V, la matrice $A = (a_{i,j})_{1\leqslant i,j\leqslant d}$ d'une forme symplectique est caractérisée par $A \in \mathsf{GL}_d(K)$ et $(\forall i,j \in \{1,\dots,d\})\,(a_{i,j} = -a_{j,i}$ et $a_{i,i} = 0)$. Lorsque $\mathsf{car}(K) \neq 2$, cette dernière condition équivaut à ${}^{\mathrm{t}}A = -A$.

Proposition 4.1.3. Soit (V,ψ) un espace symplectique. Alors $\dim(V) = 2g$ est paire, et il existe une base $\mathbf{e} = (e_1,\dots,e_{2g})$ de V dans laquelle la matrice de ψ est

$$J_{2g} = \begin{pmatrix} 0 & \mathrm{I}_g \\ -\mathrm{I}_g & 0 \end{pmatrix} \in \mathsf{M}_{2g}(\mathbf{Z})$$

(une telle base s'appelle une base de **symplectique**).

Démonstration. Si $V \neq 0$, soit $e_1 \in V\backslash\{0\}$. Comme ψ est non dégénérée, il existe $e_{g+1} \in V$ avec $\psi(e_1,e_{g+1}) = 1$: on a alors $\psi(e_{g+1},e_1) = -1$, de sorte que la matrice de ψ restreinte à $V_1 := \mathsf{Vect}_K(e_1,e_{g+1})$ est $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Un calcul simple montre que $V = V_1 \oplus V_1^\perp$, de sorte que $(V_1^\perp, \psi_{|V_1^\perp})$ est un espace symplectique de dimension $\dim_K(V) - 2$. Une récurrence immédiate sur $\dim_K(V)$ permet de conclure. □

Corollaire 4.1.4. Si $A \in \mathsf{M}_n(K)$ est antisymétrique à coefficients diagonaux nuls, alors $\det(A)$ est un carré dans K.

Démonstration. C'est trivial si $\det(A) = 0$. Si $\det(A) \neq 0$, alors A munit K^n d'une structure symplectique : d'après la proposition 4.1.3, on a $n = 2g$ et il existe une base symplectique. Si P désigne la matrice de changement de base de la base canonique vers une base symplectique, on a ${}^tPAP = J_{2g}$, donc $\det(P)^2 \det(A) = \det(J_{2g}) = 1$, et donc $\det(A) = \left(\frac{1}{\det(P)}\right)^2$. □

Définition 4.1.5. Si W est un sous-K-espace vectoriel de V, on a [a] $\dim_K(W)+\dim_K(W^\perp) = \dim_K(V) = 2g$: la dimension d'un sous-espace isotrope est donc $\leqslant g$. Un **lagrangien** est un sous-espace isotrope W de dimension maximale. D'après la proposition 4.1.3, on a $\dim_K(W) = g$ et donc $W = W^\perp$.

a. Cela résulte de la non dégénérescence de ψ.

4.2. **Groupes symplectiques.**

Définition 4.2.1. Le **groupe symplectique** (resp. **groupe des similitudes symplectiques**) de (V, ψ) est [a]

$$\mathsf{Sp}(\psi) = \{f \in \mathsf{End}_K(V) \,|\, (\forall x, y \in V)\ \psi(f(x), f(y)) = \psi(x, y)\} \subset \mathsf{GL}(V)$$

$$(resp.\ \mathsf{GSp}(\psi) = \{f \in \mathsf{End}_K(V) \,|\, (\exists \nu(f) \in K^\times)\ (\forall x, y \in V)\ \psi(f(x), f(y)) = \nu(f).\psi(x, y)\} \subset \mathsf{GL}(V))$$

Soit R un anneau. Le **groupe symplectique** est

$$\mathsf{Sp}_{2g}(R) = \left\{M \in \mathsf{M}_{2g}(R) \,|\, {}^tMJ_{2g}M = J_{2g}\right\} \subset \mathsf{GL}_{2g}(R)$$

On définit de même le groupe $\mathsf{GSp}_{2g}(R)$.

a. L'inclusion dans $\mathsf{GL}(V)$ résulte de ce que ψ est non dégénérée.

Remarque 4.2.2. Le choix d'une base symplectique fournit un isomorphisme $\mathsf{Sp}(V, \psi) \simeq \mathsf{Sp}_{2g}(K)$ (resp. $\mathsf{Sp}(V, \psi) \simeq \mathsf{GSp}_{2g}(K)$). Le groupe $\mathsf{Sp}(\psi)$ agit simplement transitivement sur l'ensemble des bases symplectiques de (V, ψ).

Exercice 4.2.3. Si $\dim_K(V) = 2$, il n'y a qu'une seule forme alternée ψ à multiplication par un scalaire près : on a $\mathsf{GSp}(\psi) = \mathsf{GL}(V)$ et $\mathsf{Sp}(\psi) = \mathsf{SL}(V)$.

Proposition 4.2.4. Si K est algébriquement clos, la suite

$$1 \to \mathsf{Sp}_{2g}(K) \to \mathsf{GSp}_{2g}(K) \xrightarrow{\nu} K^\times \to 1$$

est exacte.

Démonstration. On a bien sûr la suite exacte $1 \to \mathsf{Sp}_{2g}(K) \to \mathsf{GSp}_{2g}(K) \xrightarrow{\nu} K^\times$. Si $\lambda \in K^\times$ on a $\lambda\,\mathrm{I}_{2g} \in \mathsf{GSp}_{2g}(K)$ et $\nu(\lambda\,\mathrm{I}_{2g}) = \lambda^2$. Comme $K^\times \to K^\times$; $x \mapsto x^2$ est surjectif, cela prouve l'exactitude à droite. □

Si $M \in \mathsf{Sp}_{2g}(K)$, on a $\det(M) \in \{\pm 1\}$. Matriciellement, si $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathsf{M}_{2g}(R)$, on a $M \in \mathsf{Sp}_{2g}(R)$ si et seulement si

$$\begin{cases} {}^tAC = {}^tCA \\ {}^tBD = {}^tDB \\ {}^tAD - {}^tCB = \mathrm{I}_g \end{cases}$$

Cela implique en particulier que $\mathsf{Sp}_2(R) = \mathsf{SL}_2(R)$ (*cf* exercice 4.2.3).
Si $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathsf{Sp}_{2g}(R)$, alors $M^{-1} = \begin{pmatrix} {}^tD & -{}^tC \\ -{}^tB & {}^tA \end{pmatrix}$ et ${}^tM = J_{2g}M^{-1}J_{2g}^{-1}$. Par ailleurs, comme ${}^tJ_{2g} = -J_{2g}$, on a $M \in \mathsf{Sp}_{2g}(R) \Rightarrow {}^tM \in \mathsf{Sp}_{2g}(R)$.

4.2.5. *Un sous-groupe utile du groupe symplectique.* Soit $\mathsf{S}_g(K)$ le K-espace vectoriel des matrices symétriques. Munissons $\mathsf{GL}_g(K)$ de la loi de goupe opposée au produit habituel et $\mathsf{S}_g(K)$ de l'action de $\mathsf{GL}_g(K)$ donnée par $(A, S) \mapsto {}^tASA$. La loi de groupe sur le produit semi-direct $\mathsf{S}_g(K) \rtimes \mathsf{GL}_g(K)$ est donc donnée par

$$(S_1, A_1) \cdot (S_2, A_2) = (S_1 + {}^tA_1S_2A_1, A_2A_1)$$

Proposition 4.2.6. On a un morphisme de groupes injectif

$$\mathsf{S}_g(K) \rtimes \mathsf{GL}_g(K) \to \mathsf{Sp}_{2g}(K);\ (S, A) \mapsto \begin{pmatrix} {}^tA & SA^{-1} \\ 0 & A^{-1} \end{pmatrix}$$

Proposition 4.2.7. Le centre de $\mathsf{Sp}_{2g}(K)$ est $\{\pm\,\mathrm{I}_{2g}\}$, celui de $\mathsf{GSp}_{2g}(K)$ est $K^\times\,\mathrm{I}_{2g}$.

Démonstration. Soit $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathsf{GSp}_{2g}(K)$ appartenant au commutant de $\mathsf{Sp}_{2g}(K)$ (avec $A, B, C, D \in \mathsf{M}_g(K)$). On a $\begin{pmatrix} \mathrm{I}_g & \mathrm{I}_g \\ 0 & \mathrm{I}_g \end{pmatrix} \in \mathsf{Sp}_{2g}(K)$ (*cf* proposition 4.2.6). Comme $\begin{pmatrix} \mathrm{I}_g & \mathrm{I}_g \\ 0 & \mathrm{I}_g \end{pmatrix} M = \left(\begin{smallmatrix} A & B+D \\ C & D \end{smallmatrix}\right)$ et $M \begin{pmatrix} \mathrm{I}_g & \mathrm{I}_g \\ 0 & \mathrm{I}_g \end{pmatrix} = \left(\begin{smallmatrix} A & A+B \\ C & C+D \end{smallmatrix}\right)$, on a $C = 0$ et $A = D$. De même, on a $B = 0$ (car ${}^{\mathrm{t}}M$ commute aux éléments de $\mathsf{Sp}_{2g}(K)$ vu que ce dernier est stable par transposition), d'où $M = \left(\begin{smallmatrix} A & 0 \\ 0 & A \end{smallmatrix}\right)$ avec $A \in \mathsf{GL}_g(K)$. Par ailleurs, si $U \in \mathsf{GL}_g(K)$, on a $\begin{pmatrix} U & 0 \\ 0 & {}^{\mathrm{t}}U^{-1} \end{pmatrix} \in \mathsf{Sp}_{2g}(K)$ (*cf* proposition 4.2.6) : on a $\begin{pmatrix} U & 0 \\ 0 & {}^{\mathrm{t}}U^{-1} \end{pmatrix} M = M \begin{pmatrix} U & 0 \\ 0 & {}^{\mathrm{t}}U^{-1} \end{pmatrix}$, ce qui implique $UA = AU$, *i.e.* $A \in \mathsf{Z}(\mathsf{GL}_g(K)) = K^\times \mathrm{I}_g$, ce qui prouve que $\mathsf{Z}(\mathsf{GSp}_{2g}(K)) = K^\times \mathrm{I}_{2g}$. Si $M \in \mathsf{Z}(\mathsf{Sp}_{2g}(K))$, on a en outre ${}^{\mathrm{t}}AA = A^2 = \mathrm{I}_g$, donc $M \in \{\pm \mathrm{I}_{2g}\}$. □

Remarque 4.2.8. Les groupes $\mathsf{Sp}_{2g}(K)/\{\pm \mathrm{I}_{2g}\}$ sont simples excepté $\mathsf{Sp}_2(\mathbf{F}_2)/\{\pm \mathrm{I}_{2g}\}$, $\mathsf{Sp}_2(\mathbf{F}_3)/\{\pm \mathrm{I}_{2g}\}$ et $\mathsf{Sp}_4(\mathbf{F}_2)/\{\pm \mathrm{I}_{2g}\}$ (*cf* [1, Théorème 5.2]).

4.2.9. *Action sur le demi-espace de Siegel.*

Définition 4.2.10. Le **demi-espace de Siegel** est

$$\mathscr{H}_g := \{Z \in \mathsf{M}_g(\mathbf{C}),\ {}^{\mathrm{t}}Z = Z,\ \mathrm{Im}(Z) \gg 0\}$$

Remarque 4.2.11. Lorsque $g = 1$, ce n'est autre que le **demi-plan de Poincaré** $\mathscr{H} = \{z \in \mathbf{C},\ \mathrm{Im}(z) > 0\}$.

Proposition 4.2.12. Le groupe $\mathsf{Sp}_{2g}(\mathbf{R})$ agit sur le demi-espace de Siegel $\mathscr{H}_g$ par

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \cdot Z = (AZ + B)(CZ + D)^{-1}$$

pour tout $Z \in \mathscr{H}_g$.

Démonstration. Si $Z_1, Z_2 \in \mathsf{M}_g(\mathbf{C})$, on a ${}^{\mathrm{t}}\binom{Z_1}{\mathrm{I}_g} J_{2g} \binom{Z_2}{\mathrm{I}_g} = {}^{\mathrm{t}}Z_1 - Z_2$, de sorte que

$$Z \in \mathscr{H}_g \Leftrightarrow \left({}^{\mathrm{t}}\tbinom{Z}{\mathrm{I}_g} J_{2g} \tbinom{Z}{\mathrm{I}_g} = 0 \text{ et } -\frac{1}{2i} {}^{\mathrm{t}}\tbinom{\overline{Z}}{\mathrm{I}_g} J_{2g} \tbinom{Z}{\mathrm{I}_g} \gg 0 \right)$$

Si $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, on a $M\binom{Z}{\mathrm{I}_g} = \binom{E}{F}$ avec $E = AZ + B$ et $F = CZ + D$. On a donc

$$\begin{cases} {}^{\mathrm{t}}EF - {}^{\mathrm{t}}FE = {}^{\mathrm{t}}\binom{E}{F} J_{2g} \binom{E}{F} = {}^{\mathrm{t}}\binom{Z}{\mathrm{I}_g} {}^{\mathrm{t}}M J_{2g} M \binom{Z}{\mathrm{I}_g} = {}^{\mathrm{t}}\binom{Z}{\mathrm{I}_g} J_{2g} \binom{Z}{\mathrm{I}_g} = 0 \\ E^*F - F^*E = {}^{\mathrm{t}}\binom{\overline{E}}{\overline{F}} J_{2g} \binom{E}{F} = {}^{\mathrm{t}}\binom{\overline{Z}}{\mathrm{I}_g} {}^{\mathrm{t}}M J_{2g} M \binom{Z}{\mathrm{I}_g} = {}^{\mathrm{t}}\binom{\overline{Z}}{\mathrm{I}_g} J_{2g} \binom{Z}{\mathrm{I}_g} \end{cases}$$

i.e. ${}^{\mathrm{t}}EF = {}^{\mathrm{t}}FE$ et $-\frac{1}{2i}(E^*F - F^*E) \gg 0$. Soit $v \in \mathbf{C}^n$ tel que $Fv = 0$: on a $v^*F^* = 0$, et donc $v^*(E^*F - F^*E)v = 0$ et donc $v = 0$ vu que $-\frac{1}{2i}(E^*F - F^*E) \gg 0$. Il en résulte que F est inversible, et que $M \cdot Z = EF^{-1}$ a bien un sens. L'égalité ${}^{\mathrm{t}}EF = {}^{\mathrm{t}}FE$ s'écrit ${}^{\mathrm{t}}F^{-1}{}^{\mathrm{t}}E = EF^{-1}$: la matrice $M \cdot Z$ est symétrique. Enfin, $-\frac{1}{2i}(E^*F - F^*E) = -\frac{1}{2i}F^*(F^{-1*}E^* - EF^{-1})F$ est définie positive, *i.e.* $M \cdot Z \in \mathscr{H}_g$: on a bien une action de $\mathsf{Sp}_{2g}(\mathbf{R})$ sur $\mathscr{H}_g$. □

Remarque 4.2.13. Lorsque $g = 1$, on retrouve l'action par homographies de $\mathsf{SL}_2(\mathbf{R})$ sur le demi-plan de Poincaré.

Proposition 4.2.14. L'action est transitive, et le stabilisateur de $i\,\mathrm{I}_g$ est

$$\mathsf{Sp}_{2g}(\mathbf{R}) \cap \mathsf{O}_{2g}(\mathbf{R}) = \left\{ \left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right) \in \mathsf{M}_{2g}(\mathbf{R}) \,\middle|\, {}^{\mathrm{t}}AA + {}^{\mathrm{t}}BB = \mathrm{I}_g \text{ et } {}^{\mathrm{t}}AB = {}^{\mathrm{t}}BA \right\}$$

Ce dernier est isomorphe au groupe unitaire $\mathsf{U}_g(\mathbf{C})$ par l'application $\left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right) \mapsto A + iB$.

Démonstration. Soit $Z \in \mathscr{H}_g$: il existe $A \in \mathsf{GL}_g(\mathbf{R})$ et $S \in \mathsf{M}_g(\mathbf{R})$ symétrique tels que $Z = S + i{}^{\mathrm{t}}AA$. On a alors $\begin{pmatrix} {}^{\mathrm{t}}A & SA^{-1} \\ 0 & A^{-1} \end{pmatrix} \cdot i\,\mathrm{I}_g = Z$, ce qui implique que l'action de $\mathsf{Sp}_{2g}(\mathbf{R})$ sur $\mathscr{H}_g$ est transitive [5].
Soit $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathsf{Sp}_{2g}(\mathbf{R})$. On a $M \cdot i\,\mathrm{I}_g = i\,\mathrm{I}_g$ si et seulement si $(iA + B)(iC + D)^{-1} = i\,\mathrm{I}_g \Leftrightarrow B + iA = -C + iD$ *i.e.* $C = -B$ et $A = D$, soit $M = \left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right)$ avec ${}^{\mathrm{t}}AA + {}^{\mathrm{t}}BB = \mathrm{I}_g$ et ${}^{\mathrm{t}}AB$ symétrique. Cela équivaut à $A + iB \in \mathsf{U}_g(\mathbf{C})$. Par ailleurs, cela implique que $M \in \mathsf{O}_{2g}(\mathbf{R})$. Réciproquement, soit $M = \left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right) \in \mathsf{Sp}_{2g}(\mathbf{R}) \cap \mathsf{O}_{2g}(\mathbf{R})$: on a $M^{-1} = {}^{\mathrm{t}}M$. Comme ${}^{\mathrm{t}}M J_{2g} M = J_{2g}$, on a $M^{-1} J_{2g} M = J_{2g}$ et M commute à J_{2g}, ce qui signifie $A = D$ et $B + C = 0$ et prouve l'égalité $\mathsf{Sp}_{2g}(\mathbf{R}) \cap \mathsf{O}_{2g}(\mathbf{R}) = \left\{ \left(\begin{smallmatrix} A & B \\ -B & A \end{smallmatrix}\right) \in \mathsf{M}_{2g}(\mathbf{R}) \,\middle|\, {}^{\mathrm{t}}AA + {}^{\mathrm{t}}BB = \mathrm{I}_g \text{ et } {}^{\mathrm{t}}AB = {}^{\mathrm{t}}BA \right\}$. □

Corollaire 4.2.15. Le groupe $\mathsf{Sp}_{2g}(\mathbf{R})$ est connexe, et inclus dans $\mathsf{SL}_{2g}(\mathbf{R})$.

5. En fait, l'action du sous-groupe parabolique décrit dans la proposition 4.2.6 est transitive.

Démonstration. D'après la proposition 4.2.14, on a un homéomorphisme $\mathsf{Sp}_{2g}(\mathbf{R})/\mathsf{U}_g(\mathbf{C}) \xrightarrow{\sim} \mathscr{H}_g$. La connexité de $\mathsf{Sp}_{2g}(\mathbf{R})$ résulte donc de celle de $\mathsf{U}_g(\mathbf{C})$ et de celle de $\mathscr{H}_g$ (qui est même convexe). Comme le déterminant est à valeurs dans $\{\pm 1\}$ sur $\mathsf{Sp}_{2g}(\mathbf{R})$, il est donc constant égal à 1. □

Remarque 4.2.16. En fait, on a un homéomorphisme $\mathsf{Sp}_{2g}(\mathbf{R}) \simeq \mathsf{U}_g(\mathbf{C}) \times \mathbf{R}^{g(g+1)}$, ce qui implique $\pi_1(\mathsf{Sp}_{2g}(\mathbf{R})) \simeq \pi_1(\mathsf{U}_g(\mathbf{C})) \simeq \mathbf{Z}$. En outre, $\mathsf{Sp}_{2g}(\mathbf{R}) \cap \mathsf{O}_{2g}(\mathbf{R})$ est un sous-groupe compact maximal de $\mathsf{Sp}_{2g}(\mathbf{R})$, et ces derniers sont conjugués (*cf* [3, 6.2]).

4.2.17. *Une preuve algébrique de l'inclusion* $\mathsf{Sp}_{2g}(K) \subset \mathsf{SL}_{2g}(K)$. Soient $(X_{i,j})_{1\leqslant i<j\leqslant 2g}$ des indéterminées et $\begin{pmatrix} 0 & X_{i,j} \\ & \ddots \\ -X_{i,k} & 0 \end{pmatrix} \in \mathsf{M}_{2g}\left(\mathbf{Z}[X_{i,j}]_{1\leqslant i<j\leqslant 2g}\right)$ la matrice antisymétrique « générique ». D'après la proposition 4.1.3, elle est congruente à J_{2g} (vue comme matrice à coefficients dans le corps des fractions rationnelles $\mathbf{Q}(X_{i,j})_{1\leqslant i<j\leqslant 2g}$). Son déterminant est donc un carré de $\mathbf{Q}(X_{i,j})_{1\leqslant i<j\leqslant 2g}$. Comme l'anneau de polynômes $\mathbf{Z}[X_{i,j}]_{1\leqslant i<j\leqslant 2g}$ est factoriel, c'est en fait le carré d'un polynôme $\mathrm{Pf}_g \in \mathbf{Z}[X_{i,j}]_{1\leqslant i<j\leqslant 2g}$ (qu'on normalise par $\mathrm{Pf}_g(J_{2g}) = 1$).

Définition 4.2.18. Le polynôme Pf_g s'appelle le pfaffien : si R est un anneau et $A \in \mathsf{M}_{2g}(R)$ une matrice antisymétrique à coefficients diagonaux nuls, on a $\det(A) = \mathrm{Pf}_g(A)^2$.

Proposition 4.2.19. Si $B \in \mathsf{GL}_{2g}(R)$, on a $\mathrm{Pf}_g({}^tBAB) = \det(B)\,\mathrm{Pf}_g(A)$.

Démonstration. On a $\mathrm{Pf}_g({}^tBAB)^2 = \det({}^tBAB) = \det(B)^2\det(A) = \det(B)^2\,\mathrm{Pf}(A)^2$ ce qui implique l'égalité $\mathrm{Pf}_g({}^tBAB) = \pm\det(B)\,\mathrm{Pf}_g(A)$. Le signe est toujours + : cela se vérifie avec les matrices génériques, en évaluant en $A = J_{2g}$ et $B = \mathrm{I}_{2g}$. □

Corollaire 4.2.20. Pour tout corps (et même tout anneau) K, on a $\mathsf{Sp}_{2g}(K) \subset \mathsf{SL}_{2g}(K)$.

Démonstration. Si $M \in \mathsf{Sp}_{2g}(K)$, on a $\det(M) = \det(M)\,\mathrm{Pf}_g(J_{2g}) = \mathrm{Pf}_g({}^tMJ_{2g}M) = \mathrm{Pf}_g(J_{2g}) = 1$. □

5. Prolongements

5.1. Le groupe orthogonal euclidien.

Définition 5.1.1. Si $n \in \mathbf{N}_{>0}$, on pose $\mathsf{PO}_n(\mathbf{R}) = \mathsf{O}_n(\mathbf{R})/\{\pm \mathrm{I}_n\}$ (qu'on appelle *groupe projectif orthogonal*) et $\mathsf{PSO}_n(\mathbf{R}) = \mathsf{SO}_n(\mathbf{R})/\,\mathsf{Z}(\mathsf{SO}_n(\mathbf{R}))$.

Théorème 5.1.2. Le groupe $\mathsf{SO}_3(\mathbf{R})$ est simple.

Démonstration. Soit G un sous-groupe distingué de $\mathsf{SO}_3(\mathbf{R})$ tel que $G \neq \{\mathrm{I}_3\}$. Montrons que $G = \mathsf{SO}_3(\mathbf{R})$. Comme $\mathsf{SO}_3(\mathbf{R})$ est engendré par les renversements (*cf* corollaire 3.3.8), et comme les les renversements sont conjugués (car $\mathsf{SO}_3(\mathbf{R})$ agit transitivement sur les plans), il suffit de montrer que G contient un renversement.
• Notons G_0 la composante connexe de G contenant I_3. C'est un sous-groupe de G (l'application $G_0 \times G_0 \to G$; $(g,h) \mapsto gh^{-1}$ est continue : par connexité de $G_0 \times G_0$, son image est connexe et contient I_3, donc incluse dans G_0). Le sous groupe G_0 est un distingué dans $\mathsf{SO}_3(\mathbf{R})$ (l'argument précédent reste valide en considérant l'application $\mathsf{SO}_3(\mathbf{R}) \times G_0 \to G$; $(g,h) \mapsto g^{-1}hg$.
• Supposons $G_0 = \{\mathrm{I}_3\}$. Soit G' une composante connexe de G. L'application $G' \times G' \to G$; $(g,h) \mapsto gh^{-1}$ est continue, donc d'image connexe incluse dans G et contenant I_3 : elle est constante égale à I_3, de sorte que G' est un singleton. On a $G \neq \{\mathrm{I}_3\}$: soit $g \in G\backslash\{\mathrm{I}_3\}$. L'application $\mathsf{SO}_3(\mathbf{R}) \to G$; $h \mapsto h^{-1}gh$ est constante égale à g car continue et d'image connexe dans G. Pour tout $h \in \mathsf{SO}_3(\mathbf{R})$, on a donc $h^{-1}gh = g$. Si Δ désigne l'axe de la rotation g, alors $h(\Delta) \subset \mathsf{Ker}(g - \mathrm{I}_3) = \Delta$, et donc $h(\Delta) \subset \Delta$. Ceci est absurde, car il n'existe pas de droite de $\mathbf{R}^3$ stabilisée par $\mathsf{SO}_3(\mathbf{R})$.
• Supposons que $G_0 \neq \{\mathrm{I}_3\}$. Si $g \in \mathsf{SO}_3(\mathbf{R})$ est une rotation d'angle θ, il existe une base orthonormale de $\mathbf{R}^3$ dans laquelle sa matrice est $\begin{pmatrix} \cos(\theta) & -\sin(\theta) & 0 \\ \sin(\theta) & \cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$, si bien que $\mathsf{Tr}(g) = 2\cos(\theta) + 1 \in [-1, 3]$. L'application $\varphi\colon \mathsf{SO}_3(\mathbf{R}) \to \mathbf{R}$; $g \mapsto \frac{\mathsf{Tr}(g)-1}{2}$ est continue. Montrons l'existence d'un élément $r \in G_0$ tel que $\varphi(r) = 0$ (car alors $r^2 \in G_0$ est renversement). Soit $g \in G_0\backslash\{\mathrm{I}_3\}$. Quitte à remplacer g par g^{-1}, on peut supposer qu'une mesure θ de l'angle de la rotation g appartient à $]0, \pi]$. Si $\theta \in \left]0, \frac{\pi}{2}\right[$, et si $N = \left\lfloor \frac{\pi}{2\theta} \right\rfloor + 1 \in \mathbf{N}$, la rotation $g^N \in G_0$ est d'angle $N\theta \in \left[\frac{\pi}{2}, \pi\right]$. Dans tous les cas, G_0 contient un élément g tel que $\varphi(g) \leqslant 0$. L'image de G_0 par φ étant connexe dans $\mathbf{R}$, elle contient $[\varphi(g), 1]$ donc 0. □

Théorème 5.1.3. Si $n \geqslant 5$, le groupe $\mathsf{PSO}_n(\mathbf{R})$ est simple.

Démonstration. Le cas $n = 3$ n'est autre que le théorème 5.1.2. Soit $\overline{G}$ un sous-groupe distingué non trivial de $\mathsf{PSO}_n(\mathbf{R})$: il lui correspond un sous-groupe G de $\mathsf{SO}_n(\mathbf{R})$ distingué et contenant strictement $\mathsf{Z}(\mathsf{SO}_n(\mathbf{R}))$. Là encore, il s'agit de montrer que G contient un renversement.

• Soit $W \subset \mathbf{R}^n$ un sous-espace de dimension 3. L'application $\mathsf{SO}(W) \to \mathsf{SO}_n(\mathbf{R})$; $g \mapsto g \oplus \mathrm{Id}_{W^\perp}$ identifie $\mathsf{SO}(W) \simeq \mathsf{SO}_3(\mathbf{R})$ à un sous-groupe de $\mathsf{SO}_n(\mathbf{R})$. Le sous-groupe $\mathsf{SO}(W) \cap G$ de $\mathsf{SO}(W)$ est distingué : comme ce dernier est simple d'après le théorème 5.1.2, on a $\mathsf{SO}(W) \cap G = \{\mathrm{I}_n\}$ ou $\mathsf{SO}(W) \cap G = \mathsf{SO}(W)$. Dans le deuxième cas, le groupe G contient un renversement et donc $G = \mathsf{SO}_n(\mathbf{R})$: il s'agit de montrer qu'il existe un tel W tel que $\mathsf{SO}(W) \cap G \neq \{\mathrm{I}_n\}$.

• Soit $g \in G \backslash \{\pm \mathrm{I}_n\}$. Comme g n'est pas une homothétie, il existe un plan $P \subset \mathbf{R}^n$ tel que $g(P) \neq P$. Soit alors σ le renversement par rapport à $P^\perp$ (de sorte que $\mathsf{Ker}(\sigma + \mathrm{I}_n) = P$). On a $\sigma \in \mathsf{SO}_n(\mathbf{R})$, donc $\sigma g^{-1}\sigma^{-1} \in G$ (parce que G est distingué dans $\mathsf{SO}_n(\mathbf{R})$), donc $\rho = g\sigma g^{-1}\sigma^{-1} \in G$. Par ailleurs, $g\sigma g^{-1}$ est le renversement par rapport à $g(P)^\perp$. Il en résulte que ρ est le produit des deux renversements $\sigma^{-1} = \sigma$ et $g\sigma g^{-1}$, de sorte que ρ laisse fixe $P^\perp \cap g(P)^\perp$, qui est un sous-espace de dimension $\geqslant n - 4 \geqslant 1$: l'élément $\rho \in G$ admet un point fixe $x \in \mathbf{R}^n \backslash \{0\}$ (de sorte que $\rho \neq -\mathrm{I}_n$). Comme $g(P) \neq P$, on a $\rho \neq \mathrm{I}_n$: il existe $y \in \mathbf{R}^n$ tel que $\rho(y)$ et y ne soient pas colinéaires.

• Posons alors $s = \tau_y \tau_x$ (où τ_x et τ_y sont les réflexions d'hyperplans $x^\perp$ et $y^\perp$ respectivement). On a $s \in \mathsf{SO}_n(\mathbf{R})$, donc $s\rho^{-1}s^{-1} \in G$ et $g' = \rho s \rho^{-1} s^{-1} \in G$. On a $\rho s \rho^{-1} = \tau_{\rho(y)}\tau_{\rho(x)}$ donc $g' = \tau_{\rho(y)}\tau_{\rho(x)}\tau_x^{-1}\tau_y^{-1}$. Comme $\rho(x) = x$, $\tau_x^{-1} = \tau_x$ et $\tau_y^{-1} = \tau_y$, on a $g' = \tau_{\rho(y)}\tau_y \neq \mathrm{I}_n$ (car $\rho(y)$ et y ne sont pas colinéaires). On a $\dim_{\mathbf{R}}(\mathsf{Vect}(y, \rho(y)) = 2$: soit $W \subset \mathbf{R}^n$ un sous-espace de dimension 3 contenant $\mathsf{Vect}(y, \rho(y))$. Comme $g'_{|W^\perp} \neq \mathrm{Id}_{W^\perp}$, on a $\mathsf{SO}(W) \cap G \neq \{\mathrm{I}_n\}$, ce qu'on voulait. □

Références

[1] E. Artin – *Algèbre géométrique*, μ_B, Dunod, 1983.

[2] W. Fulton & J. Harris – *Representation theory : a first course*, Graduate Texts in Mathematics, vol. 129, Springer Verlag, 1991.

[3] R. Mneimné & F. Testard – *Introduction à la théorie des groupes de Lie classiques*, Collection Méthodes, Hermann, 1986.

[4] D. Perrin – *Cours d'algèbre*, Ellipses, 1996.

Institut de Mathématiques de Bordeaux, Université Bordeaux, 351, cours de la Libération, 33405 Talence, France

E-mail address: olivier.brinon@math.u-bordeaux.fr