L3
ALGÈBRE 1
NOTES DE COURS

11 septembre 2012

L3
ALGÈBRE 1
NOTES DE COURS

TABLE DES MATIÈRES

Références bibliographiques

On pourra s'appuyer utilement sur les ouvrages suivants :

Daniel Perrin *Cours d'algèbre* (Chapitres 1, 2) : l'ouvrage le plus accessible
Jean Dieudonné *La géométrie des groupes classiques* (Chapitre 2) : tout sur les groupes classiques, plus difficile à lire
Anthony Knapp *Basic Algebra* (Tous chapitres) : très bon manuel, disponible en ligne depuis l'École à `http://www.springerlink.com/content/k7g576/`
Jean-Pierre Serre *Représentations linéaires des groupes finis* (Chapitre 4) : référence sur le chapitre 4

CHAPITRE 1

GROUPES

1.1. Généralités sur les groupes

1.1.1. Groupes et morphismes. — Un **groupe** G est la donnée d'un ensemble G, muni d'une loi de composition

$$\mathrm{G} \times \mathrm{G} \longrightarrow \mathrm{G}, \quad (g,h) \longmapsto gh,$$

satisfaisant les propriétés suivantes :

1° associativité : pour tous $g_1, g_2, g_3 \in \mathrm{G}$, $(g_1 g_2) g_3 = g_1 (g_2 g_3)$;

2° existence d'un élément neutre (nécessairement unique) : il existe $e \in \mathrm{G}$, tel que $ge = eg = g$ pour tout $g \in \mathrm{G}$;

3° inverse : tout élément $g \in \mathrm{G}$ admet un inverse (nécessairement unique), c'est-à-dire un élément $g^{-1} \in \mathrm{G}$ tel que $gg^{-1} = g^{-1}g = e$.

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

Un **morphisme de groupes** est la donnée d'une application $f : \mathrm{G}_1 \to \mathrm{G}_2$ entre deux groupes, satisfaisant, pour tous $g, h \in \mathrm{G}$,

$$f(gh) = f(g) f(h).$$

Si f est bijective, alors f^{-1} est aussi un morphisme et on dit que f est un **isomorphisme**. Si en outre $\mathrm{G}_1 = \mathrm{G}_2 = \mathrm{G}$, alors on dit que f est un automorphisme de G.

Exemples. — 1° $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ sont des groupes ; la même chose reste vraie en remplaçant $\mathbb{R}$ par le corps des complexes $\mathbb{C}$, ou plus généralement par n'importe quel corps [1] $\mathbb{K}$; encore plus généralement, pour un anneau commutatif A, on a le groupe multiplicatif $(\mathrm{A}^\times, *)$ des unités de A (les éléments de A inversibles dans A).

2° L'application exponentielle est un morphisme de groupes, $\exp : (\mathbb{C}, +) \to (\mathbb{C}^*, \times)$.

3° $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe d'ordre n (l'**ordre d'un groupe fini** G est son cardinal, noté $|\mathrm{G}|$).

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

4° Le *groupe diédral* D_n des symétries et rotations du plan préservant un polygone régulier à n côtés est un groupe d'ordre $2n$.

5° Le *groupe symétrique* S_n des bijections d'un ensemble à n éléments est un groupe d'ordre $n!$

6° Le groupe orthogonal $\mathrm{O}(n,\mathbb{R})$ des transformations orthogonales de $\mathbb{R}^n$.

7° Si $\mathbb{K}$ est un corps, alors les matrices inversibles $n\times n$ à coefficients dans $\mathbb{K}$ forment le **groupe général linéaire** $\mathrm{GL}(n,\mathbb{K})$; le déterminant $\det : \mathrm{GL}(n,\mathbb{K}) \to \mathbb{K}^*$ est un morphisme ; si E est un $\mathbb{K}$-espace vectoriel de dimension n, alors le groupe des applications linéaires bijectives de E dans E est isomorphe à $\mathrm{GL}(n,\mathbb{K})$.

8° Plus généralement, si A est un anneau commutatif, alors on peut former le groupe $\mathrm{GL}(n,\mathrm{A})$ des matrices inversibles à coefficients dans A : il s'agit exactement des matrices M telles que $\det \mathrm{M} \in \mathrm{A}^\times$; par exemple le groupe $\mathrm{GL}(n,\mathbb{Z})$ est constitué des matrices à coefficients entiers, de déterminant ± 1.

9° Si G_1 et G_2 sont deux groupes, alors on peut former un groupe appelé **produit direct** $\mathrm{G}_1 \times \mathrm{G}_2$, en munissant ce produit de la loi interne $(g_1,g_2)(h_1,h_2) = (g_1h_1, g_2h_2)$.

10° L'ensemble des automorphismes d'un groupe G, muni de la composition, est un groupe noté $\mathrm{Aut}\,\mathrm{G}$.

1.1.2. Sous-groupes, générateurs. — Une partie H d'un groupe G est appelée un **sous-groupe** 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 $h_1h_2 \in \mathrm{H}$;

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

Exemples. — 1° L'intersection de sous-groupes est un sous-groupe.

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

3° $a\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$ pour tout $a \in \mathbb{R}$ (on obtient ainsi tous les sous-groupes non denses).

4° Si $f : \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes, alors le **noyau** et l'**image** de f,

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

sont des sous-groupes de G et G′ respectivement ; le morphisme f est injectif si et seulement si $\ker f = \{e\}$.

5° La signature $\varepsilon : \mathrm{S}_n \to \{\pm 1\}$ est un morphisme, dont le noyau est le *groupe alterné* A_n.

6° Le noyau du déterminant $\det : \mathrm{GL}(n,\mathbb{K}) \to \mathbb{K}^*$ est le **groupe spécial linéaire** des matrices de déterminant 1, il est noté $\mathrm{SL}(n,\mathbb{K})$; exercice : montrer que, si $\mathbb{K} = \mathbb{F}_q$, corps fini à q éléments, alors les ordres de ces groupes sont

$$|\mathrm{GL}(n,\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}), \tag{1}$$

$$|\mathrm{SL}(n,\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-2})q^{n-1}. \tag{2}$$

7° Le noyau du déterminant sur le groupe diédral D_n est le sous-groupe des rotations d'angle multiple de $\frac{2\pi}{n}$.

8° Le **centre** d'un groupe G,

$$\mathrm{Z}(\mathrm{G}) = \{g \in \mathrm{G}, gx = xg \text{ pour tout } x \in \mathrm{G}\}$$

est un sous-groupe de G ; le groupe G est abélien si et seulement si Z(G) = G ; par exemple, le centre de $\mathrm{GL}(n,\mathbb{K})$ est constitué des homothéties, et le centre de $\mathrm{SL}(n,\mathbb{K})$ des homothéties de rapport une racine n-ième de l'unité dans le corps $\mathbb{K}$.

9° Si $g \in \mathrm{G}$, on peut considérer le morphisme de groupes

$$\phi_g : \mathbb{Z} \longrightarrow \mathrm{G}, \quad n \longmapsto g^n; \tag{3}$$

l'image de ϕ_g est le plus petit sous-groupe de G contenant g, on l'appelle le *sous-groupe engendré par g* et on le note $\langle g\rangle$; s'il est infini (ce qui se produit si $g^n \neq 1$ pour tout $n \neq 0$), on dit que l'ordre de g est infini, sinon l'**ordre** de g est par définition l'ordre de $\langle g\rangle$.

Ce dernier exemple se généralise de la manière suivante :

1.1.3 Proposition. — *Soit une partie* A *d'un groupe* G. *Alors 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. La seconde construction consiste en la description explicite :

$$\langle \mathrm{A}\rangle = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n},\ n \in \mathbb{N}, x_i \in \mathrm{A}, \epsilon_i = \pm 1\}.$$

□

1.1.4 Proposition. — *Le sous-groupe engendré par un élément* $g \in \mathrm{G}$ *est isomorphe à* $\mathbb{Z}$ *s'il est infini, à* $\mathbb{Z}/n\mathbb{Z}$ *s'il est fini, où* n *est l'ordre de* g.

Démonstration. — Le morphisme ϕ_g considéré en (3) a pour image $\langle g\rangle$. Si l'ordre de g est infini, alors ϕ_g est injectif, donc on obtient un isomorphisme $\phi_g : \mathbb{Z} \to \langle g\rangle$. Si l'ordre de $\langle g\rangle$ est fini, alors $\ker\phi_g = n\mathbb{Z}$, et l'application $\bar{\phi}_g : \mathbb{Z}/n\mathbb{Z} \to \langle g\rangle$, $\bar{m} \mapsto g^m$, est bien définie, est un morphisme de groupes, par définition injectif et surjectif, donc un isomorphisme. □

Une partie A de G est une **partie génératrice** de G, ou engendre G, si $\langle \mathrm{A}\rangle = \mathrm{G}$. On dit que G est un **groupe monogène** s'il est engendré par un seul élément, un **groupe cyclique** s'il est de plus fini.

Exemples. — 1° Le groupe diédral est engendré par la rotation r d'angle $\frac{2\pi}{n}$ et la symétrie s par rapport à l'axe horizontal : alors $srs = r^{-1}$ et $\mathrm{D}_n = \{r^k, 0 \leqslant k \leqslant n-1\} \cup \{sr^k, 0 \leqslant k \leqslant n-1\}$.

2° Voici trois ensembles différents de générateurs pour le groupe symétrique S_n :

– toutes les transpositions ;

– les transpositions (12), (23), …, $((n-1)n)$;

– la transposition (12) et le cycle $(12\cdots n)$.

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

4° Pour $n \geqslant 2$, le groupe orthogonal $\mathrm{O}(n,\mathbb{R})$ est engendré par les *réflexions* (symétries par rapport à un hyperplan), voir Chap. 2.

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

$$x\mathscr{R}y \Longleftrightarrow \exists h \in \mathrm{H},\ y = xh.$$

Les trois propriétés caractéristiques des relations d'équivalence (réflexivité, symétrie, transitivité) se vérifient immédiatement. La classe d'équivalence d'un élément $x \in \mathrm{G}$ est $x\mathrm{H} = \{xh, h \in \mathrm{H}\}$. Les $x\mathrm{H}$ pour $x \in \mathrm{G}$ 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 $\mathrm{H}x = \{hx, h \in \mathrm{H}\}$, 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 $\phi : \mathrm{G} \to \mathrm{G}$, $x \mapsto x^{-1}$, envoie $x\mathrm{H}$ sur $\mathrm{H}x^{-1}$, donc envoie classes à gauche sur classes à droite ; induisant ainsi une bijection

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

Soit $x \in \mathrm{G}$, alors l'application $\mathrm{H} \to \mathrm{G}$, $h \mapsto xh$, induit une bijection

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

En particulier, si H est fini, alors le cardinal d'une classe à gauche $x\mathrm{H}$ est égal à l'ordre de H. Les classes à gauche forment donc une partition de G par des classes de même cardinal, d'où :

***1.1.6 Proposition* (Théorème de Lagrange).** — *Si* G *est fini et* H *est un sous-groupe de* G*, alors*

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

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

En particulier, un groupe d'ordre premier p est nécessairement isomorphe au groupe cyclique $\mathbb{Z}/p\mathbb{Z}$.

1.1.7. Sous-groupes distingués. — Soit $g \in \mathrm{G}$, alors l'application

$$\iota_g : \mathrm{G} \longrightarrow \mathrm{G}, \quad x \longmapsto gxg^{-1},$$

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

$$\iota : \mathrm{G} \longrightarrow \mathrm{Aut\,G}$$

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

On dit qu'un sous-groupe H de G est un **sous-groupe distingué**, ou **sous-groupe normal**, et on note $\mathrm{H} \lhd \mathrm{G}$, s'il est stable par tout automorphisme intérieur, c'est-à-dire : pour tous $g \in \mathrm{G}$ et $h \in \mathrm{H}$, on a $ghg^{-1} \in \mathrm{H}$.

Exemples. — 1° Les sous-groupes triviaux $\{e\}$ et G de G sont distingués.

2° Dans un groupe abélien, tous les sous-groupes sont distingués.

3° Si $f : \mathrm{G} \to \mathrm{G}'$ est un morphisme de groupes, alors $\ker f \lhd \mathrm{G}$ (attention, il est faux en général que l'image soit un sous-groupe distingué) ; plus généralement, si $\mathrm{H}' \lhd \mathrm{G}'$, alors $f^{-1}(\mathrm{H}') \lhd \mathrm{G}$.

1.1.8. Quotient. — Soit H un sous-groupe de G, on souhaite munir G/H d'une structure de groupe telle que la projection $p : G \to G/H$, $x \mapsto xH$, d'un élément sur sa classe à gauche, soit un morphisme de groupes. L'élément neutre de G/H serait nécessairement eH, et donc le noyau de p serait la classe de e, c'est-à-dire H. D'après l'exemple 3 ci-dessus, il faut donc que H soit distingué dans G. Cette condition est suffisante :

1.1.9 Théorème. — *Si* H *est un sous-groupe distingué de* G*, alors il existe sur* G/H *une unique structure de groupe, telle que la projection* $p : G \to G/H$ *soit un morphisme de groupe.*

Il est important de noter que si H est distingué, alors les classes à droite sont égales aux classes à gauche : $xH = Hx$ pour tout $x \in G$, puisque $xHx^{-1} = H$. Ainsi $G/H = H\backslash G$ 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 groupe sur G/H vérifie

$$(xH)(yH) = xyH. \tag{4}$$

La première chose à faire est de vérifier que cette formule ne dépend pas des choix de x et y dans leurs classes : si $x = x'h$ et $y = y'h'$, alors

$$xy = x'hy'h' = x'y'(y'^{-1}hy')h'.$$

Puisque H est distingué, $y'^{-1}hy' \in H$ donc $xyH = x'y'H$. La formule (4) définit donc bien une loi de composition sur G/H. Il est immédiat de vérifier qu'il s'agit d'une loi de groupe. □

Si H est distingué, alors les groupes H, G et G/H s'insèrent dans une **suite exacte de groupes** :

$$1 \longrightarrow H \xrightarrow{i} G \xrightarrow{p} G/H \longrightarrow 1,$$

où $i : H \to G$ est l'inclusion du sous-groupe H dans G. Cela signifie que, dans le diagramme, le noyau de chaque flèche est égal à l'image de la flèche précédente (vérifier ce que cela veut dire à chacun des 5 groupes du diagramme, où 1 désigne le groupe $\{e\}$).

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

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle p}\downarrow & \nearrow_{\hat{f}} & \\ G/H & & \end{array}$$

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

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

1.1.11 Corollaire. — *Si $f : G \to G'$ est un morphisme de groupes, alors $\hat{f} : G/\ker f \to \operatorname{im} f$ est un isomorphisme.*

De manière équivalente, si on a une suite exacte de groupes

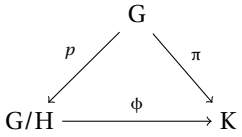
$$1 \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow 1,$$

alors $\hat{g} : G/H \to K$ est un isomorphisme.

Noter l'abus de notation très courant : on a écrit G/H au lieu de $G/f(H)$, car comme f est injective, on peut identifier H à son image $f(H) \subset G$.

Démonstration. — On applique le théorème à $\tilde{f} : G \to \operatorname{im} f$, coïncidant avec f mais dont on a restreint le but, et à $H = \ker f$, donc on obtient $\hat{f} : G/\ker f \to \operatorname{im} f$, avec $\ker \hat{f} = \ker f / \ker f = 1$ et $\operatorname{im} \hat{f} = \operatorname{im} \tilde{f} = \operatorname{im} f$. □

Exercice. — La propriété universelle caractérise le quotient : s'il existe (K, π), où K est un groupe et π un morphisme de groupes $G \to K$ tel que $\ker \pi \supset H$, et si (K, π) est universel pour cette propriété (si $\ker f \supset H$, alors il existe un unique morphisme $\hat{f} : K \to G'$ tel que $f = \hat{f} \circ \pi$), alors (K, π) est uniquement isomorphe à $(G/H, p)$, ce qui signifie qu'il existe un unique isomorphisme $\phi : G/H \to K$ rendant le diagramme suivant commutatif :



Exemples. — 1° Le groupe $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par $n\mathbb{Z}$. On peut en déduire les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$: leur image réciproque par la projection $p : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ contenant $n\mathbb{Z}$, donc de la forme $d\mathbb{Z}$ pour $d|n$, donc les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les sous-groupes cycliques engendrés par les entiers d tels que $d|n$.
Dans cet exemple, $\mathbb{Z}/n\mathbb{Z}$ est un anneau, et non seulement la loi additive passe au quotient, mais aussi la loi multiplicative (car $n\mathbb{Z}$ est un idéal : $a(n\mathbb{Z}) \subset n\mathbb{Z}$ pour tout $a \in \mathbb{Z}$), donc $\mathbb{Z}/n\mathbb{Z}$ est un anneau, l'anneau quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

2° Le groupe diédral s'insère dans la suite exacte

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow D_n \xrightarrow{\det} \{\pm 1\} \longrightarrow 1,$$

où le premier groupe est le sous-groupe (cyclique) des rotations de D_n ; ainsi $D_n/(\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$.

3° On a $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$, venant de la suite exacte

$$1 \longrightarrow A_n \longrightarrow S_n \xrightarrow{\varepsilon} \{\pm 1\} \longrightarrow 1.$$

4° Le morphisme $\iota : G \to \operatorname{Aut} G$, défini par $\iota(g)(x) = gxg^{-1}$, a pour noyau le centre Z(G) et image le sous-groupe $\operatorname{Int} G$ des automorphismes intérieurs de G, donc $\operatorname{Int} G \simeq G/Z(G)$.

5° Si $K \subset H$ sont deux sous-groupes distingués de G, alors

$$(G/K)/(H/K) \simeq G/H;$$

en effet, en appliquant la propriété universelle au morphisme $G \to G/H$, on obtient un morphisme $G/K \to G/H$, surjectif, dont le noyau est H/K.

1.1.12. Quotient d'espace vectoriel. — Si E est un $\mathbb{K}$-espace vectoriel, et $F \subset E$ un sous-espace vectoriel, alors en particulier, pour la structure de groupe abélien, F est un sous-groupe de E donc on peut former le quotient E/F. Dans ce cas, la structure de $\mathbb{K}$-espace vectoriel passe aussi au quotient, en définissant pour $x \in E$ la multiplication par le scalaire $\lambda \in \mathbb{K}$ dans E/F par $\lambda(x+F) = (\lambda x)+F$: en effet, si on prend un autre représentant $y = x+f$ ($f \in F$) de la classe de x dans E/F, alors $\lambda y = \lambda x + \lambda f$ représente bien la classe $\lambda x + F \in E/F$, puisque $\lambda f \in F$. La projection

$$p : E \longrightarrow E/F$$

est alors aussi une application linéaire de noyau F, et la propriété de factorisation (théorème 1.1.10) reste valable en remplaçant les morphismes de groupe par des applications linéaires : si $\phi : E \to E'$ est une application linéaire telle que $\ker\phi \supset F$, alors elle se factorise, de manière unique, par une application linéaire $\hat{\phi} : E/F \to E'$ telle que $\phi = \hat{\phi} \circ p$. À nouveau, cette propriété caractérise le quotient.

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

Attention, cette propriété est particulière aux espaces vectoriels : dans le cas des groupes, si $H \lhd G$, alors en général G n'est pas isomorphe au produit $H \times G/H$. Voir § 1.3.

Finalement, en appliquant la propriété de factorisation aux formes linéaires $E \to \mathbb{K}$, on observera l'identification bien utile du dual $(E/F)^*$ avec le sous-espace de E^* des formes linéaires s'annulant sur F : plus précisément, la transposée de p fournit une application linéaire

$$p^t : (E/F)^* \longrightarrow E^*, \quad f \longmapsto f \circ p,$$

dont l'image est constituée exactement des formes linéaires s'annulant sur F, à savoir $F^\perp = \{f \in E^*, \ker f \supset F\}$. On obtient ainsi un isomorphisme

$$p^t : (E/F)^* \xrightarrow{\sim} F^\perp. \tag{5}$$

1.1.13. Groupe dérivé. — Soit G un groupe, $x, y \in G$, alors x et y commutent si $xyx^{-1}y^{-1} = e$. On appelle **commutateur** un élément de G de la forme $xyx^{-1}y^{-1}$, et le groupe engendré par tous les commutateurs,

$$D(G) = \langle xyx^{-1}y^{-1}, x, y \in G \rangle,$$

est appelé **groupe dérivé** de G.

1.1.14 Proposition. *— Le groupe dérivé* D(G) *est un* ***sous-groupe caractéristique*** *de* G, *c'est-à-dire 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* G/H *est abélien, alors* $H \supset D(G)$, *et donc* G/H *est un quotient de* G/D(G).

Démonstration. — L'image du commutateur $xyx^{-1}y^{-1}$ par un automorphisme f est le commutateur $f(x)f(y)f(x)^{-1}f(y)^{-1}$, donc $f(D(G)) = D(G)$.

Puisque $xyx^{-1}y^{-1} \in \mathrm{D(G)}$ 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, alors tous ses commutateurs sont triviaux, donc pour tous $x, y \in \mathrm{G}$, il faut que $xyx^{-1}y^{-1} \in \mathrm{H}$, ce qui impose $\mathrm{D(G)} \subset \mathrm{H}$. □

1.2. Groupes opérant sur un ensemble

1.2.1. Action de groupe. — Une **action** (à gauche) d'un groupe G sur un ensemble X est la donnée d'une application

$$\Phi : \mathrm{G} \times \mathrm{X} \longrightarrow \mathrm{X}, \quad (g, x) \longmapsto g \cdot x,$$

telle que

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

2° pour tous $x \in \mathrm{X}$ et $g, g' \in \mathrm{G}$, on a $g \cdot (g' \cdot x) = (gg') \cdot x$.

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

$$\Phi_e = \mathrm{Id_X}, \quad \Phi_g \circ \Phi_h = \Phi_{gh},$$

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

$$\mathrm{G} \longrightarrow \mathrm{Bij(X)}, \quad g \longmapsto \Phi_g,$$

où Bij(X) est l'ensemble des bijections de X. (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, puisque cela signifie $\Phi_{gg'} = \Phi_{g'} \circ \Phi_g$). Une action à droite $\cdot$ se ramène à une action à gauche $\bullet$ en considérant $g \bullet x = x \cdot g^{-1}$.)

Exemples. — 1° Le groupe symétrique S_n agit sur l'ensemble $\{1, \ldots, n\}$.

2° $\mathrm{GL}(n, \mathbb{K})$ opère sur $\mathbb{K}^n$.

3° $\mathrm{O}(n, \mathbb{R})$ opère sur la sphère $\mathrm{S}^{n-1} \subset \mathbb{R}^n$.

4° $\mathrm{SL}(2, \mathbb{R})$ opère sur le demi-plan de Poincaré, $\mathscr{H} = \{z \in \mathbb{C}, \Im z > 0\}$, par $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot z = \frac{az+b}{cz+d}$.

5° Si H est un sous-groupe de G, alors G opère sur l'ensemble des classes à gauche, G/H, par $g \cdot (x\mathrm{H}) = (gx)\mathrm{H}$.

1.2.2. Orbites. — Soit G un groupe opérant sur X, et $x \in \mathrm{X}$. Le **stabilisateur**, ou **groupe d'isotropie** de x est le sous-groupe de G défini par

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

L'**orbite** de x sous G est $\mathrm{G} \cdot x = \{g \cdot x, g \in \mathrm{G}\}$. L'application

$$\mathrm{G} \longrightarrow \mathrm{G} \cdot x, \quad g \longmapsto g \cdot x,$$

se factorise en une *bijection* entre l'espace des classes à gauche de G_x et l'orbite de x :

$$\mathrm{F}_x : \mathrm{G}/\mathrm{G}_x \xrightarrow{\sim} \mathrm{G} \cdot x. \tag{6}$$

Cette bijection identifie l'action de G sur l'orbite de x avec l'action standard de G sur G/G_x, c'est-à-dire qu'on a l'identité, pour $y \in \mathrm{G} \cdot x$ et $g \in \mathrm{G}$,

$$g \cdot y = \mathrm{F}_x\big(g \cdot \mathrm{F}_x^{-1}(y)\big).$$

L'ensemble des orbites de X sous G est le quotient de X par G, noté G\X. (Le groupe est à gauche pour une action à gauche. Pour une action à droite, l'orbite de x est en bijection avec $G_x\backslash G$ et le quotient est noté X/G.)

L'action de G est **transitive** si G n'a qu'une seule orbite dans X. Par exemple, l'action de G sur G/H par $g\cdot(xH) = (gx)H$ est transitive. C'est le cas général, puisque par (6), si X entier est une orbite, alors l'action de G induit une bijection de G/G_x avec X, pour tout $x \in X$.

Exemples. — 1° Pour l'action de $O(n,\mathbb{R})$ sur $\mathbb{R}^n$, les orbites sont les sphères de rayon $r > 0$, ainsi que $\{0\}$. Le groupe d'isotropie d'un point non nul est $O(n-1)$, donc, par (6), on a une bijection $O(n-1)\backslash O(n) \simeq S^{n-1}$ (c'est en réalité un homéomorphisme si on munit le membre de gauche de la topologie quotient).

2° Le groupe $\mathbb{R}^*$ agit sur $\mathbb{R}^n - \{0\}$, et le quotient est

$$\mathbb{R}^n - \{0\}/\mathbb{R}^* = \{\text{droites réelles de } \mathbb{R}^n\},$$

appelé l'espace projectif réel, et noté $\mathbb{R}P^{n-1}$.

3° Si $\sigma \in S_n$, on considère l'action de $G = \langle\sigma\rangle$ sur $\{1,\dots,n\}$; alors $\{1,\dots,n\}$ est la réunion disjointe des orbites :

$$\{1,\dots,n\} = \cup_1^r O_i;$$

on peut poser

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in O_i, \\ x & x \in O_i; \end{cases}$$

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 retrouve ainsi que toute permutation se décompose de manière unique comme produit de cycles disjoints.

L'action de G est **fidèle** si $\cap_{x\in X} G_x = \{e\}$. Observons que le morphisme $\Phi : G \to \mathrm{Bij}(X)$, induit par l'action, a précisément pour noyau $\cap_{x\in X} G_x$, donc l'action est fidèle si et seulement si Φ est injective. Sinon l'action Φ se factorise :

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

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

***1.2.3 Exemple* (Théorème de Cayley).** — L'action de G sur lui-même par translation à gauche, $g\cdot x = gx$, est fidèle. Si G est fini, on en déduit un morphisme injectif $G \hookrightarrow S_{|G|}$.

1.2.4. Conjugaison. — Il y a une autre action de G sur lui-même, donnée par le morphisme $G \to \mathrm{Aut}G$ qui à g associe l'automorphisme intérieur induit par g : donc $g\cdot x = gxg^{-1}$ (action par **conjugaison**). Dans ce cas, le groupe d'isotropie d'un élément $x \in G$ est appelé le **centralisateur** de x, et noté $C(x)$.

Explicitons cette action dans le cas du groupe symétrique :

1.2.5 Proposition. — *Si* $\sigma \in \mathrm{S}_n$ *est un cycle d'ordre* p*, donc* $\sigma = (a_1 \cdots a_p)$*, et* $\tau \in \mathrm{S}_n$*, alors*

$$\tau\sigma\tau^{-1} = (\tau(a_1) \cdots \tau(a_p)). \tag{7}$$

Tous les cycles d'ordre p *sont conjugués dans* S_n.

Plus généralement, les classes de conjugaison de S_n *sont en bijection avec les partitions de* n *:*

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

Démonstration. — Si $x \notin \{\tau(a_1), \ldots, \tau(a_p)\}$, alors $\tau^{-1}(x) \notin \{a_1, \ldots, a_p\}$ 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 disjoints de longueurs $(k_i)_{i=1,\ldots,r}$, qu'on peut ordonner de sorte que $1 \leqslant k_1 \leqslant \cdots \leqslant k_r$. Alors

$$\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdots (\tau\sigma_r\tau^{-1}) \tag{8}$$

est encore un produit de cycles disjoints de mêmes longueurs $(k_i)_{i=1,\ldots,r}$ 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 (7) et (8), il est évident que deux permutations correspondant à la même partition sont conjuguées. □

De manière générale, la conjugaison préserve toutes les propriétés géométriques d'une transformation. Par exemple, si $\sigma \in \mathrm{O}(3,\mathbb{R})$ est une rotation autour d'une droite D, et $\tau \in \mathrm{O}(3,\mathbb{R})$, alors $\tau\sigma\tau^{-1}$ est une rotation de même angle autour de $\tau(\mathrm{D})$. Ou encore, si $\sigma \in \mathrm{S}_n$ admet un point fixe p, alors $\tau(p)$ est un point fixe de $\tau\sigma\tau^{-1}$. Plus généralement, les stabilisateurs des points d'une orbite sont tous conjugués, comme le lecteur le vérifiera aisément :

1.2.6 Lemme. — *Si* G *agit sur l'ensemble* X*, alors* $\mathrm{G}_{g\cdot x} = g\mathrm{G}_x g^{-1}$ *pour tous* $x \in \mathrm{X}$ *et* $g \in \mathrm{G}$.

1.2.7 Proposition **(Formule des classes)**. — *Si* G *et* X *sont finis, alors*

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

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

Démonstration. — La démonstration est immédiate : X est la réunion disjointe des orbites, et par (6), 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 $g \in \mathrm{G}$, et on note X^{G} l'ensemble des points fixes de X sous G.

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

$$|\mathrm{X}^{\mathrm{G}}| \equiv |\mathrm{X}| \mod p.$$

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

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

1.2.9 Corollaire. — *Si* $|\mathrm{G}| = p^2$ *avec* p *premier, alors* G *est abélien.*

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

Démonstration de la proposition. — Par la formule des classes,

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

Si x n'est pas un point fixe, alors $\mathrm{G}_x \subsetneq \mathrm{G}$, donc $[\mathrm{G} : \mathrm{G}_x] > 1$ et divise $|\mathrm{G}|$ 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 $\mathrm{G}^{\mathrm{G}} = \mathrm{Z}(\mathrm{G})$ donc $|\mathrm{Z}(\mathrm{G})| \equiv |\mathrm{G}| \mod p$, ce qui impose $|\mathrm{Z}(\mathrm{G})| > 1$. □

Démonstration du corollaire. — D'après la proposition, on a $|\mathrm{Z}(\mathrm{G})| = p$ ou p^2. Si $x \in \mathrm{G}$, alors le centralisateur $\mathrm{C}(x)$ de x contient à la fois $\mathrm{Z}(\mathrm{G})$ et x. Si $x \notin \mathrm{Z}(\mathrm{G})$, on déduit que $|\mathrm{C}(x)| \geqslant |\mathrm{Z}(\mathrm{G})| + 1 \geqslant p + 1$, donc $|\mathrm{C}(x)| = p^2$ et $\mathrm{C}(x) = \mathrm{G}$, c'est-à-dire $x \in \mathrm{Z}(\mathrm{G})$: contradiction. Donc il faut toujours que $x \in \mathrm{Z}(\mathrm{G})$, donc $\mathrm{Z}(\mathrm{G}) = \mathrm{G}$ et G est abélien. □

1.2.10. Les théorèmes de Sylow. — Si G est un groupe fini, et p un facteur premier de $|\mathrm{G}|$, écrivons $|\mathrm{G}| = p^\alpha m$, avec $p \nmid m$. Un ***p*-sous-groupe de Sylow** de G (ou, plus brièvement, un p-Sylow) est un sous-groupe d'ordre p^α de G.

1.2.11 Exemple. — Si $\mathrm{G} = \mathrm{GL}(n, \mathbb{F}_p)$, considérons le sous-groupe H des matrices triangulaires supérieures, avec des 1 sur la diagonale (matrices *unipotentes*) :

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

Alors H est un p-Sylow de G. En effet, $|\mathrm{H}| = p^{\frac{n(n-1)}{2}}$, alors que d'après (1), on a $\alpha = \frac{n(n-1)}{2}$.

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

1.2.12 Lemme. — *Si* S *est un p-Sylow de* G *et* $\mathrm{H} \subset \mathrm{G}$*, alors il existe* $g \in \mathrm{G}$ *tel que* $g\mathrm{S}g^{-1} \cap \mathrm{H}$ *soit un p-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 (proposition 1.2.7) assure qu'il existe au moins une classe gS telle que

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

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

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

1° G *contient un p-Sylow ;*

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

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

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

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

Démonstration. — 1° Le groupe G s'injecte dans un groupe symétrique S_N (exemple 1.2.3), lequel s'injecte dans $GL(N,\mathbb{F}_p)$, en envoyant une permutation $\sigma \in S_N$ sur l'application linéaire u_σ permutant les éléments de base $(e_i)_{i=1,\dots,N}$ par σ, donc définie par $u_\sigma(e_i) = e_{\sigma(i)}$. On peut ainsi considérer G comme un sous-groupe de $GL(N,\mathbb{F}_p)$, qui admet un p-Sylow par l'exemple ci-dessus. Par le lemme 1.2.12, G admet un p-Sylow.

2-3° Si $H \subset G$ est un p-groupe et $S \subset G$ un p-Sylow, alors, toujours par le lemme 1.2.12, il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-Sylow de H, donc soit égal à H puisque H est un p-groupe. Donc $H \subset gSg^{-1}$ qui est un p-Sylow. Si en outre H était déjà un p-Sylow, alors il a le même ordre que gSg^{-1}, donc $H = gSg^{-1}$.

4° Soit X l'ensemble des p-Sylow de G. On a donc une action transitive de G sur X par conjugaison, ce qui implique que $|X|$ divise $|G|$. Restreignons en outre l'action de G à un p-Sylow particulier S. Pour montrer $|X| \equiv 1 \mod p$, d'après la proposition 1.2.8, il suffit de montrer que $|X^S| = 1$. En réalité, on va montrer que S est le seul point fixe de l'action de S sur X.

Pour le montrer, introduisons pour un sous-groupe quelconque $H \subset G$ son **normalisateur** défini par

$$N(H) = \{g \in G, gHg^{-1} = H\}. \tag{9}$$

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

$$H \lhd N(H).$$

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 $S \subset N(S')$. Ainsi S et S' sont des p-Sylow de $N(S')$, alors que $S' \lhd N(S')$: donc $S = S'$. □

Les théorèmes de Sylow ont de nombreuses conséquences, voir TD. En particulier :

1.2.15 Corollaire. — *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,* G *admet un élément d'ordre p.*

Démonstration. — En regardant un p-Sylow, il suffit de le montrer pour un p-groupe. Un p-groupe admet évidemment un élément d'ordre p. Comme le centre Z(G) est non trivial, on peut raisonner par récurrence sur α en se ramenant au quotient de G par un sous-groupe d'ordre p de Z(G). □

1.3. Produit semi-direct

1.3.1. Suite exacte scindée et produit semi-direct. — Supposons qu'on ait une suite exacte courte

$$1 \longrightarrow \mathrm{H} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{K} \longrightarrow 1,$$

ce qui est équivalent à dire que $\bar{\mathrm{H}} = i(\mathrm{H})$ est un sous-groupe distingué de G et $\mathrm{K} = \mathrm{G}/\mathrm{H}$. (Dans cette section, par souci de clarté, on va distinguer le groupe H de son image $\bar{\mathrm{H}} \subset \mathrm{G}$ par l'injection i). On dit aussi que G est une **extension** de H par K. On va étudier un cas où l'on peut reconstruire le groupe G à partir de H et de K : on dit que la suite exacte est **scindée** si elle admet une **section**, c'est-à-dire un morphisme

$$r : \mathrm{K} \longrightarrow \mathrm{G}, \quad \text{tel que} \quad p \circ r = \mathrm{Id}_{\mathrm{K}},$$

ce qui peut se traduire par le diagramme commutatif :

$$1 \longrightarrow \mathrm{H} \xrightarrow{i} \mathrm{G} \underset{r}{\overset{p}{\rightleftarrows}} \mathrm{K} \longrightarrow 1$$

Il est équivalent de dire qu'existe un sous-groupe $\bar{\mathrm{K}} \subset \mathrm{G}$ tel que $p|_{\bar{\mathrm{K}}} : \bar{\mathrm{K}} \to \mathrm{K}$ soit un isomorphisme (la relation entre les deux est $\bar{\mathrm{K}} = \mathrm{im}\, r$). Dans ce cas, on a les propriétés suivantes :

- $\bar{\mathrm{K}} \cap \bar{\mathrm{H}} = \{e\}$: en effet, $\mathrm{im}\, i = \bar{\mathrm{H}} = \ker p$;
- l'application $\bar{\mathrm{H}} \times \bar{\mathrm{K}} \to \mathrm{G}$, $(h,k) \mapsto hk$ est une bijection : en effet, tout élément $x \in \mathrm{G}$ s'écrit de manière unique $x = hk$ avec nécessairement $k = r \circ p(x)$ et $h = xk^{-1}$;
- la loi de G s'écrit

$$(hk)(h'k') = (h\,k h' k^{-1})(kk') = (h\phi_k(h'))(kk'),$$
$$(hk)^{-1} = \phi_{k^{-1}}(h^{-1})k^{-1},$$

  où $k \mapsto \phi_k$ définit une application $\mathrm{K} \to \mathrm{Aut}\,\mathrm{H}$, donc une action de K sur H par morphismes de groupe (en fait, par automorphismes intérieurs de G, qui laissent bien sûr stable $\bar{\mathrm{H}}$ puisque $\bar{\mathrm{H}} \lhd \mathrm{G}$).

Réciproquement, étant donnés deux groupes H et K, et une action de K sur H par morphismes de groupes, c'est-à-dire un morphisme

$$\phi : \mathrm{K} \longrightarrow \mathrm{Aut}\,\mathrm{H}, \quad k \longmapsto \phi_k,$$

alors on peut construire le **produit semi-direct** $\mathrm{G} = \mathrm{H} \rtimes \mathrm{K}$ par :

- comme ensemble, $\mathrm{G} = \mathrm{H} \times \mathrm{K}$;
- l'élément neutre de G est (e,e) ;
- la loi de groupe est donnée par $(h,k)(h',k') = (h\phi_k(h'), kk')$.

On vérifie facilement qu'on obtient ainsi un groupe, et qu'en outre, en définissant $i(h) = (h,1)$ et $p(h,k) = k$, on a la suite exacte

$$1 \longrightarrow \mathrm{H} \xrightarrow{i} \mathrm{G} \xrightarrow{p} \mathrm{K} \longrightarrow 1.$$

On retrouve $\bar{\mathrm{H}} = \{(h,e)\}$ et $\bar{\mathrm{K}} = \{(e,k)\}$.

On a finalement démontré la proposition suivante :

1.3.2 Proposition. *— Soit* G *un groupe.*

1° Si G *contient deux sous-groupes* H *et* K *tels que* $\mathrm{H} \lhd \mathrm{G}$, $\mathrm{H} \cap \mathrm{K} = \{e\}$ *et* $\mathrm{G} = \mathrm{HK}$, *alors* $\mathrm{G} \simeq \mathrm{H} \rtimes \mathrm{K}$ *pour l'opération* $k \cdot h = khk^{-1}$.

2° Si on a une suite exacte courte $1 \to H \to G \to K \to 1$ *admettant une section* $r : K \to G$, *alors* $G \simeq H \rtimes K$ *pour l'opération* $k \cdot h = r(k)hr(k)^{-1}$. □

1.3.3 Remarque. — Si $G = H \rtimes K$, alors les propriétés suivantes sont équivalentes (exercice) :

1° l'action de K sur H est triviale ;

2° le produit semi-direct est un produit direct : $G = H \times K$;

3° $\bar{K} \lhd G$.

Exemples. — 1° La suite exacte

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow D_n \xrightarrow{\det} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

est scindée, une section est obtenue en envoyant $1 \in \mathbb{Z}/2\mathbb{Z}$ sur l'une des symétries de D_n, donc $D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

2° La suite exacte

$$1 \longrightarrow A_n \longrightarrow S_n \xrightarrow{\epsilon} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

est scindée, en envoyant $1 \in \mathbb{Z}/2\mathbb{Z}$ sur une transposition, donc $S_n \simeq A_n \rtimes \mathbb{Z}/2\mathbb{Z}$; on remarquera que pour $n = 3$ on dispose d'un autre groupe, $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, s'insérant dans une suite exacte avec $A_3 = \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.

3° On a une suite exacte

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

qui n'est pas scindée : sinon $\mathbb{Z}/4\mathbb{Z}$ serait un produit semi-direct, mais puisqu'abélien, tous ses sous-groupes sont distingués et il serait forcément un produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

4° La suite exacte

$$1 \longrightarrow SL(n,\mathbb{K}) \longrightarrow GL(n,\mathbb{K}) \xrightarrow{\det} \mathbb{K}^* \longrightarrow 1$$

est scindée, en envoyant $\lambda \in \mathbb{K}^*$ sur la matrice diagonale dont le premier coefficient diagonal est λ et les autres 1, donc $GL(n,\mathbb{K}) \simeq SL(n,\mathbb{K}) \rtimes \mathbb{K}^*$.

5° Le groupe $\mathrm{Aff}(\mathbb{R}^n)$ des transformations affines de $\mathbb{R}^n$ admet la suite exacte scindée

$$1 \longrightarrow \mathbb{R}^n \longrightarrow \mathrm{Aff}(\mathbb{R}^n) \longrightarrow GL(n,\mathbb{R}) \longrightarrow 1,$$

où $\mathbb{R}^n$ est le sous-groupe des translations, donc $\mathrm{Aff}(\mathbb{R}^n) = \mathbb{R}^n \rtimes GL(n,\mathbb{R})$.

1.3.4. Automorphismes des groupes cycliques. — Rappelons sans démonstration la proposition suivante, conséquence du théorème de Bezout :

1.3.5 Proposition. — *Soit* $n \in \mathbb{N}^*$, $s \in \mathbb{Z}$. *Alors sont équivalents :*

1° $(s,n) = 1$;

2° *s engendre le groupe additif* $\mathbb{Z}/n\mathbb{Z}$;

3° *s appartient au groupe des unités* $(\mathbb{Z}/n\mathbb{Z})^\times$ *de l'anneau* $\mathbb{Z}/n\mathbb{Z}$.

Notons $\phi(n)$ l'*indicatrice d'Euler* de n,

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \mathrm{card}\{s \in [1,n], (s,n) = 1\}.$$

Si p est premier, alors $\phi(p) = p-1$, plus généralement $\phi(p^\alpha) = p^{\alpha-1}(p-1)$.

1.3.6 Proposition. — *1° Le groupe des automorphismes du groupe additif $\mathbb{Z}/n\mathbb{Z}$ est $(\mathbb{Z}/n\mathbb{Z})^\times$. C'est donc un groupe abélien d'ordre $\phi(n)$.*

2° Si on décompose n en facteurs premiers, $n = \prod p_i^{\alpha_i}$, alors on a un isomorphisme d'anneaux

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z},$$

et un isomorphisme de groupes

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

3° $\phi(n) = \prod p_i^{\alpha_i - 1}(p_i - 1) = n\prod(1 - \frac{1}{p_i})$.

4° $n = \sum_{d|n} \phi(d)$.

Démonstration. — 1° On a un morphisme de groupes

$$(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}\,\mathbb{Z}/n\mathbb{Z}, \quad a \longmapsto (x \mapsto ax),$$

dont l'inverse associe à $f \in \mathrm{Aut}\,\mathbb{Z}/n\mathbb{Z}$ sa valeur $f(1) \in \mathbb{Z}/n\mathbb{Z}$.

2° C'est une conséquence immédiate du :

***1.3.7 Lemme* (Lemme chinois).** — *Si p et q sont premiers entre eux, alors $\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ comme anneaux.*

Le morphisme d'anneau $f : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, donné par $f(n) = (n, n)$, a exactement pour noyau l'idéal $pq\mathbb{Z}$. Il se factorise donc par un morphisme injectif $\hat{f} : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, qui est un isomorphisme puisque les deux membres ont même cardinal. Cela démontre le lemme chinois. (Exercice : calculer explicitement l'inverse). Il est facile de le généraliser à plusieurs facteurs $\mathbb{Z}/n_i\mathbb{Z}$, où les n_i sont premiers entre eux deux à deux.

3° La formule résulte immédiatement de 2° et de $\phi(p^\alpha) = p^{\alpha-1}(p-1)$.

4° Le groupe $\mathbb{Z}/n\mathbb{Z}$ admet exactement un sous-groupe d'ordre d pour chaque $d|n$, cyclique et engendré par $\frac{n}{d}$. Par conséquent, les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les générateurs de ce sous-groupe, donc sont au nombre de $\phi(d)$. On compte alors les éléments de $\mathbb{Z}/n\mathbb{Z}$ suivant leurs ordres possibles, pour obtenir la formule voulue. □

Pour p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. Son groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ est alors cyclique, donc isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$, comme il résulte du résultat plus général suivant :

1.3.8 Proposition. — *Soit $\mathbb{K}$ un corps (commutatif) et G un sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$. Alors G est cyclique.*

Démonstration. — Soit $n = |\mathrm{G}|$. L'observation de base est que si $x \in \mathrm{G}$ alors $x^n = 1$. Comme le polynôme $\mathrm{X}^n - 1$ a au plus n racines dans $\mathbb{K}$, on déduit que G est exactement l'ensemble des racines de $\mathrm{X}^n - 1$.

Par conséquent, un élément de G d'ordre d engendre exactement le sous-groupe $\mathrm{H}_d = \{x \in \mathbb{K}^*, x^d = 1\}$. Donc, ou bien il n'y a pas d'élément d'ordre d dans G, ou bien ce sont les éléments d'ordre d dans le groupe cyclique H_d, qui sont au nombre de $\phi(d)$. Ainsi le nombre ν_d d'éléments d'ordre d dans G est 0 ou $\phi(d)$. Comme $n = \sum_{d|n} \phi(d) = \sum_{d|n} \nu_d$, il faut que $\nu_d = \phi(d)$, en particulier $\nu_n = \phi(n) > 0$, donc G est cyclique. □

On termine d'élucider la structure du groupe d'automorphismes de $\mathbb{Z}/n\mathbb{Z}$ dans la proposition suivante :

1.3.9 Proposition. — *Soit p un nombre premier et $\alpha \geqslant 1$.*

1° Si p est impair, alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

2° Pour $p = 2$, on a $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$, et pour $\alpha \geqslant 3$ on obtient $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. — On a la congruence suivante, pour $k \geqslant 0$:

$$(p+1)^{p^k} \equiv 1 + p^{k+1} \mod p^{k+2}.$$

La démonstration de cette formule est laissée au lecteur. On en déduit :

$$(p+1)^{p^{\alpha-2}} \equiv 1 + p^{\alpha-1} \mod p^\alpha,$$
$$(p+1)^{p^{\alpha-1}} \equiv 1 + p^\alpha \mod p^{\alpha+1},$$

d'où résulte que dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ on a $(p+1)^{p^{\alpha-2}} \neq 1$ mais $(p+1)^{p^{\alpha-1}} = 1$. L'ordre de $p+1$ dans le groupe multiplicatif $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est donc $p^{\alpha-1}$.

Par ailleurs, on dispose d'un générateur x du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$, donc d'ordre $p-1$. Considérant le morphisme d'anneau surjectif $\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, on peut relever x en un élément $\tilde{x} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, dont l'ordre est un multiple de $p-1$. Donc une puissance y de $\tilde{x}$ est d'ordre exactement $p-1$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

On dispose donc dans le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ de l'élément $p+1$ d'ordre $p^{\alpha-1}$ et d'un élément y d'ordre $p-1$. On applique alors le lemme suivant, variante du lemme chinois (la démonstration est laissée en exercice) :

1.3.10 Lemme. — *Si deux éléments a et b d'un groupe G ont des ordres r, s premiers entre eux, et si $ab = ba$, alors ab est d'ordre rs dans G.*

Il résulte du lemme que $(p+1)y$ est d'ordre $(p-1)p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, donc $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

Passons à la seconde partie de la proposition. Elle s'appuie sur la congruence, laissée en exercice :

$$5^{2^k} \equiv 1 + 2^{k+2} \mod 2^{k+3}.$$

Comme ci-dessus, on déduit que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. On considère alors le morphisme de groupes

$$f : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times = \{1, -1\}.$$

Son noyau est d'ordre $2^{\alpha-2}$, et contient 5, d'ordre $2^{\alpha-2}$: il est donc cyclique. On obtient ainsi une suite exacte

$$1 \longrightarrow \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \longrightarrow (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \xrightarrow{f} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

Mais $\mathbb{Z}/2\mathbb{Z}$ se relève en le sous-groupe $\{\pm 1\} \subset (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$, donc la suite est scindée. Puisque $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est abélien, il faut que ce soit un produit direct : $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

La connaissance des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ permet de construire des produits semi-directs. Voici un exemple d'application :

1.3.11 Théorème. — *Soit $p < q$ deux nombres premiers, et G un groupe d'ordre pq. Alors :*

– *ou bien $p \nmid q-1$, et G est cyclique ;*

– *ou bien* $p|q-1$*, alors il y a, à isomorphisme près, deux possibilités pour* G *: un groupe cyclique ou un produit semi-direct* $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Voir TD.

1.4. Groupes abéliens de type fini

Le but de cette section est le théorème 1.4.7 de structure des groupes abéliens de type fini. C'est un cas particulier du théorème de structure des modules de type fini sur un anneau principal, qui sera vu en Algèbre 2, car un groupe abélien est la même chose qu'un $\mathbb{Z}$-module.

1.4.1. Engendrement fini. — Un groupe est de **type fini** s'il possède une partie génératrice finie.

Si G est un groupe abélien de type fini, alors G est engendré par un nombre fini d'éléments : $G = \langle x_1, \dots, x_r \rangle$. Cela signifie que le morphisme de groupes,

$$\mathbb{Z}^r \longrightarrow G, \quad (n_i)_{i=1,\dots,r} \longmapsto \sum_1^r n_i x_i, \tag{10}$$

est surjectif.

1.4.2 Proposition. *— 1° Si on a un morphisme entre deux groupes abéliens,* $f : G \to H$*, tel que* $\ker f$ *et* $\operatorname{im} f$ *soient finiment engendrés, alors* G *est finiment engendré.*

2° Si G *abélien est finiment engendré, alors tout sous-groupe de* G *est finiment engendré.*

Démonstration. — 1° Soient $y_1 = f(x_1), \dots, y_r = f(x_r) \in H$ un ensemble de générateurs pour $\operatorname{im} f$. Soit $x \in G$, alors il existe des entiers n_i tels que $f(x) = \sum_1^r n_i y_i$, donc $x - \sum_1^r n_i x_i \in \ker f$. Fixant un ensemble de générateurs $z_1, \dots, z_s$ pour $\ker f$, on déduit que $x - \sum_1^r n_i x_i = \sum_1^s m_j z_j$, donc G est engendré par la famille finie obtenue en réunissant les (x_i) et les (z_j).

2° On raisonne par récurrence sur le nombre n de générateurs de G. Si G est engendré par n éléments, on a un morphisme surjectif

$$\mathbb{Z}^n \xrightarrow{p} G \longrightarrow 0.$$

Soit $K = p(\mathbb{Z}^{n-1})$ et $f : G \to G/K$ la projection. Soit H un sous-groupe de G : alors $f(H)$ est monogène (sous-groupe de G/K qui est monogène), et $\ker f|_H = H \cap K$ est finiment engendré par l'hypothèse de récurrence, donc H est finiment engendré. □

1.4.3. Groupes abéliens libres de type fini. — Un groupe abélien est **libre** s'il est isomorphe à un produit, fini ou infini, de copies de $\mathbb{Z}$. Un groupe G abélien libre de type fini est donc isomorphe à un produit fini $\mathbb{Z}^r$. Cela signifie qu'il existe $r \in \mathbb{N}$ et des éléments $x_i \in G$ pour $i = 1, \dots, r$, de sorte que le morphisme (10) soit un isomorphisme. Un tel ensemble $(x_i)_{i=1,\dots,r}$ est appelé une base de G. Plus généralement, on dira qu'un ensemble $(x_i)_{i=1,\dots,r}$ d'éléments de G est linéairement indépendant si (10) est injectif.

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

1.4.4 Lemme. — *Soit* A *une matrice $m \times n$ à coefficients dans $\mathbb{Z}$. Alors il existe des matrices* $P \in GL(m,\mathbb{Z})$ *et* $Q \in GL(n,\mathbb{Z})$*, telles que*

$$PAQ^{-1} = \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \end{pmatrix}, \tag{11}$$

où les d_i sont des entiers positifs satisfaisant $d_1|\cdots|d_r$, appelés ***facteurs invariants****. Ils sont entièrement déterminés par* A.

Le lemme montre qu'une matrice à coefficients entiers est déterminée, à équivalence près, non seulement par son rang r (le seul invariant pour les matrices à coefficients dans un corps), mais aussi par les diviseurs d_i.

Admettons pour le moment le lemme 1.4.4. On en déduit assez rapidement tous les théorèmes importants de la théorie.

1.4.5 Théorème. — *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 $(x_i)_{i=1,\dots,n}$, alors toute famille linéairement indépendante d'éléments de G a au plus n éléments. Soit donc une famille $(y_j)_{j=1,\dots,m}$ d'éléments de G : puisque (x_i) est une base, on obtient une matrice à coefficients entiers $A = (A_{ij})$ définie par $y_j = \sum_i A_{ij} x_i$. On peut interpréter A en disant que A est la matrice du morphisme $\mathbb{Z}^m \to G$ qui envoie e_j sur y_j, où $(e_j)_{j=1,\dots,m}$ est la base standard de $\mathbb{Z}^m$. Appliquant le lemme 1.4.4, on déduit qu'existent des matrices P et Q telles que PAQ^{-1} ait la forme (11), c'est-à-dire $PAQ^{-1}e_j = d_j x_j$, ou encore $AQ^{-1}e_j = d_j P^{-1} x_j$. Si $j > n$ on a nécessairement $d_j = 0$, d'où une relation entre les $y_j = Ae_j$. Donc pour que la famille (y_j) soit linéairement indépendante, il faut que $m \leqslant n$. □

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

1° *$(d_1 e_1,\dots,d_r e_r)$ soit une base de* H *;*

2° *on ait les divisibilités $d_1|d_2|\cdots|d_r$.*

Démonstration. — On prend une base (x_i) de G, et un ensemble (y_j) de générateurs de $H \subset G$. Alors chaque y_j se décompose sur la base : $y_j = \sum_i A_{ij} x_i$. Appliquant le lemme 1.4.4, on déduit que dans la base $(e_i = Q(x_i))$ de G, la partie génératrice de H, donnée par les $(P(y_j))$, est donnée par $(d_1 e_1,\dots,d_r e_r, 0,\dots)$. Le théorème s'en déduit immédiatement. □

On déduit du théorème 1.4.6 le théorème de structure suivant :

1.4.7 Théorème. — *Soit* G *un groupe abélien de type fini. Alors il existe des entiers r et s, des entiers naturels $d_1|d_2|\cdots|d_s$, tous uniquement déterminés par* G*, tels que*

$$G \simeq \mathbb{Z}^r \times \left(\times_1^s \mathbb{Z}/d_i\mathbb{Z}\right).$$

Par le lemme chinois, le second morceau du produit s'écrit aussi comme

$$\times_j \mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}, \tag{12}$$

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 s'écrit $d_s = \prod p_{j'}^{\alpha_{j'}}$, on enlève alors les j' de $\{j\}$ pour obtenir d_{s-1} comme le ppcm des $p_j^{\alpha_j}$ restants, etc.

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

$$\mathbb{Z}^n \xrightarrow{f} \mathrm{G} \longrightarrow 0.$$

On applique le théorème 1.4.6 au noyau $\mathrm{H} = \ker f$, donc il existe une base $(e_i)_{i=1,\dots,n}$ de $\mathbb{Z}^n$, telle que $(d_1 e_1, \dots, d_r e_r)$ soit une base de H. Cela identifie H au sous-groupe

$$d_1\mathbb{Z} \times \cdots \times d_r\mathbb{Z} \subset \mathbb{Z}^n.$$

D'où $\mathrm{G} \simeq \mathbb{Z}^n/\mathrm{H} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^{n-r}$.

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

$$\mathrm{T} = \{x \in \mathrm{G}, \exists n \in \mathbb{N}, nx = 0\}$$

est nécessairement le facteur $\times_i \mathbb{Z}/d_i\mathbb{Z}$, donc $\mathrm{G}/\mathrm{T} \simeq \mathbb{Z}^r$ est un groupe abélien libre de rang r, donc r est bien déterminé. Il reste donc à montrer que, pour le groupe fini T, les d_i sont uniquement déterminés, ou, ce qui est équivalent, les facteurs $p_j^{\alpha_j}$ figurant dans (12). En se limitant au sous-groupe des éléments dont l'ordre est une puissance de p (c'est le p-Sylow de T), on est ramené au cas où les $d_j = p^{\alpha_j}$, donc

$$\mathrm{T} = \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\alpha_s}\mathbb{Z}, \quad \alpha_1 \leqslant \cdots \leqslant \alpha_s.$$

Considérons le sous-groupe $\mathrm{T}_j = \{p^j x, x \in \mathrm{T}\}$. Alors $|\mathrm{T}_j| = \prod_{\alpha_i > j} p^{\alpha_i - j}$, et en particulier $|\mathrm{T}_j/\mathrm{T}_{j+1}| = p^{\sharp\{i,\alpha_i>j\}}$. On récupère ainsi les exposants α_j à partir des sous-groupes T_j, complètement déterminés par T. □

1.4.8. Démonstration du lemme 1.4.4. — Commençons par l'unicité des coefficients d_i. Il est clair que d_1 est le pgcd de tous les coefficients de A (les pgcd des coefficients de A et PAQ^{-1} sont égaux), donc est déterminé par A. 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,

$$m_k(\mathrm{PAQ}^{-1}) = m_k(\mathrm{A}), \quad \mathrm{P} \in \mathrm{GL}(m,\mathbb{Z}), \mathrm{Q} \in \mathrm{GL}(n,\mathbb{Z}). \tag{13}$$

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

Démontrons donc (13). Il suffit de montrer que, pour toute matrice P à coefficients entiers,

$$m_k(\mathrm{A}) | m_k(\mathrm{PA}). \tag{14}$$

En effet, si P est inversible, cela implique $m_k(\mathrm{A})|m_k(\mathrm{PA})|m_k(\mathrm{P}^{-1}\mathrm{PA}) = m_k(\mathrm{A})$, 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 (13).

Finalement, on montre directement (14) 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 sur un corps, on fait agir des transformations élémentaires qui peuvent s'interpréter comme la multiplication à droite ou à gauche par une matrice élémentaire. La différence avec le cas d'un corps étant qu'on ne peut pas diviser.

Les opérations disponibles sont donc les suivantes :

– la multiplication à gauche par la matrice $\mathrm{Id}+a\mathrm{E}_{ij}$ permet d'ajouter à la i-ème ligne la j-ème ligne, multipliée par un entier a ;
– la multiplication à droite par la matrice $\mathrm{Id}+a\mathrm{E}_{ij}$ permet d'ajouter à la j-ème colonne la i-ème colonne, multipliée par un entier a ;
– la multiplication à gauche ou à droite par une matrice de transposition permet d'échanger des lignes ou des colonnes.

La méthode utilise une récurrence sur la taille de la matrice.

Soit λ le pgcd 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 λ. Faisons le sur les deux premiers coefficients a_{11} et a_{12} : si $a_{12}=0$, il n'y a rien à faire, sinon, effectuons la division euclidienne $a_{11}=ba_{12}+c$ avec $0\leqslant c<|a_{12}|$; en effectuant la transformation élémentaire dans laquelle la seconde ligne, multipliée par b, est soustraite de la première, puis la permutation de la première et de la seconde ligne, les coefficients (a_{11},a_{12}) sont transformés en (a_{12},c). En itérant, l'algorithme d'Euclide nous indique qu'on finit par arriver au couple $((a_{11},a_{12}),0)$. Il est maintenant clair qu'en répétant ce procédé sur chaque ligne, on arrive à la première colonne souhaitée, $(\lambda 0\cdots 0)$.

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 $(\lambda_2 0\cdots 0)$, 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 plus nuls. Néanmoins on a gagné quelque chose : $\lambda_2\leqslant\lambda_1$, 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 d'ordre (1,1) décroissent, $\lambda_1\geqslant\lambda_2\geqslant\lambda_3\geqslant\cdots$. Donc cette suite se stabilise, à un moment donné, on obtient par exemple une première ligne $(\lambda_n 0\cdots 0)$, de sorte que λ_n soit aussi le pgcd des coefficients de la première colonne, donc divise tous les coefficients de la première colonne. Il suffit alors de retrancher à la i-ème ligne le 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 la matrice diagonale

$$\begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_r \end{pmatrix}, \quad \text{où } \delta_2|\delta_3|\cdots|\delta_r.$$

Dans la construction, il n'y a pas de raison a priori que $\delta_1|\delta_2$. En fait, on peut remplacer le couple (δ_1, δ_2) par (d_1, p_2), où d_1 et p_2 sont les pgcd et ppcm de δ_1 et δ_2 : en effet, par l'application d'une transformation élémentaire, puis du procédé précédent répété deux fois, on obtient successivement (en n'écrivant que les deux premières lignes et colonnes, sur lesquelles les opérations ont lieu)

$$\begin{pmatrix} \delta_1 & \\ & \delta_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} \delta_1 & \\ \delta_2 & \delta_2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_1 & * \\ 0 & * \end{pmatrix} \rightsquigarrow \begin{pmatrix} d_1 & \\ & p_2 \end{pmatrix}$$

où le dernier coefficient est forcément le ppcm p_2 de δ_1 et δ_2, car le déterminant de la matrice reste inchangé (au signe près).

Appliquant le même procédé au couple (p_2, δ_3), on peut le remplacer par (d_2, p_3). Puisque $d_1 = \mathrm{pgcd}(\delta_1, \delta_2)$, $d_2 = \mathrm{pgcd}(p_2, \delta_3)$, et $\delta_2|\delta_3$, on obtient $d_1|d_2$. En itérant le procédé, on remplace les coefficients $(\delta_1, \ldots, \delta_r)$ par $(d_1, \ldots, d_r)$ avec $d_1|\cdots|d_r$. □

1.5. Groupes simples et suites de composition

1.5.1. Groupes simples. — Un groupe G est **simple** si 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.

L'exemple de base d'un groupe simple non abélien est le groupe alterné :

1.5.2 Théorème. — *Pour $n \neq 4$, le groupe alterné A_n est simple.*

Le théorème est faux pour $n = 4$, en effet, le groupe A_4 contient le groupe de Klein des doubles transpositions :

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

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

L'importance historique du théorème réside dans la conséquence que le groupe symétrique S_n n'est pas résoluble (voir § 1.5.4) pour $n \geqslant 5$. Par théorie de Galois, cela implique que l'équation générale de degré $n \geqslant 5$ n'est pas résoluble par radicaux, voir le cours d'Algèbre 2.

1.5.3 Corollaire. — *1° Si $n \neq 4$, les sous-groupes distingués de S_n sont $\{e\}$, A_n et S_n.*
2° Pour $n \geqslant 5$ on a $\mathrm{D}(\mathrm{A}_n) = \mathrm{A}_n$. Pour $n \geqslant 2$ on a $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$.

Démonstration. — La première partie du corollaire est une conséquence immédiate du théorème, puisque si $\mathrm{H} \lhd \mathrm{S}_n$, alors $\mathrm{H} \cap \mathrm{A}_n \lhd \mathrm{A}_n$, donc $\mathrm{H} \cap \mathrm{A}_n = \mathrm{A}_n$ ou $\{e\}$. Pour la seconde partie, on utilise que $\mathrm{D}(\mathrm{A}_n) \lhd \mathrm{A}_n$, donc est égal à $\{e\}$ ou A_n pour $n \neq 4$: mais la première hypothèse signifie que A_n est abélien. De $\mathrm{D}(\mathrm{S}_n) \lhd \mathrm{S}_n$ et $\mathrm{D}(\mathrm{S}_n) \subset \mathrm{A}_n$ (car la signature d'un

commutateur est toujours 1) on déduit le second énoncé pour $n \neq 4$; le cas $n = 4$ est laissé au lecteur. □

Démonstration du théorème. — Pour un sous-groupe distingué H de G, on utilise les deux faits suivants : si $x \in G$ et $y \in H$ alors

- $xyx^{-1} \in H$ (toute la classe de conjugaison de y est dans H) ;
- $xyx^{-1}y^{-1} \in H$ (donne un moyen de construire des éléments de H dans d'autres classes de conjugaison).

La méthode de preuve consiste alors, à partir d'un élément d'un sous-groupe distingué $H \neq \{e\}$ de A_n, à en fabriquer suffisamment pour assurer qu'en réalité $H = A_n$.

Première étape : pour $n \geqslant 5$ tous les 3-cycles sont conjugués dans A_n, et toutes les doubles transpositions sont conjuguées dans A_n. En effet, deux 3-cycles sont toujours conjugués dans S_n, par exemple écrivons $(123) = \sigma c \sigma^{-1}$, avec $\sigma \in S_n$, alors on a aussi $(123) = \sigma' c \sigma'^{-1}$ avec $\sigma' = (45)\sigma$, et au moins l'un des deux éléments σ ou σ' est dans A_n. On déduit que si H contient un 3-cycle, alors il contient tous les 3-cycles, et donc est égal à A_n qui est engendré par les 3-cycles. Le même type de raisonnement s'applique aux doubles transpositions.

Seconde étape : si H contient une double transposition, ou un 5-cycle, alors il contient un 3-cycle car, si $n \geqslant 5$, et $a, b, \ldots, e$ sont distincts,

$$(abc) = (ae)(cd)(ad)(ce)(ab)(de),$$
$$(abd) = (abc)(abcde)(abc)^{-1}(abcde)^{-1}.$$

Dans les deux cas, on en déduit que $H = A_n$. Cela résoud complètement le cas $n = 5$, puisque A_5 ne contient que des doubles transpositions, des 3-cycles et des 5-cycles.

Troisième étape : on montre que si A_{n-1} est simple, alors A_n est simple. On commence par montrer que H contient toujours un élément non trivial envoyant 1 sur lui-même : supposons $\sigma \in H$, avec $\sigma(1) = i \neq 1$, on va corriger σ en un élément $\sigma' \in H$ tel que $\sigma'(1) = 1$: soit $j \notin \{1, i\}$ tel que $\sigma(j) \neq j$, et $l, m \notin \{1, i, j, \sigma(j)\}$. Alors l'élément de H

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

vérifie $\sigma'(1) = 1$ et $\sigma'(j) = l \neq j$. Donc $\sigma' \neq e$ et $\sigma' \in G_1 \cap H$, où

$$G_1 = \{\sigma \in A_n, \sigma(1) = 1\} \simeq A_{n-1}.$$

Ainsi $H \cap G_1 \neq \{e\}$. Or $H \cap G_1 \lhd G_1$ donc, par l'hypothèse de récurrence, $H \cap G_1 = G_1$ et H contient donc un 3-cycle. Donc $H = A_n$. □

1.5.4. Le 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 de sous-groupes emboîtés,

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{e\},$$

telle que $G_i \lhd G_{i-1}$ et G_i/G_{i-1} soit simple.

1.5.5 Exemple. — Le groupe symétrique S_4 admet la suite de composition suivante :

$$S_4 \supset A_4 \supset K \supset \mathbb{Z}/2\mathbb{Z} \supset 1,$$

avec quotient successifs $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$.

Dans cet exemple, tous les quotients simples sont abéliens. Un groupe dont tous les quotients dans une suite de composition sont abéliens est appelé **résoluble**.

Une autre suite de composition $G = G'_0 \supset G'_1 \supset \cdots \supset G'_s = \{e\}$ est dite **équivalente** à la première si $r = s$ et il existe une permutation $\sigma \in S_r$ 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 : il dit ainsi qu'en un certain sens tous les groupes 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 !

***1.5.6 Théorème* (Jordan-Hölder).** — *Tout groupe fini admet une suite de composition. Cette suite est unique, à équivalence près.*

Démonstration. — L'existence d'une suite de composition est simple : on définit G_1 comme un sous-groupe distingué non trivial maximal, alors G/G_1 est simple car un sous-groupe distingué de G/G_1 remonterait 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.

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

1.5.7 Lemme. — *Si* $H_1 \subset G$ *et* $K_1 \subset G$ *sont deux sous-groupes distingués distincts, tels que* G/H_1 *et* G/K_1 *soient simples, alors*

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

Admettons le lemme pour le moment. On raisonne par récurrence : supposons le résultat vrai pour les groupes dont la suite de composition a une longueur inférieure ou égale à $r-1$. Alors, si G a deux suites de composition, $(H_i)_{i\leqslant r}$ et $(K_j)_{j\leqslant s}$, on introduit une suite de composition $(L_k)_{2\leqslant k\leqslant t}$ pour $H_1 \cap K_1$:

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

Compte tenu du lemme, tous les quotients apparaissant dans ce schéma sont simples. Par conséquent, nous avons deux suites de composition pour H_1, à savoir $(H_i)_{2\leqslant i\leqslant r}$ et $(L_k)_{2\leqslant k\leqslant t}$. Par l'hypothèse de récurrence, il faut que $r = t$ et, à permutation près, les quotients $(H_1/H_2, \ldots, H_{r-1}/H_r)$ sont isomorphes aux quotients

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

Puisqu'on dispose maintenant de la suite de composition (L_k) de K_1, de longueur $r-1$, on peut appliquer aussi l'hypothèse de récurrence à K_1 pour obtenir que $s = t = r$, et que les $(K_1/K_2, \ldots, K_{r-1}/K_r)$ sont isomorphes aux

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

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

Démonstration du lemme 1.5.7. — Le noyau de la projection $K_1 \to G_1/H_1$ est $H_1 \cap K_1$, donc on a une injection

$$K_1/H_1 \cap K_1 \hookrightarrow G_1/H_1.$$

Comme K_1 est distingué dans G, on obtient que $K_1/H_1 \cap K_1$ est distingué dans G_1/H_1. Par simplicité de ce dernier, il faut alors que $K_1/H_1 \cap K_1 = G_1/H_1$. □

CHAPITRE 2

GROUPES CLASSIQUES

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. La théorie des corps sera vue dans le cours d'Algèbre 2.

Soit $\mathbb{K}$ un corps. On dispose d'un morphisme d'anneau,

$$\phi : \mathbb{Z} \longrightarrow \mathbb{K},$$

défini par

$$\phi(n) = n \cdot 1 = 1 + \cdots + 1.$$

Alors le noyau de ϕ est un idéal $p\mathbb{Z} \subset \mathbb{Z}$, et fournit un morphisme injectif

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

Puisque $\mathbb{K}$ est un corps, $\mathbb{Z}/p\mathbb{Z}$ doit être 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** $\mathbb{K}$, notée $\mathrm{car}\,\mathbb{K}$.

On obtient immédiatement les propriétés suivantes :

- Si $\mathrm{car}\,\mathbb{K} = p \neq 0$, alors $p \cdot 1 = 0$ dans $\mathbb{K}$, donc pour tout $x \in \mathbb{K}$ on a $p \cdot x = p(1 \cdot x) = (p \cdot 1)x = 0$.
- Si $\mathbb{K}$ est un corps fini, alors $p = \mathrm{car}\,\mathbb{K} > 0$ et $\mathbb{K} \supset \mathrm{im}\,\phi = \mathbb{F}_p$, un sous-corps de $\mathbb{K}$ appelé **sous-corps premier**. Comme $\mathbb{K}$ est un $\mathbb{F}_p$-espace vectoriel, il faut que $|\mathbb{K}| = p^\alpha$ où $\alpha = \dim_{\mathbb{F}_p} \mathbb{K}$. (Si $\mathrm{car}\,\mathbb{K} = 0$, alors $\mathbb{K}$ contient $\mathbb{Q}$ comme sous-corps, c'est le sous-corps premier de $\mathbb{K}$).
- Si $\mathrm{car}\,\mathbb{K} = p > 0$, alors $\mathrm{F} : x \mapsto x^p$ est un morphisme de corps, appelé **morphisme de Frobenius**. En effet, par la formule du binôme,

$$(x+y)^p = x^p + \mathrm{C}_p^1 x^{p-1} y + \cdots + y^p = x^p + y^p \tag{17}$$

  car $p | \mathrm{C}_p^i$ pour $1 \leqslant i \leqslant p-1$. Si $\mathbb{K}$ est fini, alors F est un automorphisme (il est nécessairement injectif, puisque son noyau est un idéal, qui ne peut être que 0 ou $\mathbb{K}$, mais

F(1) = 1 donc c'est 0). Le sous-corps premier de $\mathbb{K}$ est exactement

$$\{x \in \mathbb{K}, \mathrm{F}(x) = x\}.$$

La dernière propriété dont nous aurons besoin est légèrement plus difficile, et nous ne la démontrerons pas, renvoyant au cours d'Algèbre 2.

Proposition. — *Si $q = p^\alpha$, où p est un nombre premier et α un entier naturel, il existe, à isomorphisme près, un et seul corps fini $\mathbb{F}_q$ de cardinal q.*

Puisque le groupe multiplicatif d'un tel corps est d'ordre $q-1$, ses éléments satisfont

$$x^q = x.$$

Les éléments du corps cherché sont donc exactement les racines du polynôme $\mathrm{X}^q - \mathrm{X}$. Réciproquement, le corps $\mathbb{F}_q$ sera construit comme le corps de rupture du polynôme $\mathrm{X}^q - \mathrm{X}$ sur $\mathbb{F}_p$, c'est-à-dire le plus petit sur-corps de $\mathbb{F}_p$ dans lequel le polynôme $\mathrm{X}^q - \mathrm{X}$ est à racines simples. Si on admet l'existence d'une clôture algébrique $\bar{\mathbb{F}}_p$ de $\mathbb{F}_p$, alors le corps $\mathbb{F}_q$ s'écrit

$$\mathbb{F}_q = \{x \in \bar{\mathbb{F}}_p, x^q = x\}.$$

C'est un sous-corps de $\bar{\mathbb{F}}_p$ car, de manière similaire à (17), on a $(x+y)^q = x^q + y^q$.

2.1. Le groupe linéaire

Soit $\mathbb{K}$ un corps (commutatif), E un $\mathbb{K}$-espace vectoriel de dimension n, alors on dispose du groupe GL(E) des transformations linéaires inversibles de E. Par le choix d'une base de E, ce groupe s'identifie au groupe $\mathrm{GL}(n,\mathbb{K})$ des matrices $n \times n$ inversibles à coefficients dans $\mathbb{K}$. On a vu dans le chapitre 1 la décomposition en produit semi-direct

$$\mathrm{GL}(n,\mathbb{K}) = \mathrm{SL}(n,\mathbb{K}) \rtimes \mathbb{K}^*.$$

2.1.1. Générateurs. — On étudie les éléments de GL(E) les plus simples possibles, à savoir les transformations laissant fixe un hyperplan de E. Soit donc $u \in \mathrm{GL(E)}$ laissant fixe l'hyperplan $\mathrm{H} \subset \mathrm{E}$, mais $u \neq \mathrm{Id}$. Alors $\mathrm{D} = \mathrm{im}(u - \mathrm{Id})$ est une droite. Fixant un générateur a de D, on déduit que u s'écrit

$$u(x) = x + f(x)a, \tag{18}$$

où $f \in \mathrm{E}^*$ est une forme linéaire telle que $\ker f = \mathrm{H}$ (autrement dit, $f \in \mathrm{H}^\perp$). Deux cas se présentent :

1° $\mathrm{E} = \mathrm{H} \oplus \mathrm{D}$, alors dans une base $(e_1, \ldots, e_n = a)$ de E telle que $(e_1, \ldots, e_{n-1})$ soit une base de H, on obtient la matrice diagonale

$$u = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \lambda \end{pmatrix} \tag{19}$$

avec $\det u = \lambda \neq 1$ puisque $u \neq \mathrm{Id}$; on dit que u est une **dilatation** d'hyperplan H, de droite D, et de rapport λ ;

2° $\mathrm{D} \subset \mathrm{H}$, alors on choisit une base $(e_1, \dots, e_{n-1} = a, e_n)$ de E telle que $(e_1, \dots, e_{n-1})$ soit une base de H et $f(e_n) = 1$: dans cette base u s'écrit

$$u = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}; \tag{20}$$

en particulier $\det u = 1$ et u n'est pas diagonalisable ; on dit que u est une **transvection** de droite D et d'hyperplan H.

Une transvection donnée par la formule (18) sera notée $u = \tau(f, a)$. Cette écriture n'est pas unique, puisque $\tau(f, a) = \tau(\lambda f, \lambda^{-1} a)$.

On a

$$\tau(f, a)\tau(g, a) = \tau(f + g, a)$$

donc l'espace des transvections de droite donnée (auxquelles on ajoute l'identité) est un sous-groupe de GL(E) isomorphe à l'espace vectoriel dual E^*. En particulier il est abélien.

Si $g \in \mathrm{GL(E)}$ alors

$$g\tau(f, a)g^{-1} = \tau(f \circ g^{-1}, g(a))$$

est une transvection de droite $g(\mathrm{D})$ et d'hyperplan $g(\mathrm{H})$. On en déduit :

2.1.2 Proposition. — *Le centre de* GL(E) *est réduit aux homothéties, donc* $\mathrm{Z(GL(E))} \simeq \mathbb{K}^*$. *Le centre de* SL(E) *est* $\mathrm{SL(E)} \cap \mathrm{Z(GL(E))} \simeq \{\lambda \in \mathbb{K}, \lambda^n = 1\}$.

Démonstration. — Si $u \in \mathrm{GL(E)}$ commute avec tout élément de SL(E), alors pour toute transvection τ de droite D on a

$$\tau = u\tau u^{-1}$$

qui est une transvection de droite $u(\mathrm{D})$, donc il faut que $u(\mathrm{D}) = \mathrm{D}$. Donc u fixe toutes les droites de E, ce qui entraîne que u est une homothétie. □

2.1.3 Théorème. — *Les transvections engendrent le groupe* SL(E). *Les transvections et les dilatations engendrent le groupe* GL(E).

Démonstration. — La seconde partie de l'énoncé se ramène à la première, car si $u \in \mathrm{GL(E)}$ et δ est une dilatation de rapport $\det u$, alors $\delta^{-1}u \in \mathrm{SL(E)}$, donc est un produit de transvections : ainsi u est le produit de la dilatation δ et d'un produit de transvections.

Reste à montrer la première partie. On commence par :

2.1.4 Lemme. — *Si* $x, y \in \mathrm{E} - \{0\}$ *et* $\dim \mathrm{E} \geqslant 2$, *alors il existe un produit* u *de transvections tel que* $u(x) = y$.

Démontrons le lemme : si x et y ne sont pas colinéaires, on prend une base (e_i) de E telle que $x = e_n$ et $y = e_{n-1} + e_n$, alors la transvection (20) envoie bien x sur y ; si x et y sont colinéaires, soit $z \notin \mathbb{K}x$, il suffit de composer une transvection envoyant x sur z avec une autre envoyant z sur y.

Revenons maintenant à la démonstration du théorème, que l'on va faire par récurrence sur $\dim \mathrm{E}$. Pour $\dim \mathrm{E} = 1$, il n'y a rien à montrer. Si $\dim \mathrm{E} \geqslant 2$, si $v \in \mathrm{SL(E)}$ et $x \in \mathrm{E}$, alors, quitte à composer v par un produit de transvections envoyant $v(x)$ sur x, on peut supposer

que $v(x) = x$. Notons D la droite engendrée par x, alors v induit une application linéaire $\bar{v} : E/D \to E/D$, également de déterminant 1 (si on choisit un supplémentaire F de D dans E, alors dans $E = D \oplus F$ la matrice de v est triangulaire supérieure par blocs, et les deux blocs diagonaux sont 1 et $\bar{v}$). Par l'hypothèse de récurrence, $\bar{v} = \prod_i \tau(\bar{x}_i, f_i)$, avec $\bar{x}_i \in E/D$ et $f_i \in (E/D)^* \simeq D^\perp$. Relevant $\bar{x}_i$ en $x_i \in E$, alors $w = \prod_i \tau(x_i, f_i)$ satisfait :

– $w(x) = v(x) = x$ car $f_i \in D^\perp$ c'est-à-dire $f_i(x) = 0$;
– le morphisme induit $\bar{w} \in SL(E/D)$ coïncide avec $\bar{v}$.

Il en résulte que $\mathrm{im}(w^{-1}v - \mathrm{Id}) \subset D$, donc $w^{-1}v$ est ou bien l'identité, ou bien une transvection de droite D. Ainsi v est un produit de transvections. □

2.1.5. Conjugaison, commutateurs. — À partir des formes matricielles (19) et (20), il est évident que deux dilatations sont conjuguées dans GL(E) si et seulement si elles ont même rapport, et que deux transvections sont toujours conjuguées dans GL(E). On en déduit :

2.1.6 Proposition. *— 1° Deux transvections de* SL(E) *sont toujours conjuguées dans* SL(E) *si* $\dim E \geqslant 3$.

2° Si $\dim E = 2$*, une transvection est toujours conjuguée dans* SL(E) *à une matrice* $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$*, où* $\lambda \in \mathbb{K}^*$*, et* $\lambda, \mu \in \mathbb{K}^*$ *définissent deux transvections conjuguées si et seulement si* $\frac{\lambda}{\mu}$ *est un carré dans* $\mathbb{K}$.

Démonstration. — Si on a deux transvections u et v, alors il existe $g \in GL(E)$ telle que $v = gug^{-1}$. On veut corriger g en $gs \in SL(E)$ de sorte que $v = (gs)u(gs)^{-1}$. Il suffit donc de trouver $s \in GL(E)$, de sorte que $\det s = (\det g)^{-1}$ et $sus^{-1} = u$. En se plaçant dans une base où u est de la forme (20), on voit qu'il suffit de prendre pour s la dilatation

$$s = \begin{pmatrix} (\det g)^{-1} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix},$$

ce qui est possible dès que $\dim E \geqslant 3$. Le cas de la dimension 2 est laissé en exercice. □

2.1.7 Théorème. *— 1° On a* $D(SL(n,\mathbb{K})) = SL(n,\mathbb{K})$ *sauf si* $n = 2$ *et* $\mathbb{K} = \mathbb{F}_2$ *ou* $\mathbb{F}_3$.

2° On a $D(GL(n,\mathbb{K})) = SL(n,\mathbb{K})$ *sauf si* $n = 2$ *et* $\mathbb{K} = \mathbb{F}_2$.

On a $GL(2,\mathbb{F}_2) = SL(2,\mathbb{F}_2) = S_3$ (l'isomorphisme se voit en considérant l'action sur l'ensemble des 3 droites de $\mathbb{F}_2^2$), dont le groupe dérivé est A_3. D'autre part, on peut montrer que $SL(2,\mathbb{F}_3) = H_8 \rtimes \mathbb{Z}/3\mathbb{Z}$, où H_8 est le «groupe des quaternions», d'ordre 8, et que $D(SL(2,\mathbb{F}_3)) = H_8$.

Démonstration. — Le déterminant d'un commutateur est 1, donc le groupe dérivé est toujours inclus dans $SL(n,\mathbb{K})$. Pour montrer qu'il est égal, on fera trois raisonnements, qui, ensemble, couvriront l'ensemble des cas. À chaque fois, on montre que le groupe dérivé contient les transvections, et donc tout le groupe $SL(n,\mathbb{K})$.

Le premier raisonnement est le suivant. Soit τ une transvection ; si $\mathrm{car}\,\mathbb{K} \neq 2$, alors $\tau^2 \neq \mathrm{Id}$ est encore une transvection ; si $n \geqslant 3$, les transvections sont conjuguées dans $SL(n,\mathbb{K})$, donc $\tau^2 = s\tau s^{-1}$ pour un $s \in SL(n,\mathbb{K})$ et $\tau = s\tau s^{-1}\tau^{-1}$, donc $\tau \in D(SL(n,\mathbb{K}))$. Si $n = 2$ les transvections sont conjuguées dans $GL(2,\mathbb{K})$ donc le même raisonnement avec $s \in$

$\mathrm{GL}(2,\mathbb{K})$ montre que $\tau \in \mathrm{D}(\mathrm{GL}(n,\mathbb{K}))$. Le théorème est ainsi démontré dès que $\mathrm{car}\mathbb{K} \neq 2$ et $n \geqslant 3$ pour le groupe SL, et $\mathrm{car}\mathbb{K} \neq 2$ et n quelconque pour le groupe GL (en particulier on obtient le cas $n = 2$ et $\mathbb{K} = \mathbb{F}_3$ pour GL, alors que dans ce cas le théorème est faux pour SL).

Le deuxième raisonnement démarre par l'observation suivante : si $s = \left(\begin{smallmatrix} \lambda & \\ & \lambda^{-1} \end{smallmatrix}\right)$ et $t = \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right)$, alors $sts^{-1}t^{-1} = \left(\begin{smallmatrix} 1 & \lambda^2-1 \\ & 1 \end{smallmatrix}\right)$. On obtient ainsi une transvection si $\lambda^2 - 1 \neq 0$, donc si $\lambda^2 \neq 1$, ce qu'on peut assurer si $\mathbb{K} \neq \mathbb{F}_2, \mathbb{F}_3$. Fixant un tel λ, toute transvection admet une base où elle s'écrit $\left(\begin{smallmatrix} 1 & \lambda^2-1 \\ & 1 \end{smallmatrix}\right)$, donc est un commutateur dans $\mathrm{SL}(2,\mathbb{K})$. Cela s'étend immédiatement en toute dimension, donc si $\mathbb{K} \neq \mathbb{F}_2, \mathbb{F}_3$, toute transvection est un commutateur, et ainsi $\mathrm{D}(\mathrm{SL}(n,\mathbb{K})) = \mathrm{SL}(n,\mathbb{K})$.

Le troisième raisonnement utilise le calcul

$$s = \begin{pmatrix} & -1 & \\ 1 & & \\ & & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix}, \quad \text{alors } tst^{-1}s^{-1} = \begin{pmatrix} 1 & & 1 \\ & 1 & -1 \\ & & 1 \end{pmatrix},$$

qui est encore une transvection. Cela couvre le cas $n \geqslant 3$ pour un corps quelconque, et en particulier pour le dernier cas manquant $\mathbb{K} = \mathbb{F}_2$. □

2.1.8. Simplicité. — On définit l'**espace projectif** $\mathbb{K}\mathrm{P}^{n-1} = \mathbb{K}^n - \{0\}/\mathbb{K}^*$ des droites de $\mathbb{K}^n$. En particulier, $\mathbb{K}\mathrm{P}^1 = \{(x,1), x \in \mathbb{K}\} \cup \{(1,0)\} \simeq \mathbb{K} \cup \{\infty\}$, appelé droite projective, est constitué d'une copie de $\mathbb{K}$ et d'un «point à l'infini».

L'action de $\mathrm{GL}(n,\mathbb{K})$ sur $\mathbb{K}^n$ induit une action sur $\mathbb{K}\mathrm{P}^{n-1}$. Le noyau de l'action est constitué des transformations $g \in \mathrm{GL}(n,\mathbb{K})$ qui fixent chaque droite, c'est-à-dire des homothéties. Par passage au quotient, on obtient ainsi une action fidèle sur $\mathbb{K}\mathrm{P}^{n-1}$ du **groupe projectif linéaire** $\mathrm{PGL}(n,\mathbb{K}) = \mathrm{GL}(n,\mathbb{K})/\mathrm{Z}(\mathrm{GL}(n,\mathbb{K}))$. De manière analogue, on obtient une action fidèle du groupe $\mathrm{PSL}(n,\mathbb{K}) = \mathrm{SL}(n,\mathbb{K})/\mathrm{Z}(\mathrm{SL}(n,\mathbb{K}))$.

Dans le cas d'un corps fini, on pourra vérifier en exercice les cardinaux des groupes ainsi construits :

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

Le but de cette section est :

2.1.9 Théorème. *— Le groupe* $\mathrm{PSL}(n,\mathbb{K})$ *est simple sauf si* $n = 2$ *et* $\mathbb{K} = \mathbb{F}_2$ *ou* $\mathbb{F}_3$.

Les exceptions ne sont effectivement pas simples : $\mathrm{PSL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2) = \mathrm{S}_3$ comme on l'a vu ci-avant, et on peut vérifier que l'action sur $\mathbb{F}_3\mathrm{P}^1$ (qui compte 4 points) identifie $\mathrm{PSL}(2,\mathbb{F}_3) \simeq \mathrm{A}_4$ et $\mathrm{PGL}(2,\mathbb{F}_3) \simeq \mathrm{S}_4$.

Ce n'est pas par hasard que les exceptions sont les mêmes dans les théorèmes 2.1.7 et 2.1.9. 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 $\mathrm{SL}(n,\mathbb{K})$ sur l'espace projectif $\mathbb{K}\mathrm{P}^{n-1}$.

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 est un sous-groupe maximal de G.

Un cas particulier d'action primitive est donnée par une **action 2-transitive**, c'est-à-dire telle que pour tous $x_1, x_2, y_1, y_2 \in X$, $x_1 \neq x_2$, $y_1 \neq y_2$, il existe $g \in G$ tel que $g \cdot x_1 = y_1$ et $g \cdot x_2 = y_2$ (c'est-à-dire : l'action de G sur $X \times X - \Delta$, où $\Delta = \{(x,x), x \in X\}$, 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 forcément un sous-groupe maximal, ce qu'on va obtenir en montrant que, pour tout $g \in G - G_x$, on a $G = G_x \cup G_x g G_x$. Fixons $g \in G - G_x$, soit $y = g \cdot x \neq x$: si $k \in G - G_x$, alors, puisque G_x est transitif sur $X - \{x\}$, il existe $h \in G_x$ tel que $k \cdot x = h \cdot y = hg \cdot x$, donc $g^{-1}h^{-1}k \in G_x$ donc $k \in G_x g G_x$, ce qu'il fallait montrer.

Le théorème permettant de montrer la simplicité d'un groupe à partir d'une action primitive est le suivant :

2.1.10 Théorème. — *Supposons que le groupe* G *agisse primitivement sur* X. *Si on se donne, pour chaque* $x \in X$, *un sous-groupe* $T_x \subset G$ *tel que :*

1° T_x *est abélien ;*

2° $T_{g \cdot x} = g T_x g^{-1}$ *pour tout* $g \in G$ *et* $x \in X$ *;*

3° $\cup_{x \in X} T_x$ *engendre* G.

Alors tout sous-groupe distingué de G *agissant non trivialement sur* X *contient* D(G).

Commençons par voir comment cet énoncé permet de démontrer le théorème 2.1.9 :

Démonstration du théorème 2.1.9. — L'action de $PSL(n,\mathbb{K})$ sur $X = \mathbb{K}P^{n-1}$ est 2-transitive, donc primitive. On applique le théorème 2.1.10 en utilisant pour $x \in X$ le groupe des transvections de vecteur x. Il satisfait les hypothèses du théorème, donc un sous-groupe distingué de $PSL(n,\mathbb{K})$, non réduit à {Id}, doit contenir $D(PSL(n,\mathbb{K})) = PSL(n,\mathbb{K})$ d'après le théorème 2.1.9. □

Démonstration du théorème 2.1.10. — Soit N un sous-groupe distingué et $x \in X$. Puisque G_x est maximal, le sous-groupe NG_x est égal à G_x ou à G ; dans la première hypothèse, il faut que $N \subset G_x$ donc, pour tout $g \in G$, on a $N = gNg^{-1} \subset G_{g \cdot x}$, donc N agit trivialement sur X. On a donc montré que si N n'agit pas trivialement sur X, alors $NG_x = G$, et en particulier N agit transitivement sur X.

On montre alors qu'en outre $G = NT_x$. En effet, si $n \in N$, alors

$$T_{n \cdot x} = n T_x n^{-1} \subset NT_x;$$

puisque N est transitif sur X, on a $T_y \subset NT_x$ pour tout $y \in X$ et donc $G = NT_x$ puisque les $(T_y)_{y \in X}$ engendrent G.

Finalement, puisque T_x est abélien, G/N est abélien donc $N \supset D(G)$. □

2.2. Formes sesquilinéaires

Soit E un $\mathbb{K}$-espace vectoriel. Dans cette section, on introduit les trois types de formes bilinéaire ou sesquilinéaire que l'on va étudier.

2.2.1. Formes bilinéaires. — Une **forme bilinéaire** sur E est une application $B : E \times E \to \mathbb{K}$ telle que, pour chaque $y \in E$, les applications partielles $x \mapsto B(x,y)$ et $x \mapsto B(y,x)$ soient $\mathbb{K}$-linéaires. Une telle forme est **symétrique** si $B(x,y) = B(y,x)$ pour tous $x, y \in E$, **anti-symétrique** si $B(x,y) = -B(y,x)$ pour tous $x, y \in E$. Si $\mathrm{car}\,\mathbb{K} \neq 2$, cette dernière condition est équivalente au fait que B soit **alternée**, c'est-à-dire que $B(x,x) = 0$ pour tout $x \in E$.

Soit (e_i) une base de E, supposé de dimension finie, et B une forme bilinéaire. La **matrice** M de B est donnée par $M_{ij} = B(e_i, e_j)$. Si deux éléments de E sont donnés par les vecteurs colonnes X et Y, alors $B(X,Y) = X^t MY$. La forme B est (anti-)symétrique si la matrice M est (anti-)symétrique. Si P est la matrice de passage de la base (e_i) à la base (e'_i), alors on a une formule classique : la matrice de B dans la nouvelle base est donnée par

$$M' = P^t MP.$$

Si $\det M \neq 0$, la valeur de $\det M$ dans le groupe multiplicatif $\mathbb{K}^*/(\mathbb{K}^*)^2$ est bien définie, et s'appelle le **discriminant** de B. Quand $\det M = 0$, on convient que le discriminant est nul aussi.

Associé à une forme bilinéaire symétrique on obtient la **forme quadratique**

$$q(x) = B(x,x).$$

Supposons $\mathrm{car}\,\mathbb{K} \neq 2$, alors on récupère la forme B à partir de q par la formule

$$B(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)).$$

2.2.2. Formes sesquilinéaires. — Il y a une variante des formes quadratiques quand le corps est équipée d'une involution $\sigma \in \mathrm{Aut}\,\mathbb{K}$. L'exemple principal sera $\mathbb{K} = \mathbb{C}$ avec $\sigma(z) = \bar{z}$, et pour simplifier les notations plus loin, on notera toujours l'involution σ sous la forme $\sigma(\lambda) = \bar{\lambda}$, quel que soit le corps. La décomposition $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$ s'étend de la manière suivante à tout corps muni d'une involution : on a une décomposition

$$\mathbb{K} = \mathbb{K}_0 \oplus \mathbb{K}_1,$$

où $\mathbb{K}_0$ et $\mathbb{K}_1$ sont les espaces propres de σ pour les valeurs propres 1 et -1. Ainsi $\mathbb{K}_0$ est un sous-corps de $\mathbb{K}$, et si $a \in \mathbb{K}_1$ alors $a^2 \in \mathbb{K}_0$ puisque $\sigma(a^2) = (\sigma(a))^2 = a^2$. Choisissant un $a \in \mathbb{K}_1 - \{0\}$, on déduit immédiatement que $\mathbb{K}_1 = a\mathbb{K}_0$ donc $\mathbb{K} = \mathbb{K}_0 \oplus a\mathbb{K}_0$.

2.2.3 Exemple. — Si p est premier et $q = p^2$, alors le morphisme de Frobenius $\sigma(x) = x^p$ est une involution de $\mathbb{F}_q$.

On dit alors qu'une application linéaire u entre deux $\mathbb{K}$-espaces vectoriels est σ-linéaire si $u(\lambda x) = \bar{\lambda} u(x)$ pour tout vecteur x et tout scalaire $\lambda \in \mathbb{K}$. Une **forme σ-sesquilinéaire** est une application $B : E \times E \to \mathbb{K}$ telle que pour tout $y \in E$, l'application $x \mapsto B(x,y)$ soit σ-linéaire et l'application $x \mapsto B(y,x)$ soit linéaire. La forme sesquilinéaire B est **hermitienne** si en outre $\overline{B(x,y)} = B(y,x)$ pour tous $x, y \in E$.

Dans une base (e_i) de E, la matrice M de E est donnée par $M_{ij} = B(e_i, e_j)$. Sur des vecteurs colonnes, on a alors $B(X,Y) = \bar{X}^t MY$, et la matrice de B dans une autre base est $\bar{P}^t MP$, où P est la matrice de passage. Le déterminant de M définit donc un discriminant qui est, ou bien nul, ou bien un élément du groupe multiplicatif

$$\mathbb{K}^\times / \{\bar{k}k, k \in \mathbb{K}^\times\}.$$

Pour une forme sesquilinéaire hermitienne, la matrice satisfait $\bar{M}^t = M$.

Associée à une forme sesquilinéaire hermitienne est la **forme hermitienne**

$$h(x) = B(x,x).$$

On récupère, si $\mathrm{car}\,\mathbb{K} \neq 2$, la forme sesquilinéaire à partir de h par la formule

$$B(x,y) = \frac{1}{4}\big(h(x+y) - h(x-y) + \frac{1}{a}(h(x+ay) - h(x-ay))\big).$$

2.3. Orthogonalité

Dans la suite, B désignera l'un des trois types de forme vus plus haut sur un espace vectoriel E de dimension finie : une forme bilinéaire alternée, une forme bilinéaire symétrique, ou une forme sesquilinéaire hermitienne. Dans les deux derniers cas, on supposera toujours $\mathrm{car}\,\mathbb{K} \neq 2$. Dans le cas où l'on parle d'application σ-linéaire, on écrit implicitement que dans les deux premiers cas $\sigma = \mathrm{Id}_{\mathbb{K}}$, alors σ-linéaire se réduit à linéaire.

2.3.1. Premières propriétés. — On dit que deux vecteurs x et y sont **orthogonaux** si $B(x,y) = 0$. L'**orthogonal** d'une partie F de E est le sous-espace vectoriel, noté $F^\perp$, des vecteurs de E orthogonaux à tous les éléments de F.

Le **noyau** de B sur E est le sous-espace $E^\perp$. On dit que B est **non dégénérée** si $E^\perp = 0$.

2.3.2 Proposition. — *Les conditions suivantes sont équivalentes :*

1° B *est non dégénérée ;*

2° *l'application* σ*-linéaire* $\hat{B} : E \to E^*$ *qui à* $x \in E$ *associe la forme linéaire* $y \mapsto B(x,y)$ *est injective ;*

3° *la matrice de* B *dans une base est inversible.*

Démonstration. — La première condition est que $\hat{B}$ soit injective, elle est donc équivalente à la seconde en dimension finie. Enfin, la matrice de $\hat{B}$ dans une base de E et sa base duale dans E^* est égale à la matrice de B, ce qui donne la troisième condition. □

Si B est dégénérée, alors B induit une forme de même type sur $E/\ker B$, qui est non dégénérée. Une autre manière de réaliser la forme sur le quotient est de choisir un supplémentaire quelconque U de $\ker B$ dans E, alors la projection sur le quotient réalise un isomorphisme isométrique

$$(U, B|_U) \xrightarrow{\sim} (E/\ker B, B).$$

Une forme dégénérée se ramène ainsi toujours à une forme non dégénérée sur un quotient, et *dans la suite on supposera toujours les formes non dégénérées*, sauf mention explicite du contraire.

2.3.3 Proposition. — *Si* B *est non dégénérée, et si* $F \subset E$ *est un sous-espace de* E*, alors* $\dim F + \dim F^\perp = \dim E$. *En particulier, si* $F \cap F^\perp = 0$ *(ce qui est équivalent à* $B|_F$ *est non dégénérée), alors* $E = F \oplus F^\perp$.

Démonstration. — L'application de restriction des formes linéaires, $r : E^* \to F^*$, est surjective. Donc

$$r \circ \hat{B} : E \to F^*, \quad x \mapsto B(x, \cdot),$$

est σ-linéaire surjective. Or $\ker(r \circ \hat{B}) = F^\perp$, d'où la formule sur la dimension en écrivant que la dimension de E est la somme des dimensions du noyau et de l'image de $r \circ \hat{B}$. □

Formules sur l'orthogonal (la seconde est vraie aussi en dimension infinie) :

$$(F^\perp)^\perp = F, \quad (F+G)^\perp = F^\perp \cap G^\perp, \quad (F \cap G)^\perp = F^\perp + G^\perp.$$

2.3.4. Groupe d'isométries. — Soit E et E′ deux espaces vectoriels sur $\mathbb{K}$, équipés de formes B et B′ de même type (pas forcément non dégénérées). Un morphisme *injectif* $f : E \to E'$ est une **isométrie** si pour tous $x, y \in E$ on a

$$B'(f(x), f(y)) = B'(x, y).$$

Si B et B′ sont des formes bilinéaires symétriques, ou sesquilinéaires hermitiennes, il suffit que $q'(f(x)) = q(x)$ (resp. $h'(f(x)) = h(x)$) pour tout $x \in E$.

Si B est non dégénérée, alors l'injectivité découle de la propriété d'isométrie. Si en outre $(E', B') = (E, B)$ alors une isométrie doit être 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, le **groupe orthogonal** $O(E, q)$;
- pour une forme hermitienne, le **groupe unitaire** $U(E, h)$;
- pour une forme alternée, le **groupe symplectique** $Sp(E, B)$.

Dans tous les cas, si M est la matrice de la forme B dans une base, alors une matrice A représente une isométrie si $\bar{A}^t M A = M$.

Dans le cas orthogonal, cela s'écrit $A^t M A = M$ qui implique $\det(A)^2 = 1$ donc $\det A = \pm 1$. Le **groupe spécial orthogonal** est alors défini comme $SO(E, q) = O(E, q) \cap SL(E)$.

Dans le cas unitaire, on obtient l'équation $\bar{A}^t M A = M$ qui implique $\overline{\det(A)} \det(A) = 1$. Le **groupe spécial unitaire** est alors défini comme $SU(E, h) = U(E, h) \cap SL(E)$.

Enfin, le groupe symplectique n'a pas de forme spéciale car il est déjà inclus dans SL(E), comme on le verra plus loin.

Exemples d'isométries : symétries et quasi-symétries. — On se place dans le cas d'une forme quadratique ou hermitienne. Si $x \in E$ n'est pas isotrope, et $\alpha = -1$ dans le cas quadratique (resp. $\alpha \in \mathbb{K}$ satisfait $\bar{\alpha}\alpha = 1$ dans le cas hermitien), alors une **symétrie** (resp. **quasi-symétrie**) par rapport à $x^\perp$ est une transformation de valeurs propres 1 et α sur la décomposition

$$E = x^\perp \oplus \mathbb{K}x.$$

Il s'agit manifestement d'une isométrie, donnée explicitement par la formule

$$s(y) = y + (\alpha - 1)\frac{B(x, y)}{B(x, x)}x.$$

Comme on le verra plus loin, les symétries engendrent le groupe orthogonal, et les quasi-symétries engendrent le groupe unitaire.

2.3.5. Décomposition en somme directe orthogonale : premier cas. — Supposons B bilinéaire symétrique ou sesquilinéaire hermitienne. On dit qu'un vecteur $x \in E$ est **isotrope** si $B(x,x) = 0$. Si B est non dégénérée, il existe nécessairement un vecteur non isotrope x. Dans ce cas, $\mathbb{K}x \cap x^\perp = 0$ donc $E = \mathbb{K}x \oplus x^\perp$, et la restriction de B à $x^\perp$ est à nouveau non dégénérée. Par récurrence sur la dimension, on obtient l'existence d'une **base orthogonale** (e_i), 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, dans le cas symétrique,

$$q(x) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2,$$

et dans le cas hermitien,

$$h(x) = \alpha_1 \bar{x}_1 x_1 + \cdots + \alpha_n \bar{x}_n x_n.$$

Dans une base $(\frac{e_i}{a_i})$ où $a_i \in \mathbb{K}^*$, les coefficients α_i deviennent

$$\begin{cases} \frac{\alpha_i}{a_i^2} & \text{dans le cas symétrique,} \\ \frac{\alpha_i}{\bar{a}_i a_i} & \text{dans le cas hermitien.} \end{cases}$$

On remarquera que, dans le cas hermitien, puisque $\overline{B(e_i,e_i)} = B(e_i,e_i)$, en fait $\alpha_i \in \mathbb{K}_0$.

Exemples. — 1° Si $\mathbb{K} = \mathbb{C}$, ou plus généralement un corps algébriquement clos, on peut toujours trouver a_i tel que $a_i^2 = \alpha_i$. Il en résulte que toute forme quadratique sur $\mathbb{K}$ admet une base dans laquelle elle s'écrit

$$q(x) = x_1^2 + \cdots + x_n^2.$$

Son groupe orthogonal est noté $O(n,\mathbb{C})$ ou $O(n,\mathbb{K})$.

2° Si $\mathbb{K} = \mathbb{R}$, alors on peut toujours trouver a_i tel que $a_i^2 = \pm\alpha_i$. En réarrangeant la base, on déduit que toute forme quadratique sur $\mathbb{R}$ admet une base dans laquelle elle s'écrit

$$q(x) = x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_n^2.$$

Le couple $(r, s = n-r)$ est la signature de q, on verra plus loin que c'est un invariant de q. Son groupe orthogonal est noté $O(r,s,\mathbb{R})$, ou le plus souvent $O(r,s)$.

3° Si $\mathbb{K} = \mathbb{F}_q$, alors $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ est d'ordre 2 (car le noyau de $x \mapsto x^2$ dans $\mathbb{F}_q^\times$ est $\{\pm 1\}$). Donc on peut ramener chaque α_i à être égal à 1 ou à un scalaire non nul $\alpha \notin (\mathbb{F}_q^\times)^2$. En fait on peut faire mieux, et cela donne toutes les formes quadratiques possibles sur $\mathbb{F}_q$:

2.3.6 Proposition. — *Pour $\mathbb{K} = \mathbb{F}_q$, toute forme quadratique non dégénérée admet une base où elle s'écrit sous l'une des deux formes suivantes :*

$$q(x) = x_1^2 + \cdots + x_{n-1}^2 + x_n^2,$$
$$q(x) = x_1^2 + \cdots + x_{n-1}^2 + \alpha x_n^2,$$

où α est un scalaire non nul fixé qui n'est pas un carré dans $\mathbb{F}_q$.

Notons que les deux formes proposées ne peuvent pas être équivalentes, puisque leurs discriminants sont 1 et α, qui sont différents dans $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$.

Démonstration. — Par récurrence sur n. Si $n \geqslant 2$, on va montrer qu'il existe e_1 tel que $q(e_1) = 1$. Alors $E = \mathbb{K}e_1 \oplus e_1^\perp$, et l'hypothèse de récurrence montre le résultat.

Écrivons q dans une base orthogonale : $q(x) = \sum \alpha_i x_i^2$. Contentons-nous du sous-espace engendré par les deux premiers vecteurs, donc $q(x) = \alpha_1 x_1^2 + \alpha_2 x_2^2$. Puisqu'il y a $\frac{q+1}{2}$ carrés

dans $\mathbb{F}_q$ (en comptant 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 $\mathbb{F}_q$. Mais puique $q < 2\frac{q+1}{2}$, il faut qu'existe (x_1, x_2) tels que $\alpha_1 x_1^2$ et $1-\alpha_2 x_2^2$ coïncident, c'est-à-dire $q(x) = 1$. □

4° Si $\mathbb{K} = \mathbb{C}$ et σ est la conjugaison complexe, alors $\alpha_i \in \mathbb{R}$, et on peut trouver $a_i \in \mathbb{C}$ tel que $\bar{a}_i a_i = \pm\alpha_i$. Ainsi, toute forme hermitienne sur $\mathbb{C}$ admet une base dans laquelle elle s'écrit

$$h(x) = \bar{x}_1 x_1 + \cdots + \bar{x}_r x_r - \bar{x}_{r+1} x_{r+1} - \cdots - \bar{x}_n x_n.$$

Son groupe unitaire est noté $\mathrm{U}(r, s, \mathbb{C})$, ou le plus souvent $\mathrm{U}(r, s)$.

5° Si $\mathbb{K} = \mathbb{F}_{p^2}$ et $\sigma(\lambda) = \lambda^p$, alors le morphisme

$$\mathbb{F}_{p^2}^\times \longrightarrow \mathbb{F}_p^\times, \quad x \longmapsto \bar{x}x = x^{p+1},$$

est surjectif (un générateur de $\mathbb{F}_{p^2}^\times$, d'ordre $p^2-1 = (p-1)(p+1)$ est envoyé sur un élément d'ordre $p-1$, donc un générateur de $\mathbb{F}_p^\times$). Il en résulte que tout élément $\alpha_i \in \mathbb{F}_p^\times$ peut s'écrire $\bar{a}_i a_i$, et donc toute forme hermitienne sur $\mathbb{F}_{p^2}$ admet une base dans laquelle elle s'écrit

$$h(x) = \bar{x}_1 x_1 + \cdots + \bar{x}_n x_n.$$

Son groupe unitaire est noté $\mathrm{U}(n, \mathbb{F}_{p^2})$.

2.3.7. Décomposition en somme directe orthogonale : deuxième cas. — Un **plan hyperbolique** est un sous-espace P de dimension 2 possédant une base (e_1, e_2) dans laquelle

$$\mathrm{B}(e_1, e_1) = \mathrm{B}(e_2, e_2) = 0, \quad \mathrm{B}(e_1, e_2) = 1.$$

Bien sûr, cela implique que e_1 et e_2 soient des vecteurs isotropes. Réciproquement :

2.3.8 Lemme. *— Si x est un vecteur isotrope, il existe un vecteur y tel que (x, y) soit la base d'un plan isotrope.*

Démonstration. — En effet, on peut toujours trouver x' tel que $\mathrm{B}(x, x') = 1$, puis on prend $y = x' - \frac{1}{2}\mathrm{B}(x', x')x$ qui satisfait les propriétés voulues. □

Par exemple, la forme quadratique en deux variables,

$$q(x_1, x_2) = x_1^2 - x_2^2,$$

n'est pas isotrope, donc est un plan hyperbolique. En effet, dans la base $(e_1 + e_2, e_1 - e_2)$, on obtient pour q la formule

$$q(y_1, y_2) = 2y_1 y_2.$$

La base $(e_1 + e_2, e_1 - e_2)$ est donc une base hyperbolique.

L'avantage d'un plan hyperbolique P sur un vecteur isotrope est que $\mathrm{B}|_\mathrm{P}$ est non dégénérée, ou de manière équivalente $\mathrm{P} \cap \mathrm{P}^\perp = 0$. Il en résulte que, pour un plan hyperbolique,

$$\mathrm{E} = \mathrm{P} \oplus \mathrm{P}^\perp.$$

Plaçons-nous à nouveau dans les cas symétrique ou hermitien. Supposons que E admette un vecteur isotrope. Par le lemme, il admet alors un plan hyperbolique P, et $\mathrm{E} = \mathrm{P} \oplus \mathrm{P}^\perp$. La forme B est alors non dégénérée sur $\mathrm{P}^\perp$, et on peut recommencer la même

opération sur $P^\perp$, si celui-ci admet un vecteur isotrope. Finalement, on fabrique une décomposition

$$E = P_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_\nu \overset{\perp}{\oplus} F,$$

où les P_i sont des plans hyperboliques, et F est un **sous-espace anisotrope**, c'est-à-dire dépourvu de vecteur isotrope. L'entier ν est l'**indice** de la forme, on verra plus loin que c'est un invariant. Une somme orthogonale de plans hyperboliques comme ci-dessus $P_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_\nu$ est appelée un **sous-espace hyperbolique**.

2.3.9. Décomposition en somme directe orthogonale : troisième cas. — On se place maintenant dans le cas d'une forme bilinéaire alternée. Dans ce cas, deux vecteurs x et y tels que $B(x,y) \neq 0$ engendrent toujours un plan hyperbolique P, et $E = P \oplus P^\perp$. Puisque B est non dégénérée, E contient nécessairement un tel plan hyperbolique, et par conséquent, en itérant la construction, on obtient une décomposition orthogonale :

$$E = P_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_\nu.$$

Choisissons alors une base $(e_i)_{i=1,\ldots,2\nu}$, de sorte que $(e_i, e_{i+\nu})$ soit une base standard de P_i. Dans cette base, la matrice de B est

$$J_\nu = \begin{pmatrix} 0 & \mathrm{Id}_\nu \\ -\mathrm{Id}_\nu & 0 \end{pmatrix}. \tag{21}$$

Ainsi, toutes les formes bilinéaires alternées non dégénérées admettent une base dans laquelle leur matrice est J_ν. En particulier, la dimension de l'espace doit être paire. Il n'y a donc, à équivalence près, qu'une seule forme alternée sur un $\mathbb{K}$-espace vectoriel de dimension $n = 2\nu$, et on notera son groupe $\mathrm{Sp}(\nu, \mathbb{K})$.

Ce groupe peut être décrit explicitement : une matrice $M \in \mathrm{Sp}(\nu, \mathbb{K})$ si et seulement si $M^t J_\nu M = J_\nu$; décomposant la matrice M par blocs,

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

il vient $M \in \mathrm{Sp}(\nu, \mathbb{K})$ si et seulement si

$$A^t C = C^t A, \quad B^t D = D^t B, \quad A^t D - C^t B = \mathrm{Id}_\nu. \tag{22}$$

2.4. Le théorème de Witt

Soit E muni d'une forme B bilinéaire symétrique ou alternée, ou d'une forme sesquilinéaire hermitienne. On dit qu'un sous-espace F de E est **isotrope** si $B|_F$ est dégénérée (ce qui est équivalent à $\ker B|_F = F \cap F^\perp \neq 0$). Dans ce cas, on obtient une forme induite, non dégénérée, sur $F/F \cap F^\perp$.

Le sous-espace F est **totalement isotrope** si $B|_{F^\perp} = 0$ (ce qui est équivalent à $F = F^\perp$).

Par exemple, si $P_1 \perp P_2 \perp \cdots \perp P_r$ sont des plans hyperboliques orthogonaux, de base (e_i, f_i), alors $\langle e_1, \ldots, e_r \rangle$ est totalement isotrope. Cet exemple est en fait général, comme le montre le :

2.4.1 Lemme. *— Soit* F *un sous-espace de* E, *et* $F_0 = \ker B|_F = F \cap F^\perp$. *Soit* G *un supplémentaire de* F_0 *dans* F, *et* $(e_1, \ldots, e_r)$ *une base de* F_0. *Alors il existe* $(f_1, \ldots, f_r)$ *dans* E *tels que*

– $\mathrm{P}_i = \langle e_i, f_i \rangle$ *est un plan hyperbolique orthogonal à* G ;
– $\bar{\mathrm{F}} = \mathrm{G} \overset{\perp}{\oplus} (\overset{\perp}{\oplus} \mathrm{P}_i)$ *est non isotrope.*
En outre, toute isométrie $f : \mathrm{F} \to \mathrm{E}'$ *se prolonge en une isométrie* $f : \bar{\mathrm{F}} \to \mathrm{E}'$.

Démonstration. — Puisque $\mathrm{B}|_{\mathrm{G}}$ est non dégénérée, en considérant $\mathrm{G}^\perp$ on est ramené au cas où $\mathrm{G} = 0$, c'est-à-dire au cas où F est totalement isotrope. Le cas où $r = 1$ est le lemme 2.3.8. On raisonne ensuite par récurrence sur r : si $\mathrm{F}_1 = \langle e_2, \dots, e_r \rangle$, alors soit H_1 un supplémentaire de F_1 dans $\mathrm{F}_1^\perp$ contenant e_1, donc $\mathrm{F}_1^\perp = \mathrm{F}_1 \oplus \mathrm{H}_1$ et $\mathrm{B}|_{\mathrm{H}_1}$ s'identifie à la forme non dégénérée induite sur $\mathrm{F}_1^\perp/\mathrm{F}_1$. On peut appliquer le lemme 2.3.8 au vecteur $e_1 \in \mathrm{H}_1$, donc il existe $f_1 \in \mathrm{H}_1$ tel que (e_1, f_1) soit une base d'un plan hyperbolique P_1, orthogonal à $e_2, \dots, e_r$ puisque $\mathrm{H}_1 \subset \mathrm{F}_1^\perp$. On applique alors l'hypothèse de récurrence au sous-espace totalement isotrope F_1 de $\mathrm{P}_1^\perp$.

L'extension des isométries se montre en étendant $\operatorname{im} f$ dans E' de la même manière que F. □

2.4.2 Lemme. — *Si* $\mathrm{B}(x,x) = \mathrm{B}(y,y) \neq 0$, *il existe une isométrie* f *telle que* $f(x) = y$.

Démonstration. — Commençons par le cas d'une forme quadratique. De $q(x+y) + q(x-y) = 2(q(x)+q(y)) = 4q(x)$, on déduit que l'un au moins des deux vecteurs $x+y$ et $x-y$ est non isotrope, disons par exemple $x+y$. Alors la symétrie hyperplane par rapport à $(x+y)^\perp$ envoie x sur $-y$, et on la compose par $-\mathrm{Id}$.

Le cas hermitien est similaire : on peut supposer par exemple que $x+y$ n'est pas isotrope, et on cherche une quasi-symétrie par rapport à $(x+y)^\perp$,

$$s(z) = z + (\alpha - 1)\frac{\mathrm{B}(x+y,z)}{\mathrm{B}(x+y,x+y)}(x+y),$$

avec $\bar{\alpha}\alpha = 1$. Le bon choix est

$$\alpha = 1 - \frac{\mathrm{B}(x+y,x+y)}{\mathrm{B}(x+y,x)} = -\frac{\mathrm{B}(x+y,y)}{\mathrm{B}(x+y,x)} = -\frac{\overline{\mathrm{B}(x+y,x)}}{\mathrm{B}(x+y,x)}$$

qui satisfait manifestement $\bar{\alpha}\alpha = 1$. □

***2.4.3 Théorème* (Witt).** — *Soient deux espaces isométriques,* (E, B) *et* $(\mathrm{E}', \mathrm{B}')$. *Soit* F *un sous-espace de* E *et* $u : \mathrm{F} \to \mathrm{E}'$ *une isométrie. Alors il existe une isométrie* $v : \mathrm{E} \to \mathrm{E}'$ *telle que* $v|_{\mathrm{F}} = u$.

Démonstration. — Par le lemme 2.4.1, on est ramené au cas où F est non isotrope.

Dans le cas d'une forme alternée, le résultat est alors immédiat en complétant F et $u(\mathrm{F})$ par des sommes de plans hyperboliques.

Dans le cas d'une forme quadratique ou hermitienne, le cas où $\dim \mathrm{F} = 1$ est fourni par le lemme 2.4.2. En général, on raisonne par récurrence sur $\dim \mathrm{F}$: si $\dim \mathrm{F} \geqslant 2$, on peut décomposer $\mathrm{F} = \mathrm{F}_1 \overset{\perp}{\oplus} \mathrm{F}_2$ avec F_1 et F_2 non isotropes ; par l'hypothèse de récurrence, $u|_{\mathrm{F}_1}$ se prolonge en une isométrie $v_1 : \mathrm{E} \to \mathrm{E}'$, donc en particulier $v_1|_{\mathrm{F}_1^\perp} : \mathrm{F}_1^\perp \to u(\mathrm{F}_1)^\perp$ est une isométrie ; on applique alors à nouveau l'hypothèse de récurrence à $u|_{\mathrm{F}_2} : \mathrm{F}_2 \to u(\mathrm{F}_1)^\perp$ pour le prolonger en une isométrie $v_2 : \mathrm{F}_1^\perp \to u(\mathrm{F}_1)^\perp$. On prend alors $v = u|_{\mathrm{F}_1} \oplus v_2 : \mathrm{F}_1 \oplus \mathrm{F}_1^\perp \to \mathrm{E}' = u(\mathrm{F}_1) \oplus u(\mathrm{F}_1)^\perp$. □

2.4.4 Corollaire. — *1° Si* F *et* G *sont des sous-espaces isométriques de* E*, alors* $F^\perp$ *et* $G^\perp$ *sont isométriques.*

2° Tous les sous-espaces totalement isotropes maximaux ont même dimension ν*, appelée l'indice de* B.

3° La dimension d'un sous-espace hyperbolique maximal est 2ν *; si* H *est un sous-espace hyperbolique maximal, alors* $E = H \overset{\perp}{\oplus} G$*, avec* G *anisotrope.*

4° Deux formes quadratiques ou hermitiennes sont équivalentes si et seulement si elles ont même indice et leurs restrictions à G *et* G′ *sont équivalentes.*

Démonstration. — On prouve la deuxième assertion. Si F et F′ sont totalement isotropes et $\dim F < \dim F'$, alors n'importe quel morphisme injectif $u : F \to F'$ est une isométrie, donc s'étend en une isométrie v de E. Donc $F \subsetneq v^{-1}(F')$ qui est aussi totalement isotrope, donc F n'était pas maximal. Il en résulte que tous les sous-espaces totalement isotropes maximaux ont même dimension.

Les autres assertions sont immédiates à partir du théorème de Witt. □

On notera qu'au vu de la troisième condition, il faut que $\nu \leqslant \frac{1}{2}\dim E$.

Dans le cas d'une forme quadratique sur $\mathbb{R}$, de signature (p,q), on voit que l'indice est $\inf(p,q)$, donc la signature est bien un invariant de la forme quadratique. La même chose est vraie des formes hermitiennes sur $\mathbb{C}$.

2.5. Le groupe symplectique

Dans cette section, E est muni d'une forme alternée, et on étudie le groupe symplectique Sp(E). Remarquons que si $\dim E = 2$, alors dans une base hyperbolique de E on a $B((x_1,x_2),(y_1,y_2)) = x_1y_2 - x_2y_1$. Un morphisme u de E multiplie B par $\det u$, d'où il résulte

$$\mathrm{Sp}(1,\mathbb{K}) = \mathrm{SL}(2,\mathbb{K}). \tag{23}$$

Soit une transvection $\tau(x) = x + f(x)a$, où $f \in E^*$ et $a \in \ker f$. Alors

$$B(x + f(x)a, y + f(y)a) - B(x,y) = B(a, xf(y) - yf(x)).$$

Quand x et y décrivent E, alors $xf(y) - yf(x)$ décrit $\ker f$, donc $\tau \in \mathrm{Sp}(E)$ si et seulement si $a \in (\ker f)^\perp$, ce qui signifie $f(x) = \lambda B(a,x)$ pour un $\lambda \in \mathbb{K}$. On déduit que les transvections symplectiques sont de la forme

$$\tau(x) = x + \lambda B(a,x)a, \quad a \in E, \lambda \in \mathbb{K}.$$

2.5.1 Théorème. — *Les transvections symplectiques engendrent* Sp(E).

Puisque les transvections sont de déterminant 1, il en résulte :

2.5.2 Corollaire. — *On a l'inclusion* $\mathrm{Sp}(E) \subset \mathrm{SL}(E)$. □

On verra en § 3.4 une démonstration plus directe de ce corollaire.

Démonstration du théorème. — La démonstration se fait par récurrence sur la dimension, et est une conséquence immédiate du :

2.5.3 Lemme. — *Si* $P = \langle x_1, x_2\rangle$ *et* $Q = \langle y_1, y_2\rangle$ *sont deux plans hyperboliques (*$B(x_1,x_2) = B(y_1,y_2) = 1$*), alors il existe un produit de transvections symplectiques envoyant* x_i *sur* y_i*.*

Démontrons donc le lemme. Dans un premier temps, observons que si $B(x_1,y_1) \neq 0$, alors on peut envoyer x_1 sur y_1 par la transvection symplectique

$$\tau(x) = x - \frac{B(y_1 - x_1, x)}{B(x_1,y_1)}(y_1 - x_1).$$

Si $B(x_1,y_1) = 0$, en passant par un z tel que $B(x_1,z) \neq 0$ et $B(y_1,z) \neq 0$, on déduit qu'un produit de 2 transvections symplectiques envoie x_1 sur y_1.

Dans tous les cas, on a trouvé un produit de transvections envoyant x_1 sur y_1, donc on est ramené au cas où $x_1 = y_1$; on veut donc envoyer x_2 sur y_2 en laissant x_1 fixe. À nouveau, la situation est plus simple si $B(x_2,y_2) \neq 0$: alors la transvection

$$\tau(x) = x - \frac{B(y_2 - x_2, x)}{B(x_2,y_2)}(y_2 - x_2)$$

convient, car $B(y_2 - x_2, x_1) = B(y_2,y_1) - B(x_2,x_1) = 0$. Si $B(x_2,y_2) = 0$, alors il faut à nouveau passer par un intermédiaire z, tel que $B(x_2,z) \neq 0$, $B(y_2,z) \neq 0$, mais aussi (pour fixer x_1), $B(x_1, z - x_2) = 0$ et $B(x_1, z - y_2) = 0$, ce qui revient à $B(x_1,z) = 1$. Mais $z = x_1 + y_2$ satisfait toutes ces conditions. □

On déduit du théorème que le centre de $\mathrm{Sp}(n,\mathbb{K})$ est réduit aux homothéties de $\mathrm{Sp}(n,\mathbb{K})$, à savoir $\{\pm \mathrm{Id}\}$. On considère donc le groupe projectif associé, à savoir le quotient

$$\mathrm{PSp}(n,\mathbb{K}) = \mathrm{Sp}(n,\mathbb{K})/\pm 1.$$

On énonce alors les deux théorèmes essentiels :

2.5.4 Théorème. — *On a* $\mathrm{D}(\mathrm{Sp}(n,\mathbb{K})) = \mathrm{Sp}(n,\mathbb{K})$*, sauf si* $n = 1$ *et* $\mathbb{K} = \mathbb{F}_2, \mathbb{F}_3$*, ou bien si* $n = 2$ *et* $\mathbb{K} = \mathbb{F}_2$*.*

2.5.5 Théorème. — *Le groupe* $\mathrm{PSp}(n,\mathbb{K})$ *est simple, sauf si* $n = 1$ *et* $\mathbb{K} = \mathbb{F}_2$ *ou* $\mathbb{F}_3$*, ou si* $n = 2$ *et* $\mathbb{K} = \mathbb{F}_2$*.*

Le nouveau cas exceptionnel ici (par rapport aux groupes SL) est celui de $\mathrm{Sp}(2,\mathbb{F}_2)$. On peut montrer que $\mathrm{PSp}(2,\mathbb{F}_2) \simeq \mathrm{S}_6$.

Démonstration du théorème 2.5.4. — Le cas $n = 1$ résulte de (23) et des résultats sur le groupe SL.

Si $n \geqslant 2$, donc $\dim E \geqslant 4$, écrivons $E = P \oplus P^\perp$ pour un plan hyperbolique P ; par le cas $n = 1$, les transvections de P sont des commutateurs (sauf si $\mathbb{K} = \mathbb{F}_2, \mathbb{F}_3$), donc $\mathrm{D}(\mathrm{Sp}(n,\mathbb{K}))$ contient les transvections symplectiques de droite contenue dans P, et par conjugaison toutes les transvections : donc $\mathrm{D}(\mathrm{Sp}(n,\mathbb{K})) = \mathrm{Sp}(n,\mathbb{K})$.

Si $\mathbb{K} = \mathbb{F}_3$ et $n \geqslant 2$, en regardant une décomposition $E = P_1 \overset{\perp}{\oplus} P_2 \overset{\perp}{\oplus} Q$, on se ramène au cas $E = P_1 \oplus P_2$, c'est-à-dire à $\mathrm{Sp}(2,\mathbb{F}_3)$. De même, le cas $\mathrm{Sp}(n,\mathbb{F}_2)$ pour $n \geqslant 3$ se ramène à $\mathrm{Sp}(3,\mathbb{F}_2)$. Ces deux cas spéciaux se font à la main de la manière suivante.

Commençons par $\mathrm{Sp}(2,\mathbb{F}_3)$. Il suffit de trouver deux éléments $\mathrm{U},\mathrm{V}\in\mathrm{Sp}(2,\mathbb{F}_3)$ dont le commutateur est une transvection. Dans une base où la forme symplectique est donnée par (21), on choisit

$$\mathrm{U}=\begin{pmatrix}\mathrm{A}^t & 0\\ 0 & \mathrm{A}^{-1}\end{pmatrix},\quad \mathrm{V}=\begin{pmatrix}\mathrm{I}_2 & \mathrm{B}\\ 0 & \mathrm{I}_2\end{pmatrix}.$$

D'après (22), les matrices U et V sont symplectiques, pourvu que B soit symétrique. Leur commutateur est

$$\mathrm{UVU}^{-1}\mathrm{V}^{-1}=\begin{pmatrix}\mathrm{I}_2 & \mathrm{B}-\mathrm{ABA}^t\\ 0 & \mathrm{I}_2\end{pmatrix}.$$

C'est une transvection si $\mathrm{B}-\mathrm{ABA}^t$ est de rang 1, ce qui se produit pour le choix

$$\mathrm{A}=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\quad \mathrm{B}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

Le cas de $\mathrm{Sp}(2,\mathbb{F}_3)$ se traite de manière similaire, en posant

$$\mathrm{A}=\begin{pmatrix}1 & 1 & 0\\ 0 & 0 & 1\\ 1 & 0 & 0\end{pmatrix},\quad \mathrm{B}=\begin{pmatrix}1 & 0 & 1\\ 0 & 1 & 1\\ 1 & 1 & 1\end{pmatrix}.$$

□

Démonstration du théorème 2.5.5. — Ce théorème se déduit du théorème 2.5.4, comme dans le cas des groupes PSL, par la méthode d'Iwasawa, en considérant l'action du groupe sur l'espace projectif $\mathbb{K}\mathrm{P}^{2n-1}$. Nous disposons en effet pour chaque droite $x\in\mathbb{K}\mathrm{P}^{2n-1}$ du groupe abélien (isomorphe à $\mathbb{K}$) des transvections symplectiques de droite x, et la seule hypothèse restant à vérifier pour appliquer le théorème 2.1.10 est que l'action soit primitive.

On a vu qu'un groupe agissant de manière 2-transitive sur un ensemble agit primitivement, mais $\mathrm{Sp}(n,\mathbb{K})$ n'agit pas 2-transitivement sur $\mathrm{X}=\mathbb{K}\mathrm{P}^{2n-1}$. En effet, d'après le théorème de Witt, le groupe $\mathrm{Sp}(n,\mathbb{K})$ a trois orbites sur $\mathrm{X}\times\mathrm{X}$, à savoir

1° la diagonale $\Delta=\{x=y\}$;

2° l'orbite O_1 des couples de droites (x,y) engendrant un plan hyperbolique ;

3° l'orbite O_2 des couples de droites (x,y) engendrant un plan isotrope.

Pour montrer que l'action est primitive, on doit montrer que le stabilisateur G_x d'un point $x\in\mathrm{X}$ est maximal. Supposons donc $\mathrm{G}_x\subsetneq\mathrm{H}\subset\mathrm{G}$.

Observons que si $g\mathrm{H}x\cap g'\mathrm{H}x\neq\emptyset$ alors il existe $h,h'\in\mathrm{H}$ tels que $ghx=g'h'x$, donc $h^{-1}g^{-1}g'h'\in\mathrm{G}_x$ donc $g^{-1}g'\in\mathrm{H}$, ce qui implique $g\mathrm{H}x=g'\mathrm{H}x$. Ainsi la collection des $(g\mathrm{H}x)_{g\in\mathrm{G}}$ réalise une partition de X, qui est G-invariante (l'action de G envoie orbite sur orbite).

Montrons qu'une telle partition est nécessairement triviale (il en résulte $\mathrm{H}x=\mathrm{X}$, d'où $\mathrm{G}=\mathrm{H}$ et l'action est primitive). Le graphe G de la partition est l'ensemble des couples $(y,z)\in\mathrm{X}\times\mathrm{X}$ tels que y et z soient dans la même classe. Ce graphe est invariant sous l'action de $\mathrm{Sp}(n,\mathbb{K})$, il est donc une réunion d'orbites de G dans $\mathrm{X}\times\mathrm{X}$, et il contient toujours la diagonale Δ. Le cas d'une partition triviale correspond à $\mathrm{G}=\Delta$ ou $\mathrm{G}=\mathrm{X}\times\mathrm{X}$. Si la partition n'est pas triviale, on a donc $\mathrm{G}=\Delta\cup\mathrm{O}_1$ ou $\Delta\cup\mathrm{O}_2$. Le premier cas correspond à dire que y et z sont dans une même classe s'ils engendrent un plan hyperbolique, c'est-à-dire si

$B(y,z) \neq 0$. Mais si $B(y,z) = 0$ alors il existe t tel que $B(y,t) \neq 0$ et $B(t,z) \neq 0$, donc y et z sont aussi dans la même classe, contradiction avec l'hypothèse $G = \Delta \cup O_1$. Le second cas est écarté de la même manière. □

2.5.6 Remarque. — On a implicitement utilisé la caractérisation suivante d'une action primitive : l'action de G sur X est primitive si et seulement si toute relation d'équivalence G-invariante sur X est triviale.

2.6. Le groupe orthogonal

On étudie ici quelques propriétés de base du groupe orthogonal.

2.6.1. La dimension 2. — Si $\dim E = 2$, alors, à une constante multiplicative près, toute forme quadratique s'écrit

$$q(x) = x_1^2 + Dx_2^2.$$

Il y a cas deux cas, suivant que le discriminant de q est égal on non à -1 dans $\mathbb{K}^*/(\mathbb{K}^*)^2$, c'est-à-dire suivant que $-D$ est un carré ou non dans $\mathbb{K}$. Dans les deux cas, on écrit $O(q) = SO(q) \cup O^-(q)$, où $O^-(q)$ consiste des transformations orthogonales de déterminant -1, et on donne une description complète des deux morceaux.

Dans le cas où $-D$ est un carré, alors la forme q admet des vecteurs isotropes, et donc E est un plan hyperbolique pour q : il existe une base (e_1, e_2) de E dans laquelle

$$q(x_1, x_2) = 2x_1x_2.$$

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 $O(q)$. On en déduit que les éléments de $O(q)$ sont de la forme $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{smallmatrix}\right)$ ou $\left(\begin{smallmatrix}0 & \lambda^{-1}\\ \lambda & 0\end{smallmatrix}\right)$, pour $\lambda \in \mathbb{K}^*$. Compte tenu de leur déterminant, il résulte finalement

$$SO(q) = \left\{\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{smallmatrix}\right), \lambda \in \mathbb{K}^*\right\}, \quad O^-(q) = \left\{\left(\begin{smallmatrix}0 & \lambda^{-1}\\ \lambda & 0\end{smallmatrix}\right), \lambda \in \mathbb{K}^*\right\}.$$

Les transformations de $O^-(q)$ sont toutes des symétries (par rapport à la droite engendrée par $e_1 + \lambda e_2$). Le groupe $SO(q)$ est abélien.

Exemple. — On a $SO(1,1) \simeq \mathbb{R}^*$ et $SO(2,\mathbb{C}) \simeq \mathbb{C}^*$.

Dans le second cas où $-D$ n'est pas un carré, alors la forme q est anisotrope, et on vérifie par un calcul direct que $SO(q)$ et $O^-(q)$ sont décrits par :

$$SO(q) = \{\left(\begin{smallmatrix}a & -cD\\ c & a\end{smallmatrix}\right), a^2 + c^2D = 1\}, \quad O^-(q) = \{\left(\begin{smallmatrix}a & cD\\ c & -a\end{smallmatrix}\right), a^2 + c^2D = 1\}.$$

À nouveau, le groupe $SO(q)$ est abélien, et $O^-(q)$ est constitué de symétries. [1]

1. Anticipant sur le cours d'Algèbre 2, le groupe $O(q)$ s'interprète simplement en terme du corps de rupture de q, à savoir $\mathbb{K}[\sqrt{-D}] \simeq \mathbb{K} \oplus \sqrt{-D}\mathbb{K}$: la forme quadratique q fournit une norme N sur $\mathbb{K}[\sqrt{-D}]$ satisfaisant $N(xy) = N(x)N(y)$, $SO(q)$ est le groupe des unités pour cette norme, et $O(q)$ est engendré par $SO(q)$ et la conjugaison de Galois. Dans le cas réel, ce corps est $\mathbb{C}$, le groupe des unités est le cercle (les rotations), la conjugaison de Galois la conjugaison complexe.

2.6.2. Centre et générateurs. — Rappelons que si D est une droite non isotrope, on dispose d'une symétrie orthogonale s_D par rapport à $D^\perp$. De même, si P est un plan non isotrope, alors $E = P \oplus P^\perp$, et le **renversement** r_P par rapport à $P^\perp$, défini par $r_P = (-1) \oplus 1$, est aussi une transformation orthogonale, élément de $SO(q)$.

Si $u \in O(q)$, il est immédiat que $u s_D u^{-1} = s_{u(D)}$ et $u r_P u^{-1} = r_{u(P)}$.

2.6.3 Proposition. — *Le centre de* $O(q)$ *est* $\{\pm \mathrm{Id}\}$, *et si* $\dim E \geqslant 3$ *le centre de* $SO(q)$ *est trivial si* $\dim E$ *est impaire,* $\{\pm \mathrm{Id}\}$ *si* $\dim E$ *est paire.*

Démonstration. — Si $u \in Z(O(q))$, alors $u s_D u^{-1} = s_D$ pour toute symétrie s_D, donc u préserve aussi les droites non isotropes. Mais pour montrer que u est une homothétie, il faut montrer que u préserve aussi les droites isotropes, et on va procéder différemment en traitant à la fois le cas du centre de $O(q)$ et de $SO(q)$.

Si $\dim E = 2$, la description explicite de $O(q)$ vue en § 2.6.1 donne le résultat. On peut donc supposer $\dim E \geqslant 3$.

Si $u \in O(q)$ commute aux éléments de $SO(q)$, alors $u r_P u^{-1} = r_P$ pour tout plan non isotrope P, donc u préserve les plans non isotropes. Pour montrer qu'il préserve toutes les droites, il suffit de montrer que toute droite est intersection de deux plans non isotropes.

Soit donc une droite $D = \mathbb{K}x$. Si D est non isotrope, alors $E = D \oplus D^\perp$, donc en prenant deux éléments y et z d'une base orthogonale de $D^\perp$, les plans $P = D \oplus \mathbb{K}y$ et $Q = D \oplus \mathbb{K}z$ conviennent. Si D est isotrope, on inclut D dans un plan hyperbolique P, et on complète x en une base hyperbolique (x, y) de P. Puisque $E = P \oplus P^\perp$, on peut choisir $z \in P^\perp$ non nul. Alors $Q = D \oplus \mathbb{K}(y + z)$ est encore un plan hyperbolique et $D = P \cap Q$. □

Le quotient de $SO(q)$ par son centre est le **groupe projectif orthogonal** :

$$PSO(E) = SO(E)/Z(SO(E)).$$

2.6.4 Théorème. — *Les symétriques hyperplanes engendrent* $O(q)$.

Démonstration. — On raisonne par récurrence sur la dimension. Soit $u \in O(q)$, $x_1 \in E$ non isotrope, et $x_2 = u(x_1)$. Puisque $q(x_1 + x_2) + q(x_1 - x_2) = 4q(x_1) \neq 0$, l'un au moins des deux éléments $x_1 + x_2$ et $x_1 - x_2$ est non isotrope :

- si $x_1 - x_2$ est non isotrope, alors $s_{x_1 - x_2}(x_1) = x_2$ donc $s_{x_1 - x_2} u(x_1) = x_1$;
- si $x_1 + x_2$ est non isotrope, alors $s_{x_2} s_{x_1 + x_2} = s_{x_2}(-x_2) = x_2$ 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 $x_1^\perp$. □

2.6.5 Remarque. — Cette démonstration montre que toute isométrie est produit d'au plus $2n$ symétries ($n = \dim E$). Le théorème de Cartan-Dieudonné affirme qu'il suffit d'au plus n symétries.

2.6.6 Théorème. — *Les renversements engendrent* $SO(q)$ *si* $\dim E \geqslant 3$.

Démonstration. — Par le théorème précédent, tout élément de $SO(q)$ est produit d'un nombre pair de symétries. Il suffit donc de montrer qu'un produit $s_{x_1} s_{x_2}$ de deux symétries est toujours un produit de renversements.

Si $\dim E = 3$, alors $s_{x_1} s_{x_2} = (-s_{x_1})(-s_{x_2})$, et l'opposé d'une symétrie est un renversement, d'où le résultat.

Si $\dim \mathrm{E} > 3$, on peut supposer x_1 et x_2 non colinéaires (et bien sûr non isotropes), posons $\mathrm{L} = \langle x_1, x_2 \rangle$, alors $\dim \mathrm{L} \cap \mathrm{L}^\perp \leqslant 1$ donc, par le lemme 2.4.1, il existe $\mathrm{L}' \supset \mathrm{L}$ de dimension 3, tel que $\mathrm{L}' \cap \mathrm{L}'^\perp = 0$. Alors $s_{x_1} s_{x_2}$ agit par l'identité sur $\mathrm{L}'^\perp$, donc n'agit non trivialement que sur L', de dimension 3. On est ainsi ramené à la dimension 3 : sur L', c'est le produit des renversements $-s_{x_1}|_{\mathrm{L}'}$ et $-s_{x_2}|_{\mathrm{L}'}$; on obtient alors $s_{x_1} s_{x_2}$ comme produit de leurs extensions sur E par l'identité sur $\mathrm{L}'^\perp$, qui sont encore des renversements. □

La question de la simplicité du groupe orthogonal est beaucoup plus compliquée que pour le groupe symplectique, et on ne la traitera pas dans ce cours. Il y a deux cas :

- si $\nu(q) = 0$, c'est-à-dire la forme q est anisotrope, il n'y a pas de résultat général ; dans le cas particulier $\mathbb{K} = \mathbb{R}$, on montre que $\mathrm{PSO}(n, \mathbb{R})$ est simple dès que $n = 3$ ou $n \geqslant 5$ (cf. livre de Perrin), alors que $\mathrm{PSO}(4, \mathbb{R})$ n'est pas simple [2], voir § 2.8 ;
- si $\nu(q) > 0$, c'est-à-dire q a des vecteurs isotropes, on montre que pour $n \geqslant 5$ le groupe $\mathrm{P}(\mathrm{D}(\mathrm{SO}(q)))$ est simple (cf. Dieudonné).

Exemple. — Le groupe $\mathrm{SO}(1, n)$ agit sur $\mathbb{R}^{n+1}$, sur lequel on choisit des coordonnées $(x_0, \dots, x_n)$ dans lequel la forme quadratique s'écrit

$$x_0^2 - x_1^2 - \cdots - x_n^2.$$

Le groupe laisse globalement invariante la quadrique $\{q(x) = 1\}$. Or celle-ci a deux composantes connexes, $\{x_0 > 0\}$ et $\{x_0 < 0\}$. On peut montrer que $\mathrm{SO}(1, n)$ a deux composantes connexes, d'une part le sous-groupe $\mathrm{SO}_o(1, n)$ qui préserve chaque composante connexe, d'autre part les transformations qui les échangent. Il est clair que $\mathrm{D}(\mathrm{SO}(1, n)) \subset \mathrm{SO}_o(1, n)$, en fait on peut montrer qu'il y a égalité, et que $\mathrm{SO}_o(1, n)$ est simple sauf pour $n = 1$. [3]

2.7. Le groupe unitaire

Rappelons que dans ce cas, le corps $\mathbb{K}$, qu'on supposera de caractéristique différente de 2, est muni d'une involution $\sigma(x) = \bar{x}$, de sorte que $\mathbb{K} = \mathbb{K}_0 \oplus \mathrm{I}\mathbb{K}_0$, où $\bar{\mathrm{I}} = -\mathrm{I}$ et $\mathrm{I}^2 \in \mathbb{K}_0$. Nos deux exemples standards sont $\mathbb{C}$ et $\mathbb{F}_{p^2}$.

2.7.1 Proposition. — *Supposons* $\dim \mathrm{E} = 2$ *et* E *hyperbolique pour la forme hermitienne* h. *Alors* $\mathrm{SU}(2, \mathrm{E}) \simeq \mathrm{SL}(2, \mathbb{K}_0)$.

Exemples. — On a donc $\mathrm{SU}(1,1) \simeq \mathrm{SL}(2, \mathbb{R})$ et $\mathrm{SU}(2, \mathbb{F}_{p^2}) \simeq \mathrm{SL}(2, \mathbb{F}_p)$.

Démonstration. — Dans une base hyperbolique la matrice de la forme hermitienne est $\mathrm{H} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Alors $u = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SU}(2, \mathbb{K})$ si $\det u = 1$ et $\bar{u}^t \mathrm{A} u = \mathrm{A}$, qui mène aux équations

$$ad - bc = 1, \quad a\bar{c} + \bar{a}c = 0, \quad b\bar{c} + \bar{a}d = 1, \quad b\bar{d} + \bar{b}d = 0.$$

2. Ce fait fondamental est à l'origine de propriétés spéciales importantes de la topologie et de la géométrie de dimension 4.

3. Le groupe $\mathrm{SO}_o(1, n)$ est le groupe de la géométrie hyperbolique, il agit sur la quadrique $\{q(x) = 1\}$ qui est un modèle de l'espace hyperbolique de dimension n.

Cela se résoud en $\bar{a} = a$, $\bar{d} = d$, $\bar{c} = -c$, $\bar{d} = -d$ et $ad - bc = 1$. On obtient $a, d, \mathrm{I}b, \mathrm{I}c \in \mathbb{K}_0$ et $ad - bc = 1$, soit encore $v = \left(\begin{smallmatrix} a & \mathrm{I}b \\ \mathrm{I}^{-1}c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{K}_0)$. On vérifie que l'application $u \mapsto v$ est bien un morphisme de groupes. [4] □

2.7.2. Produit scalaire hermitien. — Dans cette section uniquement, on se place sur $\mathbb{K} = \mathbb{C}$, et on regarde une forme hermitienne définie positive sur E, c'est-à-dire satisfaisant $h(x) \geqslant 0$, avec égalité si et seulement si $x = 0$. Une telle forme est un **produit scalaire hermitien**. Comme on a vu, il existe alors une base orthonormale, c'est-à-dire dans laquelle la forme s'écrit

$$h(x) = |x_1|^2 + \cdots + |x_n|^2.$$

Dans ce cas, les éléments du groupe $\mathrm{U}(h)$ jouissent d'une réduction particulièrement simple, similaire à celle, vue en classe préparatoire, des endomorphismes orthogonaux pour un produit scalaire euclidien défini positif.

Un endomorphisme u de E admet toujours un adjoint u^*, défini par

$$\mathrm{B}(x, u(y)) = \mathrm{B}(u^*(x), y)$$

pour tous $x, y \in \mathrm{E}$. Dans une base orthonormale, si u a pour matrice A, alors u^* a pour matrice $\mathrm{A}^* = \bar{\mathrm{A}}^t$. Ainsi $u \in \mathrm{U}(h)$ si $\mathrm{A}^*\mathrm{A} = \mathrm{Id}$.

Plus généralement, on dit que u est **normal** si $u^*u = uu^*$. Cette notion inclut à la fois les endomorphismes unitaires, les endomorphismes autoadoints ($u^* = u$) et anti-autoadjoints ($u^* = -u$).

2.7.3 Proposition. *— Tout endomorphisme normal pour un produit scalaire hermitien se diagonalise dans une base orthonormée.*

Les valeurs propres doivent être de module 1 pour les endomorphismes unitaires, réelles pour les endomorphismes autoadjoints, et imaginaires pures pour les endomorphismes anti-autoadjoints.

En particulier, si l'on dispose d'une seconde forme hermitienne h', alors on peut définir un endomorphisme de E par $h'(x, y) = h(x, u(y))$. Puisque $\overline{h(x, y)} = h(y, x)$, on a aussi $h'(x, y) = h(u(x), y)$, et il en résulte $u^* = u$. Donc u se diagonalise en une base h-orthonormée, ce qui signifie que dans cette base, la forme h' a une matrice diagonale :

$$h' = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}, \quad \lambda_i \in \mathbb{R}.$$

Bien sûr la seconde forme h' est définie positive si les coefficients λ_i sont strictement positifs.

---

4. On peut décrire plus intrinsèquement le morphisme $\mathrm{SL}(2, \mathbb{K}_0) \to \mathrm{SU}(2, \mathrm{E})$. Soit $\mathbb{K}$ considéré comme $\mathbb{K}_0$-espace vectoriel de dimension 2, et $\mathrm{E} = \mathrm{End}_{\mathbb{K}_0}\mathbb{K}$; E s'identifie à $\mathbb{K}^2$ par $(a, b) \in \mathbb{K}^2 \mapsto a + \sigma \circ b \in \mathrm{E}$, et devient ainsi un $\mathbb{K}$-espace vectoriel, où la multiplication par I s'identifie à la composition à droite par I. Le déterminant $\det : \mathrm{E} \to \mathbb{K}_0$ s'écrit $\det(a, b) = \bar{a}a - \bar{b}b$, donc est une forme hermitienne sur E, hyperbolique. Donc on dispose d'un morphisme $\mathrm{SL}(2, \mathbb{K}_0) \to \mathrm{SU}(2, \mathrm{E})$ en envoyant un morphisme $u \in \mathrm{SL}(2, \mathbb{K}_0)$ sur le morphisme de E donné par $v \mapsto u \circ v$.

Démonstration. — Soit u un endomorphisme normal de E. Soit λ une valeur propre de u et E_λ l'espace propre associé. Si $x \in E_\lambda$, alors $uu^*x = u^*ux = \lambda u^*x$, donc $u^*x \in E_\lambda$. Ainsi $u^*(E_\lambda) \subset E_\lambda$. On en déduit que si $y \perp E_\lambda$ et $x \in E_\lambda$, alors $B(uy, x) = B(y, u^*x) = 0$, donc on a $u(E_\lambda^\perp) \subset E_\lambda^\perp$. Une récurrence montre alors que E est somme directe orthogonale des espaces propres de u. □

2.7.4. Propriétés des groupes unitaires. — Dans cette dernière partie, on revient au cas général d'un corps général $\mathbb{K}$ et on énonce sans démonstration les propriétés de base d'un groupe unitaire sur le corps $\mathbb{K}$.

Centre : Le centre de $U(q)$ est constitué des homothéties de rapport λ tel que $\bar{\lambda}\lambda = 1$. Le centre de $SU(q)$ est constitué des homothéties de rapport satisfaisant en outre $\lambda^n = 1$. On notera

$$PSU(q) = SU(q)/Z(SU(q)).$$

Générateurs : Les quasi-symétries engendrent le groupe unitaire $U(E)$.

Simplicité : Si la forme hermitienne h est d'indice non nul, alors $PSU(n, \mathbb{K})$ est simple, à l'exception du groupe $PSU(2, \mathbb{F}_9) \simeq PSL(2, \mathbb{F}_3)$. Si l'indice est nul, donc la forme anisotrope, il n'y a pas de résultat général. Néanmoins $PSU(n, \mathbb{C})$ est simple dès que $n \geqslant 2$: en fait, comme on le verra en § 2.8, $PSU(2, \mathbb{C}) \simeq SO(3, \mathbb{R})$ qui est simple, et l'énoncé pour $n > 2$ s'en déduit.

Les énoncés sur le centre et les générateurs se démontrent de manière similaire à celui du cas orthogonal. Le résultat de simplicité dans le cas d'indice non nul vient de l'existence de transvections unitaires par rapport aux droites isotropes, qui permet grosso modo d'appliquer la méthode d'Iwasawa à l'action du groupe $PSU(h)$ sur l'espace des droites isotropes. On renvoie au livre de Dieudonné pour les détails.

2.8. Quaternions

Le corps des **quaternions**, $\mathbb{H}$, est un corps non commutatif, contenant comme sous-corps $\mathbb{R}$, et de dimension 4 comme espace vectoriel sur $\mathbb{R}$. On peut le décrire comme une algèbre de matrices 2×2 complexes :

$$\mathbb{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \alpha, \beta \in \mathbb{C} \right\}. \tag{24}$$

L'addition et la multiplication dans $\mathbb{H}$ 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 particuliers suivants :

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Les multiples réels de 1 fournissent le sous-corps $\mathbb{R} \subset \mathbb{H}$. La famille $(1, i, j, k)$ est une base de $\mathbb{H}$ vu comme espace vectoriel sur $\mathbb{R}$. On observe que

$$i^2 = j^2 = k^2 = -1, \quad ijk = -1,$$

relations desquelles on déduit aisément les autres multiplications des éléments de la base :

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Un quaternion $q = x_0 + x_1 i + x_2 j + x_3 k$, où les $x_\ell \in \mathbb{R}$, correspond à la matrice complexe donnée par $(\alpha = x_0 + i x_1, \beta = x_2 + i x_3)$, et peut s'écrire aussi

$$q = \alpha + \beta j.$$

Dans cette écriture, on fera attention que β et j ne commutent pas, en fait $j\beta = \bar{\beta} j$. L'ensemble $\{x_0 + i x_1, x_0, x_1 \in \mathbb{R}\}$ est un sous-corps de $\mathbb{H}$ isomorphe à $\mathbb{C}$. Ce n'est pas le seul car les rôles de i, j et k sont interchangeables dans $\mathbb{H}$.

Le centre de $\mathbb{H}$ est $\mathbb{R}$: en effet si $q \in Z(\mathbb{H})$, écrivons $q = \alpha + \beta j$, alors de $qi = iq$ on déduit $\beta = 0$, et de $j\alpha = \bar{\alpha} j = \alpha j$ on déduit $\alpha \in \mathbb{R}$.

Le **conjugué** d'un quaternion $q = x_0 + x_1 i + x_2 j + x_3 k$ est

$$\bar{q} = x_0 - x_1 i - x_2 j - x_3 k.$$

La conjugaison a les propriétés suivantes, immédiatement vérifiables :

1° $\overline{q_1 q_2} = \bar{q}_2 \bar{q}_1$;

2° $\mathrm{N}(q) := q\bar{q} = \bar{q}q = x_0^2 + x_1^2 + x_2^2 + x_3^2 \in \mathbb{R}$, en particulier $q^{-1} = \frac{\bar{q}}{\mathrm{N}(q)}$.

Un quaternion est réel si et seulement si $\bar{q} = q$, **imaginaire pur** si $\bar{q} = -q$. L'ensemble des quaternions imaginaires purs est $\Im(\mathbb{H}) = \{x_1 i + x_2 j + x_3 k\}$. La **partie réelle** et la **partie imaginaire** d'un quaternion sont respectivement $\frac{q+\bar{q}}{2} \in \mathbb{R}$ et $\frac{q-\bar{q}}{2} \in \Im(\mathbb{H})$.

Lemme. — *La norme* $\mathrm{N} : \mathbb{H}^* \to \mathbb{R}_+^*$ *est un morphisme de groupes multiplicatifs. Son noyau* $\ker \mathrm{N} = \{q \in \mathbb{H}, \mathrm{N}(q) = 1\}$ *est un groupe isomorphe à* $\mathrm{SU}(2)$.

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 $\mathrm{N}(q_1) \in \mathbb{R} = Z(\mathbb{H})$.

La description matricielle (24) donne immédiatement l'interprétation du noyau comme le groupe $\mathrm{SU}(2)$. □

Bien sûr N s'identifie à la norme euclidienne usuelle dans $\mathbb{H} = \mathbb{R}^4$, et donc le groupe $\mathrm{SU}(2)$ est homéomorphe à la sphère de $\mathbb{R}^4$.

Soit q un quaternion tel que $\mathrm{N}(q) = 1$, considérons la conjugaison

$$\phi_q : \mathbb{H} \longrightarrow \mathbb{H}, \quad x \longmapsto qxq^{-1}.$$

(En exercice, le lecteur pourra montrer que tous les automorphismes du corps $\mathbb{H}$ sont de ce type). Alors

$$\overline{\phi_q(x)} = q\bar{x}q^{-1},$$

donc ϕ_q préserve la décomposition $\mathbb{H} = \mathbb{R} \oplus \Im\mathbb{H}$. En outre,

$$\mathrm{N}(\phi_q(x)) = qxq^{-1}q\bar{x}q^{-1} = \mathrm{N}(x),$$

donc ϕ_q agit par isométries. En restreignant ϕ_q à $\Im\mathbb{H}$, on obtient ainsi un morphisme de groupes

$$\phi : \mathrm{SU}(2) \longrightarrow \mathrm{O}(3), \quad \text{défini par } \phi(q) = \phi_q|_{\Im\mathbb{H}}.$$

Comme le groupe SU(2), homéomorphe à la sphère de $\mathbb{R}^4$, est connexe, l'image de ϕ est connexe donc incluse dans SO(3).

2.8.1 Théorème. — *Le morphisme ϕ ainsi défini satisfait :*

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{SU}(2) \xrightarrow{\phi} \mathrm{SO}(3) \longrightarrow 1.$$

Par conséquent, $\mathrm{SO}(3) \simeq \mathrm{SU}(2)/\{\pm 1\} = \mathrm{PSU}(2)$.

Démonstration. — Le noyau de ϕ est constitué des quaternions q de norme 1 tels que $qxq^{-1} = x$ pour tout $x \in \Im\mathbb{H}$, soit $qx = xq$ pour tout $x \in \Im\mathbb{H}$. Comme c'est toujours vrai pour $x \in \mathbb{R}$, cela implique $qx = xq$ pour tout $x \in \mathbb{H}$, donc $q \in \mathrm{Z}(\mathbb{H}) = \mathbb{R}$. Donc $q = \pm 1$.

Soit $q \in \Im\mathbb{H}$ tel que $q\bar{q} = 1$, alors $q^2 = -1$, et

$$\phi_q(q) = q,$$
$$\phi_q^2(x) = q^2 x q^{-2} = x \text{ pour } x \in \Im\mathbb{H},$$

donc ϕ_q ne peut être que le renversement d'axe $\mathbb{R}q \subset \Im\mathbb{H}$. Donc l'image de ϕ contient les renversements, et donc est surjective par le théorème 2.6.6. □

L'isomorphisme entre PSU(2) et SO(3) a été montré en trouvant, grâce aux quaternions, une action de SU(2) sur $\mathbb{R}^3$. On peut aussi regarder l'action de $\mathrm{SU}(2) \times \mathrm{SU}(2)$ sur $\mathbb{R}^4 = \mathbb{H}$, définie en associant à un couple de quaternions (q_1, q_2), chacun de norme 1, le morphisme

$$\Psi_{q_1,q_2}(x) = q_1 x \bar{q}_2 = q_1 x q_2^{-1}.$$

2.8.2 Théorème. — *1° On obtient ainsi une suite exacte*

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathrm{SU}(2) \times \mathrm{SU}(2) \xrightarrow{\Psi} \mathrm{SO}(4) \longrightarrow 1,$$

donc $\mathrm{SO}(4) \simeq \mathrm{SU}(2) \times \mathrm{SU}(2)/\pm 1$.

2° On a un isomorphisme $\mathrm{PSO}(4) \simeq \mathrm{SO}(3) \times \mathrm{SO}(3)$.

En particulier PSO(4) n'est pas simple.

Démonstration. — 1° À nouveau, on a $\mathrm{N}(\phi_{q_1,q_2}(x)) = q_1 x q_2^{-1} q_2 \bar{x} q_1^{-1} = \mathrm{N}(x)$ donc l'image de ψ est bien contenue dans $\mathrm{O}(4,\mathbb{R})$, et donc par connexité de l'image dans $\mathrm{SO}(4,\mathbb{R})$.

Le noyau est constitué des (q_1, q_2) tels que $q_1 x q_2^{-1} = x$ pour tout $x \in \mathbb{H}$ donc $q_1 x = x q_2$. Faisant $x = 1$ on déduit $q_1 = q_2$, forcément élément de $\mathrm{Z}(\mathbb{H})$, donc $q_1 = q_2 = \pm 1$.

Pour montrer que ψ est surjective, on prend $u \in \mathrm{SO}(4,\mathbb{R})$, donc $u(1) = q$ tel que $\mathrm{N}(q) = 1$. Alors $\psi_{\bar{q},1} \circ u(1) = \bar{q}q1 = 1$, donc $\psi_{\bar{q},1} \circ u \in \mathrm{SO}(3,\mathbb{R})$, donc par le théorème précédent, il existe q' tel que $\psi_{\bar{q},1} \circ u = \psi_{q',q'}$.

2° En composant ψ par la projection sur PSO(4), on obtient un morphisme

$$\tilde{\psi} : \mathrm{SU}(2) \times \mathrm{SU}(2) \longrightarrow \mathrm{PSO}(4).$$

Ce morphisme est surjectif, puisque ψ est surjectif. Son noyau est constitué des (q_1, q_2) tels que $q_1 x = \epsilon x q_2$ pour tout $x \in \mathbb{H}$, où $\epsilon = \pm 1$. Pour $\epsilon = 1$ on récupère le noyau de ψ, pour $\epsilon = -1$ on obtient (faisant $x = -1$) $q_2 = -q_1$ puis $q_1 x = x q_1$ pour tout $x \in \mathbb{H}$, donc $q_1 = \pm 1$, ce qui rajoute au noyau les éléments $(1,-1)$ et $(-1,1)$. Finalement le noyau de $\tilde{\psi}$ est constitué des quatre éléments $(\pm 1, \pm 1)$, donc

$$\mathrm{PSO}(4) \simeq \mathrm{SU}(2) \times \mathrm{SU}(2)/(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{PSU}(2) \times \mathrm{PSU}(2).$$

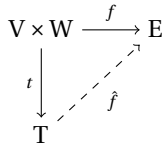
□

CHAPITRE 3

ALGÈBRE TENSORIELLE

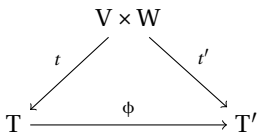
3.1. Produit tensoriel

3.1.1. Construction du produit tensoriel. — Soient V et W deux $\mathbb{K}$-espaces vectoriels. Un **produit tensoriel** de V et W est la donnée d'un espace vectoriel T et d'une application bilinéaire $t : V \times W \to T$, satisfaisant la propriété universelle suivante : si $f : V \times W \to E$ est une application bilinéaire, alors il existe une unique application linéaire $\hat{f} : T \to E$ qui factorise f par T, c'est-à-dire telle que $f = \hat{f} \circ t$. Cela se traduit par le fait que le diagramme suivant soit commutatif :



Une telle paire (T, t) est nécessairement unique, à unique isomorphisme près, au sens suivant :

***3.1.2 Théorème* (Existence et unicité).** — *Étant donné deux $\mathbb{K}$-espaces vectoriels* V *et* W*, il existe un produit tensoriel* (T, t) *de* V *et* W*, unique au sens suivant : si* (T, t) *et* (T', t') *sont des produits tensoriels de* V *et* W*, alors ils sont isomorphes, c'est-à-dire qu'il existe un isomorphisme* $\phi : T \to T'$*, unique, tel que le diagramme suivant soit commutatif :*



On parle ainsi du produit tensoriel de V *et* W*, noté* $V \otimes W$*. L'application bilinéaire* $t : V \times W \to V \otimes W$ *est notée* $(v, w) \mapsto v \otimes w$*. Un élément de* $V \otimes W$ *de type* $v \otimes w$ *est appelé* ***tenseur décomposé*** *(ou* ***tenseur pur****) ; les tenseurs décomposés engendrent* $V \otimes W$*.*

Démonstration. — Commençons par l'unicité. On applique la propriété universelle pour T à $t' : V \times W \to T'$, pour déduire l'existence de $\phi : T \to T'$ 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 $t : V \times W \to T$, on déduit que $\psi \circ \phi = \mathrm{Id}_T$. De manière analogue $\phi \circ \psi = \mathrm{Id}_{T'}$.

Reste l'existence du produit tensoriel. Compte tenu de l'unicité, n'importe quelle construction ferait l'affaire, en voici une. Soit $\mathbb{K}[V \times W]$ l'espace vectoriel engendré par les symboles (v, w) pour $v \in V$ et $w \in W$. Un élément de $\mathbb{K}[V \times W]$ est donc une somme finie $\sum f_{v,w}(v, w)$ pour des scalaires $f_{v,w}$. L'application tautologique $V \times W \to \mathbb{K}[V \times W]$ donnée par $(v, w) \mapsto (v, w)$ n'est pas bilinéaire, mais elle va le devenir si on compose par la projection sur un certain quotient $\mathbb{K}[V \times W]/S$. Pour trouver S, écrivons les relations dont nous avons besoin : pour $v, v' \in V$, $w, w' \in W$, $\lambda, \mu \in \mathbb{K}$, les quantités suivantes devraient êtres nulles :

$$((\lambda v + \mu v'), w) - \lambda(v, w) - \mu(v', w), \tag{25}$$

$$(v, \lambda w + \mu w') - \lambda(v, w) - \mu(v, w'). \tag{26}$$

Il est donc naturel de définir S comme le sous-espace vectoriel de $\mathbb{K}[V \times W]$ engendré par les expressions (25) et (26), et de définir

$$T = \mathbb{K}[V \times W]/S.$$

On définit maintenant l'application bilinéaire $t : V \times W \to T$ en associant à (v, w) la classe de (v, w) dans le quotient T. Puisque $\mathbb{K}[V \times W]$ est engendré par les éléments de type (v, w), son quotient T est engendré par les éléments de type $t((v, w))$, c'est-à-dire par les tenseurs décomposés.

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 $f : V \times W \to E$, alors on peut définir une application linéaire $g : \mathbb{K}[V \times W] \to E$ par $g((v, w)) = f(v, w)$. Puisque f est bilinéaire, g s'annule sur le sous-espace S, et donc passe au quotient pour donner une application linéaire $\hat{f} : T \to E$. L'identité $f = \hat{f} \circ t$ est claire, et l'unicité de $\hat{f}$ provient du fait que T est engendré par les $t((v, w))$, or l'image de $t((v, w))$ par $\hat{f}$ est déterminée, puisque ce doit être $f(v, w)$. □

3.1.3 Corollaire. — *Soient* V, W *et* E *des* $\mathbb{K}$*-espaces vectoriels. Alors l'espace 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* $(V \otimes W)^*$.

On remarquera que l'espace des applications bilinéaires $V \times W \to E$ est aussi isomorphe à $\mathrm{Hom}(V, \mathrm{Hom}(W, E))$. Le corollaire s'écrit donc aussi

$$\mathrm{Hom}(V, \mathrm{Hom}(W, E)) \simeq \mathrm{Hom}(V \otimes W, E). \tag{27}$$

On exprime souvent cette propriété en disant le produit tensoriel par W est « adjoint » à $\cdot \mapsto \mathrm{Hom}(W, \cdot)$.

Démonstration. — L'isomorphisme est obtenu en passant d'une application bilinéaire $f : V \times W \to E$ à $\hat{f} \in \mathrm{Hom}(V \otimes W, E)$ par la propriété universelle. Dans l'autre direction, on obtient f à partir de $\hat{f}$ par restriction aux tenseurs décomposés. □

***3.1.4 Proposition* (Fonctorialité).** — *Si on a des applications linéaires $f : V_1 \to V_2$ et $g : W_1 \to W_2$, alors 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, $(f_1 \otimes g_1) \circ (f_2 \otimes g_2) = (f_1 \circ f_2) \otimes (g_1 \circ g_2)$.

Démonstration. — Il s'agit de compléter le diagramme commutatif :

$$\begin{array}{ccc} V_1 \times W_1 & \xrightarrow{f \times g} & V_2 \times W_2 \\ \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle t'} \\ V_1 \otimes W_1 & \overset{f \otimes g}{\dashrightarrow} & V_2 \otimes W_2 \end{array}$$

Il suffit d'appliquer la propriété universelle à $t' \circ (f \times g)$.

La seconde assertion résulte de l'unicité de $(f_1 f_2) \otimes (g_1 g_2)$ quand on applique la propriété universelle, les détails sont laissés au lecteur. □

3.1.5 Propriétés du produit tensoriel. — *Soient* V, W, Z *des* $\mathbb{K}$*-espaces vectoriels, alors*

$$\begin{aligned} \mathbb{K} \otimes V &\xrightarrow{\sim} V & k \otimes v &\longmapsto kv, \\ (V \oplus W) \otimes Z &\xrightarrow{\sim} (V \otimes Z) \oplus (W \otimes Z) & (v+w) \otimes z &\longmapsto v \otimes z + w \otimes z, \\ V \otimes W &\xrightarrow{\sim} W \otimes V & v \otimes w &\longmapsto w \otimes v, \\ V \otimes (W \otimes Z) &\xrightarrow{\sim} (V \otimes W) \otimes Z & v \otimes (w \otimes z) &\longmapsto (v \otimes w) \otimes z. \end{aligned}$$

Comme conséquence de ces propriétés, on obtient en particulier que si (v_i) et (w_j) sont des bases de V et W, alors $(v_i \otimes w_j)$ est une base de $V \otimes W$. En effet, on a $V = \oplus_i \mathbb{K} v_i$ et $W = \oplus_j \mathbb{K} w_j$, et $\mathbb{K} \otimes \mathbb{K} = \mathbb{K}$. Développant par rapport aux sommes, on obtient $V \otimes W = \oplus_{i,j} \mathbb{K} v_i \otimes w_j$. En particulier,

$$\dim V \otimes W = (\dim V)(\dim W).$$

Démonstration. — Dans le premier cas, l'application $\mathbb{K} \times V \to V$ donnée par $(k, v) \mapsto kv$ est bilinéaire, donc il y a une application induite $\mathbb{K} \otimes V \to V$, c'est elle qui est notée $k \otimes v \mapsto kv$. L'inverse est $v \mapsto 1 \otimes v$, d'où l'isomorphisme.

Les autres cas sont similaires. Attention à l'abus de notation, par exemple dans le troisième cas, l'application bilinéaire $V \times W \to W \otimes V$ donnée par $(v, w) \mapsto w \otimes v$ fournit, par la propriété universelle, une application $V \otimes W \to W \otimes V$ qui est notée abusivement $v \otimes w \mapsto w \otimes v$, alors qu'il y a dans $V \otimes W$ des tenseurs qui ne s'écrivent pas sous la forme $v \otimes w$. □

Exemples. — 1° Il y a une application linéaire

$$f : V^* \otimes W \longrightarrow \mathrm{Hom}(V, W), \quad \alpha \otimes w \longmapsto (v \mapsto \alpha(v) w).$$

Cette application, toujours injective, est un isomorphisme si $\dim V < \infty$. En effet, dans ce cas, on peut choisir une base (e_i) de V, et soit (e^i) sa base duale, alors l'inverse est fourni pour $u \in \mathrm{Hom}(V, W)$ par la formule

$$f^{-1}(u) = \sum_i e^i \otimes u(e_i).$$

Cette formule n'a de sens que pour une somme finie.

2° Le produit tensoriel $\mathbb{K}[X] \otimes \mathbb{K}[Y] \simeq \mathbb{K}[X,Y]$, par l'isomorphisme $X^i \otimes Y^j \mapsto X^i Y^j$.

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 $\mathbb{K}$, mais son comportement est plus compliqué. Si $A = \mathbb{Z}$, alors les A-modules sont des groupes abéliens, et on a par exemple $\mathbb{Z}^k \otimes \mathbb{Z}^l = \mathbb{Z}^{kl}$, mais pourquoi $\mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Q} = 0$, $\mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} = 0$, et $\mathbb{Z}/3\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$?

4° **Extension des scalaires**. Si on a un corps $\mathbb{L} \supset \mathbb{K}$, et V est un $\mathbb{K}$-espace vectoriel, alors puisque $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel, on peut former

$$V^{\mathbb{L}} = V \otimes_{\mathbb{K}} \mathbb{L}.$$

On peut donner à $V^{\mathbb{L}}$ une structure de $\mathbb{L}$-espace vectoriel de la manière suivante : si $\ell \in \mathbb{L}$, alors la multiplication m_ℓ par ℓ est un endomorphisme $\mathbb{K}$-linéaire de $\mathbb{L}$, donc on peut définir la multiplication par ℓ sur $V^{\mathbb{L}}$ comme $1 \otimes m_\ell$. Les propriétés de $\mathbb{L}$-espace vectoriel sont immédiates. On dit que $V^{\mathbb{L}}$ est obtenu à partir de V par extension des scalaires de $\mathbb{K}$ à $\mathbb{L}$.

Par exemple, si $\mathbb{K} = \mathbb{R}$ et $\mathbb{L} = \mathbb{C}$, alors $V^{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$ est la **complexification** de l'espace vectoriel réel V. Un endomorphisme $u \in \mathrm{End}_{\mathbb{R}}(V)$ s'étend en sa complexification $u^{\mathbb{C}} = u \otimes 1 \in \mathrm{End}_{\mathbb{C}}(V^{\mathbb{C}})$. Si u a une matrice A dans une base réelle (e_i) de V, alors $u^{\mathbb{C}}$ a la même matrice A dans la base complexe $(e_i \otimes 1)$ de $V^{\mathbb{C}}$.

3.2. Algèbre tensorielle

On a vu dans la section précédente que $(V_1 \otimes V_2) \otimes V_3$ et $V_1 \otimes (V_2 \otimes V_3)$ sont canoniquement isomorphes. Aussi notera-t-on généralement sans parenthèse $V_1 \otimes V_2 \otimes V_3$. Par récurrence, sont canoniquement équivalents tous les choix pour étendre cette définition à un produit tensoriel

$$V_1 \otimes V_2 \otimes \cdots \otimes V_n$$

de n espaces vectoriels.

Une autre manière familière de voir l'unicité est d'exprimer $V_1 \otimes \cdots \otimes V_n$ et l'application

$$(v_1, \ldots, v_n) \mapsto v_1 \otimes \cdots \otimes v_n \tag{28}$$

comme solution d'un problème universel. Une application n-**linéaire** $V_1 \times \cdots \times V_n \to E$ est une application qui est linéaire par rapport à chacun des facteurs V_i.

3.2.1 Lemme. — *L'application* $V_1 \times \cdots \times V_n \to V_1 \otimes \cdots \otimes V_n$ *définie par (28) est n-linéaire, et elle est universelle pour cette propriété.*

L'image de cette application est à nouveau constituée des **tenseurs décomposés**.

Démonstration. — Notons $\mathrm{Mult}^n(V_1 \times \cdots \times V_n, E)$ l'espace des applications n-linéaires de $V_1 \times \cdots \times V_n$ vers E. On a clairement

$$\mathrm{Mult}^n(V_1 \times \cdots \times V_n, E) = \mathrm{Hom}(V_1, \mathrm{Mult}^{n-1}(V_2 \times \cdots \times V_n, E)).$$

Il s'agit de montrer que $\mathrm{Hom}(V_1 \otimes \cdots \otimes V_n, E) = \mathrm{Mult}^n(V_1 \times \cdots \times V_n, E)$, où l'isomorphisme est donné par la composition avec (28). On raisonne par récurrence sur n. En appliquant

(27) on obtient

$$\begin{aligned}\mathrm{Hom}(\mathrm{V}_1\otimes\cdots\otimes\mathrm{V}_n,\mathrm{E}) &= \mathrm{Hom}(\mathrm{V}_1,\mathrm{Hom}(\mathrm{V}_2\otimes\cdots\otimes\mathrm{V}_n,\mathrm{E}))\\ &= \mathrm{Hom}(\mathrm{V}_1,\mathrm{Mult}^{n-1}(\mathrm{V}_2\times\cdots\times\mathrm{V}_n),\mathrm{E})\\ &= \mathrm{Mult}^n(\mathrm{V}_1\times\cdots\times\mathrm{V}_n,\mathrm{E}).\end{aligned}$$

□

De la même manière que pour le produit tensoriel, si on a des applications linéaires $f_i : \mathrm{V}_i \to \mathrm{W}_i$ alors on obtient une application linéaire unique

$$f_1\otimes\cdots\otimes f_n : \mathrm{V}_1\otimes\cdots\otimes\mathrm{V}_n \longrightarrow \mathrm{W}_1\otimes\cdots\otimes\mathrm{W}_n$$

telle que sur les tenseurs décomposés

$$f_1\otimes\cdots\otimes f_n(v_1\otimes\cdots\otimes v_n) = f_1(v_1)\otimes\cdots\otimes f_n(v_n).$$

3.2.2. Algèbre tensorielle. — Rappelons qu'une $\mathbb{K}$-**algèbre** est un $\mathbb{K}$-espace vectoriel A muni d'un produit qui est une application bilinéaire $\mathrm{A}\times\mathrm{A}\to\mathrm{A}$. Le produit doit être en outre associatif, c'est-à-dire

$$(xy)z = x(yz) \quad \text{pour tous } x,y,z\in\mathrm{A}.$$

L'algèbre est **graduée** si elle est munie d'une décomposition d'espace vectoriel

$$\mathrm{A} = \oplus_{n\in\mathbb{N}}\mathrm{A}_n, \quad \text{telle que } \mathrm{A}_n\cdot\mathrm{A}_m\subset\mathrm{A}_{n+m}.$$

Par exemple, l'algèbre $\mathbb{K}[\mathrm{X}]$ des polynômes à une indéterminée est graduée par le degré : $\mathbb{K}[\mathrm{X}] = \oplus\mathbb{K}\mathrm{X}^n$. L'algèbre des polynômes à plusieurs indéterminés $\mathrm{A} = \mathbb{K}[\mathrm{X}_1,\dots,\mathrm{X}_p]$ est également graduée par les polynômes homogènes : A_n est le sous-espace des polynômes homogènes de degré n, donc engendré par les $\mathrm{X}_1^{i_1}\cdots\mathrm{X}_p^{i_p}$ pour $i_1+\cdots+i_p = n$.

Un élément $x\in\mathrm{A}$ est dit **homogène** s'il existe n tel que $x\in\mathrm{A}_n$, et on dit alors que x est de degré n. Un **morphisme d'algèbres graduées** est un morphisme d'algèbres $f : \mathrm{A}\to\mathrm{B}$ qui préserve la graduation : $f(\mathrm{A}_n)\subset\mathrm{B}_n$. Un **idéal homogène** $\mathrm{I}\subset\mathrm{A}$ est un idéal (bilatère) engendré par des éléments homogènes, c'est-à-dire $\mathrm{I} = \oplus_n\mathrm{I}\cap\mathrm{A}_n$. Dans ce cas, le quotient A/I est encore une algèbre graduée, $\mathrm{A}/\mathrm{I} = \oplus_n\mathrm{A}_n/(\mathrm{I}\cap\mathrm{A}_n)$.

On définit les **puissances tensorielles** d'un espace vectoriel V par $\mathrm{T}^0\mathrm{V} = \mathbb{K}$, et pour $n\geqslant 1$

$$\mathrm{T}^n\mathrm{V} = \mathrm{V}\otimes\mathrm{V}\otimes\cdots\otimes\mathrm{V} \quad (n \text{ facteurs V}).$$

L'**algèbre tensorielle** de V est définie par

$$\mathrm{TV} = \oplus_{n\in\mathbb{N}}\mathrm{T}^n\mathrm{V}. \tag{29}$$

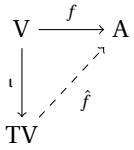
Pour en faire une algèbre, nous devons définir un produit sur TV. Nous avons en effet un produit

$$\mathrm{T}^n\mathrm{V}\times\mathrm{T}^m\mathrm{V}\longrightarrow\mathrm{T}^{n+m}\mathrm{V}, \quad (v_1\otimes\cdots\otimes v_n, v_{n+1}\otimes\cdots\otimes v_{n+m})\longmapsto v_1\otimes\cdots\otimes v_{n+m}.$$

Compte tenu des propriétés du produit tensoriel vues plus haut, ce produit est associatif et fait de TV une algèbre, munie d'une unité puisque $1\in\mathbb{K} = \mathrm{T}^0\mathrm{V}\subset\mathrm{TV}$. La décomposition (29) en fait une algèbre graduée. Noter la présence d'une injection canonique $\iota : \mathrm{V}\hookrightarrow\mathrm{TV}$ puisque $\mathrm{T}^1\mathrm{V}$ s'identifie à V.

Si V a pour base $(e_i)_{i\in\mathrm{I}}$, alors TV a pour base les $e_{i_1}\otimes\cdots\otimes e_{i_n}$ pour $n\in\mathbb{N}$ et $(i_1,\dots,i_n)\in\mathrm{I}^n$.

***3.2.3 Proposition* (Propriété universelle).** — *L'algèbre tensorielle* TV *satisfait la propriété suivante : si* $f : \mathrm{V} \to \mathrm{A}$ *est une application linéaire vers une algèbre avec unité* A*, alors 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 le diagramme suivant est commutatif :*



Démonstration. — La commutation dit

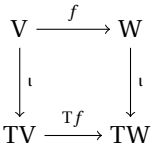
$$\hat{f}(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = f(v_1) f(v_2) \cdots f(v_n).$$

La propriété universelle de $\mathrm{T}^n\mathrm{V} = \mathrm{V}^{\otimes n}$ permet d'étendre cette formule en une application linéaire unique $\hat{f} : \mathrm{T}^n\mathrm{V} \to \mathrm{A}$. Reste à vérifier qu'on obtient ainsi un morphisme d'algèbres : il suffit de le vérifier sur les tenseurs décomposés, qui engendrent TV, or

$$\begin{aligned}\hat{f}((v_1 \otimes \cdots \otimes v_n) \otimes (v_{n+1} \otimes \cdots \otimes v_{n+m})) &= f(v_1) \cdots f(v_n) f(v_{n+1}) \cdots f(v_{n+m}) \\ &= \hat{f}(v_1 \otimes \cdots \otimes v_n) \hat{f}(v_{n+1} \otimes \cdots \otimes v_{n+m}).\end{aligned}$$

□

Comme dans tous les cas précédents, la propriété universelle implique la fonctorialité de la construction : si on a un morphisme $f : \mathrm{V} \to \mathrm{W}$, alors il y a un morphisme d'algèbres, unique, $\mathrm{T}f : \mathrm{TV} \to \mathrm{TW}$, tel que le diagramme suivant soit commutatif :



Le morphisme $\mathrm{T}f$ n'est autre que $\oplus \mathrm{T}^n f$. En outre, on a la propriété

$$\mathrm{T}(f \circ g) = \mathrm{T}f \circ \mathrm{T}g.$$

3.3. Algèbre extérieure

On a introduit dans la section précédente l'algèbre tensorielle $\mathrm{TV} = \oplus \mathrm{T}^n\mathrm{V}$, où $\mathrm{T}^n\mathrm{V}$ est canoniquement le dual de $\mathrm{Mult}^n(\mathrm{V}^n, \mathbb{K})$ (les formes n-linéaires sur V). Dans cette section, nous faisons une construction analogue pour l'espace $\mathrm{Alt}^n(\mathrm{V})$ des **formes n-linéaires alternées** sur V, c'est-à-dire satisfaisant $\alpha(v_1, \ldots, v_n) = 0$ dès que deux des vecteurs (v_i) sont égaux. Si $\mathrm{car}\mathbb{K} \neq 2$, cela est équivalent à ce que la forme n-linéaire soit antisymétrique, c'est-à-dire satisfasse pour toute permutation $\sigma \in \mathrm{S}_n$ l'identité

$$\alpha(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = \epsilon(\sigma)\alpha(v_1, \ldots, v_n).$$

L'algèbre extérieure ΛV, avec une inclusion $\iota : V \hookrightarrow \Lambda V$, sera la solution du problème universel pour les applications $f : V \to A$ de V vers une algèbre avec unité A, satisfaisant l'identité

$$f(v)^2 = 0. \tag{30}$$

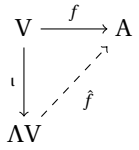
Compte tenu de la propriété universelle de l'algèbre TV, l'injection ι doit se factoriser via TV ; en même temps, comme dans les cas précédents, ΛV sera engendrée par les images des tenseurs purs, donc il est légitime de chercher ΛV comme quotient de TV,

$$\Lambda V = TV/I.$$

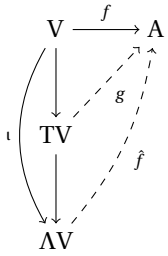
(Comme pour les anneaux, on peut définir le quotient d'une algèbre A par un idéal I, c'est-à-dire un sous-espace vectoriel $I \subset A$ satisfaisant $AI \subset I$ et $IA \subset I$. On forme alors le quotient comme espace vectoriel A/I et les propriétés $AI \subset I$ et $IA \subset A$ sont exactement ce qu'il faut pour que la multiplication passe au quotient).

Il faut mettre dans l'idéal I tout ce dont on n'a pas besoin pour factoriser les applications satisfaisant (30). Les éléments de la forme $v \otimes v$ sont de ce type, puisqu'ils sont envoyés sur 0. Il est alors naturel de définir $I \subset TV$ comme l'idéal engendré par les éléments de type $v \otimes v$, pour $v \in V$, et l'**algèbre extérieure** comme $\Lambda V = TV/I$. La composition de $V \hookrightarrow TV \to TV/I$ fournit l'application $\iota : V \to \Lambda V$.

3.3.1 Proposition. — *L'algèbre extérieure satisfait la propriété universelle suivante : si $f : V \to A$ est un morphisme 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 $\hat{f} : \Lambda V \to A$ est un morphisme d'algèbres :*



Démonstration. — Par la propriété universelle de TV, on a une factorisation de f par $g : TV \to A$. Puisque $g(v \otimes v) = f(v)^2 = 0$, il faut que g s'annule sur l'idéal I donc g passe au quotient pour fournir un morphisme d'algèbres $\hat{f} : \Lambda V = TV/I \to A$. Il est manifestement unique puisque ΛV est engendrée par les tenseurs décomposés. La démonstration se résume ainsi par le diagramme suivant :



□

Comme conséquence de la propriété universelle, ou conséquence du même énoncé pour le produit tensoriel, on obtient :

3.3.2 Proposition. — *Si $f : V \to W$ est un morphisme, alors il induit un morphisme d'algèbres $\Lambda f : \Lambda V \to \Lambda W$, tel que $\iota_W \circ f = \Lambda f \circ \iota_V$. En outre, $\Lambda(f \circ g) = \Lambda f \circ \Lambda g$.*

Décrivons maintenant de manière plus concrète l'algèbre ΛV. Pour cela, remarquons que I est un **idéal homogène** de TV, c'est-à-dire

$$I = \oplus_n I \cap T^n V.$$

C'est une conséquence du fait que I soit engendré par des éléments homogènes de degré 2 : un élément de I est une somme finie d'éléments de type $a \otimes v \otimes v \otimes b$, pour $a, b \in TV$; quitte à développer a et b, on peut supposer que a et b sont eux-mêmes homogènes de degré k et l, donc $a \otimes v \otimes v \otimes b \in T^{k+l+2}V \cap I$ et ainsi I se décompose bien sur la somme $\oplus_n I \cap T^n V$.

Il en résulte que

$$\Lambda V = \oplus_n T^n V / (T^n V \cap I) =: \oplus_n \Lambda^n V,$$

où $\Lambda^n V$ est appelée la puissance extérieure n-ième de V.

Puisque l'idéal I est engendré par les éléments $v \otimes v$, il ne coupe pas $T^0 V$ et $T^1 V = V$, donc

$$\Lambda^0 V = \mathbb{K}, \quad \Lambda^1 V = V.$$

Le morphisme $\iota : V \to \Lambda V$ est donc une injection. Le produit dans ΛV est appelé **produit extérieur** et noté $\wedge$. Ainsi ΛV est-elle engendrée par les $v_1 \wedge \cdots \wedge v_n$ pour $n \in \mathbb{N}$ et $v_i \in V$. Le fait que l'idéal soit homogène implique $\Lambda^n V \wedge \Lambda^m V \subset \Lambda^{n+m} V$ donc ΛV est aussi une algèbre graduée. Si $f : V \to W$ est un morphisme, il s'ensuit que

$$\Lambda f = \oplus \Lambda^n f, \quad \text{avec } \Lambda^n f : \Lambda^n V \longrightarrow \Lambda^n W.$$

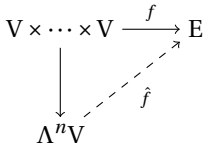
3.3.3 Proposition. — *L'algèbre ΛV est **anticommutative**, c'est-à-dire que si $\alpha \in \Lambda^n V$ et $\beta \in \Lambda^m V$ alors $\alpha \wedge \beta = (-1)^{mn} \beta \wedge \alpha$.*

Démonstration. — Il suffit de le montrer sur les produits d'éléments de V. Pour $n = m = 1$, l'identité $v \wedge w = -w \wedge v$ pour $v, w \in V$ résulte immédiatement de $v \wedge v = 0$. Le cas général s'en déduit. □

3.3.4 Propriétés de $\Lambda^n V$. — *1° L'application n-linéaire*

$$(v_1, \ldots, v_n) \mapsto v_1 \wedge \cdots \wedge v_n$$

de V^n vers $\Lambda^n V$ satisfait la propriété universelle suivante : si on a une application n-linéaire alternée $f : V \times \cdots \times V \to E$, alors il existe un unique morphisme $\hat{f} : \Lambda^n V \to E$ telle que le diagramme suivant soit commutatif :



En particulier, $\mathrm{Alt}^n(\mathrm{V}) = (\Lambda^n \mathrm{V})^*$.

2° Si $(e_i)_{i\in \mathrm{I}}$ *est une base de* V, *alors* $(e_{i_1} \wedge \cdots \wedge e_{i_n})_{i_1<\cdots<i_n}$ *est une base de* $\Lambda^n \mathrm{V}$. *En particulier, si* $d = \dim \mathrm{V} < \infty$, *alors* $\Lambda^n \mathrm{V} = 0$ *pour* $n > d$, *et*

$$\dim \Lambda^n \mathrm{V} = \mathrm{C}_d^n.$$

3° Si V *est de dimension finie, alors* $\Lambda^n(\mathrm{V}^*) \simeq (\Lambda^n \mathrm{V})^*$ *(*$= \mathrm{Alt}^n \mathrm{V}$*) par la dualité* $\Lambda^n(\mathrm{V}^*) \times \Lambda^n \mathrm{V} \to \mathbb{K}$ *donnée par*

$$\langle \alpha_1 \wedge \cdots \wedge \alpha_n, v_1 \wedge \cdots \wedge v_n \rangle = \det(\langle \alpha_i, v_j \rangle)_{1\leqslant i,j\leqslant n}.$$

4° Si V *est de dimension finie* d, *alors* $\dim \Lambda^d \mathrm{V} = 1$, *donc si* $f \in \mathrm{End}(\mathrm{V})$, *l'endomorphisme* $\Lambda^d f \in \mathrm{End}(\Lambda^d \mathrm{V})$ *est un scalaire : en fait*

$$\Lambda^d f = \det f.$$

Le troisième énoncé sera utilisé notamment dans le cours de Géométrie Différentielle : les applications de $\mathbb{R}^d$ dans $\Lambda^n(\mathbb{R}^d)^*$ sont en effet les formes différentielles sur $\mathbb{R}^d$.

Démonstration. — 1° Par la propriété universelle de $\mathrm{T}^n \mathrm{V}$, l'application n-linéaire f se factorise en $f = g \circ i$, où $g \in \mathrm{Hom}(\mathrm{T}^n \mathrm{V}, \mathrm{E})$ et i est l'application n-linéaire canonique $\mathrm{V} \to \mathrm{T}^n \mathrm{V}$. Mais, parce que f est alternée, g s'annule sur $\mathrm{I} \cap \mathrm{T}^n \mathrm{V}$, donc se factorise à travers le quotient $\Lambda^n \mathrm{V}$ en une application $f \in \mathrm{Hom}(\Lambda^n \mathrm{V}, \mathrm{E})$. L'unicité de f provient du fait que $\Lambda^n \mathrm{V}$ est engendrée par les $v_1 \wedge \cdots \wedge v_n$.

2° On sait déjà que les $(e_{i_1} \wedge \cdots \wedge e_{i_n})_{i_1<\cdots<i_n}$ engendrent $\Lambda^n \mathrm{V}$, il reste à voir qu'ils sont libres. Pour cela on va exhiber une forme linéaire qui vaut 1 sur un élément de la famille et 0 sur tous les autres. Soit e^i forme linéaire telle que $\langle e^i, e_j \rangle = 1$ si $j = i$ et 0 si $j \neq i$. Fixons $a_1 < \cdots < a_n$, alors la forme n-linéaire sur V donnée par $f(v_1, \ldots, v_n) = \det(\langle e^{a_i}, v_j \rangle)$ est alternée, donc fournit $\hat{f} \in (\Lambda^n \mathrm{V})^*$. Or $f(e_{i_1} \wedge \cdots \wedge e_{i_n}) = 1$ si $a_j \equiv i_j$ et 0 sinon.

3° Compte tenu des propriétés d'antisymétrie du déterminant, la formule proposée est antisymétrique en les α_i et en les v_i, et donc fournit une application bilinéaire $b : \Lambda^n(\mathrm{V}^*) \times \Lambda^n \mathrm{V} \to \mathbb{K}$. Si (e_i) est une base de V et (e^i) la base duale, alors $b(e^{i_1} \wedge \cdots \wedge e^{i_n}, e_{j_1} \wedge \cdots \wedge e_{j_n}) = 1$ ou 0 suivant que $i_k \equiv j_k$ ou non. Ainsi la forme b est non dégénérée, et on obtient une dualité dans laquelle $(e^{i_1} \wedge \cdots \wedge e^{i_n})$ est la base duale de $(e_{i_1} \wedge \cdots \wedge e_{i_n})$.

4° On a $\Lambda^d f(e_1 \wedge \cdots \wedge e_d) = f(e_1) \wedge \cdots \wedge f(e_d) = (\sum f_{i1} e_i) \wedge \cdots \wedge (\sum f_{id} e_i) = (\det f) e_1 \wedge \cdots \wedge e_d$ après développement. □

3.3.5. Tenseurs antisymétriques. — Supposons $\mathrm{car}\,\mathbb{K} = 0$. Dans ce cas, on peut réaliser $\Lambda^n \mathrm{V}$ comme sous-espace vectoriel de $\mathrm{T}^n \mathrm{V}$ de la manière suivante. Si $\sigma \in \mathrm{S}_n$, alors σ induit un endomorphisme $\bar{\sigma}$ de $\mathrm{T}^n \mathrm{V}$, défini sur les tenseurs décomposables par

$$\bar{\sigma}(v_1 \otimes \cdots \otimes v_n) = v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}.$$

Un tenseur $t \in \mathrm{T}^n \mathrm{V}$ est dit **antisymétrique** si $\bar{\sigma}(v) = \epsilon(\sigma) v$ pour toute permutation $\sigma \in \mathrm{S}_n$, et on notera $a^n \mathrm{V} \subset \mathrm{T}^n \mathrm{V}$ l'espace des n-tenseurs antisymétriques.

L'application n-linéaire $p : \mathrm{V}^n \to \mathrm{T}^n \mathrm{V}$, définie par

$$p(v_1, \ldots, v_n) = \frac{1}{n!} \sum_{\sigma \in \mathrm{S}_n} \epsilon(\sigma) v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)},$$

s'étend en une application linéaire $p : \mathrm{T}^n\mathrm{V} \to \mathrm{T}^n\mathrm{V}$, d'image incluse dans $a^n\mathrm{V}$, et appelée antisymétrisation : par exemple $p(v_1 \otimes v_2) = \frac{1}{2}(v_1 \otimes v_2 - v_2 \otimes v_1)$.

3.3.6 Lemme. — *L'antisymétrisation satisfait $p^2 = p$, et $\ker p = \mathrm{I} \cap \mathrm{T}^n\mathrm{V}$. Donc p est une projection sur $a^n\mathrm{V}$, et on a une décomposition*

$$\mathrm{T}^n\mathrm{V} = (\mathrm{I} \cap \mathrm{T}^n\mathrm{V}) \oplus a^n\mathrm{V},$$

dans laquelle $a^n\mathrm{V} \simeq \Lambda^n\mathrm{V}$ par passage au quotient.

On fera attention qu'en revanche, $\oplus_n a^n\mathrm{V}$ n'est pas une sous-algèbre de TV, donc on ne peut pas décrire la structure d'algèbre de $\Lambda\mathrm{V}$ ainsi.

Démonstration. — Un calcul direct montre que $p^2 = p$, donc p est une projection sur $a^n\mathrm{V}$. Manifestement $\mathrm{I} \cap \mathrm{T}^n\mathrm{V} \subset \ker p$, donc p se factorise en un morphisme $\hat{p} : \Lambda^n\mathrm{V} \to a^n\mathrm{V}$. Si π est la projection $\mathrm{T}^n\mathrm{V} \to \Lambda^n\mathrm{V}$, alors $\pi|_{a^n\mathrm{V}}$ est surjective, d'où on déduit $\pi \circ \hat{p} = \mathrm{Id}_{\Lambda^n\mathrm{V}}$. Donc $\hat{p}$ est injective et $\mathrm{I} \cap \mathrm{T}^n\mathrm{V} = \ker p$. □

3.4. Pfaffien

Soit une matrice $2n \times 2n$ à valeurs dans le corps $\mathbb{K}$, antisymétrique, $\mathrm{A} = (a_{ij})$. On lui associe

$$\rho(\mathrm{A}) = \sum_{i<j} a_{ij} e_i \wedge e_j \quad \in \Lambda^2\mathbb{K}^{2n}.$$

Alors $\rho(\mathrm{A})^n \in \Lambda^{2n}\mathbb{K}^{2n}$. Soit $(e_1, \ldots, e_{2n})$ une base standard de $\mathbb{K}^{2n}$, alors on définit le **pfaffien** de A par la formule :

$$\rho(\mathrm{A})^n = n!\,\mathrm{Pf}(\mathrm{A})\, e_1 \wedge \cdots \wedge e_{2n}. \tag{31}$$

A priori, cette formule ne définit Pf(A) que si $\mathrm{car}\,\mathbb{K} = 0$. Néanmoins, en développant $\rho(\mathrm{A})^n$, on s'aperçoit que, pour $\mathrm{car}\,\mathbb{K} = 0$, le pfaffien Pf(A) est un polynôme à coefficients entiers en les coefficients de la matrice A :

$$\mathrm{Pf} \in \mathbb{Z}[a_{ij}]. \tag{32}$$

Pour un corps quelconque, on utilise le morphisme d'anneau $\phi : \mathbb{Z} \to \mathbb{K}$ pour obtenir à partir de (32) le pfaffien $\mathrm{Pf} \in \mathbb{K}[a_{ij}]$.

Exemple. — Considérons la matrice

$$\mathrm{A} = \begin{pmatrix} 0 & \lambda_1 & & & \\ -\lambda_1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & \lambda_n \\ & & & -\lambda_n & 0 \end{pmatrix}. \tag{33}$$

Alors $\rho(\mathrm{A}) = \sum_i \lambda_i e_{2i-1} \wedge e_{2i}$, et $\mathrm{Pf}(\mathrm{A}) = \prod_i \lambda_i$.

3.4.1 Lemme. — *Pour toute matrice* P, *on a* $\rho(\mathrm{P}^t\mathrm{AP}) = \Lambda^2\mathrm{P}(\rho(\mathrm{A}))$.

Démonstration. — Par calcul direct : si $P = (p_{ij})$, $A = (a_{ij})$, alors $P^tAP = (\sum_{k,l} p_{ki}a_{kl}p_{lj})$, et

$$\begin{aligned}\rho(P^tAP) &= \sum_{i<j}\sum_{kl} p_{ki}a_{kl}p_{lj}e_i\wedge e_j = \frac{1}{2}\sum_{ijkl} p_{ki}a_{kl}p_{lj}e_i\wedge e_j\\ &= \frac{1}{2}\sum_{kl} a_{kl}P(e_k)\wedge P(e_l) = \sum_{k<l} a_{kl}P(e_k)\wedge P(e_l)\\ &= \Lambda^2 P(\rho(A)).\end{aligned}$$

□

3.4.2 Lemme. — *On a l'identité* $\mathrm{Pf}(P^tAP) = (\det P)\,\mathrm{Pf}(A)$. [1]

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 $\mathbb{K} = \mathbb{Q}$. Mettant l'égalité du lemme 3.4.1 à la puissance n, on obtient

$$\begin{aligned}n!\,\mathrm{Pf}(P^tAP)e_1\wedge\cdots\wedge e_{2n} &= \left(\Lambda^2 P(\rho(A))\right)^n\\ &= \Lambda^{2n}P(\rho(A)^n)\\ &= (\det P)\,n!\,\mathrm{Pf}(A)e_1\wedge\cdots\wedge e_{2n},\end{aligned}$$

où la deuxième égalité utilise que ΛP est un morphisme d'algèbres. □

3.4.3 Théorème. — *On a l'identité* $\mathrm{Pf}(A)^2 = \det(A)$.

Démonstration. — Le théorème est vrai sur les matrices de type (33), puisque le pfaffien est $\prod_i \lambda_i$ et le déterminant $\prod_i \lambda_i^2$. Or, par la théorie des formes alternées, toute matrice anti-symétrique s'écrit sous la forme P^tAP, où P est inversible et A de la forme (33), avec $\lambda_i = 1$ ou 0. (Il suffit de décomposer $\mathbb{K}^{2n} = F\oplus G$, avec $F = \ker A$, et de choisir une base hyperbolique de G). Le théorème découle alors du lemme 3.4.2. □

Comme conséquence, on obtient une seconde démonstration du fait que les transformations symplectiques sont de déterminant 1 :

3.4.4 Corollaire. — *On a l'inclusion* $\mathrm{Sp}(n,\mathbb{K}) \subset \mathrm{SL}(2n,\mathbb{K})$.

Démonstration. — Soit A la matrice anti-symétrique d'une forme alternée dans une base, alors

$$\mathrm{Sp}(n,\mathbb{K}) = \{P \in M_{2n}(\mathbb{K}), P^tAP = A\}.$$

Nécessairement, un élément $P \in \mathrm{Sp}(n,\mathbb{K})$ satisfait $\det(P)\,\mathrm{Pf}(A) = \mathrm{Pf}(A)$, ce qui implique $\det(P) = 1$ puisque A est inversible. □

1. En particulier, pour $P \in SO(2n)$, on a $P^t = P^{-1}$ et on obtient $\mathrm{Pf}(P^{-1}AP) = \mathrm{Pf}(A)$. Vous verrez plus tard que les matrices anti-symétriques sont l'*algèbre de Lie* du groupe $SO(2n)$, donc le pfaffien est un polynôme sur cette algèbre de Lie, invariant sous la conjugaison par les éléments du groupe $SO(2n)$. Ces polynômes invariants jouent un rôle important en théorie des groupes et algèbres de Lie, l'exemple le plus simple étant les $A \mapsto \mathrm{Tr}(A^k)$ qui sont des polynômes invariants par conjugaison sous le groupe général linéaire.

3.5. 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 $f : \mathrm{V} \to \mathrm{A}$ où A est une algèbre *commutative* avec unité. L'algèbre solution de ce problème est l'**algèbre symétrique** SV, obtenue comme le quotient

$$\mathrm{SV} = \mathrm{TV}/\mathrm{J},$$

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 $\mathrm{J} = \oplus_n \mathrm{J} \cap \mathrm{T}^n\mathrm{V}$, et on a une décomposition

$$\mathrm{SV} = \oplus \mathrm{S}^n\mathrm{V}, \quad \mathrm{S}^n\mathrm{V} = \mathrm{T}^n\mathrm{V}/(\mathrm{J} \cap \mathrm{T}^n\mathrm{V}).$$

En particulier, $\mathrm{S}^0\mathrm{V} = \mathbb{K}$ et $\mathrm{S}^1\mathrm{V} = \mathrm{V}$, d'où l'injection canonique $\mathrm{V} \hookrightarrow \mathrm{SV}$. Le produit dans l'algèbre symétrique est noté sans signe particulier : par exemple $v_1 v_2 = v_2 v_1$.

Un morphisme $f : \mathrm{V} \to \mathrm{W}$ donne un morphisme $\mathrm{S}f : \mathrm{SV} \to \mathrm{SW}$, avec $\mathrm{S}f = \oplus_n \mathrm{S}^n f$. On a bien sûr la propriété $\mathrm{S}(f \circ g) = \mathrm{S}f \circ \mathrm{S}g$.

Les propriétés de $\mathrm{S}^n\mathrm{V}$ sont les suivantes :

1° L'application n-linéaire symétrique de V^n vers $\mathrm{S}^n\mathrm{V}$, définie par $(v_1, \dots, v_n) \mapsto v_1 \cdots v_n$, est universelle pour cette propriété (une application n-linéaire f est **symétrique** si $f(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = f(v_1, \dots, v_n)$ pour tout $\sigma \in \mathrm{S}_n$) ; en particulier $(\mathrm{S}^n\mathrm{V})^* = \mathrm{Sym}^n \mathrm{V}$, l'espace des formes n-linéaires symétriques sur V.

2° Si $(e_i)_{i \in \mathrm{I}}$ est une base de V, alors une base de $\mathrm{S}^n\mathrm{V}$ est donnée par les $(e_{i_1}^{k_1} \dots e_{i_r}^{k_r})$ pour tout r-uplet $i_1 < \cdots < i_r$ et entiers k_i tels que $k_1 + \cdots k_r = n$; si $\dim \mathrm{V} = d$, on a

$$\dim \mathrm{S}^n\mathrm{V} = \mathrm{C}_{n+d-1}^{d-1}.$$

En particulier, SV est toujours de dimension infinie, contrairement à $\Lambda\mathrm{V}$.

3° L'algèbre SV est isomorphe à l'algèbre de polynômes $\mathbb{K}[\mathrm{X}_1, \dots, \mathrm{X}_d]$: si $(e_1, \dots, e_d)$ est une base de V, un isomorphisme est obtenu en envoyant e_i sur X_i.

4° Si $\mathrm{car}\,\mathbb{K} = 0$, on peut réaliser $\mathrm{S}^n\mathrm{V}$ à l'intérieur de $\mathrm{T}^n\mathrm{V}$ comme le sous-espace $s^n\mathrm{V}$ des **tenseurs symétriques**, c'est-à-dire des tenseurs t satisfaisant $\bar{\sigma}(t) = t$ pour tout $\sigma \in \mathrm{S}_n$; en effet, on dispose alors d'une **symétrisation** $q : \mathrm{T}^n\mathrm{V} \to \mathrm{T}^n\mathrm{V}$

$$q(v_1 \otimes \cdots \otimes v_n) = \frac{1}{n!} \sum_{\sigma \in \mathrm{S}_n} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)},$$

vérifiant $q^2 = q$, donc est une projection sur $s^n\mathrm{V}$, de noyau $\mathrm{J} \cap \mathrm{T}^n\mathrm{V}$. Ainsi,

$$\mathrm{T}^n\mathrm{V} = (\mathrm{J} \cap \mathrm{T}^n\mathrm{V}) \oplus s^n\mathrm{V}, \quad s^n\mathrm{V} \simeq \mathrm{S}^n\mathrm{V}.$$

5° Pour $n = 2$, si $\mathrm{car}\,\mathbb{K} \neq 2$, 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 anti-symétrique et d'un tenseur symétrique :

$$\mathrm{T}^2\mathrm{V} = a^2\mathrm{V} \oplus s^2\mathrm{V}. \tag{34}$$

CHAPITRE 4

REPRÉSENTATIONS DES GROUPES FINIS

4.1. Représentations

Soit G un groupe et V un $\mathbb{K}$-espace vectoriel. Une **représentation linéaire** de G dans V est un morphisme de groupes

$$\rho : G \longrightarrow GL(V).$$

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 $g \cdot v$ $(= \rho(g)(v))$.

Exemples. — 1° Si $V = \mathbb{C}$, alors une représentation de G dans V est un morphisme $\rho : G \to \mathbb{C}^*$; si G est fini, l'image est un groupe cyclique.

2° Si $(e_1, \ldots, e_n)$ est une base de $\mathbb{K}^n$, on obtient une représentation de S_n dans $\mathbb{K}^n$ 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.

3° Si G est défini comme un sous-groupe de GL(V) (ce qui est le cas de tous les groupes classiques), alors l'inclusion $G \hookrightarrow GL(V)$ est appelée la **représentation standard**.

4.1.1. Algèbre de groupe. — Soit G un groupe fini. À partir du groupe G on construit une l'**algèbre du groupe**, $\mathbb{K}[G]$, qui est une $\mathbb{K}$-algèbre avec unité. Comme $\mathbb{K}$-espace vectoriel, on a

$$\mathbb{K}[G] = G^{\mathbb{K}} = \{f : G \longrightarrow \mathbb{K}\}.$$

Le produit sur $\mathbb{K}[G]$ est le produit de convolution, défini par

$$f * g(x) = \sum_{y \in G} f(y) g(y^{-1}x).$$

Une autre description de ce produit peut être donnée de la manière suivante : à un élément $g \in G$ on associe $\epsilon_g \in \mathbb{K}[G]$ la fonction caractéristique de $\{g\}$ ($\epsilon_g(h) = 1$ si $g = h$ et 0 sinon). Alors $(\epsilon_g)_{g \in G}$ est une base de $\mathbb{K}[G]$, et la multiplication est définie par

$$\epsilon_g \epsilon_{g'} = \epsilon_{gg'}.$$

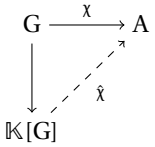
L'application

$$G \to \mathbb{K}[G]^\times, \quad g \longmapsto \epsilon_g,$$

est donc un morphisme de groupes, injectif. Il identifie G à une partie de $\mathbb{K}[G]$, et on identifiera dorénavant g et ϵ_g. Ainsi tout élément f de $\mathbb{K}[G]$ s'écrit-il

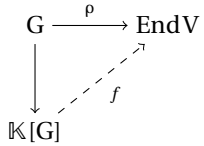
$$f = \sum_{g\in G} f_g g, \quad f_g \in \mathbb{K}.$$

4.1.2 Lemme **(Propriété universelle de** $\mathbb{K}[G]$**).** — *Si on a une application* $\chi : G \to A$*, où* A *est une* $\mathbb{K}$*-algèbre avec unité, telle que* $\operatorname{im}\chi \subset A^\times$ *et* $\chi : G \to A^\times$ *est un morphisme, alors il existe un unique morphisme d'algèbres* $\hat{\chi} : \mathbb{K}[G] \to A$ *rendant le diagramme suivant commutatif :*



Démonstration. — Il suffit de poser $\hat{\chi}(\sum_g f_g g) = \sum_g f_g \chi(g)$. □

Exemples. — 1° Si on a une représentation linéaire ρ de G dans V, on peut appliquer le lemme pour produire un morphisme d'algèbres $f : \mathbb{K}[G] \to \operatorname{End} V$:



On obtient ainsi une action de $\mathbb{K}[G]$ sur V par

$$u \in \mathbb{K}[G], v \in V, \quad u \cdot v = f(u)(v).$$

L'espace V est ainsi un $\mathbb{K}[G]$-**module à gauche** (c'est-à-dire l'application $\mathbb{K}[G] \times V \to V$ est bilinéaire et satisfait $a \cdot (b \cdot v) = (ab) \cdot v$). Réciproquement, si V est un $\mathbb{K}[G]$-module à gauche, alors on obtient une représentation de G dans V par restriction à G, donc une représentation de G dans V est la même chose que la donnée sur V d'une structure de $\mathbb{K}[G]$-module à gauche.

2° En particulier, $\mathbb{K}[G]$ est une représentation de G appelée **représentation régulière**. On peut voir aussi directement cette représentation de G quand on décrit $\mathbb{K}[G]$ comme espace des fonctions de $G \to \mathbb{K}$, alors l'action de $g \in G$ sur une fonction f est par

$$(g \cdot f)(x) = f(g^{-1}x).$$

4.1.3. Vocabulaire et propriétés. — Soit (V, ρ) une représentation de G.

La représentation est **fidèle** si ρ est injective.

Le **degré** de la représentation est $\dim V$.

Une **sous-représentation** est un sous-espace $W \subset V$ stable sous l'action de G, on parle d'un sous-espace G-invariant. Dans ce cas, on a une représentation induite sur le quotient V/W.

Exemples. — 1° Le sous-espace des vecteurs fixes sous G,

$$\mathrm{V}^{\mathrm{G}} = \{v \in \mathrm{V}, g \cdot v = v \text{ pour tout } g \in \mathrm{G}\}$$

est un sous-espace G-invariant.

2° Si V, de base $(e_1, \ldots, e_n)$, est une représentation de permutation du groupe S_n, alors

$$\mathrm{V}_0 = \{\sum_i x_i e_i, x_i \in \mathbb{K}, \sum_i x_i = 0\}$$

est une sous-représentation de V.

Un **morphisme** entre deux représentations V_1 et V_2 est une application linéaire $f : \mathrm{V}_1 \to \mathrm{V}_2$ telle que pour tout $g \in \mathrm{G}$, on ait

$$f \circ \rho_1(g) = \rho_2(g) \circ f.$$

C'est équivalent à dire que f est $\mathbb{K}[\mathrm{G}]$-linéaire. Dans ce cas, $\ker f$ et $\operatorname{im} f$ sont des sous-représentations de V_1 et V_2, et f induit un isomorphisme de représentations

$$f : \mathrm{V}_1 / \ker f \xrightarrow{\sim} \operatorname{im} f.$$

L'espace des morphismes entre V_1 et V_2 est noté $\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}_1, \mathrm{V}_2)$, ou $\mathrm{Hom}(\rho_1, \rho_2)$.

Exemple. — Soit $\mathrm{V} = \mathbb{K}[\mathrm{G}]$, alors l'espace des endomorphismes de la représentation V est $\mathrm{End}_{\mathrm{G}}\mathbb{K}[\mathrm{G}] = \mathbb{K}[\mathrm{G}]$, où l'élément $u \in \mathbb{K}[\mathrm{G}]$ agit sur $\mathbb{K}[\mathrm{G}]$ par multiplication à droite.

Si V et W sont des représentations de G, alors on peut former les représentations suivantes :

- $\mathrm{V} \oplus \mathrm{W}$ pour $\rho(g) = (\rho_{\mathrm{V}}(g), \rho_{\mathrm{W}}(g))$;
- $\mathrm{V} \otimes \mathrm{W}$ pour $\rho(g) = \rho_{\mathrm{V}}(g) \otimes \rho_{\mathrm{W}}(g)$;
- V^* pour $\check{\rho}(g) = \rho(g^{-1})^t$;
- $\mathrm{Hom}_{\mathbb{K}}(\mathrm{V}, \mathrm{W}) = \mathrm{V}^* \otimes \mathrm{W}$ pour $\rho(g)(f) = \rho_{\mathrm{W}}(g) \circ f \circ \rho_{\mathrm{V}}(g)^{-1}$; en particulier l'espace des morphismes de représentations de V vers W est

$$\mathrm{Hom}_{\mathrm{G}}(\mathrm{V}, \mathrm{W}) = \mathrm{Hom}_{\mathbb{K}}(\mathrm{V}, \mathrm{W})^{\mathrm{G}};$$

- $\mathrm{T}^k\mathrm{V}$, $\Lambda^k\mathrm{V}$, $\mathrm{S}^k\mathrm{V}$ sont aussi des représentations de G ; en particulier on notera que, comme représentation, par (34),

$$\mathrm{V} \otimes \mathrm{V} = \Lambda^2\mathrm{V} \oplus \mathrm{S}^2\mathrm{V}.$$

Enfin, la représentation V est **irréductible** si ses seules sous-représentations sont 0 et V.

Exemples. — 1° Si G est abélien et $\mathbb{K} = \mathbb{C}$ (ou un corps algébriquement clos), alors les $\rho(g)$ se diagonalisent simultanément, donc les seules représentations irréductibles de G sont de degré 1. Ainsi les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}$ sont données par l'image d'un générateur, qui doit être une racine n-ième de l'unité dans $\mathbb{C}$. On obtient ainsi les n représentations irréductibles ρ_j ($j = 0, \ldots, n-1$), données par

$$\rho_j(k) = \exp(kj\tfrac{2\pi i}{n}).$$

2° La représentation standard du groupe diédral D_n dans $\mathbb{R}^2$ est irréductible. Il en est de même de la représentation dans la complexification $\mathbb{C}^2$. (La complexification d'une représentation réelle irréductible n'est pas forcément irréductible ; trouver un contre-exemple).

4.1.4. Supplémentaire G-invariant. — Si W est une sous-représentation de V, il n'existe pas en général de supplémentaire G-invariant W′ de W dans V.

Exemple. — Le groupe des matrices triangulaires supérieures $T \subset GL(2,\mathbb{F}_p)$,

$$T = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\},$$

se représente dans $V = \mathbb{F}_p^2$ (représentation standard). Alors $W = \mathbb{K}e_1$ est une sous-représentation dépourvue de supplémentaire T-invariant. En particulier, la représentation standard $\mathbb{F}_p^2$ n'est pas isomorphe à la représentation $W \oplus V/W$.

Néanmoins, il y a quand même un résultat général d'existence de supplémentaire G-invariant :

4.1.5 Théorème. — *Si* G *est un groupe fini tel que* $\mathrm{car}\,\mathbb{K} \nmid |G|$, *et* V *est une représentation de* G, *alors tout sous-espace* G*-invariant admet un supplémentaire* G*-invariant.*

4.1.6 Corollaire. — *Si* $\mathrm{car}\,\mathbb{K} \nmid |G|$, *alors toute représentation de* G *de dimension finie est somme directe de représentations irréductibles.*

On va donner deux démonstrations du théorème, une première particulière à $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, mais qui est valable aussi pour certains groupes non finis ; et une seconde traitant tous les corps.

Première démonstration. — Supposons $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$. On choisit un produit scalaire ou un produit scalaire hermitien défini positif sur V, noté $\langle .,. \rangle_0$. Puis on définit un autre produit scalaire par

$$\langle v, w \rangle = \frac{1}{|G|} \sum_{g \in G} \langle g \cdot v, g \cdot w \rangle_0. \tag{35}$$

Ce nouveau produit scalaire est G-invariant : pour tous $g \in G$, 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 G-invariant, alors $W^\perp$ 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 compact, il est muni d'une mesure de probabilité G-invariante, la mesure de Haar : en remplaçant (35) par l'intégration sur le groupe, la démonstration s'étend à ce cas.

Seconde démonstration. — On commence par traiter le cas particulier où $W = V^G$. Pour $x \in V$ on définit

$$\pi(x) = \frac{1}{|G|} \sum_{g \in G} g \cdot x.$$

Sous l'hypothèse sur $\mathrm{car}\,\mathbb{K}$, cette formule a un sens, et est une projection G-invariante sur $W = V^G$. Donc $\ker \pi$ est le supplémentaire souhaité de W.

En général, on choisit une projection quelconque p sur W, donc $p \in \mathrm{Hom}(V,W)$. Appliquant la projection π dans la représentation $\mathrm{Hom}(V,W)$, on fabrique

$$\pi(p) = \frac{1}{|G|}\sum_{g\in G} \rho_W(g)\circ p\circ \rho_V(g)^{-1} \in \mathrm{Hom}_G(V,W) \tag{36}$$

est encore une projection sur W donc $\ker\pi(p)$ est un supplémentaire G-invariant de W. □

4.1.7 Lemme de Schur. — *1° Si ρ_1 et ρ_2 sont deux représentations irréductibles de* G*, alors tout morphisme non nul $f : \rho_1 \to \rho_2$ est inversible.*

2° Si en outre $\rho = \rho_1 = \rho_2$ et $\mathbb{K}$ est algébriquement clos, alors l'algèbre des endomorphismes de ρ est réduite aux homothéties.

Démonstration. — 1° Les sous-espaces $\ker f$ et $\mathrm{im} f$ sont G-invariants, donc triviaux.

2° Si $f \in \mathrm{End}(\rho)$ a une valeur propre λ, alors $\ker(u-\lambda)$ est G-invariant, donc égal à V tout entier. Donc f est une homothétie. □

Exemple. — Sous les hypothèses du théorème, on a

$$\mathbb{K}[G] = \oplus R_i,$$

avec R_i représentation irréductible. Si V est une représentation irréductible de G, et $v_0 \neq 0$, alors l'application

$$\nu : \mathbb{K}[G] \longrightarrow V, \quad u \longmapsto u\cdot v_0,$$

est un morphisme de représentations, donc est nécessairement surjectif. Par le lemme de Schur, il y a au moins un i tel que $\nu|_{R_i}$ soit un isomorphisme. Donc V est isomorphe à l'une des représentations R_i, et on en déduit :

4.1.8 Corollaire. — *Si* $\mathrm{car}\,\mathbb{K} \nmid |G|$*, alors, à isomorphisme près, il n'y a qu'un nombre fini de représentations irréductibles de* G*, et chacune est de degré* $\leqslant |G|$.

4.1.9 Corollaire. — *Sous la même hypothèse, soient $R_1,\dots,R_k$ les représentations irréductibles de* G*, alors toute représentation se décompose en $V = \oplus n_i R_i$, où les entiers naturels n_i sont uniquement déterminés par la représentation.*

Une démonstration plus simple de ce corollaire sera vue en § 4.2 si $\mathrm{car}\,\mathbb{K} = 0$, à l'aide de la théorie des caractères, mais la démonstration qui suit est générale.

Démonstration. — Par récurrence sur la dimension de V. Supposons $V = \oplus V_i = \oplus W_i$, où les V_i et les W_i sont des représentations irréductibles, éventuellement répétées. On va montrer qu'à permutation près, les (V_i) et les (W_i) sont le même ensemble de représentations. On dispose donc d'un isomorphisme de représentations

$$f : \oplus V_i \to \oplus W_i,$$

dont on notera l'inverse g. Notons $p_i : V \to V_i$ et $q_i : V \to W_i$ les projections. Alors $\mathrm{Id}_{V_1} = \sum p_1 g|_{W_i} q_i f|_{V_1}$, donc l'un des facteurs est non nul, quitte à réarranger les W_i on peut supposer que c'est le premier, donc $p_1 g|_{W_1} q_1 f|_{V_1} \neq 0$. Par le lemme de Schur, c'est un isomorphisme, donc

$$p_1 g|_{W_1} : W_1 \to V_1 \quad \text{et} \quad q_1 f|_{V_1} : V_1 \to W_1$$

sont aussi des isomorphismes. Pour appliquer l'hypothèse de récurrence, il suffit de montrer que

$$(1-q_1)f|_{\oplus_{i\geqslant 2}\mathrm{V}_i} : \oplus_{i\geqslant 2}\mathrm{V}_i \longrightarrow \oplus_{i\geqslant 2}\mathrm{W}_i$$

est encore un isomorphisme. En effet, si $x \in \oplus_{i\geqslant 2}\mathrm{V}_i$ est dans le noyau, alors $f(x) \in \mathrm{W}_1$, et $p_1 g(f(x)) = p_1(x) = 0$, donc, $p_1 g|_{\mathrm{W}_1}$ étant un isomorphisme, $f(x) = 0$ donc $x = 0$. □

4.2. Caractères

Dans cette section, on suppose $\mathbb{K}$ *algébriquement clos et* $\operatorname{car}\mathbb{K} \nmid |\mathrm{G}|$.

Si (V,ρ) est une représentation de G, on appelle **caractère** de ρ la fonction $\chi_\rho : \mathrm{G} \to \mathbb{K}$ définie par

$$\chi_\rho(g) = \operatorname{Tr}\rho(g).$$

En particulier, $\chi_\rho(1) = \dim \mathrm{V}$, donc le caractère détermine le degré de la représentation (on verra plus tard que si $\mathbb{K} = \mathbb{C}$, il détermine ρ tout entier).

On calcule

$$\chi_\rho(ghg^{-1}) = \operatorname{Tr}\big(\rho(g)\rho(h)\rho(g)^{-1}\big) = \operatorname{Tr}\big(\rho(h)\big) = \chi_\rho(h).$$

On dit que χ_ρ est une **fonction centrale**, ou encore **invariante par conjugaison**. L'espace de toutes les fonctions centrales sur le groupe G sera noté $\mathscr{C}(\mathrm{G})$.

Exemples. — 1° Le caractère de la représentation régulière est

$$\chi_{\mathrm{reg}}(g) = \begin{cases} |\mathrm{G}| & g = e, \\ 0 & g \neq e. \end{cases}$$

2° Le caractère de la représentation standard de D_n dans $\mathbb{C}^2$ est donné par

$$\chi(r^k) = 2\cos\big(2k\frac{\pi}{n}\big), \quad \chi(sr^k) = 0.$$

4.2.1 Propriétés. — *1° Deux représentations isomorphes ont même caractère.*

2° $\chi_{\mathrm{V}^*}(g) = \chi_{\mathrm{V}}(g^{-1})$.

3° $\chi_{\mathrm{V}\oplus\mathrm{W}} = \chi_{\mathrm{V}} + \chi_{\mathrm{W}}$ *; si* $\mathrm{W} \subset \mathrm{V}$ *alors* $\chi_{\mathrm{V}} = \chi_{\mathrm{W}} + \chi_{\mathrm{V}/\mathrm{W}}$.

4° $\chi_{\mathrm{V}\otimes\mathrm{W}} = \chi_{\mathrm{V}}\chi_{\mathrm{W}}$.

Démonstration. — Tout est évident, sauf la quatrième propriété qui découle de l'identité

$$\operatorname{Tr}(u\otimes v) = \operatorname{Tr}(u)\operatorname{Tr}(v)$$

que l'on peut vérifier dans une base. □

On introduit sur $\mathbb{K}[\mathrm{G}] = \{f : \mathrm{G} \to \mathbb{K}\}$ la forme bilinéaire symétrique

$$\langle f, g\rangle = \frac{1}{|\mathrm{G}|}\sum_{x\in\mathrm{G}} f(x^{-1})g(x).$$

En particulier, $\langle \epsilon_x, f\rangle = \frac{1}{|\mathrm{G}|}f(x^{-1})$, donc cette forme est non dégénérée.

Si $\mathbb{K} = \mathbb{C}$, on a vu que la représentation V admet un produit hermitien invariant par G. Alors $\rho(g) \in \mathrm{U}(\mathrm{V})$, et donc $\rho(g^{-1}) = \rho(g)^*$, qui implique

$$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}. \tag{37}$$

Ainsi, sur les caractères, $\langle \chi, \chi'\rangle$ est le produit scalaire hermitien standard de $\mathbb{C}[\mathrm{G}]$.

4.2.2 Théorème. — *Les caractères des représentations irréductibles forment une base orthonormée de* $\mathscr{C}(\mathrm{G})$*, l'espace des fonctions centrales sur* G.

La démonstration du théorème va utiliser les deux lemmes suivants :

4.2.3 Lemme. — *Soit* $\pi : \mathrm{Hom}_{\mathbb{K}}(\mathrm{V},\mathrm{W}) \to \mathrm{Hom}_{\mathrm{G}}(\mathrm{V},\mathrm{W}) \subset \mathrm{Hom}_{\mathbb{K}}(\mathrm{V},\mathrm{W})$ *la projection définie par (36), alors*

$$\mathrm{Tr}\,\pi = \langle \chi_{\mathrm{V}}, \chi_{\mathrm{W}} \rangle.$$

Démonstration. — Plaçons-nous dans des bases de V et W, soit E_{ij} la matrice élémentaire dont tous les termes sont nuls, sauf le terme d'ordre (i,j), égal à 1. Alors

$$\big(\rho_{\mathrm{W}}(g) \circ \mathrm{E}_{ij} \circ \rho_{\mathrm{V}}(g)^{-1}\big)_{kl} = \rho_{\mathrm{W}}(g)_{ki}\rho_{\mathrm{V}}(g^{-1})_{jl}. \tag{38}$$

Appliquant au cas particulier $i = k$ et $j = l$, on calcule

$$\begin{aligned}
\mathrm{Tr}\,\pi = \sum_{ij} \pi(\mathrm{E}_{ij})_{ij} &= \frac{1}{|\mathrm{G}|} \sum_{g\in\mathrm{G}} \sum_{ij} \rho_{\mathrm{W}}(g)_{ii}\rho_{\mathrm{V}}(g^{-1})_{jj} \\
&= \frac{1}{|\mathrm{G}|} \sum_{g\in\mathrm{G}} \big(\sum_i \rho_{\mathrm{W}}(g)_{ii}\big)\big(\sum_j \rho_{\mathrm{V}}(g^{-1})_{jj}\big) \\
&= \frac{1}{|\mathrm{G}|} \sum_{g\in\mathrm{G}} \chi_{\mathrm{W}}(g)\chi_{\mathrm{V}}(g^{-1}).
\end{aligned}$$

□

4.2.4 Lemme. — *Soit* (V,ρ) *une représentation de* G. *Si* f *est une fonction centrale sur* G, *définissons*

$$f_\rho = \frac{1}{|\mathrm{G}|} \sum_{\mathrm{G}} f(g)\rho(g^{-1}) \in \mathrm{End}_{\mathbb{K}}(\mathrm{V}).$$

Alors $f_\rho \in \mathrm{End}\,\rho$ *et* $\mathrm{Tr}(f_\rho) = \langle f, \chi_\rho \rangle$.

Démonstration. — On calcule, puisque f est centrale,

$$\rho(x)^{-1} \circ f_\rho \circ \rho(x) = \frac{1}{|\mathrm{G}|} \sum_{g\in\mathrm{G}} f(g)\rho(x^{-1}g^{-1}x) = \frac{1}{|\mathrm{G}|} \sum_{g\in\mathrm{G}} f(g)\rho(g^{-1}) = f_\rho.$$

Donc $f_\rho \in \mathrm{End}\,\rho$, et sa trace est

$$\mathrm{Tr}\, f_\rho = \frac{1}{|\mathrm{G}|} \sum_{g\in\mathrm{G}} f(g)\chi(g^{-1}) = \langle f, \chi_\rho \rangle.$$

□

Démonstration du théorème 4.2.2. — Soient V et W deux représentation irréductibles. Par le lemme de Schur, on a

$$\mathrm{Hom}_{\mathrm{G}}(\mathrm{V},\mathrm{W}) = \begin{cases} 0 & \text{V et W non isomorphes,} \\ \mathbb{K} & \text{V et W isomorphes.} \end{cases}$$

Par le lemme 4.2.3, $\langle \chi_{\mathrm{V}}, \chi_{\mathrm{W}} \rangle = \mathrm{Tr}\,\pi$ vaut 0 dans le premier cas, 1 dans le second. Donc la famille (χ_{V}) pour V irréductible est orthonormale, il reste à voir qu'elle engendre tout $\mathscr{C}(\mathrm{G})$.

Observons que si ρ est irréductible, alors par le lemme 4.2.4 appliqué à la fonction centrale χ_ρ, on déduit que f_{χ_ρ} est une homothétie, et $\mathrm{Tr}\, f_{\chi_\rho} = (\deg\rho) f_{\chi_\rho} = \langle \chi_\rho, \chi_\rho \rangle = 1$, d'où en particulier $\deg\rho$ est inversible dans $\mathbb{K}$.

Pour une fonction centrale f et une représentation irréductible ρ quelconques, f_ρ est une homothétie de rapport $\frac{\langle f, \chi_\rho \rangle}{\deg\rho}$. Si f est orthogonale à tous les caractères, alors $f_\rho = 0$ pour toutes les représentations irréductibles, et donc pour toutes les représentations. Appliquons à la représentation régulière :

$$f_{\rho_{\mathrm{reg}}} = \frac{1}{|\mathrm{G}|} \sum_{\mathrm{G}} f(g) g^{-1} = 0$$

dans $\mathbb{K}[\mathrm{G}]$, ce qui entraîne $f = 0$. □

4.2.5 Corollaire. — *1° Le nombre de représentations irréductibles de* G *est égal au nombre de classes de conjugaison de* G.

2° Soient $\rho_1, \ldots, \rho_\ell$ *les représentations irréductibles de* G. *On note* $[g]$ *la classe de conjugaison de* g *dans* G. *Alors*

$$\sum_1^\ell \chi_i(g^{-1}) \chi_i(h) = \begin{cases} \frac{|\mathrm{G}|}{|[g]|} & \text{si } h \in [g], \\ 0 & \text{sinon.} \end{cases}$$

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 $f = 1_{[g]}$ la fonction caractéristique de la classe de conjugaison de g, alors f est une fonction centrale qui se décompose sur les caractères χ_i des représentations irréductibles :

$$f = \sum \langle f, \chi_i \rangle \chi_i, \quad \langle f, \chi_i \rangle = \frac{1}{|\mathrm{G}|} |[g]| \chi_i(g^{-1}).$$

Il en résulte

$$1_{[g]}(h) = f(h) = \frac{|[g]|}{|\mathrm{G}|} \sum \chi_i(g^{-1}) \chi_i(h),$$

ce qui est exactement le résultat voulu. □

4.2.6 Corollaire. — *Si* $\mathrm{car}\,\mathbb{K} = 0$, *alors, en notant* $\rho_1, \ldots, \rho_\ell$ *les représentations irréductibles de* G *:*

- *si* $\rho \simeq \sum_1^\ell n_i \rho_i$, *alors* $n_i = \langle \chi_\rho, \chi_{\rho_i} \rangle$ *et* $\langle \chi_\rho, \chi_\rho \rangle = \sum_i n_i^2$ *; en particulier,* ρ *et* ρ' *sont équivalentes si et seulement si* $\chi_\rho = \chi_{\rho'}$ *;*
- *la représentation régulière se décompose en* $\mathbb{K}[\mathrm{G}] = \sum_1^\ell (\dim \rho_i) \rho_i$, *en particulier* $\sum_1^\ell (\dim \rho_i)^2 = |\mathrm{G}|$.

Remarques. — Le premier énoncé donne une autre démonstration du corollaire 4.1.9 si $\mathrm{car}\,\mathbb{K} = 0$. Si $\mathrm{car}\,\mathbb{K} = p \neq 0$, il est faux que le caractère détermine la représentation, par exemple le caractère de pV est nul. En revanche, le second énoncé reste vrai si $\mathrm{car}\,\mathbb{K} \neq 0$.

On verra en § 4.3 qu'on a un isomorphisme d'algèbres $\mathbb{K}[\mathrm{G}] \simeq \sum_1^\ell \mathrm{End}(\mathrm{V}_{\rho_i})$, alors que le second énoncé du corollaire ne donne que l'égalité des dimensions.

Une autre contrainte importante sur les dimensions des représentations irréductibles est que leurs dimensions divisent l'ordre du groupe. Ce théorème plus difficile sera vu en § 4.4.

Démonstration. — Si $\rho = \sum_1^\ell n_i \rho_i$ alors $\chi_\rho = \sum_1^\ell n_i \chi_{\rho_i}$ donc $n_i = \langle \chi_\rho, \chi_{\rho_i} \rangle$. Ainsi χ_ρ détermine-t-il les n_i et donc toute la représentation ρ, et $\langle \chi_\rho, \chi_\rho \rangle = \sum_1^l n_i^2$.

Appliquons cela à la représentation régulière : puisque $\chi_{\text{reg}} = |G| 1_{\{e\}}$, on obtient $\langle \chi_{\text{reg}}, \chi_i \rangle = \chi_i(e) = \deg \rho_i$, d'où il résulte que la représentation régulière est isomorphe à $\oplus_1^\ell (\deg \rho_i)\rho_i$. □

4.2.7 Proposition. — *Le groupe* G *est abélien si et seulement si toutes ses représentations irréductibles sont de degré* 1.

Démonstration. — Un groupe G est abélien si et seulement s'il a exactement |G| classes de conjugaison, donc |G| représentations irréductibles. Or $|G| = \sum_1^\ell (\deg \rho_i)^2$, donc $\ell \leqslant |G|$ avec égalité si et seulement si toutes les représentations irréductibles sont de degré 1. □

4.2.8 Corollaire. — *Si* $G \supset A$ *un sous-groupe abélien, alors toute représentation irréductible de* G *est de degré inférieur ou égal à* $\frac{|G|}{|A|}$.

Démonstration. — Soit V une représentation irréductible de G et $W \subset V$ une sous-représentation de dimension 1 de A. Alors $V' = \sum_G g \cdot W = \sum_{G/A} g \cdot W$ est une sous-représentation de V, donc $V' = V$. Mais $\dim V' \leqslant |G/A|$. □

4.2.9. Table des caractères. — On fixe $\mathbb{K} = \mathbb{C}$. Les contraintes obtenues sur les caractères sont déjà suffisantes pour obtenir une description complète des représentation irréductibles du groupe G dans certains cas. On traite ici deux exemples.

Le groupe S_3. — Il 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. Il y a donc trois représentations irréductibles de S_3, dont nous noterons les caractères χ_1, χ_2 et χ_3.

Les représentations de degré 1 se déterminent toujours de la manière suivante : ce sont des morphismes $G \to \mathbb{C}^*$, donc, abéliennes, elles se factorisent par G/D(G) (et réciproquement, une représentation d'un quotient G/H remonte toujours en une représentation de G), donc les représentations de degré 1 sont exactement les représentations du groupe abélien G/D(G), savoir dans notre cas $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$. Il y en a donc deux, facilement identifiées : la représentation triviale (disons χ_1) et la signature (disons χ_2). Par le corollaire 4.2.6, la somme des carrés des dimensions des représentations fait $|S_3| = 6$, soit $1+1+4 = 6$ donc $\deg \chi_3 = 2$. On peut alors dresser la table des caractères, qui donne la valeur de chaque caractère sur chaque classe de conjugaison :

	e	τ	σ
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

La première colonne donne juste les dimensions des représentations. La troisième ligne, a priori inconnue, est obtenue en appliquant le corollaire 4.2.5 qui dit que les colonnes sont orthogonales ; une autre méthode pour déterminer la troisième ligne est d'écrire (corollaire 4.2.6) $\chi_1 + \chi_2 + 2\chi_3 = \chi_{\text{reg}} = 6\,1_{\{e\}}$ d'où on déduit également χ_3.

On a ainsi déterminé le caractère de la troisième représentation sans la connaitre, mais on peut aussi la décrire explicitement : S_3 est le groupe de symétries d'un triangle équilatéral, et cela donne une représentation dans $\mathbb{R}^2$, et par complexification dans $\mathbb{C}^2$. Dans cette représentation, les transpositions sont envoyées sur des symétries (à trace nulle), et les cycles sur des rotations d'angle $\pm\frac{2\pi}{3}$, donc de trace -1.

La table des caractères peut être utilisée pour calculer la décomposition en composantes irréductibles d'une représentation donnée, grâce au corollaire 4.2.6. Par exemple, décomposons le produit tensoriel $\mathbb{C}^2 \otimes \mathbb{C}^2$, où $\mathbb{C}^2$ est la représentation irréductible d'ordre 2. Son caractère est $\chi_3^2 = (4\,0\,1) = \chi_1 + \chi_2 + \chi_3$. Donc

$$\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^2 \oplus \mathbb{C}_{\text{triv}} \oplus \mathbb{C}_{\text{sig}}.$$

Remarquons qu'on connaissait déjà, par (34), la décomposition $\mathbb{C}^2 \otimes \mathbb{C}^2 = S^2\mathbb{C}^2 \oplus \Lambda^2\mathbb{C}^2$. Le second morceau, de dimension 1, est $\mathbb{C}_{\text{sig}}$ (c'est le déterminant), tandis que le premier morceau se décompose en deux.

Le groupe D_4. — Le groupe de symétries 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 : $\{e\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, r^2 s\}$, $\{rs, r^3 s\}$. Le sous-groupe $\mathbb{Z}/2\mathbb{Z} = \{e, r^2 = -\mathrm{Id}\}$ est distingué, et dans le quotient les trois éléments distincts r, s et rs sont d'ordre 2, donc

$$D_4/(\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Cela nous donne donc 4 représentations de degré 1, la cinquième doit donc être d'ordre 2. Appliquant la même méthode que précédemment, on obtient le tableau des caractères :

	e	r^2	$\{r, r^3\}$	$\{s, r^2 s\}$	$\{rs, r^3 s\}$
1	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
$\mathbb{C}^2$	2	-2	0	0	0

La représentation de degré 2 ici n'est autre que la représentation standard dans $\mathbb{C}^2$.

4.3. Structure de $\mathbb{K}[G]$

Dans la suite du chapitre, $\mathbb{K}$ *est un corps algébriquement clos, de caractéristique nulle.*

Dans le cas où le groupe est abélien, les représentations complexes, de degré 1, s'identifient à leur caractère $\chi : G \to \mathbb{C}^*$. En particulier, l'ensemble des caractères est un groupe multiplicatif, appelé **groupe des caractères**, et noté $\hat{G}$. Si f est une fonction sur G, alors on peut définir

$$\hat{f} : \hat{G} \longrightarrow \mathbb{C}, \quad \hat{f}(\chi) = \langle \chi, f \rangle. \tag{39}$$

Le théorème 4.2.2 s'interprète comme une transformée de Fourier entre fonctions sur G et fonctions sur $\hat{G}$, avec la formule d'inversion

$$f = \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi.$$

C'est la même transformée de Fourier que celle que vous connaissez sur d'autres groupes abéliens comme S^1 ou $\mathbb{R}$. En revanche, pour un groupe non abélien, le théorème 4.2.2 ne fournit une telle transformée que pour les fonctions centrales. Dans cette section, on va voir ce qui se passe pour les fonctions générales.

Soit V une représentation de G. Choisissant une base de V, le terme $\rho_V(g)_{ij}$ de la matrice $\rho_V(g)$ est appelé un **coefficient** de la représentation V.

4.3.1 Lemme. — *Soient* V *et* W *deux représentations irréductibles, alors*

$$\frac{1}{|G|}\sum_G \rho_V(g)_{ki}\rho_W(g^{-1})_{jl} = \begin{cases} 0 & (V,i,k) \neq (W,j,l), \\ \frac{1}{\dim V} & (V,i,k) = (W,j,l). \end{cases} \tag{40}$$

Démonstration. — En termes de la projection $\pi : \mathrm{Hom}(V,W) \to \mathrm{Hom}_G(V,W) \subset \mathrm{Hom}(V,W)$, par la formule (40), le membre de gauche est $\pi(E_{ij})_{kl}$. Si V n'est pas isomorphe à W, alors $\pi(E_{ij}) = 0$ et c'est fini. Si $V = W$, alors π est la projection sur les homothéties, donc $\pi(E_{ij}) = 0$ si $i \neq j$, et $\pi(E_{ii}) = \frac{1}{\dim V}\mathrm{Id}_V$, ce qui achève la démonstration du lemme. □

4.3.2 Corollaire. — *Les coefficients* $\rho_V(g)_{ij}$ *des représentations irréductibles forment une base de* $\mathbb{K}[G]$.

Démonstration. — Puisque $\sum(\deg\rho)^2 = \dim G$, on a le bon nombre de coefficients, et le lemme implique qu'ils sont linéairement indépendants. □

Pour $\mathbb{K} = \mathbb{C}$, choisissons des bases orthonormales des représentations, de sorte que les $\rho(g)$ soient unitaires, alors $\rho_W(g^{-1})_{jl} = \overline{\rho_W(g)_{lj}}$. Donc les coefficients des représentations forment une base orthogonale de $\mathbb{C}[G]$, l'espace des fonctions complexes sur G. Cela donne l'extension au cas non abélien de la transformée de Fourier.

On peut préciser encore la structure d'algèbre de $\mathbb{K}[G]$:

4.3.3 Proposition. — *Soient* $V_1,\dots,V_\ell$ *les représentations irréductibles de* G. *Alors*

$$\nu : \mathbb{K}[G] \longrightarrow \oplus_1^\ell \mathrm{End}\, V_i,$$

obtenu en faisant agir $\mathbb{K}[G]$ *sur chaque* V_i*, est un isomorphisme d'algèbres.*

Remarque. — Ce théorème s'étend à tous les groupes compacts (théorème de Peter-Weyl), en remplaçant $\mathbb{C}[G]$ par l'espace $L^2(G)$ des fonctions L^2 sur G, et en prenant une somme hilbertienne (infinie) dans le second membre. Les coefficients des représentations irréductibles de dimension finie forment une base hilbertienne, c'est la généralisation des séries de Fourier aux groupes compacts.

Démonstration. — L'application ν est un morphisme entre deux algèbres de même dimension. Il suffit donc de montrer qu'il est injectif. Si $\nu(\sum_G x_g g) = 0$, c'est-à-dire $\sum_G x_g \rho_{V_i}(g) = 0$ pour tout i, alors pour tous les indices (j,k) on a encore $\sum_G x_g \rho_{V_i}(g)_{jk} = 0$. Puisque les coefficients des représentations engendrent $\mathbb{K}[G]$, cela implique $\sum_G x_g \phi(g) = 0$ pour toute fonction $\phi : G \to \mathbb{K}$, et donc finalement tous les $x_g = 0$. □

Cette proposition donne le centre de $\mathbb{K}[G]$, mais nous aurons besoin plus loin de la description suivante : soit $c \subset G$ une classe de conjugaison, et

$$e_c = \sum_{g\in c} g \quad \in \mathbb{K}[G].$$

4.3.4 Proposition. — *1° Le centre de* $\mathbb{K}[G]$ *est le sous-espace vectoriel engendré par les* e_c.
2° Le sous-groupe abélien engendré par les e_c *est un sous-anneau commutatif de* $\mathbb{K}[G]$.

Démonstration. — 1° Si $h \in G$ et $u = \sum_G u_g g$, alors $huh^{-1} = \sum_G u_{h^{-1}gh} g$ donc $u \in Z(\mathbb{K}[G])$ si et seulement si $u_{h^{-1}gh} = u_g$ pour tous $h, g \in G$, c'est-à-dire u est constante sur les classes de conjugaison.

2° Le sous-groupe abélien engendré par les e_c contient 1, il reste à voir qu'il est stable par multiplication : or

$$e_c e_{c'} = \sum_{g \in c, g' \in c'} gg',$$

mais $hgg'h^{-1} = hgh^{-1}hg'h^{-1}$ donc $\{gg'\}$ est une réunion de classes de conjugaison, donc $e_c e_{c'} = \sum_c n_c e_c$ pour des $n_c \in \mathbb{Z}$. □

4.3.5. Le cas de caractéristique non nulle. — Tous les résultats démontrés dans cette section restent vrais si la caractéristique de $\mathbb{K}$ est non nulle, pourvu qu'on ait toujours la condition $\mathrm{car}\mathbb{K} \nmid |G|$. Dans ce cas, on ne peut plus s'appuyer sur la théorie des caractères pour affirmer que $|G| = \sum(\deg\rho_i)^2$, il faut utiliser un peu plus de théorie de représentation des algèbres pour montrer directement la proposition 4.3.3. [(1)]

4.4. Propriétés d'intégralité

Dans cette section on démontre que le degré d'une représentation irréductible divise l'ordre du groupe. La démonstration nécessite d'anticiper légèrement sur le cours d'Algèbre 2.

4.4.1. Introduction aux entiers algébriques. — Soit A un anneau commutatif. On dit que $x \in A$ est un **entier algébrique** sur $\mathbb{Z}$ s'il existe $a_i \in \mathbb{Z}$ tels que

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

4.4.2 Remarque. — Si $x \in \mathbb{Q}$ est un entier algébrique, alors $x \in \mathbb{Z}$. En effet, si $x = \frac{p}{q}$ avec $(p,q) = 1$ et $q > 0$, alors $p^n + a_1 p^{n-1} q + \cdots + a_n q^n = 0$ qui implique $q | p^n$ donc $q = 1$.

4.4.3 Proposition. — *Soit* $x \in A$ *anneau commutatif, alors sont équivalents :*

1° *x est un entier algébrique ;*

2° *le sous-anneau* $\mathbb{Z}[x]$ *engendré par x est un groupe abélien de type fini ;*

3° *il existe un sous-groupe abélien de type fini de* A *contenant* $\mathbb{Z}[x]$.

---

1. Réciproquement, si la proposition 4.3.3 est vraie, il faut que $\mathrm{car}\mathbb{K} \nmid |G|$. En effet, supposons $\mathbb{K}[G] = \oplus \mathrm{End}(V_i)$, où les V_i sont les représentations irréductibles de G ; comme représentation de G, on a $\mathrm{End}V_i \simeq (\dim V_i)V_i$, donc, par le lemme de Schur, d'une part $\mathrm{Hom}_G(\mathbb{K}, \mathbb{K}[G]) = \mathbb{K}$ est engendré par $\Lambda(1) = \sum_{g \in G} g$; et d'autre part $\mathrm{Hom}_G(\mathbb{K}[G], \mathbb{K}) = \mathbb{K}$ par $\varepsilon(\sum_G x_g g) = \sum_G x_g$. Alors $\varepsilon \circ \Lambda$ doit être un isomorphisme de la représentation triviale $\mathbb{K}$, mais $\varepsilon \circ \Lambda(1) = |G|$, qui ne peut être inversible que si $\mathrm{car}\mathbb{K} \nmid |G|$.

Démonstration. — Le premier énoncé implique le deuxième : si $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, alors $\mathbb{Z}[x]$ est engendré, comme groupe abélien, par $(1, x, x^2, \ldots, x^{n-1})$.

Le passage du deuxième au troisième énoncé est évident. Reste à passer du troisième au premier : soit A_n le groupe abélien engendré par $(1, x, \ldots x^{n-1})$. Il faut montrer que la suite croissante (A_n) devient stationnaire : il existe n tel que $A_n = A_{n-1}$, c'est-à-dire $x^n \in A_{n-1}$, ou encore $x^n = a_1 x^{n-1} + \cdots + a_n$.

Pour montrer que la suite est stationnaire, utilisons que $\mathbb{Z}[x] \subset G$ sous-groupe abélien de type fini. Ainsi $\cdots \subset A_{n-1} \subset A_n \subset \cdots \subset B = \cup_n A_n \subset G$. Puisque G est de type fini, son sous-groupe abélien B aussi, donc il est engendré par des éléments $b_1, \ldots, b_k$, tous éléments d'un A_n pour un n assez grand. Alors $A_{n+1} = A_n$. □

4.4.4 Corollaire. — *L'ensemble des entiers algébriques de* A *est un sous-anneau de* A.

Démonstration. — Si x et y sont des entiers algébriques de A, alors $\mathbb{Z}[x]$ est engendré (comme groupe abélien) par $1, x, \ldots, x^p$, et $\mathbb{Z}[y]$ par $1, y, \ldots, y^q$. Alors $\mathbb{Z}[x, y]$ est engendré, comme groupe abélien par les $x^i y^j$ pour $i \leqslant p$ et $j \leqslant q$, donc est de type fini. Or il contient $x + y$ et xy qui sont donc aussi des entiers algébriques. □

4.4.5. Propriété du degré des représentations. — On peut maintenant passer à la démonstration que le degré d'une représentation irréductible divise l'ordre du groupe.

4.4.6 Lemme. — *Si* $u = \sum_G u_g g \in Z(\mathbb{K}[G])$ *avec* $u_g \in \mathbb{K}$ *entier sur* $\mathbb{Z}$*, alors* u *est entier sur* $\mathbb{Z}$.

Démonstration. — En effet $u = \sum u_c e_c$, où la somme est sur les classes de conjugaison de G. Il suffit que e_c soit entier sur $\mathbb{Z}$, ce qui découle des propositions 4.3.4 et 4.4.3. □

4.4.7 Proposition. — *Si* V *est une représentation irréductible de* G *de caractère* χ*, et* $u = \sum_G u_g g \in Z(\mathbb{K}[G])$ *avec* u_g *entier sur* $\mathbb{Z}$*, alors* $\frac{1}{\deg \rho} \sum_G u_g \chi(g)$ *est un entier algébrique sur* $\mathbb{Z}$.

Démonstration. — Utilisons le morphisme induit par la représentation, $\nu : \mathbb{K}[G] \to \mathrm{End}V$. Puisque u est central et V irréductible, $\nu(u)$ est une homothétie de trace $\sum_G u_g \chi(g)$, donc

$$\nu(u) = \frac{1}{\deg \rho} \sum_G u_g \chi(g).$$

Comme u est un entier sur $\mathbb{Z}$, son image $\nu(u)$ aussi. □

4.4.8 Théorème. — *Si* V *est irréductible, alors* $\dim V \big| |G|$.

Démonstration. — Les $\chi(g)$ sont des entiers algébriques (puisque les valeurs propres des $\rho(g)$ sont racines de $X^{|G|} - 1$), donc $u = \sum_G \chi(g^{-1}) g$ est entier sur $\mathbb{Z}$. Par la proposition,

$$\frac{1}{\dim V} \sum_G \chi(g^{-1}) \chi(g) = \frac{|G|}{\dim V}$$

est un entier algébrique, et donc un entier, d'où le résultat. □

La contrainte donnée par le théorème est très forte. Par exemple, en combinant avec le corollaire 4.2.6, on déduit immédiatement qu'un groupe d'ordre p^2 ne peut avoir que des représentations de degré 1, donc est abélien.

On peut raffiner un peu le théorème :

4.4.9 Proposition. — *Si* V *est irréductible, alors* $\dim V \big| [G : Z(G)]$.

Démonstration (J. Tate). — Le groupe $G^m = G \times \cdots \times G$ a une représentation ρ_m dans $V^{\otimes m}$, donnée par $\rho_m(g_1, \ldots, g_m) = \rho_1(g_1) \otimes \cdots \otimes \rho_m(g_m)$. Son caractère est $\chi_m(g_1, \ldots, g_m) = \chi(g_1) \cdots \chi(g_m)$, donc $\langle \chi_m, \chi_m \rangle = 1$ et ρ_m est irréductible. Si $g_i \in Z(G)$ alors $\rho(g_i)$ est une homothétie, donc si en outre $g_1 \cdots g_m = e$ alors $\rho_m(g_1, \ldots, g_m) = \mathrm{Id}$. Soit

$$S = \{(g_1, \ldots, g_m) \in Z(G)^m, g_1 \cdots g_m = e\}.$$

Alors on peut factoriser la représentation ρ_m :

$$\begin{array}{ccc} G^m & \xrightarrow{\rho_m} & GL(V^{\otimes m}) \\ \downarrow & \nearrow_{\hat{\rho}_m} & \\ G^m/S & & \end{array}$$

Ainsi $\dim V^{\otimes m} = (\dim V)^m$ divise $|G^m/S| = \frac{|G|^m}{|Z(G)|^{m-1}}$, donc pour tout $m \geqslant 2$,

$$|Z(G)|^{m-1} \Big| \Big(\frac{|G|}{\dim V}\Big)^m , \quad \text{qui implique} \quad |Z(G)| \Big| \frac{|G|}{\dim V} .$$

□

4.5. Le théorème de Burnside

Le but ici est de démontrer le théorème suivant, dû à Burnside :

4.5.1 Théorème. — *Si p et q sont premiers entre eux, tout groupe d'ordre $p^a q^b$ est résoluble.*

Pour démontrer le théorème, il suffit de prouver qu'un tel groupe ne peut pas être simple, sauf à être abélien. En effet tous les quotients d'une suite de composition du groupe sont aussi d'ordre $p^{a'} q^{b'}$: simples, ils doivent alors être abéliens.

La démonstration de ce résultat de théorie des groupes fait appel à la théorie des caractères. Dans toute cette section, on se limite au corps $\mathbb{K} = \mathbb{C}$.

4.5.2. Compléments sur les entiers algébriques. — Si α est un entier algébrique, alors l'idéal $I = \{P \in \mathbb{Q}[X], P(\alpha) = 0\}$ est engendré par un polynôme unitaire ϖ, appelé **polynôme minimal** de α. Les autres racines de ϖ sont les **conjugués** de α, donc tout polynôme à coefficients rationnels s'annulant sur α s'annule aussi sur ses conjugués. Observons les propriétés suivantes :

1° ϖ est aussi le polynôme minimal des conjugués de α ;

2° ϖ est à racines simples ;

3° ϖ est à coefficients entiers ;

4° $n^{\deg P} P(\frac{X}{n})$ est le polynôme minimal de $n\alpha$.

La première propriété est évidente, sinon ϖ n'est pas minimal. Pour la seconde, si ϖ a une racine double, alors ϖ' s'annule aussi sur cette racine, donc ϖ n'est pas minimal ; les coefficients de ϖ sont des rationnels, mais aussi des entiers algébriques (puisque les fonctions symétriques des conjugués de α), donc des entiers ; le dernier item est évident.

Si le polynôme minimal de α_1 est $\varpi(x) = x^p + a_1 x^{p-1} + \cdots + a_p$, alors c'est aussi le polynôme caractéristique de la matrice

$$\mathrm{A} = \begin{pmatrix} 0 & & & -a_p \\ 1 & & & \\ & \ddots & & \vdots \\ & & 1 & -a_1 \end{pmatrix},$$

donc les conjugués $\alpha_2, \ldots, \alpha_p$ de α_1 sont réalisés comme les valeurs propres de la matrice A. Si on a un autre entier algébrique β_1, on réalise de même ses conjugués $(\beta_j)_{j \leqslant q}$ comme valeurs propres d'une matrice B. Alors les valeurs propres de

$$\mathrm{A} \otimes 1 + 1 \otimes \mathrm{B}$$

sont les $\alpha_i + \beta_j$. [2] En particulier, les conjugués algébriques de $\alpha_1 + \beta_1$ sont de la forme $\alpha_i + \beta_j$ (mais ne sont pas nécessairement tous ces nombres). Cela donne le cas $n = 2$ du lemme suivant, duquel on déduit immédiatement le cas général :

4.5.3 Lemme. — *Si $\alpha_1, \ldots, \alpha_n$ sont des entiers algébriques, alors les conjugués algébriques de $\alpha_1 + \cdots + \alpha_n$ sont de la forme $\alpha'_1 + \cdots + \alpha'_n$, où α'_i est un conjugué algébrique de α_i.* □

La démonstration du théorème de Burnside utilisera la proposition suivante :

4.5.4 Proposition. — *Si $\alpha_1, \ldots, \alpha_n$ sont des racines de l'unité dans $\mathbb{C}$, et $\frac{1}{n}\sum \alpha_i$ est un entier algébrique, alors $\alpha_1 = \cdots = \alpha_n$ ou $\sum_1^n \alpha_i = 0$.*

Démonstration. — Les conjugués algébriques de $\sum \alpha_i$ sont de la forme $\sum \alpha'_i$, où les α'_i sont des conjugués algébriques des α_i, donc également des racines de l'unité. Il en résulte que les conjugués algébriques de $a = \frac{1}{n}\sum \alpha_i$ sont de la forme $a' = \frac{1}{n}\sum \alpha'_i$. Par conséquent, ils satisfont $|a'| \leqslant 1$. Si les α_i ne sont pas tous égaux, alors $|a| < 1$, donc

$$\Big| \prod_{a' \text{ conjugué de } a} a' \Big| < 1.$$

Mais $\prod a' \in \mathbb{Z}$, donc $a = 0$. □

4.5.5. Démonstration du théorème de Burnside. — Le théorème de Burnside sera une conséquence de deux théorèmes, que nous commençons par démontrer.

4.5.6 Théorème. — *Si V est une représentation irréductible, et c une classe de conjugaison de G telle que $(\dim \mathrm{V}, |c|) = 1$, alors pour tout $g \in c$ ou bien $\chi_{\mathrm{V}}(g) = 0$ ou bien $\rho_{\mathrm{V}}(g)$ est une homothétie.*

2. C'est une autre manière de montrer que les entiers algébriques forment un anneau. La somme de deux entiers algébriques est obtenue comme valeur propre de $\mathrm{A} \otimes 1 + 1 \otimes \mathrm{B}$, et le produit de $\mathrm{A} \otimes \mathrm{B}$.

Démonstration. — Soit $n = \dim V$ et $\alpha_1, \dots, \alpha_n$ les valeurs propres de $\rho_V(g)$. Par la proposition 4.4.7, $\frac{1}{n}|c|\chi(g)$ est un entier algébrique ; puisque $(n, |c|) = 1$, en appliquant Bezout, $\frac{1}{n}\chi(g) = \frac{\alpha_1+\cdots\alpha_n}{n}$ est un entier algébrique. Par la proposition 4.5.4, ou bien $\chi(g) = 0$ ou bien $\alpha_1 = \cdots = \alpha_n$, c'est-à-dire $\rho(g)$ est une homothétie. □

4.5.7 Théorème. — *Si c est une classe de conjugaison de* G*, d'ordre p^k avec p premier, alors* G *contient un sous-groupe distingué non trivial.*

Démonstration. — Soient $(V_i, \rho_i)_{i=1,\dots,\ell}$ les représentations irréductibles de G. On va trouver un sous-groupe distingué non trivial de G comme l'un des $\ker\rho_i$. Soit $g \in c$, par orthogonalité

$$\sum_1^\ell \chi_i(e)\chi_i(g) = \sum_1^\ell (\dim V_i)\chi_i(g) = 0. \tag{41}$$

Posons

$$\{1, \dots, r\} = I_1 \cup I_2 \cup I_3,$$

où $I_1 = \{1\}$ ne contient que la représentation triviale, et I_2 contient les i tels que $p | \dim V_i$, et I_3 les $i \neq 1$ tels que $p \nmid \dim V_i$.

Si $i \in I_2$, alors $\frac{\dim V_i}{p}\chi_i(g)$ est un entier algébrique, donc $a = \sum_{i\in I_2} \frac{\dim V_i}{p}\chi_i(g)$ aussi. De (41) on tire

$$\chi_1(g) + \sum_{i\in I_2} (\dim V_i)\chi_i(g) + \sum_{i\in I_3} (\dim V_i)\chi_i(g) = 1 + pa + \sum_{i\in I_3} (\dim V_i)\chi_i(g) = 0.$$

Puisque a est un entier algébrique, il ne peut pas être égal à $-\frac{1}{p}$, donc la dernière somme est non nulle. Donc il existe $i \in I_3$ tel que $\chi_i(g) \neq 0$. Puisque $p \nmid \dim V_i$, par le théorème 4.5.6, il faut que $\rho_i(g)$ soit une homothétie, nécessairement la même pour tous les éléments de la classe de conjugaison c. Donc, prenant $g_1 \neq g_2$ dans c, on obtient $\rho_i(g_1^{-1}g_2) = \mathrm{Id}_{V_i}$. Ainsi $\ker\rho_i$ est non trivial. □

Démonstration du théorème de Burnside. — Il s'agit de montrer que si G n'est pas abélien, il n'est pas simple. Si le centre n'est pas trivial, il n'y a rien à démontrer. Si $Z(G) = \{e\}$, par le théorème 4.5.7, G ne contient pas de classe de conjugaison d'ordre p^k ou q^k, donc toutes les classes de conjugaison différentes de $\{e\}$ ont un ordre divisible par pq. Mais cela contredit le compte des éléments de G :

$$p^a q^b = 1 + \sum_c |c|.$$

□

4.6. Représentation induite

Soit H un sous-groupe du groupe G, alors une représentation V de G se restreint en une représentation de H, qu'on notera $\mathrm{Res}^G_H V$. Le caractère de cette restriction est la restriction $\chi|_H$ du caractère χ de G.

On va construire une opération dans l'autre sens, associant à une représentation V de H une représentation de G, appelée **représentation induite**, et notée $\mathrm{Ind}^G_H V$.

4.6.1. Point de vue des représentations. — On définit la représentation induite par

$$\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V} = \{f : \mathrm{G} \to \mathrm{V}, f(hx) = \rho_{\mathrm{V}}(h)f(x) \quad \forall x \in \mathrm{G}, \forall h \in \mathrm{H}\},$$

avec l'action de G donnée par

$$g(f)(x) = f(xg).$$

On obtient bien une représentation de G, car [3]

$$g(g'(f))(x) = g'(f)(xg) = f(xgg') = (gg')(f)(x).$$

Exemple. — Si $\mathrm{H} = \{e\}$ et $\mathrm{V} = \mathbb{K}$, alors $\mathrm{Ind}_{\{e\}}^{\mathrm{G}}\mathbb{K} = \mathbb{K}[\mathrm{G}]$.

Un élément $f \in \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$ est déterminé par une valeur sur chaque classe à droite $\mathrm{H}x$, d'où il résulte que

$$\dim_{\mathbb{K}} \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V} = [\mathrm{G} : \mathrm{H}] \dim_{\mathbb{K}} \mathrm{V}.$$

Exercice. — Si $\mathrm{E} \subset \mathrm{H} \subset \mathrm{G}$ sont des sous-groupes, et V est une représentation de E, alors [4]

$$\mathrm{Ind}_{\mathrm{E}}^{\mathrm{G}}\mathrm{V} = \mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{Ind}_{\mathrm{E}}^{\mathrm{H}}\mathrm{V}.$$

4.6.2. Point de vue des caractères. — Si $\mathrm{H} \subset \mathrm{G}$ on définit une application entre les espaces de fonctions centrales,

$$\mathscr{C}(\mathrm{H}) \longrightarrow \mathscr{C}(\mathrm{G}), \quad f \longmapsto f^{\mathrm{G}}.$$

On part de l'extension naïve, $f^0 : \mathrm{G} \to \mathbb{K}$, définie par

$$f^0(x) = \begin{cases} f(x) & x \in \mathrm{H}, \\ 0 & \text{sinon}, \end{cases}$$

qu'on rend invariante par conjugaison :

$$f^{\mathrm{G}}(g) = \sum_{x \in \mathrm{H}\backslash\mathrm{G}} f^0(xgx^{-1}) = \frac{1}{|\mathrm{H}|} \sum_{x \in \mathrm{G}} f^0(xgx^{-1}).$$

4.6.3 Théorème. — *Soit* V *une représentation de* $\mathrm{H} \subset \mathrm{G}$ *de caractère* χ*, alors* $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V}$ *a pour caractère* χ^{G}.

---

3. Il existe une interprétation plus intrinsèque, mais que nous n'utiliserons pas au niveau de ce cours, de la représentation induite en termes de produit tensoriel de modules sur une algèbre. Si L (resp. M) est un module à gauche (resp. à droite) sur l'algèbre A, alors on peut définir un produit tensoriel $\mathrm{L} \otimes_{\mathrm{A}} \mathrm{M}$, dans lequel $\ell \otimes (am) = (\ell a) \otimes m$. Alors

$$\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}}\mathrm{V} = \mathbb{K}[\mathrm{G}] \otimes_{\mathbb{K}[\mathrm{H}]} \mathrm{V},$$

où $\mathbb{K}[\mathrm{G}] = \{f : \mathrm{G} \to \mathbb{K}\}$ est un $\mathbb{K}[\mathrm{H}]$-module à droite (par $(fh)(x) = f(hx)$), et aussi un $\mathbb{K}[\mathrm{G}]$-module à gauche (par $(fg)(x) = f(xg)$), ce qui induit sur le produit tensoriel la structure de $\mathbb{K}[\mathrm{G}]$-module à gauche. Ainsi la représentation induite s'obtient-elle par une construction similaire à l'extension des scalaires vue en § 3.1 : ici on étend les scalaires de $\mathbb{K}[\mathrm{H}]$ à $\mathbb{K}[\mathrm{G}]$.

4. En termes du produit tensoriel,

$$\mathbb{K}[\mathrm{G}] \otimes_{\mathbb{K}[\mathrm{H}]} (\mathbb{K}[\mathrm{H}] \otimes_{\mathbb{K}[\mathrm{E}]} \mathrm{V}) = (\mathbb{K}[\mathrm{G}] \otimes_{\mathbb{K}[\mathrm{H}]} \mathbb{K}[\mathrm{H}]) \otimes_{\mathbb{K}[\mathrm{E}]} \mathrm{V} = \mathbb{K}[\mathrm{G}] \otimes_{\mathbb{K}[\mathrm{E}]} \mathrm{V}.$$

Démonstration. — Soit $\sigma = Hx_\sigma$ une classe à droite, et

$$V_\sigma = \{f \in \mathrm{Ind}_H^G V, f(x) = 0 \text{ si } x \notin \sigma\}.$$

Alors

$$\mathrm{Ind}_H^G V = \oplus_{\sigma \in H\backslash G} V_\sigma \text{ et } g \cdot V_\sigma = V_{\sigma g^{-1}}.$$

Dans le calcul de la trace de $\rho(g)$, seuls interviennent les V_σ tel que $g \cdot V_\sigma = V_\sigma$, c'est-à-dire tels que $\sigma g^{-1} = \sigma$, soit $x_\sigma g x_\sigma^{-1} \in H$. Sous cette hypothèse, calculons la trace de l'action de g sur V_σ, en identifiant

$$V_\sigma \longrightarrow V \text{ par } f \longmapsto f(x_\sigma).$$

Alors $g \cdot f \mapsto f(x_\sigma g) = f(x_\sigma g x_\sigma^{-1} x_\sigma) = (x_\sigma g x_\sigma^{-1}) \cdot f(x_\sigma)$ donc la trace de $g|_{V_\sigma}$ est $\chi(x_\sigma g x_\sigma^{-1})$. □

Exemple. — $D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \supset \mathbb{Z}/n\mathbb{Z}$ est engendré par une rotation r et une symétrie s, telles que $srs^{-1} = r^{-1}$. Le caractère de la représentation standard est

$$\chi(r^k) = e^{2\pi i \frac{k}{n}} + e^{-2\pi i \frac{k}{n}}, \quad \chi(r^k s) = 0.$$

Il est induit du caractère de $\mathbb{Z}/n\mathbb{Z}$,

$$\psi(r^k) = e^{2\pi i \frac{k}{n}}.$$

Exercice : en utilisant la définition, reconstruire directement la représentation induite à partir de celle de $\mathbb{Z}/n\mathbb{Z}$.

4.6.4. Réciprocité de Frobenius. —

***4.6.5 Théorème* (Point de vue des représentations).** — *Soit* $H \subset G$, V *une représentation de* G, W *une représentation de* H, *alors*

$$\mathrm{Hom}_G(V, \mathrm{Ind}_H^G W) = \mathrm{Hom}_H(\mathrm{Res}_H^G V, W).$$

***4.6.6 Théorème* (Point de vue des caractères).** — *Soit* ϕ *une fonction centrale sur* G, *et* ψ *une fonction centrale sur* H. *Alors*

$$\langle \phi, \psi^G \rangle = \langle \phi|_H, \psi \rangle.$$

Le lien entre les deux théorèmes est le suivant : soient $\phi_1, \ldots, \phi_r$ les caractères irréductibles de G. Si V et V′ sont des représentations de G, alors

$$\chi_V = \sum n_i \phi_i, \quad \chi_W = \sum n_i' \phi_i,$$

où n_i et n_i' sont les multiplicités de V_i dans V et V′. Alors

$$\langle \chi_V, \chi_{V'} \rangle = \sum n_i n_i' = \dim \mathrm{Hom}_G(V, V').$$

En appliquant le second théorème aux caractères χ_V et χ_W de V et W, on trouve $\langle \chi_V, \chi_W^G \rangle = \langle \chi_V|_H, \chi_W \rangle$, c'est-à-dire l'égalité des dimensions des deux espaces vectoriels $\mathrm{Hom}_G(V, \mathrm{Ind}_H^G W)$ et $\mathrm{Hom}_H(\mathrm{Res}_H^G V, W)$. Le premier théorème exhibe en outre un isomorphisme naturel entre ces deux espaces vectoriels (voir la démonstration).

Cas particulier important :

4.6.7 Corollaire. — *Si* V *et* W *sont irréductibles, la multiplicité de* V *dans* $\mathrm{Ind}_H^G W$ *est égale à la multiplicité de* W *dans* $\mathrm{Res}_H^G V$. □

Démonstration du théorème 4.6.6. — Par un calcul direct :

$$\begin{aligned}\langle \phi, \psi^g \rangle &= \frac{1}{|G|} \sum_{x \in G} \phi(x^{-1}) \psi^G(x) \\ &= \frac{1}{|G|} \sum_{x \in G, y \in H\backslash G} \phi(x^{-1}) \psi^0(yxy^{-1}) \\ &= \frac{1}{|G|} \sum_{x \in G, y \in H\backslash G} \phi(yx^{-1}y^{-1}) \psi^0(yxy^{-1}) \\ &= \frac{1}{|H|} \sum_{h \in H} \phi(h^{-1}) \psi(h) \\ &= \langle \phi|_H, \psi \rangle.\end{aligned}$$

□

Démonstration du théorème 4.6.5. — On veut identifier $E = \mathrm{Hom}_G(V, \mathrm{Ind}_H^G W)$ avec $E' = \mathrm{Hom}_H(\mathrm{Res}_H^G V, W)$. On définit deux morphismes :

$$\begin{aligned} F : E &\longrightarrow E' & \qquad G : E' &\longrightarrow E \\ \alpha &\longmapsto \big(F(\alpha)v = (\alpha v)(e)\big) & \beta &\longmapsto \big((G(\beta)v)(x) = \beta(xv)\big)\end{aligned}$$

Le fait que F et G soient bien définis et inverses l'un de l'autre est laissé en exercice. □

Exemple : le groupe du tétraèdre T. — Le groupe des isométries directes du tétraèdre s'identifie au groupe alterné A_4 par l'action sur les sommets. On a $|T| = 12$, et les classes de conjugaison sont $O_1 = \{e\}$, $O_2 = \{(12)(34), (13)(24), (14)(23)\}$, $O_3 = \{(123), (214), (341), (432)\}$, $O_4 = \{(132), (241), (314), (423)\}$.

Comme $T \rhd K = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = O_1 \cup O_2$, le groupe de Klein, avec $T/K = \mathbb{Z}/3\mathbb{Z}$, on obtient trois représentations de degré 1, de caractères χ_1, χ_2 et χ_3. La quatrième représentation est donc de degré 3, et a pour caractère χ_4. On obtient ainsi la table des caractères de T :

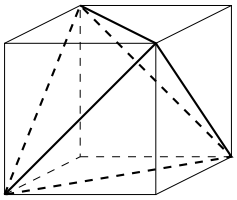
	O_1	O_2	O_3	O_4
χ_1	1	1	1	1
χ_2	1	1	j	j^2
χ_3	1	1	j^2	j
χ_4	3	-1	0	0

Une autre manière de voir la représentation de degré 3 est la suivante : soit V la représentation de K de degré 1 telle que $\rho_V((12)(34)) = \rho_V((13)(24)) = -1$, alors par la réciprocité de Frobenius, $\mathrm{Ind}_K^T V$, de dimension 3, ne saurait contenir l'une des trois représentations de degré 1 comme composante, puisque toutes se restreignent à K en la représentation triviale. Par conséquent, $\mathrm{Ind}_K^T V$ est irréductible. Le calcul de son caractère par le théorème 4.6.3 donne

$$\chi(g) = \chi_V^0(g) + \chi_V^0(\sigma g \sigma^{-1}) + \chi_V^0(\sigma^2 g \sigma^{-2}),$$

où $\sigma \in T$ engendre le quotient T/K. Cela redonne immédiatement χ_4.

Exemple : le groupe de l'octaèdre ou du cube O. — Le groupe du cube s'identifie à S_4 par action sur les grandes diagonales. En inscrivant un tétraèdre dans un cube, on obtient $O \triangleright T$, avec $O/T = \mathbb{Z}/2\mathbb{Z}$.



Les classes de conjugaison sont :

O_1 : la classe triviale $O_1 = \{e\}$;

O_2 : les symétries autour des axes des faces, $|O_2| = 3$;

O_3 : les rotations d'angle $\pm\frac{2\pi}{3}$ autour des grandes diagonales, $|O_3| = 8$;

O_4 : les rotations d'angle $\pm\frac{\pi}{2}$ des faces, $|O_4| = 6$;

O_5 : les symétries d'axe joignant les milieux de deux arêtes opposées, $|O_5| = 6$.

Seules les trois premières classes intersectent T.

Trouvons les cinq représentations irréductibles : deux représentations de degré 1, V_1 et V_2, proviennent du quotient $\mathbb{Z}/2\mathbb{Z}$, et la représentation standard V_3 donne une représentation de degré 3. Les deux représentations restantes sont de degré p et q satisfaisant $p^2 + q^2 = 13$, ce qui impose $p = 2$ et $q = 3$.

La représentation irréductible de degré 2 peut se construire de la manière suivante : soit V la représentation de T de caractère $\chi_V = (1\,j\,j^2)$, et $S = \mathrm{Ind}_T^O V$, donc $\deg S = 2$. Par réciprocité de Frobenius, V_1 et V_2 ne sont pas facteurs de S donc S est irréductible, de caractère

$$\chi_S(g) = \chi_V^0(g) + \chi_V^0(\sigma g \sigma^{-1}) \quad \text{pour un } \sigma \notin T.$$

Cela donne la table de caractères suivante, où la dernière ligne est obtenue par orthogonalité :

	O_1	O_2	O_3	O_4	O_5
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	3	-1	0	1	-1
χ_4	2	2	-1	0	0
χ_5	3	-1	0	-1	1

On observe que $\chi_5 = \chi_2\chi_3$, d'où il résulte que $V_5 = V_2 \otimes V_3$ qui est donc irréductible. Cela finit de fournir une interprétation à toutes les représentations irréductibles.

[Index]Index