ALGÈBRE 1

6 janvier 2016

ALGÈBRE 1

TABLE DES MATIÈRES

CHAPITRE I

GROUPES

1. Généralités sur les groupes

1.1. Définition. — Un *groupe* est la donnée d'un ensemble G muni d'une loi de composition

$$\begin{array}{ccc} \mathrm{G}\times\mathrm{G} & \to & \mathrm{G} \\ (g_1, g_2) & \mapsto & g_1 g_2 \end{array}$$

et d'un *élément neutre* $e \in \mathrm{G}$ satisfaisant les propriétés suivantes

1° **associativité** : pour tous g_1, g_2, g_3 dans G, on a

$$(g_1 g_2) g_3 = g_1 (g_2 g_3)\ ;$$

2° **élément neutre** (nécessairement unique)

$$\forall g \in \mathrm{G} \qquad ge = eg = g\ ;$$

3° **inverse** : chaque élément g de G admet un inverse (nécessairement unique), c'est-à-dire un élément g^{-1} de G tel que

$$g g^{-1} = g^{-1} g = e.$$

On note aussi souvent 1 l'élément neutre. Pour tout élément g d'un groupe G, et tout $n \in \mathbf{Z}$, on note

$$g^n = \begin{cases} \overbrace{g \cdots g}^{n \text{ fois}} & \text{si } n > 0\ ; \\ e & \text{si } n = 0\ ; \\ \underbrace{g^{-1} \cdots g^{-1}}_{-n \text{ fois}} & \text{si } n < 0. \end{cases}$$

Si $m, n \in \mathbf{Z}$, on a alors la formule habituelle

$$g^{m+n} = g^m g^n.$$

On dit que G est *abélien* (ou commutatif) si, pour tous $g_1, g_2 \in \mathrm{G}$, on a $g_1 g_2 = g_2 g_1$. Dans ce cas, on note généralement la loi de composition additivement $(g_1 + g_2)$, l'élément neutre 0, et l'inverse de g est appelé l'*opposé*, noté $-g$.

On dit que le groupe G est *fini* si c'est un ensemble fini. On appelle alors son cardinal son *ordre,* noté |G|.

Si G et G′ sont des groupes, on peut former un groupe $G \times G'$ appelé *produit direct* en munissant l'ensemble produit de la loi de composition $(g_1, g_1')(g_2, g_2') = (g_1 g_2, g_1' g_2')$.

Exemples 1.1. — 1° La paire $(\mathbf{Z}, +)$ est un groupe abélien.

2° Si **K** est un corps [1] (comme **Q**, **R** ou **C**), $(\mathbf{K}, +)$ et $(\mathbf{K}^\times, \times)$ sont des groupes abéliens ; plus généralement, pour un anneau A, on a le groupe abélien $(A, +)$ et le groupe multiplicatif $(A^\times, \times)$ des unités de A (les éléments de A inversibles dans A).

3° Pour tout entier $n \in \mathbf{N}^*$, la paire $(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe fini d'ordre n. Ces groupes sont dits *cycliques*.

4° Si X est un ensemble, l'ensemble Bij(X) des bijections de X dans X, muni de la composition des applications, est un groupe. En particulier, le groupe symétrique $\mathfrak{S}_n$ des bijections de l'ensemble $\{1, \dots, n\}$ est un groupe fini d'ordre $n!$, non abélien pour $n \geqslant 3$.

5° Si **K** est un corps, les matrices $n \times n$ inversibles à coefficients dans **K** forment le *groupe général linéaire* $\mathrm{GL}_n(\mathbf{K})$. Si E est un **K**-espace vectoriel, les applications linéaires bijectives de E dans E forment un groupe GL(E) ; si E est de dimension finie n, le choix d'une base de E fournit un isomorphisme entre GL(E) et $\mathrm{GL}_n(\mathbf{K})$. Les applications affines bijectives de E dans E (c'est-à-dire les applications du type $x \mapsto u(x) + b$, avec $u \in \mathrm{GL(E)}$ et $b \in \mathrm{E}$) forment aussi un groupe, le *groupe général affine,* noté GA(E).

6° Plus généralement, si A est un anneau commutatif, on peut former le groupe $\mathrm{GL}_n(\mathrm{A})$ des matrices inversibles d'ordre n à coefficients dans A : il s'agit exactement des matrices dont le déterminant est dans $A^\times$ [2]. Par exemple, le groupe $\mathrm{GL}_n(\mathbf{Z})$ est constitué des matrices $n \times n$ à coefficients entiers de déterminant ± 1.

Exercice 1.2. — Soit G un groupe tel que $g^2 = e$ pour tout $g \in \mathrm{G}$. Montrer que G est abélien.

Exercice 1.3. — Montrer que $\mathrm{GL}_n(\mathbf{Q})$ est dense dans $\mathrm{GL}_n(\mathbf{R})$.

1.2. Sous-groupes, générateurs. — Une partie H d'un groupe G est appelée un *sous-groupe* (on note $\mathrm{H} \leq \mathrm{G}$, et $\mathrm{H} < \mathrm{G}$ si de plus $\mathrm{H} \neq \mathrm{G}$) si la loi de composition de G se restreint à H et en fait un groupe, ce qui est équivalent aux propriétés suivantes :

1° $e \in \mathrm{H}$;

2° pour tous $h_1, h_2 \in \mathrm{H}$, on a $h_1 h_2 \in \mathrm{H}$;

3° pour tout $h \in \mathrm{H}$, on a $h^{-1} \in \mathrm{H}$.

Exemples 1.4. — 1° L'intersection d'une famille quelconque de sous-groupes d'un groupe G est un sous-groupe de G.

2° Les sous-groupes de **Z** sont les $n\mathbf{Z}$ pour $n \in \mathbf{N}$.

---

1. Dans ces notes, un corps est toujours commutatif, sauf mention expresse du contraire.

2. Si une matrice M admet un inverse M^{-1} à coefficients dans A, on obtient, en prenant les dérteminants dans la formule $\mathrm{M} \cdot \mathrm{M}^{-1} = \mathrm{I}_n$, la relation $\det(\mathrm{M}) \det(\mathrm{M}^{-1}) = 1$, qui entraîne que $\det(\mathrm{M})$ est inversible dans A. Inversement, si $\det(\mathrm{M})$ est inversible dans A, la formule $\mathrm{M} \cdot {}^t\mathrm{com}(\mathrm{A}) = \det(\mathrm{M})\mathrm{I}_n$ entraîne que M admet un inverse à coefficients dans A.

3° Le groupe $\mathrm{O}_n(\mathbf{R})$ des matrices M de taille $n \times n$ réelles orthogonales (c'est-à-dire qui satisfont ${}^t\mathrm{MM} = \mathrm{I}_n$) est un sous-groupe du groupe $\mathrm{GL}_n(\mathbf{R})$.

4° Soit n un entier $\geqslant 2$. Le *groupe diédral* D_n des transformations orthogonales de $\mathbf{R}^2$ préservant les sommets d'un polygone régulier à n côtés centré à l'origine est un sous-groupe d'ordre $2n$ de $\mathrm{O}_2(\mathbf{R})$: si r est la rotation d'angle $\frac{2\pi}{n}$ et s la symétrie par rapport à une droite passant par l'un des sommets, on a

$$\mathrm{D}_n = \{\mathrm{Id}, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\},$$

avec $rsrs = \mathrm{Id}$. On peut voir aussi D_n comme un sous-groupe du groupe $\mathfrak{S}_n$, puisque ses éléments permutent les n sommets du polygone.

5° Le *centre*

$$\mathrm{Z(G)} = \{h \in \mathrm{G} \mid \forall g \in \mathrm{G} \quad gh = hg\}$$

d'un groupe G est un sous-groupe de G. Le groupe G est abélien si et seulement si $\mathrm{Z(G)} = \mathrm{G}$. Par exemple, le centre de $\mathrm{GL}_n(\mathbf{K})$ est constitué des homothéties.

Exercice 1.5. — Quel est le centre du groupe D_n ?

Exercice 1.6. — Quel est le centre du groupe $\mathfrak{S}_n$?

Proposition 1.7. — *Soit* A *une partie d'un groupe* G. *Il existe un plus petit sous-groupe de* G *contenant* A. *On l'appelle* sous-groupe engendré *par* A *et on le note* $\langle \mathrm{A} \rangle$.

Démonstration. — Il y a deux constructions équivalentes. La première consiste à définir $\langle \mathrm{A} \rangle$ comme l'intersection de tous les sous-groupes de G contenant A (utiliser l'ex. 1.4.1°). La seconde construction consiste en la description explicite :

$$\langle \mathrm{A} \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \mid n \in \mathbf{N},\ x_i \in \mathrm{A},\ \varepsilon_i \in \{1, -1\}\}.$$

□

Une partie A de G est une *partie génératrice* de G, ou engendre G, ou est un ensemble de générateurs de G, si $\langle \mathrm{A} \rangle = \mathrm{G}$. On dit que G est *de type fini* s'il admet une partie génératrice finie. Tout groupe fini est bien sûr de type fini.

Attention : un sous-groupe d'un groupe de type fini n'est pas nécessairement de type fini (*cf.* exerc. 1.11) !

Exemples 1.8. — 1° Soit $n \in \mathbf{N}^*$. Le groupe $\mathbf{Z}/n\mathbf{Z}$ est engendré par la classe de tout entier premier à n.

2° Voici trois ensembles de générateurs pour le groupe symétrique $\mathfrak{S}_n$:
– toutes les transpositions ;
– les transpositions $(12), (23), \dots, ((n-1)\ n)$;
– la transposition (12) et le cycle $(12\cdots n)$.

3° Avec les notations précédentes, le groupe diédral D_n est engendré par la rotation r et la symétrie s.

Exercice 1.9. — Montrer qu'un groupe de type fini est dénombrable.

Exercice 1.10. — Montrer que le groupe $(\mathbf{Q}, +)$ n'est pas de type fini.

Exercice 1.11. — Soit G le sous-groupe (de type fini) de $\mathrm{GL}_2(\mathbf{Q})$ engendré par les matrices $\begin{pmatrix}2 & 0\\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. Montrer que le sous-groupe de G qui consiste en les éléments de G dont les coefficients diagonaux sont tous les deux égaux à 1 n'est pas de type fini [3].

1.3. Morphismes (de groupes). — Un *morphisme de groupes* est la donnée d'une application $f : \mathrm{G} \to \mathrm{G}'$ entre groupes, satisfaisant

$$\forall g_1, g_2 \in \mathrm{G} \qquad f(g_1 g_2) = f(g_1) f(g_2).$$

Si f est bijective, son inverse f^{-1} est aussi un morphisme (de groupes) et on dit que f est un *isomorphisme*. Si en outre $\mathrm{G} = \mathrm{G}'$, on dit que f est un *automorphisme* de G.

Si $f : \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes, le *noyau* et l'*image* de f,

$$\ker(f) = \{g \in \mathrm{G} \mid f(g) = e\} \qquad , \qquad \mathrm{im}(f) = \{f(g) \mid g \in \mathrm{G}\}$$

sont des sous-groupes de G et G′ respectivement. Plus généralement, l'image inverse par f de tout sous-groupe de G′ est un sous-groupe de G, et l'image par f de tout sous-groupe de G est un sous-groupe de G′.

Le morphisme f est injectif si et seulement si $\ker(f) = \{e\}$; il est surjectif si et seulement si $\mathrm{im}(f) = \mathrm{G}'$.

Exemples 1.12. — 1° Soit $n \in \mathbf{N}$. La surjection canonique $\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ est un morphisme surjectif. Son noyau est le sous-groupe $n\mathbf{Z}$ de $\mathbf{Z}$.

2° La signature $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme de groupes, surjectif lorsque $n \geqslant 2$, dont le noyau est le *groupe alterné* $\mathfrak{A}_n$.

Ce groupe est engendré par les 3-cycles (abc), car $(ab)(ac) = (acb)$ et $(ab)(cd) = (acb)(acd)$.

3° L'application exponentielle $\exp : (\mathbf{C}, +) \to (\mathbf{C}^\times, \times)$ est un morphisme surjectif. Son noyau est le sous-groupe $2i\pi\mathbf{Z}$ de $\mathbf{C}$.

4° Soit $\mathbf{K}$ un corps. Le déterminant $\det : \mathrm{GL}_n(\mathbf{K}) \to \mathbf{K}^\times$ est un morphisme surjectif. Son noyau est le *groupe spécial linéaire* des matrices de déterminant 1 ; il est noté $\mathrm{SL}_n(\mathbf{K})$.

5° L'ensemble des automorphismes d'un groupe G, muni de la loi de composition des applications, est un groupe noté Aut(G).

Si $g \in \mathrm{G}$, l'application

$$\begin{array}{rccc} \iota_g : & \mathrm{G} & \longrightarrow & \mathrm{G} \\ & x & \longmapsto & gxg^{-1} \end{array}$$

est un automorphisme de G. Un tel automorphisme de G est appelé *automorphisme intérieur* de G et

$$\iota : \mathrm{G} \longrightarrow \mathrm{Aut}(\mathrm{G})$$

est un morphisme de groupes dont le noyau est le centre Z(G).

3. Un théorème de Higman, Neumann et Neumann dit que les sous-groupes des groupes de type fini sont tous les groupes dénombrables (dont la plupart ne sont pas de type fini !).

1.4. Classes à gauche. — Soit H un sous-groupe d'un groupe G. On définit sur G une relation d'équivalence $\mathscr{R}$ par

$$g_1 \mathscr{R} g_2 \iff \exists h \in \mathrm{H} \quad g_2 = g_1 h.$$

Les trois propriétés caractéristiques des relations d'équivalence (réflexivité, symétrie, transitivité) se vérifient facilement. La classe d'équivalence d'un élément $x \in \mathrm{G}$ est $g\mathrm{H} = \{gh \mid h \in \mathrm{H}\}$. Les parties gH (pour $g \in \mathrm{G}$) sont appelées *classes à gauche* de G, et l'ensemble quotient de G par $\mathscr{R}$, c'est-à-dire l'ensemble des classes à gauche, est noté G/H. Si cet ensemble est fini, son cardinal, noté [G : H], est appelé l'*indice* de H dans G.

On peut définir aussi les *classes à droite* comme les ensembles $\mathrm{H}g = \{hg \mid h \in \mathrm{H}\}$, et l'ensemble des classes à droite est noté H\G. Heureusement, il est à peu près indifférent d'utiliser des classes à droite ou à gauche, car l'application inverse $\phi : \mathrm{G} \to \mathrm{G}$, $g \mapsto g^{-1}$, envoie gH sur $\mathrm{H}g^{-1}$, donc envoie classes à gauche sur classes à droite, induisant ainsi une bijection

$$\mathrm{G/H} \longrightarrow \mathrm{H\backslash G}.$$

Soit $g \in \mathrm{G}$. L'application $\mathrm{H} \to \mathrm{G}$, $h \mapsto gh$, induit une bijection

$$\mathrm{H} \longrightarrow g\mathrm{H}.$$

En particulier, si H est fini, le cardinal d'une classe à gauche gH est égal à l'ordre de H. Les classes à gauche forment donc une partition de G par des classes de même cardinal. On en déduit le résultat suivant.

Théorème de Lagrange 1.13. — *Soit* H *un sous-groupe d'un groupe fini* G. *On a*

$$|\mathrm{G}| = |\mathrm{H}|[\mathrm{G} : \mathrm{H}].$$

En particulier, l'ordre d'un sous-groupe de G *divise l'ordre de* G.

> ***Exercice 1.14.*** — Soit G un groupe de type fini et soit H un sous-groupe d'indice fini de G. Montrer que H est de type fini (*Indication :* si $a_1, \dots, a_m$ engendrent G, et si $g_1\mathrm{H}, \dots, g_n\mathrm{H}$ sont les classes à gauche, avec $g_1 = e$, on pourra montrer que l'ensemble fini $\mathrm{H} \cap \{g_i^{-1} a_k g_j \mid 1 \leqslant k \leqslant m,\ 1 \leqslant i, j \leqslant n\}$ engendre H).

1.5. Sous-groupes distingués. — On dit qu'un sous-groupe H d'un groupe G est un *sous-groupe distingué*, ou *sous-groupe normal*, et on note $\mathrm{H} \trianglelefteq \mathrm{G}$ (et $\mathrm{H} \triangleleft \mathrm{G}$ si de plus $\mathrm{H} \neq \mathrm{G}$), s'il est stable par tout automorphisme intérieur, c'est-à-dire si

$$\forall g \in \mathrm{G} \quad \forall h \in \mathrm{H} \qquad ghg^{-1} \in \mathrm{H}.$$

Pour tout groupe G, les sous-groupes $\{e\}$ et G de G sont distingués. Le groupe G est dit *simple* s'il n'a pas d'autre sous-groupe distingué et si $\mathrm{G} \neq \{e\}$.

Si $f : \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes, $\ker(f) \trianglelefteq \mathrm{G}$ (attention, il est faux en général que l'image soit un sous-groupe distingué) ; plus généralement, si $\mathrm{H}' \trianglelefteq \mathrm{G}'$, on a $f^{-1}(\mathrm{H}') \trianglelefteq \mathrm{G}$.

Il est important de noter que si H est distingué dans G, les classes à droite sont égales aux classes à gauche : pour tout $g \in \mathrm{G}$, on a $g\mathrm{H} = \mathrm{H}g$ puisque $g\mathrm{H}g^{-1} = \mathrm{H}$. Ainsi G/H = H\G. La réciproque est vraie : si H est un sous-groupe de G tel que G/H = H\G, alors H est distingué dans G.

Exemples 1.15. — 1° Dans un groupe abélien, tous les sous-groupes sont distingués.

2° Le groupe alterné $\mathfrak{A}_n$ est distingué dans le groupe symétrique $\mathfrak{S}_n$, car c'est le noyau du morphisme signature. Si $n \geqslant 3$, ce dernier n'est donc pas simple.

3° Si $\mathbf{K}$ est un corps, le sous-groupe $\mathrm{SL}_n(\mathbf{K})$ de $\mathrm{GL}_n(\mathbf{K})$ est distingué, car c'est le noyau du morphisme déterminant.

Exercice 1.16. — Soit G un groupe et soit H un sous-groupe de G d'indice 2. Montrer que H est distingué dans G.

1.6. Quotients. — Soit H un sous-groupe d'un groupe G. On souhaite munir G/H d'une structure de groupe telle que l'application (surjective)

$$\begin{array}{rcl} p : \mathrm{G} & \longrightarrow & \mathrm{G/H} \\ g & \longmapsto & g\mathrm{H} \end{array}$$

qui envoie un élément sur sa classe à gauche soit un morphisme de groupes. L'élément neutre de G/H doit nécessairement être $p(e) = e\mathrm{H}$, donc le noyau de p doit être la classe de e, c'est-à-dire H. Il faut donc que H soit distingué dans G. Montrons que cette condition est suffisante.

Théorème 1.17. — *Si* H *est un sous-groupe distingué de* G*, il existe sur* G/H *une unique structure de groupe telle que la surjection* $p : \mathrm{G} \to \mathrm{G/H}$ *soit un morphisme de groupes.*

Si H est un sous-groupe distingué de G, on a G/H = H\G et on obtient le même groupe quotient en considérant les classes à droite ou à gauche.

Démonstration. — Pour que p soit un morphisme de groupes, il faut que la loi de composition sur G/H vérifie

$$(g_1\mathrm{H})(g_2\mathrm{H}) = g_1 g_2 \mathrm{H}. \tag{1}$$

La première chose à faire est de vérifier que cette formule ne dépend pas des choix de g_1 et g_2 dans leurs classes : si $g_1 = g_1' h_1$ et $g_2 = g_2' h_2$, on a

$$g_1 g_2 = g_1' h_1 g_2' h_2 = g_1' g_2' (g_2'^{-1} h_1 g_2') h_2.$$

Puisque H est distingué dans G, on a $g_2'^{-1} h_1 g_2' \in \mathrm{H}$, donc $g_1 g_2 \mathrm{H} = g_1' g_2' \mathrm{H}$. La formule (1) définit donc bien une loi de composition sur G/H. On vérifie qu'il s'agit d'une loi de groupe. □

Soit H un sous-groupe distingué d'un groupe G et soit $p : \mathrm{G} \to \mathrm{G/H}$ la surjection canonique. On vérifie que les applications

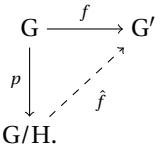
$$\begin{array}{rcl} \{\text{sous-groupes de G/H}\} & \longrightarrow & \{\text{sous-groupes de G contenant H}\} \\ \mathrm{K}' & \longmapsto & p^{-1}(\mathrm{K}') \\ p(\mathrm{K}) & \longleftarrow & \mathrm{K} \end{array}$$

sont des bijections inverses l'une de l'autre. De plus, K′ est distingué dans G/H si et seulement si $p^{-1}(\mathrm{K}')$ est distingué dans G.

Exemple 1.18. — Le groupe $\mathbf{Z}/n\mathbf{Z}$ est le groupe quotient de $\mathbf{Z}$ par $n\mathbf{Z}$. On peut en déduire les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$: leur image réciproque par la surjection $p : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$ contenant $n\mathbf{Z}$, donc de la forme $d\mathbf{Z}$ pour $d|n$, donc les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont exactement les sous-groupes cycliques engendrés par les entiers d tels que $d|n$.

En particulier, le groupe $\mathbf{Z}/n\mathbf{Z}$ est simple si et seulement si n est un nombre premier.

***Théorème 1.19* (Propriété universelle du quotient).** — *Soit* G *un groupe, soit* H *un sous-groupe distingué de* G *et soit* $f : \mathrm{G} \to \mathrm{G}'$ *un morphisme de groupes. Si* $\ker(f) \supseteq \mathrm{H}$*, il existe un unique morphisme* $\hat{f} : \mathrm{G}/\mathrm{H} \to \mathrm{G}'$ *tel que* $f = \hat{f} \circ p$*, c'est-à-dire que le diagramme suivant est commutatif*



En outre, $\ker(\hat{f}) = \ker(f)/\mathrm{H}$ *et* $\mathrm{im}(\hat{f}) = \mathrm{im}(f)$.

Démonstration. — On veut poser $\hat{f}(x\mathrm{H}) = f(x)$. Cela a un sens à condition que $f(xh) = f(x)$ pour tout $h \in \mathrm{H}$, c'est-à-dire $f(h) = e$, ce qui est précisément le cas puisque $\ker(f) \supseteq \mathrm{H}$. L'application $\hat{f} : \mathrm{G}/\mathrm{H} \to \mathrm{G}'$ ainsi définie est manifestement unique. On vérifie que c'est un morphisme, avec le noyau et l'image indiqués. □

Corollaire 1.20. — *Si* $f : \mathrm{G} \to \mathrm{G}'$ *est un morphisme de groupes,* $\hat{f} : \mathrm{G}/\ker(f) \to \mathrm{im}(f)$ *est un isomorphisme.*

Démonstration. — On applique le théorème à $\tilde{f} : \mathrm{G} \to \mathrm{im}(f)$, coïncidant avec f mais dont on a restreint le but, et à $\mathrm{H} = \ker(f)$. On obtient $\hat{f} : \mathrm{G}/\ker(f) \to \mathrm{im}(f)$, avec $\ker \hat{f} = \ker(f)/\ker(f) = \{e\}$ et $\mathrm{im}\, \hat{f} = \mathrm{im}\, \tilde{f} = \mathrm{im}(f)$. □

Corollaire 1.21. — *Le sous-groupe* $\langle g \rangle$ *engendré par un élément* g *d'un groupe* G *est isomorphe à* $\mathbf{Z}$ *s'il est infini, à* $\mathbf{Z}/n\mathbf{Z}$ *s'il est fini, avec* $n \in \mathbf{N}^*$*. On appelle alors* n *l'*ordre *de* g.

En particulier, par le théorème de Lagrange (th. 1.13), l'ordre d'un élément d'un groupe fini G divise l'ordre de G, et un groupe d'ordre un nombre premier p est nécessairement isomorphe au groupe cyclique $\mathbf{Z}/p\mathbf{Z}$.

Démonstration. — Le morphisme

$$\begin{array}{rccc} \phi_g : & \mathbf{Z} & \longrightarrow & \mathrm{G} \\ & n & \longmapsto & g^n \end{array}$$

a pour image $\langle g \rangle$. Soit ϕ_g est injectif, auquel cas il induit un isomorphisme $\mathbf{Z} \xrightarrow{\sim} \langle g \rangle$, soit son noyau est un sous-groupe $n\mathbf{Z}$ de $\mathbf{Z}$, avec $n \in \mathbf{N}^*$ (ex. 1.4.2°), auquel cas ϕ_g induit, par le corollaire précédent, un isomorphisme $\hat{\phi}_g : \mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} \langle g \rangle$. □

Exemples 1.22. — 1° On a un isomorphisme $\mathfrak{S}_n/\mathfrak{A}_n \simeq \mathbf{Z}/2\mathbf{Z}$ provenant du morphisme signature (on peut aussi dire que ce groupe quotient a deux éléments, donc il est nécessairement isomorphe à $\mathbf{Z}/2\mathbf{Z}$).

2° La restriction du déterminant au groupe diédral $D_n < O_2(\mathbf{R})$ induit une surjection $D_n \to \{\pm 1\}$. Son noyau est le sous-groupe de D_n engendré par la rotation r. Il est d'indice 2 et est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

3° Le morphisme $\iota : G \to \mathrm{Aut}(G)$, défini par $\iota(g)(x) = gxg^{-1}$, a pour noyau le centre $Z(G)$ et image le sous-groupe $\mathrm{Int}(G)$ des automorphismes intérieurs de G, donc $\mathrm{Int}(G) \simeq G/Z(G)$.

4° Le groupe $\mathrm{Int}(G)$ des automorphismes intérieurs de G est distingué dans $\mathrm{Aut}(G)$. On appelle le quotient $\mathrm{Out}(G) := G/\mathrm{Int}(G)$ le groupe des automorphismes extérieurs de G.

Proposition 1.23. — *Soit* G *un groupe et soit* H *un sous-groupe distingué de* G.

1° Si G *est de type fini (cf. §1.2),* G/H *est aussi de type fini*[4].

2° Si H *et* G/H *sont de type fini,* G *est de type fini.*

Démonstration. — 1° L'image dans G/H d'une partie génératrice finie de G est une partie génératrice finie de G/H.

2° Soit A une partie finie de G dont l'image dans G/H engendre G/H, et soit B une partie génératrice finie de H. Soit x un élément de G. Sa classe dans G/H s'écrit

$$\overline{x} = \overline{x}_1^{\varepsilon_1}\overline{x}_2^{\varepsilon_2}\cdots\overline{x}_m^{\varepsilon_m} = \overline{x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_m^{\varepsilon_m}},$$

avec $\varepsilon_1\ldots,\varepsilon_m \in \{1,-1\}$ et $x_1,\ldots,x_m \in A$. Cela entraîne

$$x_m^{-\varepsilon_m}\cdots x_2^{-\varepsilon_2}x_1^{-\varepsilon_1}x \in H.$$

et on peut donc écrire

$$x_m^{-\varepsilon_m}\cdots x_2^{-\varepsilon_2}x_1^{-\varepsilon_1}x = y_1^{\varepsilon'_1}y_2^{\varepsilon'_2}\cdots y_n^{\varepsilon'_n},$$

avec $\varepsilon'_1\ldots,\varepsilon'_n \in \{1,-1\}$ et $y_1,\ldots,y_n \in B$. On en déduit

$$x = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_m^{\varepsilon_m}y_1^{\varepsilon'_1}y_2^{\varepsilon'_2}\cdots y_n^{\varepsilon'_n},$$

ce qui prouve que $A \cup B$ engendre G. □

Exercice 1.24. — Soit $\mathbf{F}_q$ un corps fini à q éléments. Montrer

$$\begin{aligned} |\mathrm{GL}_n(\mathbf{F}_q)| &= (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}),\\ |\mathrm{SL}_n(\mathbf{F}_q)| &= (q^n-1)(q^n-q)\cdots(q^n-q^{n-2})q^{n-1}. \end{aligned}$$

Exercice 1.25. — On rappelle que $\mathrm{GL}_n(\mathbf{Z})$ est le groupe des matrices carrées d'ordre n à coefficients entiers, dont le déterminant est ± 1.

a) Montrer que les éléments de $\mathrm{GL}_2(\mathbf{Z})$ qui sont d'ordre fini sont d'ordre 1,2,3,4 ou 6 (*Indication :* on pourra considérer les valeurs propres des matrices d'ordre fini).

b) Déterminer une fonction $f : \mathbf{N} \to \mathbf{N}$ telle que tous les éléments de $\mathrm{GL}_n(\mathbf{Z})$ qui sont d'ordre fini sont d'ordre $\leqslant f(n)$ (Attention, c'est beaucoup plus difficile !).

Exercice 1.26. — Soient K et H des sous-groupes distingués d'un groupe G avec $K \leq H$. Montrer que le sous-groupe H/K de G/K est distingué et que $(G/K)/(H/K) \simeq G/H$.

Exercice 1.27. — Soient H et K des sous-groupes d'un groupe G, avec $H \trianglelefteq G$. Montrer que $HK := \{hk \mid h \in H,\ k \in K\}$ est un sous-groupe de G, que $HK = KH = HKH$, que $H \cap K$ est distingué dans K et que les groupes HK/H et $K/(H \cap K)$ sont isomorphes.

4. On a vu dans l'exerc. 1.11 que H n'est pas nécessairement de type fini.

Exercice 1.28. — Soit **K** un corps et soit E un **K**-espace vectoriel. Montrer que le groupe des translations de E est un sous-groupe distingué du groupe affine GA(E) (*cf.* ex. 1.1.5°) isomorphe au groupe additif (abélien) (E, +) et que le groupe quotient est isomorphe à GL(E).

Exercice 1.29. — Le but de cet exercice est de montrer que tout sous-groupe *fini* G du groupe multiplicatif d'un corps **K** est cyclique. En particulier, le groupe multiplicatif d'un corps fini est cyclique.

La seule propriété qu'on utilisera est que l'équation $x^n = 1_{\mathbf{K}}$ a au plus n solutions dans **K**. Soit g un élément de G d'ordre maximal d et soit h un autre élément de G, d'ordre e.

a) *Supposons que e ne divise pas d*. Il existe alors q, puissance de nombre premier, qui divise e mais pas d. Soit r l'ordre de $gh^{e/q}$. Montrer que q divise $\mathrm{ppcm}(d,r)$, puis que r est divisible par $\mathrm{ppcm}(d,q)$, et aboutir à une contradiction (*Indication :* on pourra calculer $(h^{er/q})^{d/\mathrm{pgcd}(d,r)}$).

b) On a donc $e \mid d$. En déduire que g engendre G.

Exercice 1.30. — Soit $\mathbf{F}_q$ un corps fini à q éléments. Le but de cet exercice est de montrer que l'ordre maximal d'un élément de $\mathrm{GL}_n(\mathbf{F}_q)$ est exactement $q^n - 1$.

a) Soit $M \in \mathrm{GL}_n(\mathbf{F}_q)$. Montrer que l'ensemble $\{P(M) \mid P \in \mathbf{F}_q[X]\}$ contient au plus q^n éléments (*Indication :* on pourra utiliser le théorème de Cayley-Hamilton). En déduire que l'ordre de M dans le groupe que $\mathrm{GL}_n(\mathbf{F}_q)$ est au plus $q^n - 1$. Montrer par un exemple que cet ordre ne divise pas nécessairement $q^n - 1$.

b) Inversement, montrer qu'il existe un élément de $\mathrm{GL}_n(\mathbf{F}_q)$ d'ordre $q^n - 1$ (*Indication :* on admettra qu'il existe un corps $\mathbf{F}_{q^n}$ de cardinal q^n contenant $\mathbf{F}_q$ comme sous-corps (*cf.* th. II.1.1) ; si x engendre le groupe multiplicatif $(\mathbf{F}_{q^n}, \times)$ (exerc. 1.29), on considérera une matrice de polynôme caractéristique le polynôme minimal de x sur $\mathbf{F}_q$).

1.7. Quotients d'espaces vectoriels. — Si V est un **K**-espace vectoriel et $W \subseteq V$ un sous-espace vectoriel, alors en particulier, pour la structure de groupe abélien, W est un sous-groupe de V donc on peut former le quotient V/W. Dans ce cas, la structure de **K**-espace vectoriel passe aussi au quotient, en définissant pour $x \in V$ la multiplication par le scalaire $\lambda \in \mathbf{K}$ dans V/W par $\lambda(x + W) = (\lambda x) + W$: en effet, si on prend un autre représentant $y = x + f$ ($f \in W$) de la classe de x dans V/W, alors $\lambda y = \lambda x + \lambda f$ représente bien la classe $\lambda x + W \in V/W$ puisque $\lambda f \in W$. La surjection

$$p : V \longrightarrow V/W$$

est alors aussi une application linéaire de noyau W et la propriété de factorisation (théorème 1.19) reste valable en remplaçant les morphismes de groupes par des applications linéaires : si $\phi : V \to V'$ est une application linéaire telle que $\ker\phi \supseteq W$, elle se factorise, de manière unique, par une application linéaire $\hat{\phi} : V/W \to V'$ telle que $\phi = \hat{\phi} \circ p$. À nouveau, cette propriété caractérise le quotient.

Si on choisit dans V un supplémentaire W' de W, de sorte que $V = W \oplus W'$, la restriction $p|_{W'} : W' \to V/W$ est un isomorphisme linéaire. Via cet isomorphisme, l'application linéaire induite au quotient, $\hat{\phi}$, peut s'identifier à la restriction $\phi|_{W'}$, mais ce n'est pas intrinsèque, car le supplémentaire W' n'est pas unique.

Attention, cette propriété est particulière aux espaces vectoriels : dans le cas des groupes, si $H \trianglelefteq G$, en général G n'est pas isomorphe au produit $H \times G/H$ (*cf.* ex. 1.22.2°).

2. Groupes opérant sur un ensemble

2.1. Actions de groupe. — Une *action* (à gauche [5]) d'un groupe G sur un ensemble X est la donnée d'une application

$$\begin{array}{ccc} \mathrm{G}\times\mathrm{X} & \longrightarrow & \mathrm{X} \\ (g,x) & \longmapsto & g\cdot x \end{array}$$

telle que

1° pour tout $x\in\mathrm{X}$, on a $e\cdot x = x$;

2° pour tout $x\in\mathrm{X}$ et tous $g_1, g_2\in\mathrm{G}$, on a $g_1\cdot(g_2\cdot x) = (g_1g_2)\cdot x$.

Il résulte de cette définition que, si on pose $\Phi_g(x) = g\cdot x$, on a

$$\Phi_e = \mathrm{Id}_\mathrm{X}, \quad \Phi_{g_1}\circ\Phi_{g_2} = \Phi_{g_1g_2}.$$

Une action du groupe G sur l'ensemble X est donc la même chose qu'un morphisme de groupes

$$\begin{array}{ccc} \Phi : \mathrm{G} & \longrightarrow & \mathrm{Bij}(\mathrm{X}) \\ g & \longmapsto & \Phi_g, \end{array} \tag{2}$$

où Bij(X) est le groupe des bijections de X.

Exemples 2.1. — 1° Pour tout ensemble X, le groupe Bij(X) agit sur X. En particulier, le groupe symétrique $\mathfrak{S}_n$ agit sur l'ensemble $\{1,\dots,n\}$.

2° Soit **K** un corps. Le groupe $\mathrm{GL}_n(\mathbf{K})$ opère sur $\mathbf{K}^n$.

3 ° Le groupe $\mathrm{SL}_2(\mathbf{R})$ opère sur le demi-plan de Poincaré $\mathscr{H} = \{z\in\mathbf{C} \mid \mathrm{Im}(z) > 0\}$ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot z = \frac{az+b}{cz+d}.$$

4° Si $\mathrm{H}\leq\mathrm{G}$, alors G opère sur l'ensemble G/H des classes à gauche par $g\cdot(x\mathrm{H}) = (gx)\mathrm{H}$. Dans le cas particulier où $\mathrm{H} = \{e\}$, on obtient l'action de G sur lui-même par translation à gauche.

2.2. Orbites. — Soit G un groupe opérant sur X. On vérifie que la relation

$$x\mathscr{R}y \iff \exists g\in\mathrm{G} \quad y = g\cdot x$$

est une relation d'équivalence sur X. La classe d'équivalence d'un élément x de X est son *orbite*

$$\mathrm{G}x := \{g\cdot x \mid g\in\mathrm{G}\},$$

de sorte que G est réunion disjointes de orbites sous G. On appelle l'ensemble des orbites de X sous G le *quotient de* X *par* G, noté $\mathrm{G}\backslash\mathrm{X}$ [6].

---

5. On utilise parfois les actions *à droite*, notées $(g,x)\mapsto x\cdot g$, et satisfaisant la relation $(x\cdot g)\cdot g' = x\cdot(gg')$. Ce n'est pas une action à gauche, mais une action à droite, notée $\cdot_d$, se ramène à une action à gauche, notée $\cdot$, en considérant $g\cdot x = x\cdot_d g^{-1}$.

6. Dans cette notation, le groupe est placé à gauche pour une action à gauche. Pour une action à droite, l'orbite de x est en bijection avec $\mathrm{G}_x\backslash\mathrm{G}$ et le quotient est noté X/G.

Le *stabilisateur* de x est le sous-groupe de G défini par

$$G_x := \{g \in G \mid g \cdot x = x\}.$$

L'application

$$\begin{array}{ccc} G & \longrightarrow & Gx \\ g & \longmapsto & g \cdot x \end{array}$$

se factorise en une *bijection*

$$G/G_x \xrightarrow{\sim} Gx \tag{3}$$

entre l'espace des classes à gauche de G_x et l'orbite de x. En particulier, si G est fini, il résulte du théorème de Lagrange (th. 1.13) que les orbites sont finies et que leur cardinal divise $|G|$.

Les stabilisateurs des points d'une même orbite sont tous conjugués : pour tout $x \in X$ et tout $g \in G$, on a

$$G_{gx} = gG_xg^{-1}.$$

L'action de G est *transitive* si G n'a qu'une seule orbite dans X. Dans ce cas, par (3), l'action de G induit une bijection de G/G_x avec X, pour tout $x \in X$. En particulier, si G est fini, X l'est aussi et son cardinal divise $|G|$.

L'action de G est *fidèle* si l'application Φ de (2) est injective. Dans le cas général, Φ se factorise en

$$\begin{array}{ccc} G & \xrightarrow{\Phi} & \mathrm{Bij}(X) \\ \downarrow & \nearrow_{\hat{\Phi}} & \\ G/\ker\Phi. & & \end{array}$$

On obtient donc une action fidèle du quotient $G/\ker\Phi$ sur X : toute action se factorise ainsi en une action fidèle.

Exemples 2.2. — 1° Soit $\mathbf{K}$ un corps. Pour $n \geqslant 1$, l'action de $GL_n(\mathbf{K})$ sur $\mathbf{K}^n$ est fidèle et les orbites sont $\mathbf{K}^n - \{0\}$ et $\{0\}$. L'action du groupe affine $GA(\mathbf{K}^n)$ (*cf.* ex. 1.1.5°) sur $\mathbf{K}^n$ est fidèle et transitive.

2° Pour l'action (fidèle) du groupe orthogonal $O_n(\mathbf{R})$ sur $\mathbf{R}^n$ (*cf.* ex. II.4.3.2°), les orbites sont les sphères de rayon > 0, ainsi que $\{0\}$. Le stabilisateur d'un point non nul est (isomorphe à) $O_{n-1}(\mathbf{R})$, donc, par (3), on a une bijection $O_n(\mathbf{R})/O_{n-1}(\mathbf{R}) \simeq \mathbf{S}^{n-1}$.

3° L'action décrite plus haut du groupe $SL_2(\mathbf{R})$ sur le demi-plan de Poincaré est transitive. Elle n'est pas fidèle (le noyau de l'action est $\{\pm I_2\}$).

4° Soit $\mathbf{K}$ un corps. Le groupe $\mathbf{K}^\times$ agit sur $\mathbf{K}^n - \{0\}$ et le quotient est

$$\mathbf{K}^\times \backslash (\mathbf{K}^n - \{0\}) = \{\text{droites vectorielles de } \mathbf{K}^n\},$$

appelé l'espace projectif (sur $\mathbf{K}$) et noté $\mathbf{P}^{n-1}(\mathbf{K})$.

5° Si $\sigma \in \mathfrak{S}_n$, on considère l'action du groupe $\langle\sigma\rangle$ sur $\{1, \ldots, n\}$. Alors $\{1, \ldots, n\}$ est la réunion disjointe des orbites :

$$\{1, \ldots, n\} = \bigsqcup_1^r O_i.$$

On peut poser

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{si } x \in \mathrm{O}_i, \\ x & \text{si } x \notin \mathrm{O}_i. \end{cases}$$

Alors σ_i est un cycle de support O_i, on a $\sigma_i\sigma_j = \sigma_j\sigma_i$ et

$$\sigma = \sigma_1 \cdots \sigma_r.$$

On démontre ainsi que toute permutation se décompose (de manière unique) comme produit de cycles à supports disjoints (qui commutent donc deux à deux).

***Exemple 2.3* (Théorème de Cayley).** — L'action de G sur lui-même par translation à gauche, définie par $g \cdot x = gx$, est fidèle. Si G est fini, on en déduit un morphisme injectif $\mathrm{G} \hookrightarrow \mathfrak{S}_{|\mathrm{G}|}$ (qui dépend de la façon dont on numérote les éléments de G).

Exercice 2.4. — Soit G un groupe fini d'ordre n.
a) Montrer que G est isomorphe à un sous-groupe de $\mathfrak{A}_{2n}$, et même de $\mathfrak{A}_{n+2}$.
b) Soit $\mathbf{K}$ un corps. Montrer que G est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbf{K})$ et à un sous-groupe de $\mathrm{SL}_{n+1}(\mathbf{K})$.
c) Montrer que G est isomorphe à un sous-groupe de $\mathrm{O}_{n-1}(\mathbf{R})$.

Exercice 2.5. — Soit G un groupe fini d'ordre $2n$, avec n impair.
a) Montrer que G contient un élément d'ordre 2 (*Indication :* on pourra compter le nombre de paires (g, g^{-1})).
b) Montrer que l'image du morphisme injectif $\mathrm{G} \hookrightarrow \mathfrak{S}_{2n}$ donné par le théorème de Cayley (ex. 2.3) n'est pas contenue dans $\mathfrak{A}_{2n}$.
c) En déduire que G contient un sous-groupe distingué d'indice 2.

Exercice 2.6. — Soit G un groupe opérant fidèlement et transitivement sur un ensemble X de cardinal p premier et soit $\mathrm{H} \trianglelefteq \mathrm{G}$ un sous-groupe distingué, $\mathrm{H} \neq \{e\}$. Montrer que H opère transitivement sur X.

Exercice 2.7. — Soit G un sous-groupe de $\mathfrak{S}_n$ opérant transitivement sur l'ensemble $\{1, \ldots, n\}$ et contenant une transposition et un p-cycle, où p est un nombre premier $> n/2$. Le but de l'exercice est de montrer $\mathrm{G} = \mathfrak{S}_n$.

Si $a, b \in \{1, \ldots, n\}$, on écrit $a \sim b$ si $a = b$, ou si $a \neq b$ et que la transposition (ab) est dans G.
a) Montrer que $\sim$ est une relation d'équivalence sur l'ensemble $\{1, \ldots, n\}$.
b) Si $a \sim b$ et $g \in \mathrm{G}$, montrer $g(a) \sim g(b)$.
c) Montrer que toutes les classes d'équivalence pour $\sim$ ont le même cardinal r et que $r \geqslant 2$.
d) Soit s le nombre de classes d'équivalence pour $\sim$. Montrer $n = rs$ et $r \geqslant p$. Conclure.

2.3. Conjugaison. — Il y a une autre action de G sur lui-même, donnée par le morphisme $\mathrm{G} \to \mathrm{Aut}(\mathrm{G})$ défini par $g \cdot x = gxg^{-1}$ (action par *conjugaison*). Dans ce cas, le stabilisateur d'un élément $x \in \mathrm{G}$ est appelé le *centralisateur* de x, noté $\mathrm{C}(x)$. Les orbites sont appelées *classes de conjugaison* de G.

Explicitons cette action dans le cas du groupe symétrique.

Proposition 2.8. — *Si $\sigma = (a_1 \cdots a_k) \in \mathfrak{S}_n$ est un k-cycle et $\tau \in \mathfrak{S}_n$, on a*

$$\tau\sigma\tau^{-1} = (\tau(a_1) \cdots \tau(a_k)). \tag{4}$$

Tous les k-cycles sont conjugués dans $\mathfrak{S}_n$.

Les classes de conjugaison de $\mathfrak{S}_n$ sont en bijection avec les partitions de n :

$$n = k_1 + \cdots + k_r, \quad r \in \mathbf{N},\ 1 \leqslant k_1 \leqslant \cdots \leqslant k_r.$$

Démonstration. — Si $x \notin \{\tau(a_1), \ldots, \tau(a_k)\}$, alors $\tau^{-1}(x) \notin \{a_1, \ldots, a_k\}$ donc $\tau\sigma\tau^{-1}(x) = x$. Si en revanche $x = \tau(a_i)$, alors $\tau\sigma\tau^{-1}(x) = \tau\sigma(a_i) = \tau(a_{i+1})$. Cela prouve la première partie de la proposition.

Pour la seconde, écrivons $\sigma = \sigma_1 \cdots \sigma_r$ comme produit de cycles à supports disjoints de longueurs $k_1, \ldots, k_r$, qu'on peut ordonner de sorte que $1 \leqslant k_1 \leqslant \cdots \leqslant k_r$. Alors

$$\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdots (\tau\sigma_r\tau^{-1}) \tag{5}$$

est encore un produit de cycles disjoints de mêmes longueurs $k_1, \ldots, k_r$ que ceux de σ, donc une classe de conjugaison détermine bien une partition de $n = k_1 + \cdots + k_r$. Réciproquement, compte tenu des formules (4) et (5), on voit que des permutations correspondant à la même partition sont conjuguées. □

Exemple 2.9. — 1° Les 2 partitions de 2 sont $1+1$ et 2. Les classes de conjugaison correspondantes dans $\mathfrak{S}_2$ sont $\{\mathrm{Id}\}$ et $\{(1,2)\}$.

2° Les 3 partitions de 3 sont $1+1+1$, $1+2$ et 3. Les classes de conjugaison correspondantes dans $\mathfrak{S}_3$ sont $\{\mathrm{Id}\}$, $\{(1,2),(1,3),(2,3)\}$ et $\{(1,2,3),(1,3,2)\}$.

3° Les 5 partitions de 4 sont $1+1+1+1$, $1+1+2$, $2+2$, $1+3$ et 4. Les classes de conjugaison correspondantes dans $\mathfrak{S}_4$ sont $\{\mathrm{Id}\}$, les 6 transpositions, les 3 doubles transpositions, les 8 3-cycles et les 6 4-cycles.

De manière générale, la conjugaison préserve les propriétés d'une transformation. Par exemple, si $\sigma \in \mathrm{O}_3(\mathbf{R})$ est une rotation autour d'une droite D et $\tau \in \mathrm{O}_3(\mathbf{R})$, alors $\tau\sigma\tau^{-1}$ est une rotation de même angle autour de la droite $\tau(\mathrm{D})$.

Exercice 2.10. — Soit p un nombre premier impair et soit q une puissance de p. Le but de cet exercice est de décrire les classes de conjugaison de $\mathrm{G} := \mathrm{SL}_2(\mathbf{F}_q)$. On rappelle $|\mathrm{G}| = q(q^2-1)$ (exerc. 1.24).

Pour tout $a \in \mathbf{F}_q$ et tout $\lambda \in \mathbf{F}_q^\times$, on pose

$$\mathrm{U}_a := \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \qquad \mathrm{V}_\lambda := \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}.$$

a) Si $a \in \mathbf{F}_q^\times$, calculer le cardinal de la classe de conjugaison de U_a.

b) Si $a, b \in \mathbf{F}_q^\times$, donner une condition nécessaire et suffisante sur a et b pour que U_a et U_b soient conjuguées dans G.

c) Mêmes questions pour les matrices V_λ, pour $\lambda \in \mathbf{F}_q - \{0, 1, -1\}$.

Soit $\mathrm{M} \in \mathrm{G}$. *On note* λ *et* λ^{-1} *ses valeurs propres, c'est-à-dire les racines de son polynôme caractéristique, avec* $\lambda + \lambda^{-1} = \mathrm{tr}(\mathrm{M})$. *Elles sont a priori dans une extension quadratique de* $\mathbf{F}_q$, *c'est-à-dire dans* $\mathbf{F}_{q^2}$. *Si* $e \in \mathbf{F}_q - \mathbf{F}_q^2$, *une telle extension est donnée par* $\mathbf{F}_{q^2} = \mathbf{F}_q[\sqrt{e}]$ *: tout élément de* $\mathbf{F}_q^2$ *s'écrit de façon unique* $a + b\sqrt{e}$, *avec* $a, b \in \mathbf{F}_q$.

d) On suppose $\lambda = 1$. Montrer que M est conjuguée dans G à une matrice U_a, avec $a \in \mathbf{F}_q$.

e) On suppose $\lambda \in \mathbf{F}_q - \{0, 1, -1\}$. Montrer que M est conjuguée dans G à V_λ.

f) On suppose enfin $\lambda \notin \mathbf{F}_q$ et on écrit $\lambda = a + b\sqrt{e}$, avec $a, b \in \mathbf{F}_q$, $b \neq 0$. Montrer que $a^2 - eb^2 = 1$ et que M est conjuguée dans G à la matrice $\mathrm{R}_{a,b} := \begin{pmatrix} a & eb \\ b & a \end{pmatrix}$ ou à la matrice $\mathrm{R}_{a,-b}$.

f) Montrer que dans G, il y a 2 classes de conjugaison avec 1 seul élément, puis 4 classes de conjugaison, chacune avec $\frac{1}{2}(q^2-1)$ éléments, puis $\frac{1}{2}(q-3)$ classes de conjugaison, chacune avec $q(q+1)$ éléments, puis $\frac{1}{2}(q-1)$ classes de conjugaison, chacune avec $q(q-1)$ éléments, soit au total

$$2\times 1+4\times\frac{1}{2}(q^2-1)+\frac{1}{2}(q-3)\times q(q+1)+\frac{1}{2}(q-1)\times q(q-1)=q(q^2-1)=|\mathrm{G}|$$

éléments.

2.4. Formule des classes et p-groupes. — La formule des classes n'est que la reformulation du fait qu'un ensemble sur lequel un groupe G agit est réunion disjointe des orbites. Son intérêt provient du fait que lorsque G est fini, le cardinal de chaque orbite divise |G|.

***Proposition 2.11* (Formule des classes).** — *Soit* G *un groupe fini agissant sur un ensemble fini* X*. On a*

$$\mathrm{card}(\mathrm{X})=\sum_{x\in\mathrm{R}}[\mathrm{G}:\mathrm{G}_x],$$

où $\mathrm{R}\subseteq\mathrm{X}$ *est un ensemble contenant exactement un point de chaque orbite.*

Démonstration. — La démonstration est facile : X est la réunion disjointe des orbites et par (3), chaque orbite est en bijection avec G/G_x pour un élément x de l'orbite. □

Un point $x\in\mathrm{X}$ est un *point fixe de l'action* de G si $g\cdot x=x$ pour tout $g\in\mathrm{G}$, c'est-à-dire si l'orbite de x est réduite à $\{x\}$. On note X^{G} l'ensemble des points fixes de X sous G.

Exemple 2.12. — Soit $\mathbf{K}$ un corps. Le groupe $\mathbf{K}^\times$ agit sur $\mathbf{K}^n$ par multiplication. L'origine 0 est le seul point fixe ; les autres points ont un stabilisateur trivial. Si $\mathbf{K}$ est un corps fini $\mathbf{F}_q$ avec q éléments, le cardinal de $\mathbf{K}^n$ est q^n et la formule des classes s'écrit donc (*cf.* ex. 2.2.4°)

$$q^n=1+(q-1)\,\mathrm{card}(\mathbf{P}^{n-1}(\mathbf{F}_q)).$$

Proposition 2.13. — *1° Si un* p-groupe G *(c'est-à-dire un groupe fini non trivial d'ordre une puissance du nombre premier* p*) agit sur* X*, alors*

$$\mathrm{card}(\mathrm{X}^{\mathrm{G}})\equiv\mathrm{card}(\mathrm{X})\pmod{p}.$$

En particulier, si $p\nmid\mathrm{card}(\mathrm{X})$*, l'action de* G *sur* X *a au moins un point fixe.*

2° Si G *est un* p*-groupe, le centre de* G *n'est pas réduit à* $\{e\}$*.*

Démonstration. — Par la formule des classes, on a

$$\mathrm{card}(\mathrm{X})=\mathrm{card}(\mathrm{X}^{\mathrm{G}})+\sum_{x\in\mathrm{R}-\mathrm{X}^{\mathrm{G}}}[\mathrm{G}:\mathrm{G}_x].$$

Si x n'est pas un point fixe, $\mathrm{G}_x<\mathrm{G}$, donc $[\mathrm{G}:\mathrm{G}_x]>1$ et divise |G| qui est une puissance de p, donc $p|[\mathrm{G}:\mathrm{G}_x]$. La première partie de la proposition en résulte.

La seconde partie s'obtient en appliquant le résultat à l'action de G sur lui-même par conjugaison : dans ce cas, on a $\mathrm{G}^{\mathrm{G}}=\mathrm{Z}(\mathrm{G})$, donc $|\mathrm{Z}(\mathrm{G})|\equiv|\mathrm{G}|\pmod{p}$, ce qui impose $|\mathrm{Z}(\mathrm{G})|>1$. □

***Exercice 2.14* (Lemme de Cauchy).** — Soit G un groupe fini et soit p un nombre premier divisant |G|. En utilisant une action convenable de $\mathbf{Z}/p\mathbf{Z}$ sur l'ensemble

$$X = \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = e\},$$

prouver que G admet un élément d'ordre p (*cf.* cor. 2.24 pour une généralisation).

Corollaire 2.15. — *1° Si* G *est un groupe d'ordre p^2 avec p premier,* G *est abélien.*
2° Un p-groupe simple est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

On a déjà vu que tout groupe d'ordre p est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

Comme on le verra plus loin, il n'y a à isomorphisme près que deux groupes (abéliens) d'ordre p^2, à savoir $\mathbf{Z}/p^2\mathbf{Z}$ et $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

Démonstration. — 1° D'après la proposition, on a $|Z(G)| = p$ ou p^2. Si $x \in G$, le centralisateur $C(x)$ de x contient à la fois Z(G) et x. Si $x \notin Z(G)$, on déduit que $|C(x)| \geqslant |Z(G)|+1 \geqslant p+1$, donc $|C(x)| = p^2$ puisque $|C(x)|$ divise $|G| = p^2$. On a donc $C(x) = G$, c'est-à-dire $x \in Z(G)$: contradiction. Donc on a toujours $x \in Z(G)$, donc $Z(G) = G$ et G est abélien.

2° Si G est un p-groupe simple, son centre Z(G), qui est un sous-groupe distingué de G non trivial, est égal à G. Le groupe G est donc abélien et, étant simple, il est isomorphe à $\mathbf{Z}/p\mathbf{Z}$. □

Exercice 2.16. — Soit p un nombre premier. Montrer qu'il existe un groupe non abélien de cardinal p^3 (*Indication :* utiliser l'ex. 2.19).

***Exercice 2.17* (Lemme d'Ore).** — Soit G un groupe fini, soit p le plus petit facteur premier de |G| et soit H un sous-groupe de G d'indice p. Montrer que H est distingué dans G (*Indication :* on pourra s'intéresser au noyau de l'action de l'ex. 2.1.4°).

***Exercice 2.18* (Formule de Burnside).** — Soit G un groupe fini opérant sur un ensemble fini X. Le fixateur d'un élément $g \in G$ est par définition l'ensemble $\mathrm{Fix}(g) := \{x \in X \mid g \cdot x = x\}$. Montrer que le nombre d'orbites pour l'action de G sur X est donné par la formule

$$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

(*Indication :* on pourra calculer de plusieurs façons le cardinal de l'ensemble $\{(g, x) \in G \times X \mid g \cdot x = x\}$).

2.5. Théorèmes de Sylow. — Soit G un groupe fini et soit p un facteur premier de |G|. Écrivons $|G| = p^\alpha m$, avec $p \nmid m$. Un *p-sous-groupe de Sylow* de G (ou, plus brièvement, un p-sous-groupe de Sylow) est un sous-groupe d'ordre p^α de G [7].

Exemple 2.19. — Soit $q = p^\beta$ une puissance d'un nombre premier p. Dans $G = GL_n(\mathbf{F}_q)$, considérons le sous-groupe $T_n(\mathbf{F}_q)$ des matrices triangulaires supérieures, avec des 1 sur

7. Peter Ludwig Mejdell Sylow, mathématicien norvégien (1832–1918), a démontré en 1872 les théorèmes qui portent son nom et sont regroupés dans le th. 2.21.

la diagonale (matrices *unipotentes*) :

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Alors $\mathrm{T}_n(\mathbf{F}_q)$ est un p-sous-groupe de Sylow de G. En effet, $|\mathrm{T}_n(\mathbf{F}_q)| = q^{\frac{n(n-1)}{2}}$, alors que d'après l'exerc. 1.24, on a $\alpha = \beta\frac{n(n-1)}{2}$.

Pour montrer l'existence d'un p-sous-groupe de Sylow dans tout groupe fini, nous avons besoin d'abord de passer d'un groupe à ses sous-groupes.

Lemme 2.20. — *Si* S *est un p-sous-groupe de Sylow de* G *et* $\mathrm{H} \leq \mathrm{G}$*, il existe* $g \in \mathrm{G}$ *tel que* $g\mathrm{S}g^{-1} \cap \mathrm{H}$ *soit un p-sous-groupe de Sylow de* H.

Démonstration. — Le groupe H agit à gauche sur l'ensemble G/S des classes à gauche par $h\cdot(g\mathrm{S}) = (hg)\mathrm{S}$. Le stabilisateur d'une classe gS est $\mathrm{H}_{g\mathrm{S}} = g\mathrm{S}g^{-1} \cap \mathrm{H}$. Puisque $p \nmid m = |\mathrm{G}/\mathrm{S}|$, la formule des classes (prop. 2.11) assure qu'il existe au moins une classe gS telle que

$$p \nmid [\mathrm{H} : \mathrm{H}_{g\mathrm{S}}].$$

Mais puisque $\mathrm{H}_{g\mathrm{S}}$ est contenu dans $g\mathrm{S}g^{-1}$, qui est un p-groupe, $\mathrm{H}_{g\mathrm{S}}$ est lui-même un p-groupe, et donc un p-sous-groupe de Sylow de H. □

Théorème de Sylow 2.21. — *Soit* G *un groupe fini et soit p un facteur premier de* $|\mathrm{G}|$*. Écrivons* $|\mathrm{G}| = p^\alpha m$*, avec* $p \nmid m$*. Alors :*

1° G *contient un p-sous-groupe de Sylow ;*

2° *tout p-sous-groupe de* G *est contenu dans un p-sous-groupe de Sylow ;*

3° *tous les p-sous-groupes de Sylow sont conjugués dans* G *;*

4° *le nombre de p-sous-groupes de Sylow divise m et est congru à* 1 *modulo p.*

Corollaire 2.22. — *Sous les mêmes hypothèses, un p-sous-groupe de Sylow de* G *est distingué dans* G *si et seulement si c'est l'unique p-sous-groupe de Sylow de* G.

Démonstration du théorème. — 1° Si $\mathrm{N} := |\mathrm{G}|$, le groupe G s'injecte dans un groupe symétrique $\mathfrak{S}_\mathrm{N}$ (ex. 2.3), lequel s'injecte dans $\mathrm{GL}_\mathrm{N}(\mathbf{F}_p)$, en envoyant une permutation $\sigma \in \mathfrak{S}_\mathrm{N}$ sur l'application linéaire u_σ permutant les éléments de base $(e_1, \ldots, e_\mathrm{N})$ par σ, donc définie par $u_\sigma(e_i) = e_{\sigma(i)}$. On peut ainsi considérer G comme un sous-groupe de $\mathrm{GL}_\mathrm{N}(\mathbf{F}_p)$, qui admet un p-sous-groupe de Sylow par l'ex. 2.19. Par le lemme 2.20, G admet un p-sous-groupe de Sylow.

2-3° Si $\mathrm{H} \leq \mathrm{G}$ est un p-groupe et $\mathrm{S} \leq \mathrm{G}$ un p-sous-groupe de Sylow, toujours par le lemme 2.20, il existe $g \in \mathrm{G}$ tel que $g\mathrm{S}g^{-1} \cap \mathrm{H}$ est un p-sous-groupe de Sylow de H, donc est égal à H puisque H est un p-groupe. Donc $\mathrm{H} \leq g\mathrm{S}g^{-1}$, qui est un p-sous-groupe de Sylow. Si en outre H était déjà un p-sous-groupe de Sylow, il a le même ordre que $g\mathrm{S}g^{-1}$, donc $\mathrm{H} = g\mathrm{S}g^{-1}$.

4° Soit X l'ensemble des p-sous-groupes de Sylow de G. On a donc une action transitive de G sur X par conjugaison, ce qui implique que card(X) divise |G|. Restreignons maintenant l'action de G à un p-sous-groupe de Sylow particulier S. Pour montrer $\mathrm{card}(X) \equiv 1 \pmod{p}$, d'après la prop. 2.13, il suffit de montrer $\mathrm{card}(X^S) = 1$. On va montrer que S est le seul point fixe de l'action de S sur X.

Pour cela, introduisons pour un sous-groupe quelconque $H \leq G$ son *normalisateur* (dans G) défini par

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}. \tag{6}$$

Il s'agit, pour l'action de G sur l'ensemble de ses sous-groupes par conjugaison, du stabilisateur de H. Une propriété évidente, mais importante, est

$$H \trianglelefteq N_G(H).$$

Revenons maintenant à la démonstration : supposons que $S' \in X^S$, donc $sS's^{-1} = S'$ pour tout $s \in S$. Il en résulte que $S \leq N_G(S')$. Ainsi S et S′ sont des p-sous-groupes de Sylow de $N_G(S')$ donc sont conjugués dans $N_G(S')$ par le 3°. Comme $S' \trianglelefteq N_G(S')$, on en déduit $S = S'$. □

Exemples 2.23. — 1° La démonstration du point 4° montre que le nombre de p-sous-groupes de Sylow est l'indice du normalisateur d'un quelconque d'entre eux (ils sont tous conjugués).

2° Soit q une puissance de p. Le théorème de Sylow entraîne que tout p-sous-groupe de $GL_n(\mathbf{F}_q)$ est constitué, dans une base convenable, de matrices unipotentes triangulaires supérieures (*cf.* ex. 2.19). On peut montrer (*cf.* exerc. 2.28) que le nombre de p-sous-groupes de Sylow de $GL_n(\mathbf{F}_q)$ est

$$\frac{q^n-1}{q-1} \cdot \frac{q^{n-1}-1}{q-1} \cdots \frac{q^2-1}{q-1}.$$

3° Les p-sous-groupes de Sylow du groupe $\mathfrak{S}_p$ sont les sous-groupes engendrés par les p-cycles. Il y a $(p-1)!$ p-cycles, donc $(p-2)!$ p-sous-groupes de Sylow. On obtient la congruence $(p-2)! \equiv 1 \pmod{p}$.

Le théorème de Sylow a de nombreuses conséquences ; en voici une.

Corollaire 2.24. — *Si le groupe* G *satisfait* $|G| = p^\alpha m$ *avec* $p \nmid m$, *alors pour tout* $\beta \leqslant \alpha$, *il existe un sous-groupe de* G *d'ordre* p^β. *En particulier, si* $p \mid |G|$, *il existe dans* G *un élément d'ordre* p.

Démonstration. — En regardant un p-sous-groupe de Sylow, il suffit de le montrer pour un p-groupe S non trivial.

On a vu (prop. 2.13.2°) que son centre Z(S) est un p-groupe non trivial. Si $g \in Z(S)$ est non trivial, il est d'ordre p^γ, avec $\gamma \in \mathbf{N}^*$, et le sous-groupe H engendré par $g^{p^{\gamma-1}}$ est d'ordre p. Il est aussi distingué dans S.

On peut raisonner par récurrence sur |S| : pour $0 < \beta \leqslant \alpha$, il existe alors un sous-groupe de S/H d'ordre $p^{\beta-1}$, dont l'image inverse dans S est un sous-groupe de S d'ordre p^β. □

Que dit le théorème de Sylow dans le cas d'un groupe *abélien* fini G ? Tout p-sous-groupe de Sylow S est alors distingué, donc unique (cor. 2.22). Montrons que ce p-sous-groupe de Sylow est

$$\mathrm{T}_p(\mathrm{G}) := \{g \in \mathrm{G} \mid \exists n \in \mathbf{N} \quad p^n g = 0\}, \tag{7}$$

le *sous-groupe de p-torsion* de G (conformément à la tradition, on note additivement l'opération du groupe abélien G). On vérifie facilement que $\mathrm{T}_p(\mathrm{G})$ est un sous-groupe de G (mais on se sert ici du fait que G est abélien !).

Ensuite, l'ordre de tout élément de S est une puissance de p, donc $\mathrm{S} \leq \mathrm{T}_p(\mathrm{G})$. Mais l'ordre de tout élément de $\mathrm{T}_p(\mathrm{G})$ est aussi une puissance de p, donc l'ordre de $\mathrm{T}_p(\mathrm{G})$ est aussi une puissance de p (cor. 2.24). Par définition d'un p-sous-groupe de Sylow, on en déduit $\mathrm{S} = \mathrm{T}_p(\mathrm{G})$.

Exercice 2.25. — Soit G un groupe fini d'ordre n, vu comme sous-groupe de $\mathfrak{S}_n$ (ex. 2.3). Le but de cet exercice est de déterminer à quelle condition nécessaire et suffisante sur G celui-ci n'est pas contenu dans le groupe alterné $\mathfrak{A}_n$ (auquel cas G contient le sous-groupe $\mathrm{G} \cap \mathfrak{A}_n$, d'indice 2 donc distingué, et G n'est pas simple si $n > 2$).
a) Soit g un élément de G d'ordre m. Montrer que la permutation de G associée se décompose en produit de n/m m-cycles à supports disjoints.
b) Si $\mathrm{G} \not\leq \mathfrak{A}_n$, en déduire que G est d'ordre pair et que les 2-sous-groupes de Sylow de G sont cycliques.
c) Inversement, on suppose que G est d'ordre pair et qu'un 2-sous-groupe de Sylow de G est cyclique. Montrer que $\mathrm{G} \not\leq \mathfrak{A}_n$ (on généralise ainsi le résultat de l'exerc. 2.5).

Exercice 2.26. — Soit G un groupe fini d'ordre $2^n m$, avec $n \geqslant 1$ et m impair. On suppose que tout 2-sous-groupe de Sylow de G est cyclique. Montrer qu'il existe un sous-groupe de G qui contient tous les sous-groupes d'ordre impair de G et que ce sous-groupe est distingué dans G (*Indication :* on pourra procéder par récurrence sur n, en utilisant l'exerc. 2.25).

Exercice 2.27. — Soit p un nombre premier.
a) Décrire les p-sous-groupes de Sylow de $\mathfrak{S}_p$, puis de $\mathfrak{S}_{p+b}$, pour chaque $b \in \{0, \dots, p-1\}$, puis de $\mathfrak{S}_{ap+b}$, pour chaque $a, b \in \{0, \dots, p-1\}$. Combien y en a-t-il ?
b) Montrer que les permutations $(1,2,3)$ et $(1,4,7)(2,5,8)(3,6,9)$ engendrent un 3-sous-groupe de Sylow de $\mathfrak{S}_9$ et que celui-ci n'est pas abélien.
c) Décrire les p-sous-groupes de Sylow de $\mathfrak{S}_{p^2}$ et montrer qu'ils ne sont pas abéliens si $p \geqslant 3$.

Exercice 2.28. — Soit p un nombre premier et soit $\mathbf{F}_q$ un corps de cardinal une puissance q de p.
a) Décrire un p-sous-groupe de Sylow S du groupe $\mathrm{G} := \mathrm{GL}_n(\mathbf{F}_q)$ ainsi que son normalisateur $\mathrm{N}_{\mathrm{G}}(\mathrm{S})$ (*cf.* (6)).
b) En déduire le nombre de p-sous-groupes de Sylow de G (*Indication :* on pourra utiliser l'ex. 2.23.1°).

Exercice 2.29. — Soient p et q des nombres premiers et soit G un groupe d'ordre pq.
a) Montrer que G n'est pas simple (*Indication :* on pourra compter les p- ou q-sous-groupes de Sylow de G).
b) Si $p < q$ et que p ne divise pas $q-1$, montrer que G est cyclique (*Indication :* on pourra montrer que G contient un unique p-sous-groupe de Sylow et un unique q-sous-groupe de Sylow).

Exercice 2.30. — Soient p et q des nombres premiers tels que p ne divise pas $q-1$ et $p<q$. Montrer que tout groupe d'ordre p^2q est abélien.

Exercice 2.31. — a) Soit G un groupe fini simple. Écrivons $|G| = p^\alpha m$, avec $p \nmid m$, $m \geqslant 2$ et $\alpha \geqslant 1$, et notons n_p le nombre de ses p-sous-groupes de Sylow. Montrer que $|G|$ divise $n_p!$.
b) Montrer qu'il n'existe pas de groupe simple de cardinal 1 000 000.

Exercice 2.32. — Soient p et q des nombres premiers vérifiant $p<q$ et soit G un groupe d'ordre $p^m q^n$, avec $0 \leqslant m \leqslant 2$ et $n \geqslant 0$. Montrer que G n'est pas simple (*Indication :* dans le cas $p=2$ et $q=3$, on pourra utiliser l'exerc. 2.31 ; dans le cas $|G|=12$, on pourra compter les éléments d'ordre 3).

Exercice 2.33. — Soient p et q des nombres premiers et soit G un groupe d'ordre p^2q. Montrer que G n'est pas simple (*Indication :* on pourra utiliser l'exerc. 2.32).

Exercice 2.34. — Soient p et q des nombres premiers et soit G un groupe d'ordre p^3q. Montrer que G n'est pas simple (*Indication :* si $|G| \neq 24$, on pourra compter les éléments d'ordre q et montrer que G contient un sous-groupe distingué qui est un p-sous-groupe de Sylow ou un q-sous-groupe de Sylow ; si $|G|=24$, on pourra montrer $G \simeq \mathfrak{S}_4$).

Exercice 2.35. — Montrer qu'un groupe fini simple non abélien d'ordre <168 est d'ordre 60 (*Indication :* on pourra utiliser les résultats des exercices précédents).

Exercice 2.36. — Montrer que tout groupe d'ordre 132 contient des sous-groupes d'ordre 12, 33 et 44.

Exercice 2.37. — Montrer qu'un groupe d'ordre 2907 n'est pas simple.

Exercice 2.38. — Montrer qu'un groupe d'ordre 945 n'est pas simple (*Indication :* on pourra considérer l'action d'un tel groupe G sur l'ensemble X de ses 3-sous-groupes de Sylow puis considérer les normalisateurs d'un 7-sous-groupe de Sylow de G dans G puis dans Bij(X)).

Exercice 2.39. — Montrer qu'un groupe d'ordre 6375 n'est pas simple.

Exercice 2.40. — Le but de cet exercice est de montrer que tout groupe simple G d'ordre 60 est isomorphe à $\mathfrak{A}_5$.
a) Montrer que le nombre de 2-sous-groupes de Sylow de G est soit 5, soit 15. Conclure dans le premier cas. On suppose donc dans la suite que G a 15 2-sous-groupes de Sylow.
b) Montrer qu'il existe deux 2-sous-groupes de Sylow S_1 et S_2 de G dont l'intersection a 2 éléments.
c) Montrer que le normalisateur $N := N_G(S_1 \cap S_2)$ est d'ordre 12 (*cf.* (6)).
d) Montrer que l'action de G par translation sur G/N fournit un morphisme injectif $G \to \mathfrak{S}_5$.
e) Conclure.

Exercice 2.41. — Soit p un nombre premier. Montrer que tout groupe d'ordre $2p$ est soit cyclique, soit isomorphe au groupe diédral D_p.

Exercice 2.42 **(Méthode de Frattini)**. — Soit G un groupe fini.
a) Soit $H \trianglelefteq G$ un sous-groupe distingué et soit S' un p-sous-groupe de Sylow de H. Montrer l'égalitép-sous-groupe de Sylow

$$G = HN_G(S') := \{hk \mid h \in H,\ k \in N_G(S')\}$$

(*Indication :* si $g \in G$, on pourra utiliser le fait que $gS'g^{-1} \leq H$ est conjugué *dans* H à S').

b) Soit maintenant $S \leq G$ un p-sous-groupe de Sylow de G et soit $M \leq G$ un sous-groupe contenant $N_G(S)$. Montrer $M = N_G(M)$ (*Indication :* on pourra appliquer a) à $M \trianglelefteq N_G(M)$ et à son p-sous-groupe de Sylow S).

***Exercice 2.43* (Automorphismes de $\mathfrak{S}_n$).** — Soit $n \in \mathbf{N}^*$.
a) Soit ϕ un automorphisme de $\mathfrak{S}_n$ qui transforme toute transposition en une transposition. Montrer que ϕ est un automorphisme intérieur.
b) Soit $\sigma \in \mathfrak{S}_n$. Déterminer le cardinal du centralisateur $C(\sigma) := \{\tau \in \mathfrak{S}_n \mid \tau\sigma\tau^{-1} = \sigma\}$ de σ.
c) En déduire que si $n \neq 6$, on a $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$.
d) On suppose $n \geqslant 5$ et $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$. Montrer que tous les sous-groupes d'indice n de $\mathfrak{S}_n$ sont conjugués.
e) En utilisant les 5-sous-groupes de Sylow de $\mathfrak{S}_5$, montrer qu'il existe un sous-groupe d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1,\dots,6\}$.
f) En déduire $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

***Exercice 2.44* (Sous-groupes de Sylow d'un sous-groupe).** — Soit G un groupe et soit H un sous-groupe de G. Soit p un nombre premier divisant l'ordre de H.
a) Montrer que tout p-sous-groupe de Sylow de H est contenu dans un p-sous-groupe de Sylow de G.
b) Montrer qu'un p-sous-groupe de Sylow de G contient au plus un p-sous-groupe de Sylow de H.

En particulier, le nombre de p-sous-groupes de Sylow de H est inférieur ou égal au nombre de p-sous-groupes de Sylow de G.

***Exercice 2.45* (Sous-groupes de Sylow d'un groupe quotient).** — Soit G un groupe et soit N un sous-groupe distingué de G. Soit p un nombre premier divisant l'ordre de G/N.
a) Montrer que pour tout p-sous-groupe de Sylow S de G, l'image de S par la surjection canonique $G \to G/N$ est un p-sous-groupe de Sylow de G/N.
b) Montrer que tout p-sous-groupe de Sylow de G/N est obtenu comme en a).

En particulier, le nombre de p-sous-groupes de Sylow de G/N est inférieur ou égal au nombre de p-sous-groupes de Sylow de G.

3. Groupes abéliens de type fini

Le but de cette section est de démontrer le th. 3.6 de structure des groupes abéliens de type fini.

3.1. Structure des groupes cycliques. — On rappelle que les groupes cycliques sont les $\mathbf{Z}/n\mathbf{Z}$, pour $n \in \mathbf{N}^*$.

***Proposition 3.1* (Lemme chinois).** — *Si on décompose un entier positif n en facteurs premiers, $d = \prod p_i^{\alpha_i}$, on a un isomorphisme*

$$\mathbf{Z}/d\mathbf{Z} \simeq \prod \mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}.$$

Notre démonstration montre en fait que c'est un isomorphisme d'anneaux. C'est important, car cela entraîne un isomorphisme

$$(\mathbf{Z}/n\mathbf{Z})^\times \simeq \prod (\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z})^\times.$$

entre groupes multiplicatifs des unités.

Démonstration. — En procédant par récurrence sur le nombre de facteurs dans la décomposition de d, on voit qu'il suffit de montrer l'énoncé suivant : *si d et e sont premiers entre eux,*

$$\mathbf{Z}/de\mathbf{Z} \simeq \mathbf{Z}/d\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z}.$$

Le morphisme $f : \mathbf{Z} \to \mathbf{Z}/d\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z}$ donné par $f(x) = (\bar{x}, \bar{x})$ a pour noyau $de\mathbf{Z}$. Il se factorise donc par un morphisme injectif $\hat{f} : \mathbf{Z}/de\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z}$, qui est un isomorphisme puisque les deux membres ont même cardinal. Cela démontre l'isomorphisme cherché. □

3.2. Engendrement fini. — Rappelons qu'un groupe est de type fini s'il possède une partie génératrice finie. Si G est abélien, cela signifie qu'il existe des éléments $x_1, \dots, x_r$ de G tels que le morphisme de groupes

$$\begin{array}{ccc} \mathbf{Z}^r & \longrightarrow & \mathrm{G} \\ (a_1, \dots, a_r) & \longmapsto & \sum_1^r a_i x_i \end{array} \tag{8}$$

est surjectif (conformément à la tradition, on note additivement l'opération du groupe abélien G).

Proposition 3.2. — *Si* G *est un groupe abélien est de type fini, tout sous-groupe de* G *est abélien de type fini*[8].

Démonstration. — On raisonne par récurrence sur le nombre r de générateurs de G. Si G est engendré par r éléments, on a un morphisme surjectif

$$\mathbf{Z}^r \overset{p}{\twoheadrightarrow} \mathrm{G}.$$

Posons $\mathrm{K} = p(\mathbf{Z}^{r-1} \times \{0\})$ (engendré donc par $r-1$ éléments) et soit $f : \mathrm{G} \to \mathrm{G/K}$ la surjection. La composée $f \circ p : \mathbf{Z}^n \twoheadrightarrow \mathrm{G/K}$ se factorise en

$$\mathbf{Z}^r \twoheadrightarrow \mathbf{Z}^r/(\mathbf{Z}^{r-1} \times \{0\}) \overset{\widehat{f \circ p}}{\twoheadrightarrow} \mathrm{G/K}.$$

Comme $\mathbf{Z}^r/(\mathbf{Z}^{r-1} \times \{0\})$ est isomorphe à $\mathbf{Z}$, le groupe G/K est isomorphe à un $\mathbf{Z}/d\mathbf{Z}$ (cor. 1.20).

Si H est un sous-groupe de G, le noyau $\mathrm{H} \cap \mathrm{K}$ de $\mathrm{H} \hookrightarrow \mathrm{G} \to \mathrm{G/K}$ est de type fini par l'hypothèse de récurrence, tandis que l'image, sous-groupe de $\mathbf{Z}/d\mathbf{Z}$, est aussi engendrée par un élément (ex. 1.18). Cette image est isomorphe à $\mathrm{H}/\mathrm{H} \cap \mathrm{K}$, qui est donc de type fini. On peut ainsi appliquer la prop. 1.23.2° pour en déduire que H est de type fini. □

3.3. Groupes abéliens libres de type fini. — Un groupe abélien est *libre de type fini* s'il est isomorphe à un produit $\mathbf{Z}^r$ [9]. Cela signifie qu'il existe $r \in \mathbf{N}$ et des éléments $x_1, \dots, x_r$ de G

8. On a vu dans l'exerc. 1.11 que ce n'est en général plus vrai pour un groupe G non abélien.

9. Un groupe est *abélien libre* s'il est isomorphe à une somme directe

$$\mathbf{Z}^{(\mathrm{I})} := \{(z_i)_{i \in \mathrm{I}} \in \mathbf{Z}^{\mathrm{I}} \mid \exists \mathrm{J} \text{ fini } \subseteq \mathrm{I} \ \ \forall i \in \mathrm{I}\text{–}\mathrm{J} \quad z_i = 0\},$$

pour un certain ensemble I. Il est alors de type fini si et seulement si l'ensemble I est fini (pourquoi ?).

Attention à la confusion avec la notion (plus compliquée) de « groupe libre », qui ne sera pas vue dans ce cours. Les seuls groupes libres qui sont abéliens sont $\{e\}$ et $\mathbf{Z}$.

tels que le morphisme (8) soit un isomorphisme. Une telle famille $(x_1,\dots,x_r)$ est appelée une base de G. Plus généralement, on dira qu'une famille $(x_1,\dots,x_r)$ d'éléments de G est linéairement indépendante si le morphisme (8) est injectif.

Tout notre traitement dans cette section repose sur le lemme fondamental suivant, donnant la classification des matrices équivalentes à coefficients entiers.

Lemme 3.3. — *Soit* A *une matrice $m\times n$ à coefficients dans* $\mathbf{Z}$. *Il existe des matrices* $\mathrm{P}\in\mathrm{GL}(m,\mathbf{Z})$ *et* $\mathrm{Q}\in\mathrm{GL}_n(\mathbf{Z})$ *telles que*

$$\mathrm{PAQ}=\begin{pmatrix} d_1 & & & & & & \\ & \ddots & & & & & \\ & & d_s & & & & \\ & & & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & \cdots\ 0 \end{pmatrix}, \tag{9}$$

où $d_1,\cdots,d_s$ sont des entiers positifs satisfaisant $d_1\mid\cdots\mid d_s$, appelés facteurs invariants *de la matrice* A. *Ils sont entièrement déterminés par* A.

Le groupe $\mathrm{GL}_n(\mathbf{Z})$ a été défini dans l'ex. 1.1.6°. Il est composé des matrices carrées d'ordre n à coefficients dans $\mathbf{Z}$ inversibles dont l'inverse est aussi à coefficients dans $\mathbf{Z}$. C'est équivalent à dire que le déterminant vaut ±1.

Le lemme montre qu'une matrice à coefficients entiers est déterminée, à équivalence près, non seulement par son rang s (le seul invariant pour les matrices à coefficients dans un corps), mais aussi par ses facteurs invariants $d_1,\dots,d_s$.

Admettons pour le moment le lemme 3.3. On en déduit assez rapidement tous les théorèmes importants de la théorie.

Théorème 3.4. — *Toutes les bases d'un groupe abélien libre de type fini* G *ont le même nombre d'éléments, appelé le* rang *de* G.

Démonstration. — Il suffit de montrer que si un groupe abélien libre G a une base $(x_1,\dots,x_r)$, toute famille linéairement indépendante d'éléments de G a au plus r éléments. Soit donc une famille $(y_1,\dots,y_n)$ d'éléments de G : puisque $(x_1,\dots,x_r)$ est une base, on obtient une matrice $\mathrm{A}=(a_{ij})$ de taille $r\times n$ à coefficients entiers définie par

$$y_j=\sum_{i=1}^{r}a_{ij}x_i.$$

On peut interpréter A comme la matrice du morphisme $\mathbf{Z}^n\to\mathrm{G}$ qui envoie ε_j sur y_j, où $(\varepsilon_1,\dots,\varepsilon_n)$ est la base standard de $\mathbf{Z}^n$. Appliquant le lemme 3.3, on déduit qu'existent des matrices inversibles P et Q telles que PAQ ait la forme (9). Si $n>r$, on a $\mathrm{PAQ}\varepsilon_n=0$, donc $\mathrm{AQ}\varepsilon_n=0$, d'où une relation entre les $y_j=\mathrm{A}\varepsilon_j$ donnée par la dernière colonne de Q. Donc pour que la famille $(y_1,\dots,y_n)$ soit linéairement indépendante, il faut $n\leqslant r$. □

***Théorème 3.5* (de la base adaptée)**. — *Un sous-groupe* H *d'un groupe abélien* G *libre de rang fini s est libre de rang $s\leqslant r$. En outre, il existe une base $(e_1,\dots,e_r)$ de* G *et des entiers positifs $d_1,\dots,d_s$ tels que*

– $(d_1e_1,\dots,d_se_s)$ *est une base de* H ;
– *on a les divisibilités* $d_1 \mid \cdots \mid d_s$.

Démonstration. — On prend une base $(x_1,\dots,x_r)$ de G (qui induit un isomorphisme $\phi : \mathbf{Z}^r \xrightarrow{\sim} \mathrm{G}$) et des générateurs $(y_1,\dots,y_n)$ de $\mathrm{H} \leq \mathrm{G}$ (prop. 3.2). Chaque y_j se décompose sur la base en $y_j = \sum_{i=1}^{r} a_{ij}x_i$, où la matrice $\mathrm{A} = (a_{ij})$ est de taille $r \times n$.

Si $(\varepsilon_1,\dots,\varepsilon_n)$ est la base standard de $\mathbf{Z}^n$, le morphisme $f : \mathbf{Z}^n \xrightarrow{\mathrm{A}} \mathbf{Z}^r \xrightarrow{\phi}{\sim} \mathrm{G}$, d'image H, envoie ε_j sur y_j.

Appliquons le lemme 3.3 à la matrice A et considérons la factorisation

$$\mathbf{Z}^n \xrightarrow{\mathrm{Q}}{\sim} \mathbf{Z}^n \xrightarrow{\mathrm{A}} \mathbf{Z}^r \xrightarrow{\mathrm{P}}{\sim} \mathbf{Z}^r \xrightarrow{\mathrm{P}^{-1}}{\sim} \mathbf{Z}^r \xrightarrow{\phi}{\sim} \mathrm{G}$$

de $f \circ \mathrm{Q}$. L'isomorphisme $\phi \circ \mathrm{P}^{-1} : \mathbf{Z}^r \xrightarrow{\sim} \mathrm{G}$ correspond à une nouvelle base $(e_1,\dots,e_r)$ de G et $\mathrm{H} = \mathrm{im}(f \circ \mathrm{Q})$ est alors engendré par $(d_1e_1,\dots,d_se_s)$. Comme ces éléments forment une famille linéairement indépendante, c'est une base de H. Le théorème est donc démontré. □

3.4. Structure des groupes abéliens de type fini. — On déduit du th. 3.5 le théorème de structure suivant.

Théorème 3.6. — *Soit* G *un groupe abélien de type fini. Il existe des entiers* r *et* s*, et des entiers naturels* $1 < d_1 \mid \cdots \mid d_s$*, tous uniquement déterminés par* G*, tels que*

$$\mathrm{G} \simeq \mathbf{Z}^r \times \left(\prod_1^s \mathbf{Z}/d_i\mathbf{Z} \right).$$

Bien entendu, le groupe G est fini si et seulement si $r = 0$; il est abélien libre si et seulement si $s = 0$.

Par le lemme chinois (prop. 3.1), le second morceau du produit s'écrit aussi

$$\prod_{j \in \mathrm{J}} \mathbf{Z}/p_j^{\alpha_j}\mathbf{Z}, \tag{10}$$

où les p_j sont des nombres premiers, éventuellement répétés. Réciproquement, on récupère, de manière unique, les facteurs invariants d_i à partir de la collection des $p_j^{\alpha_j}$: le plus grand facteur d_s est le ppcm des $p_j^{\alpha_j}$, et il s'écrit $d_s = \prod_{j' \in \mathrm{J}'} p_{j'}^{\alpha_{j'}}$. On obtient alors d_{s-1} comme le ppcm des $p_j^{\alpha_j}$ pour $j \in \mathrm{J}-\mathrm{J}'$, etc.

Autrement dit, on écrit tous les $p_j^{\alpha_j}$ dans un tableau avec une ligne pour chaque nombre premier, en ordre croissant dans chaque ligne, et en alignant chaque ligne sur la dernière colonne. On obtient les facteurs invariants en prenant les produits par colonne.

Exemple 3.7. — Pour le groupe $(\mathbf{Z}/2\mathbf{Z})^2 \times (\mathbf{Z}/2^2\mathbf{Z}) \times (\mathbf{Z}/2^3\mathbf{Z}) \times (\mathbf{Z}/3\mathbf{Z})^3 \times (\mathbf{Z}/5\mathbf{Z}) \times (\mathbf{Z}/5^2\mathbf{Z})$, on obtient le tableau

$$\begin{array}{cccc} 2 & 2 & 2^2 & 2^3 \\ & 3 & 3 & 3 \\ & & 5 & 5^2 \end{array}$$

Les facteurs invariants sont donc 2, 6, 60, 600.

Démonstration du théorème. — Puisque G est de type fini, on dispose d'un morphisme surjectif

$$\mathbf{Z}^n \xrightarrow{f} \!\!\!\!\rightarrow \mathrm{G}.$$

On applique le th. 3.5 à $\mathrm{H} = \ker(f)$: il existe donc une base $(e_1, \dots, e_n)$ de $\mathbf{Z}^n$ telle que $(d_1 e_1, \dots, d_s e_s)$ soit une base de H, avec $d_1 \mid \cdots \mid d_s$. Cela identifie H au sous-groupe

$$d_1\mathbf{Z} \times \cdots \times d_s\mathbf{Z} \subseteq \mathbf{Z}^n.$$

D'où $\mathrm{G} \simeq \mathbf{Z}^n/\mathrm{H} \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z} \times \mathbf{Z}^{n-s}$. On retire ensuite ceux des d_i qui sont égaux à 1 pour obtenir l'existence de la décomposition du théorème.

Reste à montrer l'unicité de r, s et des d_i. Le sous-groupe

$$\mathrm{T}(\mathrm{G}) = \{x \in \mathrm{G} \mid \exists m \in \mathbf{N}^* \quad mx = 0\}$$

des *éléments de torsion de* G est nécessairement le facteur $\prod_i \mathbf{Z}/d_i\mathbf{Z}$, donc $\mathrm{G}/\mathrm{T}(\mathrm{G}) \simeq \mathbf{Z}^r$ est un groupe abélien libre, dont le rang r est ainsi bien déterminé. Il reste donc à montrer que, pour le groupe fini T(G), les d_i sont uniquement déterminés, ou, ce qui est équivalent, les facteurs $p_j^{\alpha_j}$ figurant dans (10).

En se limitant au sous-groupe des éléments dont l'ordre est une puissance de p (c'est le sous-groupe $\mathrm{T}_p(\mathrm{G})$ de p-torsion défini en (7)), on est ramené à montrer que dans l'écriture

$$\mathrm{T}_p(\mathrm{G}) = \mathbf{Z}/p^{\alpha_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{\alpha_s}\mathbf{Z}, \quad \alpha_1 \leqslant \cdots \leqslant \alpha_s,$$

les α_j sont complètement déterminés par G.

Considérons, pour chaque entier $i > 0$, le sous-groupe $\mathrm{T}_{p,i} = \{x \in \mathrm{G} \mid p^i x = 0\}$ de $\mathrm{T}_p(\mathrm{G})$. On a $|\mathrm{T}_{p,i}| = \prod_{\alpha_j \leqslant i} p^{\alpha_j} \prod_{\alpha_j > i} p^j$ et en particulier $|\mathrm{T}_{p,i+1}/\mathrm{T}_{p,i}| = p^{\mathrm{card}\{j \mid \alpha_j > i\}}$. On récupère ainsi les exposants α_j à partir des sous-groupes $\mathrm{T}_{p,i}$, complètement déterminés par G. □

Exercice 3.8. — Pour tout groupe G abélien de type fini, on note $r(\mathrm{G})$ l'entier r qui apparaît dans l'énoncé du th. 3.6.
a) Montrer que $r(\mathrm{G})$ est le plus grand entier n tel que G contienne un sous-groupe isomorphe à $\mathbf{Z}^n$.
b) Montrer que $r(\mathrm{G})$ est le plus grand entier n tel que G ait un quotient isomorphe à $\mathbf{Z}^n$.
c) Soit H un sous-groupe de G. Montrer $r(\mathrm{G}) = r(\mathrm{H}) + r(\mathrm{G}/\mathrm{H})$.

Exercice 3.9. — a) Soient G_1 et G_2 des groupes abéliens finis. On suppose que pour chaque entier $m > 0$, le nombre d'éléments de G_1 d'ordre m est égal au nombre d'éléments de G_2 d'ordre m. Montrer que G_1 et G_2 sont isomorphes.
b) Montrer que la conclusion de a) ne subsiste pas si on suppose plus l'un des groupes finis G_1 et G_2 abélien (*Indication :* pour p premier impair, on pourra considérer le groupe $\mathrm{T}_3(\mathbf{F}_p)$ défini dans l'ex. I.2.19).

Exercice 3.10. — Soit G un groupe abélien de type fini et soit $f : \mathrm{G} \to \mathrm{G}$ un morphisme surjectif. Le but de cet exercice est de démontrer que f est un isomorphisme. Soit $\mathrm{T}(\mathrm{G}) \leq \mathrm{G}$ le sous-groupe de torsion de G.
a) Montrer que f induit un morphisme surjectif $\hat{f} : \mathrm{G}/\mathrm{T}(\mathrm{G}) \to \mathrm{G}/\mathrm{T}(\mathrm{G})$.
b) Montrer que $\hat{f}$ est un isomorphisme.
c) En déduire que f est un isomorphisme.

3.5. Démonstration du lemme 3.3. — Commençons par l'unicité des entiers d_i [10]. On remarque que d_1 est le pgcd (positif) de tous les coefficients de A ; en effet, le pgcd des coefficients de A divise tous les coefficients de PAQ et inversement, le pgcd des coefficients de PAQ divise tous les coefficients de $\mathrm{A} = \mathrm{P}^{-1}(\mathrm{PAQ})\mathrm{Q}^{-1}$.

Étendons cette observation de la manière suivante. Notons

$$m_k(\mathrm{A}) = \text{pgcd des mineurs d'ordre } k \text{ de A.}$$

Pour $k = 1$, on retrouve le pgcd des coefficients de A. Le point crucial est l'invariance par équivalence :

$$\forall \mathrm{P} \in \mathrm{GL}(m, \mathbf{Z}) \quad \forall \mathrm{Q} \in \mathrm{GL}_n(\mathbf{Z}) \qquad m_k(\mathrm{PAQ}) = m_k(\mathrm{A}). \tag{11}$$

Il en résulte $m_k(\mathrm{A}) = d_1 \cdots d_k$, et donc les d_i sont entièrement déterminés par A.

Pour prouver (11), il suffit de montrer que, pour toute matrice P à coefficients entiers,

$$m_k(\mathrm{A}) \mid m_k(\mathrm{PA}). \tag{12}$$

En effet, si P est inversible, cela implique $m_k(\mathrm{A}) \mid m_k(\mathrm{PA}) \mid m_k(\mathrm{P}^{-1}\mathrm{PA}) = m_k(\mathrm{A})$, donc $m_k(\mathrm{PA}) = m_k(\mathrm{A})$. Par passage à la transposée, cela fournit aussi $m_k(\mathrm{AQ}) = m_k(\mathrm{A})$ et donc (11).

Finalement, on montre directement (12) en exprimant les mineurs de PA comme combinaisons linéaires à coefficients entiers des mineurs de A : les détails sont laissés au lecteur.

Passons à présent à l'existence de P et Q. Comme pour la classification à équivalence près des matrices à coefficients dans un corps, on effectue des opérations élémentaires, qui peuvent s'interpréter comme la multiplication à droite ou à gauche par certaines matrices, dont des matrices carrées dites *élémentaires* qui ne diffèrent de la matrice identité que par un seul coefficient, situé hors de la diagonale. La différence avec le cas d'un corps est qu'on ne peut pas diviser.

Plus précisément, notons E_{ij} la matrice dont tous les coefficients sont nuls, sauf celui situé à la i-ème ligne et la j-ème colonne, qui vaut 1.

Les opérations qu'on s'autorise sont les suivantes :

- la multiplication à gauche par la matrice $\mathrm{Id} + a\mathrm{E}_{ij}$, qui permet d'ajouter à la i-ème ligne la j-ème ligne, multipliée par un entier a ;
- la multiplication à droite par la matrice $\mathrm{Id} + a\mathrm{E}_{ij}$, qui permet d'ajouter à la j-ème colonne la i-ème colonne, multipliée par un entier a.

Remarquons tout de suite que grâce à ces opérations, on peut échanger deux lignes ou deux colonnes, quitte à changer le signe d'une d'elles, en procédant ainsi :

$$\begin{pmatrix} \mathrm{L}_i \\ \mathrm{L}_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} \mathrm{L}_i \\ \mathrm{L}_i + \mathrm{L}_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} -\mathrm{L}_j \\ \mathrm{L}_i + \mathrm{L}_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} -\mathrm{L}_j \\ \mathrm{L}_i \end{pmatrix}. \tag{13}$$

---

10. On peut aussi déduire l'unicité des d_i de l'énoncé d'unicité du th. 3.6 (obtenu indépendamment du lemme !) en procédant de la façon suivante : soit H_A le sous-groupe de $\mathbf{Z}^m$ engendré par les colonnes de A. Multiplier à gauche par P revient à appliquer un automorphisme de $\mathbf{Z}^m$, tandis que multiplier à droite par Q ne change pas H. Les groupes (abéliens de type fini) $\mathbf{Z}^m/\mathrm{H}_\mathrm{A}$ et $\mathbf{Z}^m/\mathrm{H}_{\mathrm{PAQ}}$ sont donc isomorphes. Or ce dernier est $\mathbf{Z}^{m-s} \times \left(\prod_1^s \mathbf{Z}/d_i\mathbf{Z}\right)$. Par le th. 3.6, les d_i sont donc uniquement déterminés par $\mathbf{Z}^m/\mathrm{H}_\mathrm{A}$, donc par A.

L'argument présenté dans le texte a l'avantage d'expliquer comment obtenir concrètement les d_i à partir des coefficients de A.

Nous allons montrer que partant de A, à l'aide de ces seules opérations élémentaires, on peut arriver à une matrice du type voulu, sauf que d_s ne sera pas nécessairement positif. La preuve utilise une récurrence sur la taille de la matrice.

Soit λ_1 le pgcd (positif) des coefficients de la première colonne. On va appliquer des opérations élémentaires sur les lignes pour obtenir une première colonne dont tous les coefficients sont nuls, sauf le coefficient a_{11} qui sera égal à $\pm\lambda_1$. Faisons-le sur les deux premiers coefficients a_{11} et a_{21}. Quitte à échanger les deux premières lignes, on peut supposer $|a_{11}| \geqslant |a_{21}|$. Si $a_{21} = 0$, il n'y a rien à faire ; sinon, effectuons la division euclidienne $a_{11} = ba_{21} + c$ avec $0 \leqslant c < |a_{21}|$; en effectuant la transformation élémentaire dans laquelle la seconde ligne, multipliée par b, est soustraite de la première, les coefficients (a_{11}, a_{21}) sont transformés en (c, a_{21}), avec $|a_{21}|+|c| < |a_{11}|+|a_{21}|$. En itérant, l'algorithme d'Euclide nous indique qu'on finit par arriver au couple $(\mathrm{pgcd}(a_{11}, a_{21}), 0)$. Il est clair qu'en répétant ce procédé sur chaque ligne, on arrive à la première colonne souhaitée,

$$\begin{pmatrix} \pm\lambda_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

La même méthode peut alors être appliquée à la première ligne, en utilisant des opérations élémentaires sur les colonnes, pour obtenir une matrice dont la première ligne a la forme $(\pm\lambda_2 0 \cdots 0)$, où λ_2 est le pgcd des coefficients de la première ligne. Malheureusement, on a ainsi modifié la première colonne, donc ses coefficients ne sont peut-être plus nuls. Néanmoins, on a gagné quelque chose : $0 \leqslant \lambda_2 \leqslant \lambda_1$, puisque c'est le pgcd de λ_1 et des autres coefficients. On itère alors la construction, en mettant alternativement des 0 sur la première colonne et la première ligne : les coefficients à la place (1,1), positifs, décroissent : $\lambda_1 \geqslant \lambda_2 \geqslant \lambda_3 \geqslant \cdots \geqslant 0$. Cette suite se stabilise donc : à un moment donné, on obtient par exemple une première ligne $(\delta_1 0 \cdots 0)$ où δ_1 est aussi un pgcd des coefficients de la première colonne, donc divise tous ces coefficients. Il suffit alors de retrancher à chaque ligne un multiple adéquat de la première pour arriver à une matrice de la forme

$$\begin{pmatrix} \delta_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \mathrm{B} & \\ 0 & & & \end{pmatrix}.$$

On applique l'hypothèse de récurrence sur B pour parvenir à une matrice

$$\begin{pmatrix} \delta_1 & & & & & & \\ & \delta_2 & & & & & \\ & & \ddots & & & & \\ & & & \delta_s & & & \\ & & & & 0 & & \\ & & & & & \ddots & \end{pmatrix}, \quad \text{où} \quad \delta_2 \mid \cdots \mid \delta_s.$$

Dans la construction, il n'y a pas de raison a priori que $\delta_1 \mid \delta_2$. Mais on peut remplacer le couple (δ_1, δ_2) par (d_1, m_2), où d_1 et m_2 sont des pgcd et ppcm de δ_1 et δ_2 : en effet, par l'application d'une transformation élémentaire, puis du procédé précédent, on obtient successivement (en n'écrivant que les deux premières lignes et colonnes, sur lesquelles les opérations ont lieu)

$$\begin{pmatrix} \delta_1 & 0 \\ 0 & \delta_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} \delta_1 & 0 \\ \delta_2 & \delta_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_1 & d_1' \\ 0 & m_2' \end{pmatrix},$$

où on a en fait $m_2' = m_2$, puisque le déterminant de la matrice reste inchangé : $d_1 m_2 = \delta_1 \delta_2 = d_1 m_2'$. De plus, le pgcd des coefficients, à savoir d_1, reste aussi inchangé, donc $d_1 \mid d_1'$. Une dernière opération élémentaire nous permet d'arriver à la forme voulue $\begin{pmatrix} d_1 & 0 \\ 0 & m_2 \end{pmatrix}$.

Appliquant le même procédé au couple (m_2, δ_3), on peut le remplacer par le couple $(\mathrm{pgcd}(m_2, \delta_3), \mathrm{ppcm}(m_2, \delta_3))$. Puisque $d_1 = \mathrm{pgcd}(\delta_1, \delta_2)$ et $\delta_2 \mid \delta_3$, d_1 divise $d_2 := \mathrm{pgcd}(m_2, \delta_3)$. En itérant le procédé, on remplace les coefficients $(\delta_1, \dots, \delta_r)$ par $(d_1, \dots, d_r)$ avec $d_1 \mid \cdots \mid d_r$.

Il reste à régler la question des signes : si on se restreint toujours à nos opérations élémentaires, on peut changer les signes deux par deux en faisant deux fois les opérations décrites en (13) :

$$\begin{pmatrix} \mathrm{L}_i \\ \mathrm{L}_j \end{pmatrix} \rightsquigarrow \begin{pmatrix} -\mathrm{L}_j \\ \mathrm{L}_i \end{pmatrix} \rightsquigarrow \begin{pmatrix} -\mathrm{L}_i \\ -\mathrm{L}_j \end{pmatrix}.$$

Cela termine la récurrence : seul d_s peut encore être négatif (et uniquement dans le cas $m = n = s$). Pour montrer le lemme, il suffit ensuite, si $d_s < 0$, de multiplier à droite par $\mathrm{I}_n - 2\mathrm{E}_{ss}$ (et c'est la seule fois qu'on multiplie par une matrice de déterminant -1 !). □

Exemple 3.11 **(Théorème de Mordell)**. — Une courbe elliptique sur $\mathbf{Q}$ est l'ensemble E des solutions $(x, y) \in \mathbf{Q}^2$ d'une équation du type

$$y^2 = x^3 + ax + b,$$

avec $(a, b) \in \mathbf{Q}^2$ et $4a^3 + 27b^2 \neq 0$, auquel on adjoint un point O [11]. On peut mettre une structure de groupe abélien sur E, d'élément neutre O, définie par

$$\mathrm{P} + \mathrm{Q} + \mathrm{R} = \mathrm{O} \iff \text{les points P, Q, R sont alignés.}$$

Il est non trivial de montrer que cela définit bien une loi de groupe. Le théorème de Mordell (1922) dit que $(\mathrm{E}, +)$ *est un groupe abélien de type fini* (la preuve est longue, mais elle peut être expliquée à des élèves de première année).

Un théorème de Mazur (1977) décrit tous les groupes de torsion $\mathrm{T}(\mathrm{E})$ qu'on peut obtenir : ce sont les $\mathbf{Z}/d\mathbf{Z}$, pour $d \in \{0, 1, \dots, 10, 12\}$ et les $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/d\mathbf{Z}$, pour $d \in \{2, 4, 6, 8\}$. Les rangs possibles du groupe abélien libre $\mathrm{E}/\mathrm{T}(\mathrm{E})$ sont beaucoup plus mystérieux : le plus grand rang calculé explicitement est 28 (Elkies, 2006) ; on conjecture, mais on ne sait pas

11. Le bon point de vue est de regarder les points de la courbe dans le plan projectif (*cf.* p. 55), donnés par l'équation homogène $y^2 z = x^3 + axz^2 + bz^3$; le point O est alors le point à l'infini $(0 : 1 : 0)$.

démontrer, que des rangs arbitrairement grands devraient être possibles. Voici la courbe d'Elkies (l'équation est présentée sous une forme légèrement différente) :

$$\begin{aligned} y^2+xy+y &= x^3-x^2 \\ &\quad -2006776241557552658503320820933854275093023031217895650 2x \\ &\quad +3448161179503055646703298569039072037485594435931918036126 \\ &\quad 60082962919394487322434 29. \end{aligned}$$

Pour la courbe plus simple d'équation $y^2 = x^3 - x$, on a $\mathrm{E} = \{\mathrm{O}, (0,0), (1,0), (-1,0)\}$ et $(\mathrm{E}, +) \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

4. Le groupe $\mathrm{GL}_n(\mathbf{Z})$

Notre démonstration du lemme 3.3 permet d'obtenir des générateurs pour les groupes $\mathrm{GL}_n(\mathbf{Z})$ et $\mathrm{SL}_n(\mathbf{Z})$. Expliquons pourquoi.

Partons d'une matrice $\mathrm{A} \in \mathrm{GL}_n(\mathbf{Z})$. Il est clair que ses facteurs invariants sont tous égaux à 1, c'est-à-dire que la réduction finale de A est la matrice I_n. On a donc écrit $\mathrm{A} = \mathrm{PQ}$, où la matrice P (resp. Q) est produit de matrices correspondant aux opérations réalisées sur les lignes (resp. colonnes). Si on relit la preuve du lemme 3.3, on voit que ces opérations sont de deux types :

- la multiplication à gauche (ou à droite) par la matrice élémentaire $\mathrm{I}_n + a\mathrm{E}_{ij}$, qui n'est autre que $(\mathrm{I}_n + \mathrm{E}_{ij})^a$;
- la multiplication par $\mathrm{I}_n - 2\mathrm{E}_{nn}$.

Les premières opérations ne changent pas le déterminant. La deuxième opération n'est nécessaire que si on est arrivé par l'algorithme de la preuve à la matrice $\mathrm{I}_n - 2\mathrm{E}_{nn}$, c'est-à-dire dans le cas $\det(\mathrm{A}) = -1$.

On en déduit le résultat suivant.

Théorème 4.1. — *1° Le groupe* $\mathrm{SL}_n(\mathbf{Z})$ *est de type fini : il est engendré par les matrices élémentaires* $\mathrm{I}_n + \mathrm{E}_{ij}$, *pour* $i, j \in \{1, \dots, n\}$, $i \neq j$.

2° Le groupe $\mathrm{GL}_n(\mathbf{Z})$ *est de type fini : il est engendré par les matrices précédentes et la matrice* $\mathrm{I}_n - 2\mathrm{E}_{nn}$.

En particulier, le groupe $\mathrm{SL}_2(\mathbf{Z})$ est engendré par les deux matrices

$$\mathrm{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \mathrm{U} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

(et il ne peut pas être engendré par une seule matrice, puisqu'il n'est pas abélien). Le groupe $\mathrm{GL}_n(\mathbf{Z})$ peut aussi être engendré par seulement trois éléments (*cf.* exerc. 4.3).

Exercice 4.2. — a) Montrer que le groupe $\mathrm{SL}_2(\mathbf{Z})$ est engendré par les deux matrices

$$\mathrm{S} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \mathrm{T}^{-1}\mathrm{UT} \qquad \mathrm{R} := \mathrm{ST} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

b) Montrer que les matrices S et R sont d'ordre fini.

c) Montrer que l'image de tout morphisme $\mathrm{SL}_2(\mathbf{Z}) \to \mathbf{C}^\times$ est contenue dans le groupe $\boldsymbol{\mu}_{12}$ des racines $12^{\text{ème}}$ de l'unité [12].

Exercice 4.3. — Montrer que pour tout n, le groupe $\mathrm{GL}_n(\mathbf{Z})$ peut être engendré par trois éléments (*Indication :* on pourra montrer qu'il est engendré par la matrice $\mathrm{I}_n + \mathrm{E}_{12}$ et deux matrices de permutation bien choisies).

Exercice 4.4. — Pour tout $n \geqslant 2$, on pose

$$\mathrm{A} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & 1 & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

Montrer que pour $n \neq 4$, les matrices A et ${}^t\mathrm{A}$ engendrent le groupe $\mathrm{SL}_n(\mathbf{Z})$ (*Indication :* on pourra calculer $\mathrm{A}^{-1}\,{}^t\mathrm{A}\mathrm{A}\,{}^t\mathrm{A}^{-1}\mathrm{A}$) [13].

Exercice 4.5. — Soit R un anneau euclidien (par exemple $\mathbf{Z}$ si vous ne savez pas ce que c'est). Pour tout $\mathrm{A} \in \mathrm{GL}_n(\mathrm{R})$, montrer qu'il existe une matrice $\mathrm{P} \in \mathrm{GL}_n(\mathrm{R})$ produit de matrices élémentaires $\mathrm{I}_n + \mathrm{E}_{ij}$ (avec $i \neq j$) telle que

$$\mathrm{PA} = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ 0 & \cdots & 0 & \text{dét}(\mathrm{A}) \end{pmatrix}.$$

Exercice 4.6. — a) Soit G un groupe de type fini et soit H un groupe fini. Montrer que l'ensemble des morphismes $\mathrm{G} \to \mathrm{H}$ est fini.
b) Soit G un groupe de type fini, soit $f : \mathrm{G} \to \mathrm{G}$ un morphisme surjectif, soit H un groupe fini et soit $g : \mathrm{G} \to \mathrm{H}$ un morphisme. Montrer $\ker(f) \subseteq \ker(g)$ (*Indication :* on pourra utiliser a) pour montrer qu'il existe $m > n > 0$ tels que $g \circ f^m = g \circ f^n$ puis, si $a \in \ker(f)$, introduire $b_n \in \mathrm{G}$ tel que $a = f^n(b_n)$).
c) Soit $f : \mathrm{SL}_n(\mathbf{Z}) \to \mathrm{SL}_n(\mathbf{Z})$ un morphisme surjectif. Montrer que f est un isomorphisme.

5. Groupes simples et suites de composition

5.1. Groupes simples. — Rappelons qu'un groupe G est simple s'il est non trivial et que ses seuls sous-groupes distingués sont $\{e\}$ et G. Un groupe simple est donc un groupe qui n'a pas de quotient non trivial : on ne peut pas espérer le comprendre à partir de groupes plus petits. Les groupes simples sont les blocs de base de la théorie des groupes.

12. Ce résultat est optimal : l'application $f : \mathrm{SL}_2(\mathbf{Z}) \to \boldsymbol{\mu}_{12}$ donnée par

$$f\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \exp\Big(i\pi\big((1-c^2)(bd+3(c-1)d+c+3)+c(a+d-3)\big)/6\Big)$$

est surjective, mais ce n'est pas évident de montrer que c'est un morphisme !

13. Pour $n = 4$, un calcul sur machine montre que le sous-groupe de $\mathrm{SL}_4(\mathbf{Z}/2\mathbf{Z})$ engendré par A et ${}^t\mathrm{A}$ est d'indice 8 dans $\mathrm{SL}_4(\mathbf{Z}/2\mathbf{Z})$ (il est en fait isomorphe à $\mathfrak{A}_8$) ; on peut en déduire que le sous-groupe de $\mathrm{SL}_4(\mathbf{Z})$ engendré par A et ${}^t\mathrm{A}$ est encore d'indice 8 dans $\mathrm{SL}_4(\mathbf{Z})$ (Gow, R., Tamburini, M. C., Generation of $\mathrm{SL}_n(\mathbf{Z})$ by a Jordan unipotent matrix and its transpose, *Linear Algebra Appl.* **181** (1993), 63–71).

Les groupe abéliens simples sont les $\mathbf{Z}/p\mathbf{Z}$, avec p premier. Le *théorème de Feit et Thompson* (1963) affirme que tout groupe fini simple non abélien est d'ordre pair (son ordre est même divisible par 4 grâce à l'exerc. 2.5).

Une série infinie de groupes simples non abéliens est donnée par les groupes alternés.

Théorème 5.1. — *Pour $n = 3$ ou $n \geqslant 5$, le groupe alterné $\mathfrak{A}_n$ est simple.*

La conclusion du théorème est fausse pour $n = 4$. En effet, le groupe $\mathfrak{A}_4$ contient le groupe de Klein des doubles transpositions :

$$K = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\},$$

qui est distingué, puisqu'une conjugaison doit envoyer une double transposition sur une double transposition.

Corollaire 5.2. — *Si $n \neq 4$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{e\}$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$.*

Démonstration. — Si $n = 2$, le corollaire est trivial. On suppose donc $n = 3$ ou $n \geqslant 5$.

Si $H \trianglelefteq \mathfrak{S}_n$, alors $H \cap \mathfrak{A}_n \trianglelefteq \mathfrak{A}_n$, donc $H \cap \mathfrak{A}_n = \mathfrak{A}_n$ ou $\{e\}$ par le th. 5.1.

Dans le premier cas, l'indice $[H : \mathfrak{A}_n]$ divise $[\mathfrak{S}_n : \mathfrak{A}_n] = 2$; s'il vaut 1, on a $H = \mathfrak{A}_n$, s'il vaut 2, on a $H = \mathfrak{S}_n$.

Dans le second cas ($H \cap \mathfrak{A}_n = \{e\}$), la composée $H \hookrightarrow \mathfrak{S}_n \to \mathfrak{S}_n/\mathfrak{A}_n \simeq \mathbf{Z}/2\mathbf{Z}$ est injective, donc soit H est trivial, soit il est de cardinal 2. Si $|H| = 2$, son élément non trivial σ est d'ordre 2, donc est un produit $(ab)(\cdot\cdot)\cdots$ de transpositions à supports disjoints. Comme $n \geqslant 3$, on peut choisir $c \notin \{a, b\}$; le produit $(ac)\sigma(ac)^{-1}$ envoie alors c sur b. Il est donc distinct de σ et de e mais est dans H, ce qui contredit $|H| = 2$. □

Démonstration du théorème. — Soit $H \neq \{e\}$ un sous-groupe distingué de $\mathfrak{A}_n$. On utilise le fait essentiel que si $\sigma \in \mathfrak{A}_n$ et $\tau \in H$, le conjugué $\sigma\tau\sigma^{-1}$ de τ est dans H. La méthode de preuve consiste alors, à partir d'un élément non trivial τ de H, à en fabriquer suffisamment pour assurer $H = \mathfrak{A}_n$. On suppose $n \geqslant 5$, le case $n = 3$ étant trivial.

Première étape : tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$, et toutes les doubles transpositions sont conjuguées dans $\mathfrak{A}_n$.

En effet, on sait que deux 3-cycles sont toujours conjugués dans $\mathfrak{S}_n$; écrivons alors par exemple $(123) = \sigma\tau\sigma^{-1}$, avec $\sigma \in \mathfrak{S}_n$ et τ un 3-cycle. On a alors aussi

$$(123) = (45)(123)(45)^{-1} = (45)\sigma\tau\sigma'^{-1}(45)^{-1} = \sigma'\tau\sigma'^{-1},$$

avec $\sigma' = (45)\sigma$, et l'un des deux éléments σ ou σ' est dans $\mathfrak{A}_n$. On déduit que si H contient un 3-cycle, il contient tous les 3-cycles, et donc est égal à $\mathfrak{A}_n$ (qui est engendré par les 3-cycles par l'ex. 1.12.2°).

Le même type de raisonnement s'applique aux doubles transpositions : si $(12)(34) = \sigma\nu\sigma^{-1}$, alors $(12)(34) = ((12)\sigma)\nu((12)\sigma)^{-1}$.

Seconde étape : si H contient une double transposition (donc toutes les doubles transpositions), ou un 5-cycle, il contient un 3-cycle.

En effet, comme $n \geqslant 5$, si a, b, c, d, e sont distincts, on a

$$(abc) = \underbrace{(ae)(cd)}_{\text{dans H}}\,\underbrace{(ad)(ce)}_{\text{dans H}}\,\underbrace{(ab)(de)}_{\text{dans H}},$$

$$(abd) = \underbrace{(abc)(abcde)(abc)^{-1}}_{\text{dans H}}\,\underbrace{(abcde)^{-1}}_{\text{dans H}}.$$

Dans les deux cas, on en déduit $\mathrm{H} = \mathfrak{A}_n$. Cela résout complètement le cas $n = 5$, puisque $\mathfrak{A}_5$ ne contient que l'identité, des doubles transpositions, des 3-cycles et des 5-cycles.

Troisième étape : on montre que si $\mathfrak{A}_{n-1}$ est simple, $\mathfrak{A}_n$ est simple. On commence par montrer que H contient toujours un élément non trivial envoyant 1 sur lui-même. Supposons $\sigma \in \mathrm{H}$, avec $\sigma(1) = i \neq 1$; on va corriger σ en un élément $\sigma' \in \mathrm{H}$ tel que $\sigma'(1) = 1$. Soit $j \notin \{1, i\}$ tel que $\sigma(j) \neq j$ (σ n'est pas la transposition $(1, i)$) et soient l, m distincts $\notin \{1, i, j, \sigma(j)\}$ (on a $n \geqslant 6$) ; alors l'élément

$$\sigma' = (jlm)\sigma^{-1}(jlm)^{-1}\sigma$$

de H vérifie $\sigma'(1) = 1$ et $\sigma'(j) = l \neq j$. Donc $\sigma' \neq e$ et $\sigma' \in \mathrm{G}_1 \cap \mathrm{H}$, où

$$\mathrm{G}_1 = \{\sigma \in \mathfrak{A}_n \mid \sigma(1) = 1\} \simeq \mathfrak{A}_{n-1}.$$

Ainsi $\mathrm{H} \cap \mathrm{G}_1 \neq \{e\}$. Or $\mathrm{H} \cap \mathrm{G}_1 \trianglelefteq \mathrm{G}_1$ donc, par l'hypothèse de récurrence, $\mathrm{H} \cap \mathrm{G}_1 = \mathrm{G}_1$ et H contient donc un 3-cycle. Donc $\mathrm{H} = \mathfrak{A}_n$. □

5.2. Théorème de Jordan-Hölder. — La notion de suite de composition exprime l'idée de « casser en morceaux simples » un groupe : une *suite de composition* d'un groupe G est une suite finie

$$\mathrm{G} = \mathrm{G}_0 \rhd \mathrm{G}_1 \rhd \cdots \rhd \mathrm{G}_r = \{e\} \tag{14}$$

de sous-groupes emboîtés où chaque groupe quotient $\mathrm{G}_i/\mathrm{G}_{i+1}$ est simple.

Exemples 5.3. — 1° Le groupe $\mathbf{Z}/6\mathbf{Z}$ admet la suite de composition

$$\mathbf{Z}/6\mathbf{Z} \rhd \mathbf{Z}/3\mathbf{Z} \rhd \{0\},$$

avec quotients successifs $\mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/3\mathbf{Z}$, aini que la suite

$$\mathbf{Z}/6\mathbf{Z} \rhd \mathbf{Z}/2\mathbf{Z} \rhd \{0\},$$

avec quotients successifs $\mathbf{Z}/3\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z}$.

2° Soit $n = \prod p_i^{\alpha_i}$ une décomposition en produit de facteurs premiers d'un entier positif non nul. Il résulte du lemme chinois (prop. 3.1) que le groupe $\mathbf{Z}/n\mathbf{Z}$ admet une suite de composition dont les quotients successifs sont les $\mathbf{Z}/p_i\mathbf{Z}$, chacun répété α_i fois.

Plus généralement, il résulte du th. 3.6 que tout groupe abélien fini d'ordre n admet une suite de composition dont les quotients successifs sont les $\mathbf{Z}/p_i\mathbf{Z}$, chacun répété α_i fois.

3° Le groupe symétrique $\mathfrak{S}_4$ admet la suite de composition

$$\mathfrak{S}_4 \rhd \mathfrak{A}_4 \rhd \mathrm{K} \rhd \mathbf{Z}/2\mathbf{Z} \rhd \{e\},$$

avec quotients successifs $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}$ et $\mathbf{Z}/2\mathbf{Z}$.

4° Pour $n = 3$ ou $n \geqslant 5$, une suite de composition pour $\mathfrak{S}_n$ est donnée par

$$\mathfrak{S}_n \rhd \mathfrak{A}_n \rhd \{e\},$$

avec quotients successifs $\mathbf{Z}/2\mathbf{Z}$ et $\mathfrak{A}_n$.

5° Le groupe $\mathbf{Z}$ n'a pas de suite de composition : en effet, tout sous-groupe de $\mathbf{Z}$ est du type $m\mathbf{Z}$, et m est premier si on veut que le quotient $\mathbf{Z}/m\mathbf{Z}$ soit simple. Il reste donc isomorphe à $\mathbf{Z}$ et on ne peut pas atteindre $\{0\}$ en un nombre fini de pas.

Une suite de composition $G = G'_0 \rhd G'_1 \rhd \cdots \rhd G'_s = \{e\}$ est dite *équivalente* à la suite (14) si $r = s$ et qu'il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que $G_{\sigma(i)}/G_{\sigma(i)+1} \simeq G'_i/G'_{i+1}$.

Le théorème suivant indique l'existence et l'unicité des suites de composition pour les groupes finis : il dit ainsi qu'en un certain sens tous les groupes finis sont construits à partir de ces blocs de base. La classification des groupes finis simples est un énorme travail, achevé dans les années 80, donc ces blocs de base sont connus, mais cela n'entraîne pas du tout qu'on connaisse tous les groupes finis en général !

***Théorème 5.4* (Jordan-Hölder).** — *Tout groupe fini admet une suite de composition. Deux telles suites sont équivalentes.*

Le théorème ne dit pas que les termes d'une suite de composition d'un groupe fini G ne dépendent que du groupe G (*cf.* ex. 5.3.1°) ; seuls les quotients successifs ont cette propriété. Ces quotients simples (comptés avec les répétitions éventuelles) sont appelés les *facteurs simples* de G.

Attention : ils ne caractérisent pas le groupe G à isomorphisme près : les groupes $\mathfrak{S}_4$, $(\mathbf{Z}/2\mathbf{Z})^3 \times \mathbf{Z}/3\mathbf{Z}$ et $\mathbf{Z}/24\mathbf{Z}$ ont les mêmes facteurs simples (*cf.* ex. 5.3) mais ne sont pas isomorphes deux à deux.

Remarquons que l'unicité (à équivalence près) de la suite de composition pour $\mathbf{Z}/n\mathbf{Z}$ entraîne, grâce à l'ex. 5.3.2°, celle de la décomposition de l'entier non nul n en produit de facteurs premiers.

Démonstration. — L'existence d'une suite de composition est facile : si $G \neq \{e\}$, on définit G_1 comme un sous-groupe distingué maximal distinct de G. Alors le groupe non trivial G/G_1 est simple car un sous-groupe distingué de G/G_1 remonte en un sous-groupe distingué de G contenant G_1, qui ne saurait être que G_1 ou G ; dans le premier cas, le sous-groupe de G/G_1 est $\{e\}$, dans le second, G/G_1 entier. On recommence le raisonnement à partir de G_1 pour construire G_2. La construction s'arrête quelque part puisque les cardinaux des G_i décroissent strictement (le fait que G soit fini est bien sûr essentiel ici).

La démonstration de l'unicité va utiliser le lemme suivant.

Lemme 5.5. — *Soit* G *un groupe. Si* $H_1 \lhd G$ *et* $K_1 \lhd G$ *sont des sous-groupes distingués distincts tels que* G/H_1 *et* G/K_1 *sont simples, alors* $H_1 \cap K_1$ *est distingué dans* H_1 *et dans* K_1 *et*

$$G/H_1 \simeq K_1/(H_1 \cap K_1), \quad G/K_1 \simeq H_1/(H_1 \cap K_1).$$

Admettons le lemme pour le moment. On raisonne par récurrence, en supposant le résultat vrai pour les groupes dont une suite de composition a une longueur inférieure ou égale à $r-1$.

Soient $(H_1, \ldots, H_r)$ et $(K_1, \ldots, K_s)$, avec $r \leqslant s$, des suites de composition de G. Si $H_1 = K_1$, on applique à ce groupe l'hypothèse de récurrence, et on en déduit que les suites de composition $(H_2, \ldots, H_r)$ et $(K_2, \ldots, K_s)$ sont équivalentes, d'où la conclusion dans ce cas.

Supposons donc $H_1 \neq K_1$ et introduisons une suite de composition $(L_2, \dots, L_t)$ pour le groupe fini $H_1 \cap K_1$. On considère le diagramme

$$\begin{array}{ccccccccccc} & & H_1 & \rhd & H_2 & & \rhd & \cdots & \rhd & H_r = \{e\} & \\ & \lhd & & \lhd & & & & & & & \\ G & & & & L_2 = H_1 \cap K_1 & \rhd & & \cdots & \rhd & L_t = \{e\} & \\ & \lhd & & \lhd & & & & & & & \\ & & K_1 & \rhd & K_2 & & \rhd & & \cdots & \rhd & K_s = \{e\} \end{array}$$

Compte tenu du lemme, tous les quotients apparaissant dans ce diagramme sont simples. Par conséquent, nous avons deux suites de composition pour H_1, à savoir $(H_2, \dots, H_r)$ et $(L_2, \dots, L_t)$. Par l'hypothèse de récurrence, on a $r = t$ et, à permutation près, les quotients $(H_1/H_2, \dots, H_{r-1}/H_r)$ sont isomorphes aux quotients

$$\big(H_1/(H_1 \cap K_1) \simeq G/K_1, (H_1 \cap K_1)/L_3, \dots, L_{r-1}/L_r\big). \tag{15}$$

Puisqu'on dispose maintenant de la suite de composition (L_k) de K_1, de longueur $r-1$, on peut aussi appliquer l'hypothèse de récurrence à K_1 pour obtenir $s = r$, et que les $(K_1/K_2, \dots, K_{r-1}/K_r)$ sont isomorphes aux

$$\big(K_1/(H_1 \cap K_1) \simeq G/H_1, (H_1 \cap K_1)/L_3, \dots, L_{r-1}/L_r\big). \tag{16}$$

De la comparaison de (15) et (16) résulte que les suites de composition (H_i) et (K_j) de G sont équivalentes. □

Démonstration du lemme 5.5. — Le noyau du morphisme canonique $K_1 \to G/H_1$ étant $H_1 \cap K_1$, on a une injection

$$K_1/(H_1 \cap K_1) \hookrightarrow G/H_1.$$

Comme K_1 est distingué dans G, on obtient que $K_1/(H_1 \cap K_1)$ est distingué dans G/H_1. Par simplicité de ce dernier, on obtient soit $K_1/(H_1 \cap K_1) \simeq G/H_1$, soit $K_1/(H_1 \cap K_1) = \{e\}$.

Dans le second cas (qu'on veut exclure), on a $K_1 \subseteq H_1$ et H_1/K_1 est un sous-groupe distingué non trivial du groupe simple G/K_1. Comme $H_1 \neq G$ (puisque G/H_1, étant simple, est non trivial), H_1/K_1 est trivial, ce qui contredit l'hypothèse $H_1 \neq K_1$.

On a donc montré le premier isomorphisme du lemme, et le second se montre de façon analogue. □

Exercice 5.6. — Soit G un groupe (quelconque).
a) Soit H un sous-groupe distingué de G. Supposons que G admette une suite de composition $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\}$. Montrer qu'on peut « extraire » de la suite $(H \cap G_i)_{0 \leqslant i \leqslant r}$ une suite de composition pour H.
b) En déduire la généralisation suivante du th. 5.5 : *deux suites de composition de* G *sont équivalentes* (*Indication :* reprendre la preuve ci-dessus et utiliser a)).
c) Montrer que l'énoncé de b) ne s'étend pas aux suites de composition infinies (*Indication :* pour chaque nombre premier p, on pourra considérer la suite $(p^i\mathbf{Z})_{i \geqslant 0}$ de sous-groupes de $\mathbf{Z}$).

Exercice 5.7. — Soit H un sous-groupe distingué d'un groupe fini G. Montrer que la collection de facteurs simples de G est la réunion de la collection des facteurs simples de H et de la collection des facteurs simples de G/H (il peut bien sûr y avoir des répétitions).

5.3. Groupe dérivé. — Des éléments x et y d'un groupe G commutent si leur *commutateur*

$$[x,y] := xyx^{-1}y^{-1} \tag{17}$$

vaut e. Le sous-groupe

$$\mathrm{D(G)} = \langle [x,y] \mid x,y \in \mathrm{G} \rangle$$

de G engendré par tous les commutateurs est appelé *groupe dérivé* de G.

Le groupe dérivé est trivial si et seulement si G est abélien.

Proposition 5.8. — *Le groupe dérivé* D(G) *est un* sous-groupe caractéristique *de* G*, c'est-à-dire qu'il est stable par tout automorphisme de* G*. En particulier, il est distingué.*

Le quotient G/D(G) *est abélien et c'est le plus grand quotient abélien de* G *au sens suivant : si* $\mathrm{H} \leq \mathrm{G}$*, on a* $\mathrm{D(G)} \leq \mathrm{H}$ *si et seulement si* $\mathrm{H} \trianglelefteq \mathrm{G}$ *et* G/H *est abélien. En d'autres termes, tout quotient abélien de* G *est un quotient de* G/D(G).

On peut dire aussi que tout morphisme de G vers un groupe abélien se factorise à travers G/D(G). Si par exemple G = D(G), tout morphisme de G vers un groupe abélien est trivial.

Démonstration. — L'image du commutateur $[x,y]$ par un automorphisme f de G est le commutateur $[f(x), f(y)]$, donc $f(\mathrm{D(G)}) = \mathrm{D(G)}$.

Puisque $[x,y] \in \mathrm{D(G)}$ pour tous $x, y \in \mathrm{G}$, tous les commutateurs sont nuls dans le quotient G/D(G), donc G/D(G) est abélien. Si G/H est abélien, tous ses commutateurs sont triviaux, donc pour tous $x, y \in \mathrm{G}$, il faut $[x,y] \in \mathrm{H}$, ce qui impose $\mathrm{D(G)} \leq \mathrm{H}$. □

Proposition 5.9. — *Pour* $n \geqslant 5$*, on a* $\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$*. Pour* $n \geqslant 2$*, on a* $\mathrm{D}(\mathfrak{S}_n) = \mathfrak{A}_n$*.*

Démonstration. — Comme $\mathrm{D}(\mathfrak{A}_n)$ est distingué dans $\mathfrak{A}_n$, il est, par le th. 5.1, égal, pour $n \neq 4$,

– soit à $\{e\}$, auquel cas $\mathfrak{A}_n$ est abélien, ce qui ne se produit pas pour $n \geqslant 5$,

– soit à $\mathfrak{A}_n$.

Ceci montre la première assertion. D'autre part, $\mathrm{D}(\mathfrak{S}_n) \leq \mathfrak{A}_n$ (car la signature d'un commutateur est toujours 1), et $\mathrm{D}(\mathfrak{S}_n)$ est distingué dans $\mathfrak{S}_n$ donc dans $\mathfrak{A}_n$. On conclut comme ci-dessus pour $n \neq 4$.

On peut aussi remarquer que tout 3-cycle

$$(abc) = (ab)(abc)(ab)^{-1}(abc)^{-1} = [(ab),(abc)]$$

est un commutateur. Ainsi, le groupe $\mathrm{D}(\mathfrak{S}_n)$ contient tous les 3-cycles, donc est $\mathfrak{A}_n$ pour tout n. □

Exercice 5.10. — Soit H un sous-groupe d'un groupe G. Montrer que D(H) est un sous-groupe de D(G) et qu'il est distingué dans D(G) si H est distingué dans G.

Exercice 5.11. — Soit n un entier $\geqslant 2$. Décrire tous les morphismes de $\mathfrak{S}_n$ dans $\mathbf{C}^\times$.

Exercice 5.12. — Montrer que groupe dérivé $D(SL_2(\mathbf{Z}))$ est d'indice divisant 12 dans $SL_2(\mathbf{Z})$ (*Indication :* si R et S sont les générateurs de $SL_2(\mathbf{Z})$ définis dans l'exerc. 4.2.a), on pourra calculer S^2, S^4, R^3 et R^6) [14].

Exercice 5.13. — Soit G un groupe. On note S l'ensemble de tous les commutateurs $[x,y]$ de G.

Le but de ce long exercice est de montrer que si S est fini, le groupe qu'il engendre, D(G), est aussi fini.

a) Montrer que l'inverse d'un élément de S est encore dans S.

b) Pour tout entier $m \geqslant 0$, on note S_m le sous-ensemble de G formé des produits d'au plus m éléments de S. Montrer $D(G) = \bigcup_{m\geqslant 0} S_m$.

c) Pour tout z dans G et tout s dans S, montrer que zsz^{-1} est dans S.

d) Pour tous x_1, y_1, x_2, y_2, x_3, y_3 dans G, montrer la formule

$$[x_1,y_1][x_2,y_2][x_3,y_3] = [x_1,y_1][x_3,y_3][z^{-1}x_2z, z^{-1}y_2z],$$

où $z = [x_3,y_3]$.

e) On suppose dans cette question que l'indice $[G : Z(G)]$ du centre de G (*cf.* 1.4.5°) est fini et on le note n.

α) Montrer que S est fini de cardinal $r \leqslant n^2$. On note $S = \{s_1,\dots,s_r\}$.

β) Montrer que tout élément de S_m peut s'écrire $s_1^{m_1}\cdots s_r^{m_r}$, avec $m_1,\dots,m_r \in \mathbf{N}$ et $m_1 + \cdots + m_r \leqslant m$ (*Indication :* on pourra utiliser la formule de d)).

γ) Montrer que pour tout $s \in S$, on a $s^n \in Z(G)$.

δ) Montrer que pour tout entier $m \geqslant 0$, on a $S_m \subseteq S_{nr}$ (*Indication :* on pourra procéder par récurrence sur m et démontrer les relations $[x,y]^{n+1} = y^{-1}[x,y]^n y[x,y] = y^{-1}[x,y]^{n-1}[x,y^2]y$).

ε) En déduire que D(G) est fini (de cardinal $\leqslant n^{n^3}$).

f) On suppose dans cette question S fini. Par c), le groupe G agit par conjugaison sur S et on note K le noyau du morphisme composé $D(G) \hookrightarrow G \to \mathrm{Bij}(S)$.

α) Montrer que K est d'indice fini dans D(G) et qu'il est contenu dans Z(D(G)).

β) En déduire que D(D(G)) est fini. Il est distingué dans G par l'exerc. 5.10 ; on pose $H := G/D(D(G))$.

γ) Montrer que D(H) est abélien et en déduire que pour tout $x \in H$ et tout $d \in D(H)$, on a $[x,d]^2 = [x,d^2]$.

δ) En déduire que le sous-groupe $[H,D(H)]$ de H engendré par les $[x,d]$, pour $x \in H$ et $d \in D(H)$, est fini et distingué dans H. On pose $M := H/[H,D(H)]$.

ε) En déduire que D(M) est fini, puis que D(G) est fini.

6. Groupes résolubles

Dans l'ex. 5.3.3° du groupe symétrique $\mathfrak{S}_4$, tous les facteurs simples sont abéliens. C'est un exemple de groupe résoluble.

C'est une notion essentielle pour l'application de la théorie de Galois à la résolution par radicaux des équations polynomiales. Elle admet plusieurs définitions équivalentes

14. Il ressort de la note 12 que l'indice est exactement 12 (*cf.* aussi exerc. II.2.14). On peut montrer que $D(SL_2(\mathbf{Z}))$ est le sous-groupe de $SL_2(\mathbf{Z})$ engendré par les matrices $[S,T] = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$ et $[S,T^{-1}] = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

que nous allons expliquer. Étant donné un groupe G, on définit une suite de sous-groupes

$$G =: D^0(G) \trianglerighteq D^1(G) \trianglerighteq D^2(G) \trianglerighteq \cdots$$

en posant, pour tout entier $n \in \mathbf{N}$,

$$D^{n+1}(G) := D(D^n(G)).$$

Noter que $D^{n+1}(G)$ est distingué dans $D^n(G)$ (et même dans G par l'exerc. 5.10) et que les groupes quotients $D^n(G)/D^{n+1}(G)$ sont abéliens.

Proposition 6.1. — *On dit qu'un groupe* G *est* résoluble *s'il vérifie l'une des conditions équivalentes suivantes :*

(i) il existe $n \in \mathbf{N}$ *tel que* $D^n(G) = \{e\}$;

(ii) il existe une suite

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_r = \{e\}$$

de sous-groupes emboîtés où chaque groupe G_i/G_{i+1} *est abélien.*

Démonstration. — Il est clair que (i) entraîne (ii). Supposons donc qu'il existe une suite comme dans (ii). Puisque G_0/G_1 est abélien, on a vu plus haut que G_1 contient D(G). On montre de la même façon, par récurrence sur n, que G_n contient $D^n(G)$ pour tout $n \in \{0,\dots,r\}$, donc que $D^r(G)$ est trivial. □

Exemples 6.2. — 1° Tout groupe abélien est résoluble.

2° Le groupe $\mathfrak{S}_n$ est résoluble pour $n \leqslant 4$, mais pas pour $n \geqslant 5$ puisqu'on a alors $D^m(\mathfrak{S}_n) = \mathfrak{A}_n$ pour tout $m \geqslant 1$ (prop. 5.9).

L'importance de ce résultat réside dans le fait que, par la théorie de Galois, il implique que l'équation générale de degré $n \geqslant 5$ n'est pas résoluble par radicaux. Cela explique aussi la terminologie.

3° Un groupe G qui est résoluble et simple est cyclique d'ordre premier : en effet, on a $D(G) \neq G$ (sinon la condition (i) du théorème ne pourrait être vérifiée) et comme $D(G) \trianglelefteq G$, on a $D(G) = \{e\}$ puisque G est simple. Le groupe G est donc abélien ; étant simple, il est cyclique d'ordre premier.

4° Si **K** est un corps, le groupe affine GA(**K**) (*cf.* ex. 1.1.5°) est résoluble (*cf.* exerc. 1.28). En revanche, pour $n \geqslant 2$ et $\mathrm{card}(\mathbf{K}) \geqslant 4$, les groupes $SL_n(\mathbf{K})$ et $GL_n(\mathbf{K})$ ne le sont pas puisque leur groupe dérivé est $SL_n(\mathbf{K})$ (th. II.2.6).

La propriété d'être résoluble passe aux sous-groupes et aux groupes quotients.

Proposition 6.3. — *Soit* G *un groupe et soit* H *un sous-groupe de* G.

1° Si G *est résoluble,* H *est résoluble.*

2° Si $H \trianglelefteq G$*, on a*

$$G \textit{ résoluble} \iff H \textit{ et } G/H \textit{ résolubles.}$$

Démonstration. — 1° Pour tout entier n, $D^n(H)$ est contenu dans $D^n(G)$. Le premier point résulte donc de la prop. 6.1.(i).

2° Si G est résoluble, avec $D^n(G) = \{e\}$, on vient de voir que H l'est aussi (avec $D^n(H) = \{e\}$). Les commutateurs de G/H sont les images par la surjection canonique $G \to G/H$ des commutateurs de G. Le groupe D(G/H) est donc l'image de D(G), puis le groupe $D^n(G/H)$ est l'image de $D^n(G)$, donc $D^n(G/H) = \{e\}$ et G/H est résoluble.

Inversement, supposons H et G/H résolubles, avec $\mathrm{D}^m(\mathrm{H})$ et $\mathrm{D}^n(\mathrm{G/H})$ triviaux. Comme $\mathrm{D}^n(\mathrm{G/H})$, qui est trivial, est l'image de $\mathrm{D}^n(\mathrm{G})$ par la surjection canonique, ce dernier est contenu dans H. On a alors

$$\mathrm{D}^{m+n}(\mathrm{G}) = \mathrm{D}^m(\mathrm{D}^n(\mathrm{G})) \leq \mathrm{D}^m(\mathrm{H}) = \{e\},$$

donc G est résoluble. □

Exemple 6.4. — Le groupe $\mathrm{SL}_n(\mathbf{Z})$ n'est pas résoluble pour $n \geqslant 2$ [15].

Proposition 6.5. — *Soit* G *un groupe fini. Les conditions suivantes sont équivalentes :*
(i) G *est résoluble ;*
(ii) les facteurs simples de G *sont cycliques d'ordre premier.*

Démonstration. — Pour montrer que (ii) implique (i), on peut procéder par récurrence sur la longueur d'une suite de composition $\mathrm{G} = \mathrm{G}_0 \rhd \mathrm{G}_1 \rhd \cdots \rhd \mathrm{G}_r = \{e\}$ (dont les quotients successifs sont donc cycliques d'ordre premier). L'hypothèse de récurrence entraîne que G_1 est résoluble. Comme $\mathrm{G/G}_1$ est cyclique, donc abélien, il est aussi résoluble et on conclut que G est résoluble par la prop. 6.3.2°.

Inversement, si G est résoluble, la même proposition dit que tous ses facteurs simples sont résolubles. Étant simples, il sont cycliques d'ordre premier (ex. 6.2.3°). □

Le *théorème de Burnside* dit que tout groupe fini dont l'ordre a au plus deux facteurs premiers est résoluble. On peut le démontrer en utilisant la théorie des représentations, qui sera présentée au chap. IV. La preuve est astucieuse, mais du niveau de ce cours. Plusieurs cas particuliers sont proposés en exercice ci-dessous.

Ce n'est pas le cas du *théorème de Feit et Thompson* (1963), qui affirme que tout groupe fini d'ordre impair est résoluble. Sa démonstration occupe plusieurs centaines de pages. Il est équivalent à dire que tout groupe fini simple non abélien est d'ordre pair (pourquoi ?).

Exercice 6.6. — Soit p un nombre premier. Montrer qu'un p-groupe est résoluble.

Exercice 6.7. — Soient p et q des nombres premiers.
a) Montrer que tout groupe d'ordre pq est résoluble (*Indication :* on pourra utiliser l'exerc. 2.29).
b) Montrer que tout groupe d'ordre p^2q est résoluble (*Indication :* on pourra utiliser l'exerc. 2.33).
c) Montrer que tout groupe d'ordre p^3q est résoluble (*Indication :* on pourra utiliser l'exerc. 2.34).

Exercice 6.8. — Soient p et q des nombres premiers, avec $p \leqslant q$, et soit G un groupe d'ordre $p^m q^n$, avec $0 \leqslant m \leqslant 2$ et $n \geqslant 0$. Montrer que G est résoluble (*Indication :* on pourra utiliser l'exerc. 2.32).

Exercice 6.9. — Soit q un nombre premier impair et soit G un groupe d'ordre $8q^n$. Le but de cet exercice est de montrer que G est résoluble. On note n_q le nombre de q-sous-groupes de Sylow de G.
a) Montrer que G est résoluble si $(q, n_q) \notin \{(3,4),(7,8)\}$.

15. Pour $n \geqslant 3$, cela résulte de l'exerc. II.2.9 ; pour tout $n \geqslant 2$, on peut utiliser le fait que l'application $\mathrm{SL}_n(\mathbf{Z}) \to \mathrm{SL}_n(\mathbf{Z}/5\mathbf{Z})$ de réduction modulo 5 est surjective, que le groupe $\mathrm{SL}_n(\mathbf{Z}/5\mathbf{Z})$ n'est pas résoluble (ex. 6.2.4°), et appliquer la prop. 6.3.

b) On suppose $q = 3$ et $n_q = 4$. Montrer que G est résoluble (*Indication :* on pourra considérer l'action transitive de G sur l'ensemble des 3-sous-groupes de Sylow et appliquer l'exerc. 6.8 âĂą son noyau).
c) On suppose $q = 7$ et $n_q = 8$. Montrer que G est résoluble (*Indication :* on pourra considérer l'action transitive de G sur l'ensemble des 7-sous-groupes de Sylow ; pour le cas $n = 1$, on pourra compter les éléments d'ordre 7).

Exercice 6.10. — Soient p, q et r des nombres premiers et soit G un groupe d'ordre pqr. Montrer que G est résoluble.

Exercice 6.11. — Montrer que tout groupe d'ordre 72 est résoluble (*Indication :* on pourra considérer les 3-sous-groupes de Sylow et utiliser l'exerc. 2.31).

Exercice 6.12. — Montrer que tout groupe d'ordre 495 est résoluble (*Indication :* on pourra considérer les 5- et 11-sous-groupes de Sylow, montrer que l'un d'eux est distingué, puis utiliser les exercices précédents).

Exercice 6.13. — Montrer que tout groupe d'ordre 2907 est résoluble (*Indication :* on pourra utiliser l'exerc. 2.37).

Exercice 6.14. — Soit $\mathbf{K}$ un corps et soit n un entier $\geqslant 1$. Montrer que le sous-groupe T de $\mathrm{GL}_n(\mathbf{K})$ formé des matrices triangulaires supérieures est résoluble (*Indication :* on pourra étudier la suite des groupes dérivés $\mathrm{D}^m(\mathrm{T})$).

Exercice 6.15. — Soit p un nombre premier. Le groupe affine $\mathrm{GA}(\mathbf{F}_p)$ (*cf.* ex. 1.1.5°) est résoluble (*cf.* ex. 6.2.4°) et il opère transitivement et fidèlement sur l'ensemble $\mathbf{F}_p = \{0, \dots, p-1\}$. On peut le voir comme un sous-groupe de $\mathfrak{S}_{\mathbf{F}_p} = \mathfrak{S}_p$; son cardinal est $p(p-1)$ (exerc. 1.28).

Le but de cet exercice est de montrer que tout sous-groupe *résoluble* $\mathrm{H} \leq \mathfrak{S}_p$ qui opère transitivement est conjugué à un sous-groupe de $\mathrm{GA}(\mathbf{F}_p)$; en particulier, son ordre divise $p(p-1)$ (c'est un résultat dû à Galois).

Soit $\mathrm{H} = \mathrm{H}_0 \rhd \mathrm{H}_1 \rhd \cdots \rhd \mathrm{H}_r = \{e\}$ une suite de sous-groupes emboîtés où chaque groupe $\mathrm{H}_i/\mathrm{H}_{i+1}$ est abélien d'ordre premier (prop. 6.5).
a) Soit τ la translation $x \mapsto x+1$. Déterminer les p-sous-groupes de Sylow de G. En déduire que si g est un élément de $\mathfrak{S}_p$ tel que $g\tau g^{-1}$ est dans G, alors $g \in \mathrm{G}$.
b) Montrer que le groupe H_{r-1} agit transitivement sur $\mathbf{F}_p$ (*Indication :* on pourra utiliser l'exerc. 2.6), puis qu'il est d'ordre p.
c) Soit τ' un générateur de H_{r-1}. Montrer qu'il existe $g \in \mathfrak{S}_p$ tel que $g\tau' g^{-1} = \tau$. On pose $\mathrm{H}'_i := g\mathrm{H}_i g^{-1}$.
d) Conclure $\mathrm{H} \leq g^{-1}\mathrm{G}g$ (*Indication :* on pourra montrer $\mathrm{H}'_i \leq \mathrm{G}$ par récurrence descendante sur i, en utilisant b)).

Exercice 6.16. — Soit p un nombre premier. Le but de cet exercice est de montrer qu'un sous-groupe H de $\mathfrak{S}_p$ qui opère transitivement est résoluble si et seulement si aucun élément de H autre que l'identité laisse deux éléments de $\{1, \dots, p\}$ fixes.
a) On suppose que H est résoluble. Montrer que H a cette propriété (*Indication :* on pourra utiliser l'exercice précédent).
b) On suppose que H a cette propriété. On note $\mathrm{H}_x \leq \mathrm{H}$ le stabilisateur d'un point x de $\{1, \dots, p\}$. Montrer que les $(\mathrm{H}_x - \{\mathrm{Id}\})_{x \in \{1,\dots,p\}}$ forment, avec l'ensemble S des éléments de H sans aucun point fixe, une partition de $\mathrm{H} - \{\mathrm{Id}\}$. Montrer l'égalité $|\mathrm{H}| = p|\mathrm{H}_x|$ et en déduire le cardinal de S.

c) Montrer que H contient un p-cycle σ (*Indication :* on pourra utiliser le lemme de Cauchy (exerc. 2.14)) et que $S = \{\sigma, \dots, \sigma^{p-1}\}$.
d) Montrer que S est stable par conjugaison par tout élément de H (*Indication :* on pourra utiliser la question b) de l'exercice précédent). En déduire que H est conjugué à un sous-groupe du groupe affine $GA(\mathbf{F}_p)$ et conclure.

7. Groupes nilpotents

Dans le paragraphe précédent, nous avons considéré la suite dérivée descendante $(D^n(G))$ de sous-groupes distingués d'un groupe G. On peut construire une suite ascendante $(Z^n(G))$ de sous-groupes distingués de G de la façon suivante.

On pose $Z_0(G) := \{e\}$ et $Z_1(G) := Z(G)$, le centre du groupe G. Il est bien distingué dans G. Supposons $Z^n(G) \trianglelefteq G$ construit. On note alors $Z_{n+1}(G) \trianglelefteq G$ l'image inverse par la surjection canonique $G \to G/Z_n(G)$ du centre de $G/Z_n(G)$, c'est-à-dire

$$Z_{n+1}(G) = \{g \in G \mid \forall x \in G \quad gxg^{-1}x^{-1} \in Z_n(G)\}.$$

On obtient ainsi une suite croissante de sous-groupes

$$\{e\} = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq Z_2(G) \trianglelefteq \cdots$$

où les quotients successifs sont abéliens.

Définition 7.1. — On dit qu'un groupe G est *nilpotent* s'il existe $n \in \mathbf{N}$ tel que $Z_n(G) = G$.

Exemples 7.2. — 1° Tout groupe abélien est nilpotent, puisque $Z_1(G) = G$.

2° Le groupe $\mathfrak{S}_n$ est nilpotent pour $n \leqslant 2$, mais pas pour $n \geqslant 3$, puisqu'on a alors $Z(\mathfrak{S}_n) = \{\mathrm{Id}\}$ (exerc. 1.6).

Exercice 7.3. — Soit p un nombre premier. Montrer qu'un p-groupe est nilpotent.

Exercice 7.4. — Montrer que le groupe D_n est nilpotent si et seulement si n est une puissance de 2 (*Indication :* utiliser l'exerc. 1.5).

Exercice 7.5. — Soit $\mathbf{K}$ un corps et soit n un entier $\geqslant 1$. Montrer que le sous-groupe de $GL_n(\mathbf{K})$ formé des matrices triangulaires supérieures avec des 1 sur la diagonale est nilpotent.

On peut aussi caractériser les groupes nilpotents à l'aide d'une autre suite de sous-groupes, cette fois descendante. Il s'agit de la suite $(C^n(G))$ définie récursivement par

$$C^0(G) = G \qquad C^{n+1}(G) := [G, C^n(G)] := \langle \{[x, y] \mid x \in G, y \in C^n(G)\} \rangle$$

(on rappelle la notation de (17) : $[x, y] = xyx^{-1}y^{-1}$).

Montrons tout d'abord, par récurrence sur n, que $C^n(G)$ est distingué dans G. Pour tout $x \in G$, tout $y \in C^n(G)$, et tout $z \in G$, on a

$$z[x, y]z^{-1} = [zxz^{-1}, zyz^{-1}].$$

Si $C^n(G)$ est distingué dans G, on a $zyz^{-1} \in C^n(G)$, donc $z[x, y]z^{-1} \in C^{n+1}(G)$. On en déduit que les générateurs de $zC^{n+1}(G)z^{-1}$ sont dans $C^{n+1}(G)$, donc que $C^{n+1}(G)$ est aussi distingué dans G.

Cela entraîne les inclusions

$$G = C^0(G) \trianglerighteq C^1(G) \trianglerighteq C^2(G) \trianglerighteq \cdots$$

où les quotients successifs sont abéliens, puisque $C^{n+1}(G) \supseteq D(C^n(G))$.

Proposition 7.6. — *Un groupe* G *est nilpotent si et seulement si il existe* $n \geqslant 0$ *tel que* $C^n(G) = \{e\}$.

Démonstration. — Supposons tout d'abord G nilpotent, avec $Z_n(G) = G$. Nous allons montrer par récurrence sur $m \in \{0, \dots, n\}$ l'inclusion $C^m(G) \subseteq Z_{n-m}(G)$, qui donne $C^n(G) = \{e\}$, c'est-à-dire le résultat cherché, pour $m = n$.

Pour $m = 0$, cette inclusion est $G \subseteq Z_n(G)$: elle est vraie par hypothèse.

Supposons $C^m(G) \subseteq Z_{n-m}(G)$. Pour montrer $C^{m+1}(G) \subseteq Z_{n-m-1}(G)$, il suffit de montrer que $[x, y]$ est dans $Z_{n-m-1}(G)$ pour tout $x \in G$ et tout $y \in C^m(G)$. Par hypothèse, on a $y \in Z_{n-m}(G)$, donc la classe $\overline{y}$ de y dans $G/Z_{n-m-1}(G)$ est dans le centre de ce groupe, de sorte que $\overline{[x, y]} = [\overline{x}, \overline{y}] = \overline{e}$. On en déduit $[x, y] \in Z_{n-m-1}(G)$.

Supposons inversement $C^n(G) = \{e\}$. Nous allons montrer par récurrence sur $m \in \{0, \dots, n\}$ l'inclusion $C^{n-m}(G) \subseteq Z_m(G)$, qui donne $Z_n(G) = G$, c'est-à-dire le résultat cherché, pour $m = n$.

Pour $m = 0$, cette inclusion est $C^n(G) \subseteq \{e\}$: elle est vraie par hypothèse.

Supposons $C^{n-m}(G) \subseteq Z_m(G)$. Soit $y \in C^{n-m-1}(G)$. Pour tout $x \in G$, on a alors $[x, y] \in Z_m(G)$, c'est-à-dire $[\overline{x}, \overline{y}] = \overline{e}$ dans $G/Z_m(G)$. On en déduit que $\overline{y}$ est dans le centre de $G/Z_m(G)$, donc que y est dans $Z_{m+1}(G)$, ce qui montre le pas de récurrence. □

Corollaire 7.7. — *Tout groupe nilpotent est résoluble.*

Démonstration. — Cela résulte du fait qu'on a $D^n(G) \subseteq C^n(G)$ pour tout $n \geqslant 0$. □

Corollaire 7.8. — *Le produit de deux groupes nilpotents est nilpotent.*

Démonstration. — Cela résulte du fait qu'on a $C^n(G \times H) \subseteq C^n(G) \times C^n(H)$ pour tout $n \geqslant 0$. □

La propriété d'être nilpotent passe aussi aux sous-groupes et aux groupes quotients.

Corollaire 7.9. — *Soit* G *un groupe nilpotent et soit* H *un sous-groupe de* G.

1° Le groupe H *est nilpotent.*

2° Si $H \trianglelefteq G$, *le groupe* G/H *est nilpotent*[16].

Démonstration. — Pour le premier point, cela résulte du fait qu'on a $C^n(H) \subseteq C^n(G)$ pour tout $n \geqslant 0$.

Pour le second point, les commutateurs de G/H sont les images par la surjection canonique $G \to G/H$ des commutateurs de G. On en déduit que $C^n(G/H)$ est l'image par p de $C^n(G)$. □

16. Mais attention : H et G/H peuvent être nilpotents sans que G le soit ! C'est le cas par exemple pour $H = \mathbf{Z}/6\mathbf{Z}$, nilpotent, sous-groupe distingué de $G = D_6$, non nilpotent (exerc. 7.4), bien que $G/H \simeq \mathbf{Z}/2\mathbf{Z}$ le soit.

En particulier, il résulte du cor. 7.9 et de l'exerc. 7.5 que tout sous-groupe de $\mathrm{GL}_n(\mathbf{K})$ formé de matrices triangulaires supérieures avec des 1 sur la diagonale est nilpotent [17].

Exercice 7.10. — Soit G un groupe fini. Le but de cet exercice est de montre l'équivalence des conditions suivantes :
(i) G est nilpotent ;
(ii) G est isomorphe au produit de ses sous-groupes de Sylow, c'est-à-dire à un produit de p-groupes (pour des p peut-être différents).

a) Montrer l'implication (ii)⇒(i).
On suppose maintenant G *nilpotent (fini).*
b) Soit $\mathrm{H} < \mathrm{G}$ un sous-groupe propre de G. Montrer que son normalisateur $\mathrm{N_G(H)}$ (*cf.* (6)) contient strictement H (*Indication :* on pourra considérer le plus grand entier $m < n$ tel que $\mathrm{C}^m(\mathrm{G}) \leq \mathrm{H}$, choisir $g \in \mathrm{C}^{m+1}(\mathrm{G}) - \mathrm{H}$, et montrer $g \in \mathrm{N_G(H)}$).
c) Soit S un p-sous-groupe de Sylow de G. Montrer S est distingué dans G (*Indication :* on pourra utiliser l'exerc. 2.42.b)).
d) Soient S et S' des sous-groupes de Sylow distincts de G. Montrer $\mathrm{S} \cap \mathrm{S}' = \{e\}$ et que tout élément de S commute avec tout élément de S'. En déduire (ii).

Exercice 7.11. — Soit G un groupe nilpotent. Montrer que le produit de deux éléments de G d'ordre fini est d'ordre fini. Plus précisément, si $x^m = y^m = e$ et $\mathrm{C}^n(\mathrm{G}) = \{e\}$, on a $(xy)^{m^n} = e$ (*Indication :* on pourra procéder par récurrence sur n).

8. Croissance des groupes de type fini

L'exerc. 7.10 ci-dessus montre qu'en un certain sens, les groupes nilpotents finis ne sont pas très intéressants. Nous allons voir dans cette section que la théorie des groupes nilpotents infinis est beaucoup plus riche.

Rappelons (§1.2) qu'un groupe G est *de type fini* s'il existe une partie génératrice finie $\mathrm{A} = \{a_1, \ldots, a_r\} \subseteq \mathrm{G}$. Pour tout entier $m \geqslant 0$, on note $\mathrm{B_{G,A}}(m)$ l'ensemble des éléments de G qui peuvent s'écrire comme produits d'au plus m éléments de $\mathrm{A} \cup \mathrm{A}^{-1}$. On veut étudier la fonction (croissante)

$$\begin{aligned} \beta_{\mathrm{G,A}} : \mathbf{N} &\longrightarrow \mathbf{N} \\ m &\longmapsto \mathrm{card}(\mathrm{B_{G,A}}(m)). \end{aligned}$$

Exemple 8.1. — Considérons la partie génératrice $\mathrm{A} = \{1\}$ du groupe $\mathbf{Z}$. On a alors $\beta_{\mathbf{Z},\mathrm{A}}(0) = 1$ et, pour $n \geqslant 1$, on a $\mathrm{B_{G,A}}(m) = \{-m, \ldots, 0, \ldots, m\}$, donc

$$\forall\, m \geqslant 1 \qquad \beta_{\mathbf{Z},\mathrm{A}}(m) = m + 1.$$

La partie $\mathrm{B} = \{2, 3\}$ est encore génératrice. On peut montrer (ce n'est pas complètement trivial) qu'on a

$$\forall\, m \geqslant 2 \qquad \beta_{\mathbf{Z},\mathrm{B}}(0) = m + 1.$$

17. Ellis Kolchin a démontré en 1948 que plus généralement, tout sous-groupe de $\mathrm{GL}_n(\mathbf{K})$ formé de matrices unipotentes (c'est-à-dire de la forme $\mathrm{I}_n + \mathrm{N}$, où N est une matrice nilpotente) est nilpotent, en montrant qu'il existe une base de $\mathbf{K}^n$ dans laquelle tous les éléments du groupe ont une matrice triangulaire supérieure (avec des 1 sur la diagonale).

La fonction peut donc dépendre de la partie génératrice choisie. Ceci dit, nous nous intéresserons non pas au calcul précis de ces fonctions, mais à leur comportement lorsque n tend vers l'infini. Dans l'exemple, on voit que $\beta_{\mathbf{Z},\mathrm{A}}$ et $\beta_{\mathbf{Z},\mathrm{A}}$ sont toutes deux polynomiales de même degré. De façon générale, on a toujours la borne

$$\beta_{\mathrm{G,A}}(m) \leqslant (2\,\mathrm{card}(\mathrm{A})+1)^m.$$

La croissance est donc au plus exponentielle.

Les fonctions obtenues lorsqu'on change de partie génératrice peuvent être comparées. Pour cela, nous introduisons la relation d'ordre entre fonctions croissantes $\mathbf{N} \to \mathbf{R}^+$ définie par

$$\beta_1 \preceq \beta_2 \quad \Longleftrightarrow \quad (\exists c>0\ \exists a \in \mathbf{N}^*\ \forall m \in \mathbf{N}^* \quad \beta_1(m) \leqslant c\beta_2(am)).$$

On dit que de telles fonctions β_1 et β_2 sont *équivalentes*, et on écrit $\beta_1 \sim \beta_2$, si $\beta_1 \preceq \beta_2$ et $\beta_2 \preceq \beta_1$.

Exemples 8.2. — 1° Toute fonction bornée est équivalente à toute fonction constante.

2° Des fonctions poynomiales sont équivalentes si et seulement si elles sont de même degré.

3° Pour tout $a>0$, les fonctions $m \mapsto e^m$ et $m \mapsto e^{am}$ sont équivalentes.

Proposition 8.3. — *Soit* G *un groupe de type fini et soient* A *et* A′ *des parties génératrices finies de* G. *Les fonctions* $\beta_{\mathrm{G,A}}$ *et* $\beta_{\mathrm{G,A'}}$ *sont équivalentes.*

On parlera ainsi (abusivement) de *la* fonction de croissance β_{G} de G.

Démonstration. — Il suffit bien sûr de montrer $\beta_{\mathrm{G,A}} \preceq \beta_{\mathrm{G,A'}}$. Soit a un entier tel que tous les éléments de A soient dans $\mathrm{B}_{\mathrm{G,A'}}(a)$. On a alors aussi $\mathrm{A}^{-1} \subseteq \mathrm{B}_{\mathrm{G,A'}}(a)$, d'où on déduit

$$\mathrm{B}_{\mathrm{G,A}}(m) \subseteq \mathrm{B}_{\mathrm{G,A'}}(am)$$

et la proposition. □

Exercice 8.4. — Soit H un sous-groupe d'un groupe de type fini G.
a) Si H est de type fini, montrer $\beta_{\mathrm{H}} \preceq \beta_{\mathrm{G}}$.
b) Si H est d'indice fini dans G, il est de type fini (exerc.1.14) ; montrer $\beta_{\mathrm{H}} \sim \beta_{\mathrm{G}}$.

Définition 8.5. — Soit G un groupe de type fini.

Le groupe G est *à croissance polynomiale* (de degré au plus d) si $\beta_{\mathrm{G}}(m) \preceq m^d$.

Le groupe G est *à croissance exponentielle* si $\beta_{\mathrm{G}}(m) \sim e^m$.

Il existe des groupes de type fini qui ne sont ni à croissance polynomiale, ni à croissance exponentielle ! C'est un problème très difficile de recherche actuelle de construire des groupes de type fini dont la fonction de croissance est « exotique ».

Exemples 8.6. — 1°Un groupe abélien de type fini est à croissance polynomiale de degré au plus le nombre de générateurs [18].

18. Plus précisément, il résulte du th. 3.6 que la croissance est polynomiale de degré au plus le nombre r apparaissant dans ce théorème.

2° Pour $n \geqslant 2$, les groupes $\mathrm{SL}_n(\mathbf{Z})$ (qui sont de type fini par le th. 4.1) sont à croissance exponentielle [19].

Proposition 8.7. — *Soit* G *un groupe de type fini. Les groupes* $\mathrm{C}^n(\mathrm{G})/\mathrm{C}^{n+1}(\mathrm{G})$ *sont abéliens de type fini.*

Démonstration. — On a déjà remarqué que ces quotients sont abéliens. On montre par récurrence sur n qu'ils sont de type fini. Soient $a_1, \ldots, a_r$ des générateurs de G.

Pour $n = 0$, il est clair que $\mathrm{C}^0(\mathrm{G})/\mathrm{C}^1(\mathrm{G}) = \mathrm{G}/\mathrm{C}^1(\mathrm{G})$ est engendré par les classes de $a_1, \ldots, a_r$.

Supposons donc que $\mathrm{C}^n(\mathrm{G})/\mathrm{C}^{n+1}(\mathrm{G})$ est engendré par les classes de $b_1, \ldots, b_s \in \mathrm{C}^n(\mathrm{G})$. Nous allons montrer que $\mathrm{C}^{n+1}(\mathrm{G})/\mathrm{C}^{n+2}(\mathrm{G})$ est engendré par les classes des $[a_i^{\pm 1}, b_j^{\pm 1}]$, pour $1 \leqslant i \leqslant r$ et $1 \leqslant j \leqslant s$. Il suffit de montrer que tout commutateur $[x, z]$, avec $x \in \mathrm{G}$ et $z \in \mathrm{C}^n(\mathrm{G})$, est produit de ces éléments modulo $\mathrm{C}^{n+2}(\mathrm{G})$.

Nous allons utiliser les deux identités suivantes, valables pour tous éléments x, y et z d'un groupe, que le lecteur est invité à vérifier par lui-même :

$$[xy, z] = [y, z]\,[[z, y], x]\,[x, z], \tag{18}$$

$$[x, yz] = [x, y]\,[x, z]\,[[z, x], y]. \tag{19}$$

Si on prend $z \in \mathrm{C}^n(\mathrm{G})$ dans (18), on obtient

$$[x_1 x_2, z] = [x_1, z]\,[x_2, z] \qquad \text{dans} \quad \mathrm{C}^{n+1}(\mathrm{G})/\mathrm{C}^{n+2}(\mathrm{G})$$

puisque $[[z, x_2], x_1] \in \mathrm{C}^{n+2}(\mathrm{G})$. Ceci entraîne que le groupe $\mathrm{C}^{n+1}(\mathrm{G})/\mathrm{C}^{n+2}(\mathrm{G})$ est engendré par les classes des $[a_i^{\pm 1}, z]$ pour $1 \leqslant i \leqslant r$ et $z \in \mathrm{C}^n(\mathrm{G})$. Il suffit ensuite de décomposer z en produit des b_j et de leurs inverses et d'utiliser (19) de la même façon pour conclure. □

J. A. Wolf a montré (1968) que les groupes nilpotents de type fini sont à croissance polynomiale, donc aussi les groupes de type fini qui possèdent un sous-groupe nilpotent d'indice fini (exerc. 8.4.b)).

La réciproque est un résultat spectaculaire de M. Gromov (1981).

Théorème 8.8. — *Un groupe de type fini est à croissance polynomiale si et seulement si il possède un sous-groupe nilpotent d'indice fini.*

Démonstration. — Il est hors de question de démontrer ici le théorème de Gromov ; nous renvoyons au célèbre blog de T. Tao (http ://terrytao.wordpress.com/) pour une démonstration « élémentaire ».

Nous nous contenterons d'expliquer le théorème de Wolf dans le cas où $\mathrm{C}^2(\mathrm{G}) = [\mathrm{G}, [\mathrm{G}, \mathrm{G}]]$ est trivial, c'est-à-dire quand tout commutateur est dans le centre de G (le cas où $\mathrm{C}^1(\mathrm{G})$ est trivial est l'ex. 8.6.1°).

Soit donc $\mathrm{A} = \{a_1, \ldots, a_r\}$ un ensemble fini de générateurs de G, stable par inversion et contenant e. Pour tout entier $m \geqslant 0$, un élément g de $\mathrm{B}_{\mathrm{G},\mathrm{A}}(m)$ est produit de m éléments

19. C'est plus difficile ! Brièvement, on peut supposer $n = 2$, considérer le sous-groupe H de $\mathrm{SL}_2(\mathbf{Z})$ engendré par les matrices $\mathrm{M} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $\mathrm{N} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, et montrer qu'aucun produit $\mathrm{M}^{a_1}\mathrm{N}^{b_1}\mathrm{M}^{a_2}\mathrm{N}^{b_2}\cdots\mathrm{M}^{a_r}\mathrm{N}^{b_r}$ n'est l'identité I_2 lorsque $r > 0$ et que les a_i et b_i sont des entiers non nuls (on dit que H est un groupe *libre*) : cela entraîne alors $\beta_{\mathrm{H},\{\mathrm{M},\mathrm{N}\}}(m) \geqslant 4^m$ pour tout m. On conclut alors avec l'exerc. 8.4.a).

de A. Si on rencontre dans ce produit $a_j a_i$, avec $j > i$, on l'écrit $a_i a_j [a_j^{-1}, a_i^{-1}]$. Comme $[a_j^{-1}, a_i^{-1}]$ commute avec tous les éléments de G, on peut l'envoyer ensuite toute à la droite du produit. Cette opération nous permet d'écrire, après au plus $(m-1)+\cdots+1$ pas,

$$g = a_1^{k_1} \dots a_r^{k_r} c,$$

avec $k_i \geqslant 0$ et $k_1 + \cdots + k_r = n$, et où c est un produit d'au plus $m(m-1)/2$ commutateurs $[a_i, a_j]$. On en déduit

$$\beta_{G,A}(m) \leqslant O(m^r)\, \beta_{[G,G],[A,A]}(m(m-1)/2).$$

Comme le groupe [G, G] est abélien de type fini (en fait, ici, engendré par les $[a_i, a_j]$, pour $1 \leqslant i < j \leqslant r$), on en déduit que G est à croissance polynomiale (de degré $\leqslant r + r^2$).

Ceci démontre le théorème de Wolf dans ce cas particulier. La preuve dans le cas général (qui procède par récurrence sur un entier n tel que $C^n(G)$ est trivial, en utilisant le même algorithme) est laissée au lecteur. □

Remarque 8.9. — Il existe des groupes de type fini résolubles à croissance exponentielle. Plus précisément, J. Milnor et J. Wolf ont montré (1968) qu'un groupe de type fini résoluble qui ne contient aucun sous-groupe nilpotent d'indice fini est à croissance exponentielle. On sait construire explicitement de tels groupes.

CHAPITRE II

GROUPES CLASSIQUES

1. Préliminaires sur les corps

Les groupes classiques qu'on étudie dans ce chapitre sont définis sur des corps, et quelques propriétés de base de la théorie des corps seront utiles. Le but de cette section préliminaire est de les rappeler.

Soit **K** un corps. On dispose d'un morphisme d'anneaux

$$\phi : \mathbf{Z} \longrightarrow \mathbf{K}$$

défini par

$$\phi(n) = n \cdot 1_{\mathbf{K}} = \overbrace{1_{\mathbf{K}} + \cdots + 1_{\mathbf{K}}}^{n \text{ fois}}$$

si $n \geqslant 0$, et $\phi(n) = -\phi(-n)$ si $n < 0$. Le noyau de ϕ est un idéal $p\mathbf{Z} \subseteq \mathbf{Z}$ et fournit un morphisme injectif

$$\hat{\phi} : \mathbf{Z}/p\mathbf{Z} \longrightarrow \mathbf{K}.$$

Puisque **K** est un corps, $\mathbf{Z}/p\mathbf{Z}$ est intègre et donc p est un nombre premier s'il est non nul.

Le nombre p (un entier premier ou bien 0) est appelé la *caractéristique du corps* **K**, notée car(**K**).

On a les propriétés suivantes :

- Si car(**K**) = 0, alors **K** contient **Q** comme sous-corps. C'est le plus petit sous-corps de **K** ; on l'appelle le *sous-corps premier* de **K**.
- Si car(**K**) = $p > 0$, on a $p \cdot 1_{\mathbf{K}} = 0$ dans **K**, donc pour tout $x \in \mathbf{K}$ on a $p \cdot x = p(1_{\mathbf{K}} \cdot x) = (p \cdot 1_{\mathbf{K}})x = 0$. L'image de ϕ est le sous-corps premier de **K** ; il est isomorphe à $\mathbf{F}_p$ (qui est une autre notation pour le corps $\mathbf{Z}/p\mathbf{Z}$).
- Toujours si car(**K**) = $p > 0$, l'application

$$\begin{array}{rcl} \mathrm{F}_{\mathbf{K}} : \mathrm{K} & \longrightarrow & \mathrm{K} \\ x & \longmapsto & x^p \end{array}$$

est un morphisme de corps, appelé *morphisme de Frobenius*. En effet, la formule du binôme fournit les égalités

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \cdots + y^p = x^p + y^p$$

car $p \mid \binom{p}{i}$ pour $1 \leqslant i \leqslant p-1$. Le morphisme $\mathrm{F}_{\mathbf{K}}$ est injectif ($x^p = 0$ entraîne $x = 0$) mais pas nécessairement surjectif (si c'est le cas, on dit que le corps $\mathbf{K}$ est *parfait*).

– Si $\mathbf{K}$ est un corps fini, ϕ ne peut être injectif, donc $p = \mathrm{car}(\mathbf{K}) > 0$. Le corps $\mathbf{K}$ est alors un $\mathbf{F}_p$-espace vectoriel, nécessairement de dimension finie d, d'où $|\mathbf{K}| = p^d$. Le morphisme de Frobenius $\mathrm{F}_{\mathbf{K}}$, étant une application injective entre ensembles finis de même cardinal, est bijectif.

Le groupe multiplicatif $(\mathbf{K}^\times, \times)$ étant d'ordre $q-1$, le théorème de Lagrange fournit $x^{q-1} = 1$ pour tout $x \in \mathbf{K}^\times$, donc $x^q = x$ pour tout $x \in \mathbf{K}$, c'est-à-dire que $\mathrm{F}_{\mathbf{K}}^d$ est l'identité de $\mathbf{K}$. En particulier, $\mathrm{F}_{\mathbf{F}_p}$ est l'identité. En d'autres termes, le sous-corps premier $\mathbf{F}_p$ de $\mathbf{K}$ est contenu dans l'ensemble

$$\{x \in \mathbf{K} \mid \mathrm{F}(x) = x\}$$

des racines du polynôme $\mathrm{X}^p - \mathrm{X}$. Comme cet ensemble a au plus p éléments, ils sont égaux.

La dernière propriété dont nous aurons besoin est plus difficile et nous ne la démontrerons pas ici.

Théorème 1.1. — *Si $q = p^d$, où p est un nombre premier et $d \in \mathbf{N}^*$, il existe, à isomorphisme près, un et un seul corps de cardinal q. On le note $\mathbf{F}_q$.*

On peut soit construire ce corps comme le corps de rupture du polynôme $\mathrm{X}^q - \mathrm{X}$ sur $\mathbf{F}_p$, c'est-à-dire le plus petit sur-corps de $\mathbf{F}_p$ dans lequel le polynôme $\mathrm{X}^q - \mathrm{X}$ est scindé en produit de facteurs du premier degré, soit, si on admet l'existence d'une clôture algébrique $\bar{\mathbf{F}}_p$ de $\mathbf{F}_p$, comme

$$\mathbf{F}_q := \{x \in \bar{\mathbf{F}}_p \mid x^q = x\}$$

(c'est bien un sous-corps de $\bar{\mathbf{F}}_p$, puisque c'est l'ensemble des points fixes de l'automorphisme $\mathrm{F}_{\bar{\mathbf{F}}_p}^d$ de $\bar{\mathbf{F}}_p$).

Exemple 1.2. — Voici les tables d'addition et de multiplication du corps $\mathbf{F}_4$ (on a noté ses éléments $0, 1, a, b$) :

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

×	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Exercice 1.3. — Montrer que le groupe abélien $(\mathbf{F}_{p^d}, +)$ est isomorphe à $(\mathbf{Z}/p\mathbf{Z})^d$.

2. Le groupe linéaire

Soit $\mathbf{K}$ un corps (commutatif). On rappelle que $\mathrm{GL}_n(\mathbf{K})$ est le groupe des matrices $n \times n$ inversibles à coefficients dans $\mathbf{K}$ et que $\mathrm{SL}_n(\mathbf{K})$ est le sous-groupe distingué des matrices de déterminant 1.

Pour tous $i, j \in \{1, \ldots, n\}$, on a défini dans le §I.3.5 les matrices E_{ij} et, pour $i \neq j$ et $\alpha \in \mathbf{K}$, les matrices élémentaires $\mathrm{I}_n + \alpha \mathrm{E}_{ij}$. Ce sont des éléments de $\mathrm{SL}_n(\mathbf{K})$.

2.1. Centre. — Rappelons que le centre d'un groupe est le sous-groupe formé des éléments qui commutent avec tous les éléments du groupe. Il est clair que les homothéties $\lambda \mathrm{I}_n$, pour $\lambda \in \mathbf{K}^\times$, sont dans le centre de $\mathrm{GL}_n(\mathbf{K})$.

Proposition 2.1. — *Soit* $\mathbf{K}$ *un corps et soit* n *un entier* $\geqslant 2$.

1° Le centre de $\mathrm{GL}_n(\mathbf{K})$ *est réduit aux homothéties, c'est-à-dire* $\mathrm{Z}(\mathrm{GL}_n(\mathbf{K})) \simeq \mathbf{K}^\times$.

2° Le centre de $\mathrm{SL}_n(\mathbf{K})$ *est* $\mathrm{SL}_n(\mathbf{K}) \cap \mathrm{Z}(\mathrm{GL}_n(\mathbf{K}))$, *qui est isomorphe à* $\mu_n(\mathbf{K}) := \{\lambda \in \mathbf{K} \mid \lambda^n = 1\}$.

Démonstration. — Soit $\mathrm{A} = (a_{ij})$ une matrice de $\mathrm{GL}_n(\mathbf{K})$ qui commute à tous les éléments de $\mathrm{SL}_n(\mathbf{K})$. On a alors, pour tous $i \neq j$,

$$\mathrm{A}(\mathrm{I}_n + \mathrm{E}_{ij}) = (\mathrm{I}_n + \mathrm{E}_{ij})\mathrm{A},$$

c'est-à-dire $\mathrm{AE}_{ij} = \mathrm{E}_{ij}\mathrm{A}$. Or la matrice AE_{ij} est formée de la i-ème colonne de A placée comme j-ème colonne, avec des 0 ailleurs. De la même façon, la matrice $\mathrm{E}_{ij}\mathrm{A}$ est formée de la j-ème ligne de A placée comme i-ème ligne, avec des 0 ailleurs. On en déduit $a_{ii} = a_{jj}$, puis $a_{jk} = 0$ pour tout $k \neq j$, et $a_{li} = 0$ pour tout $l \neq i$. La matrice A est donc une homothétie.

Cela montre à la fois les deux énoncés de la proposition. □

2.2. Générateurs. — Nous avons étudié dans le § 4 des générateurs du groupes $\mathrm{GL}_n(\mathbf{Z})$ et $\mathrm{SL}_n(\mathbf{Z})$ en utilisant la réduction par opérations élémentaires d'une matrice à coefficients entiers. La même méthode s'applique aux matrices aux coefficients dans un corps quelconque (en plus facile, car étant dans un corps, on peut diviser par tout élément non nul !) pour démontrer le théorème suivant.

Théorème 2.2. — *Soit* $\mathbf{K}$ *un corps et soit* n *un entier* $\geqslant 2$.

1° Le groupe $\mathrm{SL}_n(\mathbf{K})$ *est engendré par les matrices élémentaires* $\mathrm{I}_n + \alpha \mathrm{E}_{ij}$, *pour* $i, j \in \{1, \ldots, n\}$, $i \neq j$ *et* $\alpha \in \mathbf{K}$.

2° Le groupe $\mathrm{GL}_n(\mathbf{K})$ *est engendré par les matrices précédentes et les matrices* $\mathrm{I}_n + (\lambda - 1)\mathrm{E}_{nn}$, *pour* $\lambda \in \mathbf{K}^\times$.

Exercice 2.3. — Montrer que $\mathrm{SL}_n(\mathbf{R})$ est connexe et que $\mathrm{GL}_n(\mathbf{R})$ a deux composantes connexes.

Exercice 2.4. — Montrer que $\mathrm{SL}_n(\mathbf{Q})$ est dense dans $\mathrm{SL}_n(\mathbf{R})$.

Exercice 2.5. — a) Soit p un nombre premier. Montrer que la réduction modulo p des coefficients d'une matrice induit un morphisme de groupes $\mathrm{SL}_n(\mathbf{Z}) \to \mathrm{SL}_n(\mathbf{Z}/p\mathbf{Z})$ qui est surjectif (*Indication :* on pourra utiliser le th. 2.2.1°).

b) Montrer que ce résultat reste vrai en remplaçant p par n'importe quel entier $\mathrm{N} \geqslant 2$.

2.3. Conjugaison, commutateurs. — Rappelons que le groupe dérivé d'un groupe est le sous-groupe engendré par ses commutateurs (§ I.5.3).

D'autre part, étant donnés un corps $\mathbf{K}$ et un entier $n \geqslant 1$, on définit le *groupe projectif linéaire*

$$\mathrm{PGL}_n(\mathbf{K}) := \mathrm{GL}_n(\mathbf{K})/\mathrm{Z}(\mathrm{GL}_n(\mathbf{K})) = \mathrm{PGL}_n(\mathbf{K})/\{\text{homothéties}\}$$

et son sous-groupe

$$\mathrm{PSL}_n(\mathbf{K}) := \mathrm{SL}_n(\mathbf{K})/\mathrm{Z}(\mathrm{SL}_n(\mathbf{K})) = \mathrm{PSL}_n(\mathbf{K})/\{\text{homothéties de déterminant 1}\}.$$

Leur centre est trivial par construction.

Théorème 2.6. *— Soit $\mathbf{K}$ un corps et soit n un entier $\geqslant 2$.*

1° On a $\mathrm{D}(\mathrm{SL}_n(\mathbf{K})) = \mathrm{SL}_n(\mathbf{K})$ (et donc $\mathrm{D}(\mathrm{PSL}_n(\mathbf{K})) = \mathrm{PSL}_n(\mathbf{K})$) sauf si $n = 2$ et $\mathbf{K} = \mathbf{F}_2$ ou $\mathbf{F}_3$.

2° On a $\mathrm{D}(\mathrm{GL}_n(\mathbf{K})) = \mathrm{SL}_n(\mathbf{K})$ (et donc $\mathrm{D}(\mathrm{PGL}_n(\mathbf{K})) = \mathrm{PSL}_n(\mathbf{K})$) sauf si $n = 2$ et $\mathbf{K} = \mathbf{F}_2$.

On verra plus bas que les groupes $\mathrm{GL}_2(\mathbf{F}_2) = \mathrm{SL}_2(\mathbf{F}_2)$ sont isomorphes au groupe symétrique $\mathfrak{S}_3$, dont le groupe dérivé est $\mathfrak{A}_3$. D'autre part, on peut montrer que le groupe $\mathrm{D}(\mathrm{SL}_2(\mathbf{F}_3))$ est d'indice 3 dans le groupe $\mathrm{SL}_2(\mathbf{F}_3)$. Ces cas sont donc bien des exceptions aux conclusions du théorème.

Démonstration. — Le déterminant d'un commutateur est 1, donc le groupe dérivé de $\mathrm{GL}_n(\mathbf{K})$ est toujours inclus dans $\mathrm{SL}_n(\mathbf{K})$. Pour montrer qu'il est égal, on montre que le groupe dérivé contient toutes les matrices élémentaires, et donc tout le groupe $\mathrm{SL}_n(\mathbf{K})$.

En utilisant la formule $\mathrm{E}_{ij}\mathrm{E}_{kl} = \delta_{jk}\mathrm{E}_{il}$, on obtient facilement les formules suivantes, pour i, j, k distincts :

$$\begin{aligned}(\mathrm{I}_n + \alpha\mathrm{E}_{ij})^{-1} &= \mathrm{I}_n - \alpha\mathrm{E}_{ij}\\ (\mathrm{I}_n + \alpha\mathrm{E}_{ij})(\mathrm{I}_n + \beta\mathrm{E}_{jk})(\mathrm{I}_n + \alpha\mathrm{E}_{ij})^{-1}(\mathrm{I}_n + \beta\mathrm{E}_{jk})^{-1} &= \mathrm{I}_n - \alpha\beta\mathrm{E}_{ik}.\end{aligned}$$

Cela montre le 1° (donc aussi le 2°) pour $n \geqslant 3$ (c'est nécessaire pour pouvoir choisir les trois indices i, j, k distincts).

Lorsque $n = 2$, il suffit de montrer que les matrices $\mathrm{I}_2 + \alpha\mathrm{E}_{12}$ et $\mathrm{I}_2 + \alpha\mathrm{E}_{21}$ sont des commutateurs.

On écrit les formules suivantes : pour $\beta \notin \{0, 1, -1\}$ (ce qui est possible si $|\mathbf{K}| > 3$), on a

$$\begin{pmatrix}\beta & 0\\ 0 & \beta^{-1}\end{pmatrix}\begin{pmatrix}1 & \frac{\alpha}{\beta^2-1}\\ 0 & 1\end{pmatrix}\begin{pmatrix}\beta & 0\\ 0 & \beta^{-1}\end{pmatrix}^{-1}\begin{pmatrix}1 & \frac{\alpha}{\beta^2-1}\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix},$$

(et une formule analogue pour $\mathrm{I} + \alpha\mathrm{E}_{21}$), ce qui montre le 1°, et pour $\beta \notin \{0, 1\}$, (ce qui est possible si $|\mathbf{K}| > 2$), on a

$$\begin{pmatrix}\beta & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & \frac{\alpha}{\beta-1}\\ 0 & 1\end{pmatrix}\begin{pmatrix}\beta & 0\\ 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}1 & \frac{\alpha}{\beta-1}\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & \alpha\\ 0 & 1\end{pmatrix},$$

ce qui montre le 2°. □

Exercice 2.7. *—* Soit $\mathbf{K}$ un corps et soit n un entier $\geqslant 2$. Quel est le groupe dérivé du groupe affine $\mathrm{GA}(\mathbf{K}^n)$ (*cf.* ex. 1.1.5°) ?

Exercice 2.8. — Soit K un corps fini et soit n un entier $\geqslant 1$. Décrire tous les morphismes de $\mathrm{GL}_n(\mathbf{K})$ dans $\mathbf{K}^\times$ (*Indication :* on pourra utiliser l'exerc. I.1.29).

Exercice 2.9. — Montrer que pour $n \geqslant 3$, le groupe dérivé $\mathrm{D}(\mathrm{SL}_n(\mathbf{Z}))$ est $\mathrm{SL}_n(\mathbf{Z})$ [1].

Comme annoncé plus haut, nous allons maintenant montrer que certains des « petits » groupes linéaires sont des groupes de permutations.

On a déjà défini dans l'ex. I.2.2.4° l'espace projectif $\mathbf{P}^{n-1}(\mathbf{K}) = \mathbf{K}^n - \{0\}/\mathbf{K}^\times$ des droites vectorielles de $\mathbf{K}^n$. En particulier,

$$\mathbf{P}^1(\mathbf{K}) = \{\mathbf{K}(x,1) \mid x \in \mathbf{K}\} \cup \{\mathbf{K}(1,0)\} \simeq \mathbf{K} \cup \{\infty\},$$

appelé droite projective, est constitué d'une copie de $\mathbf{K}$ et d'un « point à l'infini ».

L'action de $\mathrm{GL}_n(\mathbf{K})$ sur $\mathbf{K}^n$ induit une action sur $\mathbf{P}^{n-1}(\mathbf{K})$. Le noyau de l'action est constitué des automorphismes linéaires de $\mathbf{K}^n$ qui fixent chaque droite, c'est-à-dire des homothéties [2]. Par passage au quotient, on obtient ainsi une action fidèle du groupe projectif linéaire $\mathrm{PGL}_n(\mathbf{K})$ sur $\mathbf{P}^{n-1}(\mathbf{K})$.

Exemple 2.10 **(Homographies)**. — On représente souvent l'élément de $\mathbf{P}^{n-1}(\mathbf{K})$ correspondant à la droite vectorielle engendrée par le vecteur (non nul) $(x_1,\dots,x_n)$ de $\mathbf{K}^n$ par ses *coordonnées homogènes* $(x_1 : \dots : x_n)$ (on a $(x_1 : \dots : x_n) = (\lambda x_1 : \dots : \lambda x_n)$ pour tout $\lambda \in \mathbf{K}^\times$). Lorsque $n = 2$, la bijection $\mathbf{P}^1(\mathbf{K}) \simeq \mathbf{K} \cup \{\infty\}$ construite ci-dessus envoie $(x_1 : x_2)$ sur x_1/x_2 si $x_2 \neq 0$ et sur ∞ si $x_2 = 0$. Une matrice $\mathrm{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{K})$ agit sur $\mathbf{P}^1(\mathbf{K})$ en envoyant $(x_1 : x_2)$ sur $(ax_1 + bx_2 : cx_1 + dx_2)$. Via la bijection ci-dessus, elle agit donc sur $\mathbf{K} \cup \{\infty\}$ par (si par exemple $bc \neq 0$)

$$\begin{aligned} x \in \mathbf{K} - \{-d/c\} &\mapsto \frac{ax+b}{cx+d} \\ -d/c &\mapsto \infty \\ \infty &\mapsto a/c \end{aligned}$$

Plus généralement, on appelle *homographie* toute bijection de $\mathbf{P}^{n-1}(\mathbf{K})$ induite par l'action d'un élément de $\mathrm{GL}_n(\mathbf{K})$.

Exemples 2.11. — 1° Le groupe $\mathrm{GL}_n(\mathbf{R})$ (resp. $\mathrm{SL}_n(\mathbf{R})$) (resp. $\mathrm{PGL}_n(\mathbf{R})$) (resp. $\mathrm{PSL}_n(\mathbf{R})$) est une *variété différentiable* de dimension n^2 (resp. n^2-1) (resp. n^2-1) (resp. n^2-1).

2° Le groupe $\mathrm{GL}_n(\mathbf{C})$ (resp. $\mathrm{SL}_n(\mathbf{C})$) (resp. $\mathrm{PGL}_n(\mathbf{C})$) (resp. $\mathrm{PSL}_n(\mathbf{C})$) est une *variété complexe* de dimension n^2 (resp. n^2-1) (resp. n^2-1) (resp. n^2-1).

---

1. On peut montrer que $\mathrm{D}(\mathrm{SL}_2(\mathbf{Z}))$ est d'indice 12 dans $\mathrm{SL}_2(\mathbf{Z})$ (note I.14).

2. On utilise ici un petit argument classique : si u est un automorphisme linéaire d'un $\mathbf{K}$-espace vectoriel V qui fixe chaque droite vectorielle de V, alors, pour tout $x \in \mathrm{V}$ non nul, il existe $\lambda_x \in \mathbf{K}^\times$ tel que $u(x) = \lambda_x x$. Si x et y sont colinéaires, on a $\lambda_x = \lambda_y$; sinon, on écrit, par linéarité de u,

$$\lambda_{x+y}(x+y) = u(x+y) = u(x) + u(y) = \lambda_x x + \lambda_y y.$$

On en déduit $\lambda_{x+y} = \lambda_x = \lambda_y$, de sorte que u est une homothétie.

Dans le cas d'un corps fini, on a déjà vu dans l'exerc. I.1.24 les cardinaux de certains de ces groupes :

$$\begin{aligned} |\mathrm{GL}_n(\mathbf{F}_q)| &= q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q-1), \\ |\mathrm{SL}_n(\mathbf{F}_q)| = |\mathrm{PGL}_n(\mathbf{F}_q)| &= q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1), \end{aligned}$$

d'où on déduit, en utilisant la prop. 2.1.2° et le fait que $\mathbf{F}_q^\times$ est cyclique d'ordre $q-1$,

$$|\mathrm{PSL}_n(\mathbf{F}_q)| = \frac{|\mathrm{SL}_n(\mathbf{F}_q)|}{\mathrm{pgcd}(n,q-1)}.$$

En particulier, $|\mathrm{PSL}_2(\mathbf{F}_q)| = q(q^2-1)/\mathrm{pgcd}(2,q-1)$. Noter aussi les égalités

$$\mathrm{GL}_n(\mathbf{F}_2) = \mathrm{PGL}_n(\mathbf{F}_2) = \mathrm{SL}_n(\mathbf{F}_2) = \mathrm{PSL}_n(\mathbf{F}_2)$$

pour tout n (il n'y a qu'un seul déterminant non nul possible dans $\mathbf{F}_2$, à savoir 1, et une seule homothétie non nulle, l'identité !).

Nous avons indiqué dans le tableau ci-dessous les cardinaux des premiers de ces groupes, ainsi que les isomorphismes avec certains groupes de permutations [3] :

q	2			3	4		5	7	8	9
n	2	3	4	2	2	3	2	2	2	2
PSL	6 $\simeq \mathfrak{S}_3$	168	8!/2 $\simeq \mathfrak{A}_8$	12 $\simeq \mathfrak{A}_4$	60 $\simeq \mathfrak{A}_5$	8!/2 $\not\simeq \mathfrak{A}_8$	60 $\simeq \mathfrak{A}_5$	168 $\simeq \mathrm{PSL}_3(\mathbf{F}_2)$	504	6!/2 $\simeq \mathfrak{A}_6$
PGL				24 $\simeq \mathfrak{S}_4$	60 $\simeq \mathfrak{A}_5$		120 $\simeq \mathfrak{S}_5$			6! $\not\simeq \mathfrak{S}_6$
SL				24 $\not\simeq \mathfrak{S}_4$						

Certains de ces isomorphismes sont étonnants et pas faciles du tout à démontrer et encore moins à construire explicitement. D'autres sont plus simples à voir.

L'isomorphisme $\mathrm{PSL}_2(\mathbf{F}_2) \simeq \mathfrak{S}_3$ est facile : on a vu que $\mathbf{P}^1(\mathbf{F}_2)$ a 3 éléments ; le groupe $\mathrm{PSL}_2(\mathbf{F}_2)$ agit fidèlement sur cet ensemble, ce qui fournit un morphisme injectif

$$\mathrm{PSL}_2(\mathbf{F}_2) \longrightarrow \mathrm{Bij}(\mathbf{P}^1(\mathbf{F}_2)) \simeq \mathfrak{S}_3$$

qui, comme ces deux groupes ont le même ordre, est un isomorphisme.

De façon analogue, le groupe $\mathrm{PGL}_2(\mathbf{F}_3)$ agit fidèlement sur l'ensemble $\mathbf{P}^1(\mathbf{F}_3)$, qui a 4 éléments, ce qui fournit un morphisme injectif

$$\mathrm{PGL}_2(\mathbf{F}_3) \longrightarrow \mathfrak{S}_4$$

qui, comme ces deux groupes ont le même ordre, est un isomorphisme.

Le sous-groupe $\mathrm{PSL}_2(\mathbf{F}_3) < \mathrm{PGL}_2(\mathbf{F}_3)$ est d'indice 2 ; il est donc distingué dans $\mathfrak{S}_4$ (exerc. I.1.16) et isomorphe à $\mathfrak{A}_4$ (pourquoi ?).

3. On sait que ce sont les seuls tels isomorphismes (*cf.* Artin, E., The orders of the linear groups, *Comm. P. App. Math* **8** (1955), 355–365).

Exercice 2.12. — Montrer que les groupes $\mathrm{SL}_2(\mathbf{F}_3)$ et $\mathfrak{S}_4$ ne sont pas isomorphes (*Indication :* on pourra regarder leur centre).

Exercice 2.13. — Les groupes $\mathrm{PSL}_3(\mathbf{F}_4)$ et $\mathrm{PSL}_4(\mathbf{F}_2)$ ont même cardinal. Le but de cet exercice est de montrer qu'ils ne sont pas isomorphes.
a) Soit p un nombre premier. Montrer que pour toute puissance q de p, le sous-groupe $\mathrm{T}_n(\mathbf{F}_q)$ de $\mathrm{SL}_n(\mathbf{F}_q)$ formé des matrices triangulaires supérieures unipotentes (*cf.* ex. I.2.19) est un p-sous-groupe de Sylow de $\mathrm{SL}_n(\mathbf{F}_q)$ et que son image dans $\mathrm{PSL}_n(\mathbf{F}_q)$ est un p-sous-groupe de Sylow de $\mathrm{PSL}_n(\mathbf{F}_q)$.
b) Montrer que le centre de $\mathrm{T}_3(\mathbf{F}_4)$ est formé des matrices $\begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, pour $\alpha \in \mathbf{F}_4$.
c) Montrer que le centre de $\mathrm{T}_4(\mathbf{F}_2)$ est d'ordre 2. Conclure.

Exercice 2.14. — On rappelle (exerc. I.5.12) que le groupe dérivé $\mathrm{D}(\mathrm{SL}_2(\mathbf{Z}))$ est d'indice divisant $\leqslant 12$ dans $\mathrm{SL}_2(\mathbf{Z})$.
a) Montrer que $\mathrm{SL}_2(\mathbf{Z})$ a un quotient d'ordre 2 et un quotient d'ordre 3 (*Indication :* on pourra utiliser l'exerc. 2.5, pour $p = 2$ et 3).
b) En déduire que l'indice de $\mathrm{D}(\mathrm{SL}_2(\mathbf{Z}))$ dans $\mathrm{SL}_2(\mathbf{Z})$ est 6 ou 12 (on peut montrer que c'est 12 (*cf.* note I.14) ; comparer avec l'exerc. 2.9).

2.4. Simplicité. — Une des raisons de notre intérêt pour les groupes linéaires est qu'ils donnent lieu, lorsqu'ils sont finis, à des séries infinies de groupes simples (tout comme les groupes alternés ; *cf.* th. I.5.1).

Le but de cette section est de démontrer le résultat suivant.

Théorème 2.15. — *Soit* $\mathbf{K}$ *un corps. Le groupe* $\mathrm{PSL}_n(\mathbf{K})$ *est simple sauf si* $n = 2$, *et* $\mathbf{K} = \mathbf{F}_2$ *ou* $\mathbf{F}_3$.

Les exceptions ne sont effectivement pas simples : $\mathrm{PSL}_2(\mathbf{F}_2) \simeq \mathfrak{S}_3$ admet $\mathfrak{A}_3$ comme sous-groupe distingué propre, tandis que $\mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathfrak{A}_4$ admet un sous-groupe distingué d'indice 3 (ex. I.5.3.3°).

En prenant pour $\mathbf{K}$ un corps fini $\mathbf{F}_q$, on obtient donc ainsi une troisième série de groupes finis simples (les deux premières étant formées des groupes d'ordre premier d'un côté et des groupes alternés de l'autre) [4]. Il y a quelques coïncidences qui sont toutes indiquées dans le tableau p. 56.

Le premier nouveau groupe simple fini qu'on découvre dans ce tableau est donc le groupe $\mathrm{PSL}_3(\mathbf{F}_2)$, d'ordre 168 (*cf.* exerc. I.2.35). Le suivant est $\mathrm{PSL}_2(\mathbf{F}_8)$, d'ordre 504. Le plus petit groupe fini simple qui n'est ni cyclique, ni un groupe alterné, ni un groupe spécial linéaire est d'ordre 6048 ; c'est le groupe $\mathrm{PSU}_3(\mathbf{F}_9)$ qui sera défini dans le § 10.4 [5].

L'isomorphisme $\mathrm{PSL}_2(\mathbf{F}_7) \simeq \mathrm{PSL}_3(\mathbf{F}_2)$ découle abstraitement du fait que tous les groupes simples (*cf.* th. 2.15) d'ordre 168 sont isomorphes (de même, tous les groupes

4. Pour des raisons que vous comprendrez plus tard, le groupe $\mathrm{PSL}_n(\mathbf{F}_q)$ est aussi noté $\mathrm{A}_{n-1}(q)$.

5. Le suivant est le groupe de Mathieu M_{11}, de cardinal 7920, qui peut être défini comme le sous-groupe de $\mathfrak{S}_{11}$ engendré par le 11-cycle $(1,2,3,4,5,6,7,8,9,10,11)$ et la permutation $(3,7,11,8)(4,10,5,6)$. Il a été construit par Mathieu en 1861 (d'une autre façon !). C'est un des 26 groupes finis simples *sporadiques :* il ne fait pas partie d'une série infinie comme les groupes cycliques, alternés, ou projectifs spéciaux linéaires.

simples d'ordre 60 sont isomorphes (exerc. I.2.40), ce qui montre deux des isomorphismes du tableau) [6].

Ce n'est pas par hasard que les exceptions sont les mêmes dans les th. 2.6 et 2.15. En effet, on va présenter ici une démonstration où le second théorème est déduit du premier par la *méthode d'Iwasawa*, qui s'appuie sur l'action du groupe $\mathrm{PSL}_n(\mathbf{K})$ sur l'espace projectif $\mathbf{P}^{n-1}(\mathbf{K})$.

Plus généralement, supposons qu'un groupe G agisse sur un ensemble X. On dira que G agit *primitivement* sur X si

1° l'action de G sur X est transitive ;

2° le stabilisateur G_x d'un point de X (donc de tout point de X) est un sous-groupe maximal de G, c'est-à-dire que les seuls sous-groupes de G contenant G_x sont G_x et G.

Un cas particulier d'action primitive est donnée par une *action 2-transitive*, c'est-à-dire telle que

$$\forall x_1, x_2, y_1, y_2 \in \mathrm{X} \qquad (x_1 \neq x_2, y_1 \neq y_2 \implies \exists g \in \mathrm{G} \quad g \cdot x_1 = y_1 \quad g \cdot x_2 = y_2).$$

Autrement dit, l'action de G sur $\mathrm{X} \times \mathrm{X} - \Delta$, où $\Delta = \{(x, x) \mid x \in \mathrm{X}\}$, définie par $g \cdot (x, y) = (g \cdot x, g \cdot y)$ est transitive.

En effet, il suffit de vérifier qu'un stabilisateur G_x est un sous-groupe maximal. Soit donc $\mathrm{H} \leq \mathrm{G}$ un sous-groupe contenant strictement G_x et soit $h \in \mathrm{H} - \mathrm{G}_x$, de sorte que $y := h \cdot x \neq x$. Soit $g \in \mathrm{G} - \mathrm{G}_x$, de sorte que $z := g \cdot x \neq x$. Il existe alors $k \in \mathrm{G}$ tel que $k \cdot (x, z) = (x, y)$, c'est-à-dire $k \in \mathrm{G}_x$ et $k \cdot z = y$. Cette seconde relation s'écrit $(kg) \cdot x = h \cdot x$, c'est-à-dire $h^{-1}kg \in \mathrm{G}_x < \mathrm{H}$. Comme h et k sont dans H, on en déduit que tout élément g de $\mathrm{G} - \mathrm{G}_x$ est dans H, soit $\mathrm{H} = \mathrm{G}$.

Le théorème permettant de montrer la simplicité d'un groupe à partir d'une action primitive est le suivant.

Théorème 2.16. — *Supposons que le groupe* G *agisse primitivement sur* X. *Si on se donne, pour chaque* $x \in \mathrm{X}$, *un sous-groupe* $\mathrm{T}_x \leq \mathrm{G}$ *tel que*

1° T_x *est abélien ;*

2° $\mathrm{T}_{g \cdot x} = g\mathrm{T}_x g^{-1}$ *pour tout* $g \in \mathrm{G}$ *et tout* $x \in \mathrm{X}$ *;*

3° $\bigcup_{x \in \mathrm{X}} \mathrm{T}_x$ *engendre* G *;*

alors tout sous-groupe distingué de G *agissant non trivialement sur* X *contient* D(G).

Démonstration. — Soit H un sous-groupe distingué de G agissant non trivialement sur X et soit $x \in \mathrm{X}$. Puisque G_x est maximal, le sous-groupe $\mathrm{HG}_x \leq \mathrm{G}$ (*cf.* exerc. I.1.27) est égal soit à G_x, soit à G.

Dans le premier cas, on a $\mathrm{H} \leq \mathrm{G}_x$ donc, pour tout $g \in \mathrm{G}$,

$$\mathrm{H} = g\mathrm{H}g^{-1} \leq g\mathrm{G}_x g^{-1} = \mathrm{G}_{g \cdot x}$$

ce qui, puisque G agit transitivement sur X, contredit le fait que H n'agit pas trivialement sur X.

6. Dans le même ordre d'idées, on sait que les seuls groupes simples d'ordre $8!/2$ sont (à isomorphisme près) $\mathfrak{A}_8 \simeq \mathrm{PSL}_4(\mathbf{F}_2)$ et $\mathrm{PSL}_3(\mathbf{F}_4)$.

On a donc $\mathrm{HG}_x = \mathrm{G}$. Comme l'action de G sur X est transitive, on a

$$\mathrm{X} = \mathrm{G}\cdot x = \mathrm{HG}_x \cdot x = \mathrm{H}\cdot x,$$

donc l'action de H sur X reste transitive. Montrons qu'en outre $\mathrm{G} = \mathrm{HT}_x$. En effet, si $h \in \mathrm{H}$, on a par 2°

$$\mathrm{T}_{h\cdot x} = h\mathrm{T}_x h^{-1} \subseteq \mathrm{HT}_x\mathrm{H} = \mathrm{HT}_x,$$

puisque $\mathrm{H} \trianglelefteq \mathrm{G}$. Puisque H agit transitivement sur X, on a donc $\mathrm{T}_y \leq \mathrm{HT}_x$ pour tout $y \in \mathrm{X}$, donc $\mathrm{G} = \mathrm{HT}_x$ puisque les $(\mathrm{T}_y)_{y\in\mathrm{X}}$ engendrent G par 3°.

Finalement,

$$\mathrm{G}/\mathrm{H} = \mathrm{HT}_x/\mathrm{H} \simeq \mathrm{T}_x/(\mathrm{H}\cap\mathrm{T}_x)$$

(exerc. I.1.27) est abélien puisque T_x l'est, de sorte que $\mathrm{H} \supseteq \mathrm{D}(\mathrm{G})$. □

Nous aurons encore besoin d'une autre définition. Soit a un élément non nul d'un **K**-espace vectoriel V de dimension finie n. On appelle *transvection* de vecteur a tout automorphisme de V de la forme

$$x \mapsto x + \ell(x)a,$$

où $\ell : \mathrm{V} \to \mathbf{K}$ est une forme linéaire telle que $\ell(a) = 0$ (si $\ell \neq 0$ et $\mathrm{H} := \ker(\ell)$, on dit aussi transvection d'hyperplan H ; notons que la transvection est l'identité sur H). On note cet automorphisme $\tau(\ell, a)$. On vérifie que

$$\tau(0,a) = \mathrm{Id}_\mathrm{V} \quad \text{et} \quad \tau(\ell,a)\circ\tau(\ell',a) = \tau(\ell+\ell',a),$$

de sorte que les transvections de vecteur a forment un sous-groupe abélien de GL(V).

Si $u \in \mathrm{GL}(\mathrm{V})$, le conjugué

$$u\circ\tau(\ell,a)\circ u^{-1} = \tau(\ell\circ u^{-1}, u(a))$$

est une transvection de vecteur $u(a)$ et d'hyperplan $u(\mathrm{H})$.

Enfin, si $\ell \neq 0$, on choisit une base $(a, e_2, \ldots, e_{n-1})$ de $\ker(\ell)$, que l'on complète en une base de V par un vecteur e_n. La matrice de $\tau(\ell, a)$ dans cette base est la matrice élémentaire $\mathrm{I}_n + \ell(e_n)\mathrm{E}_{1n}$. Toutes les matrices élémentaires sont en fait des matrices de transvection. Il résulte du th. 2.2.2° que les transvections engendrent SL(V).

Nous pouvons maintenant démontrer le th. 2.15.

Démonstration du th. 2.15. — L'action de $\mathrm{PSL}_n(\mathbf{K})$ sur $\mathrm{X} = \mathbf{P}^{n-1}(\mathbf{K})$ est fidèle et 2-transitive (il suffit en effet de remarquer qu'étant données des paires de points distincts de $\mathbf{P}^{n-1}(\mathbf{K})$, correspondant à des paires $(\mathrm{D}_1, \mathrm{D}_2)$ et $(\mathrm{D}'_1, \mathrm{D}'_2)$ de droites distinctes de $\mathbf{K}^n$, il existe un automorphisme linéaire de $\mathbf{K}^n$ qui envoie D_1 sur D'_1 et D_2 sur D'_2) donc primitive.

Pour chaque $x \in \mathbf{P}^{n-1}(\mathbf{K})$, correspondant à une droite vectorielle $\mathrm{D} \subseteq \mathbf{K}^n$, on prend pour groupe T_x le groupe des transvections de $\mathbf{K}^n$ de vecteur un générateur de D. Comme on vient de l'expliquer, toutes les hypothèses du th. 2.16 sont vérifiées, donc un sous-groupe distingué de $\mathrm{PSL}_n(\mathbf{K})$, non réduit à {Id}, doit contenir $\mathrm{D}(\mathrm{PSL}_n(\mathbf{K})) = \mathrm{PSL}_n(\mathbf{K})$ (th. 2.6). □

Exercice 2.17. — a) Vérifier que les groupes $\mathfrak{A}_3$ et $\mathfrak{A}_4$ sont des quotients de $\mathrm{SL}_2(\mathbf{F}_3)$ et le groupe $\mathfrak{A}_5$ est un quotient de $\mathrm{SL}_2(\mathbf{F}_5)$.

b) Montrer que pour $m \geqslant 6$, le groupe $\mathfrak{A}_m$ n'est un quotient d'aucun groupe $\mathrm{SL}_2(\mathbf{F}_p)$ (*Indication :* on pourra utiliser les exerc. I.5.1 et I.5.7) [7].

***Exercice 2.18* (Une autre démonstration de la simplicité de $\mathrm{PSL}_n(\mathbf{K})$ pour $n \geqslant 3$)**

Soit G un sous-groupe distingué de $\mathrm{SL}_n(\mathbf{K})$ contenant strictement le centre $\mathrm{Z}(\mathrm{SL}_n(\mathbf{K}))$ et soit g un élément de G qui n'est pas une homothétie. On suppose $n \geqslant 3$.

a) Montrer que les transvections de $\mathbf{K}^n$ engendrent $\mathrm{SL}_n(\mathbf{K})$. En déduire qu'il existe une transvection τ, de vecteur a, avec laquelle g ne commute pas. On pose $h := g\tau g^{-1}\tau^{-1} \neq \mathrm{Id}$.

b) Pour tout $x \in \mathbf{K}^n$, montrer que $h(x) - x$ est combinaison linéaire de a et $g(a)$. Soit H un hyperplan de $\mathbf{K}^n$ contenant ces vecteurs (il en existe car $n \geqslant 3$). Montrer $h(\mathrm{H}) = \mathrm{H}$.

c) On suppose qu'il existe une transvection d'hyperplan H ne commutant pas avec h. Montrer que G contient une transvection autre que l'identité (*Indication :* on pourra considérer le commutateur de h et la transvection).

d) On suppose maintenant au contraire que h commute avec toutes les transvections d'hyperplan H. Montrer que h est une transvection.

e) Montrer que les transvections de $\mathbf{K}^n$ autres que l'identité sont toutes conjuguées dans $\mathrm{SL}_n(\mathbf{K})$. En déduire $\mathrm{G} = \mathrm{SL}_n(\mathbf{K})$.

***Exercice 2.19* (Une autre démonstration de la simplicité de $\mathrm{PSL}_2(\mathbf{K})$ pour $|\mathbf{K}| \notin \{2,3,5\}$)**

Soit G un sous-groupe distingué de $\mathrm{SL}_2(\mathbf{K})$.

a) On suppose que tout élément de G s'écrit $\mathrm{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $a \neq 0$. Montrer que tout élément de G est diagonal, puis que $\mathrm{G} \subseteq \{\mathrm{I}_2, -\mathrm{I}_2\}$ (*Indication :* on pourra calculer $(\mathrm{I}_2 + t\mathrm{E}_{12})\mathrm{M}(\mathrm{I}_2 + t\mathrm{E}_{12})^{-1}$ et $(\mathrm{I}_2 + t\mathrm{E}_{21})\mathrm{M}(\mathrm{I}_2 + t\mathrm{E}_{21})^{-1}$).

b) On suppose au contraire que G contient une matrice du type $\mathrm{M} = \begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix}$. Soient $\alpha, \beta, \gamma \in \mathbf{K}$, avec $\beta \neq 0$. On pose $\mathrm{P}_{\alpha,\beta} := \begin{pmatrix} \alpha & \beta \\ -\beta^{-1} & 0 \end{pmatrix}$. Calculer

$$\begin{aligned} \mathrm{M}' &:= \mathrm{M}\mathrm{P}_{\alpha,\beta}\mathrm{M}^{-1}\mathrm{P}_{\alpha,\beta}^{-1}, \\ \mathrm{M}'' &:= \mathrm{M}'(\mathrm{I}_2 + \gamma\mathrm{E}_{12})\mathrm{M}'^{-1}(\mathrm{I}_2 + \gamma\mathrm{E}_{12})^{-1}, \\ \mathrm{M}''' &:= \mathrm{P}_{0,1}\mathrm{M}''\mathrm{P}_{0,1}^{-1}. \end{aligned}$$

En déduire que si $|\mathbf{K}| \notin \{2,3,5\}$, on a $\mathrm{G} = \mathrm{SL}_2(\mathbf{K})$.

c) Conclure.

***Exercice 2.20* (Une autre démonstration de la simplicité de $\mathrm{PSL}_2(\mathbf{F}_5)$)**

On peut montrer par des calculs du même type que ceux de l'exercice précédent que $\mathrm{PSL}_2(\mathbf{F}_5)$ est simple, conformément au th. 2.15. On peut aussi le démontrer de la façon suivante.

a) Montrer qu'il existe un morphisme injectif $\mathrm{PGL}_2(\mathbf{F}_5) \to \mathfrak{S}_6$.

b) En déduire que $\mathrm{PGL}_2(\mathbf{F}_5)$ est isomorphe à $\mathfrak{S}_5$ (*Indication :* on pourra calculer les ordres des groupes en présence et utiliser l'exerc. I.2.43).

---

7. On peut montrer que pour $m \geqslant 6$, le groupe $\mathfrak{A}_m$ n'est un quotient d'aucun groupe $\mathrm{SL}_2(\mathbf{Z}/\mathrm{N}\mathbf{Z})$ pour $\mathrm{N} \geqslant 2$, mais que pour $m \geqslant 9$, le groupe $\mathfrak{A}_m$ est en revanche quotient de $\mathrm{SL}_2(\mathbf{Z})$. Comme l'application de restriction $r_\mathrm{N} := \mathrm{SL}_2(\mathbf{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbf{Z}/\mathrm{N}\mathbf{Z})$ est surjective, le noyau de l'application $\mathrm{SL}_2(\mathbf{Z}) \twoheadrightarrow \mathfrak{A}_m$ est un sous-groupe (distingué) de $\mathrm{SL}_2(\mathbf{Z})$, d'indice fini, qui ne contient aucun $\ker(r_\mathrm{N}) = \{\mathrm{M} \in \mathrm{SL}_2(\mathbf{Z}) \mid \mathrm{M} \equiv \mathrm{I}_2 \pmod{\mathrm{N}}\}$. On dit que ce n'est pas un sous-groupe de congruence (l'existence de ces sous-groupes a été annoncée par Klein en 1879 et publiée indépendamment par Fricke et Pick en 1887). En revanche, c'est un théorème difficile de Bass, Lazard et Serre de 1964 que pour $n \geqslant 3$, tout sous-groupe de $\mathrm{SL}_n(\mathbf{Z})$ d'indice fini est un sous-groupe de congruence.

c) En déduire que $\mathrm{PSL}_2(\mathbf{F}_5)$ est isomorphe à $\mathfrak{A}_5$. C'est donc un groupe simple par le th. I.5.1.

3. Formes bilinéaires et quadratiques

Soit V un **K**-espace vectoriel. Dans cette section, on introduit les types de formes bilinéaires que l'on va étudier.

3.1. Définitions. — Une *forme bilinéaire* sur V est une application $b : \mathrm{V} \times \mathrm{V} \to \mathbf{K}$ telle que, pour chaque $y \in \mathrm{V}$, les applications partielles $x \mapsto b(x,y)$ et $x \mapsto b(y,x)$ sont **K**-linéaires. Une telle forme est

– *symétrique* si $b(x,y) = b(y,x)$ pour tous $x, y \in \mathrm{V}$;
– *alternée* si $b(x,x) = 0$ pour tout $x \in \mathrm{V}$.

Cette dernière condition entraîne (et, si $\mathrm{car}(\mathbf{K}) \neq 2$, lui est équivalente) le fait que b est

– *antisymétrique*, c'est-à-dire qu'elle vérifie $b(x,y) = -b(y,x)$ pour tous $x, y \in \mathrm{V}$.

Étant donnée une forme bilinéaire symétrique b, on définit la *forme quadratique* associée

$$f(x) := b(x,x).$$

On a alors

$$f(x+y) = f(x) + 2b(x,y) + f(y).$$

Si $\mathrm{car}(\mathbf{K}) \neq 2$ [8], on récupère la forme b à partir de f par la formule

$$b(x,y) = \frac{1}{2}(f(x+y) - f(x) - f(y)) \tag{20}$$

dite « de polarisation ».

Si V est de dimension finie n, la *matrice* M de la forme bilinéaire b dans une base $(e_1, \ldots, e_n)$ de V est la matrice $(b(e_i, e_j))_{1 \leqslant i,j \leqslant n}$. Si des éléments de V sont représentés par les vecteurs colonnes X et Y, alors $b(\mathrm{X}, \mathrm{Y}) = {}^t\mathrm{XMY}$. La forme b est (anti)symétrique si et seulement si la matrice M est (anti)symétrique. Si P est la matrice de passage de la base (e_i) à une base (e'_i), la matrice de b dans la nouvelle base est donnée par

$$\mathrm{M}' = {}^t\mathrm{PMP}.$$

Supposons b symétrique et notons f la forme quadratique associée. Si $\det(\mathrm{M}) \neq 0$, la classe de $\det(\mathrm{M})$ dans le groupe multiplicatif quotient $\mathbf{K}^\times / \mathbf{K}^{\times 2}$ est bien définie et s'appelle le *discriminant* de f, noté $\mathrm{disc}(f)$. Quand $\det(\mathrm{M}) = 0$, on convient que le discriminant est nul aussi [9].

La forme quadratique f est donnée par la formule

$$f(x_1 e_1 + \cdots + x_n e_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j,$$

8. Si $\mathrm{car}(\mathbf{K}) = 2$, il faut définir une forme quadratique sur V comme une application $f : \mathrm{V} \to \mathbf{K}$ telle que l'application $(x,y) \mapsto f(x+y) - f(x) - f(y)$ soit bilinéaire.

9. Cette notion n'a pas d'intérêt dans le cas alterné car nous verrons plus tard que $\det(\mathrm{M})$ est toujours un carré.

où $a_{ii} = f(e_i) = b(e_i, e_i)$ et $a_{ij} = 2b(e_i, e_j)$ si $i < j$. En d'autres termes, une forme quadratique sur un espace vectoriel de dimension finie est donnée par un *polynôme homogène de degré 2* en les composantes d'un vecteur [10].

3.2. Quadriques. — Attention de ne pas étendre aux formes bilinéaires symétriques générales les propriétés que vous pouvez connaître des *produits scalaires*. Ceux-ci correspondent au cas des formes bilinéaires symétriques définies positives sur un espace vectoriel réel, ce qui est un cas très particulier.

Il faut plutôt penser à une forme quadratique en termes géométriques de la façon suivante. Une *quadrique affine* $\mathrm{Q} \subseteq \mathbf{K}^n$ est définie par une équation polynomiale de degré 2

$$f_2(x_1, \ldots, x_n) + f_1(x_1, \ldots, x_n) + f_0 = 0,$$

où f_i est un polynôme homogène de de degré i. L'homogénéisé

$$f(x_0, x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n) + f_1(x_1, \ldots, x_n)x_0 + f_0 x_0^2$$

est une forme quadratique sur $\mathbf{K}^{n+1}$. L'équation $f(x_0, x_1, \ldots, x_n) = 0$ définit un cône quadratique $\mathrm{C} \subseteq \mathbf{K}^{n+1}$ (et Q est l'intersection de C avec l'hyperplan affine d'équation $x_0 = 1$) mais aussi une quadrique projective

$$\bar{\mathrm{Q}} := \{(x_0 : x_1 : \ldots : x_n) \in \mathbf{P}^n(\mathbf{K}) \mid f(x_0, x_1, \ldots, x_n) = 0\}$$

(noter que l'annulation de $f(x_0, x_1, \ldots, x_n)$ ne dépend pas du choix des coordonnées homogènes $(x_0 : x_1 : \ldots : x_n)$). Bien sûr, cette quadrique peut être vide, comme par exemple la quadrique d'équation $x_0^2 + \cdots + x_n^2 = 0$ dans $\mathbf{P}^n(\mathbf{R})$ ou la quadrique d'équation $x_0^2 + x_1^2 - 3x_2^2 = 0$ dans $\mathbf{P}^2(\mathbf{Q})$.

L'application injective

$$\begin{array}{ccc} \mathbf{K}^n & \longrightarrow & \mathbf{P}^n(\mathbf{K}) \\ (x_1, \ldots, x_n) & \longmapsto & (1 : x_1 : \ldots : x_n) \end{array}$$

identifie $\mathbf{K}^n$ avec le sous-ensemble de $\mathbf{P}^n(\mathbf{K})$ défini par $x_0 \neq 0$. On retrouve la quadrique affine Q comme l'intersection de $\bar{\mathrm{Q}}$ avec ce sous-ensemble.

Exemples 3.1. — Considérons dans $\mathbf{R}^2$ la conique Q d'équation

$$x_1^2 - x_2^2 + 2x_2 + 1 = 0.$$

L'homogénéisé est $f(x_0, x_1, x_2) := x_1^2 - x_2^2 + 2x_0x_2 + x_0^2$ et définit une conique projective $\bar{\mathrm{Q}} \subseteq \mathbf{P}^2(\mathbf{R})$. Il y a deux points « à l'infini » (c'est-à-dire avec $x_0 = 0$), à savoir $(0 : 1 : 1)$ et $(0 : 1 : -1)$. Ils correspondent aux deux asymptotes de l'hyperbole Q.

10. Cette formulation reste d'ailleurs valable en caractéristique 2.

3.3. Formes non dégénérées. — Soit b une forme bilinéaire symétrique ou alternée sur un espace vectoriel V de dimension finie sur un corps **K** de caractéristique $\neq 2$.

On note $\hat{b} : \mathrm{V} \to \mathrm{V}^*$ l'application linéaire qui à $x \in \mathrm{V}$ associe la forme linéaire $y \mapsto b(x,y)$.

On définit le *noyau* de b comme celui de $\hat{b}$, c'est-à-dire

$$\ker(b) := \{x \in \mathrm{V} \mid \forall y \in \mathrm{V} \quad b(x,y) = 0\} = \{y \in \mathrm{V} \mid \forall x \in \mathrm{V} \quad b(x,y) = 0\}$$

et on dit que b est *non dégénérée* si $\ker(b) = 0$. On appelle souvent *forme symplectique* une forme alternée non dégénérée.

On définit le *rang* de b comme celui de $\hat{b}$. La matrice de $\hat{b}$ dans une base de V et sa base duale dans V^* est la matrice de b comme définie plus haut. En particulier, le rang de b est le rang de cette matrice.

Proposition 3.2. *— Les conditions suivantes sont équivalentes :*

1° *b est non dégénérée ;*

2° *l'application linéaire $\hat{b} : \mathrm{V} \to \mathrm{V}^*$ est bijective ;*

3° *la matrice de b dans une base de* V *est inversible, c'est-à-dire que le rang de b est la dimension de* V.

Démonstration. — La première condition est exactement que $\hat{b}$ soit injective. Comme V est de dimension finie, c'est équivalent à dire que $\hat{b}$ est bijective, c'est-à-dire la seconde condition, ou encore surjective, ce qui donne la troisième condition. □

La restriction de b à tout supplémentaire de $\ker(b)$ dans V est non dégénérée. Cela permet de se ramener à une forme non dégénérée, ce qu'on fera le plus souvent.

3.4. Groupe d'isométries. — Soient V et V' des espaces vectoriels sur un corps **K** *de caractéristique $\neq 2$* équipés de formes b et b' de même type (symétriques ou alternées). Une application linéaire *injective* $u : \mathrm{V} \to \mathrm{V}'$ est une *isométrie* si, pour tous $x, y \in \mathrm{V}$, on a

$$b'(u(x), u(y)) = b(x,y).$$

Si b et b' sont des formes bilinéaires symétriques, de formes quadratiques associées f et f', il suffit que

$$f'(u(x)) = f(x)$$

pour tout $x \in \mathrm{V}$.

Si b est non dégénérée, l'injectivité découle de la propriété d'isométrie. Si en outre $(\mathrm{V}', b') = (\mathrm{V}, b)$, toute isométrie est un isomorphisme et l'ensemble des isométries forme un groupe pour la composition. L'appellation habituelle de ce groupe est différente suivant les cas :

– pour une forme quadratique f, le *groupe orthogonal* $\mathrm{O}(\mathrm{V}, f)$;

– pour une forme alternée b, le *groupe symplectique* $\mathrm{Sp}(\mathrm{V}, b)$.

Dans tous les cas, si M est la matrice de la forme b dans une base, une matrice U représente une isométrie si ${}^t\mathrm{UMU} = \mathrm{M}$.

Comme b est non dégénérée, cela implique $\det(\mathrm{U})^2 = 1$ donc $\det(\mathrm{U}) = \pm 1$. Le *groupe spécial orthogonal* est alors défini comme $\mathrm{SO}(\mathrm{V}, f) := \mathrm{O}(\mathrm{V}, f) \cap \mathrm{SL}(\mathrm{V})$.

Le groupe symplectique n'a pas de forme « spéciale » car il est déjà inclus dans SL(V), comme on le verra plus loin (cor. 7.2).

4. Orthogonalité

Dans la suite, b désignera une forme bilinéaire *symétrique ou alternée* sur un espace vectoriel V *de dimension finie* sur un corps $\mathbf{K}$ *de caractéristique* $\neq 2$.

4.1. Définition. — On dit que des vecteurs x et y sont *orthogonaux* si $b(x,y)=0$; vu les propriétés de b, c'est la même chose que de demander $b(y,x)=0$: c'est donc une relation symétrique. L'*orthogonal* d'une partie W de V est le sous-espace vectoriel, noté $\mathrm{W}^\perp$, des vecteurs de V orthogonaux à tous les éléments de W. On a par exemple $\ker(b)=\mathrm{V}^\perp$.

Proposition 4.1. — *Si b est* non dégénérée *et que* W *est un sous-espace vectoriel de* V*, on a*

$$\dim(\mathrm{W})+\dim(\mathrm{W}^\perp)=\dim(\mathrm{V}).$$

En particulier, si $\mathrm{W}\cap\mathrm{W}^\perp=0$ *(ce qui est équivalent à* $b|_\mathrm{W}$ *non dégénérée),* $\mathrm{V}=\mathrm{W}\oplus\mathrm{W}^\perp$.

Démonstration. — L'application linéaire $r:\mathrm{V}^*\to\mathrm{W}^*$ de restriction des formes linéaires est surjective, donc la composée

$$\begin{array}{rcl} r\circ\hat{b}:\mathrm{V} & \to & \mathrm{W}^* \\ x & \mapsto & b(x,\cdot) \end{array}$$

est linéaire surjective. Or $\ker(r\circ\hat{b})=\mathrm{W}^\perp$, d'où la formule sur la dimension en écrivant que la dimension de V est la somme des dimensions du noyau et de l'image de $r\circ\hat{b}$. □

Voici quelques formules sur l'orthogonal (la seconde est vraie aussi en dimension infinie) :

$$(\mathrm{W}^\perp)^\perp=\mathrm{W},\quad (\mathrm{W}+\mathrm{W}')^\perp=\mathrm{W}^\perp\cap\mathrm{W}'^\perp,\quad (\mathrm{W}\cap\mathrm{W}')^\perp=\mathrm{W}^\perp+\mathrm{W}'^\perp.$$

On dit qu'un vecteur $x\in\mathrm{V}$ est *isotrope* si $b(x,x)=0$, c'est-à-dire si $x\in x^\perp$. On dit aussi que la droite $\mathbf{K}x$ est isotrope.

Un sous-espace vectoriel $\mathrm{W}\subseteq\mathrm{V}$ est *totalement isotrope* si $b|_\mathrm{W}=0$, ce qui est équivalent à $\mathrm{W}\subseteq\mathrm{W}^\perp$.

Exemple 4.2. — Comme on l'a vu dans le § 3.2, une forme quadratique f sur $\mathbf{K}^{n+1}$ définit une quadrique projective $\bar{\mathrm{Q}}\subseteq\mathbf{P}^n(\mathbf{K})$. Les points de Q sont en bijection avec les droites vectorielles $\mathrm{D}\subseteq\mathbf{K}^{n+1}$ isotropes pour f.

Si $\mathbf{K}=\mathbf{R}$, l'orthogonal $\mathrm{D}^\perp$ correspond à l'espace tangent à $\bar{\mathrm{Q}}$ en ce point ; cela résute de la formule

$$df(x)(y)=2b(x,y)$$

donnant la différentielle de f en x, obtenue en différentiant la formule de polarisation (20).

Dans l'ex. 3.1 de la conique Q d'équation $x_1^2-x_2^2+2x_2+1=0$ dans $\mathbf{K}^2$, si (a_1,a_2) est un point de Q, la droite $\mathbf{R}(1,a_1,a_2)$ est isotrope pour f (elle définit un point de $\bar{\mathrm{Q}}$) et son orthogonal pour f est défini par

$$a_1x_1-a_2x_2+x_2+a_2x_0+x_0=0.$$

La droite tangente à Q en (a_1,a_2) a donc pour équation affine $a_1x_1-a_2x_2+x_2+a_2+1=0$.

4.2. Décomposition en somme directe orthogonale : cas d'un vecteur non isotrope. — Si la forme symétrique b n'est pas nulle, il résulte de la formule (20) qu'il existe un vecteur non isotrope x. Dans ce cas, on a $\mathbf{K}x \cap x^\perp = 0$ donc $\mathrm{V} = \mathbf{K}x \oplus x^\perp$. Par récurrence sur la dimension, en considérant la restriction de b à $x^\perp$, on obtient l'existence d'une *base orthogonale* $(e_1, \dots, e_n)$, c'est-à-dire satisfaisant $b(e_i, e_j) = 0$ si $i \neq j$. Posant $\alpha_i = b(e_i, e_i)$, on obtient

$$f(x_1, \dots, x_n) = \alpha_1 x_1^2 + \cdots + \alpha_r x_r^2,$$

avec $0 \leqslant r \leqslant n$ et $\alpha_1, \dots, \alpha_r$ non nuls ; c'est la *réduction de Gauss* de la forme quadratique f. L'entier r ne dépend que de la forme f car c'est son rang.

Dans la base $(a_1 e_1, \dots, a_n e_n)$, où $a_i \in \mathbf{K}^\times$, les coefficients α_i deviennent $\alpha_i a_i^2$. Si $\alpha_1, \dots, \alpha_n$ sont des scalaires non nuls, il est d'usage de noter la forme quadratique non dégénérée $(x_1, \dots, x_n) \mapsto \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2$ sur $\mathbf{K}^n$ par le symbole

$$\langle \alpha_1, \dots, \alpha_n \rangle$$

et l'isométrie entre deux telles formes par le symbole $\simeq$. Pour tous scalaires non nuls $a_1, \dots, a_n$, on a donc

$$\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle a_1^2 \alpha_1, \dots, a_n^2 \alpha_n \rangle.$$

En d'autres termes, on peut considérer que les α_i sont dans $\mathbf{K}^\times / \mathbf{K}^{\times 2}$. On a $\mathrm{disc}(\langle \alpha_1, \dots, \alpha_n \rangle) = \alpha_1 \cdots \alpha_n$.

Le problème de la classification des formes quadratiques est de savoir quand des formes $\langle \alpha_1, \dots, \alpha_n \rangle$ et $\langle \beta_1, \dots, \beta_n \rangle$ sont isométriques, avec $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbf{K}^\times / \mathbf{K}^{\times 2}$. Une condition nécessaire est que les discriminants soient les mêmes, $\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_n$ dans $\mathbf{K}^\times / \mathbf{K}^{\times 2}$, mais elle n'est en général pas suffisante.

Exemples 4.3. — 1° Si $\mathbf{K}$ est un corps algébriquement clos (ou plus généralement si $\mathbf{K}$ est *quadratiquement clos,* c'est-à-dire $\mathbf{K} = \mathbf{K}^2$), on peut toujours trouver a_i tel que $a_i^2 = 1/\alpha_i$. Il en résulte qu'étant donnée une forme quadratique non dégénérée f sur $\mathbf{K}^n$, il existe une base dans laquelle elle s'écrit

$$f(x) = x_1^2 + \cdots + x_n^2.$$

Son groupe orthogonal (indépendant donc de f) est noté $\mathrm{O}_n(\mathbf{K})$.

2° Si $\mathbf{K} = \mathbf{R}$, on peut toujours trouver a_i tel que $a_i^2 = \pm 1/\alpha_i$. En réordonnant la base, on déduit qu'étant donnée une forme quadratique non dégénérée f sur $\mathbf{R}^n$, il existe une base dans laquelle elle s'écrit

$$f(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_n^2.$$

Le couple $(s, n-s)$ est la signature de f ; on verra plus loin (ex. 5.6.1°) que c'est un invariant de f. Son groupe orthogonal est noté $\mathrm{O}_{s,n-s}(\mathbf{R})$ et on note $\mathrm{O}_n(\mathbf{R})$ au lieu de $\mathrm{O}_{n,0}(\mathbf{R})$. Comme les groupes orthogonaux de f et de $-f$ sont les mêmes, on a $\mathrm{O}_{s,t}(\mathbf{R}) \simeq \mathrm{O}_{t,s}(\mathbf{R})$. Le discriminant est $(-1)^{n-s}$ donc ne suffit pas à distinguer les formes quadratiques.

3° Si $\mathbf{K} = \mathbf{F}_q$, alors $\mathbf{F}_q^\times / \mathbf{F}_q^{\times 2}$ est d'ordre 2 (car, q étant impair, le noyau de $x \mapsto x^2$ dans $\mathbf{F}_q^\times$ est $\{\pm 1\}$). Donc on peut ramener chaque α_i non nul à être égal à 1 ou à $\alpha \notin \mathbf{F}_q^{\times 2}$. Mais on peut en fait faire mieux.

Remarque 4.4 **(Sommes de puissances)**. — Supposons $\mathbf{K} = \mathbf{C}$. La réduction de Gauss nous dit qu'on peut décomposer tout polynôme à coefficients complexes en n variables,

homogène de degré 2, en somme de carrés d'au plus n formes linéaires. On peut se demander plus généralement si on peut décomposer un polynôme P en n variables, homogène de degré d, en somme de puissances d-ièmes de s formes linéaires

$$\mathrm{P} = \ell_1^d + \cdots + \ell_s^d.$$

À d fixé, c'est vrai pour s assez grand. Plus exactement, Alexander et Hirschowitz ont montré en 1995 que lorsque $d \geqslant 3$ et que P est « général » (en un sens que je ne préciserai pas ; disons pour P choisi au hasard), on peut prendre pour s le plus petit entier supérieur à $\frac{1}{n}\binom{n+d-1}{d}$, sauf si $(d,n) \in \{(3,5),(4,3),(4,4),(4,5)\}$, où il faut ajouter 1 à ce nombre (ces exceptions étaient connues depuis le XX$^{\text{ème}}$ siècle ; d'autre part, Sylvester avait déjà démontré en 1851qu'une forme cubique *générale* en 4 variables s'écrit comme somme des cubes de 5 formes linéaires, et ceci de façon unique).

En revanche, pour certains polynômes P, la valeur minimale de s peut être bien sûr strictement inférieure à ce nombre (par exemple pour $\mathrm{P}(x) = x_1^d$!) mais aussi, ce qui est plus surprenant, strictement supérieure. On ne sait pas déterminer la valeur minimale de s pour laquelle *tout* polynôme en n variables, homogène de degré d, est somme de puissances d-ièmes de s formes linéaires.

Proposition 4.5. — *Étant donnée une forme quadratique f non dégénérée sur $\mathbf{F}_q^n$, il existe une base dans laquelle elle s'écrit sous l'une des deux formes suivantes :*

$$f(x) = \begin{cases} x_1^2 + \cdots + x_{n-1}^2 + x_n^2, \\ x_1^2 + \cdots + x_{n-1}^2 + \alpha x_n^2, \end{cases}$$

où α est un scalaire non nul fixé qui n'est pas un carré dans $\mathbf{F}_q$.

Notons que les deux formes proposées ne sont pas équivalentes, puisque leurs discriminants sont 1 et α, qui sont différents dans $\mathbf{F}_q^\times/\mathbf{F}_q^{\times 2}$. On déduit de la proposition que des formes quadratiques non dégénérées sur $\mathbf{F}_q^n$ sont équivalentes si et seulement si elles ont même discriminant.

Démonstration. — Par récurrence sur n. Si $n \geqslant 2$, on va montrer qu'il existe e_1 tel que $f(e_1) = 1$. Alors $\mathbf{F}_q^n = \mathbf{K}e_1 \oplus e_1^\perp$ et l'hypothèse de récurrence montre le résultat.

Écrivons f dans une base orthogonale, $f(x) = \sum_{i=1}^n \alpha_i x_i^2$. Puisqu'il y a $\frac{q+1}{2}$ carrés dans $\mathbf{F}_q$ (en comptant 0) et que $\alpha_1\alpha_2 \neq 0$, les quantités $\alpha_1 x_1^2$ et $1-\alpha_2 x_2^2$ décrivent toutes deux un ensemble à $\frac{q+1}{2}$ éléments quand x_1 (resp. x_2) décrit $\mathbf{F}_q$. Puisque $2\frac{q+1}{2} > q$, il existe x_1, x_2 tels que $\alpha_1 x_1^2$ et $1-\alpha_2 x_2^2$ coïncident, c'est-à-dire $f(x_1, x_2, 0, \ldots, 0) = 1$. □

On a donc *a priori* deux groupes orthogonaux pour chaque dimension, selon que le discriminant de la forme est trivial ou non. Cependant les groupes orthogonaux de $\langle 1, \ldots, 1\rangle$ et de $\langle \alpha, \ldots, \alpha\rangle$ sont les mêmes et la seconde forme est de discriminant α^n.

Si $n = 2m+1$ est impair, on a donc un seul groupe orthogonal, noté $\mathrm{O}_{2m+1}(\mathbf{F}_q)$.

Si $n = 2m$ est pair, on note les deux groupes orthogonaux $\mathrm{O}_{2m}^+(\mathbf{F}_q)$ et $\mathrm{O}_{2m}^-(\mathbf{F}_q)$ [11] (il ressort de (28) que leurs cardinaux sont différents : ils ne sont donc pas isomorphes).

11. Plus précisément, le groupe $\mathrm{O}_{2m}^+(\mathbf{F}_q)$ est le groupe d'isométries de toute forme quadratique de discriminant $(-1)^m$ et $\mathrm{O}_{2m}^-(\mathbf{F}_q)$ le groupe d'isométries de toute forme quadratique de discriminant $(-1)^m\alpha$.

4° Si $\mathbf{K} = \mathbf{Q}$, on a une infinité de discriminants possibles, puisque le groupe $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ est infini. Étant donnée une forme quadratique sur $\mathbf{Q}$, on peut aussi la voir comme une forme quadratique sur $\mathbf{R}$ et considérer sa signature. Mais, même à discriminant et signature fixés, il existe encore une infinité de classes d'équivalence de formes quadratiques sur $\mathbf{Q}$ [12].

Exercice 4.6. — Soit $\mathbf{K}$ un corps. Pour tous α, β dans $\mathbf{K}^\times$ tels que $\alpha+\beta \neq 0$, montrer $\langle \alpha, \beta\rangle \simeq \langle \alpha+\beta, \alpha\beta(\alpha+\beta)\rangle$.

Exemple 4.7 **(Pinceaux de formes quadratiques)**. — Soit V un espace vectoriel de dimension n sur un corps $\mathbf{K}$ algébriquement clos (de caractéristique $\neq 2$) et soient f et f' des formes quadratiques sur V. On suppose f non dégénérée. Le *pinceau* engendré par f et f' est l'ensemble de formes quadratiques

$$\{f_\lambda := \lambda f - f' \mid \lambda \in \mathbf{K}\}.$$

On choisit une base de V dans laquelle la matrice de f est I_n (ex. 4.3.1°) ; soit M la matrice de g dans cette même base. La forme quadratique f_λ est dégénérée si et seulement si $\det(\lambda \mathrm{I}_n - \mathrm{M}) = 0$, c'est-à-dire si λ est valeur propre de M. Supposons ces valeurs propres $\lambda_1, \ldots, \lambda_n$ toutes distinctes (c'est le cas « général »). La matrice M est alors diagonalisable [13] : il existe une base $(e_1, \ldots, e_n)$ de V composée de vecteurs propres de M. Plus précisément, $\mathrm{ME}_i = \lambda_i \mathrm{E}_i$, où E_i est la matrice (colonne) des composantes de e_i dans la base de départ. On a alors, pour $i \neq j$,

$$b'(e_i, e_j) = {}^t\mathrm{E}_i \mathrm{ME}_j = \lambda_j\, {}^t\mathrm{E}_i \mathrm{E}_j,$$

qui est aussi égal, par symétrie de b', à

$$b'(e_j, e_i) = {}^t\mathrm{E}_j \mathrm{ME}_i = \lambda_i\, {}^t\mathrm{E}_j \mathrm{E}_i = \lambda_i\, {}^t\mathrm{E}_i \mathrm{E}_j.$$

Comme $\lambda_i \neq \lambda_j$, on en déduit $0 = {}^t\mathrm{E}_i \mathrm{E}_j = b(e_i, e_j) = b'(e_i, e_j)$. La base $(e_1, \ldots, e_n)$ est donc orthogonale à la fois pour f et pour f'. En remplaçant e_i par $e_i/\sqrt{b(e_i, e_i)}$, on obtient une base de V dans laquelle

$$\begin{aligned} f(x) &= x_1^2 + \cdots + x_n^2, \\ f'(x) &= \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2. \end{aligned}$$

C'est le cas le plus simple. Dans tous les cas, on peut définir pour tout pinceau de formes quadratiques une suite de nombres appelée *symbole de Segre* du pinceau et, pour chaque symbole, une « forme normale » des quadriques du pinceau.

Exercice 4.8 **(Pinceaux de formes quadratiques, suite)**. — Soit V un espace vectoriel de dimension n sur un corps $\mathbf{K}$ algébriquement clos (de caractéristique $\neq 2$) et soient f et f' des formes quadratiques sur V. On suppose f non dégénérée et on pose

$$\mathrm{X} := \{x \in \mathrm{V} \mid f(x) = f'(x) = 0\}.$$

12. Pour décrire ces classes d'équivalence, il faut voir une forme quadratique sur $\mathbf{Q}$ comme une forme quadratique non seulement sur son complété $\mathbf{R}$, mais aussi sur chacun des corps p-adiques $\mathbf{Q}_p$, où p est un nombre premier impair : des formes quadratiques sur $\mathbf{Q}$ sont équivalentes si et seulement si elles le sont dans $\mathbf{R}$ et dans chacun des $\mathbf{Q}_p$ (« Théorème de Hasse-Minkowski » ; Serre, J.-P., *Cours d'arithmétique,* chap. IV, th. 9 ; *cf.* aussi prop. 7). Sur chacun de ces corps, il y a un invariant facile à calculer qui permet de tester l'équivalence (c'est la signature sur le corps $\mathbf{R}$ et un invariant dans $\{\pm 1\}$ sur les corps $\mathbf{Q}_p$).

13. Attention : la matrice M est symétrique, mais cela n'entraîne pas en général qu'elle est diagonalisable !

C'est un cône dans V.

a) Montrer l'équivalence des conditions suivantes :

(i) il existe une base $\mathscr{B}$ de V et $\lambda_1,\dots,\lambda_n \in \mathbf{K}$ distincts tels que, pour tout $x \in$ V de coordonnées $(x_1,\dots,x_n)$ dans $\mathscr{B}$,

$$\begin{aligned} f(x) &= x_1^2+\cdots+x_n^2, \\ f'(x) &= \lambda_1 x_1^2+\cdots+\lambda_n x_n^2; \end{aligned}$$

(ii) l'ensemble des $\lambda \in \mathbf{K}$ tels que la forme quadratique $\lambda f - f'$ soit dégénérée a n éléments ;

(iii) pour tout $x \in \mathrm{X}-\{0\}$, les orthogonaux de x pour f et pour f' sont des hyperplans distincts de V.

(*Indication :* l'équivalence (i) $\Leftrightarrow$ (ii) est l'ex. 4.7 ci-dessus.)

b) On suppose les conditions équivalentes de a) satisfaites et n impair. Montrer que X contient exactement 2^{n-1} sous-espaces vectoriels de V de dimension $(n-1)/2$ et qu'ils forment une unique orbite sous l'action du groupe μ_2^n (où $\mu_2 = \{1,-1\} \simeq \mathbf{Z}/2\mathbf{Z}$ est le groupe des racines carrées de 1 dans $\mathbf{K}$) donnée dans la base $\mathscr{B}$ de V de la condition (i) ci-dessus par $(\varepsilon_1,\dots,\varepsilon_n)\cdot(x_1,\dots,x_n) = (\varepsilon_1 x_1,\dots,\varepsilon_n x_n)$.

(*Commentaire :* le cas $n = 3$ est relativement facile. Le cas général peut se faire au prix de calculs assez lourds, pour lesquels on peut consulter la partie 3 de la thèse de M. Reid à www.maths.warwick.ac.uk/ miles/3folds/qu.pdf).

4.3. Décomposition en somme directe orthogonale : cas d'un vecteur isotrope. — La forme b est ici symétrique ou alternée, non dégénérée.

Lemme 4.9. — *Si x est un vecteur isotrope non nul, il existe un vecteur isotrope y tel que $b(x,y) = 1$.*

Dans la base (x,y) du plan P engendré par x et y, la matrice de b est $\begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$, où $\varepsilon = 1$ ou -1 selon que b est symétrique ou alternée. On dit que P est un *plan hyperbolique*.

Démonstration. — Comme b est non dégénérée et que x n'est pas nul, on peut toujours trouver x' tel que $b(x,x') = 1$, puis on prend $y = x' - \frac{1}{2}b(x',x')x$, qui satisfait les propriétés voulues. □

L'intérêt d'un plan hyperbolique P est que $b|_{\mathrm{P}}$ est non dégénérée ou, de manière équivalente, $\mathrm{P} \cap \mathrm{P}^\perp = 0$. Il en résulte

$$\mathrm{V} = \mathrm{P} \oplus \mathrm{P}^\perp.$$

La forme b est encore non dégénérée sur $\mathrm{P}^\perp$ et on peut recommencer la même opération sur $\mathrm{P}^\perp$, si celui-ci admet un vecteur isotrope non nul. Finalement, on fabrique une décomposition en somme directe orthogonale

$$\mathrm{V} = \mathrm{P}_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \mathrm{P}_\nu \overset{\perp}{\oplus} \mathrm{W},$$

où $\mathrm{P}_1,\dots,\mathrm{P}_\nu$ sont des plans hyperboliques et où le seul vecteur isotrope de W est 0 ; on dit que W est un *sous-espace anisotrope*.

L'entier ν est l'*indice* de la forme b ; on verra plus loin (cor. 5.5.2°) que c'en est un invariant. Une somme orthogonale de plans hyperboliques comme ci-dessus $\mathrm{P}_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \mathrm{P}_\nu$ est appelée un *espace hyperbolique*.

On a obtenu à ce stade deux formes de réduction pour une forme quadratique f :
– une décomposition dite de Gauss en $\langle \alpha_1, \ldots, \alpha_n \rangle$;
– une décomposition en somme directe orthogonale d'un espace hyperbolique et d'un espace anisotrope.

Remarquons que toute forme $\langle \alpha, -\alpha \rangle$ ($\alpha \in \mathbf{K}^\times$) est un plan hyperbolique, puisqu'elle contient un vecteur isotrope non nul, $(1,1)$. Concrètement, cette forme s'écrit $f(x_1, x_2) = \alpha x_1^2 - \alpha x_2^2$ dans une base (e_1, e_2) et $f(y_1, y_2) = 2y_1y_2$ dans la base $(\frac{1}{\alpha}(e_1 + e_2), e_1 - e_2)$, qui est donc hyperbolique.

Exemples 4.10. — 1° Si $\mathbf{K}$ est quadratiquement clos, toute forme quadratique non dégénérée sur $\mathbf{K}^n$ peut s'écrire $\langle 1, -1, 1, -1, \ldots, \rangle$. C'est donc la somme directe orthogonale de $\lfloor n/2 \rfloor$ plans hyperboliques et, si n est impair, de la forme anisotrope $\langle 1 \rangle$.

2° Si $\mathbf{K} = \mathbf{R}$, on a vu (ex. 4.3.2°) que toute forme quadratique non dégénérée s'écrit

$$\langle \underbrace{1, \ldots, 1}_{s \text{ fois}}, \underbrace{-1, \ldots, -1}_{t \text{ fois}} \rangle.$$

Si $s \leqslant t$, c'est donc la somme directe orthogonale de s plans hyperboliques et de la forme définie négative (donc anisotrope) $\langle \underbrace{-1, \ldots, -1}_{t-s \text{ fois}} \rangle$.

Exercice 4.11. — Soit $\mathbf{K}$ un corps de caractéristique différente de 2 et soit f une forme quadratique non dégénérée sur un $\mathbf{K}$-espace vectoriel V de dimension finie non nulle. Soit $a \in \mathbf{K}$. On dit que f *représente* a s'il existe $v \in \mathrm{V}$ non nul tel que $f(v) = a$.
a) La forme quadratique $\langle 1, 1, 1, -7 \rangle$ sur $\mathbf{Q}^4$ représente-t-elle 0 ?
b) Si f représente 0, montrer que f représente tout élément de $\mathbf{K}$.
c) Soit g une forme quadratique non dégénérée sur un $\mathbf{K}$-espace vectoriel W de dimension finie non nulle. Montrer que les propriétés suivantes sont équivalentes :
(i) il existe $a \in \mathbf{K}^*$ qui est représenté à la fois par f et par g ;
(ii) la forme quadratique $h(v, w) = f(v) - g(w)$ sur l'espace vectoriel $\mathrm{V} \oplus \mathrm{W}$ représente 0.

4.4. Décomposition en somme directe orthogonale : cas alterné. — On suppose b alternée (et non dégénérée). Dans ce cas, tout vecteur est isotrope et on obtient comme ci-dessus une décomposition en somme directe orthogonale (l'espace W est nécessairement nul)

$$\mathrm{V} = \mathrm{P}_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \mathrm{P}_\nu.$$

En particulier, la dimension de V est paire (égale à 2ν) et, à isométrie près, il n'y a qu'une seule forme alternée non dégénérée sur un $\mathbf{K}$-espace vectoriel de dimension paire 2ν ; on notera son groupe d'isométries $\mathrm{Sp}_{2\nu}(\mathbf{K})$.

Dans une base $(e_1, \ldots, e_{2\nu})$ telle que $(e_i, e_{i+\nu})$ est une base standard de P_i, la matrice de b est

$$\mathrm{J}_{2\nu} = \begin{pmatrix} 0 & \mathrm{I}_\nu \\ -\mathrm{I}_\nu & 0 \end{pmatrix}. \tag{21}$$

On a alors

$$\mathrm{Sp}_{2\nu}(\mathbf{K}) = \{ \mathrm{U} \in \mathrm{GL}_{2\nu}(\mathbf{K}) \mid {}^t\mathrm{U}\mathrm{J}_{2\nu}\mathrm{U} = \mathrm{J}_{2\nu} \}. \tag{22}$$

Décomposant la matrice par blocs,

$$U = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

il vient $U \in \mathrm{Sp}_{2\nu}(\mathbf{K})$ si et seulement si

$$ {}^tAC = {}^tCA, \quad {}^tBD = {}^tDB, \quad {}^tAD - {}^tCB = I_\nu. \tag{23}$$

En particulier, on a $\mathrm{Sp}_2(\mathbf{K}) = \mathrm{SL}_2(\mathbf{K})$. On a en fait l'inclusion

$$\mathrm{Sp}_{2\nu}(\mathbf{K}) \subseteq \mathrm{SL}_{2\nu}(\mathbf{K})$$

pour tout $\nu \geqslant 1$, mais elle n'est pas facile à démontrer (cor. 7.2 et cor. III.4.8).

5. Théorème de Witt

Le théorème de Witt est un théorème de prolongement des isométries. Il est essentiel dans la théorie.

***Théorème 5.1* (Witt).** — *Soient* (V, b) *et* (V', b') *des espaces isométriques non dégénérés. Soit* W *un sous-espace de* V *et soit* $u : W \to V'$ *une isométrie. Il existe une isométrie* $v : V \to V'$ *telle que* $v|_W = u$.

Commençons par le cas simple où W est de dimension 1, engendré par un vecteur x. Le vecteur $y := u(x)$ vérifie $b(x,x) = b(y,y)$ et il s'agit de trouver une isométrie v telle que $v(x) = y$. Pour résoudre ce problème, nous aurons besoin de la construction suivante.

***Exemple 5.2* (Réflexions).** — Si $b(x,x) \neq 0$ (en particulier, b est symétrique), on a $V = x^\perp \oplus \mathbf{K}x$ et la *réflexion* (ou symétrie hyperplane) par rapport à $x^\perp$ est l'endomorphisme s_x de V de valeurs propres 1 et -1 sur cette décomposition. Il s'agit manifestement d'une isométrie, donnée explicitement par la formule

$$s_x(y) = y - 2\frac{b(x,y)}{b(x,x)}x.$$

Si $b(x,x) = b(y,y) \neq 0$ et qu'on note la forme quadratique associée f, le théorème de WItt résulte alors du lemme suivant.

Lemme 5.3. — *Si* $f(x) = f(y) \neq 0$, *il existe une isométrie* v *telle que* $v(x) = y$.

Démonstration. — De $f(x+y) + f(x-y) = 2(f(x) + f(y)) = 4f(x)$, on déduit que l'un au moins des vecteurs $x+y$ et $x-y$ est non isotrope, disons par exemple $x+y$. Alors la réflexion par rapport à $(x+y)^\perp$ envoie x sur $-y$, et on la compose par $-\mathrm{Id}$. □

Le deuxième cas qu'on va traiter est celui d'un espace W totalement isotrope (c'est-à-dire tel que $b|_W \equiv 0$). On construit pour cela un espace hyperbolique contenant W.

Lemme 5.4. — *Soit* V *un espace vectoriel muni d'une forme bilinéaire symétrique ou alternée non dégénérée, soit* W *un sous-espace vectoriel totalement isotrope de* V *et soit* $(e_1, \ldots, e_r)$ *une base de* W. *Il existe* $(e'_1, \ldots, e'_r)$ *dans* V *tels que*

- *chaque* $P_i := \langle e_i, e'_i \rangle$ *est un plan hyperbolique ;*
- $P_1, \ldots, P_r$ *sont en somme directe orthogonale.*

En outre, toute isométrie $W \to V'$ *se prolonge en une isométrie* $P_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r \to V'$.

Démonstration. — Le cas $r = 1$ est le lemme 4.9. On raisonne ensuite par récurrence sur r. Posons $W_1 = \langle e_2, \ldots, e_r \rangle$.

L'hyperplan $e_1^\perp$ contient e_1 et W_1 ; soit V_1 un supplémentaire de e_1 dans $e_1^\perp$ contenant W_1. La restriction de b à V_1 est non dégénérée ; on applique l'hypothèse de récurrence à son sous-espace totalement isotrope W_1 et il existe donc des plans hyperboliques $P_2, \ldots, P_r$ dans V_1 avec les propriétés du lemme. La somme directe $P_2 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r$ est alors orthogonale à e_1 et la restriction de b y est non dégénérée. Son orthogonal contient donc e_1 et la restriction de b y est aussi non dégénérée. On peut y appliquer le lemme 4.9 au vecteur e_1 : il existe e_1' orthogonal à $P_2 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r$ et formant avec e_1 un plan hyperbolique.

L'extension d'une isométrie $u : W \to V'$ se montre en étendant $\mathrm{im}(u)$ dans V' de la même manière que W : comme b est non dégénérée, u est injective et $u(W) = \langle u(e_1), \ldots, u(e_r) \rangle$ est un sous-espace totalement isotrope de V' ; on construit alors des plans hyperboliques $\langle u(e_i), e_i'' \rangle$ et on prolonge u en envoyant chaque e_i' sur e_i''. □

Démonstration du th. 5.1. — On commence par étendre u à un sous-espace $\bar{W}$ de V contenant W sur laquelle la forme b est non dégénérée.

Soit W' un supplémentaire de $W \cap W^\perp$ dans W. La restriction de b à W' est non dégénérée, donc aussi la restriction de b à $W'^\perp$. Ce dernier espace contient le sous-espace vectoriel totalement isotrope $W \cap W^\perp$. Par le lemme 5.4, on peut donc étendre $u|_{W'^\perp}$ à un sous-espace hyperbolique H de $W'^\perp$ (sur laquelle b est non dégénérée). On a ainsi étendu u en $\bar{u}$ au sous-espace $\bar{W} := H \overset{\perp}{\oplus} W'$, sur lequel b est non dégénérée. Remarquons que la restriction de b' à $u(\bar{W})$ est aussi non dégénérée.

Si b est alternée, les restrictions (non dégénérées) de b à $\bar{W}^\perp$ et de b' à $\bar{u}(\bar{W})^\perp$ sont équivalentes (à isométrie près, il n'y a qu'une seule forme alternée non dégénérée sur un espace vectoriel de dimension paire). On a ainsi étendu u à $\bar{W} \overset{\perp}{\oplus} \bar{W}^\perp = V$.

Supposons donc b symétrique. De plus, comme (V, b) et (V', b') sont isométriques, on peut les supposer égaux. Le cas $\dim(\bar{W}) = 1$ est alors fourni par le lemme 5.3.

On raisonne alors par récurrence sur $\dim(\bar{W})$. Si $\dim(\bar{W}) \geqslant 2$, on écrit $\bar{W} = W_1 \overset{\perp}{\oplus} W_2$, avec W_1 et W_2 non nuls, où la restriction de b à W_1 et à W_2 est non dégénérée (*cf.* § 4.2). Par l'hypothèse de récurrence, $u|_{W_1}$ se prolonge en une isométrie v_1 de V, qui induit par restriction une isométrie $v_1|_{W_1^\perp} : W_1^\perp \xrightarrow{\sim} u(W_1)^\perp$. On applique alors à nouveau l'hypothèse de récurrence à $u|_{W_2} : W_2 \to u(W_1)^\perp$ pour le prolonger en une isométrie $v_2 : W_1^\perp \xrightarrow{\sim} u(W_1)^\perp$. On prend alors $v = u|_{W_1} \oplus v_2 : W_1 \oplus W_1^\perp \to u(W_1) \oplus u(W_1)^\perp$. □

Corollaire 5.5. — *1° Si* W *et* W' *sont des sous-espaces isométriques de* V, *les sous-espaces* $W^\perp$ *et* $W'^\perp$ *sont isométriques.*

2° Tous les sous-espaces totalement isotropes maximaux ont même dimension ν, *appelée l'indice de b.*

3° Tous les sous-espaces hyperboliques maximaux ont même dimension 2ν.

4° Si H *est un sous-espace hyperbolique maximal, on peut écrire* $V = H \overset{\perp}{\oplus} W$, *avec* W *sans vecteur isotrope non nul (*W *est anisotrope).*

On notera qu'au vu de 3°, on a $\nu \leqslant \frac{1}{2}\dim(V)$.

D'autre part, dans le cas alterné, le corollaire résulte de la classification des formes alternées non dégénéréees ; on a $\nu = \frac{1}{2}\dim(V)$ et l'espace anisotrope W du 4° est nul.

Démonstration. — Le 1° résulte du théorème de Witt.

On prouve le 2°. Si W et W′ sont totalement isotropes et $\dim(W) \leqslant \dim(W')$, n'importe quelle application linéaire injective $u : W \to W'$ est une isométrie, donc s'étend en une isométrie v de V. Alors W est contenu dans $v^{-1}(W')$, qui est aussi totalement isotrope. Il en résulte que tous les sous-espaces totalement isotropes maximaux ont même dimension.

Tout sous-espace hyperbolique contient un sous-espace totalement isotrope de dimension moitié, et inversement, comme on l'a vu dans le lemme 5.4, tout sous-espace totalement isotrope est contenu dans un sous-espace hyperbolique de dimension double. Le 3° résulte donc du 2°.

Le 4° a déjà été vu dans le § 4.3. □

Exemples 5.6. — 1° Si **K** est un corps quadratiquement clos, une forme quadratique non dégénérée de dimension n est d'indice $\lfloor n/2 \rfloor$ (ex. 4.10.1°).

2° Dans le cas d'une forme quadratique non dégénérée sur $\mathbf{R}^n$, de signature $(s, t = n-s)$, on voit que l'indice est $\inf(s, t)$ (ex. 4.10.2°), donc la signature est bien un invariant de la forme quadratique.

3° Dans le cas d'un corps fini $\mathbf{F}_q$ (de caractéristique différente de 2), rappelons que les formes quadratiques sont de deux types :

$$\langle 1, \dots, 1\rangle \quad \text{et} \quad \langle 1, \dots, 1, \alpha\rangle,$$

avec $\alpha \notin \mathbf{F}_q^2$. D'autre part, toute forme quadratique sur un espace de dimension $\geqslant 3$ admet un vecteur isotrope non nul (cela résulte de la démonstration de la prop. 4.5). L'espace F du cor. 5.5 est donc de dimension $\leqslant 2$.

En dimension 2,

– la forme $\langle 1, -1\rangle$ a un vecteur isotrope non nul, $(1, 1)$;

– la forme $\langle 1, -\alpha\rangle$ n'a pas de vecteur isotrope non nul.

Si la dimension de l'espace est $2m+1$, impaire, W est de dimension 1 et l'indice de la forme quadratique est m. On rappelle qu'on a un seul groupe orthogonal, noté $O_{2m+1}(\mathbf{F}_q)$.

Si la dimension de l'espace est $2m$, paire, soit $W = 0$ et l'indice de la forme quadratique est m, soit W est de type $\langle 1, -\alpha\rangle$ et l'indice est $m-1$. On a déjà noté les groupes orthogonaux correspondants $O^+_{2m}(\mathbf{F}_q)$ et $O^-_{2m}(\mathbf{F}_q)$, respectivement (*cf.* note 11 ; la forme quadratique $\langle 1, -1, \dots, 1, -1\rangle$ étant visiblement d'indice m, on voit que le discriminant associé est bien $(-1)^m$).

Exercice 5.7. — Soit q une puissance de nombre premier impair et soit f une forme quadratique non dégénérée sur $\mathbf{F}_q^n$. Calculer le cardinal de l'ensemble

$$\{x \in \mathbf{F}_q^n \mid f(x) = 1\}$$

(*Indication :* on distinguera plusieurs cas selon le discriminant de f et la parité de n).

Exercice 5.8. — On considère sur $\mathbf{R}^{2n}$ la forme quadratique

$$f(x_1, \dots, x_{2n}) = x_1 x_{n+1} + \cdots + x_n x_{2n}.$$

Pour toute partie J de $\{1,\dots,2n\}$ de cardinal n, on note V^{J} le sous-espace vectoriel de $\mathbf{R}^{2n}$ défini par les équations $x_j = 0$ pour tout $j \in \mathrm{J}$.
a) Déterminer le rang et la signature de f.
b) Soit $a : \mathbf{R}^n \to \mathbf{R}^n$ une application linéaire. À quelle condition sur la matrice de a le graphe V_a de a (vu comme un sous-espace vectoriel de $\mathbf{R}^n \times \mathbf{R}^n = \mathbf{R}^{2n}$) est-il totalement isotrope pour f ? Montrer qu'on obtient ainsi tous les espaces V totalement isotropes maximaux (c'est-à-dire de dimension n) tels que $\mathrm{V} \cap \mathrm{V}^{\{1,\dots,n\}} = \{0\}$.
c) Si $a, b : \mathbf{R}^n \to \mathbf{R}^n$ sont des applications linéaires, peut-on dire de la parité de la dimension de $\mathrm{V}_a \cap \mathrm{V}_b$?
d) Pour toute partie J de $\{1,\dots,2n\}$ de cardinal n, et toute application linéaire $a : \mathbf{R}^n \to \mathbf{R}^n$, définir comme dans b) des sous-espaces $\mathrm{V}^{\mathrm{J}}_a \subseteq \mathbf{R}^{2n}$ totalement isotropes maximaux tels que $\mathrm{V}^{\mathrm{J}}_a \cap \mathrm{V}^{\mathrm{J}} = \{0\}$.
e) Pour toutes parties J et K de $\{1,\dots,2n\}$ de cardinal n, montrer que
– soit $\mathrm{card}(\mathrm{J} \cap \mathrm{K}) \not\equiv n \pmod 2$ et, pour tout a et b, on a $\mathrm{V}^{\mathrm{J}}_a \neq \mathrm{V}^{\mathrm{K}}_b$;
– soit $\mathrm{card}(\mathrm{J} \cap \mathrm{K}) \equiv n \pmod 2$ et « la plupart » des $\mathrm{V}^{\mathrm{J}}_a$ sont aussi des $\mathrm{V}^{\mathrm{K}}_b$.

6. Groupe de Witt

Soit $\mathbf{K}$ un corps. On considère l'ensemble des classes d'équivalence (ou d'isométrie) de $\mathbf{K}$-espaces vectoriels munis d'une forme quadratique non dégénérée. Cette ensemble est muni d'une addition (commutative et associative) correspondant à la somme directe orthogonale et l'élément neutre correspond à la forme quadratique nulle sur l'espace vectoriel nul. Le 1° du cor. 5.5 dit exactement que l'addition est simplifiable :

$$[f] + [g] = [f'] + [g] \Longrightarrow [f] = [f'].$$

C'est un semi-groupe mais ce n'est pas un groupe, puisque $\dim([f] + [g]) = \dim([f]) + \dim([g])$, donc $[f] + [g]$ n'est nul que si $[f]$ et $[g]$ le sont. De la même façon qu'on passe du semi-groupe simplifiant $\mathbf{N}$ au groupe $\mathbf{Z}$, on associe à cette situation le *groupe de Grothendieck-Witt* $\mathrm{GW}(\mathbf{K})$ de $\mathbf{K}$: c'est l'ensemble des couples $([f_1], [f_2])$ (auquel il faut penser comme la différence formelle $[f_1] - [f_2]$) modulo la relation déquivalence

$$([f_1], [f_2]) \sim ([g_1], [g_2]) \Longrightarrow [f_1] + [g_2] = [f_2] + [g_1].$$

On vérifie que $\mathrm{GW}(\mathbf{K})$ est bien un groupe, muni de morphismes de groupes surjectifs

$$\dim : \mathrm{GW}(\mathbf{K}) \twoheadrightarrow \mathbf{Z} \qquad \mathrm{disc} : \mathrm{GW}(\mathbf{K}) \twoheadrightarrow \mathbf{K}^\times / \mathbf{K}^{\times 2}.$$

Notons par ailleurs la relation $[f] + [-f] = \dim(f)[\mathrm{P}]$, où $-f$ est la forme quadratique opposée à f (sur le même espace vectoriel) et P est un plan hyperbolique.

On définit le *groupe de Witt* $\mathrm{W}(\mathbf{K})$ de $\mathbf{K}$ comme le quotient de $\mathrm{GW}(\mathbf{K})$ par le sous-groupe $\mathbf{Z}[\mathrm{P}]$ engendré par $[\mathrm{P}]$. C'est encore un groupe abélien dans lequel l'opposé de $[f]$ est $[-f]$. En utilisant l'écriture diagonale des formes quadratiques, on a les relations suivantes dans $\mathrm{W}(\mathbf{K})$:

$$\begin{aligned}
[\langle \alpha_{\sigma(1)}, \dots, \alpha_{\sigma(m)} \rangle] &= [\langle \alpha_1, \dots, \alpha_m \rangle] \quad \text{pour tout } \sigma \in \mathfrak{S}_m, \\
[\langle \alpha_1, \dots, \alpha_m \rangle] + [\langle \beta_1, \dots, \beta_n \rangle] &= [\langle \alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \rangle], \\
-[\langle \alpha_1, \dots, \alpha_m \rangle] &= [\langle -\alpha_1, \dots, -\alpha_m \rangle], \\
[\langle \alpha, -\alpha \rangle] &= 0.
\end{aligned}$$

On a un morphisme

$$\overline{\dim} : \mathrm{W}(\mathbf{K}) \twoheadrightarrow \mathbf{Z}/2\mathbf{Z}$$

mais le discriminant ne passe pas au quotient puisque $\mathrm{disc}(\mathrm{P}) = -1$.

Le 1° du cor. 5.5 dit que les éléments de $\mathrm{W}(\mathbf{K})$ peuvent être représentés par des formes quadratiques anisotropes. On a plus précisément

$$\mathrm{W}(\mathbf{K}) = \{\text{classes d'isométrie de formes quadratiques anisotropes}\}.$$

En effet, si des formes quadratiques anisotropes f_1 et f_2 ont même image dans $\mathrm{W}(\mathbf{K})$, il existe des entiers positifs n_1 et n_2 tels que $f_1 \overset{\perp}{\oplus} \mathrm{P}^{n_1} \sim f_2 \overset{\perp}{\oplus} \mathrm{P}^{n_2}$. Le cor. 5.5 entraîne que f_1 et f_2 sont isométriques.

Exemples 6.1. — 1° Si $\mathbf{K}$ est un corps quadratiquement clos, $\overline{\dim} : \mathrm{W}(\mathbf{K}) \twoheadrightarrow \mathbf{Z}/2\mathbf{Z}$ est un isomorphisme (ex. 5.6.1°).

2° Si -1 est un carré dans $\mathbf{K}$, on a $[f] = [-f]$ pour tout forme quadratique f, donc tout élément de $\mathrm{W}(\mathbf{K})$ est d'ordre 2.

3° Toute forme quadratique réelle anisotrope est isométrique à $\pm\langle 1, \dots, 1\rangle$. On a donc $\mathrm{W}(\mathbf{R}) \simeq \mathbf{Z}$. On peut en déduire un isomorphisme $\dim \oplus s : \mathrm{GW}(\mathbf{R}) \xrightarrow{\sim} \mathbf{Z} \oplus \mathbf{Z}$, où s est le morphisme signature, défini par $s([\langle 1\rangle]) = 1$.

4° Dans le cas d'un corps fini $\mathbf{F}_q$ (de caractéristique différente de 2), on a

$$\mathrm{W}(\mathbf{K}) \simeq \begin{cases} \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} & \text{si } -1 \in \mathbf{K}^2, \\ \mathbf{Z}/4\mathbf{Z} & \text{si } -1 \notin \mathbf{K}^2. \end{cases}$$

En effet, si on note comme d'habitude α un élément de $\mathbf{F}_q - \mathbf{F}_q^2$, il y a 4 (classes d'isométrie de) formes quadratiques anisotropes : 0, $\langle 1\rangle$, $\langle \alpha\rangle$ et $\langle 1, -\alpha\rangle$. Le groupe $\mathrm{W}(\mathbf{F}_q)$ a donc 4 éléments, et il est isomorphe soit à $\mathbf{Z}/4\mathbf{Z}$, soit à $(\mathbf{Z}/2\mathbf{Z})^2$. Si -1 est un carré dans $\mathbf{F}_q$, on est dans le second cas par 2°. Dans le cas contraire, on peut prendre $\alpha = -1$ et $[\langle 1\rangle] + [\langle 1\rangle] = [\langle 1, 1\rangle] = [\langle 1, -\alpha\rangle]$; on est donc dans le premier cas : $\mathrm{W}(\mathbf{F}_q)$ est isomorphe à $\mathbf{Z}/4\mathbf{Z}$, avec comme générateur $[\langle 1\rangle]$.

5° Le groupe $\mathrm{W}(\mathbf{Q})$ est connu. Il contient le groupe cyclique $\mathbf{Z}$ engendré par $1_{\mathrm{W}(\mathbf{Q})}$, et le quotient est $\bigoplus_{p \text{ premier}} \mathrm{W}(\mathbf{F}_p)$.

***Remarque 6.2* (Idéal fondamental et conjecture de Milnor)**. — On peut aussi mettre sur $\mathrm{W}(\mathbf{K})$ une structure d'anneau en définissant une forme quadratique sur le produit tensoriel (exerc. III.1.8) de deux espaces munis d'une forme quadratique. Cela revient à poser

$$[\langle \alpha_1, \dots, \alpha_m\rangle] \cdot [\langle \beta_1, \dots, \beta_n\rangle] = [\langle \alpha_i \beta_j, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\rangle].$$

Le morphisme $\overline{\dim} : \mathrm{W}(\mathbf{K}) \twoheadrightarrow \mathbf{Z}/2\mathbf{Z}$ est alors un morphisme d'anneaux et on appelle son noyau $\mathrm{I}(\mathbf{K})$ l'*idéal fondamental* de $\mathrm{W}(\mathbf{K})$. Un élément de $\mathrm{I}(\mathbf{K})$ est donc représenté par une forme quadratique sur un espace vectoriel de dimension paire. Le morphisme *discriminant signé* est défini ainsi :

$$\begin{aligned} \mathrm{disc}_s : \mathrm{I}(\mathbf{K}) &\longrightarrow \mathbf{K}^\times/\mathbf{K}^{\times 2} \\ [f] &\longmapsto (-1)^{\dim(f)/2} \mathrm{disc}(f). \end{aligned}$$

On montre qu'il induit un isomorphisme $\mathrm{I}(\mathbf{K})/\mathrm{I}(\mathbf{K})^2 \xrightarrow{\sim} \mathbf{K}^\times/\mathbf{K}^{\times 2}$.

La conjecture de Milnor, montrée par Voevodsky en 1996 (démonstration pour laquelle il a obtenu la médaille Fields en 2002) identifie tous les quotients successifs $I(\mathbf{K})^r/I(\mathbf{K})^{r+1}$ en termes de groupes dits de K-théorie de Milnor.

7. Groupe symplectique

Dans cette section, le $\mathbf{K}$-espace vectoriel V, de dimension finie paire 2ν, est muni d'une forme alternée non dégénérée (on dit aussi *forme symplectique*) b et on étudie le groupe symplectique $\mathrm{Sp}(V, b)$.

On rappelle que V est somme directe orthogonale de ν plans hyperboliques.

7.1. Générateurs. — Soit une transvection $\tau(x) = x + \ell(x)a$, où $\ell \in V^*$ et $a \in \ker(\ell)$ (*cf.* § 2.4). On a

$$\begin{aligned} b(\tau(x), \tau(y)) &= b(x + \ell(x)a, y + \ell(y)a) \\ &= b(x, y) + \ell(y)b(x, a) + \ell(x)b(a, y). \end{aligned}$$

Si on prend pour ℓ une forme linéaire $\lambda b(a, \cdot)$, la transvection τ est symplectique ; toutes les transvections de la forme

$$\tau(x) = x + \lambda b(a, x)a, \quad a \in V, \lambda \in \mathbf{K} \tag{24}$$

sont donc symplectiques.

Remarquons que si $\dim(V) = 2$, dans une base hyperbolique de V, on a $b((x_1, x_2), (y_1, y_2)) = x_1y_2 - x_2y_1$. Un morphisme u de V multiplie b par $\det(u)$, d'où il résulte (comme on peut aussi le voir sur les équations (23))

$$\mathrm{Sp}_2(\mathbf{K}) = \mathrm{SL}_2(\mathbf{K}). \tag{25}$$

En dimension 2, toutes les transvections sont symplectiques.

Théorème 7.1. — *Les transvections symplectiques engendrent* $\mathrm{Sp}(V)$.

Corollaire 7.2. — *Le groupe symplectique* $\mathrm{Sp}(V)$ *est un sous-groupe de* $\mathrm{SL}(V)$.

On verra dans le cor. III.4.8 une autre démonstration de ce corollaire.

Démonstration. — Les transvections ont déterminant 1. □

Démonstration du théorème. — La démonstration se fait par récurrence sur la dimension, en commencant par la dimension 0 (!).

Si $V \neq 0$, il contient un plan hyperbolique $P = \langle x_1, x_2 \rangle$. Soit $u \in \mathrm{Sp}(V)$. Alors $Q := u(P) = \langle u(x_1), u(x_2) \rangle$ est aussi un plan hyperbolique. Si on admet (provisoirement) le lemme ci-dessous, il existe un produit v de transpositions symplectiques tel que $v(x_1) = u(x_1)$ et $v(x_2) = u(x_2)$. La composée $v^{-1}u$ est alors l'identité sur P, donc laisse stable son orthogonal $P^\perp$. Sa restriction à $P^\perp$ en est un automorphisme symplectique, qui est donc, par hypothèse de récurrence, produit de transvections symplectiques de $P^\perp$. Prolongées par l'identité sur P, ces transvections symplectiques deviennent des transvections symplectiques de V, dont le produit est $v^{-1}u$. Ainsi, u est bien produit de transvections symplectiques de V. □

Lemme 7.3. — *Si* $\mathrm{P} = \langle x_1, x_2\rangle$ *et* $\mathrm{Q} = \langle y_1, y_2\rangle$ *sont des plans hyperboliques (avec* $b(x_1,x_2) = b(y_1,y_2) = 1$*), il existe un produit d'au plus 4 transvections symplectiques envoyant* x_1 *sur* y_1 *et* x_2 *sur* y_2.

Démonstration. — Observons que si $b(x_1,y_1) \neq 0$, on peut envoyer x_1 sur y_1 par la transvection symplectique

$$\tau(x) = x - \frac{b(y_1 - x_1, x)}{b(x_1,y_1)}(y_1 - x_1).$$

Dans le cas général, en passant par un z tel que $b(x_1,z) \neq 0$ et $b(z,y_1) \neq 0$ (qui existe parce que V n'est pas réunion des hyperplans $x_1^\perp$ et $y_1^\perp$!), on voit qu'un produit de 2 transvections symplectiques envoie x_1 sur y_1.

On est ainsi ramené au cas $x_1 = y_1$ et on veut donc envoyer x_2 sur y_2 en laissant x_1 fixe. À nouveau, la situation est plus simple si $b(x_2,y_2) \neq 0$: la transvection

$$\tau(x) = x - \frac{b(y_2 - x_2, x)}{b(x_2,y_2)}(y_2 - x_2)$$

convient alors, car $b(y_2 - x_2, x_1) = b(y_2,y_1) - b(x_2,x_1) = 0$. Si $b(x_2,y_2) = 0$, il faut à nouveau passer par un intermédiaire z tel que $b(x_2,z) \neq 0$, $b(z,y_2) \neq 0$, mais aussi (pour fixer x_1), $b(z - x_2, x_1) = 0$ et $b(y_2 - z, x_1) = 0$, ce qui revient à $b(x_1,z) = 1$. Mais $z = x_1 + y_2$ satisfait toutes ces conditions. □

On déduit d'ailleurs de ce lemme que toute isométrie d'un espace symplectique de dimension 2ν est produit d'au plus 4ν transvections symplectiques.

Remarque 7.4. — On peut montrer [14] que le groupe $\mathrm{Sp}_{2\nu}(\mathbf{K})$ est engendré par les matrices par blocs (*cf.* (23))

$$\begin{pmatrix} \mathrm{I}_\nu & \alpha(\mathrm{E}_{ij} + \mathrm{E}_{ji}) \\ 0 & \mathrm{I}_\nu \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \mathrm{I}_\nu + \alpha\mathrm{E}_{ij} & 0 \\ 0 & \mathrm{I}_\nu - \alpha\mathrm{E}_{ji} \end{pmatrix}, \quad \text{pour } 1 \leqslant i,j \leqslant \nu,\ \alpha \in \mathbf{K},$$

et leur transposée [15].

Exercice 7.5. — Montrer que $\mathrm{Sp}_{2\nu}(\mathbf{R})$ est connexe.

Exercice 7.6. — Montrer que $\mathrm{Sp}_{2\nu}(\mathbf{Q})$ est dense dans $\mathrm{Sp}_{2\nu}(\mathbf{R})$.

7.2. Centre. — Soit u une isométrie commutant avec toute isométrie. Elle commute en particulier avec toutes les transvections symplectiques, de sorte que, pour tout $a \in \mathrm{V}$ et tout $x \in \mathrm{V}$, on a

$$u(x) + b(a,u(x))\,a = \tau(u(x)) = u(\tau(x)) = u(x) + b(a,x)\,u(a).$$

Étant donné $a \neq 0$, on peut choisir x de façon que $b(a,x) \neq 0$ et on en déduit que $u(a)$ est proportionnel à a pour tout $a \in \mathrm{V}$. L'automorphisme u est alors une homothétie (*cf.* note 2), de rapport λ. Comme il est symplectique, on a $\lambda = \pm 1$.

---

14. O'Meara, O. T., *Symplectic Groups,* Mathematical Surveys **16**, American Mathematical Society, Providence, R.I., 1978.

15. Le groupe $\mathrm{Sp}_{2\nu}(\mathbf{Z})$, qu'on peut définir comme le sous-groupe de $\mathrm{Sp}_{2\nu}(\mathbf{Q})$ formé des matrices à coefficients entiers, est engendré, pour $\nu \geqslant 2$, par quatre matrices explicites (Hua, L. K., Reiner, I., On the generators of the symplectic modular group, *Trans. Amer. Math. Soc.* **65** (1949), 415–426).

Le centre de $\mathrm{Sp}_{2\nu}(\mathbf{K})$ est donc réduit à $\{\pm \mathrm{I}_{2\nu}\}$. On considère le groupe projectif associé, à savoir le quotient

$$\mathrm{PSp}_{2\nu}(\mathbf{K}) = \mathrm{Sp}_{2\nu}(\mathbf{K})/\{\pm \mathrm{I}_{2\nu}\}.$$

C'est un sous-groupe de $\mathrm{PSL}(2\nu, \mathbf{K})$; il agit donc fidèlement sur l'espace projectif $\mathbf{P}^{2\nu-1}(\mathbf{K})$.

Exemples 7.7. — 1° Les groupes $\mathrm{Sp}_{2\nu}(\mathbf{R})$ et $\mathrm{PSp}_{2\nu}(\mathbf{R})$) sont des *variétés différentiables* de dimension $\nu(2\nu+1)$.

2° Les groupes $\mathrm{Sp}_{2\nu}(\mathbf{C})$ et $\mathrm{PSp}_{2\nu}(\mathbf{C})$) sont des *variétés complexes* de dimension $\nu(2\nu+1)$.

7.3. Cardinal des groupes symplectiques finis.— On suppose q impair (*cf.* rem. 7.11 pour le cas de la caractéristique 2). Comme pour les groupes linéaires, il est facile de dénombrer les éléments de $\mathrm{Sp}_{2\nu}(\mathbf{F}_q)$: il suffit de compter le nombre de bases hyperboliques. On obtient

$$\begin{aligned}
|\mathrm{Sp}_{2\nu}(\mathbf{F}_q)| &= (q^{2\nu}-1)\frac{(q^{2\nu}-q^{2\nu-1})}{q-1}(q^{2\nu-2}-1)\frac{(q^{2\nu-2}-q^{2\nu-3})}{q-1}\cdots(q^2-1)\frac{(q^2-q)}{q-1} \\
&= q^{2\nu-1+2\nu-3+\cdots+1}(q^{2\nu}-1)(q^{2\nu-2}-1)\cdots(q^2-1) \\
&= q^{\nu^2}(q^{2\nu}-1)(q^{2\nu-2}-1)\cdots(q^2-1), \qquad (26) \\
|\mathrm{PSp}_{2\nu}(\mathbf{F}_q)| &= \frac{1}{2}|\mathrm{PSp}_{2\nu}(\mathbf{F}_q)| \\
&= \frac{1}{2}q^{\nu^2}(q^{2\nu}-1)(q^{2\nu-2}-1)\cdots(q^2-1).
\end{aligned}$$

On rappelle (*cf.* (25)) que le groupe $\mathrm{Sp}_2(\mathbf{F}_q)$ est le même que le groupe $\mathrm{SL}_2(\mathbf{F}_q)$.

***Exercice 7.8* (p-sous-groupes de Sylow de $\mathrm{Sp}_{2\nu}(\mathbf{F}_q)$).** — L'espace vectoriel $\mathbf{F}_q^{2\nu}$ est muni de la forme symplectique de matrice $\mathrm{J}_{2\nu} = \begin{pmatrix} 0 & \mathrm{I}_\nu \\ -\mathrm{I}_\nu & 0 \end{pmatrix}$ dans la base canonique (*cf.* (21)).

Soit $\mathrm{W} \subseteq \mathbf{F}_q^{2\nu}$ le sous-espace vectoriel engendré par les ν premiers vecteurs de la base canonique. On considère le sous-groupe

$$\mathrm{H} := \{u \in \mathrm{Sp}_{2\nu}(\mathbf{F}_q) \mid u(\mathrm{W}) = \mathrm{W}\}.$$

a) Montrer que la restriction à W induit un morphisme surjectif $\phi : \mathrm{H} \twoheadrightarrow \mathrm{GL}(\mathrm{W}) = \mathrm{GL}(\nu, \mathbf{F}_q)$ (*Indication :* on pourra utiliser les relations (23)).

b) Montrer que le noyau de ϕ est isomorphe au groupe additif des matrices symétriques $\nu \times \nu$ (*Indication :* on pourra utiliser les relations (23)).

c) En déduire que $\mathrm{S} := \phi^{-1}(\mathrm{T}_\nu(\mathbf{F}_q))$ est un p-sous-groupe de Sylow de $\mathrm{Sp}_{2\nu}(\mathbf{F}_q)$ (*cf.* exerc. I.2.13 pour la définition du p-sous-groupe de Sylow $\mathrm{T}_\nu(\mathbf{F}_q)$ de $\mathrm{GL}_\nu(\mathbf{F}_q)$). Donner une description matricielle de S en utilisant les relations (23).

7.4. Groupe dérivé. — On rappelle que le groupe dérivé $\mathrm{D}(\mathrm{G})$ d'un groupe G est le sous-groupe de G engendré par les commutateurs de G.

Théorème 7.9. — *On suppose* $\mathrm{car}(\mathbf{K}) \neq 2$ *et* $\nu \geqslant 2$. *On a* $\mathrm{D}(\mathrm{Sp}_{2\nu}(\mathbf{K})) = \mathrm{Sp}_{2\nu}(\mathbf{K})$.

Démonstration. — Par le th. 7.1, il suffit de montrer que toute transvection symplectique peut s'écrire comme un commutateur. Soit $\tau(x) = x + \lambda b(e,x)e$, avec $e \in \mathrm{V}$ et $\lambda \in \mathbf{K}$, une telle transvection. Le vecteur e est contenu dans un plan hyperbolique $\mathrm{P} = \langle e, f\rangle$ (lemme 4.9) et, comme $\nu \geqslant 2$, on peut écrire $\mathrm{V} = \mathrm{P} \overset{\perp}{\oplus} \mathrm{Q} \overset{\perp}{\oplus} \mathrm{W}$, où $\mathrm{Q} = \langle e', f'\rangle$ est aussi un plan hyperbolique.

Dans une base de V obtenue en complétant (e, e', f, f') par une base de W, la transvection τ a pour matrice par blocs $\begin{pmatrix} N(\lambda) & 0 \\ 0 & I_{2\nu-4} \end{pmatrix}$, où

$$N(\lambda) := \begin{pmatrix} 1 & 0 & \lambda & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Il suffit donc d'exprimer la matrice $N(\tau)$ comme commutateurs d'éléments de $\mathrm{Sp}_4(\mathbf{K})$. D'après (23), les matrices

$$U_1 = \begin{pmatrix} A_1 & 0 \\ 0 & {}^tA_1^{-1} \end{pmatrix}, \quad U_2 = \begin{pmatrix} I_2 & A_2 \\ 0 & I_2 \end{pmatrix}$$

sont symplectiques, pourvu que A_2 soit symétrique. Si on prend

$$A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \frac{1}{2}\lambda \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

on vérifie l'égalité $U_1U_2U_1^{-1}U_2^{-1} = N(\lambda)$, ce qui termine la démonstration. □

Simplicité. — La simplicité des groupes projectifs symplectiques finis fournit une nouvelle liste infinie de groupes finis simples.

Théorème 7.10. — *On suppose* $\mathrm{car}(\mathbf{K}) \neq 2$ *et* $\nu \geqslant 2$. *Le groupe* $\mathrm{PSp}_{2\nu}(\mathbf{K})$ *est simple.*

Démonstration. — Ce théorème se déduit du th. 7.9, comme dans le cas des groupes PSL, par la méthode d'Iwasawa, en considérant l'action fidèle et transitive du groupe sur l'espace projectif $X := \mathbf{P}^{2\nu-1}(\mathbf{K})$. Nous disposons en effet pour chaque droite $x \in X$ du groupe abélien (isomorphe à $\mathbf{K}$) des transvections symplectiques de droite x, et la seule hypothèse restant à vérifier pour appliquer le th. 2.16 est que l'action est primitive, c'est-à-dire que les stabilisateurs sont des sous-groupes maximaux.

L'action de $\mathrm{Sp}_{2\nu}(\mathbf{K})$ sur X est transitive : étant deux droites vectorielles de V, il existe par le théorème de Witt une isométrie qui envoie l'une sur l'autre (*cf.* aussi la preuve du lemme 7.3). Mais cette action n'est pas 2-transitive : l'action diagonale de $G := \mathrm{Sp}_{2\nu}(\mathbf{K})$ sur $\{(x, y) \in X \times X \mid x \neq y\}$ a deux orbites :

– l'orbite O_1 des couples de droites (x, y) engendrant un plan hyperbolique ;

– l'orbite O_2 des couples de droites (x, y) engendrant un plan totalement isotrope.

En effet, la restriction de la forme symplectique b à un plan est soit hyperbolique, soit nulle. Par le théorème de Witt, étant donnés deux plans dans V du même type, il existe une isométrie de V envoyant l'un sur l'autre.

Pour montrer que l'action est primitive, on doit donc revenir à la définition et montrer que le stabilisateur G_x d'un point $x \in X$ est maximal. Supposons donc $G_x < H \leq G$. On doit montrer $H = G$.

On rappelle que $Hx := \{hx \mid h \in H\} \subseteq X$ est l'orbite de x sous l'action induite de H ; comme $G_x \neq H$, elle n'est pas réduite à $\{x\}$. Regardons les sous-ensembles gHx de X lorsque g décrit G (parmi eux, on trouve l'orbite Hx).

Tout d'abord, leur réunion $\bigcup_{g\in G} gHx$ contient $\bigcup_{g\in G} gx$, qui n'est autre que l'orbite de x ; c'est donc bien X tout entier puisque l'action de G sur X est transitive.

Ensuite, si $gHx \cap g'Hx \neq \emptyset$, il existe $h, h' \in H$ tels que $ghx = g'h'x$, donc $h^{-1}g^{-1}g'h' \in G_x$ donc $g^{-1}g' \in H$, ce qui implique $gHx = g'Hx$. Ainsi les $(gHx)_{g\in G}$ distincts réalisent une partition de X.

Posons

$$\Gamma := \{(y,z) \in X \times X \mid y \neq z,\ y \text{ et } z \text{ sont dans le même } gHx\}.$$

Comme $Hx \neq \{x\}$, l'ensemble Γ n'est pas vide.

Si $(y,z) \in \Gamma$, on a $y, z \in g_0Hx$ pour un certain $g_0 \in G$ et pour tout $g \in G$, gy et gz sont dans gg_0Hx. En d'autres termes, Γ est stable par l'action diagonale de G, donc c'est une réunion d'orbites. Mais il n'y a que deux orbites.

Si $\Gamma = O_1$, on a, pour tout $y \neq z$,

$$y \text{ et } z \text{ sont dans le même } gHx \iff y \text{ et } z \text{ engendrent un plan hyperbolique}$$

Mais pour toutes droites distinctes y et z, il existe $t \in X$ qui n'est orthogonal ni à y ni à z (tout simplement parce que V ne peut être la réunion des deux hyperplans $y^\perp$ et $z^\perp$). Les droites y et t engendrent alors un plan hyperbolique, donc y et t sont dans le même gHx ; mais de même, les droites z et t engendrent alors un plan hyperbolique, donc z et t sont dans le même gHx. On en déduit que y et z sont dans le même gHx. Comme y et z sont quelconques distinctes, cela contredit $\Gamma = O_1$.

On écarte de façon similaire le cas $\Gamma = O_2$. On a donc $\Gamma = O_1 \sqcup O_2$: toutes droites distinctes y et z sont dans le même gHx. En particulier, tout $y \neq x$ est dans Hx. Pour tout $g' \in G$, ou bien $g'x = x$ et $g \in G_x \subseteq H$, ou bien $y := g'x \neq x$ et il existe $h \in H$ tel que $g'x = hx$, soit $h^{-1}g' \in G_x \subseteq H$. On en déduit $g' \in H$ et $H = G$.

On a donc montré que les stabilisateurs sont des sous-groupes maximaux de G. L'action de $G = Sp_{2\nu}(\mathbf{K})$ sur $X = \mathbf{P}^{2\nu-1}(\mathbf{K})$ est primitive. Comme elle est aussi fidèle, le th. 7.9 dit alors que tout sous-groupe distingué non trivial de $Sp_{2\nu}(\mathbf{K})$ contient $D(Sp_{2\nu}(\mathbf{K}))$. Par le th. 7.9, il est donc égal à $Sp_{2\nu}(\mathbf{K})$, qui est ainsi un groupe simple. □

***Remarque 7.11* (Cas de la caractéristique 2).** — Pour tout corps $\mathbf{K}$, on peut toujours définir un groupe comme en (22) par

$$Sp_{2\nu}(\mathbf{K}) := \{U \in GL_{2\nu}(\mathbf{K}) \mid {}^tUJ_{2\nu}U = J_{2\nu}\}.$$

Beaucoup des résultats démontrés plus haut lorsque $\mathrm{car}(\mathbf{K}) \neq 2$ restent vrais en caractéristique 2. On en particulier :

- $Sp_2(\mathbf{K}) \simeq SL_2(\mathbf{K})$;
- $Sp_{2\nu}(\mathbf{K}) \leq SL_{2\nu}(\mathbf{K})$;
- $Z(Sp_{2\nu}(\mathbf{K})) = \{\pm I_{2\nu}\}$ (le centre est donc trivial en caractéristique 2) ;
- $|Sp_{2\nu}(\mathbf{F}_q)|$ est donné par la formule (26) et, en caractéristique 2, $PSp_{2\nu}(\mathbf{F}_q) = Sp_{2\nu}(\mathbf{F}_q)$;
- pour $\nu \geqslant 2$, on a $D(Sp_{2\nu}(\mathbf{K})) = Sp_{2\nu}(\mathbf{K})$ et $PSp_{2\nu}(\mathbf{K})$ est simple, sauf pour $Sp_4(\mathbf{F}_2) = PSp_4(\mathbf{F}_2) \simeq \mathfrak{S}_6$, dont le groupe dérivé est $\mathfrak{A}_6$ (prop. I.5.9).

On obtient donc une quatrième série de groupes finis simples $PSp_{2\nu}(\mathbf{F}_q)$ [16].

16. Pour des raisons que vous comprendrez plus tard, ce groupe est aussi noté $C_\nu(q)$, pour $\nu \geqslant 2$.

8. Groupe orthogonal

On étudie ici quelques propriétés de base du groupe orthogonal. La situation est beaucoup plus compliquée que dans le cas symplectique, vu qu'il peut y avoir beaucoup de formes quadratiques non équivalentes sur un même espace vectoriel.

8.1. La dimension 2. — Si $\dim(V) = 2$, à une constante multiplicative près (ce qui ne change pas le groupe orthogonal associé), toute forme quadratique s'écrit

$$f(x) = x_1^2 - \alpha x_2^2.$$

Il y a deux cas, suivant que α est un carré ou non dans $\mathbf{K}$.

Cas où α est un carré. La forme f admet alors des vecteurs isotropes non nuls et V est un plan hyperbolique pour f : il existe une base (e_1, e_2) de V dans laquelle

$$f(x_1, x_2) = 2x_1x_2.$$

Les droites engendrées par e_1 et e_2 étant les seules directions isotropes, elles sont ou bien préservées, ou bien échangées par un élément du groupe orthogonal $O(V, f)$. On en déduit que les éléments de $O(V, f)$ sont de la forme $R_\lambda := \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ ou $S_\lambda := \begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & 0 \end{pmatrix}$, pour $\lambda \in \mathbf{K}^\times$. On a donc

$$\begin{aligned} \mathrm{SO}(V, f) &\simeq \{R_\lambda \mid \lambda \in \mathbf{K}^\times\}, \\ \mathrm{O}(V, f) &\simeq \{R_\lambda, S_\lambda \mid \lambda \in \mathbf{K}^\times\} = \mathrm{SO}(V, f) \sqcup S_1 \cdot \mathrm{SO}(V, f). \end{aligned}$$

Les transformations S_λ de $O(V, f) - SO(V, f)$ sont des réflexions (par rapport à la droite engendrée par $e_1 + \lambda e_2$). Le groupe $SO(V, f)$ est abélien. Comme

$$S_1 R_\lambda S_1^{-1} = R_{\lambda^{-1}},$$

le groupe $O(V, f)$ n'est pas abélien, sauf si $\mathbf{K} = \mathbf{F}_3$ (dans ce cas, c'est $\{I_2, -I_2, S_1, -S_1\}$, isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$).

Exemples 8.1. — 1° Lorsque $\mathbf{K}$ est quadratiquement clos, on est toujours dans ce cas.

2° Lorsque $\mathbf{K} = \mathbf{R}$, on est dans ce cas uniquement lorsque la signature est $(1, 1)$. On a donc $SO_{1,1}(\mathbf{R}) \simeq \mathbf{R}^\times$. Dans une base orthogonale, où la forme quadratique est donnée par $x_1^2 - x_2^2$, on vérifie que les isométries directes ont pour matrice

$$\begin{pmatrix} \frac{\varepsilon}{\sqrt{1-\beta^2}} & \frac{-\varepsilon\beta}{\sqrt{1-\beta^2}} \\ \frac{-\varepsilon\beta}{\sqrt{1-\beta^2}} & \frac{\varepsilon}{\sqrt{1-\beta^2}} \end{pmatrix}.$$

avec $\varepsilon = \pm 1$. Le facteur $\frac{1}{\sqrt{1-\beta^2}}$ (qui est relié au paramètre λ de la rotation R_λ définie ci-dessus par la formule $\beta = \frac{1-\lambda}{1+\lambda}$, tandis que ε est le signe de λ) est celui qui intervient dans les formules de Lorentz en relativité (la vitesse de la lumière est ici égale à 1 ; voir exerc. 11.6).

3° Lorsque $\mathbf{K} = \mathbf{F}_q$, on est dans ce cas pour la forme $\langle 1, -1 \rangle$. Avec les notations de la note 11 et de l'ex. 5.6.3°, on a $SO_2^+(\mathbf{F}_q) \simeq \mathbf{F}_q^\times$, cyclique d'ordre $q - 1$. On vérifie que $O_2^+(\mathbf{F}_q)$ est isomorphe au groupe diédral D_{q-1} (*cf.* ex. I.1.4.4°).

Cas où α n'est pas un carré. La forme f est alors anisotrope et on vérifie par un calcul direct qu'on a

$$\begin{aligned} \mathrm{SO}(\mathrm{V},f) &\simeq \left\{ \mathrm{R}_{a,c} := \begin{pmatrix} a & c\alpha \\ c & a \end{pmatrix} \mid a^2 - \alpha c^2 = 1 \right\}, \\ \mathrm{O}(\mathrm{V},f) &\simeq \left\{ \mathrm{R}_{a,c},\ \mathrm{S}_{a,c} := \begin{pmatrix} a & -c\alpha \\ c & -a \end{pmatrix} \mid a^2 - \alpha c^2 = 1 \right\} \\ &= \mathrm{SO}(\mathrm{V},f) \sqcup \mathrm{S}_{1,0} \cdot \mathrm{SO}(\mathrm{V},f). \end{aligned}$$

À nouveau, le groupe $\mathrm{SO}(\mathrm{V},f)$ est abélien. Ses éléments sont appelés *rotations* et $\mathrm{O}(\mathrm{V},f) - \mathrm{SO}(\mathrm{V},f)$ est constitué de réflexions : l'isométrie de matrice $\mathrm{S}_{a,c}$ dans la base (e_1,e_2) est la symétrie orthogonale par rapport à la droite engendrée par $(1+a)e_1 + ce_2$.

Les groupes $\mathrm{SO}(\mathrm{V},f)$ et $\mathrm{O}(\mathrm{V},f)$ s'interprètent en terme du corps $\mathbf{K}[\sqrt{\alpha}] = \{a + c\sqrt{\alpha} \mid a, c \in \mathbf{K}\}$. Si $x = a + c\sqrt{\alpha} \in \mathbf{K}$, son « conjugué » est $\bar{x} = a - c\sqrt{\alpha}$ et le morphisme « norme » $\mathrm{N} : \mathbf{K}[\sqrt{\alpha}] \to \mathbf{K}$ défini par $\mathrm{N}(x) = x\bar{x}$ vérifie $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$ et $(\mathrm{N}(x) = 0) \Leftrightarrow (x = 0)$.

Si $x \in \mathbf{K}[\sqrt{\alpha}]^\times$, il opère sur le $\mathbf{K}$-espace vectoriel $\mathbf{K}[\sqrt{\alpha}]$, de dimension 2, par la multiplication par x, ce qui donne un morphisme de groupes injectif

$$\rho : \mathbf{K}[\sqrt{\alpha}]^\times \to \mathrm{GL}_2(\mathbf{K}).$$

Si $x = a + c\sqrt{\alpha}$, la matrice de $\rho(x)$ dans la base $\{1, \sqrt{\alpha}\}$ de $\mathbf{K}[\sqrt{\alpha}]$ est $\begin{pmatrix} a & c\alpha \\ c & a \end{pmatrix}$. Il s'ensuit que ρ induit un isomorphisme entre le groupe (abélien) des éléments de $\mathbf{K}[\sqrt{\alpha}]$ de norme 1 et le groupe $\mathrm{SO}(\mathrm{V},f)$.

La conjugaison peut aussi être vue comme un élément de $\mathrm{GL}_2(\mathbf{K})$, dont la matrice dans la base $\{1, \sqrt{\alpha}\}$ de $\mathbf{K}[\sqrt{\alpha}]$ est $\mathrm{S}_{1,0}$. Le groupe $\mathrm{O}(\mathrm{V},f)$ est donc isomorphe au sous-groupe des automorphismes de $\mathbf{K}[\sqrt{\alpha}]$ engendré par la multiplication par les éléments de norme 1 et la conjugaison.

Le centre de $\mathrm{O}(\mathrm{V},f)$ est $\{\pm \mathrm{Id}_\mathrm{V}\}$: si la multiplication par $x \in \mathbf{K}[\sqrt{\alpha}]$ est dans le centre, elle commute à la conjugaison, c'est-à-dire qu'on a pour tout $y \in \mathbf{K}[\sqrt{\alpha}]$ de norme 1,

$$\overline{xy} = x\overline{y}.$$

On en déduit $\overline{x} = x$, donc $x \in \mathbf{K}$. Comme $\mathrm{N}(x) = 1$, on a $x = \pm 1$.

Dans le cas $\mathbf{K} = \mathbf{R}$, le corps $\mathbf{R}[\sqrt{\alpha}]$ est $\mathbf{C}$, la conjugaison est la conjugaison complexe et le groupe des éléments de norme 1 est le groupe des complexes de module 1.

Exemples 8.2. — 1° Lorsque $\mathbf{K} = \mathbf{R}$, on est dans ce cas uniquement lorsque la signature est $(2,0)$ (forme définie positive) ou $(0,2)$ (forme définie négative) ; les deux cas donnent le même groupe spécial orthogonal $\mathrm{SO}_2(\mathbf{R})$, qui est donc isomorphe au groupe multiplicatif des nombres complexes de module 1. On retrouve la description usuelle du groupe des isométries du plan euclidien :

$$\begin{aligned} \mathrm{SO}_2(\mathbf{R}) &= \left\{ \mathrm{R}_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mid \theta \in \mathbf{R} \right\}, \\ \mathrm{O}_2(\mathbf{R}) &= \left\{ \mathrm{R}_\theta,\ \mathrm{S}_\theta := \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \mid \theta \in \mathbf{R} \right\}. \end{aligned}$$

2° Lorsque $\mathbf{K} = \mathbf{F}_q$, avec les notations de la note 11 et de l'ex. 5.6.3°, le corps $\mathbf{F}_q[\sqrt{\alpha}]$ est $\mathbf{F}_{q^2}$, la conjugaison est $x \mapsto x^q$ (*cf.* ex. 9.1), donc $\mathrm{N}(x) = x^{q+1}$ et le groupe $\mathrm{SO}_2^-(\mathbf{F}_q)$ est isomorphe au groupe multiplicatif $\{x \in \mathbf{F}_{q^2}^\times \mid x^{q+1} = 1\}$, cyclique d'ordre $q+1$ (*cf.* (28)). De plus, comme $\mathrm{S}_{1,0}\mathrm{R}_{a,c}\mathrm{S}_{1,0}^{-1} = \mathrm{R}_{a,-c} = \mathrm{R}_{a,c}^{-1}$, on voit que le groupe $\mathrm{O}_2^-(\mathbf{F}_q)$ est isomorphe au groupe diédral D_{q+1} (*cf.* ex. I.1.4.4°).

8.2. Le groupe $\mathrm{SO}_3(\mathbf{R})$. — Commençons par un petit résultat plus général que ce dont nous aurons besoin.

Lemme 8.3. — *Soit* $\mathbf{K}$ *un corps et soit* f *la forme quadratique sur* $\mathbf{K}^n$ *définie par*

$$f(x_1, \dots, x_n) = x_1^2 + \cdots + x_n^2.$$

Toute isométrie qui est directe si n est impair, indirecte si n est pair, admet 1 comme valeur propre.

Démonstration. — Soit U la matrice d'une telle isométrie dans la base canonique de $\mathbf{K}^n$. On a alors ${}^t\mathrm{UU} = \mathrm{I}_n$ et

$$\begin{aligned}\text{dét}(\mathrm{I}_n - \mathrm{U}) = \text{dét}({}^t\mathrm{UU} - \mathrm{U}) &= \text{dét}({}^t\mathrm{U} - \mathrm{I}_n)\det(\mathrm{U}) \\ &= \text{dét}(\mathrm{U} - \mathrm{I}_n)\det(\mathrm{U}) = (-1)^n \det(\mathrm{U})\,\text{dét}(\mathrm{I}_n - \mathrm{U}).\end{aligned}$$

Si $(-1)^n \det(\mathrm{U}) = -1$, comme la caractéristique de $\mathbf{K}$ n'est pas 2, on en déduit $\text{dét}(\mathrm{I}_n - \mathrm{U}) = 0$. □

En particulier, pour toute isométrie directe u de l'espace euclidien $\mathbf{R}^3$, il existe x de norme 1 tel que $u(x) = x$. L'isométrie u laisse alors stable le plan $x^\perp$ sur lequel u est une rotation. Dans n'importe quelle base orthonormale commençant par x, la matrice de u est donc

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

On peut en particulier déterminer l'angle θ au signe près par la relation

$$\mathrm{tr}(u) = 1 + 2\cos\theta.$$

Notons d'ailleurs que le signe de θ n'est bien déterminé que si on choisit une orientation de l'espace $\mathbf{R}^3$ *et* une orientation de l'axe $\mathbf{R}x$.

Soit $\mathbf{B}^3$ la boule unité fermée de centre 0 dans $\mathbf{R}^3$, que l'on suppose orienté. À tout $y \in \mathbf{B}^3$ non nul, on associe la rotation d'axe $\mathbf{R}y$ et d'angle $\|y\|\pi$; à 0, on associe $\mathrm{Id}_{\mathbf{R}^3}$. On obtient ainsi toutes les rotations, d'où une surjection

$$p : \mathbf{B}^3 \to \mathrm{SO}_3(\mathbf{R})$$

dont on vérifie qu'elle est continue. Inversement, étant donnée une rotation u, on choisit un vecteur x directeur unitaire de son axe de façon que l'angle θ de la rotation soit dans $[0, \pi]$ (c'est-à-dire $\sin\theta \geqslant 0$). L'antécédent de u par p est $y = x\theta/\pi$; il est unique sauf si $\theta = \pi$, c'est-à-dire lorsque u est un renversement, auquel cas il y a deux antécédents, x et $-x$. L'application p est donc injective sur l'intérieur de $\mathbf{B}^3$ et elle identifie tout vecteur de sa frontière $\mathbf{S}^3$ avec son opposé. Or, topologiquement, cette sphère n'est rien d'autre que la demi-sphère unité $\mathbf{S}'^4 \subseteq \mathbf{R}^4$. On en déduit que $\mathrm{SO}_3(\mathbf{R})$ est homéomorphe au quotient de

$\mathbf{S}^4$ par la relation d'équivalence $y \sim -y$. Ce dernier espace n'est autre que $\mathbf{P}^3(\mathbf{R})$ (associer à une droite vectorielle de $\mathbf{R}^4$ ses deux points d'intersection avec $\mathbf{S}^4$). On a montré :

Le groupe topologique $\mathrm{SO}_3(\mathbf{R})$ *est homéomorphe à* $\mathbf{P}^3(\mathbf{R})$.

Revenant à l'interprétation de $\mathrm{SO}_3(\mathbf{R})$ comme $\mathbf{B}^3/\sim$, on « voit » que l'image dans $\mathrm{SO}_3(\mathbf{R})$ d'un diamètre de $\mathbf{B}^3$ est un lacet γ qui n'est pas homotope à zéro : $[\gamma] \neq 0$ dans $\pi_1(\mathrm{SO}_3(\mathbf{R}))$. En revanche, si on fait l'aller-retour le long du diamètre, il devient un lacet dans $\mathbf{B}^3$, qu'on peut donc contracter sur un point. On a donc $2[\gamma] = 0$ dans $\pi_1(\mathrm{SO}_3(\mathbf{R}))$.

On peut montrer

$$\pi_1(\mathrm{SO}_3(\mathbf{R})) = \langle[\gamma]\rangle \simeq \mathbf{Z}/2\mathbf{Z}.$$

Le revêtement universel de $\mathrm{SO}_3(\mathbf{R})$ est le groupe $\mathrm{SU}_2(\mathbf{C})$ (déf. 10.1) ou $\mathrm{Spin}_3(\mathbf{R})$ (*cf.* § III.6.4) : un morphisme $\mathrm{SU}_2(\mathbf{C}) \to \mathrm{SO}_3(\mathbf{R})$ de noyau $\{\pm \mathrm{I}_2\}$ sera étudié dans le th. 11.2 (*cf.* aussi note 29).

8.3. Le groupe de Lorentz $\mathrm{SO}_{1,3}(\mathbf{R})$. — Le groupe $\mathrm{SO}_{1,3}(\mathbf{R})$ des isométries directes de l'espace vectoriel $\mathbf{R}^4$ muni de la forme quadratique

$$f(x_0, \ldots, x_3) = x_0^2 - x_1^2 - x_2^2 - x_3^2$$

(espace-temps de Minkowski) est important en physique. On l'appelle le *groupe de Lorentz*.

On note $(e_0, \ldots, e_3)$ la base canonique de $\mathbf{R}^4$ et $\mathrm{H} = \langle e_1, e_2, e_3\rangle = e_0^\perp$ la partie « espace ». La paire $(\mathrm{H}, -f)$ est donc l'espace euclidien standard à trois dimensions. Si $x \in \mathrm{H}$ est unitaire ($f(x) = -1$), la restriction de f au plan $\mathrm{P}_x := \langle e_0, x\rangle$ a pour signature $(1,1)$. Une isométrie directe de P_x a donc pour matrice

$$\begin{pmatrix} \frac{\varepsilon}{\sqrt{1-\beta^2}} & \frac{-\varepsilon\beta}{\sqrt{1-\beta^2}} \\ \frac{-\varepsilon\beta}{\sqrt{1-\beta^2}} & \frac{\varepsilon}{\sqrt{1-\beta^2}} \end{pmatrix}$$

dans la base (e_0, x) (ex. 8.1.2°). On note $r_{\varepsilon,\beta,x}$ l'isométrie directe de V qui a cette matrice sur P_x et qui est l'identité sur $\mathrm{P}_x^\perp$. Elle « préserve le sens du temps » si $\varepsilon = 1$, elle l'inverse si $\varepsilon = -1$.

On appelle *rotation espace* les rotations de H (prolongées par l'identité sur $\mathbf{R}e_0$).

Proposition 8.4. *— Dans l'espace-temps de Minkowski, toute isométrie directe peut s'écrire comme le produit d'un $r_{\varepsilon,\beta,x}$ et d'une rotation espace.*

On verra plus bas (p. 86) que ε ne dépend que de l'isométrie, pas de la décomposition : il vaut 1 si l'isométrie préserve le sens du temps, -1 sinon.

Démonstration. — On écrit $u(e_0) = ae_0 + bx$, avec $x \in \mathrm{H}$ et $f(x) = -1$. Si on exprime le fait que $f(u(e_0)) = f(e_0) = 1$, on obtient $a^2 - b^2 = 1$, donc $|a| \geqslant 1$. On choisit β du signe de b avec $\beta^2 = 1 - \frac{1}{a^2} \geqslant 0$ et on prend $\varepsilon = a/|a|$. On a alors $u(e_0) = r_{\varepsilon,\beta,x}(e_0)$. On en déduit $r_{\varepsilon,\beta,x}^{-1} u(e_0) = e_0$. L'isométrie directe $r_{\varepsilon,\beta,x}^{-1} u$ laisse donc stable H et s'y restreint en une rotation, ce qui montre la proposition. □

8.4. Centre et générateurs. — Rappelons que si D est une droite non isotrope, on dispose d'une symétrie orthogonale (réflexion) s_D (de déterminant -1) par rapport à $D^\perp$. De même, si P est un plan sur lequel la forme quadratique est non dégénérée, on a $V = P \oplus P^\perp$ et le *renversement* r_P, défini par $r_P = (-1) \oplus 1$, est aussi une transformation orthogonale, élément de $SO(V, f)$.

Si $u \in O(V, f)$, on vérifie qu'on a $us_D u^{-1} = s_{u(D)}$ et $ur_P u^{-1} = r_{u(P)}$.

Proposition 8.5. — *Le centre de* $O(V, f)$ *est* $\{\pm \mathrm{Id}_V\}$*, sauf si* $\mathbf{K} = \mathbf{F}_3$ *et* V *est un plan hyperbolique*[17].

Si $\dim(V) \geqslant 3$*, le centre de* $SO(V, f)$ *est trivial si* $\dim(V)$ *est impair,* $\{\pm \mathrm{Id}_V\}$ *si* $\dim(V)$ *est pair.*

Si $\dim(V) = 2$, on a vu (§8.1) que $SO(V, f)$ est toujours abélien.

Démonstration. — Si $\dim(V) = 2$, la description explicite de $O(V, f)$ vue au § 8.1 donne le résultat. On suppose donc $\dim(V) \geqslant 3$.

Si $u \in O(V, f)$ commute aux éléments de $SO(V, f)$, on a $r_{u(P)} = ur_P u^{-1} = r_P$ pour tout plan hyperbolique P, donc $u(P) = P$ et u préserve les plans sur lesquels la forme f est non dégénérée.

Montrons que toute droite $D = \mathbf{K}x$ est intersection de deux plans P et Q de ce type.

Si D est non isotrope, on a $V = D \overset{\perp}{\oplus} D^\perp$, donc en prenant deux éléments distincts y et z d'une base orthogonale de $D^\perp$ (ce qui est possible puisque $\dim(V) \geqslant 3$), les plans $P = D \overset{\perp}{\oplus} \mathbf{K}y$ et $Q = D \overset{\perp}{\oplus} \mathbf{K}z$ conviennent. Si D est isotrope, on inclut D dans un plan hyperbolique P (sur lequel f est non dégénérée) et on complète x en une base (x, y) de P. Puisque $V = P \overset{\perp}{\oplus} P^\perp$ et que $\dim(V) \geqslant 3$, on peut choisir $z \in P^\perp$ non nul. Alors on peut prendre $Q = D \oplus \mathbf{K}(y + z)$.

Il s'ensuite que si $u \in O(V, f)$ commute à tous les éléments de $SO(V, f)$, il préserve toutes les droites ; c'est donc une homothétie (*cf.* note 2). Cela termine la preuve. □

Le quotient de $SO(V, f)$ par son centre est le *groupe projectif orthogonal*

$$PSO(V, f) := SO(V, f)/Z(SO(V, f)).$$

C'est un sous-groupe de $PSL(V)$; il opère donc fidèlement sur l'espace projectif $\mathbf{P}(V)$. On définit de la même façon le sous-groupe $PO(V, f) \leq PGL(V)$.

Exemples 8.6. — 1° Les groupes $O_{s,n-s}(\mathbf{R})$, $SO_{s,n-s}(\mathbf{R})$ et $PSO_{s,n-s}(\mathbf{R})$ sont des *variétés différentiables* de dimension $n(n-1)/2$. Leur nature topologique est différente : pour $n \geqslant 2$, parmi les groupes SO, seul $SO_n(\mathbf{R})$ est compact, et seul $SO_n(\mathbf{R})$ est connexe (*cf.* ex. 8.12.3°, exerc. 8.11 ; mais il n'est pas simplement connexe pour $n \geqslant 2$ (rem. 11.4)).

2° Les groupes $O_n(\mathbf{C})$, $SO_n(\mathbf{C})$ et $PSO_n(\mathbf{C})$ sont des *variétés complexes* de dimension $n(n-1)/2$.

Théorème 8.7. — *Les réflexions engendrent* $O(V, f)$.

17. On a vu que dans ce cas, $O(V, f)$ est abélien de cardinal 4.

Démonstration. — On raisonne par récurrence sur la dimension. Soit $u \in \mathrm{O}(\mathrm{V}, f)$ et soit $x_1 \in \mathrm{V}$ non isotrope ; on pose $x_2 := u(x_1)$. Puisque $f(x_1 + x_2) + f(x_1 - x_2) = 4f(x_1) \neq 0$, l'un au moins des éléments $x_1 - x_2$ ou $x_1 + x_2$ est non isotrope :

– si $x_1 - x_2$ est non isotrope, $s_{x_1-x_2}(x_1) = x_2$, donc $s_{x_1-x_2}u(x_1) = x_1$;

– si $x_1 + x_2$ est non isotrope, $s_{x_2}s_{x_1+x_2}(x_1) = s_{x_2}(-x_2) = x_2$, donc $s_{x_1+x_2}s_{x_2}u(x_1) = x_1$.

Dans les deux cas, on est ramené au cas où u fixe un vecteur non isotrope x_1, et on applique l'hypothèse de récurrence dans $x_1^\perp$. □

Remarque 8.8. — Cette démonstration montre que toute isométrie est produit d'au plus $2n$ réflexions ($n = \dim(\mathrm{V})$). Le théorème de Cartan-Dieudonné affirme qu'il suffit d'au plus n réflexions.

Théorème 8.9. — *Si* $\dim(\mathrm{V}) \geqslant 3$, *les renversements engendrent* $\mathrm{SO}(\mathrm{V}, f)$.

Démonstration. — Par le théorème précédent, tout élément de $\mathrm{SO}(\mathrm{V}, f)$ est produit d'un nombre pair de réflexions. Il suffit donc de montrer qu'un produit $s_{x_1}s_{x_2}$ de deux réflexions est un produit de renversements.

Si $\dim(\mathrm{V}) = 3$, on a $s_{x_1}s_{x_2} = (-s_{x_1})(-s_{x_2})$ et l'opposé d'une réflexion est un renversement (puisque la dimension de V est 3), d'où le résultat.

Si $\dim(\mathrm{V}) \geqslant 3$, on peut supposer x_1 et x_2 non colinéaires. Considérons le plan $\mathrm{P} := \langle x_1, x_2\rangle$. On va construire un espace vectoriel $\mathrm{W} \supseteq \mathrm{P}$, de dimension 3, sur lequel f est non dégénérée.

Si $\mathrm{P} \cap \mathrm{P}^\perp = \{0\}$, on prend $y \in \mathrm{P}^\perp$ non isotrope et $\mathrm{W} := \langle x_1, x_2, y\rangle$.

Si $\mathrm{P} \cap \mathrm{P}^\perp$ est non nul, il est de dimension 1 (car il ne contient pas x_1), engendré par un vecteur z. On prend $y \notin z^\perp$ et $\mathrm{W} := \langle x_1, x_2, y\rangle$. Un vecteur de $\mathrm{W} \cap \mathrm{W}^\perp$ est orthogonal à z, donc est dans P ; comme il est orthogonal à P, il est colinéaire à z. Enfin, comme il est orthogonal à y, il est nul.

Alors $s_{x_1}s_{x_2}$ agit par l'identité sur $\mathrm{W}^\perp$, donc laisse aussi stabel W. On est ainsi ramené au cas de la dimension 3 : sur W, l'isométrie $s_{x_1}|_\mathrm{W} s_{x_2}|_\mathrm{W}$ est le produit des renversements $-s_{x_1}|_\mathrm{W}$ et $-s_{x_2}|_\mathrm{W}$; on obtient alors $s_{x_1}s_{x_2}$ comme produit de leurs extensions sur V par l'identité sur $\mathrm{W}^\perp$, qui sont encore des renversements. □

Exercice 8.10. — Montrer que $\mathrm{O}_n(\mathbf{Q})$ est dense dans $\mathrm{O}_n(\mathbf{R})$ et que $\mathrm{SO}_n(\mathbf{Q})$ est dense dans $\mathrm{SO}_n(\mathbf{R})$ (*Indication :* on pourra utiliser le th. 8.7).

Exercice 8.11. — Lorsque $n \geqslant 2$, montrer que $\mathrm{SO}_n(\mathbf{R})$ est connexe et que $\mathrm{O}_n(\mathbf{R})$ a deux composantes connexes (*Indication :* on pourra utiliser le th. 8.7).

8.5. Norme spinorielle et groupe dérivé. — La situation pour le groupe orthogonal est beaucoup plus compliquée que pour le groupe symplectique et nous ne donnerons pas toutes les démonstrations ni tous les détails. Une des raisons en est l'existence d'un morphisme

$$\theta : \mathrm{O}(\mathrm{V}, f) \to \mathbf{K}^\times / \mathbf{K}^{\times 2}$$

appelé *norme spinorielle,* qui vérifie la propriété

$$\theta(s_x) = f(x) \in \mathbf{K}^\times / \mathbf{K}^{\times 2}, \tag{27}$$

pour tout $x \in \mathrm{V}$ non isotrope. Nous ne démontrerons que plus tard (§ III.6.3, cor. 6.8) l'existence de ce morphisme [18]. Notons cependant que comme $\mathbf{K}^\times/\mathbf{K}^{\times 2}$ est abélien, son noyau, noté $\mathrm{O}'(\mathrm{V},f)$, contient le groupe dérivé $\mathrm{D}(\mathrm{O}(\mathrm{V},f))$, et le noyau $\mathrm{SO}'(\mathrm{V},f) := \mathrm{O}'(\mathrm{V},f) \cap \mathrm{SO}(\mathrm{V},f)$ de sa restriction à $\mathrm{SO}(\mathrm{V},f)$ contient $\mathrm{D}(\mathrm{SO}(\mathrm{V},f))$.

Exemples 8.12. — 1° Lorsque $\mathbf{K}$ est quadratiquement clos, $\mathbf{K}^\times/\mathbf{K}^{\times 2}$ est trivial, donc aussi θ.

2° Si $\mathbf{K} = \mathbf{R}$, le groupe $\mathbf{R}^\times/\mathbf{R}^{\times 2}$ a deux éléments, à savoir les classes de 1 et de -1.

Si f est définie positive, θ prend ses valeurs dans $\mathbf{R}^{\times +}/\mathbf{R}^{\times 2}$, donc θ est trivial et $\mathrm{SO}'_n(\mathbf{R}) = \mathrm{SO}_n(\mathbf{R})$.

Si f est définie négative, toute réflexion a pour image -1 dans $\mathbf{R}^\times/\mathbf{R}^{\times 2}$, donc θ est le morphisme déterminant et est trivial sur $\mathrm{SO}_n(\mathbf{R})$.

Pour avoir un morphisme θ intéressant, il faut donc regarder les groupes $\mathrm{O}_{s,t}(\mathbf{R})$ avec s et t non nuls (c'est-à-dire les cas où l'indice est $\geqslant 1$). Dans le cas de $\mathrm{O}_{1,m}(\mathbf{R})$, la forme f est donnée sur $\mathbf{R}^{m+1}$ par

$$f(x_0,\dots,x_m) = x_0^2 - x_1^2 - \cdots - x_m^2.$$

Ce groupe agit sur la quadrique affine $\mathrm{Q} := \{x \in \mathbf{R}^{m+1} \mid f(x) = 1\}$. Or celle-ci a deux composantes connexes Q^+ et Q^- selon que x_0 est positif ou négatif. On peut donc définir un morphisme de groupes

$$\theta' : \mathrm{O}_{1,m}(\mathbf{R}) \longrightarrow \mathfrak{S}_{\{\mathrm{Q}^+,\mathrm{Q}^-\}} \simeq \mathbf{Z}/2\mathbf{Z}.$$

Si x n'est pas isotrope, on vérifie que $\theta'(s_x) = \mathrm{Id}$ si et seulement si $f(x) < 0$ (on voit bien ce qui se passe sur un dessin en dimension 2). Cela signifie que le morphisme θ' n'est autre que le produit dét·θ, donc qu'on a l'égalité [19]

$$\mathrm{SO}'_{1,m}(\mathbf{R}) = \{u \in \mathrm{SO}_{1,m}(\mathbf{R}) \mid u(\mathrm{Q}^+) = \mathrm{Q}^+\},$$

sous-groupes d'indice 2 dans $\mathrm{SO}_{1,m}(\mathbf{R})$.

En relativité, on travaille dans l'espace-temps de Minkowski, qui correspond au cas $m = 3$; le groupe $\mathrm{SO}_{1,3}(\mathbf{R})$ est le groupe de Lorentz (§8.3) et le groupe $\mathrm{SO}'_{1,3}(\mathbf{R})$ des transformations qui préservent le sens du temps, le *groupe de Lorentz restreint* (*cf.* exerc. 11.6).

La situation est analogue si $s, t \geqslant 2$, mais la quadrique Q définie ci-dessus est maintenant connexe. Il faut regarder à la place les sous-espaces vectoriels maximaux $\mathrm{W} \subseteq \mathbf{R}^{s+t}$ sur lesquels la forme f est définie positive, comme par exemple $\langle e_1,\dots,e_s\rangle$. On voit facilement qu'ils sont tous de dimension s et on vérifie qu'ils forment une « famille connexe » (dans le cas $s = 1$, ce sont les droites engendrées par les points de Q, qui sont paramétrées par une de ses composantes connexes). On peut alors définir de manière continue une orientation o_W sur chacun de ces sous-espaces vectoriels W. L'image de W par une isométrie u est encore un sous-espace du même type et on obtient

$$\mathrm{SO}'_{s,t}(\mathbf{R}) = \{u \in \mathrm{SO}_{s,t}(\mathbf{R}) \mid u(o_\mathrm{W}) = o_{u(\mathrm{W})}\}.$$

---

18. Comme les réflexions engendrent $\mathrm{O}(\mathrm{V},f)$, la relation (27) définit uniquement θ ; cependant, il faut vérifier que cette définition a un sens, c'est-à-dire que si $u \in \mathrm{O}(\mathrm{V},f)$ se décompose en $u = s_{x_1} \circ \cdots \circ s_{x_r}$, alors $f(x_1)\cdots f(x_r) \in \mathbf{K}^\times/\mathbf{K}^{\times 2}$ est indépendant de la décomposition de u choisie.

19. Le groupe $\mathrm{SO}'_{1,m}(\mathbf{R})$ est le groupe de la géométrie hyperbolique, il agit transitivement sur Q^+, qui est un modèle de l'espace hyperbolique de dimension m. Le stabilisateur de e_0 est isomorphe à $\mathrm{SO}_m(\mathbf{R})$, qui est connexe par l'exerc. 8.11. Cela permet de montrer que $\mathrm{SO}'_{1,m}(\mathbf{R})$ est connexe.

De façon plus « concrète », dans une base où la forme quadratique s'écrit

$$f(x_1,\dots,x_{s+t}) = x_1^2+\cdots+x_s^2-x_{s+1}^2-\cdots-x_{s+t}^2,$$

la matrice U d'un élément de $\mathrm{SO}_{s,t}(\mathbf{R})$ s'écrit sous forme de blocs

$$\mathrm{U}=\begin{pmatrix}\mathrm{A} & \mathrm{B}\\ \mathrm{C} & \mathrm{D}\end{pmatrix},$$

où la matrice A est carrée d'ordre s. On voit que la matrice A est inversible [20]. On a alors

$$\mathrm{SO}'_{s,t}(\mathbf{R}) = \{\mathrm{U}\in\mathrm{SO}_{s,t}(\mathbf{R}) \mid \det(\mathrm{A})>0\} = \{\mathrm{U}\in\mathrm{SO}_{s,t}(\mathbf{R}) \mid \det(\mathrm{D})>0\}.$$

On peut montrer que ce groupe est connexe [21].

3° Lorsque (V,f) est un plan hyperbolique, on note r_λ la « rotation » de matrice R_λ dans une base hyperbolique (e_1,e_2) de V (*cf.* § 8.1). On a

$$r_\lambda = s_{\lambda e_1-e_2}s_{e_1-e_2},$$

donc $\theta(r_\lambda) = f(\lambda e_1-e_2)f(e_1-e_2) = 4\lambda \equiv \lambda$ dans $\mathbf{K}^\times/\mathbf{K}^{\times 2}$ et le morphisme $\theta|_{\mathrm{SO}(\mathrm{V},f)}$: $\mathrm{SO}(\mathrm{V},f)\to\mathbf{K}^\times/\mathbf{K}^{\times 2}$ est surjectif.

Si l'indice ν de f est $\geqslant 1$, c'est-à-dire qu'il existe un vecteur isotrope non nul, V contient un plan hyperbolique. L'exemple 3° ci-dessus montre que le morphisme

$$\theta|_{\mathrm{SO}(\mathrm{V},f)} : \mathrm{SO}(\mathrm{V},f)\to\mathbf{K}^\times/\mathbf{K}^{\times 2}$$

est alors surjectif. En particulier, si $\nu\geqslant 1$ et que $\mathbf{K}$ n'est pas quadratiquement clos ($\mathbf{K}^{\times 2}\neq\mathbf{K}^\times$), on a $\mathrm{D}(\mathrm{O}(\mathrm{V},f))\subseteq\mathrm{SO}'(\mathrm{V},f)\subsetneq\mathrm{SO}(\mathrm{V},f)$.

On a en fait un résultat plus précis [22].

***Théorème 8.13* (Eichler).** — *Soit f une forme quadratique non dégénérée sur un espace vectoriel* V *de dimension* $\geqslant 3$. *Si l'indice* ν *de f est* $\geqslant 1$ *(c'est-à-dire si f a un vecteur isotrope non nul), on a*

$$\mathrm{SO}'(\mathrm{V},f) = \mathrm{D}(\mathrm{O}(\mathrm{V},f)) = \mathrm{D}(\mathrm{SO}(\mathrm{V},f))$$

et $\mathrm{SO}(\mathrm{V},f)/\mathrm{D}(\mathrm{SO}(\mathrm{V},f))\simeq\mathbf{K}^\times/\mathbf{K}^{\times 2}$.

Exemples 8.14. — 1° Si $\mathbf{K}=\mathbf{R}$ et que f est définie positive ou négative, on peut montrer qu'on a $\mathrm{D}(\mathrm{O}_n(\mathbf{R})) = \mathrm{D}(\mathrm{SO}_n(\mathbf{R})) = \mathrm{SO}_n(\mathbf{R})$.

Si $st>0$ et $s+t\geqslant 3$ (de sorte que f est d'indice $\geqslant 1$), le théorème montre que $\mathrm{D}(\mathrm{SO}_{s,t}(\mathbf{R}))$ est d'indice 2 dans $\mathrm{SO}_{s,t}(\mathbf{R})$.

3° Lorsque $\mathbf{K}=\mathbf{F}_q$, le groupe $\mathbf{F}_q^\times/\mathbf{F}_q^{\times 2}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$ et l'indice est toujours $\geqslant 1$ dès que $n\geqslant 3$ (ex. 5.6.3°) ; le groupe $\mathrm{D}(\mathrm{SO}(\mathbf{F}_q^n,f))$ est alors d'indice 2 dans $\mathrm{SO}(\mathbf{F}_q^n,f)$.

---

20. En effet, en développant la relation ${}^t\mathrm{U}\begin{pmatrix}\mathrm{I}_s & 0\\ 0 & -\mathrm{I}_t\end{pmatrix}\mathrm{U}=\begin{pmatrix}\mathrm{I}_s & 0\\ 0 & -\mathrm{I}_t\end{pmatrix}$, on obtient entre autres ${}^t\mathrm{AA}=\mathrm{I}_s+{}^t\mathrm{CC}$, ce qui entraîne que la matrice ${}^t\mathrm{AA}$ est définie positive, donc que A est inversible (on obtient en fait même $|\det(\mathrm{A})|\geqslant 1$). Il en est de même pour D.

21. Comme dans la note 19, qui explique ces faits lorsque $s=1$, la deuxième égalité et la connexité de $\mathrm{SO}'_{s,t}(\mathbf{R})$ résultent, lorsque $s,t\geqslant 2$, du fait que $\mathrm{SO}'_{s,t}(\mathbf{R})$ opère transitivement sur la quadrique connexe Q, et que le stabilisateur de e_0 est isomorphe à $\mathrm{SO}'_{s-1,t}(\mathbf{R})$.

22. *Cf.* Dieudonné, J., *La géométrie des groupes classiques*, Springer Verlag, 1955, chap. II, § 6.5. Ce n'est plus vrai pour $\dim(\mathrm{V})=2$, puisque $\mathrm{SO}(\mathrm{V},f)$ est alors abélien (§ 8.1), mais on a encore $\mathrm{SO}'(\mathrm{V},f)=\mathrm{D}(\mathrm{O}(\mathrm{V},f))$.

4° Supposons $\mathbf{K} = \mathbf{Q}$. Si $\nu(f) \geqslant 1$ et $n \geqslant 3$, le th. 8.13 donne $\mathrm{SO}(\mathbf{Q}^n, f)/\mathrm{D}(\mathrm{O}(\mathbf{Q}^n, f)) \simeq \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ qui est un groupe infini (dans lequel tout élément est d'ordre 2).

Le cas où l'indice est nul est beaucoup moins bien connu. Lorsque $\mathbf{K} = \mathbf{Q}$, Meyer a montré qu'une forme quadratique f d'indice nul sur $\mathbf{Q}^n$, avec $n \geqslant 5$, est nécessairement définie négative ou définie positive vue comme forme quadratique sur $\mathbf{R}^n$. Dans ce cas, Kneser a montré que l'image de $\theta|_{\mathrm{SO}(\mathbf{Q}^n, f)}$ est $\mathbf{Q}^{\times +}/\mathbf{Q}^{\times 2}$ et que son noyau $\mathrm{SO}'(\mathbf{Q}^n, f)$ est encore $\mathrm{D}(\mathrm{SO}(\mathbf{Q}^n, f))$. On n'est donc pas très loin du cas $\nu \geqslant 1$: le groupe dérivé $\mathrm{D}(\mathrm{SO}(\mathbf{Q}^n, f))$ est encore d'indice infini dans $\mathrm{SO}(\mathbf{Q}^n, f)$.

La structure des groupes $\mathrm{O}(\mathbf{Q}^3, f)$ et $\mathrm{O}(\mathbf{Q}^4, f)$ est beaucoup moins bien connue (dans ce cas d'indice nul).

8.6. Centre. — On peut montrer que pour $\dim(\mathrm{V}) \geqslant 3$, le centre du groupe $\mathrm{D}(\mathrm{SO}(\mathrm{V}, f))$ consiste en les homothéties de ce groupe, c'est-à-dire Id_V et, éventuellement, $-\mathrm{Id}_\mathrm{V}$.

On a d'autre part la formule

$$\theta(-\mathrm{Id}_\mathrm{V}) = \mathrm{disc}(f).$$

En effet, dans une base $(e_1, \ldots, e_n)$ de V où $f(x) = \sum_{i=1}^n \alpha_i x_i^2$, on écrit $-\mathrm{Id}_\mathrm{V} = s_{e_1} \cdots s_{e_n}$, d'où $\theta(-\mathrm{Id}_\mathrm{V}) = f(e_1) \cdots f(e_n) = \prod_{i=1}^n \alpha_i = \mathrm{disc}(f)$.

On en déduit que pour $\dim(\mathrm{V}) \geqslant 3$ et $\nu \geqslant 1$, le centre de $\mathrm{D}(\mathrm{SO}(\mathrm{V}, f)) = \mathrm{SO}'(\mathrm{V}, f)$ est d'ordre 2 si $\mathrm{disc}(f) = 1$ et $\dim(\mathrm{V})$ pair, trivial sinon.

8.7. Simplicité. — Vu les résultats de la section précédente, le seul groupe qui a des chances d'être simple est le quotient $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathrm{V}, f)))$ du groupe dérivé $\mathrm{D}(\mathrm{SO}(\mathrm{V}, f))$ par son centre.

Nous nous contenterons de passer en revue quelques résultats connus, en renvoyant au livre de Dieudonné, J., *La géométrie des groupes classiques,* pour les preuves et des discussions plus approfondies.

Cas $\nu(f) = 0$ (forme anisotrope).— Il n'y a pas de résultat général, mais certains cas particuliers sont complètement décrits.

Lorsque $\mathbf{K} = \mathbf{R}$ (où $\mathrm{D}(\mathrm{SO}_n(\mathbf{R})) = \mathrm{SO}_n(\mathbf{R})$), on a

– le groupe $\mathrm{PSO}_4(\mathbf{R})$ n'est pas simple [23] (th. 11.3) ;
– le groupe $\mathrm{PSO}_n(\mathbf{R})$ est simple pour $n = 3$ ou $n \geqslant 5$.

Lorsque $\mathbf{K} = \mathbf{Q}$, on a :

– le groupe $\mathrm{O}(\mathbf{Q}^3, f)$ admet une suite décroissante de sous-groupes distingués dont l'intersection est $\{\mathrm{Id}\}$;
– pour $n \geqslant 5$, le groupe $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{Q}^n, f))) = \mathrm{PSO}'(\mathbf{Q}^n, f)$ est simple.

Cas $\nu(f) \geqslant 1$.— La situation est plus claire : *lorsque $n \geqslant 3$, le groupe* $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{K}^n, f))) = \mathrm{PSO}'(\mathbf{K}^n, f)$ *est simple,* avec deux exceptions [24].

---

23. Ce fait fondamental est à l'origine de propriétés spéciales importantes de la topologie et de la géométrie de dimension 4.

24. On a plus précisément :
– si $n = 3$, le groupe $\mathrm{D}(\mathrm{SO}(\mathbf{K}^3, f))$ est isomorphe à $\mathrm{PSL}_2(\mathbf{K})$, donc il est simple pour $\mathbf{K} \neq \mathbf{F}_3$ (th. 2.15) ;
– si $n = 4$ et $\mathrm{disc}(f) \neq 1$ dans $\mathbf{K}^\times/\mathbf{K}^{\times 2}$, le groupe $\mathrm{D}(\mathrm{SO}(\mathbf{K}^4, f)) = \mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{K}^4, f)))$ est isomorphe à $\mathrm{PGL}_2(\mathbf{K}[\sqrt{\mathrm{disc}(f)}])$ et il est donc simple (th. 2.15) ;

Ce cas inclut celui des corps finis $\mathbf{F}_q$ dès que $n \geqslant 3$. Rappelons qu'en dimension impaire, on a un seul groupe orthogonal, noté $\mathrm{O}_{2m+1}(\mathbf{F}_q)$ alors qu'en dimension paire, on en a deux, notés $\mathrm{O}^+_{2m}(\mathbf{F}_q)$ (discriminant $(-1)^m$, indice m) et $\mathrm{O}^-_{2m}(\mathbf{F}_q)$ (discriminant $\neq (-1)^m$, indice $m-1$) (ex. 5.6.3°).

Donnons les cardinaux. On a tout d'abord :

$$\begin{aligned} |\mathrm{SO}_{2m+1}(\mathbf{F}_q)| &= q^{m^2}(q^{2m}-1)(q^{2m-2}-1)\cdots(q^2-1), \\ |\mathrm{SO}^{\varepsilon}_{2m}(\mathbf{F}_q)| &= (q^m-\varepsilon)q^{m(m-1)}(q^{2m-2}-1)\cdots(q^2-1), \end{aligned} \tag{28}$$

où $\varepsilon = \pm 1$ ($\varepsilon = 1$ si $(-1)^m \mathrm{disc}(f)$ est un carré dans $\mathbf{F}_q$ et -1 sinon).

Par le th. 8.13, le groupe dérivé est d'indice 2 dans tous les cas. Dans le cas de la dimension impaire, son centre est trivial et

$$|\mathrm{P}(\mathrm{D}(\mathrm{SO}_{2m+1}(\mathbf{F}_q)))| = \frac{1}{2}q^{m^2}(q^{2m}-1)(q^{2m-2}-1)\cdots(q^2-1).$$

Dans le cas de la dimension paire, le centre est trivial si et seulement si $\mathrm{disc}(f) \neq 1$. Tous calculs faits, on arrive à

$$\begin{aligned} |\mathrm{P}(\mathrm{D}(\mathrm{SO}^+_{2m}(\mathbf{F}_q)))| &= \frac{q^m-1}{\mathrm{pgcd}(4,q^m-1)}q^{m(m-1)}(q^{2m-2}-1)\cdots(q^2-1), \\ |\mathrm{P}(\mathrm{D}(\mathrm{SO}^-_{2m}(\mathbf{F}_q)))| &= \frac{q^m+1}{\mathrm{pgcd}(4,q^m+1)}q^{m(m-1)}(q^{2m-2}-1)\cdots(q^2-1). \end{aligned}$$

On peut définir aussi ces groupes en caractéristique 2. On obtient ainsi trois autres séries infinies de groupes finis simples, à savoir [25]

$$\mathrm{P}(\mathrm{D}(\mathrm{SO}_{2m+1}(\mathbf{F}_q))),\ \mathrm{P}(\mathrm{D}(\mathrm{SO}^+_{2m}(\mathbf{F}_q)))\text{ et }\mathrm{P}(\mathrm{D}(\mathrm{SO}^-_{2m}(\mathbf{F}_q))).$$

9. Formes sesquilinéaires et hermitiennes

9.1. Formes sesquilinéaires. — Il y a une variante des formes bilinéaires quand le corps $\mathbf{K}$ (qu'on supposera toujours de caractéristique $\neq 2$) est équipé d'une involution de corps σ. L'exemple principal sera $\mathbf{K} = \mathbf{C}$ avec $\sigma(z) = \bar{z}$ et, pour simplifier les notations, on notera toujours l'involution σ de $\mathbf{K}$ sous la forme $\sigma(\lambda) = \bar{\lambda}$, quel que soit le corps.

La décomposition $\mathbf{C} = \mathbf{R} \oplus i\mathbf{R}$ s'étend de la manière suivante à tout corps muni d'une involution : comme $\mathrm{car}(\mathbf{K}) \neq 2$, on a une décomposition $\mathbf{K} = \mathbf{K}_0 \oplus \mathbf{K}_1$, où $\mathbf{K}_0$ et $\mathbf{K}_1$ sont les espaces propres de σ pour les valeurs propres 1 et -1, et $\mathbf{K}_0$ est un sous-corps de $\mathbf{K}$. Si $\sigma \neq \mathrm{Id}_{\mathbf{K}}$, on peut choisir $\mathrm{I} \in \mathbf{K}_1 - \{0\}$; on a alors

$$\mathbf{K} = \mathbf{K}_0 \oplus \mathrm{I}\mathbf{K}_0 \quad \text{avec } \mathrm{I}^2 \in \mathbf{K}_0^\times.$$

Exemple 9.1. — Si q est une puissance de nombre premier impair, le morphisme $\sigma : x \mapsto x^q$ est une involution du corps $\mathbf{K} = \mathbf{F}_{q^2}$. Le corps fixe $\mathbf{K}_0$ est le sous-corps $\mathbf{F}_q$ de $\mathbf{F}_{q^2}$.

– si $n = 4$ et $\mathrm{disc}(f) = 1$ dans $\mathbf{K}^\times/\mathbf{K}^{\times 2}$, le groupe $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{K}^4, f)))$ est isomorphe à $\mathrm{PSL}_2(\mathbf{K}) \times \mathrm{PSL}_2(\mathbf{K})$ et il est donc simple pour $\mathbf{K} \neq \mathbf{F}_3$ (th. 2.15) ;

– le groupe $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{K}^n, f)))$ est simple pour $n \geqslant 5$.

25. Pour des raisons que vous comprendrez plus tard, ces groupes sont aussi notés $\mathrm{B}_m(q)$, $\mathrm{D}_m(q)$ et ${}^2\mathrm{D}_m(q)$, respectivement.

On dit qu'un morphisme de groupes additifs u entre $\mathbf{K}$-espaces vectoriels est σ-linéaire si $u(\lambda x) = \bar{\lambda} u(x)$ pour tout vecteur x et tout $\lambda \in \mathbf{K}$. Une *forme σ-sesquilinéaire* est une application $b : \mathrm{V} \times \mathrm{V} \to \mathbf{K}$ telle que pour tout $y \in \mathrm{V}$, l'application $x \mapsto b(x, y)$ soit σ-linéaire et l'application $y \mapsto b(x, y)$ soit linéaire. Pour tous x et y dans V et tout $\lambda \in \mathbf{K}$, on a donc

$$b(x, \lambda y) = \lambda b(x, y) \quad \text{et} \quad b(\lambda x, y) = \bar{\lambda} b(x, y).$$

Dans une base (e_i) de V, la matrice M de b est définie par $\mathrm{M}_{ij} = b(e_i, e_j)$. Sur des vecteurs colonnes, on a alors $b(\mathrm{X}, \mathrm{Y}) = \mathrm{X}^* \mathrm{M} \mathrm{Y}$ et la matrice de b dans une autre base est $\mathrm{P}^* \mathrm{M} \mathrm{P}$, où P est la matrice de passage (pour toute matrice N, on note $\mathrm{N}^* := {}^t\bar{\mathrm{N}}$).

La forme sesquilinéaire b est *hermitienne* si en outre

$$b(y, x) = \overline{b(x, y)}$$

pour tous $x, y \in \mathrm{V}$. C'est le cas si et seulement si sa matrice M satisfait $\mathrm{M}^* = \mathrm{M}$ (on dit aussi que M est une matrice hermitienne)

Associée à une forme sesquilinéaire hermitienne est la *forme hermitienne*

$$h(x) = b(x, x).$$

On récupère, puisque $\mathrm{car}(\mathbf{K}) \neq 2$, la forme sesquilinéaire à partir de h par la formule

$$b(x, y) = \frac{1}{4}\big(h(x + y) - h(x - y) + \frac{1}{\mathrm{I}}(h(x + \mathrm{I}y) - h(x - \mathrm{I}y))\big).$$

On définit comme dans le cas symétrique le rang d'une forme sesquilinéaire hermitienne, la notion de forme sesquilinéaire hermitienne non dégénérée, d'isométrie, de vecteurs orthogonaux, de sous-espace totalement isotrope, de plan hyperbolique.

La réduction de Gauss (*cf.* § 4.2) décompose une forme hermitienne sous la forme

$$h(x) = \alpha_1 \bar{x}_1 x_1 + \cdots + \alpha_r \bar{x}_r x_r.$$

avec $\alpha_1, \ldots, \alpha_r \in \mathbf{K}_0^\times$.

Le théorème de Witt reste valable (avec des modifications dans la démonstration, en particulier dans celle du lemme 5.3) et on peut définir de la même façon l'indice d'une forme hermitienne.

10. Groupe unitaire

10.1. Définition. — On définit le *groupe unitaire* $\mathrm{U}(\mathrm{V}, h)$ d'une forme hermitienne h non dégénérée sur un espace vectoriel V comme le groupe des isométries de (V, h). Si M est la matrice (inversible) dans une base de V de la forme sesquilinéaire hermitienne b associée, ce groupe est isomorphe au groupe

$$\{\mathrm{U} \in \mathrm{GL}(\mathrm{V}) \mid \mathrm{U}^* \mathrm{M} \mathrm{U} = \mathrm{M}\}.$$

Le *groupe spécial unitaire* est défini comme d'habitude par

$$\mathrm{SU}(\mathrm{V}, h) := \mathrm{U}(\mathrm{V}, h) \cap \mathrm{SL}(\mathrm{V}).$$

Exemple 10.1. — 1° Si $\mathbf{K} = \mathbf{C}$ et σ est la conjugaison complexe, on peut trouver $a_i \in \mathbf{C}$ tel que $\bar{a}_i a_i = \pm\alpha_i$. Ainsi, pour toute forme hermitienne h non dégénérée sur $\mathbf{C}^n$, il existe une base dans laquelle elle s'écrit

$$h(x) = \bar{x}_1 x_1 + \cdots + \bar{x}_s x_s - \bar{x}_{s+1} x_{s+1} - \cdots - \bar{x}_n x_n.$$

L'indice est $\inf(s, n-s)$. Le groupe unitaire associé est noté $\mathrm{U}_{s,n-s}(\mathbf{C})$. Il est isomorphe à

$$\left\{ \mathrm{U} \in \mathrm{GL}_n(\mathbf{C}) \;\middle|\; \mathrm{U}^* \begin{pmatrix} \mathrm{I}_s & 0 \\ 0 & -\mathrm{I}_{n-s} \end{pmatrix} \mathrm{U} = \begin{pmatrix} \mathrm{I}_s & 0 \\ 0 & -\mathrm{I}_{n-s} \end{pmatrix} \right\}.$$

On note $\mathrm{U}_n(\mathbf{C})$ lorsque $s = n$. Les groupes $\mathrm{U}_{s,n-s}(\mathbf{C})$ (resp. $\mathrm{SU}_{s,n-s}(\mathbf{C})$) sont des *variétés différentiables* de dimension n^2 (resp. $n^2 - 1$).

2° Si $\mathbf{K} = \mathbf{F}_{q^2}$ (avec q puissance de nombre premier impair) et $\sigma(\lambda) = \lambda^q$, le morphisme

$$\begin{array}{ccc} \mathbf{F}_{q^2}^\times & \longrightarrow & \mathbf{F}_q^\times \\ \lambda & \longmapsto & \bar{\lambda}\lambda = \lambda^{q+1} \end{array}$$

est surjectif. En effet, un générateur du groupe cyclique $\mathbf{F}_{q^2}^\times$ est d'ordre $q^2 - 1 = (q-1)(q+1)$; il est donc envoyé sur un élément d'ordre $q-1$, c'est-à-dire un générateur de $\mathbf{F}_q^\times$. Il en résulte que tout élément α_i de $\mathbf{F}_q^\times$ peut s'écrire $\bar{a}_i a_i$, et donc, pour toute forme hermitienne h non dégénérée sur $\mathbf{F}_{q^2}^n$, il existe une base dans laquelle elle s'écrit

$$h(x) = \bar{x}_1 x_1 + \cdots + \bar{x}_n x_n = x_1^{q+1} + \cdots + x_n^{q+1}.$$

Toutes les formes non dégénérées sur $\mathbf{F}_{q^2}^n$ sont donc équivalentes et iI existe aussi une base dans laquelle la forme s'écrit $h(x) = \bar{x}_1 x_1 - \bar{x}_2 x_2 + \cdots + (-1)^{n+1} \bar{x}_n x_n$. L'indice est donc $\lfloor n/2 \rfloor$. En particulier, tout plan est hyperbolique.

Le groupe unitaire est noté $\mathrm{U}_n(\mathbf{F}_{q^2})$. Il est isomorphe au groupe

$$\{\mathrm{U} \in \mathrm{GL}_n(\mathbf{F}_{q^2}) \mid {}^t\mathrm{U}^{(q)}\mathrm{U} = \mathrm{I}_n\},$$

où $\mathrm{U}^{(q)}$ est la matrice obtenue à partir de U en élevant tous ses coefficients à la puissance q. On a

$$|\mathrm{U}_n(\mathbf{F}_{q^2})| = (q^n - (-1)^n) q^{n-1} (q^{n-1} - (-1)^{n-1}) q^{n-2} \cdots (q^2 - 1) q(q+1).$$

Exercice 10.2. — Soit $\mathrm{M} \in \mathrm{GL}_n(\mathbf{F}_{q^2})$ une matrice telle que ${}^t\mathrm{M} = \mathrm{M}^{(q)}$. Montrer qu'il existe une matrice $\mathrm{P} \in \mathrm{GL}_n(\mathbf{F}_{q^2})$ tel que $\mathrm{M} = {}^t\mathrm{P}^{(q)}\mathrm{P}$.

10.2. La dimension 2. — Comme dans le cas orthogonal, le cas de la dimension 2 peut être décrit par calcul direct. Nous envisageons les deux types de formes qui peuvent intervenir dans les cas $\mathbf{K} = \mathbf{C}$ ou $\mathbf{F}_{q^2}$.

Cas de la forme hermitienne $\bar{x}_1 x_1 + \bar{x}_2 x_2$.

Proposition 10.3. — *Supposons* $\dim(\mathrm{V}) = 2$ *et* $h(x_1, x_2) = \bar{x}_1 x_1 + \bar{x}_2 x_2$. *Alors*

$$\mathrm{SU}(\mathrm{V}, h) \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbf{K},\ \bar{\alpha}\alpha + \bar{\beta}\beta = 1 \right\}.$$

En particulier, $\mathrm{SU}_2(\mathbf{C})$ est un groupe non commutatif. Il est homéomorphe à la sphère unité $\mathbf{S}^3$ dans l'espace euclidien $\mathbf{R}^4$.

Démonstration. — La matrice $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est dans $SU(V,h)$ si et seulement si $\det(U) = 1$ et $U^*U = I_2$. Ces conditions entraînent $\begin{pmatrix} \bar\alpha & \bar\gamma \\ \bar\beta & \bar\delta \end{pmatrix} = U^* = U^{-1} = {}^tU^c = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$, c'est-à-dire $\gamma = -\bar\beta$ et $\delta = \bar\alpha$, donc $\bar\alpha\alpha + \bar\beta\beta = 1$. □

Cas d'un plan hyperbolique. C'est le cas où $h(x_1,x_2) = \bar x_1 x_1 - \bar x_2 x_2 = \frac{1}{2}\big((\overline{x_1+x_2})(x_1-x_2) + (\overline{x_1-x_2})(x_1+x_2)\big)$. On peut donc se placer dans une base où la forme hermitienne est donnée par $h(x_1,x_2) = \bar x_1 x_2 + \bar x_2 x_1$.

Proposition 10.4. — *Supposons* $\dim(V) = 2$ *et* V *hyperbolique pour la forme hermitienne* h. *Alors* $SU(V,h) \simeq SL_2(\mathbf{K}_0)$.

Exemple 10.5. — On a donc $SU_{1,1}(\mathbf{C}) \simeq SL_2(\mathbf{R})$ et $SU_2(\mathbf{F}_{q^2}) \simeq SL_2(\mathbf{F}_q)$.

Démonstration. — Dans une base hyperbolique, la matrice de la forme hermitienne h est $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Alors, $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est dans $SU(V,h)$ si $\det(U) = 1$ et $U^*MU = M$, ce qui entraîne $\begin{pmatrix} \bar\alpha & \bar\gamma \\ \bar\beta & \bar\delta \end{pmatrix} = U^* = MU^{-1}M = M{}^tU^cM = \begin{pmatrix} \alpha & -\gamma \\ -\beta & \delta \end{pmatrix}$, c'est-à-dire $\bar\alpha = \alpha$, $\bar\delta = \delta$, $\bar\beta = -\beta$ et $\bar\gamma = -\gamma$, ou encore $\alpha, \delta, I\beta, I\gamma \in \mathbf{K}_0$ et $\alpha\delta - \beta\gamma = 1$, soit $U' := \begin{pmatrix} \alpha & I\beta \\ I^{-1}\gamma & \delta \end{pmatrix} \in SL_2(\mathbf{K}_0)$. On vérifie que l'application $U \mapsto U'$ est bien un morphisme de groupes [26]. □

10.3. Produit scalaire hermitien. — Dans cette section uniquement, on suppose $\mathbf{K} = \mathbf{C}$ et on considère une forme hermitienne h définie positive sur un $\mathbf{C}$-espace vectoriel V de dimension n, c'est-à-dire satisfaisant $h(x) \geqslant 0$ pour tout $x \in V$, avec égalité si et seulement si $x = 0$. Une telle forme est en particulier non dégénérée ; on l'appelle un *produit scalaire hermitien*. On a vu qu'il existe alors une base orthonormale, c'est-à-dire une base dans laquelle la forme h s'écrit

$$h(x) = |x_1|^2 + \cdots + |x_n|^2.$$

Dans ce cas, les éléments du groupe $U(V,h)$ jouissent d'une réduction particulièrement simple, similaire à celle des endomorphismes orthogonaux pour un produit scalaire euclidien défini positif.

---

26. On peut décrire plus intrinsèquement le morphisme $SL_2(\mathbf{K}_0) \to SU(V,h)$ comme suit. On considère $\mathbf{K}$ comme un $\mathbf{K}_0$-espace vectoriel de dimension 2. L'espace vectoriel $V := \mathrm{End}_{\mathbf{K}_0}\mathbf{K}$ des endomorphismes $\mathbf{K}_0$-linéaires de $\mathbf{K}$ est naturellement un $\mathbf{K}$-espace vectoriel de dimension 2, puisque (Id, σ) en est une base. Si $\alpha = a + Ia'$ et $\beta = b + Ib'$ sont dans $\mathbf{K}$, la matrice de l'endomorphisme $\alpha\mathrm{Id} + \beta\sigma$ de $\mathbf{K}$ dans la base $(1, I)$ est $\begin{pmatrix} a+b & (a'-b')I^2 \\ a'+b' & a-b \end{pmatrix}$, dont le déterminant est $\bar\alpha\alpha - \bar\beta\beta$. C'est donc une forme hermitienne sur V, hyperbolique puisque le vecteur $(1,1)$ est isotrope.

On dispose d'autre part d'une application $\mathbf{K}$-linéaire $\phi : V = \mathrm{End}_{\mathbf{K}_0}\mathbf{K} \to \mathrm{End}_{\mathbf{K}}(V)$ qui envoie $u \in V$ sur l'endomorphisme ϕ_u de V donné par $v \mapsto u \circ v$. Comme $\det(\phi_u(v)) = \det(u)\det(v)$, on voit que ϕ_u est unitaire pour la forme hermitienne dét si et seulement si $\det(u) = 1$. L'application ϕ induit donc un morphisme de groupes $SL(\mathbf{K}) \to U(V, \det)$. On vérifie ensuite que ce morphisme est à valeurs dans $SU(V, \det)$ (c'est-à-dire que $\det(\phi_u) = 1$ si $\det(u) = 1$) et qu'il est surjectif.

Un endomorphisme u de V admet toujours un adjoint u^* défini par

$$b(x, u(y)) = b(u^*(x), y)$$

pour tous $x, y \in \mathrm{V}$. En particulier, $u \in \mathrm{U}(\mathrm{V}, h)$ si et seulement si $u^* = u^{-1}$.

Dans une base orthonormale, si u a pour matrice U, alors u^* a pour matrice U^*.

Plus généralement, on dit qu'un endomorphisme u de V est *normal* si $u^* u = u u^*$. Cette notion inclut les endomorphismes unitaires ($u^* = u^{-1}$), autoadoints ($u^* = u$) et antiautoadjoints ($u^* = -u$).

Proposition 10.6. — *Tout endomorphisme normal pour un produit scalaire hermitien se diagonalise dans une base orthonormale.*

Les valeurs propres sont de module 1 pour les endomorphismes unitaires, réelles pour les endomorphismes autoadjoints et imaginaires pures pour les endomorphismes antiautoadjoints.

Démonstration de la proposition. — Soit u un endomorphisme normal de V. Soit λ une valeur propre (complexe) de u et soit V_λ l'espace propre associé. Si $x \in \mathrm{V}_\lambda$, on a

$$u(u^*(x)) = u^*(u(x)) = u^*(\lambda x) = \lambda u^*(x),$$

donc $u^*(x) \in \mathrm{V}_\lambda$. Ainsi $u^*(\mathrm{V}_\lambda) \subseteq \mathrm{V}_\lambda$.

Si $y \in \mathrm{V}_\lambda^\perp$ et $x \in \mathrm{V}_\lambda$, on obtient $b(x, u(y)) = b(u^*(x), y) = 0$, donc $u(\mathrm{V}_\lambda^\perp) \subseteq \mathrm{V}_\lambda^\perp$. Une récurrence sur la dimension de V montre alors que V est somme directe orthogonale des espaces propres de u. □

Si l'on dispose d'une seconde forme hermitienne h', on peut lui associer, puisque h est non dégénérée, un endomorphisme u de V qui vérifie

$$\forall x, y \in \mathrm{V} \qquad b'(x, y) = b(x, u(y)).$$

On a aussi

$$b(u(x), y) = \overline{b(y, u(x)} = \overline{b'(y, x)} = b'(x, y) = b(x, u(y)),$$

de sorte que $u^* = u$. D'après la proposition, u se diagonalise dans une base h-orthonormale, ce qui signifie que dans cette base, la forme b' a une matrice diagonale

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}, \quad \text{avec } \lambda_1, \ldots, \lambda_n \in \mathbf{R}.$$

La forme h' est définie positive si et seulement si les λ_i sont tous strictement positifs.

10.4. Propriétés des groupes unitaires. — On énonce sans démonstration quelques propriétés des groupes unitaires pour une forme hermitienne h sur un $\mathbf{K}$-espace vectoriel de dimension $n \geqslant 2$.

Centre : Le centre de $\mathrm{U}(\mathbf{K}^n, h)$ est constitué des homothéties de rapport λ tel que $\bar{\lambda}\lambda = 1$.

Le centre de $\mathrm{SU}(\mathbf{K}^n, h)$ est constitué des homothéties de rapport satisfaisant en outre $\lambda^n = 1$. Pour $\mathbf{K} = \mathbf{C}$, c'est donc le groupe des racines n-ièmes de l'unité. Pour $\mathbf{K} = \mathbf{F}_{q^2}$, c'est le groupe des racines $\mathrm{pgcd}(q+1, n)$-ièmes de l'unité.

On notera

$$\mathrm{PSU}(\mathbf{K}^n, h) := \mathrm{SU}(\mathbf{K}^n, h)/\mathrm{Z}(\mathrm{SU}(\mathbf{K}^n, h)).$$

Simplicité : Si la forme hermitienne h est d'indice $\geqslant 1$, le groupe $\mathrm{PSU}(\mathbf{K}^n, h)$ est simple (c'est donc le cas pour les groupes $\mathrm{PSU}_{s,t}(\mathbf{C})$ avec $s, t > 0$, et $\mathrm{PSU}_n(\mathbf{F}_{q^2})$ pour $n \geqslant 2$), à l'exception du groupe $\mathrm{PSU}_2(\mathbf{F}_9) \simeq \mathrm{PSL}_2(\mathbf{F}_3)$ (prop. 10.4).

Si l'indice est nul, donc la forme anisotrope, il n'y a pas de résultat général. Néanmoins $\mathrm{PSU}_n(\mathbf{C})$ est simple dès que $n \geqslant 2$: en fait, comme on le verra dans le § 11, $\mathrm{PSU}_2(\mathbf{C}) \simeq \mathrm{SO}_3(\mathbf{R})$, qui est simple, et l'énoncé pour $n > 2$ s'en déduit.

On peut définir les groupes unitaires aussi en caractéristique 2. On obtient ainsi une autre série de groupes finis simples, à savoir $\mathrm{PSU}_n(\mathbf{F}_{q^2})$ pour q puissance de nombre premier et $n \geqslant 3$ [(27)].

11. Quaternions

Le corps $\mathbf{H}$ des *quaternions* est un corps non commutatif, contenant comme sous-corps $\mathbf{R}$, et de dimension 4 comme espace vectoriel sur $\mathbf{R}$. On peut le décrire comme une algèbre de matrices 2×2 complexes :

$$\mathbf{H} := \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbf{C} \right\}. \tag{29}$$

L'addition et la multiplication dans $\mathbf{H}$ sont celles des matrices. Puisque le déterminant est $|\alpha|^2 + |\beta|^2$, seule la matrice nulle n'est pas inversible et on obtient un corps.

On distingue les éléments suivants de $\mathbf{H}$:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathrm{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathrm{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathrm{K} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Les multiples réels de 1 fournissent le sous-corps $\mathbf{R}$ de $\mathbf{H}$. La famille $(1, \mathrm{I}, \mathrm{J}, \mathrm{K})$ est une base de $\mathbf{H}$ vu comme espace vectoriel sur $\mathbf{R}$. On observe que

$$\mathrm{I}^2 = \mathrm{J}^2 = \mathrm{K}^2 = -1, \quad \mathrm{IJK} = -1,$$

relations desquelles on déduit aisément les autres multiplications des éléments de la base :

$$\mathrm{IJ} = -\mathrm{JI} = \mathrm{K}, \quad \mathrm{JK} = -\mathrm{KJ} = \mathrm{I}, \quad \mathrm{KI} = -\mathrm{IK} = \mathrm{J}.$$

On définit le *conjugué* d'un quaternion $q = x_0 + x_1\mathrm{I} + x_2\mathrm{J} + x_3\mathrm{K}$, où $x_0, \ldots, x_3 \in \mathbf{R}$, en posant

$$\bar{q} = x_0 - x_1\mathrm{I} - x_2\mathrm{J} - x_3\mathrm{K}.$$

La conjugaison a les propriétés suivantes :

1° $\overline{q_1 q_2} = \bar{q}_2 \bar{q}_1$;

2° $\mathrm{N}(q) := q\bar{q} = \bar{q}q = x_0^2 + x_1^2 + x_2^2 + x_3^2 \in \mathbf{R}$, en particulier, $\mathrm{N}(q) = 0$ si et seulement si $q = 0$, et si $q \neq 0$, on a $q^{-1} = \frac{\bar{q}}{\mathrm{N}(q)}$.

Un quaternion est

– réel si $\bar{q} = q$;

27. Ces groupes sont aussi notés ${}^2\mathrm{A}_{n-1}(q^2)$.

– *imaginaire pur* si $\bar{q} = -q$.

L'ensemble des quaternions imaginaires purs est $\mathrm{Im}(\mathbf{H}) := \{x_1\mathrm{I} + x_2\mathrm{J} + x_3\mathrm{K}\}$ et on a

$$\mathbf{H} = \mathbf{R} \oplus \mathrm{Im}(\mathbf{H}).$$

L'ensemble $\{x_0 + x_1\mathrm{I} \mid x_0, x_1 \in \mathbf{R}\}$ est un sous-corps de $\mathbf{H}$ isomorphe à $\mathbf{C}$ (ce n'est pas le seul car les rôles de I, J et K sont interchangeables dans $\mathbf{H}$ [28]). La famille $(1, \mathrm{J})$ est une base de $\mathbf{H}$ vu comme espace vectoriel sur $\mathbf{C}$. Plus précisément, on a

$$\begin{aligned} q &= x_0 + x_1\mathrm{I} + x_2\mathrm{J} + x_3\mathrm{K}, \qquad \text{où } x_0, \dots, x_3 \in \mathbf{R}, \\ &= (x_0 + x_1\mathrm{I})1 + (x_2 + x_3\mathrm{I})\mathrm{J}. \end{aligned}$$

Dans cette écriture, on fera attention que $\beta = x_2 + x_3\mathrm{I}$ et J ne commutent pas en général (on a $\mathrm{J}\beta = \bar{\beta}\mathrm{J}$).

Le centre $\mathrm{Z}(\mathbf{H})$ de $\mathbf{H}$ est $\mathbf{R}$: en effet, si $q \in \mathrm{Z}(\mathbf{H})$, écrivons comme ci-dessus $q = \alpha + \beta\mathrm{J}$, avec $\alpha, \beta \in \mathbf{C}$. De $q\mathrm{I} = \mathrm{I}q$, on déduit $\beta = 0$, et de $\alpha\mathrm{J} = \mathrm{J}\alpha = \bar{\alpha}\mathrm{J}$, on déduit $\alpha \in \mathbf{R}$.

Lemme 11.1. — *La norme* $\mathrm{N} : \mathbf{H}^\times \to \mathbf{R}^\times$ *est un morphisme de groupes multiplicatifs. Son noyau* $\ker(\mathrm{N}) = \{q \in \mathbf{H} \mid \mathrm{N}(q) = 1\}$ *est un groupe isomorphe à* $\mathrm{SU}_2(\mathbf{C})$.

Démonstration. — On a

$$\mathrm{N}(q_1 q_2) = \bar{q}_2 \bar{q}_1 q_1 q_2 = \bar{q}_2 \mathrm{N}(q_1) q_2 = \mathrm{N}(q_1)\mathrm{N}(q_2),$$

la dernière égalité étant vraie car $\mathrm{N}(q_1) \in \mathbf{R} = \mathrm{Z}(\mathbf{H})$.

La description matricielle (29) donne l'interprétation du noyau comme le groupe $\mathrm{SU}_2(\mathbf{C})$ (prop. 10.3). □

Bien sûr, N s'identifie à la norme euclidienne usuelle dans $\mathbf{H} = \mathbf{R}^4$, donc le groupe $\mathrm{SU}_2(\mathbf{C})$ est homéomorphe à la sphère de $\mathbf{R}^4$.

Soit q un quaternion tel que $\mathrm{N}(q) = 1$. Considérons la conjugaison (au sens du groupe multiplicatif (non abélien) $(\mathbf{H}^\times, \times)$)

$$\begin{aligned} \phi_q : \mathbf{H} &\longrightarrow \mathbf{H} \\ x &\longmapsto qxq^{-1} \end{aligned}$$

Puisque $q^{-1} = \bar{q}$, on a

$$\overline{\phi_q(x)} = q\bar{x}q^{-1},$$

donc ϕ_q agit par l'identité sur $\mathbf{R}$ et préserve la décomposition $\mathbf{H} = \mathbf{R} \oplus \mathrm{Im}(\mathbf{H})$. En outre,

$$\mathrm{N}(\phi_q(x)) = qxq^{-1}q\bar{x}q^{-1} = \mathrm{N}(x),$$

donc ϕ_q agit par isométries sur $\mathbf{R}^4$. En restreignant ϕ_q à $\mathrm{Im}(\mathbf{H})$, on obtient ainsi un morphisme de groupes

$$\begin{aligned} \phi : \mathrm{SU}_2(\mathbf{C}) &\longrightarrow \mathrm{O}_3(\mathbf{R}) \\ q &\longmapsto \phi_q|_{\mathrm{Im}(\mathbf{H})}. \end{aligned}$$

28. En faisant agir les automorphismes ϕ_q définis plus bas, on voit qu'on peut même changer le triplet $(\mathrm{I}, \mathrm{J}, \mathrm{K})$ en son image par n'importe quelle rotation de $\mathbf{R}^3$, donc en particulier I en $q_1\mathrm{I} + q_2\mathrm{J} + q_3\mathrm{K}$ pour $q_1, q_2, q_3 \in \mathbf{R}$ tels que $q_1^2 + q_2^2 + q_3^2 = 1$, ce qui donne une famille de sous-corps de $\mathbf{H}$ isomorphes à $\mathbf{C}$ paramétrée par la sphère $\mathbf{S}^2$.

Comme le groupe $\mathrm{SU}_2(\mathbf{C})$, homéomorphe à la sphère de $\mathbf{R}^4$, est connexe, l'image de ϕ est connexe donc incluse dans $\mathrm{SO}_3(\mathbf{R})$.

Théorème 11.2. — *Le morphisme ϕ ainsi défini est surjectif, de noyau $\{\pm 1\}$. Par conséquent,*

$$\mathrm{SO}_3(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C})/\{\pm 1\} = \mathrm{PSU}_2(\mathbf{C}).$$

Démonstration. — Le noyau de ϕ est constitué des quaternions q de norme 1 tels que $qxq^{-1} = x$ pour tout $x \in \mathrm{Im}(\mathbf{H})$, soit $qx = xq$ pour tout $x \in \mathrm{Im}(\mathbf{H})$. Comme c'est toujours vrai pour $x \in \mathbf{R}$, cela implique $qx = xq$ pour tout $x \in \mathbf{H}$, donc $q \in \mathrm{Z}(\mathbf{H}) = \mathbf{R}$ et $q = \pm 1$.

Montrons que ϕ est surjectif. Soit $q \in \mathrm{Im}(\mathbf{H})$ tel que $q\bar{q} = 1$. Alors $q^2 = -q\bar{q} = -1$ et

$$\begin{aligned} \phi_q(q) &= q, \\ \phi_q^2(x) &= \phi_{q^2}(x) = x \quad \text{pour tout } x \in \mathrm{Im}(\mathbf{H}), \end{aligned}$$

donc $\phi_q|_{\mathrm{Im}(\mathbf{H})}$, qui est une rotation autre que l'identité, est obligatoirement le renversement d'axe $\mathbf{R}q \subseteq \mathrm{Im}(\mathbf{H})$. L'image de ϕ contient ainsi les renversements et ϕ est surjective par le th. 8.9. □

L'isomorphisme entre $\mathrm{PSU}_2(\mathbf{C})$ et $\mathrm{SO}_3(\mathbf{R})$ a été montré en trouvant, grâce aux quaternions, une action de $\mathrm{SU}_2(\mathbf{C})$, identifié au groupe des quaternions de norme 1, sur $\mathbf{R}^3$. On peut aussi regarder l'action de $\mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C})$ sur $\mathbf{R}^4 = \mathbf{H}$, définie en associant à un couple de quaternions (q_1, q_2), chacun de norme 1, l'endomorphisme

$$\psi_{q_1,q_2}(x) = q_1 x \bar{q}_2 = q_1 x q_2^{-1}$$

de $\mathbf{H}$.

Théorème 11.3. — *1° On définit ainsi un morphisme*

$$\psi : \mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C}) \to \mathrm{SO}_4(\mathbf{R})$$

qui est surjectif, de noyau $\{\pm(1,1)\}$.

2° On a un isomorphisme $\mathrm{PSO}_4(\mathbf{R}) \simeq \mathrm{SO}_3(\mathbf{R}) \times \mathrm{SO}_3(\mathbf{R})$.

En particulier, le groupe $\mathrm{PSO}_4(\mathbf{R})$ n'est pas simple.

Démonstration. — 1° À nouveau, on a $\mathrm{N}(\psi_{q_1,q_2}(x)) = q_1 x q_2^{-1} q_2 \bar{x} q_1^{-1} = \mathrm{N}(x)$ donc l'image de ψ est bien contenue dans $\mathrm{O}_4(\mathbf{R})$ et même, par connexité de l'image, dans $\mathrm{SO}_4(\mathbf{R})$.

On vérifie facilement l'égalité

$$\psi_{q_1,q_2} \circ \psi_{q_1',q_2'} = \psi_{q_1 q_1', q_2 q_2'}$$

qui montre que ψ est un morphisme de groupes.

Le noyau de ψ est constitué des (q_1, q_2) tels que $q_1 x q_2^{-1} = x$ pour tout $x \in \mathbf{H}$ donc $q_1 x = xq_2$. Faisant $x = 1$ on déduit $q_1 = q_2$, forcément élément de $\mathrm{Z}(\mathbf{H})$, donc $q_1 = q_2 = \pm 1$.

Pour montrer que ψ est surjective, on prend $u \in \mathrm{SO}_4(\mathbf{R})$. Le quaternion $q := u(1)$ vérifie $\mathrm{N}(q) = 1$. On a $\psi_{\bar{q},1} \circ u(1) = \bar{q}q = 1$, donc l'isométrie $\psi_{\bar{q},1} \circ u$ laisse $\mathbf{R}$, donc aussi $\mathbf{R}^\perp = \mathrm{Im}(\mathbf{H})$, stable. Par le théorème précédent, il existe q' de norme 1 tel que $\psi_{\bar{q},1} \circ u = \phi_{q'} = \psi_{q',q'}$, c'est-à-dire $u = \psi_{\bar{q},1}^{-1} \circ \psi_{q',q'} = \psi_{qq',q'}$. Ceci montre que ψ est surjectif.

2° En composant ψ par la surjection sur $\mathrm{PSO}_4(\mathbf{R}) = \mathrm{SO}_4(\mathbf{R})/\{\pm \mathrm{I}_4\}$, on obtient un morphisme surjectif

$$\tilde{\psi} : \mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C}) \longrightarrow \mathrm{PSO}_4(\mathbf{R}).$$

Son noyau est constitué des (q_1, q_2) tels que $q_1 x q_2^{-1} = \varepsilon x$ pour tout $x \in \mathbf{H}$, où $\varepsilon = \pm 1$, c'est-à-dire $(q_1, \varepsilon q_2) \in \ker(\psi) = \{\pm(1,1)\}$. Le noyau de $\tilde{\psi}$ est donc constitué des quatre éléments $(\pm 1, \pm 1)$, donc $\mathrm{PSO}_4(\mathbf{R}) \simeq \mathrm{PSU}_2(\mathbf{C}) \times \mathrm{PSU}_2(\mathbf{C}) \simeq \mathrm{SO}_3(\mathbf{R}) \times \mathrm{SO}_3(\mathbf{R})$. □

Remarque 11.4. — Pour tout n, on peut construire (*cf.* § III.6.4) un groupe $\mathrm{Spin}_n(\mathbf{R})$ connexe, muni d'un morphisme de groupes surjectif $\mathrm{Spin}_n(\mathbf{R}) \to \mathrm{SO}_n(\mathbf{R})$ dont le noyau a deux éléments [29]. Il est unique à isomorphisme (de groupes) près.

On a vu $\mathrm{SO}_2(\mathbf{R}) \simeq \mathrm{U}_1(\mathbf{C})$ (ex. 8.2.1°). Le groupe $\mathrm{Spin}_2(\mathbf{R})$ est le groupe $\mathrm{U}_1(\mathbf{C})$ des nombres complexes de module 1, mais le morphisme $\mathrm{Spin}_2(\mathbf{R}) \to \mathrm{SO}_2(\mathbf{R})$ est l'élévation au carré.

Le th. 11.2 entraîne $\mathrm{Spin}_3(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C})$, et le th. 11.3 entraîne $\mathrm{Spin}_4(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C})$.

On peut montrer $\mathrm{Spin}_6(\mathbf{R}) \simeq \mathrm{SU}_4(\mathbf{C})$, c'est-à-dire qu'on a un morphisme surjectif $\mathrm{SU}_4(\mathbf{C}) \to \mathrm{SO}_6(\mathbf{R})$ dont le noyau est d'ordre 2 (exerc. III.4.11).

Cette construction peut aussi être effectuée dans le cas d'une forme quadratique (non dégénérée) quelconque sur $\mathbf{R}^n$ (rem. III.6.11). On obtient alors un groupe $\mathrm{Spin}'_{s,t}(\mathbf{R})$ qui est un revêtement (connexe) de degré 2 du groupe connexe $\mathrm{SO}'_{s,t}(\mathbf{R})$ (d'indice 2 dans $\mathrm{SO}_{s,t}(\mathbf{R})$) défini dans l'ex. 8.12.3° (*cf.* exerc. III.4.10).

Exercice 11.5. — Soit $\mathbf{K}$ un corps de caractéristique différente de 2 et soit V l'espace vectoriel (de dimension 4) des matrices 2×2 à coefficients dans $\mathbf{K}$.
a) Montrer que $f : \mathrm{M} \mapsto \mathrm{tr}(\mathrm{M}^2)$ est une forme quadratique sur V.
b) Montrer que $\mathrm{SL}_2(\mathbf{K})$ agit par isométries sur V par $\mathrm{P} \cdot \mathrm{M} := \mathrm{PMP}^{-1}$ et que ces isométries laissent toutes stable l'espace vectoriel $\mathrm{W} := \mathrm{I}_2^{\perp}$ (de dimension 3).
c) Montrer que la restriction de f à W est de type $\langle 1, -1, 2 \rangle$.
d) On en déduit un morphisme $\mathrm{SL}_2(\mathbf{K}) \to \mathrm{O}(\mathrm{W}, f|_{\mathrm{W}})$. Montrer qu'il est surjectif et déterminer son noyau.
e) En déduire que le groupe $\mathrm{Spin}'_{2,1}(\mathbf{R})$ est isomorphe à $\mathrm{SL}_2(\mathbf{R})$.

Exercice 11.6. — Le but de cet exercice est de montrer que le groupe $\mathrm{SO}'_{1,3}(\mathbf{R})$ défini dans l'ex. 8.12.3° est isomorphe à $\mathrm{PSL}_2(\mathbf{C})$. En particulier, $\mathrm{Spin}'_{1,3}(\mathbf{R}) \simeq \mathrm{SL}_2(\mathbf{C})$.

Soit V l'espace vectoriel réel des matrices hermitiennes 2×2.
a) Quelle est la dimension de V ?
b) Montrer que $\mathrm{GL}_2(\mathbf{C})$ agit linéairement sur V par la relation $\mathrm{P} \cdot \mathrm{M} = \mathrm{PMP}^*$.
c) Montrer que $\mathrm{SL}_2(\mathbf{C})$ agit par isométries sur V pour la forme quadratique de Lorentz de signature (1,3). On en déduit un morphisme $\phi : \mathrm{SL}_2(\mathbf{C}) \to \mathrm{O}_{1,3}(\mathbf{R})$.
d) Déterminer le noyau de ϕ.
e) Montrer que l'image de ϕ est exactement $\mathrm{SO}'_{1,3}(\mathbf{R})$ et conclure.

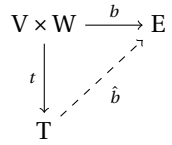
29. On dit que c'est un revêtement de degré 2 de $\mathrm{SO}_n(\mathbf{R})$; c'est en fait, pour $n \geqslant 3$, le revêtement universel de l'espace topologique $\mathrm{SO}_n(\mathbf{R})$.

CHAPITRE III

ALGÈBRE TENSORIELLE

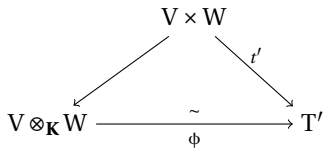
1. Produit tensoriel

Soit **K** un corps et soient V et W des **K**-espaces vectoriels. Un *produit tensoriel* de V et W est la donnée d'un **K**-espace vectoriel T et d'une application bilinéaire $t : V \times W \to T$ satisfaisant la propriété universelle suivante : si $b : V \times W \to E$ est une application bilinéaire, il existe une *unique* application *linéaire* $\hat{b} : T \to E$ telle que $b = \hat{b} \circ t$. Cela se traduit par le fait que le diagramme



est commutatif. Une telle paire (T, t) est nécessairement unique, à unique isomorphisme près, au sens suivant.

Théorème 1.1* (Existence et unicité).** — *Étant donnés des* **K-espaces vectoriels* V *et* W*, il existe un produit tensoriel* $(V \otimes_{\mathbf{K}} W, t)$*, unique au sens suivant : tout produit tensoriel* (T', t') *de* V *et* W *lui est isomorphe, c'est-à-dire qu'il existe un isomorphisme* $\phi : V \otimes_{\mathbf{K}} W \to T'$ *unique tel que le diagramme*



soit commutatif. On parle ainsi du *produit tensoriel de* V *et* W*. L'application bilinéaire* $t : V \times W \to V \otimes_{\mathbf{K}} W$ *est notée* $(v, w) \mapsto v \otimes w$*. Un élément de* $V \otimes_{\mathbf{K}} W$ *du type* $v \otimes w$ *est appelé* tenseur décomposable *; les tenseurs décomposables engendrent* $V \otimes_{\mathbf{K}} W$.

On notera la plupart du temps $V \otimes W$ au lieu de $V \otimes_{\mathbf{K}} W$.

Démonstration. — Commençons par l'unicité. On applique la propriété universelle pour $V \otimes_{\mathbf{K}} W$ à $t' : V \times W \to T'$, pour déduire l'existence d'une application linéaire $\phi : V \otimes_{\mathbf{K}} W \to T'$ unique telle que $t' = \phi \circ t$. La propriété universelle pour T' fabrique aussi $\psi : T' \to T$ tel que $t = \psi \circ t'$. Appliquant l'unicité dans la propriété universelle à l'application bilinéaire $t : V \times W \to V \otimes_{\mathbf{K}} W$, on déduit $\psi \circ \phi = \mathrm{Id}_{V \otimes_{\mathbf{K}} W}$. De manière analogue, on a $\phi \circ \psi = \mathrm{Id}_{T'}$.

Reste à construire $V \otimes_{\mathbf{K}} W$. Soit $\mathbf{K}^{(V \times W)}$ le $\mathbf{K}$-espace vectoriel de base $(e_{v,w})_{(v,w) \in V \times W}$. Un élément de $\mathbf{K}^{(V \times W)}$ est donc une somme (finie) $\sum \lambda_{v,w} e_{v,w}$ pour des scalaires $\lambda_{v,w}$ presque tous nuls. L'application $V \times W \to \mathbf{K}^{(V \times W)}$ donnée par $(v, w) \mapsto e_{v,w}$ n'est pas bilinéaire, mais elle va le devenir si on compose par la surjection sur un certain quotient $\mathbf{K}^{(V \times W)} \to S$. Pour trouver S, écrivons les relations dont nous avons besoin : pour $v, v' \in V$, $w, w' \in W$, $\lambda, \lambda' \in \mathbf{K}$, les quantités suivantes doivent êtres nulles

$$e_{\lambda v + \lambda' v', w} - \lambda e_{v,w} - \lambda' e_{v',w}, \tag{30}$$

$$e_{v, \lambda w + \lambda' w'} - \lambda e_{v,w} - \lambda' e_{v,w'}. \tag{31}$$

Il est donc naturel de définir S comme le sous-espace vectoriel de $\mathbf{K}^{(V \times W)}$ engendré par toutes les expressions (30) et (31) et de poser

$$T := \mathbf{K}^{(V \times W)} / S.$$

On définit maintenant l'application bilinéaire $t : V \times W \to T$ comme la composée

$$V \times W \longrightarrow \mathbf{K}^{(V \times W)} \twoheadrightarrow \mathbf{K}^{(V \times W)} / S = T.$$

Elle associe à (v, w) la classe, qu'on note $v \otimes w$, de $e_{v,w}$ dans le quotient T. Puisque $\mathbf{K}^{(V \times W)}$ est engendré par les $e_{v,w}$, son quotient T est engendré par les éléments de type $v \otimes w$, c'est-à-dire par les tenseurs décomposables.

Pour montrer qu'on a ainsi obtenu le produit tensoriel de V et W, il reste à montrer la propriété universelle : si on a une application bilinéaire $b : V \times W \to E$, on peut définir une application linéaire $g : \mathbf{K}^{(V \times W)} \to E$ en posant $g(e_{v,w}) = b(v, w)$. Puisque b est bilinéaire, g s'annule sur le sous-espace S et passe donc au quotient pour donner une application linéaire $\hat{b} : T \to E$. L'identité $b = \hat{b} \circ t$ est claire et l'unicité de $\hat{b}$ provient du fait que T est engendré par les $v \otimes w$; or l'image de $v \otimes w$ par $\hat{b}$ est déterminée, puisque ce doit être $b(v, w)$. □

Corollaire 1.2. — *Soient* V, W *et* E *des* $\mathbf{K}$*-espaces vectoriels. L'espace vectoriel des applications bilinéaires* $V \times W \to E$ *est isomorphe à* $\mathrm{Hom}(V \otimes W, E)$. *En particulier, l'espace des formes bilinéaires sur* $V \times W$ *est isomorphe à* $(V \otimes W)^*$.

Démonstration. — L'isomorphisme est obtenu en passant d'une application bilinéaire $b : V \times W \to E$ à $\hat{b} \in \mathrm{Hom}(V \otimes W, E)$ par la propriété universelle. Dans l'autre direction, on obtient b à partir de $\hat{b}$ par restriction aux tenseurs décomposables. □

***Proposition 1.3* (Fonctorialité).** — *Si on a des applications linéaires* $f : V_1 \to V_2$ *et* $g : W_1 \to W_2$, *il existe une et une seule application linéaire* $f \otimes g : V_1 \otimes W_1 \to V_2 \otimes W_2$ *telle que* $(f \otimes g)(v \otimes w) = f(v) \otimes g(w)$ *pour tous* v, w.

En outre, $(f_2 \otimes g_2) \circ (f_1 \otimes g_1) = (f_2 \circ f_1) \otimes (g_2 \circ g_1)$.

Démonstration. — Il s'agit de compléter le diagramme commutatif

$$\begin{array}{ccc} \mathrm{V}_1 \times \mathrm{W}_1 & \xrightarrow{f \times g} & \mathrm{V}_2 \times \mathrm{W}_2 \\ \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle t'} \\ \mathrm{V}_1 \otimes \mathrm{W}_1 & \overset{f \otimes g}{\dashrightarrow} & \mathrm{V}_2 \otimes \mathrm{W}_2. \end{array}$$

Il suffit d'appliquer la propriété universelle à l'application bilinéaire $t' \circ (f \times g)$.

La seconde assertion résulte de la propriété d'unicité de la première assertion appliquée à $(f_2 \circ f_1) \otimes (g_2 \circ g_1)$. Les détails sont laissés au lecteur. □

Propriétés du produit tensoriel 1.4. — *Soient* U, V *et* W *des* **K***-espaces vectoriels. On a des isomorphismes canoniques*

$$\begin{array}{ll} \mathbf{K} \otimes \mathrm{V} \xrightarrow{\sim} \mathrm{V} & \lambda \otimes v \longmapsto \lambda v, \\ (\mathrm{U} \oplus \mathrm{V}) \otimes \mathrm{W} \xrightarrow{\sim} (\mathrm{U} \otimes \mathrm{W}) \oplus (\mathrm{V} \otimes \mathrm{W}) & (u+v) \otimes w \longmapsto u \otimes w + v \otimes w, \\ \mathrm{U} \otimes \mathrm{V} \xrightarrow{\sim} \mathrm{V} \otimes \mathrm{U} & u \otimes v \longmapsto v \otimes u, \\ \mathrm{U} \otimes (\mathrm{V} \otimes \mathrm{W}) \xrightarrow{\sim} (\mathrm{U} \otimes \mathrm{V}) \otimes \mathrm{W} & u \otimes (v \otimes w) \longmapsto (u \otimes v) \otimes w. \end{array}$$

Attention : la colonne de droite ne définit les isomorphismes que sur les tenseurs décomposables, alors que tous les tenseurs ne le sont pas. Mais ces applications sont linéaires, donc elles sont uniquement déterminées par leur valeur sur ces tenseurs particuliers.

Démonstration. — L'application $\mathbf{K} \times \mathrm{V} \to \mathrm{V}$ donnée par $(\lambda, v) \mapsto \lambda v$ est bilinéaire, donc il y a une application linéaire induite $\mathbf{K} \otimes \mathrm{V} \to \mathrm{V}$, qui envoie $\lambda \otimes v$ sur λv. L'inverse est $v \mapsto 1 \otimes v$, d'où le premier l'isomorphisme.

Pour le deuxième isomorphisme, montrons la généralisation suivante : soit $(\mathrm{V}_i)_{i \in \mathrm{I}}$ une famille d'espaces vectoriels ; l'application

$$\begin{array}{ccc} \left(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\right) \times \mathrm{W} & \longrightarrow & \bigoplus_{i \in \mathrm{I}} (\mathrm{V}_i \otimes \mathrm{W}) \\ \left(\sum_{i \in \mathrm{I}} v_i, w\right) & \longmapsto & \sum_{i \in \mathrm{I}} v_i \otimes w \end{array}$$

est bilinéaire. Elle se factorise donc en

$$\left(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\right) \times \mathrm{W} \longrightarrow \left(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\right) \otimes \mathrm{W} \xrightarrow{\phi} \bigoplus_{i \in \mathrm{I}} (\mathrm{V}_i \otimes \mathrm{W}).$$

Inversement, les injections canoniques $\iota_i : \mathrm{V}_i \longrightarrow \oplus_{i \in \mathrm{I}} \mathrm{V}_i$ induisent par la prop. 1.3 des applications linéaires $\iota_i \otimes \mathrm{Id}_\mathrm{W} : \mathrm{V}_i \otimes \mathrm{W} \longrightarrow \left(\oplus_{i \in \mathrm{I}} \mathrm{V}_i\right) \otimes \mathrm{W}$, donc une application linéaire

$$\bigoplus_{i \in \mathrm{I}} (\iota_i \otimes \mathrm{Id}_\mathrm{W}) : \bigoplus_{i \in \mathrm{I}} (\mathrm{V}_i \otimes \mathrm{W}) \longrightarrow \left(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\right) \otimes \mathrm{W}$$

qui est un inverse de ϕ. On a donc un isomorphisme canonique

$$\left(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\right) \otimes \mathrm{W} \xrightarrow{\sim} \bigoplus_{i \in \mathrm{I}} (\mathrm{V}_i \otimes \mathrm{W}). \tag{32}$$

Les autres isomorphismes se démontrent de façon similaire. □

Si $(v_i)_{i\in \mathrm{I}}$ est une base de V, on a $\mathrm{V} \simeq \bigoplus_{i\in \mathrm{I}} \mathbf{K}v_i$ et on déduit de (32) un isomorphisme

$$\mathrm{V}\otimes \mathrm{W} \simeq \bigoplus_{i\in \mathrm{I}} (\mathbf{K}v_i \otimes \mathrm{W}).$$

Tout élément de $\mathrm{V}\otimes \mathrm{W}$ s'écrit donc de manière unique $\sum_{i\in \mathrm{I}} v_i \otimes w'_i$, où $(w'_i)_{i\in \mathrm{I}}$ est une famille presque nulle d'éléments de W.

De même, si $(w_j)_{j\in \mathrm{J}}$ est une base de W, on a $\mathrm{W} \simeq \bigoplus_{j\in \mathrm{J}} \mathbf{K}w_j$ et on déduit de (32) un isomorphisme

$$\mathrm{V}\otimes \mathrm{W} \simeq \bigoplus_{j\in \mathrm{J}} (\mathrm{V}\otimes \mathbf{K}w_j).$$

Tout élément de $\mathrm{V}\otimes \mathrm{W}$ s'écrit donc de manière unique $\sum_{j\in \mathrm{J}} v'_j \otimes w_j$, où $(v'_j)_{j\in \mathrm{J}}$ est une famille presque nulle d'éléments de V.

On a aussi un isomorphisme

$$\mathrm{V}\otimes \mathrm{W} \simeq \bigoplus_{i\in \mathrm{I},\, j\in \mathrm{J}} \mathbf{K}(v_i \otimes w_j),$$

ce qui signifie que $(v_i \otimes w_j)_{(i,j)\in \mathrm{I}\times \mathrm{J}}$ est une base de $\mathrm{V}\otimes \mathrm{W}$.

En particulier, on a

$$\dim(\mathrm{V}\otimes \mathrm{W}) = \dim(\mathrm{V})\dim(\mathrm{W}).$$

Si V_1 a pour base $(v_{1,j})_{j\in \mathrm{I}_1}$, V_2 a pour base $(v_{2,i})_{i\in \mathrm{I}_2}$, W_1 a pour base $(w_{1,l})_{l\in \mathrm{J}_1}$ et W_2 a pour base $(w_{2,k})_{k\in \mathrm{J}_2}$ et qu'on a des applications linéaires $f : \mathrm{V}_1 \to \mathrm{V}_2$ et $g : \mathrm{W}_1 \to \mathrm{W}_2$ de matrices respectives $\mathrm{A} = (a_{ij})_{i\in \mathrm{I}_2,\, j\in \mathrm{I}_1}$ et $\mathrm{B} = (b_{kl})_{k\in \mathrm{J}_2,\, l\in \mathrm{J}_1}$ dans ces bases, alors

$$(f\otimes g)(v_{1,j}\otimes w_{1,l}) = \sum_{i\in \mathrm{I}_2,\, k\in \mathrm{J}_2} a_{ij}b_{kl}\, v_{2,i}\otimes w_{2,k},$$

de sorte que la matrice de $f\otimes g$ dans les bases $(v_{1,j}\otimes w_{1,l})_{(j,l)\in \mathrm{I}_1\times \mathrm{J}_1}$ de $\mathrm{V}_1\otimes \mathrm{W}_1$ et $(v_{2,i}\otimes w_{2,k})_{(i,k)\in \mathrm{I}_2\times \mathrm{J}_2}$ de $\mathrm{V}_2\otimes \mathrm{W}_2$ est

$$\mathrm{A}\otimes \mathrm{B} := (a_{ij}b_{kl})_{(i,k)\in \mathrm{I}_2\times \mathrm{J}_2,\,(j,l)\in \mathrm{I}_1\times \mathrm{J}_1}.$$

Par exemple, si $\mathrm{V}_1, \mathrm{V}_2, \mathrm{W}_1, \mathrm{W}_2$ sont tous de dimension 2 et qu'on choisit sur $\{1,2\}\times\{1,2\}$ l'ordre $(1,1),(1,2),(2,1),(2,2)$, la matrice est

$$\mathrm{A}\otimes \mathrm{B} = \begin{pmatrix} a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix} = \begin{pmatrix} a_{11}\mathrm{B} & a_{12}\mathrm{B}\\ a_{21}\mathrm{B} & a_{22}\mathrm{B}\end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12}\\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22}\\ a_{12}b_{11} & a_{12}b_{12} & a_{22}b_{11} & a_{22}b_{12}\\ a_{12}b_{21} & a_{12}b_{22} & a_{22}b_{21} & a_{22}b_{22}\end{pmatrix}.$$

On appelle aussi cette matrice le *produit de Kronecker* des matrices A et B (on le définit de façon analogue pour des matrices de taille quelconque). Noter qu'il n'est pas commutatif (parce que l'ordre sur $\{1,2\}\times\{1,2\}$ n'est pas invariant par permutation des deux facteurs), mais que la matrice $\mathrm{B}\otimes \mathrm{A}$ est simplement obtenue à partir de $\mathrm{A}\otimes \mathrm{B}$ en faisant des permutations de lignes et de colonnes.

Exercice 1.5. — Montrer les relations

$$\mathrm{rg}(\mathrm{A}\otimes \mathrm{B}) = \mathrm{rg}(\mathrm{A})\,\mathrm{rg}(\mathrm{B}), \quad \mathrm{tr}(\mathrm{A}\otimes \mathrm{B}) = \mathrm{tr}(\mathrm{A})\,\mathrm{tr}(\mathrm{B}), \quad \det(\mathrm{A}\otimes \mathrm{B}) = \det(\mathrm{A})^b \det(\mathrm{B})^a$$

où, dans les deux dernières égalités, A est carrée d'ordre a et B carrée d'ordre b.

Exemples 1.6. — 1° L'application

$$\begin{aligned} \psi : V^* \otimes W &\longrightarrow \mathrm{Hom}(V,W) \\ \alpha \otimes w &\longmapsto (v \mapsto \alpha(v)w) \end{aligned} \tag{33}$$

est linéaire. Elle est injective : en effet, si $(w_j)_{j\in J}$ est une base de W, on a vu que tout élément de $V^* \otimes W$ s'écrit $\sum_{j\in J} \alpha_j \otimes w_j$, où $(\alpha_j)_{j\in J}$ est une famille presque nulle d'éléments de V^*. Si son image est nulle, c'est que $\sum_{j\in J} \alpha_j(v)w_j = 0$ pour tout $v \in V$, ce qui entraîne $\alpha_j(v) = 0$ pour tout $j \in J$, puisque $(w_j)_{j\in J}$ est une base de W. On a donc $\alpha_j = 0$ pour tout $j \in J$.

L'application ψ n'est pas toujours surjective : son image consiste en fait en les applications linéaires de rang fini. Elle est donc surjective si et seulement si V ou W est de dimension finie. Concrètement, si par exemple V est de dimension finie et que $(v_i)_{1\leqslant i\leqslant n}$ en est une base, de base duale $(v^i)_{1\leqslant i\leqslant n}$, on a pour $u \in \mathrm{Hom}(V,W)$ la formule

$$\psi^{-1}(u) = \sum_{i=1}^{n} v^i \otimes u(v_i).$$

2° Le produit tensoriel $\mathbf{K}[X] \otimes \mathbf{K}[Y]$ est isomorphe à $\mathbf{K}[X,Y]$, par l'application $X^i \otimes Y^j \mapsto X^i Y^j$ [1].

3° On peut définir plus généralement le produit tensoriel de modules sur un anneau commutatif A. La construction est la même que sur un corps, mais son comportement est plus compliqué. Si $A = \mathbf{Z}$, les A-modules sont les groupes abéliens et on a par exemple $\mathbf{Z}^k \otimes_{\mathbf{Z}} \mathbf{Z}^l = \mathbf{Z}^{kl}$, mais aussi $(\mathbf{Z}/n\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Q} = 0$, $(\mathbf{Z}/3\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/2\mathbf{Z}) = 0$ et $(\mathbf{Z}/3\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/3\mathbf{Z}) = \mathbf{Z}/3\mathbf{Z}$ (pourquoi ?).

4° *Extension des scalaires.* Si on a un corps $\mathbf{L} \supseteq \mathbf{K}$ et que V est un $\mathbf{K}$-espace vectoriel, puisque $\mathbf{L}$ est un $\mathbf{K}$-espace vectoriel, on peut former le $\mathbf{K}$-espace vectoriel

$$V^{\mathbf{L}} = \mathbf{L} \otimes_{\mathbf{K}} V.$$

On peut donner à $V^{\mathbf{L}}$ une structure de $\mathbf{L}$-espace vectoriel de la manière suivante : si $\ell \in \mathbf{L}$, la multiplication m_ℓ par ℓ est un endomorphisme $\mathbf{K}$-linéaire de $\mathbf{L}$, donc on peut définir la multiplication par ℓ sur $V^{\mathbf{L}}$ comme l'endomorphisme $m_\ell \otimes 1$. Les propriétés de $\mathbf{L}$-espace vectoriel sont faciles à vérifier. On dit que $V^{\mathbf{L}}$ est obtenu à partir de V par extension des scalaires de $\mathbf{K}$ à $\mathbf{L}$. On a $\dim_{\mathbf{L}}(V^{\mathbf{L}}) = \dim_K(V)$: si $(v_i)_{i\in I}$ est une $\mathbf{K}$-base de V, alors $(1 \otimes v_i)_{i\in I}$ est une $\mathbf{L}$-base de $V^{\mathbf{L}}$.

Un endomorphisme $u \in \mathrm{End}_{\mathbf{K}}(V)$ s'étend en $u^{\mathbf{L}} = \mathrm{Id}_{\mathbf{L}} \otimes u \in \mathrm{End}_{\mathbf{L}}(V^{\mathbf{L}})$. Si u a comme matrice A dans une $\mathbf{K}$-base (v_i) de V, alors $u^{\mathbf{L}}$ a la même matrice A dans la $\mathbf{L}$-base $(1 \otimes v_i)$ de $V^{\mathbf{L}}$.

Par exemple, si $\mathbf{K} = \mathbf{R}$ et $\mathbf{L} = \mathbf{C}$, alors $V^{\mathbf{C}} = \mathbf{C} \otimes_{\mathbf{R}} V$ est la *complexification* de l'espace vectoriel réel V.

Exercice 1.7. — Soient V et W des espaces vectoriels de dimension finie.
a) Quelle est l'image de l'ensemble des tenseurs décomposables par l'application (33) de l'ex. 1.6 ?
b) On sait que tout élément de $V \otimes W$ peut s'écrire comme somme de tenseurs décomposables. Quel est le nombre maximal de tenseurs décomposables dont on a besoin ?

1. Mais attention : $\mathbf{K}(X) \otimes \mathbf{K}(Y)$ n'est pas isomorphe à $\mathbf{K}(X,Y)$ (pourquoi ?) !

Exercice 1.8. — Soit f_1 (resp. f_2) une forme quadratique sur un $\mathbf{K}$-espace vectoriel V_1 (resp. V_2) de dimension finie .
a) Montrer qu'il existe une unique forme quadratique $f_1 \otimes f_2$ sur $V_1 \otimes V_2$ qui vérifie

$$\forall v_1, v_2 \in V \qquad (f_1 \otimes f_2)(v_1 \otimes v_2) = f_1(v_1) f_2(v_2).$$

b) Montrer que si f_1 et f_2 sont non dégénérées, il en est de même de $f_1 \otimes f_2$.
c) Avec les notations de § II.4.2, montrer que

$$\langle \alpha_1, \dots, \alpha_m \rangle \otimes \langle \beta_1, \dots, \beta_n \rangle = \langle \alpha_i \beta_j, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n \rangle.$$

d) Si (V_2, f_2) est somme de plans hyperboliques, montrer qu'il en est de même pour $(V_1 \otimes V_2, f_1 \otimes f_2)$.
e) En déduire que le produit tensoriel des formes quadratiques définit une structure d'anneau sur le groupe de Witt $W(\mathbf{K})$ (§ II.6).

Exercice 1.9. — a) Rappeler la structure de $\mathbf{R}$-algèbre de $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}$.
b) Montrer qu'il y a deux structures de $\mathbf{C}$-algèbre non isomorphes sur $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}$.
c) Montrer que les $\mathbf{C}$-algèbres $\mathscr{M}_2(\mathbf{C})$ et $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C}$ sont isomorphes ($\mathbf{H}$ est le corps des quaternions, *cf.* § II.11).
d) Montrer que les $\mathbf{R}$-algèbres $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{H}$ et $\mathscr{M}_4(\mathbf{R})$ sont isomorphes.

2. Algèbre tensorielle

2.1. Applications d-linéaires. — Soient $V_1, \dots, V_d, E$ des $\mathbf{K}$-espaces vectoriels. Une application *d-linéaire* $V_1 \times \cdots \times V_d \to E$ est une application qui est linéaire par rapport à chacun des facteurs V_i. On peut construire comme dans le th. 1.1 un $\mathbf{K}$-espace vectoriel $V_1 \otimes \cdots \otimes V_d$ et une application d-linéaire universelle

$$V_1 \times \cdots \times V_d \to V_1 \otimes \cdots \otimes V_d.$$

L'espace vectoriel $\mathrm{Mult}^d(V_1 \times \cdots \times V_d, E)$ des applications d-linéaires de $V_1 \times \cdots \times V_d$ vers E est alors isomorphe à l'espace vectoriel $\mathrm{Hom}(V_1 \otimes \cdots \otimes V_d, E)$.

On a vu dans la section précédente (prop. 1.4) que $(V_1 \otimes V_2) \otimes V_3$ et $V_1 \otimes (V_2 \otimes V_3)$ sont canoniquement isomorphes. On vérifie facilement qu'ils le sont aussi à $V_1 \otimes V_2 \otimes V_3$.

De la même manière que pour le produit tensoriel, si on a des applications linéaires $f_i : V_i \to W_i$, on obtient une application linéaire unique

$$f_1 \otimes \cdots \otimes f_d : V_1 \otimes \cdots \otimes V_d \longrightarrow W_1 \otimes \cdots \otimes W_d$$

qui vérifie sur les tenseurs décomposables la relation

$$(f_1 \otimes \cdots \otimes f_d)(v_1 \otimes \cdots \otimes v_d) = f_1(v_1) \otimes \cdots \otimes f_d(v_d).$$

Remarque 2.1. — Soient $V_1, \dots, V_d$ des espaces vectoriels de dimension finie. Tout élément de $V_1 \otimes \cdots \otimes V_d$ peut donc s'écrire comme somme de tenseurs décomposables. On peut se poser la question de savoir le nombre maximal de tenseurs décomposables dont on a besoin. Lorsque $d = 2$, c'est l'objet de l'exerc. 1.7. En général, on ne connaît la réponse à cette importante question que dans certains cas.

2.2. Algèbres graduées. — Rappelons qu'une **K**-*algèbre* est un **K**-espace vectoriel A muni d'un produit $A \times A \to A$ qui est une application bilinéaire et qui fait de A un anneau. Elle est donc associative, mais pas nécessairement commutative. Toutes les algèbres que nous considérerons seront munies d'une unité, c'est-à-dire d'un élément 1 tel que $a \cdot 1 = 1 \cdot a = a$ pour tout $a \in A$. On a $1 = 0$ si et seulement si $A = 0$.

L'algèbre A est *graduée* si elle est munie d'une décomposition

$$A = \bigoplus_{d \in \mathbf{N}} A_d$$

en somme directe d'espaces vectoriels telle que

$$\forall d, e \in \mathbf{N} \qquad A_d \cdot A_e \subseteq A_{d+e}.$$

Si A a une unité, on a $1 \in A_0$.

Par exemple, l'algèbre $\mathbf{K}[X]$ des polynômes à une indéterminée est graduée par $\mathbf{K}[X] = \bigoplus \mathbf{K}X^d$. L'algèbre (commutative) $A = \mathbf{K}[X_1, \dots, X_r]$ des polynômes à plusieurs indéterminés est également graduée si on définit A_d comme le sous-espace vectoriel des polynômes nuls ou homogènes de degré total d, donc engendré par les $X_1^{i_1} \cdots X_r^{i_r}$ pour $i_1 + \cdots + i_r = d$.

Un élément non nul $x \in A$ est dit *homogène* s'il existe d tel que $x \in A_d$; on dit alors que x est de degré d.

Un *morphisme d'algèbres graduées* est un morphisme d'algèbres $f : A \to B$ qui préserve la graduation : $f(A_d) \subseteq B_d$ pour tout $d \in \mathbf{N}$.

2.3. Algèbre tensorielle. — On définit les *puissances tensorielles* d'un **K**-espace vectoriel V par $T^0V = \mathbf{K}$ et, pour $d \geqslant 1$,

$$T^dV := \underbrace{V \otimes \cdots \otimes V}_{d \text{ fois}} =: V^{\otimes d}.$$

On peut voir aussi (canoniquement et par définition) le dual de T^dV comme l'espace vectoriel $\mathrm{Mult}^d(V^d, \mathbf{K})$ des formes d-linéaires sur V.

L'*algèbre tensorielle* de V est définie par

$$TV = \bigoplus_{n \in \mathbf{N}} T^dV. \tag{34}$$

Pour en faire une algèbre, nous devons définir un produit sur TV. C'est

$$\begin{array}{ccc} T^dV \times T^eV & \longrightarrow & T^{d+e}V \\ (v_1 \otimes \cdots \otimes v_d, w_1 \otimes \cdots \otimes w_e) & \longmapsto & v_1 \otimes \cdots \otimes v_d \otimes w_1 \otimes \cdots \otimes w_e. \end{array}$$

Compte tenu des propriétés du produit tensoriel vues plus haut, ce produit est bien défini ; il est associatif et fait de TV une algèbre, munie de l'unité $1 \in \mathbf{K} = T^0V$. Cette algèbre n'est pas commutative dès que $\dim(V) \geqslant 2$: on a $v_1 \otimes v_2 \neq v_2 \otimes v_1$ dès que v_1 et v_2 ne sont pas proportionnels.

La décomposition (34) en fait une algèbre graduée. Noter la présence d'une injection canonique $\iota : V \hookrightarrow TV$ puisque T^1V s'identifie à V.

Si V a pour base $(e_i)_{i \in I}$, alors TV a pour base les $e_{i_1} \otimes \cdots \otimes e_{i_d}$ pour $d \in \mathbf{N}$ et $i_1, \dots, i_d \in I$. Même si l'espace vectoriel V est de dimension finie, l'espace vectoriel TV est toujours de dimension infinie dès que $V \neq 0$.

***Proposition 2.2* (Propriété universelle).** — *L'algèbre tensorielle* TV *satisfait la propriété universelle suivante : si* $f : \mathrm{V} \to \mathrm{A}$ *est une application linéaire vers une algèbre avec unité* A*, il existe un morphisme d'algèbres* $\hat{f} : \mathrm{TV} \to \mathrm{A}$ *unique tel que* $f = \hat{f} \circ \iota$*, c'est-à-dire que le diagramme*

$$\begin{array}{ccc} \mathrm{V} & \xrightarrow{f} & \mathrm{A} \\ {\scriptstyle\iota}\downarrow & \nearrow_{\hat{f}} & \\ \mathrm{TV} & & \end{array}$$

est commutatif.

Démonstration. — Comme l'application

$$\begin{array}{ccc} \mathrm{V}^d & \longrightarrow & \mathrm{A} \\ (v_1, \dots, v_d) & \longmapsto & f(v_1) \cdots f(v_d) \end{array}$$

est d-linéaire, la propriété universelle de $\mathrm{T}^d\mathrm{V}$ permet de définir l'application linéaire $\hat{f} : \mathrm{T}^d\mathrm{V} \to \mathrm{A}$. Reste à montrer que c'est bien un morphisme d'algèbres. Il suffit de le vérifier sur les tenseurs décomposables, qui engendrent TV ; or on a

$$\begin{aligned} \hat{f}((v_1 \otimes \cdots \otimes v_d) \otimes (w_1 \otimes \cdots \otimes w_e)) &= f(v_1) \cdots f(v_d) f(w_1) \cdots f(w_e) \\ &= \hat{f}(v_1 \otimes \cdots \otimes v_d) \hat{f}(w_1 \otimes \cdots \otimes w_e), \end{aligned}$$

ce qui montre ce qu'on veut. □

Comme dans tous les cas précédents, la propriété universelle implique la fonctorialité de la construction : si on a une application linéaire $f : \mathrm{V} \to \mathrm{W}$, il y a un morphisme d'algèbres $\mathrm{T}f : \mathrm{TV} \to \mathrm{TW}$, unique, tel que le diagramme

$$\begin{array}{ccc} \mathrm{V} & \xrightarrow{f} & \mathrm{W} \\ \downarrow{\scriptstyle\iota_{\mathrm{V}}} & & \downarrow{\scriptstyle\iota_{\mathrm{W}}} \\ \mathrm{TV} & \xrightarrow{\mathrm{T}f} & \mathrm{TW} \end{array}$$

soit commutatif. Le morphisme $\mathrm{T}f$ n'est autre que $\bigoplus \mathrm{T}^d f$, où $\mathrm{T}^d f = f^{\otimes d}$ est $\underbrace{f \otimes \cdots \otimes f}_{d \text{ fois}}$, défini plus haut. En outre, on a la propriété

$$\mathrm{T}(f \circ g) = \mathrm{T}f \circ \mathrm{T}g.$$

2.4. Tenseurs covariants et contravariants. — Ce paragraphe tente d'expliquer le language et les notations utilisés en physique (et parfois aussi en géométrie différentielle). Soit V un espace vectoriel et soit V^* son espace vectoriel dual, c'est-à-dire $\mathrm{Hom}(\mathrm{V}, \mathbf{K})$. Les « tenseurs » considérés par les physiciens sont en général des éléments d'un produit tensoriel

$$\underbrace{\mathrm{V}^* \otimes \cdots \otimes \mathrm{V}^*}_{p \text{ fois}} \otimes \underbrace{\mathrm{V} \otimes \cdots \otimes \mathrm{V}}_{q \text{ fois}} = \mathrm{T}^p\mathrm{V}^* \otimes \mathrm{T}^q\mathrm{V}.$$

Un tel tenseur T est dit « p fois covariant et q fois contravariant ». Si on choisit une base $(e_1,\dots,e_n)$ de V, de base duale $(e^1,\dots,e^n)$ de V^*, on écrit

$$\mathrm{T} = \sum_{i_1,\dots,i_q,j_1,\dots,j_p} \mathrm{T}^{i_1\dots i_q}_{j_1\dots j_p}\, e^{j_1}\otimes\cdots\otimes e^{j_p}\otimes e_{i_1}\otimes\cdots\otimes e_{i_q}$$

(la famille des $e^{j_1}\otimes\cdots\otimes e^{j_p}\otimes e_{i_1}\otimes\cdots\otimes e_{i_q}$ est une base de $\mathrm{T}^p\mathrm{V}^*\otimes\mathrm{T}^q\mathrm{V}$). En physique, on utilise la convention de sommation d'Einstein et on écrit simplement

$$\mathrm{T} = \mathrm{T}^{i_1\dots i_q}_{j_1\dots j_p}\, e^{j_1}\otimes\cdots\otimes e^{j_p}\otimes e_{i_1}\otimes\cdots\otimes e_{i_q}$$

(il est entendu qu'on somme sur les indices répétés en haut et en bas). On dit que les $\mathrm{T}^{i_1\dots i_q}_{j_1\dots j_p}$ sont les coordonnées du tenseur T.

Soit $v = v^i e_i$ un élément de V. Dans une autre base $(e'_1,\dots,e'_n)$, définie par la matrice de passage $\mathrm{P} = (\mathrm{P}^i_j)$ et $e'_j = \mathrm{P}^i_j e_i$, on a $v = v'^j e'_j$, avec

$$v = v'^j e'_j = v'^j \mathrm{P}^i_j e_i,$$

d'où $v^i = \mathrm{P}^i_j v'^j$, ou encore

$$v'^j = (\mathrm{P}^{-1})^j_i\, v^i.$$

On dit que les coordonnées de v se transforment en sens inverse des vecteurs de base (d'où la terminologie « contravariant »). Inversement, pour une forme linéaire $\alpha = \alpha_j e^j = \alpha'_i e'^i$, on a

$$\alpha'_i = \alpha(e'_i) = \alpha(\mathrm{P}^j_i e_j) = \mathrm{P}^j_i \alpha_j.$$

Les composantes de α se transforment donc dans le même sens que les vecteurs de base (d'où la terminologie « covariant »). Pour un tenseur général $\mathrm{T} = (\mathrm{T}^{i_1\dots i_q}_{j_1\dots j_p})$ qui est p fois covariant et q fois contravariant, on vérifie que ses coordonnées dans la base $(e'_1,\dots,e'_d)$ sont

$$(\mathrm{T}')^{i'_1\dots i'_q}_{j'_1\dots j'_p} = (\mathrm{P}^{-1})^{i'_1}_{i_1}\cdots(\mathrm{P}^{-1})^{i'_q}_{i_q}\mathrm{P}^{j_1}_{j'_1}\cdots\mathrm{P}^{j_p}_{j'_p}\mathrm{T}^{i_1\dots i_q}_{j_1\dots j_p}.$$

Tout cela a en général lieu en présence d'une « métrique », c'est-à-dire d'une forme bilinéaire B non dégénérée sur V (produit scalaire ou forme de Lorentz ; *cf.* exerc. II.11.6).

On appelle B le *tenseur métrique* (par le cor. 1.2, on peut voir B comme un élément de $(\mathrm{V}\otimes\mathrm{V})^* \simeq \mathrm{V}^*\otimes\mathrm{V}^*$, donc comme un tenseur 2 fois covariant) et on le note par sa matrice $g_{ij} = \mathrm{B}(e_i,e_j)$ dans la base $(e_1,\dots,e_n)$ de V. Comme la forme B est non dégénérée, elle induit un isomorphisme $\hat{\mathrm{B}} : \mathrm{V} \xrightarrow{\sim} \mathrm{V}^*$ (prop. II.3.2) qui identifie les vecteurs (contravariants) aux formes linéaires (covariantes). En coordonnées, on a $\hat{\mathrm{B}}(e_j)(e_i) = \mathrm{B}(e_j,e_i) = g_{ji}$, d'où

$$\hat{\mathrm{B}}(v^j e_j) = v^j g_{ji} e^i.$$

On passe donc des coordonnées contravariantes (v^j) aux coordonnées covariantes (v_i) par la formule $v_i = v^j g_{ji}$. On peut faire le même genre de manipulations avec les tenseurs. L'exercice est laissé au lecteur.

L'isomorphisme $\hat{\mathrm{B}}$ permet aussi de transporter la métrique B en une métrique B^* sur V^*. On vérifie que la matrice $g^{ij} := \mathrm{B}^*(e^i,e^j)$ de B^* dans la base duale $(e^1,\dots,e^d)$ de V^* est la matrice inverse de la matrice (g_{ij}), c'est-à-dire $g_{ij}g^{jk} = \delta^k_i$. Ce « tenseur métrique

dual » permet de passer des coordonnées covariantes aux coordonnées contravariantes par la formule $v^j = v_i g^{ij}$. Finalement, le produit scalaire s'écrit

$$\mathrm{B}(u,v) = u^i v_i = u_i v^i = g_{ij} u^i v^j = g^{ij} u_i v_j.$$

3. Algèbre extérieure

On a introduit dans la section précédente l'algèbre tensorielle $\mathrm{TV} = \bigoplus \mathrm{T}^d\mathrm{V}$, où $\mathrm{T}^d\mathrm{V}$ est canoniquement le dual de $\mathrm{Mult}^d(\mathrm{V}^d, \mathbf{K})$ (les formes d-linéaires sur V). Dans cette section, nous faisons une construction analogue pour l'espace vectoriel $\mathrm{Alt}^d(\mathrm{V})$ des *formes d-linéaires alternées* sur V, c'est-à-dire satisfaisant $a(v_1,\dots,v_d) = 0$ dès qu'au moins deux des vecteurs $v_1,\dots,v_d$ sont égaux.

L'algèbre extérieure $\bigwedge\mathrm{V}$, avec une inclusion $\iota : \mathrm{V} \hookrightarrow \bigwedge\mathrm{V}$, sera la solution du problème universel pour les applications linéaires $f : \mathrm{V} \to \mathrm{A}$ de V vers une algèbre avec unité A, satisfaisant l'identité

$$f(v)^2 = 0. \tag{35}$$

Compte tenu de la propriété universelle de l'algèbre TV, l'injection ι doit se factoriser via TV ; en même temps, comme dans les cas précédents, $\bigwedge\mathrm{V}$ sera engendrée par les images des tenseurs décomposables. Il est donc légitime de chercher $\bigwedge\mathrm{V}$ comme quotient de TV, sous la forme [2]

$$\bigwedge\mathrm{V} := \mathrm{TV}/\mathrm{I}.$$

Il faut mettre dans l'idéal I tout ce dont on a besoin pour factoriser les applications satisfaisant (35). Les éléments de la forme $v \otimes v$, pour $v \in \mathrm{V}$ sont de ce type, puisqu'ils sont envoyés sur 0. Il est alors naturel de définir $\mathrm{I} \subseteq \mathrm{TV}$ comme l'idéal bilatère engendré par les éléments de type $v \otimes v$, pour $v \in \mathrm{V}$, c'est-à-dire l'ensemble des sommes finies d'éléments de TV du type

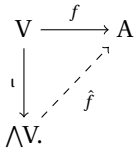
$$a \otimes v \otimes v \otimes b,$$

pour $v \in \mathrm{V}$ et $a, b \in \mathrm{TV}$, et l'*algèbre extérieure* par

$$\bigwedge\mathrm{V} = \mathrm{TV}/\mathrm{I}.$$

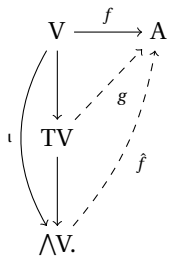
La composition $\mathrm{V} \hookrightarrow \mathrm{TV} \to \mathrm{TV}/\mathrm{I}$ fournit l'application $\iota : \mathrm{V} \to \bigwedge\mathrm{V}$.

Proposition 3.1. — *L'algèbre extérieure satisfait la propriété universelle suivante : si $f : \mathrm{V} \to \mathrm{A}$ est une application linéaire vers une algèbre avec unité, telle que $f(v)^2 = 0$ pour tout v, alors f se factorise de manière unique en $f = \hat{f} \circ \iota$, où $\hat{f} : \bigwedge\mathrm{V} \to \mathrm{A}$ est un morphisme d'algèbres :*



2. Comme pour les anneaux, on peut définir le quotient d'une algèbre A par un idéal bilatère I, c'est-à-dire un sous-espace vectoriel $\mathrm{I} \subseteq \mathrm{A}$ satisfaisant $\mathrm{AI} \subseteq \mathrm{I}$ et $\mathrm{IA} \subseteq \mathrm{I}$. On forme alors le quotient comme espace vectoriel A/I et les propriétés $\mathrm{AI} \subseteq \mathrm{I}$ et $\mathrm{IA} \subseteq \mathrm{A}$ sont exactement ce qu'il faut pour que la multiplication passe au quotient.

Démonstration. — Par la propriété universelle de TV (prop. 2.2), on a une factorisation de f par une application linéaire $g : \mathrm{TV} \to \mathrm{A}$. Puisque $g(v \otimes v) = f(v)^2 = 0$, l'application g s'annule sur l'idéal I donc g passe au quotient pour fournir un morphisme d'algèbres $\hat{f} : \bigwedge \mathrm{V} = \mathrm{TV}/\mathrm{I} \to \mathrm{A}$. Il est manifestement unique puisque $\bigwedge \mathrm{V}$ est engendré par les tenseurs décomposables. La démonstration se résume ainsi par le diagramme



□

Comme conséquence de la prop. 3.1 ou du même énoncé pour le produit tensoriel, on obtient le résultat suivant.

Proposition 3.2. — *Si $f : \mathrm{V} \to \mathrm{W}$ est une application linéaire, elle induit un morphisme d'algèbres $\bigwedge f : \bigwedge \mathrm{V} \to \bigwedge \mathrm{W}$ tel que $\iota_\mathrm{W} \circ f = \bigwedge f \circ \iota_\mathrm{V}$. En outre, $\bigwedge(f \circ g) = \bigwedge f \circ \bigwedge g$.*

Décrivons maintenant de manière plus concrète l'algèbre $\bigwedge \mathrm{V}$. Pour cela, remarquons que I est un *idéal homogène* de TV, c'est-à-dire qu'on a

$$\mathrm{I} = \bigoplus_d (\mathrm{I} \cap \mathrm{T}^d \mathrm{V}).$$

En effet, un élément de I est une somme finie d'éléments de type $a \otimes v \otimes v \otimes b$, pour $a, b \in \mathrm{TV}$ et $v \in \mathrm{V}$. En écrivant a et b comme somme d'éléments homogènes, on voit que chaque $a \otimes v \otimes v \otimes b$ est somme d'éléments homogènes qui sont dans I [3].

Il en résulte que le quotient $\bigwedge \mathrm{V} = \mathrm{TV}/\mathrm{I}$ est encore une algèbre graduée :

$$\bigwedge \mathrm{V} = \bigoplus_d \mathrm{T}^d \mathrm{V}/(\mathrm{T}^d \mathrm{V} \cap \mathrm{I}) =: \bigoplus_d \bigwedge^d \mathrm{V},$$

où $\bigwedge^d \mathrm{V}$ est appelée la *puissance extérieure d-ième* de V.

Puisque l'idéal I est engendré par les éléments $v \otimes v$, il ne rencontre $\mathrm{T}^0\mathrm{V}$ et $\mathrm{T}^1\mathrm{V} = \mathrm{V}$ qu'en 0, donc

$$\bigwedge^0 \mathrm{V} = \mathbf{K}, \quad \bigwedge^1 \mathrm{V} = \mathrm{V}$$

et le morphisme $\iota : \mathrm{V} \to \bigwedge \mathrm{V}$ est une injection.

Le produit dans $\bigwedge \mathrm{V}$ est appelé *produit extérieur* et noté $\wedge$. Le $\mathbf{K}$-espace vectoriel $\bigwedge \mathrm{V}$ est engendré par les $v_1 \wedge \cdots \wedge v_d$ pour $d \in \mathbf{N}$ et $v_1, \ldots, v_d \in \mathrm{V}$. Le fait que l'algèbre $\bigwedge \mathrm{V}$ soit graduée s'écrit

$$\bigwedge^d \mathrm{V} \wedge \bigwedge^e \mathrm{V} \subseteq \bigwedge^{d+e} \mathrm{V}.$$

3. Plus généralement, un idéal d'une algèbre graduée qui est engendré par des éléments homogènes (comme c'est le cas pour I) est homogène.

Si $f : V \to W$ est une application linéaire, il s'ensuit qu'on a

$$\bigwedge f = \bigoplus_d \bigwedge^d f, \quad \text{avec } \bigwedge^d f : \bigwedge^d V \longrightarrow \bigwedge^d W.$$

Proposition 3.3. — *L'application d-linéaire*

$$\begin{array}{ccc} V^d & \longrightarrow & \bigwedge^d V \\ (v_1, \dots, v_d) & \longmapsto & v_1 \wedge \cdots \wedge v_d \end{array}$$

est alternée. En particulier, elle est antisymétrique : pour tout $\sigma \in \mathfrak{S}_d$ et $v_1, \dots, v_d \in V$, on a

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(d)} = \varepsilon(\sigma) v_1 \wedge \cdots \wedge v_d. \tag{36}$$

Démonstration. — Par définition de I et de $\bigwedge V$, l'expression $v_1 \wedge \cdots \wedge v_d$ est nulle dès que deux consécutifs des vecteurs $v_1, \dots, v_d$ sont égaux. De $v \wedge v = w \wedge w = (v+w) \wedge (v+w) = 0$, on déduit l'identité $w \wedge v = -v \wedge w$. Cela entraîne que la relation (36) est vérifiée lorsque σ est une des transpositions $(12), (23), \dots, ((d-1)\ d)$. Or, si cette relation est vérifiée pour des permutations σ et τ et tous $v_1, \dots, v_d \in V$, on a

$$\begin{array}{rcl} v_{\tau\sigma(1)} \wedge \cdots \wedge v_{\tau\sigma(d)} & = & \varepsilon(\tau) v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(d)} \\ & = & \varepsilon(\tau)\varepsilon(\sigma) v_1 \wedge \cdots \wedge v_d, \end{array}$$

c'est-à-dire qu'elle est vérifiée pour le produit $\tau\sigma$. Comme les transpositions $(12), (23), \dots, ((d-1)\ d)$ engendrent $\mathfrak{S}_d$ (ex. I.1.8.2°), cela démontre (36).

Si deux des vecteurs $v_1, \dots, v_d$ sont égaux, on se ramène par une permutation adéquate au cas où ils sont consécutifs, d'où on déduit (en utilisant (36)) $v_1 \wedge \cdots \wedge v_d = 0$; l'application $(v_1, \dots, v_d) \mapsto v_1 \wedge \cdots \wedge v_d$ est donc bien alternée. □

Proposition 3.4. — *L'algèbre graduée $\bigwedge V$ est* anticommutative, *c'est-à-dire que si $\alpha \in \bigwedge^d V$ et $\beta \in \bigwedge^e V$, on a $\beta \wedge \alpha = (-1)^{de} \alpha \wedge \beta$.*

Démonstration. — Il suffit de le montrer lorsque α et β sont des produits extérieurs d'éléments de V. Cela se déduit de l'identité $w \wedge v = -v \wedge w$. □

Proposition 3.5 **(Propriétés de $\bigwedge^d V$).** — *1° L'application d-linéaire alternée*

$$\begin{array}{ccc} V^d & \longrightarrow & \bigwedge^d V \\ (v_1, \dots, v_d) & \longmapsto & v_1 \wedge \cdots \wedge v_d \end{array}$$

satisfait la propriété universelle suivante : si on a une application d-linéaire alternée $a : V^d \to E$, il existe une unique application linéaire $\hat{a} : \bigwedge^d V \to E$ telle que le diagramme

$$\begin{array}{ccc} V^d & \xrightarrow{a} & E \\ \downarrow & \nearrow_{\hat{a}} & \\ \bigwedge^d V & & \end{array}$$

soit commutatif. En particulier, $\mathrm{Alt}^d(V) \simeq (\bigwedge^d V)^*$.

2° Si $(e_1, \dots, e_n)$ est une base de V, alors $(e_{i_1} \wedge \cdots \wedge e_{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$ est une base de $\bigwedge^d V$. En particulier, on a $\bigwedge^d V = 0$ pour $d > n$, et

$$\dim(\bigwedge^d V) = \binom{n}{d}.$$

3° Si V *est de dimension finie n et* $0 \leqslant d \leqslant n$*, la forme bilinéaire*

$$\begin{aligned} \textstyle\bigwedge^d \mathrm{V} \times \bigwedge^{n-d} \mathrm{V} &\longrightarrow \textstyle\bigwedge^n \mathrm{V} \simeq \mathbf{K} \\ (\alpha, \beta) &\longmapsto \alpha \wedge \beta \end{aligned}$$

est non dégénérée. En particulier, on a un isomorphisme non canonique[4]

$$\left(\textstyle\bigwedge^d \mathrm{V}\right)^* \simeq \bigwedge^{n-d} \mathrm{V}.$$

4° Il existe une application bilinéaire

$$\begin{aligned} \textstyle\bigwedge^d (\mathrm{V}^*) \times \bigwedge^d \mathrm{V} &\longrightarrow \mathbf{K} \\ (\alpha_1 \wedge \cdots \wedge \alpha_d, v_1 \wedge \cdots \wedge v_d) &\longmapsto \det(\alpha_i(v_j))_{1 \leqslant i,j \leqslant d} \end{aligned}$$

et elle est non dégénérée. Si V *est de dimension finie, on en déduit un isomorphisme canonique*

$$\textstyle\bigwedge^d (\mathrm{V}^*) \simeq \left(\bigwedge^d \mathrm{V}\right)^*.$$

5° Si V *est de dimension finie n, on a* $\dim(\bigwedge^n \mathrm{V}) = 1$ *par le point 2°. Si* $u \in \mathrm{End}(\mathrm{V})$*, l'endomorphisme* $\bigwedge^n u$ *de* $\bigwedge^n \mathrm{V}$ *est donc la multiplication par un scalaire, qui est* $\det(u)$*.*

Le point 4° est utile notamment en géométrie différentielle : les applications de $\mathbf{R}^n$ dans $\bigwedge^d (\mathbf{R}^n)^*$ sont en effet les d-formes différentielles sur $\mathbf{R}^n$.

Démonstration. — 1° Par la propriété universelle de $\mathrm{T}^d\mathrm{V}$, l'application d-linéaire a se factorise en $a = g \circ i$, où $g \in \mathrm{Hom}(\mathrm{T}^d\mathrm{V}, \mathrm{E})$ et i est l'application d-linéaire canonique $\mathrm{V}^d \to \mathrm{T}^d\mathrm{V}$. Mais, parce que a est alternée, g s'annule sur $\mathrm{I} \cap \mathrm{T}^d\mathrm{V}$, donc se factorise à travers le quotient $\bigwedge^d \mathrm{V}$ en une application linéaire $\hat{a} \in \mathrm{Hom}(\bigwedge^d \mathrm{V}, \mathrm{E})$. L'unicité de $\hat{a}$ provient du fait que $\bigwedge^d \mathrm{V}$ est engendré par les $v_1 \wedge \cdots \wedge v_d$.

2° et 3° Par (36), les $(e_{i_1} \wedge \cdots \wedge e_{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$ engendrent $\bigwedge^d \mathrm{V}$ et il reste à voir qu'ils sont linéairement indépendants. C'est le cas lorsque $d = n$: il existe en effet une forme n-linéaire alternée non nulle, à savoir le déterminant (dans une base donnée), donc $\bigwedge^n \mathrm{V}$ n'est pas nul. Comme il est engendré par $e_1 \wedge \cdots \wedge e_n$, il est de dimension 1 et ce vecteur n'est pas nul.

Fixons $1 \leqslant j_1 < \cdots < j_{n-d} \leqslant n$; le seul cas où le produit extérieur de $e_{i_1} \wedge \cdots \wedge e_{i_d}$ avec $e_{j_1} \wedge \cdots \wedge e_{j_{n-d}}$ est non nul est lorsque $\{j_1, \ldots, j_{n-d}\}$ est le complémentaire de $\{i_1, \ldots, i_d\}$ dans $\{1, \ldots, n\}$. On en déduit que les $(e_{i_1} \wedge \cdots \wedge e_{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$ sont linéairement indépendants, ce qui montre le point 2°, ainsi que le point 3°.

4° Compte tenu des propriétés d'antisymétrie du déterminant, la formule proposée est alternée en les α_i et en les v_j et fournit donc bien une application bilinéaire $b : \bigwedge^d (\mathrm{V}^*) \times \bigwedge^d \mathrm{V} \to \mathbf{K}$. Si (e_i) est une base de V et (e^i) la base duale, et que $1 \leqslant i_1 < \cdots < i_d \leqslant n$ et $1 \leqslant j_1 < \cdots < j_d \leqslant n$, on a $b(e^{i_1} \wedge \cdots \wedge e^{i_d}, e_{j_1} \wedge \cdots \wedge e_{j_d}) = 1$ ou 0 suivant que $i_k = j_k$ pour tout k ou non. Ainsi la forme b est non dégénérée et on obtient une dualité dans laquelle $(e^{i_1} \wedge \cdots \wedge e^{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$ est la base duale de $(e_{i_1} \wedge \cdots \wedge e_{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$.

5° On a $\bigwedge^n u(e_1 \wedge \cdots \wedge e_n) = u(e_1) \wedge \cdots \wedge u(e_n) = (\sum_i u_{i1} e_i) \wedge \cdots \wedge (\sum_i u_{in} e_i) = \det(u) e_1 \wedge \cdots \wedge e_n$ après développement. □

4. Il dépend du choix d'un isomorphisme $\bigwedge^n \mathrm{V} \simeq \mathbf{K}$. L'isomorphisme $\bigwedge^n \mathrm{V} \otimes (\bigwedge^d \mathrm{V})^* \simeq \bigwedge^{n-d} \mathrm{V}$ est lui canonique (l'espace vectoriel $\bigwedge^n \mathrm{V}$ est de dimension 1, mais n'est pas canoniquement isomorphe à $\mathbf{K}$).

***Remarque 3.6* (Produit vectoriel).** — Vous avez peut-être déjà rencontré le produit vectoriel de deux vecteurs dans l'espace vectoriel euclidien orienté $\mathbf{R}^3$, ou plus généralement le produit vectoriel de $n-1$ vecteurs dans l'espace vectoriel euclidien orienté $V = \mathbf{R}^n$, qu'on note $v_1 \wedge \cdots \wedge v_{n-1}$ en France, mais $v_1 \times \cdots \times v_{n-1}$ dans le monde anglo-saxon ; adoptons cette dernière notation pour faire la différence avec le produit extérieur. Ce vecteur est défini par la propriété

$$\forall\, v \in V \qquad \langle v_1 \times \cdots \times v_{n-1}, v\rangle = \det(v_1, \ldots, v_{n-1}, v),$$

le déterminant étant pris dans une base orthonormale directe (il ne dépend alors pas du choix de cette base).

D'autre part, le produit extérieur des n vecteurs d'une telle base fournissent un générateur canonique de $\bigwedge^n V$ donc, par prop. 3.5.4° (et surtout la note 4), un isomorphisme canonique $\bigwedge^{n-1} V \simeq V^*$. Si on le compose avec l'isomorphisme $V^* \simeq V$ donné par le produit scalaire, on peut voir l'élément $v_1 \wedge \cdots \wedge v_{n-1}$ de $\bigwedge^{n-1} V$ comme un élément de V. Le lecteur vérifiera que ce n'est autre que le produit vectoriel $v_1 \times \cdots \times v_{n-1}$.

***Exemple 3.7* (Grassmanniennes).** — Soit V un espace vectoriel de dimension n. Pour tout sous-espace vectoriel $W \subseteq V$ de dimension d, la droite vectorielle $\bigwedge^d W$ est un sous-espace vectoriel de $\bigwedge^d V$ engendré par un tenseur décomposable. On peut donc la considérer comme un point de l'espace projectif $\mathbf{P}(\bigwedge^d V)$. Inversement, tout point de $\mathbf{P}(\bigwedge^d V)$ qui correspond à une droite engendrée par un tenseur décomposable (non nul) $v_1 \wedge \cdots \wedge v_d$ définit un sous-espace vectoriel $W \subseteq V$ de dimension d, à savoir $\langle v_1, \ldots, v_d\rangle$.

On a ainsi identifié l'ensemble des sous-espaces vectoriels de V de dimension fixée d à un sous-ensemble (dit « grassmannienne ») de l'espace projectif $\mathbf{P}(\bigwedge^d V)$; on le note $G(d, V)$ (lorsque $d = 1$, ce n'est autre que l'espace projectif $\mathbf{P}(V)$!).

Lorsque $\mathbf{K} = \mathbf{R}$, c'est une variété différentiable de dimension $d(n-d)$.

***Exercice 3.8*.** — a) Montrer que dans $\mathbf{P}(\bigwedge^2 \mathbf{K}^4)$, la grassmannienne $G(2, \mathbf{K}^4)$ est la quadrique projective définie par l'« équation » $\omega \wedge \omega = 0$.
b) Montrer que toute grassmannienne $G(d, V) \subseteq \mathbf{P}(\bigwedge^d V)$ est intersection de quadriques projectives.

***Exercice 3.9*.** — Soit $\mathbf{K}$ un corps et soit V un $\mathbf{K}$-espace vectoriel de dimension n. On a défini (prop. 3.2) un morphisme de groupes

$$\begin{array}{rccc} \phi_{GL} : GL(V) & \longrightarrow & GL\left(\bigwedge^2 V\right) \\ u & \longmapsto & \bigwedge^2 u. \end{array}$$

a) Déterminer le noyau de ϕ_{GL} (*Indication :* on pourra distinguer le cas $n = 2$).
b) Soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base de V. Soit $a \in \mathbf{K}$ et soit u l'endomorphisme de V défini par $u(e_i) = e_i + a\delta_{1i} e_2$, pour tout $i \in \{1, \ldots, n\}$. Calculer $\det\left(\bigwedge^2 u\right)$.
c) Exprimer $\det(\bigwedge^2 u)$ en fonction de $\det(u)$ (*Indication :* on pourra commencer par le cas $\det(u) = 1$).
d) Pour tout entier $d \geqslant 0$, exprimer $\det(\bigwedge^d u)$ en fonction de $\det(u)$.

3.1. Tenseurs antisymétriques. — Supposons $\mathrm{car}(\mathbf{K}) = 0$. Dans ce cas, on peut réaliser $\bigwedge^d V$ comme sous-espace vectoriel de $T^d V$ de la manière suivante. Chaque $\sigma \in \mathfrak{S}_d$ induit

un endomorphisme **K**-linéaire $\bar{\sigma}$ de $\mathrm{T}^d\mathrm{V}$ défini sur les tenseurs décomposables par

$$\bar{\sigma}(v_1 \otimes \cdots \otimes v_d) = v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(d)}.$$

Un tenseur $t \in \mathrm{T}^d\mathrm{V}$ est dit *antisymétrique* si $\bar{\sigma}(t) = \varepsilon(\sigma)\, t$ pour toute permutation $\sigma \in \mathfrak{S}_d$. On notera $a^d\mathrm{V} \subseteq \mathrm{T}^d\mathrm{V}$ le sous-espace vectoriel des tenseurs antisymétriques.

Considérons l'application linéaire d'*antisymétrisation*

$$\begin{array}{rccc} p : \mathrm{T}^d\mathrm{V} & \longrightarrow & \mathrm{T}^d\mathrm{V} \\ t & \longmapsto & \dfrac{1}{d!}\displaystyle\sum_{\sigma\in\mathfrak{S}_d} \varepsilon(\sigma)\bar{\sigma}(t). \end{array}$$

On a par exemple $p(v_1 \otimes v_2) = \frac{1}{2}(v_1 \otimes v_2 - v_2 \otimes v_1)$.

Proposition 3.10. — *L'application linéaire p est un projecteur ($p^2 = p$), de noyau $\mathrm{I} \cap \mathrm{T}^d\mathrm{V}$ et d'image $a^d\mathrm{V}$. Elle induit donc un isomorphisme $a^d\mathrm{V} \simeq \bigwedge^d\mathrm{V}$.*

On prendra garde que $\bigoplus_d a^d\mathrm{V}$ n'est pas une sous-algèbre de TV : le produit

$$\begin{aligned} & (v_1 \otimes v_2 - v_2 \otimes v_1) \otimes (w_1 \otimes w_2 - w_2 \otimes w_1) \\ = \quad & v_1 \otimes v_2 \otimes w_1 \otimes w_2 - v_1 \otimes v_2 \otimes w_2 \otimes w_1 - v_2 \otimes v_1 \otimes w_1 \otimes w_2 + v_2 \otimes v_1 \otimes w_2 \otimes w_1 \end{aligned}$$

de deux éléments de $a^2\mathrm{V}$ n'est en général pas dans $a^4\mathrm{V}$. On ne peut donc pas décrire la structure d'algèbre de $\bigwedge\mathrm{V}$ ainsi.

Démonstration. — Pour tout $\tau \in \mathfrak{S}_d$, on a

$$p(\bar{\tau}(t)) = \frac{1}{d!}\sum_{\sigma\in\mathfrak{S}_d} \varepsilon(\sigma)\bar{\sigma}\bar{\tau}(t) = \frac{1}{d!}\sum_{\sigma'\in\mathfrak{S}_d} \varepsilon(\sigma'\tau^{-1})\bar{\sigma}'(t) = \varepsilon(\tau)\, p(t), \tag{37}$$

et de la même façon

$$\bar{\tau}(p(t)) = \frac{1}{d!}\sum_{\sigma\in\mathfrak{S}_d} \varepsilon(\sigma)\bar{\tau}\bar{\sigma}(t) = \frac{1}{d!}\sum_{\sigma'\in\mathfrak{S}_d} \varepsilon(\tau^{-1}\sigma')\bar{\sigma}'(t) = \varepsilon(\tau)\, p(t),$$

de sorte que

$$p(p(t)) = \frac{1}{d!}\sum_{\tau\in\mathfrak{S}_d} \varepsilon(\tau)\bar{\tau}(p(t)) = \frac{1}{d!}\sum_{\tau\in\mathfrak{S}_d} \varepsilon(\tau)^2 p(t) = p(t).$$

L'image de p est donc contenue dans $a^d\mathrm{V}$.

Si $t \in a^d\mathrm{V}$, on a $p(t) = \frac{1}{d!}\sum_{\sigma\in\mathfrak{S}_d} \varepsilon(\sigma)\varepsilon(\sigma)\, t = t$. Donc p est l'identité sur $a^d\mathrm{V}$ et $p^2 = p$: c'est un projecteur d'image $a^d\mathrm{V}$.

Montrons maintenant que $\mathrm{I} \cap \mathrm{T}^d\mathrm{V}$ est contenu dans le noyau de p. L'espace vectoriel $\mathrm{I} \cap \mathrm{T}^d\mathrm{V}$ est engendré par les $t = v_1 \otimes \cdots \otimes v_d$, où $v_i = v_{i+1}$ pour un $i \in \{1, \ldots, d-1\}$. Prenons pour τ la transposition $(i\ \ i+1)$. On a alors $\bar{\tau}(t) = t$, donc, par (37), $p(t) = p(\bar{\tau}(t)) = \varepsilon(\tau)\, p(t) = -p(t)$. Comme on est en caractéristique nulle, on a bien $p(t) = 0$.

L'application p se factorise ainsi en une application linéaire surjective $\hat{p} : \bigwedge^d \mathrm{V} \twoheadrightarrow a^d \mathrm{V}$. Si π est la surjection canonique $\mathrm{T}^d\mathrm{V} \twoheadrightarrow \bigwedge^d \mathrm{V}$, on a

$$\begin{aligned}
\pi \circ \hat{p}(v_1 \wedge \cdots \wedge v_d) &= \pi \circ p(v_1 \otimes \cdots \otimes v_d) \\
&= \pi\Big(\frac{1}{d!} \sum_{\sigma \in \mathfrak{S}_d} \varepsilon(\sigma)\, v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(d)}\Big) \\
&= \frac{1}{d!} \sum_{\sigma \in \mathfrak{S}_d} \varepsilon(\sigma)\, v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(d)} \\
&= \frac{1}{d!} \sum_{\sigma \in \mathfrak{S}_d} \varepsilon(\sigma)^2 v_1 \wedge \cdots \wedge v_d \\
&= v_1 \wedge \cdots \wedge v_d.
\end{aligned}$$

On a donc $\pi \circ \hat{p} = \mathrm{Id}_{\bigwedge^d \mathrm{V}}$. Donc $\hat{p}$ est injective et $\mathrm{I} \cap \mathrm{T}^d\mathrm{V} = \ker(p)$. □

4. Pfaffien

Soit $\mathrm{A} = (a_{ij})$ une matrice $2n \times 2n$ alternée à coefficients dans un corps $\mathbf{K}$ de caractéristique quelconque [5]. Soit $(e_1, \ldots, e_{2n})$ la base canonique de l'espace vectoriel $\mathbf{K}^{2n}$. On pose

$$\rho(\mathrm{A}) := \sum_{1 \leqslant i < j \leqslant 2n} a_{ij} e_i \wedge e_j \quad \in \bigwedge^2 \mathbf{K}^{2n}.$$

Alors $\rho(\mathrm{A})^n \in \bigwedge^{2n} \mathbf{K}^{2n}$; on définit le *pfaffien* de A par la formule :

$$\rho(\mathrm{A})^n = n!\,\mathrm{Pf}(\mathrm{A})\, e_1 \wedge \cdots \wedge e_{2n}. \tag{38}$$

A priori, cette formule ne définit Pf(A) que si $\mathrm{car}(\mathbf{K}) = 0$. Néanmoins, en développant $\rho(\mathrm{A})^n$, on s'aperçoit que, pour $\mathrm{car}(\mathbf{K}) = 0$, le pfaffien Pf(A) est un polynôme en les coefficients de la matrice A, indépendant de $\mathbf{K}$, à coefficients entiers :

$$\mathrm{Pf} \in \mathbf{Z}[a_{ij}]. \tag{39}$$

Pour un corps $\mathbf{K}$ quelconque, on utilise le morphisme d'anneaux canonique $\phi : \mathbf{Z} \to \mathbf{K}$ pour définir à partir de (39) le pfaffien $\mathrm{Pf} \in \mathbf{K}[a_{ij}]$.

Exemple 4.1. — Considérons la matrice

$$\mathrm{A} = \begin{pmatrix}
0 & \lambda_1 & & & \\
-\lambda_1 & 0 & & & \\
& & \ddots & & \\
& & & 0 & \lambda_n \\
& & & -\lambda_n & 0
\end{pmatrix}. \tag{40}$$

Alors $\rho(\mathrm{A}) = \sum_{i=1}^n \lambda_i e_{2i-1} \wedge e_{2i}$ et $\mathrm{Pf}(\mathrm{A}) = \lambda_1 \cdots \lambda_n$.

5. Cela signifie $a_{ji} = -a_{ij}$ pour tous i, j ; en caractéristique 2, il faut ajouter la condition $a_{ii} = 0$.

Exemple 4.2. — Considérons la matrice alternée

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & a_{23} & a_{24} \\ -a_{13} & -a_{23} & 0 & a_{34} \\ -a_{14} & -a_{24} & -a_{34} & 0 \end{pmatrix}.$$

Alors

$$\begin{aligned} \rho(A)^2 &= (a_{12}e_1 \wedge e_2 + a_{13}e_1 \wedge e_3 + a_{14}e_1 \wedge e_4 + a_{23}e_2 \wedge e_3 + a_{24}e_2 \wedge e_4 + a_{34}e_3 \wedge e_4)^2 \\ &= 2(a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23})e_1 \wedge e_2 \wedge e_3 \wedge e_4 \end{aligned}$$

donc $\mathrm{Pf}(A) = a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}$.

Exercice 4.3. — Montrer la formule suivante, pour toute matrice $A = (a_{ij})$ alternée d'ordre $2n$:

$$\begin{aligned} \mathrm{Pf}(A) &= \frac{1}{2^n n!} \sum_{\sigma \in \mathfrak{S}_{2n}} \varepsilon(\sigma) a_{\sigma(1),\sigma(2)} \cdots a_{\sigma(2n-1),\sigma(2n)} \\ &= \sum_{\substack{\sigma \in \mathfrak{S}_{2n},\ \sigma(1)<\sigma(3)<\cdots<\sigma(2n-1) \\ \sigma(1)<\sigma(2),\ldots,\sigma(2n-1)<\sigma(2n)}} \varepsilon(\sigma) a_{\sigma(1),\sigma(2)} \cdots a_{\sigma(2n-1),\sigma(2n)}. \end{aligned}$$

Lemme 4.4. — *Si* $\mathrm{car}(\mathbf{K}) \neq 2$, *pour toute matrice antisymétrique* A *et tout* $P \in \mathrm{M}_{2n}(\mathbf{K})$, *on a* $\rho(PA^tP) = (\bigwedge^2 P)(\rho(A))$ *dans* $\bigwedge^2 \mathbf{K}^{2n}$.

Démonstration. — Par calcul direct : si $P = (p_{ij})$ et $A = (a_{kl})$, on a $PA^tP = (\sum_{k,l} p_{ik}a_{kl}p_{jl})_{i,j}$ et

$$\begin{aligned} \rho(PA^tP) &= \sum_{i<j} \sum_{k,l} p_{ik}a_{kl}p_{jl} e_i \wedge e_j = \frac{1}{2} \sum_{i,j,k,l} p_{ik}a_{kl}p_{jl} e_i \wedge e_j \\ &= \frac{1}{2} \sum_{k,l} a_{kl} P(e_k) \wedge P(e_l) = \sum_{k<l} a_{kl} P(e_k) \wedge P(e_l) \\ &= (\bigwedge^2 P)(\rho(A)). \end{aligned}$$

□

Lemme 4.5. — *Pour tout* $P \in \mathrm{M}_{2n}(\mathbf{K})$, *on a l'identité* $\mathrm{Pf}(PA^tP) = \det(P)\,\mathrm{Pf}(A)$.

Démonstration. — Il s'agit d'une identité entre polynômes à coefficients entiers en les coefficients de A et P, qu'il suffit de tester pour $\mathbf{K} = \mathbf{Q}$. Mettant l'égalité du lemme 4.4 à la puissance extérieure n-ième, on obtient

$$\begin{aligned} n!\,\mathrm{Pf}(PA^tP)\, e_1 \wedge \cdots \wedge e_{2n} &= \left((\bigwedge^2 P)(\rho(A))\right)^n = \left((\bigwedge P)(\rho(A))\right)^n \\ &= (\bigwedge P)(\rho(A)^n) = (\bigwedge^{2n} P)(\rho(A)^n) \\ &= \det(P)\, n!\,\mathrm{Pf}(A)\, e_1 \wedge \cdots \wedge e_{2n}, \end{aligned}$$

où la troisième égalité utilise que $\bigwedge P$ est un morphisme d'algèbres. □

Théorème 4.6. — *On a l'identité* $\mathrm{Pf}(A)^2 = \det(A)$.

Démonstration. — De nouveau, il s'agit d'une identité entre polynômes à coefficients entiers en les coefficients de A, donc il suffit de la tester pour $\mathbf{K} = \mathbf{Q}$. Le théorème est vrai sur les matrices de type (40), puisque le pfaffien est $\prod_i \lambda_i$ et le déterminant $\prod_i \lambda_i^2$. Or, par la théorie des formes alternées (sur un corps de caractéristique $\neq 2$; *cf.* §4.4), toute matrice antisymétrique s'écrit sous la forme $\mathrm{PA}^t\mathrm{P}$, où P est inversible et A de la forme (40), avec $\lambda_i = 1$ ou 0 (il suffit de décomposer $\mathbf{K}^{2n} = \ker(\mathrm{A}) \oplus \mathrm{E}$ et de choisir une base hyperbolique de E). Le théorème découle alors du lemme 4.5. □

Exercice 4.7. — Vérifier directement avec l'exerc. 4.2 la conclusion du théorème pour les matrices alternées d'ordre 4.

Comme conséquence, on obtient une seconde démonstration (valable aussi en caractéristique 2 !) du fait que les transformations symplectiques sont de déterminant 1.

Corollaire 4.8. — *Pour tout corps* **K**, *on a l'inclusion* $\mathrm{Sp}_{2n}(\mathbf{K}) \subseteq \mathrm{SL}_{2n}(\mathbf{K})$.

Démonstration. — On a

$$\mathrm{Sp}_{2n}(\mathbf{K}) = \{\mathrm{P} \in \mathrm{GL}_{2n}(\mathbf{K}) \mid {}^t\mathrm{P}\mathrm{J}_{2n}\mathrm{P} = \mathrm{J}_{2n}\},$$

où J_{2n} est la matrice alternée définie en (21). Par le lemme 4.5, un élément P de $\mathrm{Sp}_{2n}(\mathbf{K})$ satisfait $\det({}^t\mathrm{P})\,\mathrm{Pf}(\mathrm{J}_{2n}) = \mathrm{Pf}(\mathrm{J}_{2n})$, ce qui implique $\det(\mathrm{P}) = 1$ puisque J_{2n} est inversible. □

Exercice 4.9. — Soit **K** un corps ; on pose $\mathrm{V} := \mathbf{K}^4$, muni de la base canonique (e_1, e_2, e_3, e_4).
a) L'espace vectoriel $\bigwedge^4 \mathrm{V}$ est de dimension 1, donc isomorphe à **K** en envoyant le générateur $e_1 \wedge e_2 \wedge e_3 \wedge e_4$ sur 1. Montrer que le produit

$$\bigwedge^2 \mathrm{V} \times \bigwedge^2 \mathrm{V} \to \bigwedge^4 \mathrm{V} \xrightarrow{\sim} \mathbf{K}$$

provenant de la structure d'algèbre extérieure est une forme bilinéaire symétrique non dégénérée sur $\bigwedge^2 \mathrm{V}$. On note f la forme quadratique associée.
b) Soit W' l'espace vectoriel des matrices alternées d'ordre 4 à coefficients dans **K**. Montrer que le pfaffien définit une forme quadratique f' non dégénérée sur W'.
c) Le groupe $\mathrm{GL}_4(\mathbf{K})$ agit
– d'une part sur l'espace vectoriel $\mathrm{W} := \bigwedge^2 \mathrm{V}$ par $\mathrm{P} \cdot (v_1 \wedge v_2) = \mathrm{P}v_1 \wedge \mathrm{P}v_2$;
– d'autre part sur l'espace vectoriel W' par $\mathrm{P} \cdot \mathrm{M} = \mathrm{P}\mathrm{M}\,{}^t\mathrm{P}$.
Montrer qu'il existe un isomorphisme $\phi : \mathrm{W} \xrightarrow{\sim} \mathrm{W}'$ tel que

$$\forall w \in \mathrm{W} \quad f'(\phi(w)) = f(w) \qquad (\phi \text{ est une isométrie}) ;$$
$$\forall \mathrm{P} \in \mathrm{GL}_4(\mathbf{K}) \quad \phi(\mathrm{P} \cdot w) = \mathrm{P} \cdot \phi(w) \qquad (\phi \text{ est un morphisme de représentations (}\textit{cf.}\text{ § IV.1.1)}).$$

d) Montrer que la première de ces actions définit un morphisme de groupes $\psi : \mathrm{GL}_4(\mathbf{K}) \to \mathrm{O}(\mathrm{W}, f)$, qui induit un morphisme injectif $\bar{\psi} : \mathrm{SL}_4(\mathbf{K})/\{\pm \mathrm{I}_4\} \hookrightarrow \mathrm{SO}(\mathrm{W}, f)$ (*cf.* exerc. 3.9).
e) Montrer que l'image de ψ est contenue dans le groupe $\mathrm{O}'(\mathrm{W}, f)$ défini dans le § II.8.5, puis que ni ψ, ni $\bar{\psi}$ ne sont surjectifs si **K** n'est pas quadratiquement clos ($\mathbf{K}^{\times 2} \neq \mathbf{K}^\times$) (*Indication :* on pourra utiliser le th. II.2.6).
On peut montrer que $\bar{\psi}$ *induit en fait un isomorphisme* $\mathrm{SL}_4(\mathbf{K})/\{\pm \mathrm{I}_4\} \xrightarrow{\sim} \mathrm{SO}'(\mathrm{W}, f)$.

Exercice 4.10. — Le but de cet exercice est d'expliquer pourquoi le groupe $\mathrm{Spin}'_{3,3}(\mathbf{R})$ mentionné dans la rem. II.11.4 est isomorphe à $\mathrm{SL}_4(\mathbf{R})$ et pourquoi $\mathrm{Spin}'_{3,2}(\mathbf{R})$ est isomorphe à $\mathrm{Sp}_4(\mathbf{R})$. On se place dans la situation de l'exercice précédent, dont on garde les notations, avec $\mathbf{K} = \mathbf{R}$.

a) Déterminer la signature de la forme quadratique f' sur W' et en déduire que l'image de $\bar{\psi} : SL_4(\mathbf{R})/\{\pm I_4\} \to SO(W, f)$ est contenue dans le groupe $SO'_{3,3}(\mathbf{R})$ défini dans l'ex. II.8.12.2° (c'est un cas particulier de l'exerc. 4.9.e)).
On peut montrer que $\bar{\psi}$ *induit en fait un isomorphisme* $SL_4(\mathbf{R})/\{\pm I_4\} \xrightarrow{\sim} SO'_{3,3}(\mathbf{R})$, *donc que* $SL_4(\mathbf{R})$ *est bien le groupe* $\mathrm{Spin}'_{3,3}(\mathbf{R})$.

b) On pose $J := \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}$ et on note $H \subseteq W'$ l'hyperplan orthogonal à J pour la forme quadratique f'. Quelle est la signature de la restriction de la forme quadratique f' à H ?
f) Montrer que le groupe $\psi(Sp_4(\mathbf{R}))$ est contenu dans $SO'_{2,3}(\mathbf{R})$.
De nouveau, on peut montrer que $\bar{\psi}$ *induit en fait un isomorphisme* $Sp_4(\mathbf{R})/\{\pm I_4\} \xrightarrow{\sim} SO'_{2,3}(\mathbf{R})$, *donc que* $Sp_4(\mathbf{R})$ *est bien le groupe* $\mathrm{Spin}'_{2,3}(\mathbf{R}) = \mathrm{Spin}'_{3,2}(\mathbf{R})$.

Exercice 4.11. — Le but de cet exercice est d'expliquer pourquoi le groupe $\mathrm{Spin}_6(\mathbf{R})$ mentionné dans la rem. II.11.4 est isomorphe à $SU_4(\mathbf{C})$. On se place dans la situation de l'exerc. 4.9, dont on garde les notations, avec $\mathbf{K} = \mathbf{C}$. On a donc un morphisme injectif $\bar{\psi} : SL_4(\mathbf{C})/\{\pm I_4\} \hookrightarrow SO_6(\mathbf{C})$.

On note $\langle \cdot, \cdot \rangle$ la forme sesquilinéaire hermitienne définie positive standard sur $V = \mathbf{C}^4$.
a) Montrer que la formule

$$B(v_1 \wedge v_2, w_1 \wedge w_2) := \langle v_1, w_1 \rangle \langle v_2, w_2 \rangle - \langle v_1, w_2 \rangle \langle v_2, w_1 \rangle$$

définit une forme sesquilinéaire hermitienne définie positive sur $W = \bigwedge^2 \mathbf{C}^4$.
b) Montrer que le groupe $\psi(SU_4(\mathbf{C}))$ est contenu dans le groupe d'isométries $U(W, B) \simeq U_6(\mathbf{C})$.
Le morphisme ϕ *induit donc un morphisme injectif* $\bar{\phi} : SU_4(\mathbf{C})/\{\pm I_4\} \to U_6(\mathbf{C}) \cap SO_6(\mathbf{C})$ *dont on peut montrer qu'il est surjectif. D'autre part, on peut aussi montrer que le groupe* $U_6(\mathbf{C}) \cap SO_6(\mathbf{C})$ *est isomorphe à* $SO_6(\mathbf{R})$. *Donc* $SU_4(\mathbf{C})$ *est bien le groupe* $\mathrm{Spin}_6(\mathbf{R})$.

5. Algèbre symétrique

On sera ici très bref car la construction est entièrement parallèle à celle de l'algèbre extérieure. Le problème universel à résoudre ici est celui pour les morphismes $V \to A$ où A est une algèbre *commutative* avec unité. L'algèbre solution de ce problème est l'*algèbre symétrique* SV, obtenue comme le quotient

$$SV := TV/J,$$

où J est l'idéal de TV dans lequel on a mis exactement ce qu'il faut pour que le quotient soit commutatif. Donc J est l'idéal engendré par les éléments du type

$$v \otimes w - w \otimes v.$$

L'idéal J est à nouveau homogène, donc se décompose en $J = \bigoplus_d (J \cap T^d V)$, et on a

$$SV = \bigoplus S^d V, \quad S^d V = T^d V/(J \cap T^d V).$$

En particulier, $S^0 V = \mathbf{K}$ et $S^1 V = V$, d'où l'injection canonique $V \hookrightarrow SV$. Le produit dans l'algèbre symétrique est noté sans signe particulier : par exemple $v_1 v_2 = v_2 v_1$.

Une application linéaire $f : V \to W$ donne une application linéaire $Sf : SV \to SW$, avec $Sf = \bigoplus_d S^d f$. On a bien sûr la propriété $S(f \circ g) = Sf \circ Sg$.

Les propriétés de $S^d V$ sont les suivantes.

1° L'application d-linéaire

$$\begin{array}{rcl} \mathrm{V}^d & \longrightarrow & \mathrm{S}^d\mathrm{V} \\ (v_1,\dots,v_d) & \longmapsto & v_1\cdots v_d \end{array}$$

est symétrique [6] et elle est universelle pour cette propriété ; en particulier $(\mathrm{S}^d\mathrm{V})^*$ est l'espace vectoriel des formes d-linéaires symétriques sur V.

2° Si $(e_1,\dots,e_n)$ est une base de V, une base de $\mathrm{S}^d\mathrm{V}$ est donnée par les $(e_{i_1}^{k_1}\cdots e_{i_r}^{k_r})$ pour tout r-uplet $1\leqslant i_1<\cdots<i_r\leqslant n$ et entiers k_i tels que $k_1+\cdots+k_r=d$; on a donc

$$\dim(\mathrm{S}^d\mathrm{V})=\binom{n+d-1}{n-1}.$$

En particulier, si $\mathrm{V}\neq 0$, l'espace vectoriel SV est toujours de dimension infinie, contrairement à $\bigwedge\mathrm{V}$.

3° Si V est de dimension n, l'algèbre SV est isomorphe à l'algèbre de polynômes $\mathbf{K}[\mathrm{X}_1,\dots,\mathrm{X}_n]$: si $(e_1,\dots,e_n)$ est une base de V, un isomorphisme est obtenu en envoyant e_i sur X_i.

4° Si $\mathrm{car}(\mathbf{K})=0$, on peut réaliser $\mathrm{S}^d\mathrm{V}$ à l'intérieur de $\mathrm{T}^d\mathrm{V}$ comme le sous-espace $s^d\mathrm{V}$ des *tenseurs symétriques*, c'est-à-dire des tenseurs t satisfaisant $\bar{\sigma}(t)=t$ pour tout $\sigma\in\mathfrak{S}_n$; en effet, on dispose alors d'une *symétrisation*

$$\begin{array}{rcl} q:\mathrm{T}^d\mathrm{V} & \longrightarrow & \mathrm{T}^d\mathrm{V} \\ v_1\otimes\cdots\otimes v_d & \longmapsto & \dfrac{1}{d!}\displaystyle\sum_{\sigma\in\mathfrak{S}_d} v_{\sigma(1)}\otimes\cdots\otimes v_{\sigma(d)} \end{array}$$

qui est d'image $s^d\mathrm{V}$ et de noyau $\mathrm{J}\cap\mathrm{T}^d\mathrm{V}$. Elle induit ainsi un isomorphisme $s^d\mathrm{V}\simeq\mathrm{S}^d\mathrm{V}$.

5° Pour $d=2$, si $\mathrm{car}(\mathbf{K})\neq 2$, on peut toujours écrire

$$v\otimes w=\frac{1}{2}(v\otimes w-w\otimes v)+\frac{1}{2}(v\otimes w+w\otimes v)=p(v\otimes w)+q(v\otimes w),$$

donc on obtient une décomposition de tout 2-tenseur en somme d'un tenseur antisymétrique et d'un tenseur symétrique :

$$\mathrm{T}^2\mathrm{V}=a^2\mathrm{V}\oplus s^2\mathrm{V}. \tag{41}$$

***Remarque 5.1* (Foncteurs de Schur).** — Supposons $\mathrm{car}(\mathbf{K})=0$. La décomposition (41) n'est plus valable pour $\mathrm{T}^d\mathrm{V}$ lorsque $d\geqslant 3$; on a bien une inclusion [7]

$$\mathrm{T}^d\mathrm{V}\supseteq a^d\mathrm{V}\oplus s^d\mathrm{V}$$

6. Une application d-linéaire f est *symétrique* si $f(v_{\sigma(1)},\dots,v_{\sigma(d)})=f(v_1,\dots,v_d)$ pour tout $\sigma\in\mathfrak{S}_d$. De nouveau, on sait par définition de J que cette propriété est vraie lorsque σ est une transposition $(i\ i+1)$ et il faut un petit argument pour l'étendre à toutes les permutations.

7. La somme est bien directe puisque le projecteur p est l'identité sur $a^d\mathrm{V}$ mais est nul sur $s^d\mathrm{V}$.

mais elle est stricte pour $d \geqslant 3$. Il suffit pour s'en convaincre de calculer les dimensions pour $d = 3$:

$$\dim(\mathrm{T}^3\mathrm{V}) = n^3 > \dim(a^3\mathrm{V}) + \dim(s^3\mathrm{V}) = \binom{n}{3} + \binom{n+2}{3} = \frac{n(n-1)(n-2)}{6} + \frac{n(n+1)(n+2)}{6}.$$

Le bout manquant est un sous-espace vectoriel de $\mathrm{T}^3\mathrm{V}$ de dimension $2\frac{n(n^2-1)}{3}$. Il est somme directe de deux copies d'un espace vectoriel canonique noté $\mathbf{S}_{(2,1)}\mathrm{V}$ (voir exerc. 5.2).

En général, on a une décomposition canonique

$$\mathrm{V}^{\otimes d} = \bigoplus_{\substack{\lambda_1 \geqslant \cdots \geqslant \lambda_n \geqslant 0 \\ \lambda_1 + \cdots + \lambda_n = d}} \left(\mathbf{S}_{(\lambda_1,\ldots,\lambda_n)}\mathrm{V}\right)^{m_\lambda}$$

où les m_λ sont des entiers strictement positifs et les $\mathbf{S}_{(\lambda_1,\ldots,\lambda_n)}$ sont les *foncteurs* [8] *de Schur,* avec (on ne note pas les λ_i nuls)

- $\mathbf{S}_{\underbrace{(1,\ldots,1)}_{d \text{ fois}}}\mathrm{V} \simeq a^d\mathrm{V}$;
- $\mathbf{S}_{(d)}\mathrm{V} \simeq s^d\mathrm{V}$;
- $\mathbf{S}_{(\lambda_1,\ldots,\lambda_n)}\mathrm{V}$ est une représentation irréductible de GL(V) (*cf.* déf. IV.1.3) de dimension

$$\prod_{1 \leqslant i < j \leqslant n} \frac{\lambda_i - \lambda_j + j - i}{j - i}.$$

Exercice 5.2. — Soit **K** corps de caractéristique nulle et soit V un **K**-espace vectoriel.
a) Montrer que le sous-espace vectoriel S de $\mathrm{V}^{\otimes 3}$ engendré par les $v_1 \otimes v_2 \otimes v_3 + v_2 \otimes v_1 \otimes v_3 - v_1 \otimes v_3 \otimes v_2 - v_2 \otimes v_3 \otimes v_1$ est à la fois dans le noyau de l'antisymétrisation p et dans celui de la symétrisation q.
b) En déduire $\mathrm{V}^{\otimes 3} \supseteq a^3\mathrm{V} \oplus s^3\mathrm{V} \oplus \mathrm{S}$.
c) Montrer que S est dans l'image de l'application linéaire injective $f : \mathrm{V} \otimes \bigwedge^2\mathrm{V} \to \mathrm{V}^{\otimes 3}$ donnée par $v_1 \otimes (v_2 \wedge v_3) \mapsto v_1 \otimes v_2 \otimes v_3 - v_1 \otimes v_3 \otimes v_2$.
d) On considère l'application linéaire $g : \mathrm{V} \otimes \bigwedge^2\mathrm{V} \to \bigwedge^3\mathrm{V}$ donnée par la structure d'algèbre de $\bigwedge\mathrm{V}$ (avec le fait que $\bigwedge^1\mathrm{V} = \mathrm{V}$). Montrer que g est surjective et que $\mathrm{S} = f(\ker(g))$. En déduire la dimension de S.
e) Soit S' le sous-espace vectoriel de $\mathrm{V}^{\otimes 3}$ engendré par les $v_1 \otimes v_2 \otimes v_3 + v_2 \otimes v_1 \otimes v_3 - v_3 \otimes v_2 \otimes v_1 - v_3 \otimes v_1 \otimes v_2$. Montrer que S' est isomorphe à S et que

$$\mathrm{V}^{\otimes 3} = a^3\mathrm{V} \oplus s^3\mathrm{V} \oplus \mathrm{S} \oplus \mathrm{S}' \simeq \bigwedge^3\mathrm{V} \oplus \mathrm{S}^3\mathrm{V} \oplus \mathrm{S}^2.$$

Les espaces S et S' sont des copies de $\mathbf{S}_{(2,1)}\mathrm{V}$, qui est donc isomorphe au noyau de $g : \mathrm{V} \otimes \bigwedge^2\mathrm{V} \to \bigwedge^3\mathrm{V}$.

Remarque 5.3. — Soit V un **C**-espace vectoriel de dimension finie n. Tout élément de $\mathrm{S}^d\mathrm{V}$ peut s'écrire comme somme de tenseurs décomposables du type $v \cdots v$ (*cf.* rem. 2.1). On peut se poser la question de savoir le nombre maximal de tenseurs décomposables dont on a besoin (« problème de Waring »).

8. La fonctorialité signifie que pour tout $\lambda = (\lambda_1, \ldots, \lambda_n)$ et toute application linéaire $f : \mathrm{V} \to \mathrm{W}$, il existe une application linéaire canoniquement définie $\mathbf{S}_\lambda(f) : \mathbf{S}_\lambda(\mathrm{V}) \to \mathbf{S}_\lambda(\mathrm{W})$, avec $\mathbf{S}_\lambda(\mathrm{Id}) = \mathrm{Id}$ et $\mathbf{S}_\lambda(f \circ g) = \mathbf{S}_\lambda(f) \circ \mathbf{S}_\lambda(g)$ (*cf.* prop. 3.2 et § 5).

Lorsque $d = 2$, on peut interpréter un élément de S^2V comme une forme bilinéaire symétrique sur V^* ; une telle décomposition consiste alors à écrire la forme quadratique associée comme somme de carrés de formes linéaires. La réduction de Gauss nous dit qu'une forme quadratique est somme d'au plus n tels carrés. Dans ce cas, la réponse à la question est donc n.

Pour d et n quelconques, on connaît la réponse à cette importante question lorsque le tenseur à décomposer est « général » (travaux de Alexander et Hirschowitz dans les années 90) mais pas pour tous les tenseurs.

6. Algèbre de Clifford et groupe spinoriel

Dans le § II.11, on avait utilisé **H**, le corps des quaternions (une **R**-algèbre de dimension 4) et le groupe de ses éléments de norme 1 (isomorphe à $SU_2(\mathbf{C})$) agissant par conjugaison, pour construire un morphisme de groupes surjectif de $SU_2(\mathbf{C})$ vers le groupe orthogonal $O_3(\mathbf{R})$ pour la forme quadratique définie positive standard sur $\mathbf{R}^3$.

Cette construction est un cas particulier d'une construction très générale, celle de l'algèbre de Clifford d'un espace vectoriel muni d'une forme quadratique, qui nous permettra de définir le groupe et la norme spinoriels déjà mentionnés dans la rem. II.11.4 et le § II.8.5.

6.1. Algèbre de Clifford d'une forme quadratique. — On part maintenant d'un espace vectoriel V sur un corps **K** de caractéristique différente de 2, muni d'une forme quadratique f. On cherche à résoudre le problème universel pour les morphismes $g : V \to A$, où A est une **K**-algèbre avec unité, qui vérifient $g(v)^2 = f(v)1_A$ pour tout $v \in V$. L'algèbre solution de ce problème est l'*algèbre de Clifford* $C(V, f)$ (notée parfois simplement $C(f)$), obtenue comme le quotient

$$C(V, f) = TV/I(f),$$

où $I(f)$ est l'idéal bilatère de TV engendré par les éléments du type $v \otimes v - f(v)$. Contrairement aux cas des algèbres extérieure et symétrique, l'idéal $I(f)$ n'est pas engendré par des éléments homogènes ($v \otimes v$ est de degré 2 et $f(v)$ est de degré 0), donc $I(f)$ n'est pas une algèbre graduée au sens précédent [9]. On peut néanmoins la décomposer en

$$C(f) = C(f)^+ \oplus C(f)^-,$$

où $C(f)^+$ est l'ensemble des images des éléments de TV de degré pair et $C(f)^-$ l'ensemble des images des éléments de TV de degré impair. La multiplication par un élément de $C(f)^+$ laisse stable ces deux morceaux, tandis que la multiplication par un élément de $C(f)^-$ les échange. En particulier, $C(f)^+$ est une sous-algèbre de $C(f)$.

On a dans $C(f)$, pour tous $v, w \in V$, les égalités

$$v \cdot v = f(v) \tag{42}$$

$$v \cdot w + w \cdot v = 2B(v, w), \tag{43}$$

où B est la forme bilinéaire associée à f.

Si $(e_1, \ldots, e_n)$ est une base de V, on peut montrer que les produits $e_{i_1} \cdot \ldots \cdot e_{i_k}$, avec $k \geqslant 0$ et $1 \leqslant i_1 < \cdots < i_k \leqslant n$ forment une base du **K**-espace vectoriel $C(f)$, qui est donc de

9. Sauf si $f = 0$, auquel cas $C(f)$ est simplement $\bigwedge V$.

dimension 2^d. Un tel produit est dans $\mathrm{C}(f)^+$ ou $\mathrm{C}(f)^-$ selon que k est pair ou impair, donc chacun des morceaux est de dimension 2^{n-1}. En particulier, s'il est de dimension finie, V s'injecte canoniquement dans $\mathrm{C}(f)^-$.

Exemples 6.1. — 1° Considérons l'espace vectoriel $\mathrm{V} = \mathbf{R}$ et sa base canonique $(e_1 = 1)$, muni de la forme quadratique $f(x) = -x^2$. Une base de $\mathrm{C}(f)$ est alors $(1, e_1)$ avec les relations $e_1^2 = f(e_1) = -1$. L'algèbre $\mathrm{C}(f)$ est donc isomorphe au corps $\mathbf{C}$ des nombres complexes.

2° Considérons l'espace vectoriel $\mathrm{V} = \mathbf{R}^2$ et sa base canonique (e_1, e_2), muni de la forme quadratique $f(x_1, x_2) = -x_1^2 - x_2^2$. Une base de $\mathrm{C}(f)$ est alors $(1, e_1, e_2, e_1 e_2)$ avec les relations

$$e_1^2 = f(e_1) = -1 \quad , \quad e_2^2 = f(e_2) = -1 \quad , \quad e_1 \cdot e_2 = -e_2 \cdot e_1.$$

Si on pose $\mathrm{I} := e_1$, $\mathrm{J} := e_2$ et $\mathrm{K} := e_1 \cdot e_2 = \mathrm{IJ}$, on vérifie les relations des quaternions (§ II.11)

$$\mathrm{IJK} = \mathrm{K}^2 = e_1 \cdot e_2 \cdot e_1 \cdot e_2 = -e_1^2 \cdot e_2^2 = -1.$$

L'algèbre $\mathrm{C}(f)$ est donc isomorphe au corps non commutatif $\mathbf{H}$ des quaternions.

Exercice 6.2. — Déterminer la $\mathbf{R}$-algèbre $\mathrm{C}(\mathrm{V}, f)$ dans les cas suivants :
– $\mathrm{V} = \mathbf{R}$ et $f(x) = x^2$;
– $\mathrm{V} = \mathbf{R}^2$ et $f(x_1, x_2) = x_1^2 + x_2^2$;
– $\mathrm{V} = \mathbf{R}^2$ et $f(x_1, x_2) = x_1^2 - x_2^2$.

Exercice 6.3. — Pour tous $s, t \geqslant 0$, on note $\mathrm{C}(s, t)$ l'algèbre de Clifford de la forme quadratique de signature (s, t) sur $\mathrm{V} = \mathbf{R}^{s+t}$.
a) Pour tout $n \geqslant 0$, montrer qu'on a un isomorphisme de $\mathbf{R}$-algèbres

$$\mathrm{C}(0, n+2) \simeq \mathrm{C}(n, 0) \otimes_{\mathbf{R}} \mathrm{C}(0, 2)$$

(*Indication :* si $(e_1, \ldots, e_{n+2})$ est une base orthonormale de $\mathbf{R}^{n+2}$, $(e'_1, \ldots, e'_n)$ une base orthonormale de $\mathbf{R}^n$ et (e''_1, e''_2) une base orthonormale de $\mathbf{R}^2$, on pourra considérer l'application linéaire $\mathbf{R}^{n+2} \to \mathrm{C}(n, 0) \otimes_{\mathbf{R}} \mathrm{C}(0, 2)$ qui envoie e_i sur $e'_i \otimes e''_1 \cdot e''_2$ si $i \in \{1, \ldots, n\}$ et sur $1 \otimes e''_{i-n}$ si $i \in \{n+1, n+2\}$).
b) Pour tous $s, t \geqslant 0$, montrer qu'on a un isomorphisme de $\mathbf{R}$-algèbres

$$\mathrm{C}(s+1, t+1) \simeq \mathrm{C}(s, t) \otimes_{\mathbf{R}} \mathrm{C}(1, 1).$$

c) Pour tout $n \geqslant 0$, montrer qu'on a des isomorphismes de $\mathbf{R}$-algèbres

$$\begin{aligned} \mathrm{C}(0, n+8) &\simeq \mathrm{C}(0, n) \otimes_{\mathbf{R}} \mathrm{C}(0, 8) \\ \mathrm{C}(n+8, 0) &\simeq \mathrm{C}(n, 0) \otimes_{\mathbf{R}} \mathrm{C}(8, 0) \end{aligned}$$

et

$$\mathrm{C}(0, 8) \simeq \mathrm{C}(8, 0) \simeq \mathscr{M}_{16}(\mathbf{R})$$

(*Indication :* on pourra utiliser les exerc. 6.2 et 1.9).

6.2. Groupe de Clifford. — On note $\alpha : C(f) \to C(f)$ l'involution qui vaut Id sur $C(f)^+$ et $-\mathrm{Id}$ sur $C(f)^-$. Elle vérifie $\alpha(x\cdot y) = \alpha(x)\cdot\alpha(y)$, pour tous $x, y \in C(f)$.

Pour tout x dans le groupe des unités $C(f)^\times$, on considère l'endomorphisme

$$\rho_x : z \mapsto \alpha(x)\cdot z\cdot x^{-1}$$

de $C(f)$. On a $\rho_1 = \mathrm{Id}_{C(f)}$ et, pour tous $x, y \in C(f)^\times$,

$$\rho_{x\cdot y}(z) = \alpha(x\cdot y)\cdot z\cdot(x\cdot y)^{-1} = \alpha(x)\cdot\alpha(y)\cdot z\cdot y^{-1}x^{-1} = \rho_x\circ\rho_y(z).$$

L'endomorphisme ρ_x est donc inversible (d'inverse $\rho_{x^{-1}}$) et

$$\Gamma(f) := \{x \in C(f)^\times \mid \forall v \in V \quad \alpha(x)\cdot v\cdot x^{-1} \in V\}.$$

est un sous-groupe de $C(f)^\times$ stable par α appelé *groupe de Clifford* de f. On a par construction un morphisme de groupes

$$\begin{array}{rcl} \rho : \Gamma(f) & \longrightarrow & \mathrm{GL}(V) \\ x & \longmapsto & \rho_x. \end{array}$$

Remarquons que tout élément non isotrope v de V (c'est-à-dire qui vérifie $f(v) \neq 0$) est inversible dans $C(f)$, avec $v^{-1} = \frac{1}{f(v)}v$.

Proposition 6.4. *— Tout $v \in V$ non isotrope est dans $\Gamma(f)$ et ρ_v est la réflexion par rapport à l'hyperplan $v^\perp$ (ex. III.5.2).*

Démonstration. — Si B est la forme bilinéaire associée à f et que s_v est la réflexion en question, on a (ex. III.5.2)

$$\forall w \in V \qquad s_v(w) = w - 2\frac{B(v,w)}{B(v,v)}v.$$

Comme V est un sous-espace vectoriel de $C(f)$, on peut voir cette égalité entre éléments de V comme une égalité dans $C(f)$. Elle s'écrit alors, en utilisant (42) et (43),

$$\forall w \in V \qquad s_v(w) = w - (v\cdot w + w\cdot v)\cdot v^{-2}\cdot v = -v\cdot w\cdot v^{-1} = \alpha(v)\cdot w\cdot v^{-1},$$

puisque α est $-\mathrm{Id}$ sur V. □

Lemme 6.5. *— Si f est non dégénérée et V de dimension finie, le noyau de ρ est $\mathbf{K}^\times$.*

Démonstration. — Soit x un élément du noyau de ρ, qu'on écrit $x = x^+ + x^-$, avec $x^\pm \in C(f)^\pm$. On a alors $\alpha(x)\cdot v = v\cdot x$ pour tout $v \in V$, d'où $\pm x^\pm\cdot v = v\cdot x^\pm$. Choisissons une base orthogonale $(e_1,\dots,e_n)$ de V. On a alors, par (43),

$$e_i\cdot e_j = -e_j\cdot e_i \quad \text{si } i \neq j.$$

On rappelle que les $e_{i_1}\cdot\ldots\cdot e_{i_k}$, avec $1 \leqslant i_1 < \cdots < i_k \leqslant n$ forment une base du $\mathbf{K}$-espace vectoriel $C(f)$. On peut donc écrire $x^+ = x_0^+ + e_1\cdot x_1^+$, où ni $x_0^+ \in C(f)^+$, ni $x_1^+ \in C(f)^-$, ne contient de facteur e_1 dans sa décomposition sur cette base. On a alors

$$e_1\cdot x_0^+ + f(e_1)x_1^+ = e_1\cdot x^+ = x^+\cdot e_1 = x_0^+\cdot e_1 + e_1\cdot x_1^+\cdot e_1 = e_1\cdot x_0^+ - f(e_1)x_1^+.$$

Puisque f est non dégénérée, on a $f(e_1) \neq 0$, d'où on déduit $x_1^+ = 0$, c'est-à-dire que x^+ ne contient aucun facteur e_1. On appliquant ce raisonnement avec les autres e_i, on voit que x^+ ne contient aucun facteur e_i, c'est-à-dire $x^+ \in \mathbf{K}$.

Si on écrit de la même façon $x^- = x_0^- + e_1 \cdot x_1^-$, on obtient $x_1^- = 0$, c'est-à-dire $x^- \in \mathbf{K}$. Mais on a alors $x^- \in \mathbf{K} \cap \mathrm{C}(f)^- = \{0\}$.

Tout cela montre $x = x^+ \in \mathbf{K} \cap \mathrm{C}(f)^\times = \mathbf{K}^\times$. □

6.3. Norme et groupe spinoriels. — On définit une deuxième involution $t : \mathrm{C}(f) \to \mathrm{C}(f)$ de la façon suivante. Soit $\mathrm{C}(f)^0$ l'*algèbre opposée* à $\mathrm{C}(f)$, c'est-à-dire le même espace vectoriel, mais où la multiplication $x \overset{0}{\cdot} y$ est donnée par $y \cdot x$. Comme le problème universel dont l'application linéaire $\mathrm{V} \to \mathrm{C}(f)$ est la solution a une unique solution à isomorphisme près, il existe un isomorphisme d'algèbres $t : \mathrm{C}(f) \to \mathrm{C}(f)^0$. Cet isomorphisme vérifie donc $t(x \cdot y) = t(y) \cdot t(x)$, pour tous $x, y \in \mathrm{C}(f)$. De nouveau, par unicité, t est une involution.

Lorsque V est de dimension finie, de base $(e_1, \ldots, e_n)$, on peut décrire l'action de t sur une base de $\mathrm{C}(f)$:

$$t(e_{i_1} \cdot \ldots \cdot e_{i_k}) = e_{i_k} \cdot \ldots \cdot e_{i_1}.$$

On remarque que $t \circ \alpha = \alpha \circ t$. Il s'ensuite que l'application

$$x \mapsto \bar{x} := t \circ \alpha(x) = \alpha \circ t(x)$$

est une involution de $\mathrm{C}(f)$ qui commute avec α et t et vérifie $\overline{x \cdot y} = \bar{y} \cdot \bar{x}$. On définit enfin la *norme spinorielle*

$$\begin{array}{rcl} \mathrm{N} : \mathrm{C}(f) & \longrightarrow & \mathrm{C}(f) \\ x & \longmapsto & x \cdot \bar{x}. \end{array}$$

On a en particulier

$$\forall v \in \mathrm{V} \qquad \mathrm{N}(v) = -f(v). \tag{44}$$

Proposition 6.6. *— Supposons f non dégénérée et* V *de dimension finie. Par restriction, la norme spinorielle définit un morphisme de groupes* $\mathrm{N} : \Gamma(f) \to \mathbf{K}^\times$.

Démonstration. — Si $x \in \Gamma(f)$, nous allons montrer que $\mathrm{N}(x)$ est dans le noyau de ρ. Appliquons t, qui renverse l'ordre des produits et qui est l'identité sur V, à la relation $\alpha(x) \cdot v \cdot x^{-1} \in \mathrm{V}$; on obtient

$$\alpha(x) \cdot v \cdot x^{-1} = t(x^{-1}) \cdot v \cdot t(\alpha(x)),$$

d'où

$$v = t(x) \cdot \alpha(x) \cdot v \cdot x^{-1} \cdot \bar{x}^{-1} = \alpha(\bar{x} \cdot x) \cdot v \cdot (\bar{x} \cdot x)^{-1}.$$

Puisque $\bar{x} \in \mathrm{C}(f)^\times$, cela signifie $\bar{x} \cdot x \in \Gamma(f)$ et $\bar{x} \cdot x \in \ker(\rho)$, c'est-à-dire $\bar{x} \cdot x \in \mathbf{K}^\times$ par le lemme 6.5. De plus, on a $\bar{x} \in \Gamma(f)$ puisque $\Gamma(f)$ est un groupe. Appliquant ce résultat à $\bar{x}$, on obtient que $\bar{\bar{x}} \cdot \bar{x} = \mathrm{N}(x)$ est dans $\mathbf{K}^\times$.

Si $x, y \in \Gamma(f)$, on a

$$\mathrm{N}(xy) = x \cdot y \cdot \bar{y} \cdot \bar{x} = x \cdot \mathrm{N}(y) \cdot \bar{x} = x \cdot \bar{x} \mathrm{N}(y) = \mathrm{N}(x)\mathrm{N}(y),$$

où la troisième égalité a lieu puisque $\mathrm{N}(y)$ est dans $\mathbf{K}^\times$, donc commute avec tous les éléments de $\mathrm{C}(f)$. On a donc bien un morphisme de groupes. □

Proposition 6.7. *— Supposons f non dégénérée et* V *de dimension finie. L'image du morphisme de groupes* $\rho : \Gamma(f) \to \mathrm{GL}(\mathrm{V})$ *est le groupe orthogonal* $\mathrm{O}(\mathrm{V}, f)$.

Démonstration. — Soit $x \in \Gamma(f)$. Montrons tout d'abord que ρ_x est bien une isométrie, c'est-à-dire qu'on a $f(\rho_x(v)) = f(v)$ pour tout $v \in V$. On a, avec la prop. 6.6 et (44),

$$\begin{aligned} f(\rho_x(v)) &= -N(\rho_x(v)) = -\alpha(x)\cdot v\cdot x^{-1}\cdot\bar{x}^{-1}\cdot(-v)\cdot\alpha(\bar{x}) = -\alpha(x)\cdot v\cdot N(x^{-1})\cdot v\cdot\alpha(\bar{x}) \\ &= f(v)N(x^{-1})\alpha(N(x)) = f(v)N(x^{-1})N(x) = f(v). \end{aligned}$$

L'image de $\rho : \Gamma(f) \to GL(V)$ est donc contenue dans le groupe orthogonal $O(V, f)$.

Mais d'autre part, par la prop. 6.4, cette image contient toutes les réflexions. Comme celles-ci engendrent $O(V, f)$ (th. II.8.7), on a $\rho(\Gamma(f)) = O(V, f)$. □

Corollaire 6.8. — *Sous les mêmes hypothèses, on a un isomorphisme de groupes* $\hat{\rho} : \Gamma(f)/\mathbf{K}^\times \xrightarrow{\sim} O(V, f)$ *et la norme spinorielle induit un morphisme de groupes*

$$\theta : O(V, f) \to \mathbf{K}^\times/\mathbf{K}^{\times 2}$$

qui vérifie, pour tout $v \in V$ *non isotrope,* $\theta(s_v) = f(v)$.

Démonstration. — Le morphisme $\hat{\rho}$ est fourni par la factorisation canonique de ρ. L'image de $\mathbf{K}^\times \subseteq \Gamma(f)$ par la norme spinorielle $N : \Gamma(f) \to \mathbf{K}^\times$ est le sous-groupe $\mathbf{K}^{\times 2}$ des carrés non nuls. On a donc un morphisme induit $\hat{N} : \Gamma(f)/\mathbf{K}^\times \to \mathbf{K}^\times/\mathbf{K}^{\times 2}$. Il suffit de poser $\theta := \hat{N}\circ\hat{\rho}^{-1}$. □

6.4. Groupe Spin_n**.** — On se place ici dans le cas où $\mathbf{K} = \mathbf{R}$, $V = \mathbf{R}^n$ et f est (le carré de) la norme euclidienne usuelle :

$$f(x_1, \ldots, x_n) = x_1^2 + \cdots + x_n^2.$$

On pose alors

$$\mathrm{Spin}_n(\mathbf{R}) := \ker(N) \cap \Gamma(f) \cap C(f)^+ = \{x \in C(f)^+ \mid x\cdot\bar{x} = 1,\ x\cdot V\cdot x^{-1} \subseteq V\}$$

puisque α est l'identité sur $C(f)^+$. C'est un sous-groupe de $\Gamma(f)$.

Théorème 6.9. — *L'image du morphisme de groupes* $\rho|_{\mathrm{Spin}_n(\mathbf{R})} : \mathrm{Spin}_n(\mathbf{R}) \to O(V, f)$ *est le groupe* $SO(V, f)$ *et son noyau est* $\{\pm 1\}$.

Démonstration. — Vu le lemme 6.5, le noyau de la restriction de ρ à $\mathrm{Spin}_n(\mathbf{R})$ est l'intersection de $\mathbf{R}^\times$ avec $\ker(N)$. Mais sur $\mathbf{R}^\times$, la norme spinorielle est juste le carré, donc le noyau est $\{\pm 1\}$.

Soit $x \in \mathrm{Spin}_n(\mathbf{R})$. On décompose l'isométrie ρ_x en produit de réflexions $s_{v_1}\circ\cdots\circ s_{v_r}$, où on peut supposer les vecteurs $v_1, \ldots, v_r$ de V unitaires. On a alors (prop. 6.4) $s_{v_i} = \rho_{v_i}$, donc $\rho(x) = \rho(v_1\cdot\ldots\cdot v_r)$. Comme le noyau de ρ est $\mathbf{R}^\times$ (lemme 6.5), il existe $\lambda \in \mathbf{R}^\times$ tel que $x = \lambda v_1\cdot\ldots\cdot v_r$ dans $\Gamma(f)$. En prenant les normes spinorielles, on obtient (en utilisant la prop. 6.6 et (44))

$$1 = N(x) = \lambda^2 N(v_1\cdot\ldots\cdot v_r) = \lambda^2 N(v_1)\cdots N(v_r) = \lambda^2(-1)^r f(v_1)\cdots f(v_r) = \lambda^2(-1)^r.$$

Ceci n'est possible que si r est pair, ce qui entraîne

$$\det(\rho_x) = \det(s_{v_1})\cdots\det(s_{v_r}) = (-1)^r = 1.$$

Le groupe $\rho(\mathrm{Spin}_n(\mathbf{R}))$ est donc bien contenu dans $SO(V, f)$.

Inversement, tout élément u de $SO(V, f)$ se décompose en un produit de réflexions $s_{v_1}\circ\cdots\circ s_{v_r}$, avec $v_1, \ldots, v_r$ dans V de norme 1 et r pair. Comme $s_{v_i} = \rho(v_i)$, on a $u = \rho(v_1\cdot\ldots\cdot v_r)$

avec $v_1 \cdot \ldots \cdot v_r \in \ker(\mathrm{N}) \cap \Gamma(f) \cap \mathrm{C}(f)^+ = \mathrm{Spin}_n(\mathbf{R})$. L'image $\rho(\mathrm{Spin}_n(\mathbf{R}))$ est donc égale à $\mathrm{SO}(\mathrm{V}, f)$. □

Les groupes $\mathrm{Spin}_n(\mathbf{R})$ ont déjà été identifiés pour n petit (rem. II.11.4) : on a $\mathrm{Spin}_2(\mathbf{R}) \simeq \mathrm{U}_1(\mathbf{C})$, $\mathrm{Spin}_3(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C})$, $\mathrm{Spin}_4(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C})$ et $\mathrm{Spin}_6(\mathbf{R}) \simeq \mathrm{SU}_4(\mathbf{C})$.

Exercice 6.10. — Montrer que $\mathrm{Spin}_n(\mathbf{R})$ est connexe pour $n \geqslant 2$ (*Indication :* on pourra utiliser le th. 8.7 et, pour tous $v, w \in \mathrm{V}$ unitaires et orthogonaux, le chemin $t \mapsto (v\cos t - w\sin t)(v\sin t + w\cos t)$, pour $t \in [0, \pi/2]$, dans $\mathrm{Spin}_n(\mathbf{R})$).

Remarque 6.11. — Si f est une forme quadratique de signature (s, t) sur $\mathbf{R}^{s+t}$, on pose de la même façon

$$\mathrm{Spin}_{s,t}(\mathbf{R}) := \ker(\mathrm{N}) \cap \Gamma(f) \cap \mathrm{C}(f)^+.$$

Une preuve analogue à celle du th. 6.9 montre que le morphisme ρ induit par restriction un morphisme surjectif $\mathrm{Spin}_{s,t}(\mathbf{R}) \to \mathrm{SO}_{s,t}(\mathbf{R})$ de noyau $\{\pm 1\}$. Lorsque $st > 0$, ces groupes ne sont pas connexes (ex. II.8.12.2°) et on définit $\mathrm{Spin}'_{s,t}(\mathbf{R})$ comme l'image inverse du groupe connexe $\mathrm{SO}'_{s,t}(\mathbf{R})$.

CHAPITRE IV

REPRÉSENTATIONS DES GROUPES

1. Représentations

Soit G un groupe et soit V un **K**-espace vectoriel. Une *représentation linéaire* de G dans V est un morphisme de groupes

$$\rho : G \longrightarrow GL(V).$$

En d'autres termes, on représente les éléments de G comme des automorphismes de V ou plus simplement, si V est de dimension finie et qu'on en choisit une base, comme des matrices (inversibles).

On notera la représentation (V,ρ), ou simplement, en l'absence d'ambiguïté, ρ ou V. L'action d'un élément $g \in G$ sur V sera souvent notée $g \cdot v$ $(= \rho(g)(v))$. C'est une action du groupe G sur V au sens de la déf. du § I.2.1.

Exemples 1.1. — 1° Une représentation de G dans un espace vectoriel de dimension 1 est un morphisme $\rho : G \to \mathbf{K}^\times$. Si G est fini, l'image est un groupe cyclique (exerc. I.1.29).

2° Si G est défini comme un sous-groupe de GL(V) (ce qui est le cas de tous les groupes classiques), l'inclusion $G \hookrightarrow GL(V)$ est appelée la *représentation standard*.

3° Si $(e_1,\dots,e_n)$ est une base de $\mathbf{K}^n$, on obtient une représentation de $\mathfrak{S}_n$ dans $\mathbf{K}^n$ en posant $\rho(\sigma)(e_i) = e_{\sigma(i)}$. Une telle représentation est appelée *représentation de permutation*. Les $\rho(\sigma)$ sont des matrices de permutation.

4° Si G est un groupe fini, on peut composer le morphisme de groupes de Cayley (ex. I.2.3)

$$\begin{array}{ccc} G & \hookrightarrow & \mathrm{Bij}(G) \\ g & \mapsto & (x \mapsto gx) \end{array}$$

avec la construction du 3° ci-dessus pour obtenir une représentation

$$\rho_R : G \to \mathrm{Bij}(G) \to GL(\mathbf{K}^G),$$

où $\mathbf{K}^G$ est l'espace vectoriel des fonctions de G dans **K**. Si $\varepsilon_h : G \to \mathbf{K}$ est la fonction caractéristique d'un élément h de G, la famille $(\varepsilon_h)_{h\in G}$ forme une base de $\mathbf{K}^G$. On a $\rho_R(g)(\varepsilon_h) = \varepsilon_{gh}$ et, pour tout $f \in \mathbf{K}^G$, on a $\rho_R(g)(f) : g' \mapsto f(g^{-1}g')$ pour tout $g' \in G$.

Cette représentation s'appelle la *représentation régulière* de G.

1.1. Vocabulaire et propriétés. — Soit (V,ρ) une représentation de G.

La *dimension* (on dit aussi le *degré*) de la représentation est $\dim(V)$.

Une *sous-représentation* est un sous-espace vectoriel $W \subseteq V$ stable sous l'action de G ; on parle de sous-espace G-invariant. Dans ce cas, on a des représentations induites sur W et sur le quotient V/W.

Exemples 1.2. — 1° Le sous-espace vectoriel

$$V^G = \{v \in V \mid \forall g \in G \quad g \cdot v = v\}$$

des vecteurs fixes sous G est un sous-espace G-invariant : si $h \in G$ et $v \in V^G$, on a pour tout $g \in G$

$$g \cdot (h \cdot v) = g \cdot v = v = h \cdot v,$$

donc $h \cdot v \in V^G$.

2° Si $V = \mathbf{K}^n$ est la représentation de permutation du groupe $\mathfrak{S}_n$, l'hyperplan

$$V_0 = \left\{(x_1,\dots,x_n) \in V \,\middle|\, \sum_{i=1}^{n} x_i = 0\right\}$$

est une sous-représentation de V, ainsi que la droite

$$V_1 = \mathbf{K}(1,\dots,1)$$

qui en est un supplémentaire si et seulement si $\mathrm{car}(\mathbf{K}) \nmid n$

Un *morphisme* entre des représentations (V,ρ_V) et (W,ρ_W) d'un groupe G est une application linéaire $u : V \to W$ telle que

$$\forall g \in G \qquad u \circ \rho_V(g) = \rho_W(g) \circ u.$$

Dans ce cas, $\ker(u)$ et $\mathrm{im}(u)$ sont des sous-représentations de V et W, et u induit un isomorphisme de représentations

$$V/\ker(u) \xrightarrow{\sim} \mathrm{im}(u).$$

L'espace vectoriel des morphismes entre les représentations V et W est noté $\mathrm{Hom}_G(V,W)$, ou $\mathrm{Hom}(\rho_V,\rho_W)$. Des représentations ρ_V et ρ_W de dimension finie d'un groupe G sont isomorphes si et seulement si il existe une base de V et une base de W dans lesquelles, pour tout $g \in G$, les matrices de $\rho_V(g)$ et de $\rho_W(g)$ sont les mêmes.

Si V et W sont des représentations de G, on peut former les représentations suivantes :

- $V \oplus W$ pour $\rho(g) = (\rho_V(g),\rho_W(g))$;
- $V \otimes W$ pour $\rho(g) = \rho_V(g) \otimes \rho_W(g)$;
- V^* pour $\rho^*(g) = {}^t\rho(g^{-1})$;
- $\mathrm{Hom}_{\mathbf{K}}(V,W) = V^* \otimes W$ pour $\rho(g)(u) = \rho_W(g) \circ u \circ \rho_V(g)^{-1}$; en particulier l'espace des morphismes de représentations de V vers W est

$$\mathrm{Hom}_G(V,W) = \mathrm{Hom}_{\mathbf{K}}(V,W)^G;$$

- T^dV, $\bigwedge^d V$, S^dV sont aussi des représentations de G (on associe à $g \in G$ les endomorphismes $(\rho_V(g))^{\otimes d}$, $\bigwedge^d(\rho_V(g))$, et $S^d(\rho_V(g))$). Si $\mathrm{car}(\mathbf{K}) \neq 2$, on a par (41) un isomorphisme de représentations

$$V \otimes V \simeq \bigwedge^2 V \oplus S^2 V. \tag{45}$$

1.2. Représentations irréductibles. —

Définition 1.3. — Une représentation V est *irréductible* si elle est non nulle et que ses seules sous-représentations sont 0 et V.

Toute représentation de dimension 1 est bien sûr irréductible.

Exemples 1.4. — 1° Si G est abélien et que $\mathbf{K}$ est algébriquement clos, les seules représentations irréductibles V de dimension finie de G sont de dimension 1. Soit $g \in G$ et soit $W \subseteq V$ un sous-espace propre (non nul) de $\rho(g)$, pour une valeur propre $\lambda \in \mathbf{K}$. On a, puisque G est abélien,

$$\forall h \in G\ \forall x \in W \qquad \rho(g)(\rho(h)(x)) = \rho(h)(\rho(g)(x)) = \rho(h)(\lambda x) = \lambda\rho(h)(x),$$

donc $\rho(h)(x) \in W$. Le sous-espace vectoriel W de V est donc stable par tous les $\rho(h)$: c'est une sous-représentation non nulle de V. Comme V est irréductible, elle est égale à V. Ceci entraîne que tous les $\rho(g)$ sont des homothéties. Toute droite $D \subseteq V$ est alors une sous-représentation, donc D = V.

Les représentations de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{C}$ sont données par l'image d'un générateur, qui doit être une racine n-ième de l'unité dans $\mathbf{C}$. On obtient ainsi les n représentations irréductibles $\rho_0, \ldots, \rho_{n-1}$ de $\mathbf{Z}/n\mathbf{Z}$, données par

$$\forall k \in \mathbf{Z}/n\mathbf{Z} \qquad \rho_j(k) = \exp\left(\frac{2kj\pi i}{n}\right).$$

Notons que tout cela n'est plus vrai lorsque $\mathbf{K} = \mathbf{R}$: la représentation de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{R}^2$ qui fait correspondre à $k \in \mathbf{Z}/n\mathbf{Z}$ la rotation d'angle $2k\pi/n$ est irréductible lorsque $n \geqslant 3$ puisqu'aucune droite n'est laissée stable par toutes ces rotations.

2° Pour $n \geqslant 3$, la représentation standard du groupe diédral D_n dans $\mathbf{R}^2$ (ou dans $\mathbf{C}^2$) est irréductible, puisqu'aucune droite n'est laissée stable par tous les éléments de D_n.

3° Si $\dim(V) \geqslant 2$, les représentations standard de SL(V), GL(V) et Sp(V) sont irréductibles puisque ces groupes opèrent transitivement sur $V - \{0\}$. C'est aussi le cas pour $O_n(\mathbf{R})$, qui opère transitivement sur la sphère unité $\mathbf{S}^{n-1}$, qui engendre l'espace vectoriel $\mathbf{R}^n$.

4° Soient $\rho_V : G \to GL(V)$ et $\rho_W : G \to GL(W)$ des représentations de G. Si W est de dimension 1, le groupe GL(W) s'indentifie canoniquement à $K^\times$ (ex. 1.1.1°) et la représentation $\rho_{V\otimes W} : G \to GL(V \otimes W)$ est isomorphe à la représentation

$$\begin{array}{ccc} G & \to & GL(V) \\ g & \mapsto & \rho_W(g)\rho_V(g), \end{array}$$

dont les sous-espaces G-invariants sont les mêmes que ceux de ρ_V. En particulier, $\rho_{V\otimes W}$ est irréductible si et seulement si ρ_V l'est. Ce n'est plus vrai en général si $\dim(W) > 1$ (même si ρ_W est irréductible ; *cf.* (45)).

Exercice 1.5. — Soit G un groupe fini.
a) Montrer que toute représentation irréductible de G est de dimension finie $\leqslant |G|$.
b) Supposons $\mathbf{K}$ algébriquement clos. Soit $A \leq G$ un sous-groupe abélien. Montrer que toute représentation irréductible de G est de dimension $\leqslant \frac{|G|}{|A|}$.

Exercice 1.6. — Soit V un espace vectoriel réel de dimension finie $n > 0$ et soit d un entier positif.
a) Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de V. Donner une base naturelle $\mathscr{B}_d$ de l'espace vectoriel $S^d V$.
b) Montrer qu'il existe des réels $\lambda_1, \dots, \lambda_n$ tels que, si P et Q sont des monômes unitaires de degré d en n variables, alors $P(\lambda_1, \dots, \lambda_n) = Q(\lambda_1, \dots, \lambda_n)$ si et seulement si $P = Q$.
c) Montrer que GL(V) agit naturellement sur l'espace vectoriel $S^d V$. On en déduit une représentation ρ_d de GL(V) dans $S^d V$.
d) Soit W un sous-espace vectoriel non nul de $S^d V$ stable par l'action de GL(V). Montrer qu'il existe un sous-ensemble de la base $\mathscr{B}_d$ qui engendre W (*Indication :* on pourra considérer l'automorphisme g de V qui envoie e_i sur $\lambda_i e_i$).
e) En déduire que la représentation ρ_d est irréductible.
f) Montrer qu'il existe, pour tout entier $d \in \{1, \dots, n\}$, une représentation irréductible de GL(V) dans $\bigwedge^d V$.
g) Que se passe-t-il si on remplace le corps **R** par un corps quelconque ?

1.3. Supplémentaire G-invariant. — Si W est une sous-représentation de V, il n'existe pas en général de supplémentaire G-invariant de W dans V.

Exemple 1.7. — Le groupe $G \leq GL_2(\mathbf{K})$ des matrices triangulaires supérieures se représente dans $V = \mathbf{K}^2$ par la représentation standard. La droite $W = \mathbf{K}e_1$ est une sous-représentation dépourvue de supplémentaire T-invariant.

Si **K** est le corps $\mathbf{F}_p$, on a ainsi un exemple avec un groupe G fini de cardinal $p(p-1)^2$.

Néanmoins, il y a quand même un résultat général d'existence de supplémentaire G-invariant pour certains groupes finis.

Théorème 1.8. — *Si* G *est un groupe fini tel que* $\mathrm{car}(\mathbf{K}) \nmid |G|$ *et que* V *est une représentation de* G*, tout sous-espace* G*-invariant de* V *admet un supplémentaire* G*-invariant.*

Corollaire 1.9. — *Soit* G *un groupe fini tel que* $\mathrm{car}(\mathbf{K}) \nmid |G|$. *Toute représentation de* G *de dimension finie est somme directe de représentations irréductibles.*

On va donner deux démonstrations du théorème, une première particulière à $\mathbf{K} = \mathbf{R}$ ou **C**, mais qui est valable aussi pour certains groupes infinis ; une seconde traitant tous les corps.

Première démonstration. — Supposons $\mathbf{K} = \mathbf{R}$ ou **C** et V de dimension finie. On choisit un produit scalaire ou un produit scalaire hermitien sur V, noté $\langle\ ,\ \rangle_0$. Puis on définit un autre produit scalaire par

$$\langle v, w\rangle = \frac{1}{|G|} \sum_{g \in G} \langle g \cdot v, g \cdot w\rangle_0. \tag{46}$$

Ce nouveau produit scalaire est G-invariant : pour tout $g \in G$, on a

$$\langle g \cdot v, g \cdot w\rangle = \langle v, w\rangle,$$

si bien que ρ est à valeurs dans O(V) ou U(V). En particulier, si W est un sous-espace G-invariant, $W^\perp$ est aussi G-invariant et fournit le supplémentaire voulu. □

L'ingrédient essentiel de cette démonstration consiste à fabriquer un produit scalaire G-invariant par moyennisation d'un produit scalaire quelconque donné. Si G est un groupe topologique compact, il est muni d'une mesure de probabilité G-invariante, la mesure de Haar : en remplaçant (46) par l'intégration sur le groupe, la démonstration s'étend à ce cas.

Seconde démonstration. — On applique encore un procédé de moyennisation. Choisissons un projecteur quelconque $p_0 : V \to V$ d'image un sous-espace G-invariant W et posons

$$p := \frac{1}{|G|} \sum_{g \in G} \rho(g) \circ p_0 \circ \rho(g)^{-1} \in \mathrm{End}(V). \tag{47}$$

Comme $\rho(g)$ préserve W, l'image de cet endomorphisme est contenue dans W. Si $v \in W$, on a $\rho(g)^{-1}(v) \in W$, donc $p_0 \circ \rho(g)^{-1}(v) = \rho(g)^{-1}(v)$ et $p(v) = v$. Ceci montre que p est un projecteur d'image W.

Montrons que son noyau est invariant par G. Pour tout $h \in G$, on a

$$\begin{aligned} \rho(h) \circ p \circ \rho(h)^{-1} &= \frac{1}{|G|} \sum_{g \in G} \rho(h) \circ \rho(g) \circ p_0 \circ \rho(g)^{-1} \circ \rho(h)^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \rho(hg) \circ p_0 \circ \rho(hg)^{-1} = p, \end{aligned}$$

c'est-à-dire $\rho(h) \circ p = p \circ \rho(h)$. En d'autres termes, p est un endomorphisme de la représentation ρ, donc son noyau (supplémentaire de W) est bien invariant par G. □

Lemme de Schur 1.10. — *Soit* G *un groupe, soient* (V, ρ_V) *et* (W, ρ_W) *des représentations irréductibles de* G *et soit* $u : V \to W$ *un morphisme de représentations.*

1° Soit u est nul, soit c'est un isomorphisme.

2° Si $\rho_V = \rho_W$, *que* V *est de dimension finie et que* **K** *est algébriquement clos, l'application u est une homothétie.*

Démonstration. — 1° Les sous-espaces $\ker(u)$ et $\mathrm{im}(u)$ sont G-invariants, donc triviaux.

2° Si λ est une valeur propre de u, alors $\ker(u - \lambda \mathrm{Id}_V)$ est G-invariant et non nul, donc égal à V, et u est une homothétie. □

Supposons G fini et $\mathrm{car}(\mathbf{K}) \nmid |G|$. Par le cor. 1.9, on peut décomposer la représentation régulière $\mathbf{K}^G$ (ex. 1.1.4°) en somme

$$\mathbf{K}^G = \bigoplus R_i$$

de représentations irréductibles. Soit (V, ρ) une représentation de G et soit $v_0 \in V$. L'application linéaire

$$\begin{aligned} u : \mathbf{K}^G &\longrightarrow V \\ (f : G \to \mathbf{K}) &\longmapsto \sum_{g \in G} f(g) \rho(g)(v_0) \end{aligned}$$

est un morphisme de représentations. En effet, pour tout $h \in G$ et tout $g \in G$, on a $u(\varepsilon_g) = \rho(g)(v_0)$ et (*cf.* ex. 1.1.4°)

$$u \circ \rho_R(h)(\varepsilon_g) = u(\varepsilon_{hg}) = \rho(hg)(v_0) = \rho(h) \circ \rho(g)(v_0) = \rho(h) \circ u(\varepsilon_g),$$

donc $u \circ \rho_R(h) = \rho(h) \circ u$. Si $v_0 \neq 0$, l'application f n'est pas nulle (car $f(\varepsilon_e) = v_0$), et si de plus V est irréductible, f est surjective, donc il y a au moins un i tel que $f|_{R_i}$ soit non nul ; par le lemme de Schur, c'est un isomorphisme et V est isomorphe à la représentation R_i.

On en déduit le résultat suivant [1].

Proposition 1.11. — *Soit* G *un groupe fini tel que* $\mathrm{car}(\mathbf{K}) \nmid |G|$. *Il n'y a à isomorphisme près qu'un nombre fini de représentations irréductibles de* G *et chacune est de dimension* $\leqslant |G|$.

Lorsque $\mathbf{K}$ est algébriquement clos, ces résultats seront précisés dans le cor. 2.6.1° et, si de plus $\mathrm{car}(\mathbf{K}) = 0$, dans la prop. 2.8, où on montre que la dimension d'une représentation irréductible est $\leqslant \sqrt{|G|}$.

Exercice 1.12. — Si $\mathrm{car}(\mathbf{K}) \nmid |G|$, montrer que l'intersection des noyaux des représentations irréductibles de G est $\{e\}$.

Proposition 1.13. — *Soit* G *un groupe fini tel que* $\mathrm{car}(\mathbf{K}) \nmid |G|$ *et soient* $\rho_1, \ldots, \rho_\ell$ *les représentations irréductibles de* G. *Toute représentation de* G *de dimension finie se décompose en* $\bigoplus \rho_i^{n_i}$, *où les entiers naturels* n_i *sont uniquement déterminés par la représentation.*

Démonstration. — L'existence d'une telle décomposition est le cor. 1.9. Montrons l'unicité des n_i par récurrence sur la dimension de la représentation. Supposons $V := \bigoplus V_i$ isomorphe à $W := \bigoplus W_j$, où les V_i et les W_j sont des représentations irréductibles, éventuellement répétées. On va montrer qu'à permutation près, les (V_i) et les (W_j) sont la même collection de représentations. On dispose d'un isomorphisme de représentations

$$u : \bigoplus_i V_i \xrightarrow{\sim} \bigoplus_j W_j$$

dont on notera l'inverse u'. Notons $p_i : V \to V_i$ et $q_j : W \to W_j$ les projections et considérons les morphismes de représentations

$$u_j := V_1 \xrightarrow{u|_{V_1}} W \xrightarrow{q_j} W_j \xrightarrow{u'|_{W_j}} V \xrightarrow{p_1} V_1.$$

On a

$$\sum_j u_j = \sum_j p_1 \circ u'|_{W_j} \circ q_j \circ u|_{V_1} = p_1 \circ \Big(\sum_j u'|_{W_j} \circ q_j\Big) \circ u|_{V_1} = p_1 \circ u' \circ u|_{V_1} = \mathrm{Id}_{V_1}.$$

Au moins un des u_j est donc non nul et, quitte à rénuméroter les W_j, on peut supposer que c'est u_1. Les morphismes de représentations $q_1 \circ u|_{V_1} : V_1 \to W_1$ et $p_1 \circ u'|_{W_1} : W_1 \to V_1$ sont alors non nuls. Par le lemme de Schur, ce sont des isomorphismes.

Pour appliquer l'hypothèse de récurrence, il suffit de montrer que le morphisme de représentations

$$(\mathrm{Id}_W - q_1)\, u|_{\bigoplus_{i \geqslant 2} V_i} : \bigoplus_{i \geqslant 2} V_i \longrightarrow \bigoplus_{j \geqslant 2} W_j$$

1. Comme on l'a vu dans l'exerc. 1.5, la seconde partie est valable sans hypothèse sur la caractéristique du corps. Il en est de même de la première partie, mais il faut prendre garde que lorsque $\mathrm{car}(\mathbf{K}) \mid |G|$, il existe des représentations (de dimension finie) qui ne sont pas sommes de représentations irréductibles, donc il y a des représentations indécomposables qui ne sont pas irréductibles. Et malheureusement, pour certains groupes finis, le nombre de classes d'isomorphisme de représentations indécomposables est infini (en caractéristique p, Higman a démontré que c'est le cas si les p-sous-groupes de Sylow ne sont pas cycliques).

entre représentations de même dimension est encore un isomorphisme. C'est en effet le cas : si $x \in \bigoplus_{i\geqslant 2} V_i$ est dans le noyau, $u(x) \in W_1$ et $p_1 u'(u(x)) = p_1(x) = 0$, donc, $p_1 \circ u'|_{W_1}$ étant un isomorphisme, $u(x) = 0$ et $x = 0$. Ce morphisme est donc injectif. Comme source et but ont même dimension, c'est un isomorphisme. □

Sous les hypothèses de la proposition, on peut donc décomposer une représentation (V,ρ) de dimension finie du groupe G en somme directe $V = \bigoplus_i V_i$ de représentations irréductibles. *Cette décomposition n'est en général pas unique !* Dans le cas par exemple où tous les $\rho(g)$ sont l'identité (donc la seule représentation irréductible qui intervient est la représentation triviale, de dimension 1) , il s'agit simplement de décomposer V en somme directe de droites, ce qu'on peut faire de bien des façons.

2. Caractères

Dans cette section, on suppose G *fini,* **K** *algébriquement clos et* $\mathrm{car}(\mathbf{K}) \nmid |G|$.

Si (V,ρ) est une représentation de dimension finie de G, on appelle *caractère* de ρ la fonction

$$\begin{aligned} \chi_\rho : G &\longrightarrow \mathbf{K} \\ g &\longmapsto \mathrm{tr}(\rho(g)). \end{aligned}$$

On a $\chi_\rho(e) = \dim(V)$, donc le caractère détermine la dimension de la représentation (on verra dans la prop. 2.8 que le caractère détermine ρ complètement lorsque **K** est algébriquement clos).

On calcule

$$\forall g,h \in G \qquad \chi_\rho(hgh^{-1}) = \mathrm{tr}\big(\rho(h)\rho(g)\rho(h)^{-1}\big) = \mathrm{tr}\big(\rho(g)\big) = \chi_\rho(g).$$

On dit que χ_ρ est une *fonction centrale,* ou encore *invariante par conjugaison.*

De façon générale, une fonction $f : G \to \mathbf{K}$ est centrale si et seulement si elle est constante sur chaque classe de conjugaison C de G ; on notera alors $f(C)$ sa valeur sur la classe C. Le **K**-espace vectoriel de toutes les fonctions centrales sur le groupe G sera noté $\mathscr{C}(G)$. Sa dimension est donc le nombre de classes de conjugaison.

Rappelons (§ I.2.3) que les classes de conjugaisons de G sont les orbites sous l'action de G sur G définie par $g \cdot x = gxg^{-1}$ (lorsque G est abélien, ces classes sont des singletons).

Exemples 2.1. — 1° Le caractère de la représentation régulière est

$$\chi_R(g) = \begin{cases} |G| & \text{si } g = e, \\ 0 & \text{si } g \neq e. \end{cases}$$

C'est donc $|G|$ fois la fonction caractéristique $\mathbf{1}_{C_e}$ de la classe de conjugaison $C_e = \{e\}$.

2° Le caractère de la représentation standard de D_n dans $\mathbf{C}^2$ est donné par

$$\chi(r^k) = 2\cos\frac{2k\pi}{n}, \quad \chi(r^k s) = 0.$$

Il vaut donc 0 sur $\{s, rs, \ldots, r^{n-1}s\}$ (qui est la réunion de 1 ou 2 classes de conjugaison selon que n est impair ou non) et $2\cos\frac{2k\pi}{n}$ sur chaque classe de conjugaison $\{r^k, r^{-k}\}$.

3° Le groupe $\mathfrak{S}_3$ possède trois classes de conjugaison, celle de l'élément neutre e, celle à 3 éléments d'une transposition τ, et celle à 2 éléments d'un 3-cycle σ. Le caractère de la représentation standard de $\mathfrak{S}_3$ dans $\mathbf{C}^3$ vaut 3 sur e, 1 sur les transpositions et 0 sur les 3-cycles.

Plus généralement, on a vu dans la prop. I.2.8 que les classes de conjugaison de $\mathfrak{S}_n$ sont en bijection avec les partitions de n :

$$n = k_1 + \cdots + k_r, \quad r \in \mathbf{N},\ 1 \leqslant k_1 \leqslant \cdots \leqslant k_r,$$

une telle partition correspondant aux produits de cycles à supports disjoints d'ordre $k_1, \ldots, k_r$. Sur la classe de conjugaison correspondante, le caractère de la représentation standard de $\mathfrak{S}_n$ dans $\mathbf{C}^n$ vaut $\max\{i \mid k_i = 1\}$ (c'est le nombre de points fixes de la permutation).

Propriétés 2.2. — *1° Des représentations de dimension finie isomorphes ont même caractère.*

2° On a $\chi_{V^*}(g) = \chi_V(g^{-1})$.

3° On a $\chi_{V\oplus W} = \chi_V + \chi_W$.

4° Si $W \subseteq V$ *est une sous-représentation,* $\chi_V = \chi_W + \chi_{V/W}$.

5° On a $\chi_{V\otimes W} = \chi_V \chi_W$.

Démonstration. — Tout est évident, sauf la quatrième propriété qui découle de l'identité $\mathrm{tr}(u \otimes v) = \mathrm{tr}(u)\,\mathrm{tr}(v)$, qu'on peut vérifier dans une base (exerc. III.1.5). □

On introduit sur le $\mathbf{K}$-espace vectoriel $\mathbf{K}^G = \{f : G \to \mathbf{K}\}$ la forme bilinéaire symétrique

$$\langle f, f' \rangle = \frac{1}{|G|} \sum_{g \in G} f(g^{-1}) f'(g).$$

On a en particulier $\langle f, \varepsilon_g \rangle = \frac{1}{|G|} f(g^{-1})$ donc cette forme est non dégénérée.

Théorème 2.3. — *Les caractères des représentations irréductibles de dimension finie forment une base orthonormale du* $\mathbf{K}$*-espace vectoriel* $\mathscr{C}(G)$ *des fonctions centrales sur* G.

Démonstration. — La démonstration du théorème va utiliser deux lemmes. Soient (V, ρ_V) et (W, ρ_W) des représentations de G et soit $u \in \mathrm{Hom}(V, W)$. Comme dans (47), on pose

$$\pi(u) = \frac{1}{|G|} \sum_{g \in G} \rho_W(g) \circ u \circ \rho_V(g)^{-1} \in \mathrm{Hom}(V, W).$$

Lemme 2.4. — *L'endomorphisme* π *de* $\mathrm{Hom}(V, W)$ *ainsi défini est un projecteur d'image* $\mathrm{Hom}_G(V, W)$ *et*

$$\mathrm{tr}(\pi) = \langle \chi_V, \chi_W \rangle.$$

Démonstration. — On rappelle que

$$\mathrm{Hom}_G(V, W) := \{u \in \mathrm{Hom}(V, W) \mid \forall h \in G \quad u \circ \rho_V(h) = \rho_W(h) \circ u\}.$$

Pour tout $u \in \mathrm{Hom}(V,W)$ et tout $h \in G$, on a bien

$$\begin{aligned}\rho_W(h)\circ\pi(u)\circ\rho_V(h)^{-1} &= \frac{1}{|G|}\sum_{g\in G}\rho_W(h)\circ\rho_W(g)\circ u\circ\rho_V(g)^{-1}\circ\rho_V(h)^{-1}\\ &= \frac{1}{|G|}\sum_{g\in G}\rho_W(hg)\circ u\circ\rho_V(g^{-1}h^{-1})\\ &= \frac{1}{|G|}\sum_{g'\in G}\rho_W(g')\circ u\circ\rho_V(g'^{-1})\\ &= \pi(u).\end{aligned}$$

De plus, si $u \in \mathrm{Hom}_G(V,W)$, on a $\pi(u) = u$, de sorte que π est bien un projecteur d'image $\mathrm{Hom}_G(V,W)$.

On calcule maintenant $\mathrm{tr}(\pi)$ dans une base de $\mathrm{Hom}(V,W)$. Choisissons des bases de V et W et notons e_{ij} l'élément de $\mathrm{Hom}(V,W)$ dont la matrice dans ces bases a tous ses coefficients sont nuls, sauf celui situé à la i-ème ligne et la j-ème colonne, qui vaut 1. Les (e_{ij}) forment une base de $\mathrm{Hom}(V,W)$ et on a

$$\big(\rho_W(g)\circ e_{ij}\circ\rho_V(g)^{-1}\big)_{kl} = \rho_W(g)_{ki}\rho_V(g^{-1})_{jl}.$$

Appliquant ceci au cas particulier $i = k$ et $j = l$, on calcule

$$\begin{aligned}\mathrm{tr}(\pi) = \sum_{i,j}\pi(e_{ij})_{ij} &= \sum_{i,j}\frac{1}{|G|}\sum_{g\in G}\rho_W(g)_{ii}\rho_V(g^{-1})_{jj}\\ &= \frac{1}{|G|}\sum_{g\in G}\Big(\sum_i\rho_W(g)_{ii}\Big)\Big(\sum_j\rho_V(g^{-1})_{jj}\Big)\\ &= \frac{1}{|G|}\sum_{g\in G}\chi_W(g)\chi_V(g^{-1}).\end{aligned}$$

Ceci démontre le lemme. □

Si V et W sont irréductibles, on a par le lemme de Schur

$$\mathrm{Hom}_G(V,W) = \begin{cases}0 & \text{si V et W ne sont pas isomorphes,}\\ \mathbf{K} & \text{si V et W sont isomorphes.}\end{cases}$$

Comme le rang d'un projecteur est sa trace, le lemme 2.4 entraîne que $\langle\chi_V,\chi_W\rangle = \mathrm{tr}(\pi)$ vaut 0 dans le premier cas, 1 dans le second. Donc la famille des (χ_V), pour V irréductible (ou plus exactement, pour V décrivant l'ensemble des classes d'isomorphisme de représentations irréductibles de G), est orthonormale ; il reste à voir qu'elle engendre tout $\mathscr{C}(G)$.

Lemme 2.5. — *Soit* (V,ρ) *une représentation de* G. *Si* $f : G \to \mathbf{K}$ *est une fonction centrale, posons*

$$f_\rho := \frac{1}{|G|}\sum_{g\in G} f(g)\rho(g^{-1}) \in \mathrm{End}(V).$$

1° On a $f_\rho \in \mathrm{End}_G(V)$ *et* $\mathrm{tr}(f_\rho) = \langle f,\chi_\rho\rangle$.

2° Si (V,ρ) *est irréductible,* $\dim(V)\cdot 1_{\mathbf{K}}$ *est inversible dans* **K** *et* f_ρ *est l'homothétie de* V *de rapport* $\frac{\langle f,\chi_\rho\rangle}{\dim(V)}$.

Démonstration. — On calcule, puisque f est centrale,

$$\forall h \in \mathrm{G} \qquad \rho(h) \circ f_\rho \circ \rho(h)^{-1} = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\rho(hg^{-1}h^{-1})$$
$$= \frac{1}{|\mathrm{G}|} \sum_{g' \in \mathrm{G}} f(h^{-1}g'h)\rho(g'^{-1}) = \frac{1}{|\mathrm{G}|} \sum_{g' \in \mathrm{G}} f(g')\rho(g'^{-1}) = f_\rho.$$

Donc $f_\rho \in \mathrm{End}_{\mathrm{G}}(\mathrm{V})$ et sa trace est

$$\mathrm{tr}(f_\rho) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\chi_\rho(g^{-1}) = \langle f, \chi_\rho \rangle.$$

Ceci montre le premier point.

Si ρ est irréductible, on déduit du lemme de Schur 1.10 et du premier point appliqué à la fonction centrale $f = \chi_\rho$ que $(\chi_\rho)_\rho$ est une homothétie. Si λ est son rapport, on a $\mathrm{tr}((\chi_\rho)_\rho) = \dim(\mathrm{V})\lambda = \langle \chi_\rho, \chi_\rho \rangle = 1_{\mathbf{K}}$. En particulier, $\dim(\mathrm{V}) \cdot 1_{\mathbf{K}}$ est inversible dans $\mathbf{K}$.

Pour f fonction centrale quelconque, f_ρ est de nouveau une homothétie par le lemme de Schur 1.10. Comme sa trace est $\langle f, \chi_\rho \rangle$, son rapport est $\frac{\langle f, \chi_\rho \rangle}{\dim(\mathrm{V})}$. Cela montre le second point. □

Si une fonction centrale $f \in \mathscr{C}(\mathrm{G})$ est orthogonale à tous les caractères χ_ρ, on a, par le lemme, $f_\rho = 0$ pour toute représentation ρ irréductible, et donc pour toute représentation puisque $f_{\rho \oplus \rho'} = f_\rho \oplus f_{\rho'}$. Appliquant cela à la représentation régulière, on obtient $f_{\rho_{\mathrm{R}}} = 0$ donc

$$0 = f_{\rho_{\mathrm{R}}}(\varepsilon_e) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\rho_{\mathrm{R}}(g^{-1})(\varepsilon_e) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\varepsilon_{g^{-1}}$$

dans $\mathbf{K}^{\mathrm{G}}$, ce qui entraîne $f = 0$, puisque les $\varepsilon_{g^{-1}}$ forment une base de $\mathbf{K}^{\mathrm{G}}$.

Cela termine la preuve du th. 2.3 : tout $f \in \mathscr{C}(\mathrm{G})$ s'écrit $f = \sum_{\rho \text{ irr}} \langle f, \chi_\rho \rangle \chi_\rho$. □

Corollaire 2.6. — *1° Le nombre de représentations irréductibles de* G *est égal au nombre de classes de conjugaison de* G.

2° Soient $\chi_1, \ldots, \chi_\ell$ *les caractères des représentations irréductibles de* G. *Soient* C *et* C′ *des classes de conjugaison dans* G. *On a*

$$\sum_{i=1}^{\ell} \chi_i(\mathrm{C}^{-1})\chi_i(\mathrm{C}') = \begin{cases} \frac{|\mathrm{G}|}{|\mathrm{C}|} \cdot 1_{\mathbf{K}} & \textit{si } \mathrm{C} = \mathrm{C}', \\ 0 & \textit{sinon.} \end{cases}$$

L'entier $|\mathrm{C}|$ divise l'ordre de G puisque c'est le cardinal d'une orbite pour l'action de G sur lui-même par conjugaison (*cf.* § I.2.2).

Lorsque la caractéristique de $\mathbf{K}$ divise l'ordre de G, le premier énoncé n'est plus nécessairement vrai (*cf.* rem. 2.13).

Démonstration. — La dimension de $\mathscr{C}(\mathrm{G})$ est égale au nombre de classes de conjugaison dans G, d'où le premier énoncé. Pour le second, soit $\mathbf{1}_{\mathrm{C}}$ la fonction caractéristique de C. Alors $f = \mathbf{1}_{\mathrm{C}}$ est une fonction centrale qui se décompose sur la base orthonormale des caractères χ_i des représentations irréductibles :

$$\mathbf{1}_{\mathrm{C}} = \sum_{i=1}^{\ell} \langle \mathbf{1}_{\mathrm{C}}, \chi_i \rangle \chi_i, \quad \text{avec } \langle \mathbf{1}_{\mathrm{C}}, \chi_i \rangle = \frac{1}{|\mathrm{G}|} |\mathrm{C}| \chi_i(\mathrm{C}^{-1}).$$

Il en résulte

$$\mathbf{1}_C = \frac{|C|}{|G|} \sum_{i=1}^{\ell} \chi_i(C^{-1})\chi_i,$$

ce qui est exactement le résultat voulu. □

On a déjà remarqué que la décomposition $V = \bigoplus_i V_i$ d'une représentation en somme directe de représentations irréductibles n'est pas unique. En revanche, si on regroupe tous les V_i isomorphes à la même représentation irréductible, on obtient une décomposition $V = \bigoplus_j W_j$ *en composantes isotypiques* indépendante des choix.

Théorème 2.7. — *Soit* (V,ρ) *une représentation de dimension finie du groupe fini* G. *La projection de* V *sur la composante isotypique correspondant à une représentation irréductible* (U,ψ) *est donnée par*

$$p_U = \frac{\dim(U)}{|G|} \sum_{g\in G} \chi_\psi(g)\rho(g^{-1}).$$

En particulier, la décomposition en composantes isotypiques ne dépend que de la représentation (V,ρ).

Démonstration. — Soit f une fonction centrale sur G. Par sa définition même, l'endomorphisme f_ρ de V laisse stable toute sous-représentation (V_i,ρ_i) de (V,ρ) et se restreint à V_i en f_{ρ_i}. Si V_i est de plus irréductible, f_{ρ_i} est l'homothétie de V_i de rapport $\frac{\langle f,\chi_i\rangle}{\dim(V_i)}$ (lemme 2.5.2°).

Par le th. 2.3, si f est le caractère χ_ψ d'une représentation irréductible (U,ψ), l'endomorphisme $(\chi_\psi)_\rho|_{V_i}$ est donc $\frac{1}{\dim(V_i)}\mathrm{Id}_{V_i}$ si V_i est isomorphe à U et 0 sinon. Comme $p_U = \dim(U)(\chi_\psi)_\rho$, sa restriction à V_i est donc l'identité de V_i si V_i est isomorphe à U et 0 sinon. Ceci démontre le théorème. □

On peut maintenant montrer qu'en caractéristique 0, une représentation est déterminée par son caractère. On identifie aussi les représentations irréductibles comme étant celles dont le caractère est de norme 1.

Proposition 2.8. — *Notons* $\rho_1,\dots,\rho_\ell$ *les représentations irréductibles du groupe fini* G. *Soit* ρ *une représentation de* G, *qu'on décompose en* $\rho = \bigoplus_{i=1}^{\ell} \rho_i^{n_i}$ *(prop. 1.13). On a*

$$\langle\chi_\rho,\chi_{\rho_i}\rangle = n_i\cdot 1_{\mathbf{K}} \quad , \quad \langle\chi_\rho,\chi_\rho\rangle = \Big(\sum_{i=1}^{\ell} n_i^2\Big)\cdot 1_{\mathbf{K}}.$$

Si $\mathrm{car}(\mathbf{K}) = 0$,

- *des représentations* ρ *et* ρ' *de* G *sont isomorphes si et seulement si* $\chi_\rho = \chi_{\rho'}$;
- ρ *est irréductible si et seulement si* $\langle\chi_\rho,\chi_\rho\rangle = 1_{\mathbf{K}}$;
- *la représentation régulière se décompose en* $\mathbf{K}^G = \bigoplus_{i=1}^{\ell} \rho_i^{\dim(\rho_i)}$; *en particulier,* $\sum_{i=1}^{\ell} \dim(\rho_i)^2 = |G|$.

Si $\mathrm{car}(\mathbf{K}) = p \neq 0$, il est faux que le caractère détermine la représentation ; par exemple, pour toute représentation V, le caractère de V^p est nul.

Une autre contrainte importante sur les dimensions des représentations irréductibles est qu'elles divisent l'ordre du groupe. Ce théorème plus difficile (th. 3.6) sera vu dans le § 3.2 en caractéristique nulle.

Démonstration. — On a $\chi_\rho = \sum_{i=1}^{\ell} n_i \chi_{\rho_i}$, donc $\langle \chi_\rho, \chi_{\rho_i} \rangle = n_i \cdot 1_{\mathbf{K}}$ et $\langle \chi_\rho, \chi_\rho \rangle = (\sum_{i=1}^{\ell} n_i^2) \cdot 1_{\mathbf{K}}$.

Ainsi, en caractéristique nulle, χ_ρ détermine les entiers n_i et donc toute la représentation ρ, et ρ est irréductible si et seulement si $\langle \chi_\rho, \chi_\rho \rangle = 1_{\mathbf{K}}$.

Appliquons cela à la représentation régulière : puisque $\chi_R = |G| \mathbf{1}_{\{e\}}$, on obtient $\langle \chi_R, \chi_{\rho_i} \rangle = \chi_{\rho_i}(e) = \dim(\rho_i)$, d'où il résulte que la représentation régulière est isomorphe à $\bigoplus_{i=1}^{\ell} \rho_i^{\dim(\rho_i)}$. □

Proposition 2.9. — *Supposons* $\mathrm{car}(\mathbf{K}) = 0$. *Le groupe* G *est abélien si et seulement si toutes ses représentations irréductibles sont de dimension* 1.

Le nombre de ces représentations irréductibles est alors le cardinal de G.

Démonstration. — Un groupe G est abélien si et seulement si il a exactement $|G|$ classes de conjugaison, donc $|G|$ représentations irréductibles. Or $|G| = \sum_{i=1}^{\ell} \dim(\rho_i)^2$, donc $\ell \leqslant |G|$ avec égalité si et seulement si toutes les représentations irréductibles sont de dimension 1. □

Si $\mathrm{car}(\mathbf{K}) \neq 0$, la conclusion de la proposition n'est plus vraie en général, comme le montre l'exercice suivant (il existe des p-groupes non abéliens).

Exercice 2.10. — Soit p un nombre premier, soit G un p-groupe (c'est-à-dire un groupe fini de cardinal une puissance de p ; *cf.* prop. I.2.13) et soit $\mathbf{K}$ un corps de caractéristique p. Montrer que la seule représentation irréductible ρ de G dans un $\mathbf{K}$-espace vectoriel est la représentation triviale (*Indication :* si V est une telle représentation et $v \in V - \{0\}$, on pourra considérer le sous-groupe additif de V engendré par les $\rho(g)(v)$, pour g décrivant G, montrer que c'est un p-groupe, et appliquer la prop. I.2.13).

2.1. Table des caractères. — On prend $\mathbf{K} = \mathbf{C}$. Pour toute représentation (V, ρ) d'un groupe fini G, on a $\rho(g)^{|G|} = \mathrm{Id}_V$, donc les valeurs propres de $\rho(g)$ sont des racines de l'unité, et celles de $\rho(g^{-1})$ sont leurs conjugués. On a donc

$$\chi_\rho(g^{-1}) = \mathrm{tr}(\rho(g^{-1})) = \overline{\mathrm{tr}(\rho(g))} = \overline{\chi_\rho(g)}.$$

On a ainsi

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_\rho(g)}\, \chi_{\rho'}(g) \tag{48}$$

et, si $\chi_1, \ldots, \chi_\ell$ sont les caractères des représentations irréductibles de G, le cor. 2.6.2° donne

$$\sum_{i=1}^{\ell} \overline{\chi_i(C)} \chi_i(C') = \begin{cases} \frac{|G|}{|C|} & \text{si } C = C', \\ 0 & \text{sinon.} \end{cases} \tag{49}$$

Comme $\chi_\rho(g)$ est la somme des valeurs propres, on a aussi

$$\forall g \in G \qquad |\chi_\rho(g)| \leqslant \chi_\rho(e) = \dim(V).$$

De plus, $\chi_\rho(g) = \chi_\rho(e)$ si et seulement si $\rho(g) = \mathrm{Id}_V$. On a donc

$$\{g \in G \mid \chi_\rho(g) = \chi_\rho(e)\} = \ker(\rho) \trianglelefteq G.$$

De même, on a $|\chi_\rho(g)| = \chi_\rho(e)$ si et seulement si $\rho(g)$ est une homothétie.

La *table des caractères* de G donne la valeur de chaque caractère sur chaque classe de conjugaison ; les lignes correspondent aux caractères et les colonnes aux classes de conjugaison. C'est une table carrée (cor. 2.6.1°). Les relations obtenues se traduisent par le fait que

- les colonnes sont orthogonales (pour le produit scalaire hermitien standard) ;
- la colonne correspondant à la classe de conjugaison C est de norme hermitienne (au carré) $|G|/|C|$ (*cf.* (49)) ;
- les lignes sont orthogonales et de norme (au carré) $|G|$ pour le produit scalaire hermitien pondéré par le cardinal des classes de conjugaison (*cf.* (48)) ;
- la somme des lignes pondérées par les dimensions $\chi(e)$ est la ligne $|G|\ 0\ \cdots\ 0$.

Exercice 2.11. — Montrer qu'une table des caractères est une matrice inversible.

On peut utiliser cette table pour obtenir des informations sur les sous-groupes distingués de G. Un tel sous-groupe est réunion de classes de conjugaisons. Pour chaque caractère χ, la réunion des classes sur lesquelles χ prend la valeur $\chi(e)$ est un sous-groupe $G_\chi \trianglelefteq G$ et tout sous-groupe distingué de G est obtenu comme intersection de G_χ (utiliser l'exerc. 1.12).

En particulier, G est simple si et seulement si tous les G_χ à part $G_{\chi_{\text{triv}}} = G$ sont triviaux, c'est-à-dire si et seulement si dans chaque ligne excepté celle correspondant à la représentation triviale (qui est la seule composée uniquement de 1), la valeur $\chi(e)$ n'apparaît qu'une seule fois (dans la colonne correspondant à la classe $\{e\}$).

Les représentations de dimension 1 sont des morphismes $G \to \mathbf{C}^\times$ donc elles se factorisent par $G/D(G)$. Par le même raisonnement, le groupe dérivé $D(G)$ est l'intersection des G_χ pour tous les caractères χ de représentations de dimension 1.

On s'intéresse maintenant au centre $Z(G)$ de G. Si $g \in Z(G)$, alors $\rho_i(g)$ commute avec tous les $\rho_i(h)$ donc, par le lemme de Schur 1.10, c'est une homothétie de rapport une racine de l'unité et $|\chi_i(g)| = \chi_i(e)$ pour tout i. Inversement, si $|\chi_i(g)| = \chi_i(e)$, on a vu plus haut que $\rho_i(g)$ est une homothétie, donc commute avec tous les $\rho_i(h)$. Si c'est vrai pour tout i, alors $\rho(g)$ commute avec tous les $\rho(h)$ pour toute représentation ρ. En appliquant cela à une représentaiton fidèle (c'est-à-dire pour laquelle ρ est injective) comme la représentation régulière, on obtient $g \in Z(G)$.

Le centre de G est donc la réunion des classes de conjugaison C pour lesquelles $|\chi_i(C)| = \chi_i(e)$ pour tout i.

Les contraintes obtenues sur les caractères sont suffisantes pour obtenir une description complète des représentation irréductibles du groupe G dans certains cas. On traite ici quelques exemples.

Le groupe $\mathfrak{S}_3 = D_3$. — On a vu qu'il y a trois classes de conjugaison : celle de l'élément neutre e, celle des transpositions τ, et celles des 3-cycles σ. Il y a donc trois représentations irréductibles de $\mathfrak{S}_3$.

Les représentations de dimension 1 sont les morphismes $G \to G/D(G) \to \mathbf{C}^\times$. Dans notre cas, le groupe dérivé est $\mathfrak{A}_3$ et $\mathfrak{S}_3/\mathfrak{A}_3 \simeq \mathbf{Z}/2\mathbf{Z}$. Il y a donc deux représentations de dimension 1, facilement identifiées : la représentation triviale $\mathbf{C}_{\text{triv}}$ (de caractère χ_{triv}) et la

signature $\mathbf{C}_{\text{sign}}$ (de caractère χ_{sign}). Par la prop. 2.8, la somme des carrés des dimensions des représentations est $|\mathfrak{S}_3| = 6$, soit $1+1+4=6$ donc la dimension de la dernière représentation irréductible est 2. On peut alors dresser la table des caractères, en indiquant au-dessus de chaque classe de conjugaison son cardinal :

$\mathfrak{S}_3$	1	3	2
	e	τ	σ
χ_{triv}	1	1	1
χ_{sign}	1	-1	1
χ	2	0	-1

La première colonne donne la dimension des représentations. La troisième ligne, *a priori* inconnue, est obtenue en utilisant le fait que les colonnes sont orthogonales ; une autre méthode est d'écrire (prop. 2.8) $\chi_{\text{triv}} + \chi_{\text{sign}} + 2\chi = \chi_{\text{R}} = 6 \cdot \mathbf{1}_{\{e\}}$ d'où on déduit également le dernier caractère χ.

On a ainsi déterminé le caractère de la troisième représentation sans la connaître, mais on peut aussi la décrire explicitement : d'après l'ex. 1.2.2°, $\mathfrak{S}_3$ a une représentation ρ dans le plan complexe $\mathrm{V}_0 = \{(x_1,x_2,x_3) \in \mathbf{C}^3 \mid x_1+x_2+x_3 = 0\}$ dont la somme directe avec la représentation triviale de dimension 1 est la représentation de permutation, de caractère (ex. 2.1.3°) de valeurs 3,1 et 0, qui est bien la somme $\chi_{\text{triv}} + \chi$.

On reconnaît les sous-groupes distingués de $\mathfrak{S}_3$: ce sont $\mathfrak{S}_3$ (noyau de χ_{triv}), $\mathfrak{A}_3 = \{e\} \cup \{\sigma\}$ (noyau de χ_{sign}) et $\{e\}$ (noyau de χ). Le groupe dérivé est $\mathfrak{A}_3$ (noyau de χ_{sign}) et le centre est trivial.

La table des caractères peut aussi être utilisée pour calculer la décomposition en composantes irréductibles d'une représentation donnée, grâce à la prop. 2.8. Par exemple, décomposons le produit tensoriel $\mathrm{V}_0 \otimes \mathrm{V}_0$, où V_0 est la représentation irréductible d'ordre 2. Son caractère est χ^2, de valeurs 4, 0, 1 ; c'est donc $\chi_{\text{triv}} + \chi_{\text{sign}} + \chi$. On a ainsi

$$\mathrm{V}_0 \otimes \mathrm{V}_0 \simeq \mathbf{C}_{\text{triv}} \oplus \mathbf{C}_{\text{sign}} \oplus \mathrm{V}_0.$$

Remarquons qu'on connaissait déjà, par (41), la décomposition $\mathrm{V}_0 \otimes \mathrm{V}_0 = \mathrm{S}^2\mathrm{V}_0 \oplus \bigwedge^2 \mathrm{V}_0$. Le morceau $\bigwedge^2 \mathrm{V}_0$, de dimension 1, est $\mathbf{C}_{\text{sign}}$ (c'est le déterminant), tandis que le morceau $\mathrm{S}^2\mathrm{V}_0$ se décompose en deux.

Exercice 2.12. — Soit V une représentation réelle d'un groupe fini G. Montrer que la représentation $\mathrm{S}^2\mathrm{V}$ contient une sous-représentation de dimension 1 (*Indication :* on pourra utiliser la construction de la première démonstration du th. 1.8).

Le groupe D_4. — Le groupe de symétrie du carré est engendré par une rotation r d'angle $\frac{\pi}{2}$ et une symétrie s. On a $sr^k s = r^{-k}$ et $rsr^{-1} = sr^2$, ce qui donne 5 classes de conjugaison : $\{\mathrm{Id}\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, r^2 s\}$ et $\{rs, r^3 s\}$. Le sous-groupe $\mathbf{Z}/2\mathbf{Z} = \{\mathrm{Id}, -\mathrm{Id} = r^2\}$ est distingué et dans le quotient les trois éléments distincts r, s et rs sont d'ordre 2, donc

$$\mathrm{D}_4/(\mathbf{Z}/2\mathbf{Z}) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

Cela nous donne donc quatre représentations de dimension 1 correspondant aux quatre morphismes $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \to \mathbf{C}^\times$; la cinquième doit donc être de dimension 2. Appliquant

la même méthode que précédemment, on obtient la table des caractères :

D_4	1	1	2	2	2
	e	r^2	$\{r, r^3\}$	$\{s, r^2 s\}$	$\{rs, r^3 s\}$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
$\chi_1\chi_2$	1	1	-1	-1	1
χ_ρ	2	-2	0	0	0

La représentation de dimension 2 ici n'est autre que la représentation standard ρ dans $\mathbf{C}^2$ (ex. 2.1.3°).

Les sous-groupes distingués de D_4 sont D_4, $\{e, r^2, s, r^2 s\}$ (noyau de χ_1), $\{e, r, r^2, r^3\}$ (noyau de χ_2), $\{e, r^2, rs, r^3 s\}$ (noyau de $\chi_1\chi_2$), $\{e\}$ et leurs intersections. Le groupe dérivé est $\{e, r^2\}$ ($\ker(\chi_1) \cap \ker(\chi_2)$) et c'est aussi le centre $\{g \in D_4 \mid \forall i \ \ |\chi_i(g)| = \chi_i(e)\}$.

Le groupe $\mathfrak{S}_4$. — On a (prop. I.2.8) 5 classes de conjugaison, correspondant aux partitions (1111) (classe de Id), (112) (classe d'une transposition, de cardinal 6), (13) (classe d'un 3-cycle, de cardinal 8), (4) (classe d'un 4-cycle, de cardinal 6) et (22) (classe d'une double transposition, de cardinal 3) de 4, donc 5 représentations irréductibles. D'autre part, on a $D(\mathfrak{S}_4) = \mathfrak{A}_4$ (prop. I.5.9), donc deux représentations irréductibles de dimension 1, la représentation triviale $\mathbf{C}_{\text{triv}}$ et la signature $\mathbf{C}_{\text{sign}}$.

On a aussi la représentation de dimension 3 de $\mathfrak{S}_4$ dans $V_0 = \{(x_1, x_2, x_3, x_4) \in \mathbf{C}^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}$. Le caractère de $V_0 \oplus \mathbf{C}_{\text{triv}}$ a été calculé dans l'ex. 2.1.3° : il prend les valeurs 4, 2, 1, 0, 0. Le caractère de V_0 prend donc les valeurs 3, 1, 0, -1, -1. On a

$$\langle \chi_{V_0}, \chi_{V_0} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)^2 = \frac{1}{24}(9 \times 1 + 1 \times 6 + 1 \times 6 + 1 \times 3) = 1,$$

de sorte que V_0 est irréductible (prop. 2.8).

Il nous reste deux représentations irréductibles à trouver, dont la somme des carrés des dimensions est $24 - 1 - 1 - 9 = 13$. Elles sont donc de dimension 2 et 3. L'une d'elles est $V_0 \otimes \mathbf{C}_{\text{sign}}$, dont le caractère prend les valeurs 3, -1, 0, 1, -1. Elle est irréductible (on peut voir ça soit en calculant $\langle \chi_{V_0 \otimes \mathbf{C}_{\text{sign}}}, \chi_{V_0 \otimes \mathbf{C}_{\text{sign}}} \rangle$, soit en remarquant que le produit tensoriel d'une représentation irréductible et d'une représentation de dimension 1 est encore irréductible (ex. 1.4.4°)).

On a donc déjà la table de caractères partielle

$\mathfrak{S}_4$	1	6	8	6	3
	Id	(12)	(123)	(1234)	(12)(34)
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	-1	1
χ_{V_0}	3	1	0	-1	-1
$\chi_{V_0}\chi_{\text{sign}}$	3	-1	0	1	-1
χ_V	2	$\star$	$\star$	$\star$	$\star$

dont on peut compléter la dernière ligne en utilisant le fait que les colonnes sont orthogonales :

$\mathfrak{S}_4$	1	6	8	6	3
	Id	(12)	(123)	(1234)	(12)(34)
χ_{triv}	1	1	1	1	1
χ_{sign}	1	−1	1	−1	1
χ_{V_0}	3	1	0	−1	−1
$\chi_{V_0}\chi_{\text{sign}}$	3	−1	0	1	−1
χ_V	2	0	−1	0	2

Comment déterminer cette dernière représentation irréductible (V,ρ) ? L'astuce est de noter que $\rho((12)(34))$ est de trace 2, donc c'est l'identité. La représentation ρ se factorise donc par la surjection $\mathfrak{S}_4 \twoheadrightarrow \mathfrak{S}_4/K$, où $K \lhd \mathfrak{S}_4$ est d'ordre 4 (ex. I.5.3.3°). Le groupe $\mathfrak{S}_4/K$ est isomorphe à $\mathfrak{S}_3$. Il y a donc une représentation irréductible de degré 2 (comme on l'a vu plus haut).

Les sous-groupes distingués de $\mathfrak{S}_4$ sont $\mathfrak{S}_4$, $\mathfrak{A}_4$ (noyau de χ_{sign}), K (noyau de χ_V) et $\{e\}$. Le groupe dérivé est $\mathfrak{A}_4$ (noyau de χ_{sign}) et le centre est trivial puisque par exemple $\{\sigma \in \mathfrak{S}_4 \mid |\chi_{V_0}(\sigma)| = \chi_{V_0}(\text{Id}) = 3\} = \{\text{Id}\}$.

Remarque 2.13. — Cette discussion reste valable sur tout corps $\mathbf{K}$ de caractéristique autre que 2 et 3 : $\mathfrak{S}_4$ a encore, à isomorphisme près, 5 classes de représentations irréductibles. Sur un corps de caractéristique 2, il n'y en a plus que 2, à savoir $\mathbf{K}_{\text{triv}}$ et V ; en caractéristique 3, il y en a 4, à savoir toutes celles de la table ci-dessus à l'exception de V (qui devient isomorphe à $\mathbf{K}_{\text{triv}} \oplus \mathbf{K}_{\text{sign}}$).

Le groupe $\mathfrak{S}_5$. — On a (prop. I.2.8) 7 classes de conjugaison, correspondant aux partitions (11111) (classe de Id), (1112) (classe d'une transposition, de cardinal 10), (113) (classe d'un 3-cycle, de cardinal 20), (14) (classe d'un 4-cycle, de cardinal 30), (5) (classe d'un 5-cycle, de cardinal 24), (122) (classe d'une double transposition, de cardinal 15) et (23) (de cardinal 20) de 5, donc 7 représentations irréductibles. D'autre part, on a $D(\mathfrak{S}_5) = \mathfrak{A}_5$ (prop. I.5.9), donc il y a exactement deux représentations irréductibles de dimension 1, la représentation triviale $\mathbf{C}_{\text{triv}}$ et la signature $\mathbf{C}_{\text{sign}}$.

On a aussi la représentation de dimension 4 de $\mathfrak{S}_5$ dans $V_0 = \{(x_1,\dots,x_5) \in \mathbf{C}^5 \mid x_1+\cdots+x_5 = 0\}$ dont le caractère prend les valeurs 4, 2, 1, 0, −1, 0, −1. On calcule $\langle \chi_{V_0}, \chi_{V_0}\rangle = 1$, de sorte que V_0 est irréductible (prop. 2.8). La représentation $V_0 \otimes \mathbf{C}_{\text{sign}}$ est aussi irréductible (ex. 1.4.4°).

Si V est une représentation de G, on a vu que la représentation $V \otimes V$ se scinde en $S^2V \oplus \bigwedge^2 V$. Le lemme suivant nous permet de calculer les caractères.

Lemme 2.14. — *On a* $\chi_{\bigwedge^2 V}(g) = \frac{1}{2}\big(\chi_V(g)^2 - \chi_V(g^2)\big)$ *et* $\chi_{S^2V}(g) = \frac{1}{2}\big(\chi_V(g)^2 + \chi_V(g^2)\big)$.

Démonstration. — Les $\rho(g)$ étant d'ordre fini, ils sont diagonalisables (leur polynôme minimal est à racines simples). Soit $g \in G$; il existe une base $(e_1,\dots,e_n)$ de V formée de vecteurs propres de $\rho(g)$, avec valeurs propres $\lambda_1,\dots,\lambda_n$. Une base de $\bigwedge^2 V$ est donnée par les $(e_i \wedge e_j)_{1\leqslant i<j\leqslant n}$ et ce sont des vecteurs propres pour $\bigwedge^2\rho(g)$, avec valeurs propres

$(\lambda_i\lambda_j)_{1\leqslant i<j\leqslant n}$. On a donc

$$\chi_{\bigwedge^2 V}(g) = \sum_{1\leqslant i<j\leqslant n} \lambda_i\lambda_j = \frac{1}{2}\Big(\sum_{1\leqslant i\leqslant n}\lambda_i\Big)^2 - \frac{1}{2}\sum_{1\leqslant i\leqslant n}\lambda_i^2.$$

De même, les valeurs propres de $S^2\rho(g)$ sont les $(\lambda_i\lambda_j)_{1\leqslant i\leqslant j\leqslant n}$ et

$$\chi_{S^2V}(g) = \sum_{1\leqslant i\leqslant j\leqslant n} \lambda_i\lambda_j = \frac{1}{2}\Big(\sum_{1\leqslant i\leqslant n}\lambda_i\Big)^2 + \frac{1}{2}\sum_{1\leqslant i\leqslant n}\lambda_i^2.$$

Le lemme en résulte. □

On en déduit les valeurs du caractère $\chi_{\bigwedge^2 V_0}$ et on vérifie que cette représentation est irréductible.

On a donc déjà la table de caractères partielle (on note l'isomorphisme de représentations $\bigwedge^2 V_0 \simeq \bigwedge^2 V_0 \otimes \mathbf{C}_{\text{sign}}$)

$\mathfrak{S}_5$	1	10	20	30	24	15	20
	Id	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
χ_{triv}	1	1	1	1	1	1	1
χ_{sign}	1	−1	1	−1	1	1	−1
χ_{V_0}	4	2	1	0	−1	0	−1
$\chi_{V_0}\chi_{\text{sign}}$	4	−2	1	0	−1	0	1
$\chi_{\bigwedge^2 V_0}$	6	0	0	0	1	−2	0

Il nous reste deux représentations irréductibles à trouver, dont la somme des carrés des dimensions est $120-1-1-16-16-36=50$. Elles sont de dimension >1, donc toutes les deux de dimension 5. Notons l'une d'elles V et soient 5, a_1, a_2, a_3, a_4, a_5, a_6 les valeurs de son caractère. Le caractère de $V\otimes\mathbf{C}_{\text{sign}}$ prend alors les valeurs 5, $-a_1$, a_2, $-a_3$, a_4, a_5, $-a_6$. De deux choses l'une :

- soit les deux représentations manquantes ont $a_1=a_3=a_6=0$ (et chacune est isomorphe à son produit tensoriel avec $\mathbf{C}_{\text{sign}}$) ;
- soit les deux représentations manquantes sont V et $V\otimes\mathbf{C}_{\text{sign}}$.

Dans le premier cas, les colonnes 2 et 4 ne peuvent être orthogonales, donc on est dans le second cas. Les relations d'orthogonalité permettent alors de compléter la table (les calculs sont laissés au lecteur) ; on obtient

$\mathfrak{S}_5$	1	10	20	30	24	15	20
	Id	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
χ_{triv}	1	1	1	1	1	1	1
χ_{sign}	1	−1	1	−1	1	1	−1
χ_{V_0}	4	2	1	0	−1	0	−1
$\chi_{V_0}\chi_{\text{sign}}$	4	−2	1	0	−1	0	1
$\chi_{\bigwedge^2 V_0}$	6	0	0	0	1	−2	0
χ_V	5	1	−1	−1	0	1	1
$\chi_V\chi_{\text{sign}}$	5	−1	−1	1	0	1	−1

Une autre façon de compléter la table est de s'intéresser au caractère χ de la représentation S^2V_0. Il prend les valeurs (lemme 2.14) 10, 4, 1, 0, 0, 2, 1 donc

$$\langle\chi,\chi\rangle = \frac{1}{120}(100\times 1+16\times 10+4\times 15+1\times 20) = 3.$$

Cette représentation est donc somme de 3 représentations irréductibles. Comme elle est de dimension 10, ces représentations sont nécessairement de dimension 1, 4 et 5 ; on note cette dernière V. Sans même calculer $\langle\chi,\chi_{\text{triv}}\rangle$, on voit que c'est strictement positif, donc $\mathbf{C}_{\text{triv}}$ intervient dans S^2V_0 (cela résulte aussi de l'exerc. 2.12, puisque V_0 est en fait une représentation réelle). On calcule aussi $\langle\chi,\chi_{V_0}\rangle = 1$, donc $\chi = \chi_{\text{triv}}+\chi_{V_0}+\chi_V$, d'où on déduit χ_V. On voit ensuite $\chi_V \neq \chi_V\chi_{\text{sign}}$ et on complète la table.

Les sous-groupes distingués de $\mathfrak{S}_5$ sont $\mathfrak{S}_5$, $\mathfrak{A}_5$ (noyau de χ_{sign}) et $\{e\}$. Le groupe dérivé est $\mathfrak{A}_5$ (noyau de χ_{sign}) et le centre est trivial puisque par exemple $\{\sigma\in\mathfrak{S}_5 \mid |\chi_{V_0}(\sigma)| = \chi_{V_0}(\text{Id}) = 4\} = \{\text{Id}\}$.

Remarques 2.15. — 1° Il reste vrai que pour tout $n\geqslant 1$, la table des caractères du groupe $\mathfrak{S}_n$ est à coefficients entiers (mais ce n'est pas le cas pour $\mathfrak{A}_n$; *cf.* exerc. 2.17 et 2.18).

2° Dans les exemples précédents, on remarque que la dimension d'une représentation irréductible divise toujours l'ordre du groupe. C'est un fait général qui sera démontré dans le th. 3.6. On voit aussi que le caractère d'une représentation irréductible de dimension $\geqslant 2$ prend toujours la valeur 0. C'est un fait général qui sera (presque) démontré dans l'exerc. 3.9.

4° On trouve ces tables de caractères dans la littérature scientifique pour les chimistes. Les notations sont différentes : le groupe D_n est noté C_{nv} et la table des caractères de $D_3 = \mathfrak{S}_3$ apparaît ainsi

	E	$3s_v$	$2C_3$
A_1	1	1	1
A_2	1	−1	1
E	2	0	−1

La notation $3s_v$ indique qu'il y a 3 éléments dans la classe de conjugaison et s_v signifie qu'elle contient des symétries par rapport à un plan vertical (les éléments de $D_3 = \mathfrak{S}_3$ sont interprétés comme les symétries d'un triangle équilatéral situé dans un plan horizontal). La notation $2C_3$ indique qu'il y a 2 éléments dans la classe de conjugaison et C_m correspond à des rotations d'angle $2\pi/m$.

Les lettres A et B indiquent des représentations (irréductibles) de dimension 1, E des représentations de dimension 2 et T des représentations de dimension 3.

Terminons avec la preuve d'une propriété vue dans des cas particuliers dans les exemples.

Proposition 2.16. — *La représentation de $\mathfrak{S}_n$ sur l'espace vectoriel*

$$V_0 = \{(x_1,\dots,x_n)\in\mathbf{C}^n \mid x_1+\cdots+x_n = 0\}$$

est irréductible.

Démonstration. — Par la prop. 2.8, cette représentation est irréductible si et seulement si $\langle \chi_{V_0}, \chi_{V_0} \rangle = 1$. Comme la représentation de permutation $\mathbf{C}^n$ est somme de V_0 et de la représentation triviale de dimension 1, il suffit de montrer que le caractère χ de la représentation de permutation vérifie $\langle \chi, \chi \rangle = 2$.

On a vu dans l'ex. 2.1.3° que $\chi(g)$ est le nombre de points fixes de la permutation $g \in \mathfrak{S}_n$. Pour tout $a \in \{1, \dots, n\}$, posons $g_a = 0$ si $g(a) \neq a$, et $g_a = 1$ si $g(a) = a$. On a donc

$$\begin{aligned} \langle \chi, \chi \rangle &= \frac{1}{n!} \sum_{g \in \mathfrak{S}_n} \Big(\sum_{a=1}^{n} g_a \Big)^2 \\ &= \frac{1}{n!} \sum_{1 \leqslant a,b \leqslant n} \sum_{g \in \mathfrak{S}_n} g_a g_b \\ &= \frac{1}{n!} \sum_{1 \leqslant a \leqslant n} \sum_{g \in \mathfrak{S}_n} g_a + \frac{2}{n!} \sum_{1 \leqslant a < b \leqslant n} \sum_{g \in \mathfrak{S}_n} g_a g_b. \end{aligned}$$

Le premier terme de la somme vaut $\frac{1}{n!} \sum_{1 \leqslant a \leqslant n} (n-1)! = 1$ et le second vaut $\frac{2}{n!} \sum_{1 \leqslant a < b \leqslant n} (n-2)! = 1$. La proposition en résulte. □

Exercice 2.17. — Montrer que la table des caractères du groupe alterné $\mathfrak{A}_4$ est donnée par

	1	4	4	3
	Id	(123)	(132)	(12)(34)
χ_{triv}	1	1	1	1
χ	1	ω	ω^2	1
χ^2	1	ω^2	ω	1
χ_{V_0}	3	0	0	-1

où $\omega := \exp(2i\pi/3)$.

Exercice 2.18. — Montrer que la table des caractères du groupe alterné $\mathfrak{A}_5$ est donnée par

	1	20	15	12	12
	Id	(123)	(12)(34)	(12345)	(21345)
χ_{triv}	1	1	1	1	1
χ_1	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_2	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_{V_0}	4	1	0	-1	-1
χ_V	5	-1	1	0	0

Exercice 2.19. — Déterminer la table des caractères du sous-groupe $H_8 := \{\pm 1, \pm I, \pm J, \pm K\}$ du groupe multiplicatif $\mathbf{H}^\times$ des quaternions (*cf.* § II.11). Remarquer que c'est la même que celle du groupe D_4.

Exercice 2.20. — Déterminer la table des caractères du groupe $\mathrm{SL}_2(\mathbf{F}_3)$ (*cf.* exerc. I.2.12) (*Indication :* les 7 classes de conjugaison sont celles de $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (cardinal 1), de $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ (cardinal 1), de $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (cardinal 6), de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (cardinal 4), de $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ (cardinal 4), de $\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$ (cardinal 4) et de $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ (cardinal 4)).

Exercice 2.21. — Déterminer la table des caractères du groupe $T_3(\mathbf{F}_3)$ des matrices 3×3 triangulaires supérieures, avec des 1 sur la diagonale, à coefficients dans $\mathbf{Z}/3\mathbf{Z}$ (*cf.* ex. I.2.19).

Exercice 2.22. — On rappelle que le groupe $SL_2(\mathbf{F}_3)$ est de cardinal 24 et qu'il y a 7 classes de conjugaison (exerc. I.2.10) : celle de $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ (cardinal 1), celle de $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ (cardinal 1), celle de $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ (cardinal 4), celle de $\begin{pmatrix}1&-1\\0&1\end{pmatrix}$ (cardinal 4), celle de $\begin{pmatrix}-1&-1\\0&-1\end{pmatrix}$ (cardinal 4), celle de $\begin{pmatrix}-1&1\\0&-1\end{pmatrix}$ (cardinal 4) et celle de $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ (cardinal 6)).

Déterminer la table des caractères du groupe $SL_2(\mathbf{F}_3)$.

Exercice 2.23. — Soit $\mathbf{F}_q$ un corps fini et soit G le groupe des bijections de $\mathbf{F}_q$ de la forme $x\mapsto ax+b$, avec $a\in\mathbf{F}_q^\times$ et $b\in\mathbf{F}_q$. Il est donc de cardinal $q(q-1)$.
a) Montrer que G a $q-1$ représentations complexes de dimension 1 (*Indication :* utiliser le morphisme de groupes de G vers $\mathbf{F}_q^\times$ donné par a).
b) Montrer que G a q classes de conjugaison. En déduire que G a exactement q représentations complexes irréductibles.
c) En déduire que G a exactement une autre représentation complexe irréductible que celles décrites en a) et que cette représentation est de dimension $q-1$. Décrire explicitement cette représentation (*Indication :* on pourra composer l'action de G sur $\mathbf{F}_q$ avec la représentation de permutation de $\mathfrak{S}_q=\mathrm{Bij}(\mathbf{F}_q)$ sur $\mathbf{C}^q$).

Exercice 2.24. — Considérons la représentation de permutation de $\mathfrak{S}_n$ sur l'espace vectoriel $V=\mathbf{C}^n$ et sa sous-représentation irréductible (prop. 2.16)

$$V_0=\{(x_1,\dots,x_n)\in\mathbf{C}^n \mid x_1+\cdots+x_n=0\}.$$

a) Montrer qu'on a un isomorphisme de représentations $\bigwedge^k V\simeq\bigwedge^k V_0\oplus\bigwedge^{k-1}V_0$.
b) Montrer que chaque représentation $\bigwedge^k V_0$, pour $1\leqslant k\leqslant n-1$, est irréductible (*Indication :* on pourra calculer $\langle\chi_{\bigwedge^k V},\chi_{\bigwedge^k V}\rangle$).

Exercice 2.25. — On fixe un entier $n\geqslant 4$. Pour tout $g\in\mathfrak{S}_n$, on note $\phi(g)$ le nombre de points fixes de la permutation g et on pose, pour tout entier $m\geqslant 0$,

$$\varpi(n,m):=\sum_{g\in\mathfrak{S}_n}\phi(g)^m.$$

a) Calculer $\varpi(n,1)$, $\varpi(n,2)$, $\varpi(n,3)$ et $\varpi(n,4)$ (*Indication :* on pourra s'inspirer de la preuve de la prop. 2.16).
b) Le groupe $\mathfrak{S}_n$ opère sur l'espace vectoriel $V=\mathbf{C}^n$ par permutation des coordonnées. Il opère aussi sur $V\otimes V$ par

$$\forall g\in G\ \ \forall v,w\in V\qquad g\cdot(v\otimes w)=g(v)\otimes g(w).$$

Décomposer cette représentation $V\otimes V$ de $\mathfrak{S}_n$ en somme de représentations irréductibles.
c) Montrer que pour tout m, le quotient $B(n,m):=\varpi(n,m)/n!$ est un entier.
d) Pour $m<n$, montrer la relation $B(n,m+1):=\sum_{i=0}^m\binom{m}{i}B(n,i)$, avec $B(n,0):=1$. En particulier, $B(n,m)$ est indépendant de n.

3. Propriétés d'intégralité

Dans cette section, on suppose G *fini et* **K** *algébriquement clos de caractéristique 0.* Il contient alors **Q** comme sous-corps.

Dans cette section on démontre que la dimension d'une représentation irréductible (de dimension finie) divise l'ordre du groupe. La démonstration nécessite de connaître quelques propriétés des entiers algébriques, que nous allons maintenant définir.

3.1. Entiers algébriques. —

Définition 3.1. — Un élément de **K** est un entier algébrique s'il est racine d'un polynôme unitaire à coefficients dans **Z**.

Par exemple, toute racine de l'unité est un entier algébrique.

Remarque 3.2. — Si $x \in \mathbf{Q} \subseteq \mathbf{K}$ est un entier algébrique, $x \in \mathbf{Z}$. En effet, si $x = \frac{r}{s}$ avec $\mathrm{pgcd}(r,s) = 1$, alors $r^n + a_1 r^{n-1} s + \cdots + a_n s^n = 0$ qui implique $s \mid r^n$ donc $s = \pm 1$.

Si $x \in \mathbf{K}$, on note $\mathbf{Z}[x]$ le sous-anneau de **K** engendré par x, c'est-à-dire l'ensemble des $\mathrm{P}(x)$, pour $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$, ou encore le sous-groupe additif de **K** engendré par les puissances positives de x.

Proposition 3.3. — *Soit $x \in \mathbf{K}$. Les propriétés suivantes sont équivalentes :*
(i) *x est un entier algébrique ;*
(ii) *le groupe abélien $\mathbf{Z}[x]$ est de type fini ;*
(iii) *il existe un sous-groupe abélien de type fini de* **K** *contenant* $\mathbf{Z}[x]$.

Démonstration. — L'énoncé (i) implique (ii) : si $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, le groupe abélien $\mathbf{Z}[x]$ est engendré par $1, x, x^2, \ldots, x^{n-1}$.

Le passage de (ii) à (iii) est évident. Montrons que (iii) implique (i). Par la prop. I.3.2.2°, $\mathbf{Z}[x]$, qui est un sous-groupe d'un groupe abélien de type fini, est encore un groupe de type fini. Soit $\{\mathrm{P}_1(x), \ldots, \mathrm{P}_r(x)\}$ un ensemble de générateurs. Si $d := \max_{1 \leqslant i \leqslant r} \deg(\mathrm{P}_i)$, l'ensemble $\{1, x, \ldots, x^d\}$ engendre aussi $\mathbf{Z}[x]$. Comme $x^{d+1} \in \mathbf{Z}[x]$, on peut l'écrire comme combinaison linéaire à coefficients entiers de $1, x, \ldots, x^d$. Cela donne un polynôme unitaire de degrés $d+1$ à coefficients entiers qui annule x, de sorte que x est un entier algébrique. □

Corollaire 3.4. — *L'ensemble des entiers algébriques de* **K** *est un sous-anneau de* **K**.

Démonstration. — Si x et y sont des entiers algébriques, $\mathbf{Z}[x]$ est engendré (comme groupe abélien) par $1, x, \ldots, x^r$, et $\mathbf{Z}[y]$ par $1, y, \ldots, y^s$. Alors le groupe (abélien) $\mathbf{Z}[x,y]$ est engendré par les $x^i y^j$ pour $0 \leqslant i \leqslant r$ et $0 \leqslant j \leqslant s$, donc est de type fini. Or il contient $\mathbf{Z}[x-y]$ et $\mathbf{Z}[xy]$, donc $x-y$ et xy sont aussi des entiers algébriques par la proposition. □

Par exemple, les valeurs des caractères des représentations (de dimension finie) de G sont des entiers algébriques, puisque ce sont des sommes de racines de l'unité.

3.2. Propriété de la dimension des représentations. — On peut maintenant passer à la démonstration que la dimension d'une représentation irréductible (de dimension finie) divise l'ordre du groupe.

Lemme 3.5. *— Soit* C *une classe de conjugaison de* G *et soit* (V,ρ) *une représentation irréductible de* G. *Alors* $\frac{|C|\chi_\rho(C)}{\dim(V)}$ *est un entier algébrique.*

Démonstration. — Le lemme 2.5.2° appliqué à la fonction caractéristique $f = \mathbf{1}_{C^{-1}}$ de la classe $C^{-1} := \{g^{-1} \mid g \in C\}$ fournit un endomorphisme $v := |G|(\mathbf{1}_{C^{-1}})_\rho = \sum_{g\in C}\rho(g)$ qui est l'homothétie de V de rapport

$$\lambda := \frac{|G|\langle \mathbf{1}_{C^{-1}}, \chi_\rho\rangle}{\dim(V)} = \frac{|C|\chi_\rho(C)}{\dim(V)}.$$

Considérons maintenant la représentation régulière $\rho_R : G \to GL(\mathbf{K}^G)$. Dans la base canonique $(\varepsilon_g)_{g\in G}$ de $\mathbf{K}^G$, la matrice de chaque endomorphisme $\rho_R(g)$ est une matrice de permutation, donc elle est en particulier à coefficients entiers. Il en est de même pour l'endomorphisme $u = \sum_{g\in C}\rho_R(g)$ de $\mathbf{K}^G$. Mais $\mathbf{K}^G$ contient comme sous-représentation toutes les représentations irréductibles de G, donc en particulier V.

La restriction de u à V est alors l'endomorphisme v défini plus haut, qui est une homothétie de rapport λ. On en déduit que λ est valeur propre de u, donc est racine de son polynôme caractéristique, qui est unitaire à coefficients entiers. C'est donc un entier algébrique. □

Théorème 3.6. *— On suppose* G *fini et* **K** *algébriquement clos de caractéristique 0. Si* V *est une représentation irréductible de* G, *on a* $\dim(V) \mid |G|$.

Démonstration. — Si χ est le caractère de V, on a $1 = \langle\chi,\chi\rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})\chi(g)$ (th. 2.3). Notons $C_1,\dots,C_\ell$ les classes de conjugaison de G. On a alors

$$\begin{aligned}\frac{|G|}{\dim(V)} &= \frac{1}{\dim(V)}\sum_{g\in G}\chi(g^{-1})\chi(g)\\ &= \frac{1}{\dim(V)}\sum_{i=1}^{\ell}|C_i|\chi(C_i^{-1})\chi(C_i)\\ &= \sum_{i=1}^{\ell}\frac{|C_i|\chi(C_i)}{\dim(V)}\chi(C_i^{-1}).\end{aligned}$$

Comme les $\chi(C_i^{-1})$ sont des entiers algébriques, on conclut par le lemme 3.5 et le cor. 3.4 que le rationnel $\frac{|G|}{\dim(V)}$ est un entier algébrique, donc un entier (rem. 3.2 ; c'est ici que sert l'hypothèse $\mathrm{car}(\mathbf{K}) = 0$). □

Remarque 3.7. *—* La conclusion du théorème n'est plus vraie en général si le corps **K** n'est pas algébriquement clos : si $\mathbf{K} = \mathbf{R}$, la représentation de $\mathbf{Z}/3\mathbf{Z}$ comme groupe des rotations de $\mathbf{R}^2$ préservant un triangle équilatéral centré à l'origine, donc envoyant 1 sur la matrice $\begin{pmatrix}-1/2 & -\sqrt{3}/2\\ \sqrt{3}/2 & -1/2\end{pmatrix}$, est irréductible mais sa dimension, 2, ne divise pas l'ordre du groupe, 3. Sur **C**, cette représentation se scinde en somme directe de deux représentations de dimension 1.

En revanche, elle reste vraie en caractéristique $p > 0$ si $p \nmid |G|$. Mais il existe une représentation irréductible dans $\bar{\mathbf{F}}_{13}^5$ (où $\bar{\mathbf{F}}_{13}$ est une clôture algébrique de $\mathbf{F}_{13}$) du groupe $SL_2(\mathbf{F}_{13})$, d'ordre $2^3 \cdot 3 \cdot 7 \cdot 13 = 2184$ divisible par la caractéristique, 13, mais pas par la dimension, 5.

La contrainte donnée par le théorème est très forte. Par exemple, en combinant avec la prop. 2.8, on déduit qu'un groupe d'ordre p^2 ne peut avoir que des représentations irréductibles de dimension 1, donc est abélien (prop. 2.9). On retrouve ainsi le cor. I.2.15.1°.

On peut raffiner un peu le th. 3.6.

Théorème 3.8. — *On suppose* G *fini et* $\mathbf{K}$ *algébriquement clos de caractéristique 0. Si* V *est une représentation irréductible de* G, *on a* $\dim(V) \mid [G : Z(G)]$.

Démonstration (J. Tate). — Le groupe $G^m = G \times \cdots \times G$ a une représentation ρ_m dans $V^{\otimes m}$ donnée par

$$\rho_m(g_1, \ldots, g_m) = \rho(g_1) \otimes \cdots \otimes \rho(g_m).$$

Son caractère est (exerc. III.1.5)

$$\chi_m(g_1, \ldots, g_m) = \chi(g_1) \cdots \chi(g_m),$$

donc $\langle \chi_m, \chi_m \rangle = 1$ et ρ_m *est irréductible* (prop. 2.8).

Si $g_i \in Z(G)$, alors $\rho(g_i)$ commute à tous les $\rho(g)$. C'est donc un endomorphisme de la représentation (V, ρ), c'est-à-dire une homothétie $\lambda_i \mathrm{Id}_V$ (lemme de Schur 1.10). Si en outre $g_1 \cdots g_m = e$, alors $\mathrm{Id}_V = \rho(e) = \rho(g_1) \cdots \rho(g_m) = \lambda_1 \cdots \lambda_m \mathrm{Id}_V$ et $\lambda_1 \cdots \lambda_m = 1_{\mathbf{K}}$, d'où $\rho_m(g_1, \ldots, g_m) = \mathrm{Id}_{V^{\otimes m}}$. Soit

$$S = \{(g_1, \ldots, g_m) \in Z(G)^m \mid g_1 \cdots g_m = e\}.$$

C'est un sous-groupe distingué de G^m et on peut factoriser la représentation ρ_m en

$$\begin{array}{ccc} G^m & \xrightarrow{\rho_m} & GL(V^{\otimes m}) \\ \downarrow & \nearrow_{\hat{\rho}_m} & \\ G^m/S, & & \end{array}$$

où $\hat{\rho}_m$ est encore irréductible. Par le th. 3.6, $\dim(V^{\otimes m}) = (\dim(V))^m$ divise $|G^m/S| = \frac{|G|^m}{|Z(G)|^{m-1}}$, donc pour tout $m \geqslant 1$,

$$|Z(G)|^{m-1} \left| \left(\frac{|G|}{\dim(V)} \right)^m, \quad \text{qui implique} \quad |Z(G)| \left| \frac{|G|}{\dim(V)} \right. . \right.$$

□

On peut généraliser ce résultat en montrant que le degré de toute représentation irréductible divise l'indice de tout sous-groupe abélien distingué dans G.

Exercice 3.9. — Soit G un groupe fini et soit χ le caractère d'une représentation irréductible complexe ρ de G. On pose

$$N(\chi) := \prod_{g \in G} |\chi(g)|^2.$$

On admettra que $N(\chi)$ est un entier [2].
a) Montrer $N(\chi) \leqslant 1$, avec égalité si et seulement si $\dim(\rho) = 1$ (*Indication :* on pourra comparer moyenne géométrique et moyenne arithmétique).
b) En déduire que si $\dim(\rho) \geqslant 2$, il existe $g \in G$ tel que $\chi(g) = 0$.

2. La théorie de Galois nous dit $N(\chi) \in \mathbf{Q}$. D'autre part, $N(\chi) := \prod_{g \in G} \chi(g)\chi(g^{-1})$ est un entier algébrique. C'est donc un entier.