ALGÈBRE 1

30 janvier 2015

ALGÈBRE 1

TABLE DES MATIÈRES

CHAPITRE I

GROUPES

1. Généralités sur les groupes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1° $e \in \mathrm{H}$;

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

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

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

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

---

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

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

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

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

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

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

5° Le *centre*

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

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

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

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

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

***Théorème 1.18* (Propriété universelle du quotient).** — *Soit* G *un groupe, soit* H *un sous-groupe distingué de* G *et soit* $f : G \to G'$ *un morphisme de groupes. Si* $\ker(f) \supseteq H$, *il existe un unique morphisme* $\hat{f} : G/H \to G'$ *tel que* $f = \hat{f} \circ p$, *c'est-à-dire que 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 $\ker(f) \supseteq H$. L'application $\hat{f} : G/H \to G'$ ainsi définie est manifestement unique. On vérifie que c'est un morphisme, avec le noyau et l'image indiqués. □

Corollaire 1.19. — *Si* $f : G \to G'$ *est un morphisme de groupes,* $\hat{f} : G/\ker(f) \to \operatorname{im}(f)$ *est un isomorphisme.*

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 $H = \ker(f)$. On obtient $\hat{f} : G/\ker(f) \to \operatorname{im}(f)$, avec $\ker \hat{f} = \ker(f)/\ker(f) = \{e\}$ et $\operatorname{im} \hat{f} = \operatorname{im} \tilde{f} = \operatorname{im}(f)$. □

Corollaire 1.20. — *Le sous-groupe* $\langle g \rangle$ *engendré par un élément* g *d'un groupe* G *est isomorphe à* $\mathbf{Z}$ *s'il est infini, à* $\mathbf{Z}/n\mathbf{Z}$ *s'il est fini, avec* $n \in \mathbf{N}^*$. *On appelle alors* n *l'*ordre *de* g.

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

Démonstration. — Le morphisme

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

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

Exemples 1.21. — 1° Le groupe $\mathbf{Z}/n\mathbf{Z}$ est le groupe quotient de $\mathbf{Z}$ par $n\mathbf{Z}$. On peut en déduire les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$: leur image réciproque par la surjection $p : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$ contenant $n\mathbf{Z}$, donc de la forme $d\mathbf{Z}$ pour $d|n$, donc les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont exactement les sous-groupes cycliques engendrés par les entiers d tels que $d|n$.

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

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

3° La restriction du déterminant au groupe diédral $D_n < O_2(\mathbf{R})$ induit une surjection $D_n \to \{\pm 1\}$. Son noyau est le sous-groupe de D_n engendré par la rotation r. Il est d'indice 2 et est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

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

5° Le groupe $\mathrm{Int}(G)$ des automorphismes intérieurs de G est distingué dans $\mathrm{Aut}(G)$. On appelle le quotient $\mathrm{Out}(G) := G/\mathrm{Int}(G)$ le groupe des automorphismes extérieurs de G.

Proposition 1.22. — *Soit* G *un groupe et soit* H *un sous-groupe distingué de* G.

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

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

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

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

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

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

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

et on peut donc écrire

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

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

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

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

Exercice 1.23. — Soit $\mathbf{F}_q$ un corps fini à q éléments. Montrer

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

Exercice 1.24. — On rappelle que $\mathrm{GL}_n(\mathbf{Z})$ est le groupe des matrices carrées d'ordre n à coefficients entiers, dont le déterminant est ± 1.

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

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

Exercice 1.25. — Soient K et H des sous-groupes distingués d'un groupe G avec $K \leq H$. Montrer que le sous-groupe H/K de G/K est distingué et que $(G/K)/(H/K) \simeq G/H$.

Exercice 1.26. — Soient H et K des sous-groupes d'un groupe G, avec $H \trianglelefteq G$. Montrer que $HK := \{hk \mid h \in H,\ k \in K\}$ est un sous-groupe de G, que $HK = KH = HKH$, que $H \cap K$ est distingué dans K et que les groupes HK/H et $K/(H \cap K)$ sont isomorphes.

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

Exercice 1.27. — Soit **K** un corps et soit E un **K**-espace vectoriel. Montrer que le groupe des translations de E est un sous-groupe distingué du groupe affine GA(E) (*cf.* ex. 1.1.5°) isomorphe au groupe additif (abélien) (E, +) et que le groupe quotient est isomorphe à GL(E).

Exercice 1.28. — Le but de cet exercice est de montrer que tout sous-groupe *fini* G du groupe multiplicatif d'un corps **K** est cyclique. En particulier, le groupe multiplicatif d'un corps fini est cyclique.

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

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

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

Exercice 1.29. — Soit $\mathbf{F}_q$ un corps fini à q éléments. Le but de cet exercice est de montrer que l'ordre maximal d'un élément de $\mathrm{GL}_n(\mathbf{F}_q)$ est exactement $q^n - 1$.

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

b) Inversement, montrer qu'il existe un élément de $\mathrm{GL}_n(\mathbf{F}_q)$ d'ordre $q^n - 1$ (*Indication :* on admettra qu'il existe un corps $\mathbf{F}_{q^n}$ de cardinal q^n contenant $\mathbf{F}_q$ comme sous-corps (*cf.* th. II.1.1) ; si x engendre le groupe multiplicatif $(\mathbf{F}_{q^n}, \times)$ (exerc. 1.28), on considérera une matrice de polynôme caractéristique le polynôme minimal de x sur $\mathbf{F}_q$).

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

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

est alors aussi une application linéaire de noyau W et la propriété de factorisation (théorème 1.18) reste valable en remplaçant les morphismes de groupes par des applications linéaires : si $\phi : V \to V'$ est une application linéaire telle que $\ker\phi \supseteq W$, elle se factorise, de manière unique, par une application linéaire $\hat{\phi} : V/W \to V'$ telle que $\phi = \hat{\phi} \circ p$. À nouveau, cette propriété caractérise le quotient.

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

Attention, cette propriété est particulière aux espaces vectoriels : dans le cas des groupes, si $H \trianglelefteq G$, en général G n'est pas isomorphe au produit $H \times G/H$ (*cf.* ex. 1.21.3°).

2. Groupes opérant sur un ensemble

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

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

telle que

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

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

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

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

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

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

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

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

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

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

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

4° Si $\mathrm{H}\leq\mathrm{G}$, alors G opère sur l'ensemble G/H des classes à gauche par $g\cdot(x\mathrm{H}) = (gx)\mathrm{H}$.

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

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

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

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

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

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

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

---

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

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

L'application

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

se factorise en une *bijection*

$$\mathrm{G}/\mathrm{G}_x \xrightarrow{\sim} \mathrm{G}x \tag{3}$$

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

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

$$\mathrm{G}_{gx} = g\mathrm{G}_x g^{-1}.$$

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

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

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

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

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

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

3° L'action décrite plus haut du groupe $\mathrm{SL}_2(\mathbf{R})$ sur le demi-plan de Poincaré est transitive. Elle n'est pas fidèle (le noyau de l'action est $\{\pm \mathrm{I}_2\}$).

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

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

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

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

$$\{1,\dots,n\} = \bigsqcup_1^r \mathrm{O}_i.$$

On peut poser

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

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

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

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

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

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

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

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

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

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

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

Explicitons cette action dans le cas du groupe symétrique.

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

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

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

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

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

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

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

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

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

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

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

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

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

Exercice 2.10. — Soit p un nombre premier impair et soit q une puissance de p. Le but de cet exercice est de décrire les classes de conjugaison de $\mathrm{G} := \mathrm{SL}_2(\mathbf{F}_q)$. On rappelle $|\mathrm{G}| = q(q^2-1)$ (exerc. 1.23).

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

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

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

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

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

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

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

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

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

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

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

éléments.

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

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

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

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

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

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

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

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

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

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

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

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

Démonstration. — Par la formule des classes, on a

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

la diagonale (matrices *unipotentes*) :

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

Alors $\mathrm{T}_n(\mathbf{F}_q)$ est un p-Sylow de G. En effet, $|\mathrm{T}_n(\mathbf{F}_q)| = q^{\frac{n(n-1)}{2}}$, alors que d'après l'exerc. 1.23, on a $\alpha = \beta\frac{n(n-1)}{2}$.

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.

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

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

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

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

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

1° G *contient un p-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.*

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

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

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

4° Soit X l'ensemble des p-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 $|\mathrm{X}| \equiv 1 \pmod{p}$, d'après la prop. 2.13, il suffit de montrer que $|\mathrm{X}^\mathrm{S}| = 1$. En réalité, on va montrer que S est le seul point fixe de l'action de S sur X.

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

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

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

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

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

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

2° Soit q une puissance de p. Le théorème de Sylow entraîne que tout p-sous-groupe de $GL_n(\mathbf{F}_q)$ est constitué, dans une base convenable, de matrices unipotentes triangulaires supérieures (*cf.* ex. 2.19). On peut montrer (*cf.* exerc. 2.27) que le nombre de p-Sylow de $GL_n(\mathbf{F}_q)$ est

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

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

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

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

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

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

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

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

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

le *sous-groupe de p-torsion* de G (conformément à la tradition, on note additivement l'opération du groupe abélien G). On vérifie facilement que $T_p(G)$ est un sous-groupe de G (mais on se sert ici du fait que G est abélien !).

Ensuite, l'ordre de tout élément de S est une puissance de p, donc $S \leq T_p(G)$. Mais l'ordre de tout élément de $T_p(G)$ est aussi une puissance de p, donc l'ordre de $T_p(G)$ est aussi une puissance de p (cor. 2.24). Par définition d'un p-Sylow, on en déduit $S = T_p(G)$.

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

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

Exercice 2.27. — Soit p un nombre premier et soit $\mathbf{F}_q$ un corps de cardinal une puissance q de p.
a) Décrire un p-Sylow S du groupe $G := GL_n(\mathbf{F}_q)$ ainsi que son normalisateur $N_G(S)$ (*cf.* (6)).
b) En déduire le nombre de p-Sylow de G (*Indication :* on pourra utiliser l'ex. 2.23.1°).

Exercice 2.28. — Soient p et q des nombres premiers et soit G un groupe d'ordre pq.
a) Montrer que G n'est pas simple (*Indication :* on pourra compter les p- ou q-Sylow de G).
b) Si $p < q$ et que p ne divise pas $q-1$, montrer que G est cyclique (*Indication :* on pourra montrer que G contient un unique p-Sylow et un unique q-Sylow).

Exercice 2.29. — a) Soit G un groupe fini simple. Écrivons $|G| = p^\alpha m$, avec $p \nmid m$, $m \geqslant 2$ et $\alpha \geqslant 1$, et notons n_p le nombre de ses p-Sylow. Montrer que $|G|$ divise $n_p!$.
b) Montrer qu'il n'existe pas de groupe simple de cardinal 1 000 000.

Exercice 2.30. — Soient p et q des nombres premiers vérifiant $p < q$ et soit G un groupe d'ordre $p^m q^n$, avec $0 \leqslant m \leqslant 2$ et $n \geqslant 0$. Montrer que G n'est pas simple (*Indication :* dans le cas $p = 2$ et $q = 3$, on pourra utiliser l'exerc. 2.29 ; dans le cas $|G| = 12$, on pourra compter les éléments d'ordre 3).

Exercice 2.31. — Soient p et q des nombres premiers et soit G un groupe d'ordre $p^2 q$. Montrer que G n'est pas simple (*Indication :* on pourra utiliser l'exerc. 2.30).

Exercice 2.32. — Soient p et q des nombres premiers et soit G un groupe d'ordre $p^3 q$. Montrer que G n'est pas simple (*Indication :* si $|G| \neq 24$, on pourra penser à compter les éléments d'ordre q et montrer que G contient un sous-groupe distingué qui est un p-Sylow ou un q-Sylow ; si $|G| = 24$, on pourra montrer $G \simeq \mathfrak{S}_4$).

Exercice 2.33. — Montrer qu'un groupe fini simple non abélien d'ordre < 168 est d'ordre 60 (*Indication :* on pourra utiliser les résultats des exercices précédents).

Exercice 2.34. — Montrer qu'aucun groupe d'ordre 2907 n'est simple.

Exercice 2.35. — Le but de cet exercice est de montrer que tout groupe simple G d'ordre 60 est isomorphe à $\mathfrak{A}_5$.
a) Montrer que le nombre de 2-Sylow de G est soit 5, soit 15. Conclure dans le premier cas. On suppose donc dans la suite que G a 15 2-Sylow.
b) Montrer qu'il existe deux 2-Sylow S_1 et S_2 de G dont l'intersection a 2 éléments.
c) Montrer que le normalisateur $N := N_G(S_1 \cap S_2)$ est d'ordre 12 (*cf.* (6)).

d) Montrer que l'action de G par translation sur G/N fournit un morphisme injectif $G \to \mathfrak{S}_5$.
e) Conclure.

Exercice 2.36. — Soit p un nombre premier. Montrer que tout groupe d'ordre $2p$ est soit cyclique, soit isomorphe au groupe diédral D_p.

***Exercice 2.37* (Méthode de Frattini)**. — Soit G un groupe fini.
a) Soit $H \trianglelefteq G$ un sous-groupe distingué et soit S' un p-Sylow de H. Montrer l'égalité

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

(*Indication :* si $g \in G$, on pourra utiliser le fait que $gS'g^{-1} \leq H$ est conjugué *dans* H à S').
b) Soit maintenant $S \leq G$ un p-Sylow de G et soit $M \leq G$ un sous-groupe contenant $N_G(S)$. Montrer $M = N_G(M)$ (*Indication :* on pourra appliquer a) à $M \trianglelefteq N_G(M)$ et à son p-Sylow S).

***Exercice 2.38* (Automorphismes de $\mathfrak{S}_n$)**. — Soit $n \in \mathbf{N}^*$.
a) Soit ϕ un automorphisme de $\mathfrak{S}_n$ qui transforme toute transposition en une transposition. Montrer que ϕ est un automorphisme intérieur.
b) Soit $\sigma \in \mathfrak{S}_n$. Déterminer le cardinal du centralisateur $C(\sigma) := \{\tau \in \mathfrak{S}_n \mid \tau\sigma\tau^{-1} = \sigma\}$ de σ.
c) En déduire que si $n \neq 6$, alors $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$.
d) On suppose $n \geqslant 5$ et $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$. Montrer que tous les sous-groupes d'indice n de $\mathfrak{S}_n$ sont conjugués.
e) En utilisant les 5-Sylow de $\mathfrak{S}_5$, montrer qu'il existe un sous-groupe d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1,\dots,6\}$.
f) En déduire $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

***Exercice 2.39* (Sous-groupes de Sylow d'un sous-groupe)**. — Soit G un groupe et soit H un sous-groupe de G. Soit p un nombre premier divisant l'ordre de H.
a) Montrer que tout p-Sylow de H est contenu dans un p-Sylow de G.
b) Montrer qu'un p-Sylow de G contient au plus un p-Sylow de H.

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

***Exercice 2.40* (Sous-groupes de Sylow d'un groupe quotient)**. — Soit G un groupe et soit N un sous-groupe distingué de G. Soit p un nombre premier divisant l'ordre de G/N.
a) Montrer que pour tout p-Sylow S de G, l'image de S par la surjection canonique $G \to G/N$ est un p-Sylow de G/N.
b) Montrer que tout p-Sylow de G/N est obtenu comme en a).

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

3. Groupes abéliens de type fini

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

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

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

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

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

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

entre groupes multiplicatifs des unités.

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

$$\mathbf{Z}/mn\mathbf{Z} \simeq \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

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

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

$$\begin{array}{ccc} \mathbf{Z}^r & \longrightarrow & \mathrm{G} \\ (n_1, \dots, n_r) & \longmapsto & \sum_1^r n_i x_i \end{array} \tag{8}$$

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

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

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

$$\mathbf{Z}^r \xrightarrow{p} \!\!\!\!\rightarrow \mathrm{G}.$$

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

$$\mathbf{Z}^r \longrightarrow\!\!\!\!\rightarrow \mathbf{Z}^r/(\mathbf{Z}^{r-1} \times \{0\}) \xrightarrow{\widehat{f \circ p}} \!\!\!\!\rightarrow \mathrm{G/K}.$$

Comme $\mathbf{Z}^r/(\mathbf{Z}^{r-1} \times \{0\})$ est isomorphe à $\mathbf{Z}$, le groupe G/K est isomorphe à un $\mathbf{Z}/m\mathbf{Z}$ (cor. 1.19).

Si H est un sous-groupe de G, le noyau $\mathrm{H} \cap \mathrm{K}$ de $\mathrm{H} \hookrightarrow \mathrm{G} \to \mathrm{G/K}$ est de type fini par l'hypothèse de récurrence, tandis que l'image, sous-groupe de $\mathbf{Z}/m\mathbf{Z}$, est aussi engendrée

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

par un élément (ex. 1.21.1°). Cette image est isomorphe à $H/H\cap K$, qui est donc de type fini. On peut ainsi appliquer la prop. 1.22.2° pour en déduire que H est de type fini. □

3.3. Groupes abéliens libres de type fini. — Un groupe abélien est *libre de type fini* s'il est isomorphe à un produit $\mathbf{Z}^r$ [9]. Cela signifie qu'il existe $r\in\mathbf{N}$ et des éléments $x_1,\dots,x_r$ de G tels que le morphisme (8) soit un isomorphisme. Une telle famille $(x_1,\dots,x_r)$ est appelée une base de G. Plus généralement, on dira qu'une famille $(x_1,\dots,x_r)$ d'éléments de G est linéairement indépendante si le morphisme (8) est injectif.

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

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

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

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

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

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

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

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

Démonstration. — Il suffit de montrer que si un groupe abélien libre G a une base $(x_1,\dots,x_r)$, toute famille linéairement indépendante d'éléments de G a au plus r éléments. Soit donc une famille $(y_1,\dots,y_n)$ d'éléments de G : puisque $(x_1,\dots,x_r)$ est une base,

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

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

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

Attention à la confusion avec la notion (plus compliquée) de « groupe libre », qui ne sera pas vue dans ce cours. Le seul groupe libre qui est abélien est $\mathbf{Z}$.

on obtient une matrice $A = (a_{ij})$ de taille $r \times n$ à coefficients entiers définie par

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

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

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

- $(d_1 e_1, \dots, d_r e_r)$ *est une base de* H ;
- *on a les divisibilités* $d_1 \mid \cdots \mid d_r$.

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

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

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

$$\mathbf{Z}^n \xrightarrow[\sim]{Q} \mathbf{Z}^n \xrightarrow{A} \mathbf{Z}^s \xrightarrow[\sim]{P} \mathbf{Z}^s \xrightarrow[\sim]{P^{-1}} \mathbf{Z}^s \xrightarrow[\sim]{\phi} G$$

de $f \circ Q$. L'isomorphisme $\phi \circ P^{-1} : \mathbf{Z}^s \xrightarrow{\sim} G$ correspond à une nouvelle base $(e_1, \dots, e_s)$ de G et $H = \mathrm{im}(f \circ Q)$ est alors engendré par $(d_1 e_1, \dots, d_r e_r)$. Comme ces éléments forment une famille libre, c'est une base de H. Le théorème est donc démontré. □

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

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

$$G \simeq \mathbf{Z}^r \times \left(\prod_{1}^{s} \mathbf{Z}/d_i\mathbf{Z} \right).$$

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

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

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

où les p_j sont des nombres premiers, éventuellement répétés. Réciproquement, on récupère, de manière unique, les facteurs invariants d_i à partir de la collection des $p_j^{\alpha_j}$: le

plus grand facteur d_s est le ppcm des $p_j^{\alpha_j}$, et il s'écrit $d_s = \prod_{j' \in J'} p_{j'}^{\alpha_{j'}}$. On obtient alors d_{s-1} comme le ppcm des $p_j^{\alpha_j}$ pour $j \in J - J'$, etc.

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

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

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

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

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

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

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

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

D'où $\mathrm{G} \simeq \mathbf{Z}^n/\mathrm{H} \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_s\mathbf{Z} \times \mathbf{Z}^{n-s}$.

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

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

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

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

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

les α_j sont complètement déterminés par G.

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

Exercice 3.8. — Pour tout groupe G abélien de type fini, on note $r(\mathrm{G})$ l'entier r qui apparaît dans l'énoncé du th. 3.6.

a) Montrer que $r(\mathrm{G})$ est le plus grand entier n tel que G contienne un sous-groupe isomorphe à $\mathbf{Z}^n$.

b) Montrer que $r(\mathrm{G})$ est le plus grand entier n tel que G ait un quotient isomorphe à $\mathbf{Z}^n$.

c) Soit H un sous-groupe de G. Montrer $r(\mathrm{G}) = r(\mathrm{H}) + r(\mathrm{G}/\mathrm{H})$.

Exercice 3.9. — Soit G un groupe abélien de type fini et soit $f : G \to G$ un morphisme surjectif. Le but de cet exercice est de démontrer que f est un isomorphisme. Soit $T(G) \leq G$ le sous-groupe de torsion de G.
a) Montrer que f induit un morphisme surjectif $\hat{f} : G/T(G) \to G/T(G)$.
b) Montrer que $\hat{f}$ est un isomorphisme.
c) En déduire que f est un isomorphisme.

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

Étendons cette observation de la manière suivante. Notons

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

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

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

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

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

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

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

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

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

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

Les opérations qu'on s'autorise sont les suivantes :
– la multiplication à gauche par la matrice $\mathrm{Id} + aE_{ij}$, qui permet d'ajouter à la i-ème ligne la j-ème ligne, multipliée par un entier a ;

10. On peut aussi déduire l'unicité des d_i de l'énoncé d'unicité du th. 3.6 (obtenu indépendamment du lemme !) en procédant de la façon suivante : soit H_A le sous-groupe de $\mathbf{Z}^m$ engendré par les colonnes de A. Multiplier à gauche par P revient à appliquer un automorphisme de $\mathbf{Z}^m$, tandis que multiplier à droite par Q ne change pas H. Les groupes (abéliens de type fini) $\mathbf{Z}^m/H_A$ et $\mathbf{Z}^m/H_{PAQ}$ sont donc isomorphes. Or ce dernier est $\mathbf{Z}^{m-r} \times \left(\prod_1^r \mathbf{Z}/d_i\mathbf{Z}\right)$. Par le th. 3.6, les entiers $d_1, \ldots, d_r$ sont donc uniquement déterminés par $\mathbf{Z}^m/H_A$, donc par A.

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

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

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

Soit λ_1 le pgcd (positif) des coefficients de la première colonne. On va appliquer des opérations élémentaires sur les lignes pour obtenir une première colonne dont tous les coefficients sont nuls, sauf le coefficient a_{11} qui sera égal à λ_1. Faisons-le sur les deux premiers coefficients a_{11} et a_{12}. Quitte à échanger les deux premières lignes, on peut supposer $|a_{11}| \geqslant |a_{12}|$. 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, les coefficients (a_{11}, a_{12}) sont transformés en (c, a_{12}), avec $|a_{12}|+|c| < |a_{11}|+|a_{12}|$. En itérant, l'algorithme d'Euclide nous indique qu'on finit par arriver au couple $(\mathrm{pgcd}(a_{11}, a_{12}), 0)$. Il est clair qu'en répétant ce procédé sur chaque ligne, on arrive à la première colonne souhaitée, $(\lambda_1 0 \cdots 0)$.

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

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

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

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

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

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

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

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

***Exemple 3.10* (Théorème de Mordell).** — Une courbe elliptique sur $\mathbf{Q}$ est l'ensemble E des solutions $(x,y) \in \mathbf{Q}^2$ d'une équation du type

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

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

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

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

Un théorème de Mazur (1977) décrit tous les groupes de torsion T(E) qu'on peut obtenir : ce sont les $\mathbf{Z}/n\mathbf{Z}$, pour $n \in \{0,1,\dots,10,12\}$ et les $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, pour $n \in \{2,4,6,8\}$. Les rangs possibles du groupe abélien libre E/T(E) sont beaucoup plus mystérieux : le plus grand rang calculé explicitement est 28 (Elkies, 2006) ; on conjecture, mais on ne sait pas démontrer, que des rangs arbitrairement grands devraient être possibles. Voici la courbe d'Elkies (l'équation est présentée sous une forme légèrement différente) :

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

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

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

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

Partons d'une matrice $\mathrm{A} \in \mathrm{GL}_n(\mathbf{Z})$. Il est clair que ses facteurs invariants sont tous égaux à 1, c'est-à-dire que la réduction finale de A est la matrice I_n. On a donc écrit $\mathrm{A} = \mathrm{PQ}$, où la

11. Le bon point de vue est de regarder les points de la courbe dans le plan projectif (*cf.* p. 53), donnés par l'équation homogène $y^2 z = x^3 + axz^2 + bz^3$; le point O est alors le point à l'infini $(0:1:0)$.

matrice P (resp. Q) est produit de matrices correspondant aux opérations réalisées sur les lignes (resp. colonnes). Ces opérations sont de deux types :

– la multiplication à gauche (ou à droite) par la matrice élémentaire $\mathrm{I}_n + a\mathrm{E}_{ij}$, qui n'est autre que $(\mathrm{I}_n + \mathrm{E}_{ij})^a$;
– l'échange de deux lignes ou colonnes.

On en déduit le résultat suivant.

Théorème 4.1. — *Le groupe* $\mathrm{GL}_n(\mathbf{Z})$ *est de type fini : il est engendré par*

– *les matrices élémentaires* $\mathrm{I}_n + \mathrm{E}_{ij}$, *pour* $i, j \in \{1, \dots, n\}$, $i \neq j$,
– *et les matrices de transposition* $\mathrm{I}_n + \mathrm{E}_{ij} + \mathrm{E}_{ji} - \mathrm{E}_{ii} - \mathrm{E}_{jj}$, *pour* $i, j \in \{1, \dots, n\}$, $i \neq j$.

Les opérations élémentaires du premier type ne changent pas le déterminant, au contraire de celles du deuxième type. Nous allons remplacer les secondes par l'échange de deux lignes ou colonnes, suivi du *changement de l'une d'elles en son opposé*. Notons que cela peut être réalisé par des opérations élémentaires du premier type :

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

Il n'est pas difficile de voir que la démonstration du lemme 3.3 fonctionne encore avec ces opérations élémentaires restreintes, la seule différence étant qu'on ne peut pas assurer que d_n soit positif ; lorsque $\mathrm{A} \in \mathrm{GL}_n(\mathbf{Z})$, la matrice finale obtenue est $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & \det(\mathrm{A}) \end{pmatrix}$. On a donc montré le résultat suivant.

Théorème 4.2. — *1° Le groupe* $\mathrm{SL}_n(\mathbf{Z})$ *est de type fini : il est engendré par les matrices élémentaires* $\mathrm{I}_n + \mathrm{E}_{ij}$, *pour* $i, j \in \{1, \dots, n\}$, $i \neq j$.

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

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

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

(et il ne peut pas être engendré par une seule matrice, puisqu'il n'est pas abélien). Le groupe $\mathrm{GL}_n(\mathbf{Z})$ peut aussi être engendré par seulement trois éléments (*cf.* exerc. 4.4).

Exercice 4.3. — a) Montrer que le groupe $\mathrm{SL}_2(\mathbf{Z})$ est engendré par les deux matrices

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

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

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

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

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

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

Exercice 4.4. — Montrer que pour tout n, le groupe $\mathrm{GL}_n(\mathbf{Z})$ peut être engendré par trois éléments (*Indication :* on pourra montrer qu'il est engendré par la matrice $\mathrm{I}_n + \mathrm{E}_{12}$ et deux matrices de permutation bien choisies).

Exercice 4.5. — Pour tout $n \geqslant 2$, on pose

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

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

Exercice 4.6. — Soit R un anneau euclidien (par exemple $\mathbf{Z}$ si vous ne savez pas ce que c'est). Pour tout $\mathrm{A} \in \mathrm{GL}_n(\mathrm{R})$, montrer qu'il existe une matrice $\mathrm{P} \in \mathrm{GL}_n(\mathrm{R})$ produit de matrices élémentaires $\mathrm{I}_n + \mathrm{E}_{ij}$ (avec $i \neq j$) telle que

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

Exercice 4.7. — a) Soit G un groupe de type fini et soit H un groupe fini. Montrer que l'ensemble des morphismes $\mathrm{G} \to \mathrm{H}$ est fini.
b) Soit G un groupe de type fini, soit $f : \mathrm{G} \to \mathrm{G}$ un morphisme surjectif, soit H un groupe fini et soit $g : \mathrm{G} \to \mathrm{H}$ un morphisme. Montrer $\ker(f) \subseteq \ker(g)$ (*Indication :* on pourra utiliser a) pour montrer qu'il existe $m > n > 0$ tels que $g \circ f^m = g \circ f^n$ puis, si $a \in \ker(f)$, introduire $b_n \in \mathrm{G}$ tel que $a = f^n(b_n)$).
c) Soit $f : \mathrm{SL}_n(\mathbf{Z}) \to \mathrm{SL}_n(\mathbf{Z})$ un morphisme surjectif. Montrer que f est un isomorphisme.

5. Groupes simples et suites de composition

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Le même type de raisonnement s'applique aux doubles transpositions : si $(12)(34) = \sigma\nu\sigma^{-1}$, alors $(123) = ((12)\sigma)\nu((12)\sigma)^{-1}$.

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

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

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

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

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

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

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

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

$$G_1 = \{\sigma \in \mathfrak{A}_n \mid \sigma(1) = 1\} \simeq \mathfrak{A}_{n-1}.$$

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

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

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{e\} \tag{13}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Une suite de composition $G = G'_0 \rhd G'_1 \rhd \cdots \rhd G'_s = \{e\}$ est dite *équivalente* à la suite (13) si $r = s$ et qu'il existe une permutation $\sigma \in \mathfrak{S}_r$ telle que $G_{\sigma(i)}/G_{\sigma(i)+1} \simeq G'_i/G'_{i+1}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\big(H_1/(H_1 \cap K_1) \simeq G/K_1, (H_1 \cap K_1)/L_3,\dots,L_{r-1}/L_r\big). \tag{14}$$

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

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

De la comparaison de (14) et (15) résulte que les suites de composition (H_i) et (K_j) de G sont équivalentes. □

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

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

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

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

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

Exercice 5.6. — Soit H un sous-groupe distingué d'un groupe fini G. Montrer que la collection de facteurs simples de G est la réunion de la collection des facteurs simples de H et de la collection des facteurs simples de G/H (il peut bien sûr y avoir des répétitions).

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

$$[x, y] := xyx^{-1}y^{-1} \tag{16}$$

vaut e. Le sous-groupe

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

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

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

Proposition 5.7. — *Le groupe dérivé* D(G) *est un* sous-groupe caractéristique *de* G*, c'est-à-dire qu'il est stable par tout automorphisme de* G*. En particulier, il est distingué.*

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

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

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

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

Proposition 5.8. — *Pour* $n \geqslant 5$*, on a* $D(\mathfrak{A}_n) = \mathfrak{A}_n$*. Pour* $n \geqslant 2$*, on a* $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

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

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

– soit à $\mathfrak{A}_n$.

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

On peut aussi remarquer que tout 3-cycle

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

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

Exercice 5.9. — Soit H un sous-groupe d'un groupe G. Montrer que D(H) est un sous-groupe de D(G) et qu'il est distingué dans D(G) si H est distingué dans G.

Exercice 5.10. — Soit n un entier $\geqslant 2$. Décrire tous les morphismes de $\mathfrak{S}_n$ dans $\mathbf{C}^\times$.

Exercice 5.11. — Montrer que groupe dérivé $\mathrm{D}(\mathrm{SL}_2(\mathbf{Z}))$ est d'indice divisant 12 dans $\mathrm{SL}_2(\mathbf{Z})$ (*Indication :* si R et S sont les générateurs de $\mathrm{SL}_2(\mathbf{Z})$ définis dans l'exerc. 4.3.a), on pourra calculer S^2, S^4, R^3 et R^6) [14].

Exercice 5.12. — Soit G un groupe. On note S l'ensemble de tous les commutateurs $[x,y]$ de G.

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

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

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

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

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

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

où $z = [x_3,y_3]$.

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

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

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

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

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

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

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

---

14. Il ressort de la note 12 que l'indice est exactement 12 (*cf.* aussi exerc. II.2.14). On peut montrer que $\mathrm{D}(\mathrm{SL}_2(\mathbf{Z}))$ est le sous-groupe de $\mathrm{SL}_2(\mathbf{Z})$ engendré par les matrices $[\mathrm{S},\mathrm{T}] = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$ et $[\mathrm{S},\mathrm{T}^{-1}] = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$.

α) Montrer que K est d'indice fini dans D(G) et qu'il est contenu dans Z(D(G)).
β) En déduire que D(D(G)) est fini. Il est distingué dans G par l'exerc. 5.9 ; on pose H := G/D(D(G)).
γ) Montrer que D(H) est abélien et en déduire que pour tout $x \in H$ et tout $d \in D(H)$, on a $[x,d]^2 = [x,d^2]$.
δ) En déduire que le sous-groupe $[H, D(H)]$ de H engendré par les $[x,d]$, pour $x \in H$ et $d \in D(H)$, est fini et distingué dans H. On pose $M := H/[H, D(H)]$.
ε) En déduire que D(M) est fini, puis que D(G) est fini.

6. Groupes résolubles

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

C'est une notion essentielle pour l'application de la théorie de Galois à la résolution par radicaux des équations polynomiales. Elle admet plusieurs définitions équivalentes que nous allons expliquer. Étant donné un groupe G, on définit une suite de sous-groupes

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

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

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

Noter que $D^{n+1}(G)$ est distingué dans $D^n(G)$ (et même dans G par l'exerc. 5.9) et que les groupes quotients $D^n(G)/D^{n+1}(G)$ sont abéliens.

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

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

(ii) il existe une suite

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

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

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

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

2° Le groupe $\mathfrak{S}_n$ est résoluble pour $n \leqslant 4$, mais pas pour $n \geqslant 5$ puisqu'on a alors $D^m(\mathfrak{S}_n) = \mathfrak{A}_n$ pour tout $m \geqslant 1$ (prop. 5.8).

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

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

4° Si $\mathbf{K}$ est un corps, le groupe affine $\mathrm{GA}(\mathbf{K})$ (*cf.* ex. 1.1.5°) est résoluble (*cf.* exerc. 1.27). En revanche, pour $n \geqslant 2$ et $\mathrm{card}(\mathbf{K}) \geqslant 4$, les groupes $\mathrm{SL}_n(\mathbf{K})$ et $\mathrm{GL}_n(\mathbf{K})$ ne le sont pas puisque leur groupe dérivé est $\mathrm{SL}_n(\mathbf{K})$ (th. II.2.6).

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

Proposition 6.3. — *Soit* G *un groupe et soit* H *un sous-groupe de* G.
1° Si G *est résoluble,* H *est résoluble.*
2° Si $\mathrm{H} \trianglelefteq \mathrm{G}$, *on a*

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

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

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

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

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

donc G est résoluble. □

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

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

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

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

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

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

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

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

Exercice 6.7. — Soient p et q des nombres premiers.
a) Montrer que tout groupe d'ordre pq est résoluble (*Indication :* on pourra utiliser l'exerc. 2.28).
b) Montrer que tout groupe d'ordre p^2q est résoluble (*Indication :* on pourra utiliser l'exerc. 2.31).
c) Montrer que tout groupe d'ordre p^3q est résoluble (*Indication :* on pourra utiliser l'exerc. 2.32).

Exercice 6.8. — Soient p et q des nombres premiers, avec $p \leqslant q$, et soit G un groupe d'ordre $p^m q^n$, avec $0 \leqslant m \leqslant 2$ et $n \geqslant 0$. Montrer que G est résoluble (*Indication :* on pourra utiliser l'exerc. 2.30).

Exercice 6.9. — Soit q un nombre premier impair et soit G un groupe d'ordre $8q^n$. Le but de cet exercice est de montrer que G est résoluble. On note n_q le nombre de q-Sylow de G.
a) Montrer que G est résoluble si $(q, n_q) \notin \{(3,4),(7,8)\}$.
b) On suppose $q = 3$ et $n_q = 4$. Montrer que G est résoluble (*Indication :* on pourra considérer l'action transitive de G sur l'ensemble des 3-Sylow et appliquer l'exerc. 6.8 âĂą son noyau).
c) On suppose $q = 7$ et $n_q = 8$. Montrer que G est résoluble (*Indication :* on pourra considérer l'action transitive de G sur l'ensemble des 7-Sylow ; pour le cas $n = 1$, on pourra compter les éléments d'ordre 7).

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

Exercice 6.11. — Montrer que tout groupe d'ordre 72 est résoluble (*Indication :* on pourra considérer les 3-Sylow et utiliser l'exerc. 2.29).

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

Exercice 6.13. — Montrer que tout groupe d'ordre 2907 est résoluble (*Indication :* on pourra utiliser l'exerc. 2.34).

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

Exercice 6.15. — Soit p un nombre premier. Le groupe affine $\mathrm{GA}(\mathbf{F}_p)$ (*cf.* ex. 1.1.5°) est résoluble (*cf.* ex. 6.2.4°) et il opère transitivement et fidèlement sur l'ensemble $\mathbf{F}_p = \{0, \dots, p-1\}$. On peut le voir comme un sous-groupe de $\mathfrak{S}_{\mathbf{F}_p} = \mathfrak{S}_p$; son cardinal est $p(p-1)$ (exerc. 1.27).

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

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

c) Soit τ' un générateur de H_{r-1}. Montrer qu'il existe $g \in \mathfrak{S}_p$ tel que $g\tau' g^{-1} = \tau$. On pose $H'_i := gH_i g^{-1}$.
d) Conclure $H \leq g^{-1}Gg$ (*Indication :* on pourra montrer $H'_i \leq G$ par récurrence descendante sur i, en utilisant b)).

Exercice 6.16. — Soit p un nombre premier. Le but de cet exercice est de montrer qu'un sous-groupe H de $\mathfrak{S}_p$ qui opère transitivement est résoluble si et seulement si aucun élément de H autre que l'identité laisse deux éléments de $\{1,\dots,p\}$ fixes.
a) On suppose que H est résoluble. Montrer que H a cette propriété (*Indication :* on pourra utiliser l'exercice précédent).
b) On suppose que H a cette propriété. On note $H_x \leq H$ le stabilisateur d'un point x de $\{1,\dots,p\}$. Montrer que les $(H_x - \{\mathrm{Id}\})_{x\in\{1,\dots,p\}}$ forment, avec l'ensemble S des éléments de H sans aucun point fixe, une partition de $H-\{\mathrm{Id}\}$. Montrer l'égalité $|H| = p|H_x|$ et en déduire le cardinal de S.
c) Montrer que H contient un p-cycle σ (*Indication :* on pourra utiliser le lemme de Cauchy (exerc. 2.14)) et que $S = \{\sigma,\dots,\sigma^{p-1}\}$.
d) Montrer que S est stable par conjugaison par tout élément de H (*Indication :* on pourra utiliser la question b) de l'exercice précédent). En déduire que H est conjugué à un sous-groupe du groupe affine $GA(\mathbf{F}_p)$ et conclure.

7. Groupes nilpotents

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

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

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

On obtient ainsi une suite croissante de sous-groupes

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

où les quotients successifs sont abéliens.

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

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

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

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

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

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

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

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

(on rappelle la notation de (16) : $[x,y] = xyx^{-1}y^{-1}$).

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

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

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

Cela entraîne les inclusions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Corollaire 7.9. — *Soit* G *un groupe nilpotent et soit* H *un sous-groupe de* G.
1° Le groupe H *est nilpotent.*
2° Si $H \trianglelefteq G$, *le groupe* G/H *est nilpotent* [16].

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

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

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

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

a) Montrer l'implication (ii)⇒(i).
On suppose maintenant G *nilpotent (fini).*
b) Soit $H < G$ un sous-groupe propre de G. Montrer que son normalisateur $N_G(H)$ (*cf.* (6)) contient strictement H (*Indication :* on pourra considérer le plus grand entier $m < n$ tel que $C^m(G) \leq H$, choisir $g \in C^{m+1}(G) - H$, et montrer $g \in N_G(H)$).
c) Soit S un p-Sylow de G. Montrer S est distingué dans G (*Indication :* on pourra utiliser l'exerc. 2.37.b)).
d) Soient S et S′ des sous-groupes de Sylow distincts de G. Montrer $S \cap S' = \{e\}$ et que tout élément de S commute avec tout élément de S′. En déduire (ii).

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

8. Croissance des groupes de type fini

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

Rappelons (§1.2) qu'un groupe G est *de type fini* s'il existe une partie génératrice finie $A = \{a_1, \ldots, a_r\} \subseteq G$. Pour tout entier $m \geqslant 0$, on note $B_{G,A}(m)$ l'ensemble des éléments de G

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

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

qui peuvent s'écrire comme produits d'au plus m éléments de $A \cup A^{-1}$. On veut étudier la fonction (croissante)

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

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

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

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

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

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

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

La croissance est donc au plus exponentielle.

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

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

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

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

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

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

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

On parlera ainsi (abusivement) de *la* fonction de croissance β_G de G.

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

$$B_{G,A}(m) \subseteq B_{G,A'}(am)$$

et la proposition. □

Exercice 8.4. — Soit H un sous-groupe d'un groupe de type fini G.

a) Si H est de type fini, montrer $\beta_H \preceq \beta_G$.

b) Si H est d'indice fini dans G, il est de type fini (exerc.1.14) ; montrer $\beta_H \sim \beta_G$.

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

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

Le groupe G est *à croissance exponentielle* si $\beta_G(m) \sim e^m$.

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

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

2° Pour $n \geqslant 2$, les groupes $\mathrm{SL}_n(\mathbf{Z})$ (qui sont de type fini par le th. 4.2) sont à croissance exponentielle [19].

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

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

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

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

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

$$[xy, z] = [y, z]\,[[z, y], x]\,[x, z], \tag{17}$$

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

Si on prend $z \in \mathrm{C}^n(\mathrm{G})$ dans (17), on obtient

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

puisque $[[z, x_2], x_1] \in \mathrm{C}^{n+2}(\mathrm{G})$. Ceci entraîne que le groupe $\mathrm{C}^{n+1}(\mathrm{G})/\mathrm{C}^{n+2}(\mathrm{G})$ est engendré par les classes des $[a_i^{\pm 1}, z]$ pour $1 \leqslant i \leqslant r$ et $z \in \mathrm{C}^n(\mathrm{G})$. Il suffit ensuite de décomposer z en produit des b_j et de leurs inverses et d'utiliser (18) de la même façon pour conclure. □

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

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

---

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

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

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

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

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

Soit donc $A = \{a_1, \dots, a_r\}$ un ensemble fini de générateurs de G, stable par inversion et contenant e. Pour tout entier $m \geqslant 0$, un élément g de $B_{G,A}(m)$ est produit de m éléments de A. Si on rencontre dans ce produit $a_j a_i$, avec $j > i$, on l'écrit $a_i a_j [a_j^{-1}, a_i^{-1}]$. Comme $[a_j^{-1}, a_i^{-1}]$ commute avec tous les éléments de G, on peut l'envoyer ensuite toute à la droite du produit. Cette opération nous permet d'écrire, après au plus $(m-1)+\cdots+1$ pas,

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

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

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

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

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

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

CHAPITRE II

GROUPES CLASSIQUES

1. Préliminaires sur les corps

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

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

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

défini par

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

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

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

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

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

On a les propriétés suivantes :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Le groupe linéaire

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

et son sous-groupe

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

Leur centre est trivial par construction.

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

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

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

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

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

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

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

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

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

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

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

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

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

ce qui montre le 2°. □

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

Exercice 2.8. — Soit K un corps fini et soit n un entier $\geqslant 1$. Décrire tous les morphismes de $\mathrm{GL}_n(\mathbf{K})$ dans $\mathbf{K}^\times$ (*Indication :* on pourra utiliser l'exerc. I.1.28).

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

Dans le cas d'un corps fini, on a déjà vu dans l'exerc. I.1.23 les cardinaux de certains de ces groupes :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Exercice 2.14. — On rappelle (exerc. I.5.11) que le groupe dérivé $\mathrm{D}(\mathrm{SL}_2(\mathbf{Z}))$ est d'indice divisant $\leqslant 12$ dans $\mathrm{SL}_2(\mathbf{Z})$.
a) Montrer que $\mathrm{SL}_2(\mathbf{Z})$ a un quotient d'ordre 2 et un quotient d'ordre 3 (*Indication :* on pourra utiliser l'exerc. 2.5, pour $p = 2$ et 3).
b) En déduire que l'indice de $\mathrm{D}(\mathrm{SL}_2(\mathbf{Z}))$ dans $\mathrm{SL}_2(\mathbf{Z})$ est 6 ou 12 (on peut montrer que c'est 12 (*cf.* note I.14) ; comparer avec l'exerc. 2.9).

2.4. Simplicité. — Une des raisons de notre intérêt pour les groupes linéaires est qu'ils donnent lieu, lorsqu'ils sont finis, à des séries infinies de groupes simples (tout comme les groupes alternés ; *cf.* th. I.5.1).

Le but de cette section est de démontrer le résultat suivant.

Théorème 2.15. — *Soit* $\mathbf{K}$ *un corps. Le groupe* $\mathrm{PSL}_n(\mathbf{K})$ *est simple sauf si* $n = 2$, *et* $\mathbf{K} = \mathbf{F}_2$ *ou* $\mathbf{F}_3$.

Les exceptions ne sont effectivement pas simples : $\mathrm{PSL}_2(\mathbf{F}_2) \simeq \mathfrak{S}_3$ admet $\mathfrak{A}_3$ comme sous-groupe distingué propre, tandis que $\mathrm{PSL}_2(\mathbf{F}_3) \simeq \mathfrak{A}_4$ admet un sous-groupe distingué d'indice 3 (ex. I.5.3.3°).

En prenant pour $\mathbf{K}$ un corps fini $\mathbf{F}_q$, on obtient donc ainsi une troisième série de groupes finis simples (les deux premières étant formées des groupes d'ordre premier d'un côté et des groupes alternés de l'autre) [4]. Il y a quelques coïncidences qui sont toutes indiquées dans le tableau p. 54.

Le premier nouveau groupe simple fini qu'on découvre dans ce tableau est donc le groupe $\mathrm{PSL}_3(\mathbf{F}_2)$, d'ordre 168 (*cf.* exerc. I.2.33). Le suivant est $\mathrm{PSL}_2(\mathbf{F}_8)$, d'ordre 504. Le plus petit groupe fini simple qui n'est ni cyclique, ni un groupe alterné, ni un groupe spécial linéaire est d'ordre 6048 ; c'est le groupe $\mathrm{PSU}_3(\mathbf{F}_9)$ qui sera défini dans le § 10.4 [5].

L'isomorphisme $\mathrm{PSL}_2(\mathbf{F}_7) \simeq \mathrm{PSL}_3(\mathbf{F}_2)$ découle abstraitement du fait que tous les groupes simples (*cf.* th. 2.15) d'ordre 168 sont isomorphes (de même, tous les groupes

4. Pour des raisons que vous comprendrez plus tard, le groupe $\mathrm{PSL}_n(\mathbf{F}_q)$ est aussi noté $\mathrm{A}_{n-1}(q)$.

5. Le suivant est le groupe de Mathieu M_{11}, de cardinal 7920, qui peut être défini comme le sous-groupe de $\mathfrak{S}_{11}$ engendré par le 11-cycle $(1,2,3,4,5,6,7,8,9,10,11)$ et la permutation $(3,7,11,8)(4,10,5,6)$. Il a été construit par Mathieu en 1861 (d'une autre façon !). C'est un des 26 groupes finis simples *sporadiques :* il ne fait pas partie d'une série infinie comme les groupes cycliques, alternés, ou projectifs spéciaux linéaires.

simples d'ordre 60 sont isomorphes (exerc. I.2.35), ce qui montre deux des isomorphismes du tableau) [6].

Ce n'est pas par hasard que les exceptions sont les mêmes dans les th. 2.6 et 2.15. En effet, on va présenter ici une démonstration où le second théorème est déduit du premier par la *méthode d'Iwasawa*, qui s'appuie sur l'action du groupe $\mathrm{PSL}_n(\mathbf{K})$ sur l'espace projectif $\mathbf{P}^{n-1}(\mathbf{K})$.

Plus généralement, supposons qu'un groupe G agisse sur un ensemble X. On dira que G agit *primitivement* sur X si

1° l'action de G sur X est transitive ;

2° le stabilisateur G_x d'un point de X (donc de tout point de X) est un sous-groupe maximal de G, c'est-à-dire que les seuls sous-groupes de G contenant G_x sont G_x et G.

Un cas particulier d'action primitive est donnée par une *action 2-transitive*, c'est-à-dire telle que

$$\forall x_1, x_2, y_1, y_2 \in \mathrm{X} \qquad (x_1 \neq x_2, y_1 \neq y_2 \implies \exists g \in \mathrm{G} \quad g \cdot x_1 = y_1 \quad g \cdot x_2 = y_2).$$

Autrement dit, l'action de G sur $\mathrm{X} \times \mathrm{X} - \Delta$, où $\Delta = \{(x, x) \mid x \in \mathrm{X}\}$, définie par $g \cdot (x, y) = (g \cdot x, g \cdot y)$ est transitive.

En effet, il suffit de vérifier qu'un stabilisateur G_x est un sous-groupe maximal. Soit donc $\mathrm{H} \leq \mathrm{G}$ un sous-groupe contenant strictement G_x et soit $h \in \mathrm{H} - \mathrm{G}_x$, de sorte que $y := h \cdot x \neq x$. Soit $g \in \mathrm{G} - \mathrm{G}_x$, de sorte que $z := g \cdot x \neq x$. Il existe alors $k \in \mathrm{G}$ tel que $k \cdot (x, z) = (x, y)$, c'est-à-dire $k \in \mathrm{G}_x$ et $k \cdot z = y$. Cette seconde relation s'écrit $(kg) \cdot x = h \cdot x$, c'est-à-dire $h^{-1}kg \in \mathrm{G}_x < \mathrm{H}$. Comme h et k sont dans H, on en déduit que tout élément g de $\mathrm{G} - \mathrm{G}_x$ est dans H, soit $\mathrm{H} = \mathrm{G}$.

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

Théorème 2.16. — *Supposons que le groupe* G *agisse primitivement sur* X. *Si on se donne, pour chaque* $x \in \mathrm{X}$, *un sous-groupe* $\mathrm{T}_x \leq \mathrm{G}$ *tel que*

1° T_x *est abélien ;*

2° $\mathrm{T}_{g \cdot x} = g\mathrm{T}_x g^{-1}$ *pour tout* $g \in \mathrm{G}$ *et tout* $x \in \mathrm{X}$ *;*

3° $\bigcup_{x \in \mathrm{X}} \mathrm{T}_x$ *engendre* G,

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

Démonstration. — Soit H un sous-groupe distingué de G agissant non trivialement sur X et soit $x \in \mathrm{X}$. Puisque G_x est maximal, le sous-groupe $\mathrm{HG}_x \leq \mathrm{G}$ (*cf.* exerc. I.1.26) est égal soit à G_x, soit à G.

Dans le premier cas, on a $\mathrm{H} \leq \mathrm{G}_x$ donc, pour tout $g \in \mathrm{G}$,

$$\mathrm{H} = g\mathrm{H}g^{-1} \leq g\mathrm{G}_x g^{-1} = \mathrm{G}_{g \cdot x}$$

ce qui, puisque G agit transitivement sur X, contredit le fait que H n'agit pas trivialement sur X.

6. Dans le même ordre d'idées, on sait que les seuls groupes simples d'ordre $8!/2$ sont (à isomorphisme près) $\mathfrak{A}_8 \simeq \mathrm{PSL}_4(\mathbf{F}_2)$ et $\mathrm{PSL}_3(\mathbf{F}_4)$.

On a donc $HG_x = G$. Comme l'action de G sur X est transitive, on a

$$X = G \cdot x = HG_x \cdot x = H \cdot x,$$

donc l'action de H sur X reste transitive. Montrons qu'en outre $G = HT_x$. En effet, si $h \in H$, on a par 2°

$$T_{h\cdot x} = hT_x h^{-1} \subseteq HT_x H = HT_x,$$

puisque $H \trianglelefteq G$. Puisque H agit transitivement sur X, on a donc $T_y \leq HT_x$ pour tout $y \in X$, donc $G = HT_x$ puisque les $(T_y)_{y\in X}$ engendrent G par 3°.

Finalement, puisque T_x est abélien,

$$G/H = HT_x \simeq T_x/(H \cap T_x)$$

(exerc. I.1.26) est abélien, de sorte que $H \supseteq D(G)$. □

Nous aurons encore besoin d'une autre définition. Soit a un élément non nul d'un **K**-espace vectoriel V de dimension finie n. On appelle *transvection* de vecteur a tout automorphisme de V de la forme

$$x \mapsto x + \ell(x)a,$$

où $\ell : V \to \mathbf{K}$ est une forme linéaire telle que $\ell(a) = 0$ (si $\ell \neq 0$ et $H := \ker(\ell)$, on dit aussi transvection d'hyperplan H ; notons que la transvection est l'identité sur H). On note cet automorphisme $\tau(\ell, a)$. On vérifie que

$$\tau(0, a) = \mathrm{Id}_V \quad \text{et} \quad \tau(\ell, a) \circ \tau(\ell', a) = \tau(\ell + \ell', a),$$

de sorte que les transvections de vecteur a forment un sous-groupe abélien de GL(V).

Si $u \in GL(V)$, le conjugué

$$u \circ \tau(\ell, a) \circ u^{-1} = \tau(\ell \circ u^{-1}, u(a))$$

est une transvection de vecteur $u(a)$ et d'hyperplan $u(H)$.

Enfin, si $\ell \neq 0$, on choisit une base $(a, e_2, \ldots, e_{n-1})$ de $\ker(\ell)$, que l'on complète en une base de V par un vecteur e_n. La matrice de $\tau(\ell, a)$ dans cette base est la matrice élémentaire $I_n + \ell(e_n)E_{1n}$. Toutes les matrices élémentaires sont en fait des matrices de transvection. Il résulte du th. 2.2.2° que les transvections engendrent SL(V).

Nous pouvons maintenant démontrer le th. 2.15.

Démonstration du th. 2.15. — L'action de $PSL_n(\mathbf{K})$ sur $X = \mathbf{P}^{n-1}(\mathbf{K})$ est fidèle et 2-transitive (il suffit en effet de remarquer qu'étant données des paires de points distincts de $\mathbf{P}^{n-1}(\mathbf{K})$, correspondant à des paires (D_1, D_2) et (D'_1, D'_2) de droites distinctes de $\mathbf{K}^n$, il existe un automorphisme linéaire de $\mathbf{K}^n$ qui envoie D_1 sur D'_1 et D_2 sur D'_2) donc primitive.

Pour chaque $x \in \mathbf{P}^{n-1}(\mathbf{K})$, correspondant à une droite vectorielle $D \subseteq \mathbf{K}^n$, on prend pour groupe T_x le groupe des transvections de $\mathbf{K}^n$ de vecteur un générateur de D. Comme on vient de l'expliquer, toutes les hypothèses du th. 2.16 sont vérifiées, donc un sous-groupe distingué de $PSL_n(\mathbf{K})$, non réduit à {Id}, doit contenir $D(PSL_n(\mathbf{K})) = PSL_n(\mathbf{K})$ (th. 2.6). □

Exercice 2.17. — a) Vérifier que les groupes $\mathfrak{A}_3$ et $\mathfrak{A}_4$ sont des quotients de $SL_2(\mathbf{F}_3)$ et le groupe $\mathfrak{A}_5$ est un quotient de $SL_2(\mathbf{F}_5)$.

b) Montrer que pour $m \geqslant 6$, le groupe $\mathfrak{A}_m$ n'est un quotient d'aucun groupe $\mathrm{SL}_2(\mathbf{F}_p)$ (*Indication :* on pourra utiliser les exerc. I.5.1 et I.5.6) [7].

***Exercice 2.18* (Une autre démonstration de la simplicité de $\mathrm{PSL}_n(\mathbf{K})$ pour $n \geqslant 3$)**

Soit G un sous-groupe distingué de $\mathrm{SL}_n(\mathbf{K})$ contenant strictement le centre $\mathrm{Z}(\mathrm{SL}_n(\mathbf{K}))$ et soit g un élément de G qui n'est pas une homothétie. On suppose $n \geqslant 3$.

a) Montrer que les transvections de $\mathbf{K}^n$ engendrent $\mathrm{SL}_n(\mathbf{K})$. En déduire qu'il existe une transvection τ, de vecteur a, avec laquelle g ne commute pas. On pose $h := g\tau g^{-1}\tau^{-1} \neq \mathrm{Id}$.

b) Pour tout $x \in \mathbf{K}^n$, montrer que $h(x) - x$ est combinaison linéaire de a et $g(a)$. Soit H un hyperplan de $\mathbf{K}^n$ contenant ces vecteurs (il en existe car $n \geqslant 3$). Montrer $h(\mathrm{H}) = \mathrm{H}$.

c) On suppose qu'il existe une transvection d'hyperplan H ne commutant pas avec h. Montrer que G contient une transvection autre que l'identité (*Indication :* on pourra considérer le commutateur de h et la transvection).

d) On suppose maintenant au contraire que h commute avec toutes les transvections d'hyperplan H. Montrer que h est une transvection.

e) Montrer que les transvections de $\mathbf{K}^n$ autres que l'identité sont toutes conjuguées dans $\mathrm{SL}_n(\mathbf{K})$. En déduire $\mathrm{G} = \mathrm{SL}_n(\mathbf{K})$.

***Exercice 2.19* (Une autre démonstration de la simplicité de $\mathrm{PSL}_2(\mathbf{K})$ pour $|\mathbf{K}| \notin \{2,3,5\}$)**

Soit G un sous-groupe distingué de $\mathrm{SL}_2(\mathbf{K})$.

a) On suppose que tout élément de G s'écrit $\mathrm{M} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $a \neq 0$. Montrer que tout élément de G est diagonal, puis que $\mathrm{G} \subseteq \{\mathrm{I}_2, -\mathrm{I}_2\}$ (*Indication :* on pourra calculer $(\mathrm{I}_2 + t\mathrm{E}_{12})\mathrm{M}(\mathrm{I}_2 + t\mathrm{E}_{12})^{-1}$ et $(\mathrm{I}_2 + t\mathrm{E}_{21})\mathrm{M}(\mathrm{I}_2 + t\mathrm{E}_{21})^{-1}$).

b) On suppose au contraire que G contient une matrice du type $\mathrm{M} = \begin{pmatrix} 0 & b \\ -b^{-1} & d \end{pmatrix}$. Soient $\alpha, \beta, \gamma \in \mathbf{K}$, avec $\beta \neq 0$. On pose $\mathrm{P}_{\alpha,\beta} := \begin{pmatrix} \alpha & \beta \\ -\beta^{-1} & 0 \end{pmatrix}$. Calculer

$$\begin{aligned} \mathrm{M}' &:= \mathrm{M}\mathrm{P}_{\alpha,\beta}\mathrm{M}^{-1}\mathrm{P}_{\alpha,\beta}^{-1}, \\ \mathrm{M}'' &:= \mathrm{M}'(\mathrm{I}_2 + \gamma\mathrm{E}_{12})\mathrm{M}'^{-1}(\mathrm{I}_2 + \gamma\mathrm{E}_{12})^{-1}, \\ \mathrm{M}''' &:= \mathrm{P}_{0,1}\mathrm{M}''\mathrm{P}_{0,1}^{-1}. \end{aligned}$$

En déduire que si $|\mathbf{K}| \notin \{2,3,5\}$, on a $\mathrm{G} = \mathrm{SL}_2(\mathbf{K})$.

c) Conclure.

***Exercice 2.20* (Une autre démonstration de la simplicité de $\mathrm{PSL}_2(\mathbf{F}_5)$)**

On peut montrer par des calculs du même type que ceux de l'exercice précédent que $\mathrm{PSL}_2(\mathbf{F}_5)$ est simple, conformément au th. 2.15. On peut aussi le démontrer de la façon suivante.

a) Montrer qu'il existe un morphisme injectif $\mathrm{PGL}_2(\mathbf{F}_5) \to \mathfrak{S}_6$.

b) En déduire que $\mathrm{PGL}_2(\mathbf{F}_5)$ est isomorphe à $\mathfrak{S}_5$ (*Indication :* on pourra calculer les ordres des groupes en présence et utiliser l'exerc. I.2.38).

---

7. On peut montrer que pour $m \geqslant 6$, le groupe $\mathfrak{A}_m$ n'est un quotient d'aucun groupe $\mathrm{SL}_2(\mathbf{Z}/\mathrm{N}\mathbf{Z})$ pour $\mathrm{N} \geqslant 2$, mais que pour $m \geqslant 9$, le groupe $\mathfrak{A}_m$ est en revanche quotient de $\mathrm{SL}_2(\mathbf{Z})$. Comme l'application de restriction $r_\mathrm{N} := \mathrm{SL}_2(\mathbf{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbf{Z}/\mathrm{N}\mathbf{Z})$ est surjective, le noyau de l'application $\mathrm{SL}_2(\mathbf{Z}) \twoheadrightarrow \mathfrak{A}_m$ est un sous-groupe (distingué) de $\mathrm{SL}_2(\mathbf{Z})$, d'indice fini, qui ne contient aucun $\ker(r_\mathrm{N}) = \{\mathrm{M} \in \mathrm{SL}_2(\mathbf{Z}) \mid \mathrm{M} \equiv \mathrm{I}_2 \pmod{\mathrm{N}}\}$. On dit que ce n'est pas un sous-groupe de congruence (l'existence de ces sous-groupes a été annoncée par Klein en 1879 et publiée indépendamment par Fricke et Pick en 1887). En revanche, c'est un théorème difficile de Bass, Lazard et Serre de 1964 que pour $n \geqslant 3$, tout sous-groupe de $\mathrm{SL}_n(\mathbf{Z})$ d'indice fini est un sous-groupe de congruence.

c) En déduire que $\mathrm{PSL}_2(\mathbf{F}_5)$ est isomorphe à $\mathfrak{A}_5$. C'est donc un groupe simple par le th. I.5.1.

3. Formes bilinéaires et quadratiques

Soit V un **K**-espace vectoriel. Dans cette section, on introduit les types de formes bilinéaires que l'on va étudier.

3.1. Définitions. — Une *forme bilinéaire* sur V est une application $b : \mathrm{V} \times \mathrm{V} \to \mathbf{K}$ telle que, pour chaque $y \in \mathrm{V}$, les applications partielles $x \mapsto b(x,y)$ et $x \mapsto b(y,x)$ sont **K**-linéaires. Une telle forme est

– *symétrique* si $b(x,y) = b(y,x)$ pour tous $x, y \in \mathrm{V}$;
– *alternée* si $b(x,x) = 0$ pour tout $x \in \mathrm{V}$.

Cette dernière condition entraîne (et, si $\mathrm{car}(\mathbf{K}) \neq 2$, lui est équivalente) le fait que b est

– *antisymétrique*, c'est-à-dire qu'elle vérifie $b(x,y) = -b(y,x)$ pour tous $x, y \in \mathrm{V}$.

Étant donnée une forme bilinéaire symétrique b, on définit la *forme quadratique* associée

$$f(x) := b(x,x).$$

On a alors

$$f(x+y) = f(x) + 2b(x,y) + f(y).$$

Si $\mathrm{car}(\mathbf{K}) \neq 2$ [8], on récupère la forme b à partir de f par la formule

$$b(x,y) = \frac{1}{2}(f(x+y) - f(x) - f(y)) \tag{19}$$

dite « de polarisation ».

Si V est de dimension finie n, la *matrice* M de la forme bilinéaire b dans une base $(e_1, \ldots, e_n)$ de V est la matrice $(b(e_i, e_j))_{1 \leqslant i,j \leqslant n}$. Si des éléments de V sont représentés par les vecteurs colonnes X et Y, alors $b(\mathrm{X}, \mathrm{Y}) = {}^t\mathrm{XMY}$. La forme b est (anti)symétrique si et seulement si la matrice M est (anti)symétrique. Si P est la matrice de passage de la base (e_i) à une base (e'_i), la matrice de b dans la nouvelle base est donnée par

$$\mathrm{M}' = {}^t\mathrm{PMP}.$$

Supposons b symétrique et notons f la forme quadratique associée. Si $\det(\mathrm{M}) \neq 0$, la classe de $\det(\mathrm{M})$ dans le groupe multiplicatif quotient $\mathbf{K}^\times / \mathbf{K}^{\times 2}$ est bien définie et s'appelle le *discriminant* de f, noté $\mathrm{disc}(f)$. Quand $\det(\mathrm{M}) = 0$, on convient que le discriminant est nul aussi [9].

La forme quadratique f est donnée par la formule

$$f(x_1 e_1 + \cdots + x_n e_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j,$$

8. Si $\mathrm{car}(\mathbf{K}) = 2$, il faut définir une forme quadratique sur V comme une application $f : \mathrm{V} \to \mathbf{K}$ telle que l'application $(x,y) \mapsto f(x+y) - f(x) - f(y)$ soit bilinéaire.

9. Cette notion n'a pas d'intérêt dans le cas alterné car nous verrons plus tard que $\det(\mathrm{M})$ est toujours un carré.

où $a_{ii} = f(e_i) = b(e_i, e_i)$ et $a_{ij} = 2b(e_i, e_j)$ si $i < j$. En d'autres termes, une forme quadratique sur un espace vectoriel de dimension finie est donnée par un *polynôme homogène de degré 2* en les composantes d'un vecteur [10].

3.2. Quadriques. — Attention de ne pas étendre aux formes bilinéaires symétriques générales les propriétés que vous pouvez connaître des *produits scalaires*. Ceux-ci correspondent au cas des formes bilinéaires symétriques définies positives sur un espace vectoriel réel, ce qui est un cas très particulier.

Il faut plutôt penser à une forme quadratique en termes géométriques de la façon suivante. Une *quadrique affine* $\mathrm{Q} \subseteq \mathbf{K}^n$ est définie par une équation polynomiale de degré 2

$$f_2(x_1, \ldots, x_n) + f_1(x_1, \ldots, x_n) + f_0 = 0,$$

où f_i est un polynôme homogène de de degré i. L'homogénéisé

$$f(x_0, x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n) + f_1(x_1, \ldots, x_n)x_0 + f_0 x_0^2$$

est une forme quadratique sur $\mathbf{K}^{n+1}$. L'équation $f(x_0, x_1, \ldots, x_n) = 0$ définit un cône quadratique $\mathrm{C} \subseteq \mathbf{K}^{n+1}$ (et Q est l'intersection de C avec l'hyperplan affine d'équation $x_0 = 1$) mais aussi une quadrique projective

$$\bar{\mathrm{Q}} := \{(x_0 : x_1 : \ldots : x_n) \in \mathbf{P}^n(\mathbf{K}) \mid f(x_0, x_1, \ldots, x_n) = 0\}$$

(noter que l'annulation de $f(x_0, x_1, \ldots, x_n)$ ne dépend pas du choix des coordonnées homogènes $(x_0 : x_1 : \ldots : x_n)$). Bien sûr, cette quadrique peut être vide, comme par exemple la quadrique d'équation $x_0^2 + \cdots + x_n^2 = 0$ dans $\mathbf{P}^n(\mathbf{R})$ ou la quadrique d'équation $x_0^2 + x_1^2 - 3x_2^2 = 0$ dans $\mathbf{P}^2(\mathbf{Q})$.

L'application injective

$$\begin{array}{ccc} \mathbf{K}^n & \longrightarrow & \mathbf{P}^n(\mathbf{K}) \\ (x_1, \ldots, x_n) & \longmapsto & (1 : x_1 : \ldots : x_n) \end{array}$$

identifie $\mathbf{K}^n$ avec le sous-ensemble de $\mathbf{P}^n(\mathbf{K})$ défini par $x_0 \neq 0$. On retrouve la quadrique affine Q comme l'intersection de $\bar{\mathrm{Q}}$ avec ce sous-ensemble.

Exemples 3.1. — Considérons dans $\mathbf{R}^2$ la conique Q d'équation

$$x_1^2 - x_2^2 + 2x_2 + 1 = 0.$$

L'homogénéisé est $f(x_0, x_1, x_2) := x_1^2 - x_2^2 + 2x_0x_2 + x_0^2$ et définit une conique projective $\bar{\mathrm{Q}} \subseteq \mathbf{P}^2(\mathbf{R})$. Il y a deux points « à l'infini » (c'est-à-dire avec $x_0 = 0$), à savoir $(0 : 1 : 1)$ et $(0 : 1 : -1)$. Ils correspondent aux deux asymptotes de l'hyperbole Q.

10. Cette formulation reste d'ailleurs valable en caractéristique 2.

3.3. Formes non dégénérées. — Soit b une forme bilinéaire symétrique ou alternée sur un espace vectoriel V de dimension finie sur un corps **K** de caractéristique $\neq 2$.

On note $\hat{b} : \mathrm{V} \to \mathrm{V}^*$ l'application linéaire qui à $x \in \mathrm{V}$ associe la forme linéaire $y \mapsto b(x,y)$.

On définit le *noyau* de b comme celui de $\hat{b}$, c'est-à-dire

$$\ker(b) := \{x \in \mathrm{V} \mid \forall y \in \mathrm{V} \quad b(x,y) = 0\} = \{y \in \mathrm{V} \mid \forall x \in \mathrm{V} \quad b(x,y) = 0\}$$

et on dit que b est *non dégénérée* si $\ker(b) = 0$. On appelle souvent *forme symplectique* une forme alternée non dégénérée.

On définit le *rang* de b comme celui de $\hat{b}$. La matrice de $\hat{b}$ dans une base de V et sa base duale dans V^* est la matrice de b comme définie plus haut. En particulier, le rang de b est le rang de cette matrice.

Proposition 3.2. *— Les conditions suivantes sont équivalentes :*

1° *b est non dégénérée ;*

2° *l'application linéaire $\hat{b} : \mathrm{V} \to \mathrm{V}^*$ est bijective ;*

3° *la matrice de b dans une base de* V *est inversible, c'est-à-dire que le rang de b est la dimension de* V.

Démonstration. — La première condition est exactement que $\hat{b}$ soit injective. Comme V est de dimension finie, c'est équivalent à dire que $\hat{b}$ est bijective, c'est-à-dire la seconde condition, ou encore surjective, ce qui donne la troisième condition. □

La restriction de b à tout supplémentaire de $\ker(b)$ dans V est non dégénérée. Cela permet de se ramener à une forme non dégénérée, ce qu'on fera le plus souvent.

3.4. Groupe d'isométries. — Soient V et V' des espaces vectoriels sur un corps **K** *de caractéristique $\neq 2$* équipés de formes b et b' de même type (symétriques ou alternées). Une application linéaire *injective* $u : \mathrm{V} \to \mathrm{V}'$ est une *isométrie* si, pour tous $x, y \in \mathrm{V}$, on a

$$b'(u(x), u(y)) = b(x,y).$$

Si b et b' sont des formes bilinéaires symétriques, de formes quadratiques associées f et f', il suffit que

$$f'(u(x)) = f(x)$$

pour tout $x \in \mathrm{V}$.

Si b est non dégénérée, l'injectivité découle de la propriété d'isométrie. Si en outre $(\mathrm{V}', b') = (\mathrm{V}, b)$, toute isométrie est un isomorphisme et l'ensemble des isométries forme un groupe pour la composition. L'appellation habituelle de ce groupe est différente suivant les cas :

– pour une forme quadratique f, le *groupe orthogonal* $\mathrm{O}(\mathrm{V}, f)$;

– pour une forme alternée b, le *groupe symplectique* $\mathrm{Sp}(\mathrm{V}, b)$.

Dans tous les cas, si M est la matrice de la forme b dans une base, une matrice U représente une isométrie si ${}^t\mathrm{UMU} = \mathrm{M}$.

Comme b est non dégénérée, cela implique $\det(\mathrm{U})^2 = 1$ donc $\det(\mathrm{U}) = \pm 1$. Le *groupe spécial orthogonal* est alors défini comme $\mathrm{SO}(\mathrm{V}, f) := \mathrm{O}(\mathrm{V}, f) \cap \mathrm{SL}(\mathrm{V})$.

Le groupe symplectique n'a pas de forme « spéciale » car il est déjà inclus dans SL(V), comme on le verra plus loin (cor. 7.2).

4. Orthogonalité

Dans la suite, b désignera une forme bilinéaire *symétrique ou alternée* sur un espace vectoriel V *de dimension finie* sur un corps $\mathbf{K}$ *de caractéristique* $\neq 2$.

4.1. Définition. — On dit que des vecteurs x et y sont *orthogonaux* si $b(x,y)=0$; vu les propriétés de b, c'est la même chose que de demander $b(y,x)=0$: c'est donc une relation symétrique. L'*orthogonal* d'une partie W de V est le sous-espace vectoriel, noté $\mathrm{W}^\perp$, des vecteurs de V orthogonaux à tous les éléments de W. On a par exemple $\ker(b)=\mathrm{V}^\perp$.

Proposition 4.1. — *Si b est* non dégénérée *et que* W *est un sous-espace vectoriel de* V*, on a*

$$\dim(\mathrm{W})+\dim(\mathrm{W}^\perp)=\dim(\mathrm{V}).$$

En particulier, si $\mathrm{W}\cap\mathrm{W}^\perp=0$ *(ce qui est équivalent à* $b|_\mathrm{W}$ *non dégénérée),* $\mathrm{V}=\mathrm{W}\oplus\mathrm{W}^\perp$.

Démonstration. — L'application linéaire $r:\mathrm{V}^*\to\mathrm{W}^*$ de restriction des formes linéaires est surjective, donc la composée

$$\begin{array}{rcl} r\circ\hat{b}:\mathrm{V} & \to & \mathrm{W}^* \\ x & \mapsto & b(x,\cdot) \end{array}$$

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

Voici quelques formules sur l'orthogonal (la seconde est vraie aussi en dimension infinie) :

$$(\mathrm{W}^\perp)^\perp=\mathrm{W},\quad (\mathrm{W}+\mathrm{W}')^\perp=\mathrm{W}^\perp\cap\mathrm{W}'^\perp,\quad (\mathrm{W}\cap\mathrm{W}')^\perp=\mathrm{W}^\perp+\mathrm{W}'^\perp.$$

On dit qu'un vecteur $x\in\mathrm{V}$ est *isotrope* si $b(x,x)=0$, c'est-à-dire si $x\in x^\perp$. On dit aussi que la droite $\mathbf{K}x$ est isotrope.

Un sous-espace vectoriel $\mathrm{W}\subseteq\mathrm{V}$ est *totalement isotrope* si $b|_\mathrm{W}=0$, ce qui est équivalent à $\mathrm{W}\subseteq\mathrm{W}^\perp$.

Exemple 4.2. — Comme on l'a vu dans le § 3.2, une forme quadratique f sur $\mathbf{K}^{n+1}$ définit une quadrique projective $\bar{\mathrm{Q}}\subseteq\mathbf{P}^n(\mathbf{K})$. Les points de Q sont en bijection avec les droites vectorielles $\mathrm{D}\subseteq\mathbf{K}^{n+1}$ isotropes pour f.

Si $\mathbf{K}=\mathbf{R}$, l'orthogonal $\mathrm{D}^\perp$ correspond à l'espace tangent à $\bar{\mathrm{Q}}$ en ce point ; cela résute de la formule

$$df(x)(y)=2b(x,y)$$

donnant la différentielle de f en x, obtenue en différentiant la formule de polarisation (19).

Dans l'ex. 3.1 de la conique Q d'équation $x_1^2-x_2^2+2x_2+1=0$ dans $\mathbf{K}^2$, si (a_1,a_2) est un point de Q, la droite $\mathbf{R}(1,a_1,a_2)$ est isotrope pour f (elle définit un point de $\bar{\mathrm{Q}}$) et son orthogonal pour f est défini par

$$a_1x_1-a_2x_2+x_2+a_2x_0+x_0=0.$$

La droite tangente à Q en (a_1,a_2) a donc pour équation affine $a_1x_1-a_2x_2+x_2+a_2+1=0$.

4.2. Décomposition en somme directe orthogonale : cas d'un vecteur non isotrope. — Si la forme symétrique b n'est pas nulle, il résulte de la formule (19) qu'il existe un vecteur non isotrope x. Dans ce cas, on a $\mathbf{K}x \cap x^\perp = 0$ donc $\mathrm{V} = \mathbf{K}x \oplus x^\perp$. Par récurrence sur la dimension, en considérant la restriction de b à $x^\perp$, on obtient l'existence d'une *base orthogonale* $(e_1, \dots, e_n)$, c'est-à-dire satisfaisant $b(e_i, e_j) = 0$ si $i \neq j$. Posant $\alpha_i = b(e_i, e_i)$, on obtient

$$f(x) = \alpha_1 x_1^2 + \cdots + \alpha_r x_r^2,$$

avec $0 \leqslant r \leqslant n$ et $\alpha_1, \dots, \alpha_r$ non nuls ; c'est la *réduction de Gauss* de la forme quadratique f. L'entier r ne dépend que de la forme f car c'est son rang.

Dans la base $(a_1 e_1, \dots, a_n e_n)$, où $a_i \in \mathbf{K}^\times$, les coefficients α_i deviennent $\alpha_i a_i^2$. Si $\alpha_1, \dots, \alpha_n$ sont des scalaires non nuls, il est d'usage de noter la forme quadratique non dégénérée $(x_1, \dots, x_n) \mapsto \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2$ sur $\mathbf{K}^n$ par le symbole

$$\langle \alpha_1, \dots, \alpha_n \rangle$$

et l'isométrie entre deux telles formes par le symbole $\simeq$. Pour tous scalaires non nuls $a_1, \dots, a_n$, on a donc

$$\langle \alpha_1, \dots, \alpha_n \rangle \simeq \langle a_1^2 \alpha_1, \dots, a_n^2 \alpha_n \rangle.$$

En d'autres termes, on peut considérer que les α_i sont dans $\mathbf{K}^\times / \mathbf{K}^{\times 2}$. On a $\mathrm{disc}(\langle \alpha_1, \dots, \alpha_n \rangle) = \alpha_1 \cdots \alpha_n$.

Le problème de la classification des formes quadratiques est de savoir quand des formes $\langle \alpha_1, \dots, \alpha_n \rangle$ et $\langle \beta_1, \dots, \beta_n \rangle$ sont isométriques, avec $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in \mathbf{K}^\times / \mathbf{K}^{\times 2}$. Une condition nécessaire est que les discriminants soient les mêmes, $\alpha_1 \cdots \alpha_n = \beta_1 \cdots \beta_n$ dans $\mathbf{K}^\times / \mathbf{K}^{\times 2}$, mais elle n'est en général pas suffisante.

Exemples 4.3. — 1° Si $\mathbf{K}$ est un corps algébriquement clos (ou plus généralement si $\mathbf{K}$ est *quadratiquement clos,* c'est-à-dire $\mathbf{K} = \mathbf{K}^2$), on peut toujours trouver a_i tel que $a_i^2 = 1/\alpha_i$. Il en résulte qu'étant donnée une forme quadratique non dégénérée f sur $\mathbf{K}^n$, il existe une base dans laquelle elle s'écrit

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

Son groupe orthogonal (indépendant donc de f) est noté $\mathrm{O}_n(\mathbf{K})$.

2° Si $\mathbf{K} = \mathbf{R}$, on peut toujours trouver a_i tel que $a_i^2 = \pm 1/\alpha_i$. En réarrangeant la base, on déduit qu'étant donnée une forme quadratique non dégénérée f sur $\mathbf{R}^n$, il existe une base dans laquelle elle s'écrit

$$f(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_n^2.$$

Le couple $(s, n-s)$ est la signature de f ; on verra plus loin (ex. 5.6.1°) que c'est un invariant de f. Son groupe orthogonal est noté $\mathrm{O}_{s,n-s}(\mathbf{R})$ et on note $\mathrm{O}_n(\mathbf{R})$ au lieu de $\mathrm{O}_{n,0}(\mathbf{R})$. Comme les groupes orthogonaux de f et de $-f$ sont les mêmes, on a $\mathrm{O}_{s,t}(\mathbf{R}) \simeq \mathrm{O}_{t,s}(\mathbf{R})$. Le discriminant est $(-1)^{n-s}$ donc ne suffit pas à distinguer les formes quadratiques.

3° Si $\mathbf{K} = \mathbf{F}_q$, alors $\mathbf{F}_q^\times / \mathbf{F}_q^{\times 2}$ est d'ordre 2 (car, q étant impair, le noyau de $x \mapsto x^2$ dans $\mathbf{F}_q^\times$ est $\{\pm 1\}$). Donc on peut ramener chaque α_i non nul à être égal à 1 ou à $\alpha \notin \mathbf{F}_q^{\times 2}$. Mais on peut en fait faire mieux.

Proposition 4.4. — *Étant donnée une forme quadratique f non dégénérée sur $\mathbf{F}_q^n$, il existe une base dans laquelle elle s'écrit sous l'une des deux formes suivantes :*

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

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

Notons que les deux formes proposées ne sont pas équivalentes, puisque leurs discriminants sont 1 et α, qui sont différents dans $\mathbf{F}_q^\times/\mathbf{F}_q^{\times 2}$. On déduit de la proposition que des formes quadratiques non dégénérées sur $\mathbf{F}_q^n$ sont équivalentes si et seulement si elles ont même discriminant.

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

Écrivons f dans une base orthogonale, $f(x) = \sum_{i=1}^n \alpha_i x_i^2$. Puisqu'il y a $\frac{q+1}{2}$ carrés dans $\mathbf{F}_q$ (en comptant 0) et que $\alpha_1\alpha_2 \neq 0$, les quantités $\alpha_1 x_1^2$ et $1-\alpha_2 x_2^2$ décrivent toutes deux un ensemble à $\frac{q+1}{2}$ éléments quand x_1 (resp. x_2) décrit $\mathbf{F}_q$. Puisque $2\frac{q+1}{2} > q$, il existe x_1, x_2 tels que $\alpha_1 x_1^2$ et $1-\alpha_2 x_2^2$ coïncident, c'est-à-dire $f(x_1, x_2, 0, \ldots, 0) = 1$. □

On a donc *a priori* deux groupes orthogonaux pour chaque dimension, selon que le discriminant de la forme est trivial ou non. Cependant les groupes orthogonaux de $\langle 1, \ldots, 1\rangle$ et de $\langle \alpha, \ldots, \alpha\rangle$ sont les mêmes et la seconde forme est de discriminant α^n.

Si $n = 2m+1$ est impair, on a donc un seul groupe orthogonal, noté $\mathrm{O}_{2m+1}(\mathbf{F}_q)$.

Si $n = 2m$ est pair, on note les deux groupes orthogonaux $\mathrm{O}_{2m}^+(\mathbf{F}_q)$ et $\mathrm{O}_{2m}^-(\mathbf{F}_q)$ [11] (il ressort de (27) que leurs cardinaux sont différents : ils ne sont donc pas isomorphes).

4° Si $\mathbf{K} = \mathbf{Q}$, on a une infinité de discriminants possibles, puisque le groupe $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ est infini. Étant donnée une forme quadratique sur $\mathbf{Q}$, on peut aussi la voir comme une forme quadratique sur $\mathbf{R}$ et considérer sa signature. Mais, même à discriminant et signature fixés, il existe encore une infinité de classes d'équivalence de formes quadratiques sur $\mathbf{Q}$ [12].

Exercice 4.5. — Soit $\mathbf{K}$ un corps. Pour tous α, β dans $\mathbf{K}^\times$ tels que $\alpha+\beta \neq 0$, montrer $\langle \alpha, \beta\rangle \simeq \langle \alpha+\beta, \alpha\beta(\alpha+\beta)\rangle$.

***Exemple 4.6* (Pinceaux de formes quadratiques).** — Soit V un espace vectoriel de dimension n sur un corps $\mathbf{K}$ algébriquement clos (de caractéristique $\neq 2$) et soient f et f' des formes quadratiques sur V. On suppose f non dégénérée. Le *pinceau* engendré par f et f' est l'ensemble de formes quadratiques

$$\{f_\lambda := \lambda f - f' \mid \lambda \in \mathbf{K}\}.$$

11. Plus précisément, le groupe $\mathrm{O}_{2m}^+(\mathbf{F}_q)$ est le groupe d'isométries de toute forme quadratique de discriminant $(-1)^m$ et $\mathrm{O}_{2m}^-(\mathbf{F}_q)$ le groupe d'isométries de toute forme quadratique de discriminant $(-1)^m\alpha$.

12. Pour décrire ces classes d'équivalence, il faut voir une forme quadratique sur $\mathbf{Q}$ comme une forme quadratique non seulement sur son complété $\mathbf{R}$, mais aussi sur chacun des corps p-adiques $\mathbf{Q}_p$, où p est un nombre premier impair : des formes quadratiques sur $\mathbf{Q}$ sont équivalentes si et seulement si elles le sont dans $\mathbf{R}$ et dans chacun des $\mathbf{Q}_p$ (« Théorème de Hasse-Minkowski » ; Serre, J.-P., *Cours d'arithmétique,* chap. IV, th. 9 ; *cf.* aussi prop. 7). Sur chacun de ces corps, il y a un invariant facile à calculer qui permet de tester l'équivalence (c'est la signature sur le corps $\mathbf{R}$ et un invariant dans $\{\pm 1\}$ sur les corps $\mathbf{Q}_p$).

On choisit une base de V dans laquelle la matrice de f est I_n (ex. 4.3.1°) ; soit M la matrice de g dans cette même base. La forme quadratique f_λ est dégénérée si et seulement si $\det(\lambda \mathrm{I}_n - \mathrm{M}) = 0$, c'est-à-dire si λ est valeur propre de M. Supposons ces valeurs propres $\lambda_1, \ldots, \lambda_n$ toutes distinctes (c'est le cas « général »). La matrice M est alors diagonalisable [13] : il existe une base $(e_1, \ldots, e_n)$ de V composée de vecteurs propres de M. Plus précisément, $\mathrm{ME}_i = \lambda_i \mathrm{E}_i$, où E_i est la matrice (colonne) des composantes de e_i dans la base de départ. On a alors, pour $i \neq j$,

$$b'(e_i, e_j) = {}^t\mathrm{E}_i \mathrm{ME}_j = \lambda_j {}^t\mathrm{E}_i \mathrm{E}_j,$$

qui est aussi égal, par symétrie de b', à

$$b'(e_j, e_i) = {}^t\mathrm{E}_j \mathrm{ME}_i = \lambda_i {}^t\mathrm{E}_j \mathrm{E}_i = \lambda_i {}^t\mathrm{E}_i \mathrm{E}_j.$$

Comme $\lambda_i \neq \lambda_j$, on en déduit $0 = {}^t\mathrm{E}_i \mathrm{E}_j = b(e_i, e_j) = b'(e_i, e_j)$. La base $(e_1, \ldots, e_n)$ est donc orthogonale à la fois pour f et pour f'. En remplaçant e_i par $e_i / \sqrt{b(e_i, e_i)}$, on obtient une base de V dans laquelle

$$\begin{aligned} f(x) &= x_1^2 + \cdots + x_n^2, \\ f'(x) &= \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2. \end{aligned}$$

C'est le cas le plus simple. Dans tous les cas, on peut définir pour tout pinceau de formes quadratiques une suite de nombres appelée *symbole de Segre* du pinceau et, pour chaque symbole, une « forme normale » des quadriques du pinceau.

***Exercice 4.7* (Pinceaux de formes quadratiques, suite).** — Soit V un espace vectoriel de dimension n sur un corps $\mathbf{K}$ algébriquement clos (de caractéristique $\neq 2$) et soient f et f' des formes quadratiques sur V. On suppose f non dégénérée et on pose

$$\mathrm{X} := \{x \in \mathrm{V} \mid f(x) = f'(x) = 0\}.$$

C'est un cône dans V.

a) Montrer l'équivalence des conditions suivantes :

(i) il existe une base $\mathscr{B}$ de V et $\lambda_1, \ldots, \lambda_n \in \mathbf{K}$ distincts tels que, pour tout $x \in \mathrm{V}$ de coordonnées $(x_1, \ldots, x_n)$ dans $\mathscr{B}$,

$$\begin{aligned} f(x) &= x_1^2 + \cdots + x_n^2, \\ f'(x) &= \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2; \end{aligned}$$

(ii) l'ensemble des $\lambda \in \mathbf{K}$ tels que la forme quadratique $\lambda f - f'$ soit dégénérée a n éléments ;

(iii) pour tout $x \in \mathrm{X} - \{0\}$, les orthogonaux de x pour f et pour f' sont des hyperplans distincts de V.

(*Indication :* l'équivalence (i) $\Leftrightarrow$ (ii) est l'ex. 4.6 ci-dessus.)

b) On suppose les conditions équivalentes de a) satisfaites et n impair. Montrer que X contient exactement 2^{n-1} sous-espaces vectoriels de V de dimension $(n-1)/2$ et qu'ils forment une unique orbite sous l'action du groupe μ_2^n (où $\mu_2 = \{1, -1\} \simeq \mathbf{Z}/2\mathbf{Z}$ est le groupe des racines carrées de 1 dans $\mathbf{K}$) donnée dans la base $\mathscr{B}$ de V de la condition (i) ci-dessus par $(\varepsilon_1, \ldots, \varepsilon_n) \cdot (x_1, \ldots, x_n) = (\varepsilon_1 x_1, \ldots, \varepsilon_n x_n)$.

(*Commentaire :* le cas $n = 3$ est relativement facile. Le cas général peut se faire au prix de calculs assez lourds, pour lesquels on peut consulter la partie 3 de la thèse de M. Reid à www.maths.warwick.ac.uk/ miles/3folds/qu.pdf).

13. Attention : la matrice M est symétrique, mais cela n'entraîne pas en général qu'elle est diagonalisable !

4.3. Décomposition en somme directe orthogonale : cas d'un vecteur isotrope. — La forme b est ici symétrique ou alternée, non dégénérée.

Lemme 4.8. — *Si x est un vecteur isotrope non nul, il existe un vecteur isotrope y tel que $b(x,y)=1$.*

Dans la base (x,y) du plan P engendré par x et y, la matrice de b est $\begin{pmatrix}0 & 1\\ \varepsilon & 0\end{pmatrix}$, où $\varepsilon = 1$ ou -1 selon que b est symétrique ou alternée. On dit que P est un *plan hyperbolique*.

Démonstration. — Comme b est non dégénérée et que x n'est pas nul, on peut toujours trouver x' tel que $b(x,x')=1$, puis on prend $y = x' - \frac{1}{2}b(x',x')x$, qui satisfait les propriétés voulues. □

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

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

La forme b est encore non dégénérée sur $\mathrm{P}^{\perp}$ et on peut recommencer la même opération sur $\mathrm{P}^{\perp}$, si celui-ci admet un vecteur isotrope non nul. Finalement, on fabrique une décomposition en somme directe orthogonale

$$\mathrm{V} = \mathrm{P}_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \mathrm{P}_\nu \overset{\perp}{\oplus} \mathrm{W},$$

où $\mathrm{P}_1,\dots,\mathrm{P}_\nu$ sont des plans hyperboliques et où le seul vecteur isotrope de W est 0 ; on dit que W est un *sous-espace anisotrope*.

L'entier ν est l'*indice* de la forme b ; on verra plus loin (cor. 5.5.2°) que c'en est un invariant. Une somme orthogonale de plans hyperboliques comme ci-dessus $\mathrm{P}_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \mathrm{P}_\nu$ est appelée un *espace hyperbolique*.

On a obtenu à ce stade deux formes de réduction pour une forme quadratique f :
- une décomposition dite de Gauss en $\langle\alpha_1,\dots,\alpha_n\rangle$;
- une décomposition en somme directe orthogonale d'un espace hyperbolique et d'un espace anisotrope.

Remarquons que toute forme $\langle\alpha,-\alpha\rangle$ ($\alpha\in\mathbf{K}^\times$) est un plan hyperbolique, puisqu'elle contient un vecteur isotrope non nul, $(1,1)$. Concrètement, cette forme s'écrit $f(x_1,x_2) = \alpha x_1^2 - \alpha x_2^2$ dans une base (e_1,e_2) et $f(y_1,y_2) = 2y_1y_2$ dans la base $(\frac{1}{\alpha}(e_1+e_2), e_1-e_2)$, qui est donc hyperbolique.

Exemples 4.9. — 1° Si $\mathbf{K}$ est quadratiquement clos, toute forme quadratique non dégénérée sur $\mathbf{K}^n$ peut s'écrire $\langle 1,-1,1,-1,\dots,\rangle$. C'est donc la somme directe orthogonale de $\lfloor n/2\rfloor$ plans hyperboliques et, si n est impair, de la forme anisotrope $\langle 1\rangle$.

2° Si $\mathbf{K}=\mathbf{R}$, on a vu (ex. 4.3.2°) que toute forme quadratique non dégénérée s'écrit

$$\langle \underbrace{1,\dots,1}_{s\text{ fois}}, \underbrace{-1,\dots,-1}_{t\text{ fois}}\rangle.$$

Si $s\leqslant t$, c'est donc la somme directe orthogonale de s plans hyperboliques et de la forme définie négative (donc anisotrope) $\langle \underbrace{-1,\dots,-1}_{t-s\text{ fois}}\rangle$.

Exercice 4.10. — Soit **K** un corps de caractéristique différente de 2 et soit f une forme quadratique non dégénérée sur un **K**-espace vectoriel V de dimension finie non nulle. Soit $a \in \mathbf{K}$. On dit que f *représente* a s'il existe $v \in \mathrm{V}$ non nul tel que $f(v) = a$.
a) La forme quadratique $\langle 1,1,1,-7\rangle$ sur $\mathbf{Q}^4$ représente-t-elle 0 ?
b) Si f représente 0, montrer que f représente tout élément de **K**.
c) Soit g une forme quadratique non dégénérée sur un **K**-espace vectoriel W de dimension finie non nulle. Montrer que les propriétés suivantes sont équivalentes :
(i) il existe $a \in \mathbf{K}^*$ qui est représenté à la fois par f et par g ;
(ii) la forme quadratique $h(v,w) = f(v) - g(w)$ sur l'espace vectoriel $\mathrm{V} \oplus \mathrm{W}$ représente 0.

4.4. Décomposition en somme directe orthogonale : cas alterné. — On suppose b alternée (et non dégénérée). Dans ce cas, tout vecteur est isotrope et on obtient comme ci-dessus une décomposition en somme directe orthogonale (l'espace W est nécessairement nul)

$$\mathrm{V} = \mathrm{P}_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \mathrm{P}_\nu.$$

En particulier, la dimension de V est paire (égale à 2ν) et, à isométrie près, il n'y a qu'une seule forme alternée non dégénérée sur un **K**-espace vectoriel de dimension paire 2ν ; on notera son groupe d'isométries $\mathrm{Sp}_{2\nu}(\mathbf{K})$.

Dans une base $(e_1,\dots,e_{2\nu})$ telle que $(e_i, e_{i+\nu})$ est une base standard de P_i, la matrice de b est

$$\mathrm{J}_{2\nu} = \begin{pmatrix} 0 & \mathrm{I}_\nu \\ -\mathrm{I}_\nu & 0 \end{pmatrix}. \tag{20}$$

On a alors

$$\mathrm{Sp}_{2\nu}(\mathbf{K}) = \{\mathrm{U} \in \mathrm{GL}_{2\nu}(\mathbf{K}) \mid {}^t\mathrm{U}\mathrm{J}_{2\nu}\mathrm{U} = \mathrm{J}_{2\nu}\}. \tag{21}$$

Décomposant la matrice par blocs,

$$\mathrm{U} = \begin{pmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{pmatrix},$$

il vient $\mathrm{U} \in \mathrm{Sp}_{2\nu}(\mathbf{K})$ si et seulement si

$${}^t\mathrm{AC} = {}^t\mathrm{CA}, \quad {}^t\mathrm{BD} = {}^t\mathrm{DB}, \quad {}^t\mathrm{AD} - {}^t\mathrm{CB} = \mathrm{I}_\nu. \tag{22}$$

En particulier, on a $\mathrm{Sp}_2(\mathbf{K}) = \mathrm{SL}_2(\mathbf{K})$. On a en fait l'inclusion

$$\mathrm{Sp}_{2\nu}(\mathbf{K}) \subseteq \mathrm{SL}_{2\nu}(\mathbf{K})$$

pour tout $\nu \geqslant 1$, mais elle n'est pas facile à démontrer (cor. 7.2 et cor. III.4.8).

5. Théorème de Witt

Le théorème de Witt est un théorème de prolongement des isométries. Il est essentiel dans la théorie.

***Théorème 5.1* (Witt)**. — *Soient* (V, b) *et* (V', b') *des espaces isométriques non dégénérés. Soit* W *un sous-espace de* V *et soit* $u : \mathrm{W} \to \mathrm{V}'$ *une isométrie. Il existe une isométrie* $v : \mathrm{V} \to \mathrm{V}'$ *telle que* $v|_{\mathrm{W}} = u$.

Commençons par le cas simple où W est de dimension 1, engendré par un vecteur x. Le vecteur $y := u(x)$ vérifie $b(x,x) = b(y,y)$ et il s'agit de trouver une isométrie v telle que $v(x) = y$. Pour résoudre ce problème, nous aurons besoin de la construction suivante.

***Exemple 5.2* (Réflexions).** — Si $b(x,x) \neq 0$ (en particulier, b est symétrique), on a $\mathrm{V} = x^\perp \oplus \mathbf{K}x$ et la *réflexion* (ou symétrie hyperplane) par rapport à $x^\perp$ est l'endomorphisme s_x de V de valeurs propres 1 et -1 sur cette décomposition. Il s'agit manifestement d'une isométrie, donnée explicitement par la formule

$$s_x(y) = y - 2\frac{b(x,y)}{b(x,x)}x.$$

Si $b(x,x) = b(y,y) \neq 0$ et qu'on note la forme quadratique associée f, le théorème de WItt résulte alors du lemme suivant.

Lemme 5.3. — *Si $f(x) = f(y) \neq 0$, il existe une isométrie v telle que $v(x) = y$.*

Démonstration. — De $f(x+y) + f(x-y) = 2(f(x) + f(y)) = 4f(x)$, on déduit que l'un au moins des vecteurs $x+y$ et $x-y$ est non isotrope, disons par exemple $x+y$. Alors la réflexion par rapport à $(x+y)^\perp$ envoie x sur $-y$, et on la compose par $-\mathrm{Id}$. □

Le deuxième cas qu'on va traiter est celui d'un espace W totalement isotrope (c'est-à-dire tel que $b|_{\mathrm{W}} \equiv 0$). On construit pour cela un espace hyperbolique contenant W.

Lemme 5.4. — *Soit* V *un espace vectoriel muni d'une forme bilinéaire symétrique ou alternée non dégénérée, soit* W *un sous-espace vectoriel totalement isotrope de* V *et soit* $(e_1, \dots, e_r)$ *une base de* W. *Il existe* $(e'_1, \dots, e'_r)$ *dans* V *tels que*

- *chaque* $\mathrm{P}_i := \langle e_i, e'_i \rangle$ *est un plan hyperbolique ;*
- $\mathrm{P}_1, \dots, \mathrm{P}_r$ *sont en somme directe orthogonale.*

En outre, toute isométrie $\mathrm{W} \to \mathrm{V}'$ *se prolonge en une isométrie* $\mathrm{P}_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \mathrm{P}_r \to \mathrm{V}'$.

Démonstration. — Le cas $r = 1$ est le lemme 4.8. On raisonne ensuite par récurrence sur r. Posons $\mathrm{W}_1 = \langle e_2, \dots, e_r \rangle$.

L'hyperplan $e_1^\perp$ contient e_1 et W_1 ; soit V_1 un supplémentaire de e_1 dans $e_1^\perp$ contenant W_1. La restriction de b à V_1 est non dégénérée ; on applique l'hypothèse de récurrence à son sous-espace totalement isotrope W_1 et il existe donc des plans hyperboliques $\mathrm{P}_2, \dots, \mathrm{P}_r$ dans V_1 avec les propriétés du lemme. La somme directe $\mathrm{P}_2 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \mathrm{P}_r$ est alors orthogonale à e_1 et la restriction de b y est non dégénérée. Son orthogonal contient donc e_1 et la restriction de b y est aussi non dégénérée. On peut y appliquer le lemme 4.8 au vecteur e_1 : il existe e'_1 orthogonal à $\mathrm{P}_2 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} \mathrm{P}_r$ et formant avec e_1 un plan hyperbolique.

L'extension d'une isométrie $u : \mathrm{W} \to \mathrm{V}'$ se montre en étendant $\mathrm{im}(u)$ dans V' de la même manière que W : comme b est non dégénérée, u est injective et $u(\mathrm{W}) = \langle u(e_1), \dots, u(e_r) \rangle$ est un sous-espace totalement isotrope de V' ; on construit alors des plans hyperboliques $\langle u(e_i), e''_i \rangle$ et on prolonge u en envoyant chaque e'_i sur e''_i. □

Démonstration du th. 5.1. — On commence par étendre u à un sous-espace $\bar{\mathrm{W}}$ de V contenant W sur laquelle la forme b est non dégénérée.

Soit W' un supplémentaire de $W \cap W^\perp$ dans W. La restriction de b à W' est non dégénérée, donc aussi la restriction de b à $W'^\perp$. Ce dernier espace contient le sous-espace vectoriel totalement isotrope $W \cap W^\perp$. Par le lemme 5.4, on peut donc étendre $u|_{W'^\perp}$ à un sous-espace hyperbolique H de $W'^\perp$ (sur laquelle b est non dégénérée). On a ainsi étendu u en $\bar{u}$ au sous-espace $\bar{W} := H \overset{\perp}{\oplus} W'$, sur lequel b est non dégénérée. Remarquons que la restriction de b' à $u(\bar{W})$ est aussi non dégénérée.

Si b est alternée, les restrictions (non dégénérées) de b à $\bar{W}^\perp$ et de b' à $\bar{u}(\bar{W})^\perp$ sont équivalentes (à isométrie près, il n'y a qu'une seule forme alternée non dégénérée sur un espace vectoriel de dimension paire). On a ainsi étendu u à $\bar{W} \overset{\perp}{\oplus} \bar{W}^\perp = V$.

Supposons donc b symétrique. De plus, comme (V, b) et (V', b') sont isométriques, on peut les supposer égaux. Le cas $\dim(\bar{W}) = 1$ est alors fourni par le lemme 5.3.

On raisonne alors par récurrence sur $\dim(\bar{W})$. Si $\dim(\bar{W}) \geqslant 2$, on écrit $\bar{W} = W_1 \overset{\perp}{\oplus} W_2$, avec W_1 et W_2 non nuls, où la restriction de b à W_1 et à W_2 est non dégénérée (*cf.* § 4.2). Par l'hypothèse de récurrence, $u|_{W_1}$ se prolonge en une isométrie v_1 de V, qui induit par restriction une isométrie $v_1|_{W_1^\perp} : W_1^\perp \xrightarrow{\sim} u(W_1)^\perp$. On applique alors à nouveau l'hypothèse de récurrence à $u|_{W_2} : W_2 \to u(W_1)^\perp$ pour le prolonger en une isométrie $v_2 : W_1^\perp \xrightarrow{\sim} u(W_1)^\perp$. On prend alors $v = u|_{W_1} \oplus v_2 : W_1 \oplus W_1^\perp \to u(W_1) \oplus u(W_1)^\perp$. □

Corollaire 5.5. — *1° Si* W *et* W' *sont des sous-espaces isométriques de* V*, les sous-espaces* $W^\perp$ *et* $W'^\perp$ *sont isométriques.*

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

3° Tous les sous-espaces hyperboliques maximaux ont même dimension 2ν*.*

4° Si H *est un sous-espace hyperbolique maximal, on peut écrire* $V = H \overset{\perp}{\oplus} W$*, avec* W *sans vecteur isotrope non nul (*W *est anisotrope).*

On notera qu'au vu de 3°, on a $\nu \leqslant \frac{1}{2}\dim(V)$.

D'autre part, dans le cas alterné, le corollaire résulte de la classification des formes alternées non dégénéréees ; on a $\nu = \frac{1}{2}\dim(V)$ et l'espace anisotrope W du 4° est nul.

Démonstration. — Le 1° résulte du théorème de Witt.

On prouve le 2°. Si W et W' sont totalement isotropes et $\dim(W) \leqslant \dim(W')$, n'importe quelle application linéaire injective $u : W \to W'$ est une isométrie, donc s'étend en une isométrie v de V. Alors W est contenu dans $v^{-1}(W')$, qui est aussi totalement isotrope. Il en résulte que tous les sous-espaces totalement isotropes maximaux ont même dimension.

Tout sous-espace hyperbolique contient un sous-espace totalement isotrope de dimension moitié, et inversement, comme on l'a vu dans le lemme 5.4, tout sous-espace totalement isotrope est contenu dans un sous-espace hyperbolique de dimension double. Le 3° résulte donc du 2°.

Le 4° a déjà été vu dans le § 4.3. □

Exemples 5.6. — 1° Si **K** est un corps quadratiquement clos, une forme quadratique non dégénérée de dimension n est d'indice $\lfloor n/2 \rfloor$ (ex. 4.9.1°).

2° Dans le cas d'une forme quadratique non dégénérée sur $\mathbf{R}^n$, de signature $(s, t = n-s)$, on voit que l'indice est $\inf(s,t)$ (ex. 4.9.2°), donc la signature est bien un invariant de la forme quadratique.

3° Dans le cas d'un corps fini $\mathbf{F}_q$ (de caractéristique différente de 2), rappelons que les formes quadratiques sont de deux types :

$$\langle 1, \dots, 1\rangle \quad \text{et} \quad \langle 1, \dots, 1, \alpha\rangle,$$

avec $\alpha \notin \mathbf{F}_q^2$. D'autre part, toute forme quadratique sur un espace de dimension $\geqslant 3$ admet un vecteur isotrope non nul (cela résulte de la démonstration de la prop. 4.4). L'espace F du cor. 5.5 est donc de dimension $\leqslant 2$.

En dimension 2,

– la forme $\langle 1, -1\rangle$ a un vecteur isotrope non nul, $(1,1)$;

– la forme $\langle 1, -\alpha\rangle$ n'a pas de vecteur isotrope non nul.

Si la dimension de l'espace est $2m+1$, impaire, W est de dimension 1 et l'indice de la forme quadratique est m. On rappelle qu'on a un seul groupe orthogonal, noté $\mathrm{O}_{2m+1}(\mathbf{F}_q)$.

Si la dimension de l'espace est $2m$, paire, soit $\mathrm{W} = 0$ et l'indice de la forme quadratique est m, soit W est de type $\langle 1, -\alpha\rangle$ et l'indice est $m-1$. On a déjà noté les groupes orthogonaux correspondants $\mathrm{O}^+_{2m}(\mathbf{F}_q)$ et $\mathrm{O}^-_{2m}(\mathbf{F}_q)$, respectivement (*cf.* note 11 ; la forme quadratique $\langle 1, -1, \dots, 1, -1\rangle$ étant visiblement d'indice m, on voit que le discriminant associé est bien $(-1)^m$).

Exercice 5.7. — Soit q une puissance de nombre premier impair et soit f une forme quadratique non dégénérée sur $\mathbf{F}_q^n$. Calculer le cardinal de l'ensemble

$$\{x \in \mathbf{F}_q^n \mid f(x) = 1\}$$

(*Indication :* on distinguera plusieurs cas selon le discriminant de f et la parité de n).

Exercice 5.8. — On considère sur $\mathbf{R}^{2n}$ le forme quadratique

$$f(x_1, \dots, x_{2n}) = x_1 x_{n+1} + \cdots + x_n x_{2n}.$$

Pour toute partie J de $\{1, \dots, 2n\}$ de cardinal n, on note V^{J} le sous-espace vectoriel de $\mathbf{R}^{2n}$ défini par les équations $x_j = 0$ pour tout $j \in \mathrm{J}$.

a) Déterminer le rang et la signature de f.

b) Soit $a : \mathbf{R}^n \to \mathbf{R}^n$ une application linéaire. À quelle condition sur la matrice de a le graphe V_a de a (vu comme un sous-espace vectoriel de $\mathbf{R}^n \times \mathbf{R}^n = \mathbf{R}^{2n}$) est-il totalement isotrope pour f ? Montrer qu'on obtient ainsi tous les espaces V totalement isotropes maximaux (c'est-à-dire de dimension n) tels que $\mathrm{V} \cap \mathrm{V}^{\{1,\dots,n\}} = \{0\}$.

c) Si $a, b : \mathbf{R}^n \to \mathbf{R}^n$ sont des applications linéaires, peut-on dire de la parité de la dimension de $\mathrm{V}_a \cap \mathrm{V}_b$?

d) Pour toute partie J de $\{1, \dots, 2n\}$ de cardinal n, et toute application linéaire $a : \mathbf{R}^n \to \mathbf{R}^n$, définir comme dans b) des sous-espaces $\mathrm{V}^{\mathrm{J}}_a \subseteq \mathbf{R}^{2n}$ totalement isotropes maximaux tels que $\mathrm{V}^{\mathrm{J}}_a \cap \mathrm{V}^{\mathrm{J}} = \{0\}$.

e) Pour toutes parties J et K de $\{1, \dots, 2n\}$ de cardinal n, montrer que

– soit $\mathrm{card}(\mathrm{J} \cap \mathrm{K}) \not\equiv n \pmod 2$ et, pour tout a et b, on a $\mathrm{V}^{\mathrm{J}}_a \neq \mathrm{V}^{\mathrm{K}}_b$;

– soit $\mathrm{card}(\mathrm{J} \cap \mathrm{K}) \equiv n \pmod 2$ et « la plupart » des $\mathrm{V}^{\mathrm{J}}_a$ sont aussi des $\mathrm{V}^{\mathrm{K}}_b$.

6. Groupe de Witt

Soit **K** un corps. On considère l'ensemble des classes d'équivalence (ou d'isométrie) de **K**-espaces vectoriels munis d'une forme quadratique non dégénérée. Cette ensemble est muni d'une addition (commutative et associative) correspondant à la somme directe orthogonale et l'élément neutre correspond à la forme quadratique nulle sur l'espace vectoriel nul. Le 1° du cor. 5.5 dit exactement que l'addition est simplifiable :

$$[f]+[g]=[f']+[g]\Longrightarrow[f]=[f'].$$

C'est un semi-groupe mais ce n'est pas un groupe, puisque $\dim([f]+[g])=\dim([f])+\dim([g])$, donc $[f]+[g]$ n'est nul que si $[f]$ et $[g]$ le sont. De la même façon qu'on passe du semi-groupe simplifiant **N** au groupe **Z**, on associe à cette situation le *groupe de Grothendieck-Witt* $\mathrm{GW}(\mathbf{K})$ de **K** : c'est l'ensemble des couples $([f_1],[f_2])$ (auquel il faut penser comme la différence formelle $[f_1]-[f_2]$) modulo la relation déquivalence

$$([f_1],[f_2])\sim([g_1],[g_2])\Longrightarrow[f_1]+[g_2]=[f_2]+[g_1].$$

On vérifie que $\mathrm{GW}(\mathbf{K})$ est bien un groupe, muni de morphismes de groupes surjectifs

$$\dim:\mathrm{GW}(\mathbf{K})\twoheadrightarrow\mathbf{Z}\qquad\mathrm{disc}:\mathrm{GW}(\mathbf{K})\twoheadrightarrow\mathbf{K}^\times/\mathbf{K}^{\times 2}.$$

Notons par ailleurs la relation $[f]+[-f]=\dim(f)[\mathrm{P}]$, où $-f$ est la forme quadratique opposée à f (sur le même espace vectoriel) et P est un plan hyperbolique.

On définit le *groupe de Witt* $\mathrm{W}(\mathbf{K})$ de **K** comme le quotient de $\mathrm{GW}(\mathbf{K})$ par le sous-groupe $\mathbf{Z}[\mathrm{P}]$ engendré par [P]. C'est encore un groupe abélien dans lequel l'opposé de $[f]$ est $[-f]$. En utilisant l'écriture diagonale des formes quadratiques, on a les relations suivantes dans $\mathrm{W}(\mathbf{K})$:

$$\begin{aligned}
[\langle\alpha_{\sigma(1)},\dots,\alpha_{\sigma(m)}\rangle] &= [\langle\alpha_1,\dots,\alpha_m\rangle]\quad\text{pour tout }\sigma\in\mathfrak{S}_m,\\
[\langle\alpha_1,\dots,\alpha_m\rangle]+[\langle\beta_1,\dots,\beta_n\rangle] &= [\langle\alpha_1,\dots,\alpha_m,\beta_1,\dots,\beta_n\rangle],\\
-[\langle\alpha_1,\dots,\alpha_m\rangle] &= [\langle-\alpha_1,\dots,-\alpha_m\rangle],\\
[\langle\alpha,-\alpha\rangle] &= 0.
\end{aligned}$$

On a un morphisme

$$\overline{\dim}:\mathrm{W}(\mathbf{K})\twoheadrightarrow\mathbf{Z}/2\mathbf{Z}$$

mais le discriminant ne passe pas au quotient puisque $\mathrm{disc}(\mathrm{P})=-1$.

Le 1° du cor. 5.5 dit que les éléments de $\mathrm{W}(\mathbf{K})$ peuvent être représentés par des formes quadratiques anisotropes. On a plus précisément

$$\mathrm{W}(\mathbf{K})=\{\text{classes d'isométrie de formes quadratiques anisotropes}\}.$$

En effet, si des formes quadratiques anisotropes f_1 et f_2 ont même image dans $\mathrm{W}(\mathbf{K})$, il existe des entiers positifs n_1 et n_2 tels que $f_1\overset{\perp}{\oplus}\mathrm{P}^{n_1}\sim f_2\overset{\perp}{\oplus}\mathrm{P}^{n_2}$. Le cor. 5.5 entraîne que f_1 et f_2 sont isométriques.

Exemples 6.1. — 1° Si **K** est un corps quadratiquement clos, $\overline{\dim}:\mathrm{W}(\mathbf{K})\twoheadrightarrow\mathbf{Z}/2\mathbf{Z}$ est un isomorphisme (ex. 5.6.1°).

2° Si -1 est un carré dans **K**, on a $[f]=[-f]$ pour tout forme quadratique f, donc tout élément de $\mathrm{W}(\mathbf{K})$ est d'ordre 2.

3° Toute forme quadratique réelle anisotrope est isométrique à $\pm\langle 1,\dots,1\rangle$. On a donc $\mathrm{W}(\mathbf{R}) \simeq \mathbf{Z}$. On peut en déduire un isomorphisme $\dim \oplus s : \mathrm{GW}(\mathbf{R}) \xrightarrow{\sim} \mathbf{Z}\oplus\mathbf{Z}$, où s est le morphisme signature, défini par $s([\langle 1\rangle]) = 1$.

4° Dans le cas d'un corps fini $\mathbf{F}_q$ (de caractéristique différente de 2), on a

$$\mathrm{W}(\mathbf{K}) \simeq \begin{cases} \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z} & \text{si } -1 \in \mathbf{K}^2, \\ \mathbf{Z}/4\mathbf{Z} & \text{si } -1 \notin \mathbf{K}^2. \end{cases}$$

En effet, si on note comme d'habitude α un élément de $\mathbf{F}_q - \mathbf{F}_q^2$, il y a 4 (classes d'isométrie de) formes quadratiques anisotropes : 0, $\langle 1\rangle$, $\langle\alpha\rangle$ et $\langle 1,-\alpha\rangle$. Le groupe $\mathrm{W}(\mathbf{F}_q)$ a donc 4 éléments, et il est isomorphe soit à $\mathbf{Z}/4\mathbf{Z}$, soit à $(\mathbf{Z}/2\mathbf{Z})^2$. Si -1 est un carré dans $\mathbf{F}_q$, on est dans le second cas par 2°. Dans le cas contraire, on peut prendre $\alpha = -1$ et $[\langle 1\rangle] + [\langle 1\rangle] = [\langle 1,1\rangle] = [\langle 1,-\alpha\rangle]$; on est donc dans le premier cas : $\mathrm{W}(\mathbf{F}_q)$ est isomorphe à $\mathbf{Z}/4\mathbf{Z}$, avec comme générateur $[\langle 1\rangle]$.

5° Le groupe $\mathrm{W}(\mathbf{Q})$ est connu. Il contient le groupe cyclique $\mathbf{Z}$ engendré par $1_{\mathrm{W}(\mathbf{Q})}$, et le quotient est $\bigoplus_{p \text{ premier}} \mathrm{W}(\mathbf{F}_p)$.

***Remarque 6.2* (Idéal fondamental et conjecture de Milnor).** — On peut aussi mettre sur $\mathrm{W}(\mathbf{K})$ une structure d'anneau en définissant une forme quadratique sur le produit tensoriel (exerc. III.1.8) de deux espaces munis d'une forme quadratique. Cela revient à poser

$$[\langle\alpha_1,\dots,\alpha_m\rangle]\cdot[\langle\beta_1,\dots,\beta_n\rangle] = [\langle\alpha_i\beta_j, 1\leqslant i\leqslant m, 1\leqslant j\leqslant n\rangle].$$

Le morphisme $\overline{\dim} : \mathrm{W}(\mathbf{K}) \twoheadrightarrow \mathbf{Z}/2\mathbf{Z}$ est alors un morphisme d'anneaux et on appelle son noyau $\mathrm{I}(\mathbf{K})$ l'*idéal fondamental* de $\mathrm{W}(\mathbf{K})$. Un élément de $\mathrm{I}(\mathbf{K})$ est donc représenté par une forme quadratique sur un espace vectoriel de dimension paire. Le morphisme *discriminant signé* est défini ainsi :

$$\begin{array}{rcl} \mathrm{disc}_s : \mathrm{I}(\mathbf{K}) & \longrightarrow & \mathbf{K}^\times/\mathbf{K}^{\times 2} \\ [f] & \longmapsto & (-1)^{\dim(f)/2}\,\mathrm{disc}(f). \end{array}$$

On montre qu'il induit un isomorphisme $\mathrm{I}(\mathbf{K})/\mathrm{I}(\mathbf{K})^2 \xrightarrow{\sim} \mathbf{K}^\times/\mathbf{K}^{\times 2}$.

La conjecture de Milnor, montrée par Voevodsky en 1996 (démonstration pour laquelle il a obtenu la médaille Fields en 2002) identifie tous les quotients successifs $\mathrm{I}(\mathbf{K})^r/\mathrm{I}(\mathbf{K})^{r+1}$ en termes de groupes dits de K-théorie de Milnor.

7. Groupe symplectique

Dans cette section, le $\mathbf{K}$-espace vectoriel V, de dimension finie paire 2ν, est muni d'une forme alternée non dégénérée (on dit aussi *forme symplectique*) b et on étudie le groupe symplectique $\mathrm{Sp}(\mathrm{V}, b)$.

On rappelle que V est somme directe orthogonale de ν plans hyperboliques.

7.1. Générateurs. — Soit une transvection $\tau(x) = x + \ell(x)a$, où $\ell \in \mathrm{V}^*$ et $a \in \ker(\ell)$ (*cf.* § 2.4). On a

$$\begin{array}{rcl} b(\tau(x),\tau(y)) & = & b(x+\ell(x)a, y+\ell(y)a) \\ & = & b(x,y) + \ell(y)b(x,a) + \ell(x)b(a,y). \end{array}$$

Si on prend pour ℓ une forme linéaire $\lambda b(a,\cdot)$, la transvection τ est symplectique ; toutes les transvections de la forme

$$\tau(x) = x + \lambda b(a,x)a, \quad a \in \mathrm{V}, \lambda \in \mathbf{K} \tag{23}$$

sont donc symplectiques.

Remarquons que si $\dim(\mathrm{V}) = 2$, dans une base hyperbolique de V, on a $b((x_1,x_2),(y_1,y_2)) = x_1y_2 - x_2y_1$. Un morphisme u de V multiplie b par $\det(u)$, d'où il résulte (comme on peut aussi le voir sur les équations (22))

$$\mathrm{Sp}_2(\mathbf{K}) = \mathrm{SL}_2(\mathbf{K}). \tag{24}$$

En dimension 2, toutes les transvections sont symplectiques.

Théorème 7.1. — *Les transvections symplectiques engendrent* $\mathrm{Sp}(\mathrm{V})$.

Corollaire 7.2. — *Le groupe symplectique* $\mathrm{Sp}(\mathrm{V})$ *est un sous-groupe de* $\mathrm{SL}(\mathrm{V})$.

On verra dans le cor. III.4.8 une autre démonstration de ce corollaire.

Démonstration. — Les transvections ont déterminant 1. □

Démonstration du théorème. — La démonstration se fait par récurrence sur la dimension, en commencant par la dimension 0 (!).

Si $\mathrm{V} \neq 0$, il contient un plan hyperbolique $\mathrm{P} = \langle x_1, x_2\rangle$. Soit $u \in \mathrm{Sp}(\mathrm{V})$. Alors $\mathrm{Q} := u(\mathrm{P}) = \langle u(x_1), u(x_2)\rangle$ est aussi un plan hyperbolique. Si on admet (provisoirement) le lemme ci-dessous, il existe un produit v de transpositions symplectiques tel que $v(x_1) = u(x_1)$ et $v(x_2) = u(x_2)$. La composée $v^{-1}u$ est alors l'identité sur P, donc laisse stable son orthogonal $\mathrm{P}^\perp$. Sa restriction à $\mathrm{P}^\perp$ en est un automorphisme symplectique, qui est donc, par hypothèse de récurrence, produit de transvections symplectiques de $\mathrm{P}^\perp$. Prolongées par l'identité sur P, ces transvections symplectiques deviennent des transvections symplectiques de V, dont le produit est $v^{-1}u$. Ainsi, u est bien produit de transvections symplectiques de V. □

Lemme 7.3. — *Si* $\mathrm{P} = \langle x_1, x_2\rangle$ *et* $\mathrm{Q} = \langle y_1, y_2\rangle$ *sont des plans hyperboliques (avec* $b(x_1,x_2) = b(y_1,y_2) = 1$*), il existe un produit d'au plus 4 transvections symplectiques envoyant* x_1 *sur* y_1 *et* x_2 *sur* y_2.

Démonstration. — Observons que si $b(x_1,y_1) \neq 0$, on peut envoyer x_1 sur y_1 par la transvection symplectique

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

Dans le cas général, en passant par un z tel que $b(x_1,z) \neq 0$ et $b(z,y_1) \neq 0$ (qui existe parce que V n'est pas réunion des hyperplans $x_1^\perp$ et $y_1^\perp$!), on voit qu'un produit de 2 transvections symplectiques envoie x_1 sur y_1.

On est ainsi ramené au cas $x_1 = y_1$ et on veut donc envoyer x_2 sur y_2 en laissant x_1 fixe. À nouveau, la situation est plus simple si $b(x_2,y_2) \neq 0$: la transvection

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

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

On déduit d'ailleurs de ce lemme que toute isométrie d'un espace symplectique de dimension 2ν est produit d'au plus 4ν transvections symplectiques.

Remarque 7.4. — On peut montrer [14] que le groupe $\mathrm{Sp}_{2\nu}(\mathbf{K})$ est engendré par les matrices par blocs (*cf.* (22))

$$\begin{pmatrix} \mathrm{I}_\nu & \alpha(\mathrm{E}_{ij} + \mathrm{E}_{ji}) \\ 0 & \mathrm{I}_\nu \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \mathrm{I}_\nu + \alpha\mathrm{E}_{ij} & 0 \\ 0 & \mathrm{I}_\nu - \alpha\mathrm{E}_{ji} \end{pmatrix}, \quad \text{pour } 1 \leqslant i, j \leqslant \nu,\ \alpha \in \mathbf{K},$$

et leur transposée [15].

Exercice 7.5. — Montrer que $\mathrm{Sp}_{2\nu}(\mathbf{R})$ est connexe.

Exercice 7.6. — Montrer que $\mathrm{Sp}_{2\nu}(\mathbf{Q})$ est dense dans $\mathrm{Sp}_{2\nu}(\mathbf{R})$.

7.2. Centre. — Soit u une isométrie commutant avec toute isométrie. Elle commute en particulier avec toutes les transvections symplectiques, de sorte que, pour tout $a \in \mathrm{V}$ et tout $x \in \mathrm{V}$, on a

$$u(x) + b(a, u(x))\, a = \tau(u(x)) = u(\tau(x)) = u(x) + b(a, x)\, u(a).$$

Étant donné $a \neq 0$, on peut choisir x de façon que $b(a, x) \neq 0$ et on en déduit que $u(a)$ est proportionnel à a pour tout $a \in \mathrm{V}$. L'automorphisme u est alors une homothétie (*cf.* note 2), de rapport λ. Comme il est symplectique, on a $\lambda = \pm 1$.

Le centre de $\mathrm{Sp}_{2\nu}(\mathbf{K})$ est donc réduit à $\{\pm \mathrm{I}_{2\nu}\}$. On considère le groupe projectif associé, à savoir le quotient

$$\mathrm{PSp}_{2\nu}(\mathbf{K}) = \mathrm{Sp}_{2\nu}(\mathbf{K}) / \{\pm \mathrm{I}_{2\nu}\}.$$

C'est un sous-groupe de $\mathrm{PSL}(2\nu, \mathbf{K})$; il agit donc fidèlement sur l'espace projectif $\mathbf{P}^{2\nu-1}(\mathbf{K})$.

Exemples 7.7. — 1° Les groupes $\mathrm{Sp}_{2\nu}(\mathbf{R})$ et $\mathrm{PSp}_{2\nu}(\mathbf{R})$) sont des *variétés différentiables* de dimension $\nu(2\nu + 1)$.

2° Les groupes $\mathrm{Sp}_{2\nu}(\mathbf{C})$ et $\mathrm{PSp}_{2\nu}(\mathbf{C})$) sont des *variétés complexes* de dimension $\nu(2\nu + 1)$.

---

14. O'Meara, O. T., *Symplectic Groups*, Mathematical Surveys **16**, American Mathematical Society, Providence, R.I., 1978.

15. Le groupe $\mathrm{Sp}_{2\nu}(\mathbf{Z})$, qu'on peut définir comme le sous-groupe de $\mathrm{Sp}_{2\nu}(\mathbf{Q})$ formé des matrices à coefficients entiers, est engendré, pour $\nu \geqslant 2$, par quatre matrices explicites (Hua, L. K., Reiner, I., On the generators of the symplectic modular group, *Trans. Amer. Math. Soc.* **65** (1949), 415–426).

7.3. Cardinal des groupes symplectiques finis.— On suppose q impair (*cf.* rem. 7.11 pour le cas de la caractéristique 2). Comme pour les groupes linéaires, il est facile de dénombrer les éléments de $\mathrm{Sp}_{2\nu}(\mathbf{F}_q)$: il suffit de compter le nombre de bases hyperboliques. On obtient

$$\begin{aligned}
|\mathrm{Sp}_{2\nu}(\mathbf{F}_q)| &= (q^{2\nu}-1)\frac{(q^{2\nu}-q^{2\nu-1})}{q-1}(q^{2\nu-2}-1)\frac{(q^{2\nu-2}-q^{2\nu-3})}{q-1}\cdots(q^2-1)\frac{(q^2-q)}{q-1}\\
&= q^{2\nu-1+2\nu-3+\cdots+1}(q^{2\nu}-1)(q^{2\nu-2}-1)\cdots(q^2-1)\\
&= q^{\nu^2}(q^{2\nu}-1)(q^{2\nu-2}-1)\cdots(q^2-1), \qquad (25)\\
|\mathrm{PSp}_{2\nu}(\mathbf{F}_q)| &= \frac{1}{2}|\mathrm{PSp}_{2\nu}(\mathbf{F}_q)|\\
&= \frac{1}{2}q^{\nu^2}(q^{2\nu}-1)(q^{2\nu-2}-1)\cdots(q^2-1).
\end{aligned}$$

On rappelle (*cf.* (24)) que le groupe $\mathrm{Sp}_2(\mathbf{F}_q)$ est le même que le groupe $\mathrm{SL}_2(\mathbf{F}_q)$.

***Exercice 7.8* (p-sous-groupes de Sylow de $\mathrm{Sp}_{2\nu}(\mathbf{F}_q)$).** — L'espace vectoriel $\mathbf{F}_q^{2\nu}$ est muni de la forme symplectique de matrice $J_{2\nu} = \left(\begin{smallmatrix} 0 & I_\nu \\ -I_\nu & 0 \end{smallmatrix}\right)$ dans la base canonique (*cf.* (20)).

Soit $W \subseteq \mathbf{F}_q^{2\nu}$ le sous-espace vectoriel engendré par les ν premiers vecteurs de la base canonique. On considère le sous-groupe

$$H := \{u \in \mathrm{Sp}_{2\nu}(\mathbf{F}_q) \mid u(W) = W\}.$$

a) Montrer que la restriction à W induit un morphisme surjectif $\phi : H \twoheadrightarrow \mathrm{GL}(W) = \mathrm{GL}(\nu, \mathbf{F}_q)$ (*Indication :* on pourra utiliser les relations (22)).
b) Montrer que le noyau de ϕ est isomorphe au groupe additif des matrices symétriques $\nu \times \nu$ (*Indication :* on pourra utiliser les relations (22)).
c) En déduire que $S := \phi^{-1}(T_\nu(\mathbf{F}_q))$ est un p-sous-groupe de Sylow de $\mathrm{Sp}_{2\nu}(\mathbf{F}_q)$ (*cf.* exerc. I.2.13 pour la définition du p-sous-groupe de Sylow $T_\nu(\mathbf{F}_q)$ de $\mathrm{GL}_\nu(\mathbf{F}_q)$). Donner une description matricielle de S en utilisant les relations (22).

7.4. Groupe dérivé. — On rappelle que le groupe dérivé D(G) d'un groupe G est le sous-groupe de G engendré par les commutateurs de G.

Théorème 7.9. — *On suppose* $\mathrm{car}(\mathbf{K}) \neq 2$ *et* $\nu \geqslant 2$. *On a* $\mathrm{D}(\mathrm{Sp}_{2\nu}(\mathbf{K})) = \mathrm{Sp}_{2\nu}(\mathbf{K})$.

Démonstration. — Par le th. 7.1, il suffit de montrer que toute transvection symplectique peut s'écrire comme un commutateur. Soit $\tau(x) = x + \lambda b(e,x)e$, avec $e \in V$ et $\lambda \in \mathbf{K}$, une telle transvection. Le vecteur e est contenu dans un plan hyperbolique $P = \langle e, f\rangle$ (lemme 4.8) et, comme $\nu \geqslant 2$, on peut écrire $V = P \overset{\perp}{\oplus} Q \overset{\perp}{\oplus} W$, où $Q = \langle e', f'\rangle$ est aussi un plan hyperbolique. Dans une base de V obtenue en complétant (e, e', f, f') par une base de W, la transvection τ a pour matrice par blocs $\begin{pmatrix} N(\lambda) & 0 \\ 0 & I_{2\nu-4} \end{pmatrix}$, où

$$N(\lambda) := \begin{pmatrix} 1 & 0 & \lambda & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Il suffit donc d'exprimer la matrice $N(\tau)$ comme commutateurs d'éléments de $\mathrm{Sp}_4(\mathbf{K})$. D'après (22), les matrices

$$U_1 = \begin{pmatrix} A_1 & 0 \\ 0 & {}^tA_1^{-1} \end{pmatrix}, \quad U_2 = \begin{pmatrix} I_2 & A_2 \\ 0 & I_2 \end{pmatrix}$$

sont symplectiques, pourvu que A_2 soit symétrique. Si on prend

$$A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \frac{1}{2}\lambda \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

on vérifie l'égalité $U_1U_2U_1^{-1}U_2^{-1} = N(\lambda)$, ce qui termine la démonstration. □

Simplicité. — La simplicité des groupes projectifs symplectiques finis fournit une nouvelle liste infinie de groupes finis simples.

Théorème 7.10. — *On suppose* $\mathrm{car}(\mathbf{K}) \neq 2$ *et* $\nu \geqslant 2$. *Le groupe* $\mathrm{PSp}_{2\nu}(\mathbf{K})$ *est simple.*

Démonstration. — Ce théorème se déduit du th. 7.9, comme dans le cas des groupes PSL, par la méthode d'Iwasawa, en considérant l'action fidèle et transitive du groupe sur l'espace projectif $X := \mathbf{P}^{2\nu-1}(\mathbf{K})$. Nous disposons en effet pour chaque droite $x \in X$ du groupe abélien (isomorphe à $\mathbf{K}$) des transvections symplectiques de droite x, et la seule hypothèse restant à vérifier pour appliquer le th. 2.16 est que l'action est primitive, c'est-à-dire que les stabilisateurs sont des sous-groupes maximaux.

L'action de $\mathrm{Sp}_{2\nu}(\mathbf{K})$ sur X est transitive : étant deux droites vectorielles de V, il existe par le théorème de Witt une isométrie qui envoie l'une sur l'autre (*cf.* aussi la preuve du lemme 7.3). Mais cette action n'est pas 2-transitive : l'action diagonale de $G := \mathrm{Sp}_{2\nu}(\mathbf{K})$ sur $\{(x, y) \in X \times X \mid x \neq y\}$ a deux orbites :

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

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

En effet, la restriction de la forme symplectique b à un plan est soit hyperbolique, soit nulle. Par le théorème de Witt, étant donnés deux plans dans V du même type, il existe une isométrie de V envoyant l'un sur l'autre.

Pour montrer que l'action est primitive, on doit donc revenir à la définition et montrer que le stabilisateur G_x d'un point $x \in X$ est maximal. Supposons donc $G_x < H \leq G$. On doit montrer $H = G$.

On rappelle que $Hx := \{hx \mid h \in H\} \subseteq X$ est l'orbite de x sous l'action induite de H ; comme $G_x \neq H$, elle n'est pas réduite à $\{x\}$. Regardons les sous-ensembles gHx de X lorsque g décrit G (parmi eux, on trouve l'orbite Hx).

Tout d'abord, leur réunion $\bigcup_{g\in G} gHx$ contient $\bigcup_{g\in G} gx$, qui n'est autre que l'orbite de x ; c'est donc bien X tout entier puisque l'action de G sur X est transitive.

Ensuite, si $gHx \cap g'Hx \neq \emptyset$, il existe $h, h' \in H$ tels que $ghx = g'h'x$, donc $h^{-1}g^{-1}g'h' \in G_x$ donc $g^{-1}g' \in H$, ce qui implique $gHx = g'Hx$. Ainsi les $(gHx)_{g\in G}$ distincts réalisent une partition de X.

Posons

$$\Gamma := \{(y, z) \in X \times X \mid y \neq z,\ y \text{ et } z \text{ sont dans le même } gHx\}.$$

Comme $Hx \neq \{x\}$, l'ensemble Γ n'est pas vide.

Si $(y,z) \in \Gamma$, on a $y,z \in g_0 \mathrm{H} x$ pour un certain $g_0 \in \mathrm{G}$ et pour tout $g \in \mathrm{G}$, gy et gz sont dans $gg_0\mathrm{H}x$. En d'autres termes, Γ est stable par l'action diagonale de G, donc c'est une réunion d'orbites. Mais il n'y a que deux orbites.

Si $\Gamma = \mathrm{O}_1$, on a, pour tout $y \neq z$,

$$y \text{ et } z \text{ sont dans le même } g\mathrm{H}x \iff y \text{ et } z \text{ engendrent un plan hyperbolique}$$

Mais pour toutes droites distinctes y et z, il existe $t \in \mathrm{X}$ qui n'est orthogonal ni à y ni à z (tout simplement parce que V ne peut être la réunion des deux hyperplans $y^\perp$ et $z^\perp$). Les droites y et t engendrent alors un plan hyperbolique, donc y et t sont dans le même $g\mathrm{H}x$; mais de même, les droites z et t engendrent alors un plan hyperbolique, donc z et t sont dans le même $g\mathrm{H}x$. On en déduit que y et z sont dans le même $g\mathrm{H}x$. Comme y et z sont quelconques distinctes, cela contredit $\Gamma = \mathrm{O}_1$.

On écarte de façon similaire le cas $\Gamma = \mathrm{O}_2$. On a donc $\Gamma = \mathrm{O}_1 \sqcup \mathrm{O}_2$: toutes droites distinctes y et z sont dans le même $g\mathrm{H}x$. En particulier, tout $y \neq x$ est dans $\mathrm{H}x$. Pour tout $g' \in \mathrm{G}$, ou bien $g'x = x$ et $g \in \mathrm{G}_x \subseteq \mathrm{H}$, ou bien $y := g'x \neq x$ et il existe $h \in \mathrm{H}$ tel que $g'x = hx$, soit $h^{-1}g' \in \mathrm{G}_x \subseteq \mathrm{H}$. On en déduit $g' \in \mathrm{H}$ et $\mathrm{H} = \mathrm{G}$.

On a donc montré que les stabilisateurs sont des sous-groupes maximaux de G. L'action de $\mathrm{G} = \mathrm{Sp}_{2\nu}(\mathbf{K})$ sur $\mathrm{X} = \mathbf{P}^{2\nu-1}(\mathbf{K})$ est primitive. Comme elle est aussi fidèle, le th. 7.9 dit alors que tout sous-groupe distingué non trivial de $\mathrm{Sp}_{2\nu}(\mathbf{K})$ contient $\mathrm{D}(\mathrm{Sp}_{2\nu}(\mathbf{K}))$. Par le th. 7.9, il est donc égal à $\mathrm{Sp}_{2\nu}(\mathbf{K})$, qui est ainsi un groupe simple. □

***Remarque 7.11* (Cas de la caractéristique 2).** — Pour tout corps $\mathbf{K}$, on peut toujours définir un groupe comme en (21) par

$$\mathrm{Sp}_{2\nu}(\mathbf{K}) := \{\mathrm{U} \in \mathrm{GL}_{2\nu}(\mathbf{K}) \mid {}^t\mathrm{U}\mathrm{J}_{2\nu}\mathrm{U} = \mathrm{J}_{2\nu}\}.$$

Beaucoup des résultats démontrés plus haut lorsque $\mathrm{car}(\mathbf{K}) \neq 2$ restent vrais en caractéristique 2. On en particulier :

- $\mathrm{Sp}_2(\mathbf{K}) \simeq \mathrm{SL}_2(\mathbf{K})$;
- $\mathrm{Sp}_{2\nu}(\mathbf{K}) \leq \mathrm{SL}_{2\nu}(\mathbf{K})$;
- $\mathrm{Z}(\mathrm{Sp}_{2\nu}(\mathbf{K})) = \{\pm \mathrm{I}_{2\nu}\}$ (le centre est donc trivial en caractéristique 2) ;
- $|\mathrm{Sp}_{2\nu}(\mathbf{F}_q)|$ est donné par la formule (25) et, en caractéristique 2, $\mathrm{PSp}_{2\nu}(\mathbf{F}_q) = \mathrm{Sp}_{2\nu}(\mathbf{F}_q)$;
- pour $\nu \geqslant 2$, on a $\mathrm{D}(\mathrm{Sp}_{2\nu}(\mathbf{K})) = \mathrm{Sp}_{2\nu}(\mathbf{K})$ et $\mathrm{PSp}_{2\nu}(\mathbf{K})$ est simple, sauf pour $\mathrm{Sp}_4(\mathbf{F}_2) = \mathrm{PSp}_4(\mathbf{F}_2) \simeq \mathfrak{S}_6$, dont le groupe dérivé est $\mathfrak{A}_6$ (prop. I.5.8).

On obtient donc une quatrième série de groupes finis simples $\mathrm{PSp}_{2\nu}(\mathbf{F}_q)$ [16].

8. Groupe orthogonal

On étudie ici quelques propriétés de base du groupe orthogonal. La situation est beaucoup plus compliquée que dans le cas symplectique, vu qu'il peut y avoir beaucoup de formes quadratiques non équivalentes sur un même espace vectoriel.

16. Pour des raisons que vous comprendrez plus tard, ce groupe est aussi noté $\mathrm{C}_\nu(q)$, pour $\nu \geqslant 2$.

8.1. La dimension 2. — Si $\dim(V) = 2$, à une constante multiplicative près (ce qui ne change pas le groupe orthogonal associé), toute forme quadratique s'écrit

$$f(x) = x_1^2 - \alpha x_2^2.$$

Il y a deux cas, suivant que α est un carré ou non dans $\mathbf{K}$.

Cas où α est un carré. La forme f admet alors des vecteurs isotropes non nuls et V est un plan hyperbolique pour f : il existe une base (e_1, e_2) de V dans laquelle

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

Les droites engendrées par e_1 et e_2 étant les seules directions isotropes, elles sont ou bien préservées, ou bien échangées par un élément du groupe orthogonal $O(V, f)$. On en déduit que les éléments de $O(V, f)$ sont de la forme $R_\lambda := \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ ou $S_\lambda := \begin{pmatrix} 0 & \lambda^{-1} \\ \lambda & 0 \end{pmatrix}$, pour $\lambda \in \mathbf{K}^\times$. On a donc

$$\begin{aligned} SO(V, f) &\simeq \{R_\lambda \mid \lambda \in \mathbf{K}^\times\}, \\ O(V, f) &\simeq \{R_\lambda, S_\lambda \mid \lambda \in \mathbf{K}^\times\} = SO(V, f) \sqcup S_1 \cdot SO(V, f). \end{aligned}$$

Les transformations S_λ de $O(V, f) - SO(V, f)$ sont des réflexions (par rapport à la droite engendrée par $e_1 + \lambda e_2$). Le groupe $SO(V, f)$ est abélien. Comme

$$S_1 R_\lambda S_1^{-1} = R_{\lambda^{-1}},$$

le groupe $O(V, f)$ n'est pas abélien, sauf si $\mathbf{K} = \mathbf{F}_3$ (dans ce cas, c'est $\{I_2, -I_2, S_1, -S_1\}$, isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$).

Exemples 8.1. — 1° Lorsque $\mathbf{K}$ est quadratiquement clos, on est toujours dans ce cas.

2° Lorsque $\mathbf{K} = \mathbf{R}$, on est dans ce cas uniquement lorsque la signature est $(1, 1)$. On a donc $SO_{1,1}(\mathbf{R}) \simeq \mathbf{R}^\times$. Dans une base orthogonale, où la forme quadratique est donnée par $x_1^2 - x_2^2$, on vérifie que les isométries directes ont pour matrice

$$\begin{pmatrix} \frac{\varepsilon}{\sqrt{1-\beta^2}} & \frac{-\varepsilon\beta}{\sqrt{1-\beta^2}} \\ \frac{-\varepsilon\beta}{\sqrt{1-\beta^2}} & \frac{\varepsilon}{\sqrt{1-\beta^2}} \end{pmatrix}.$$

avec $\varepsilon = \pm 1$. Le facteur $\frac{1}{\sqrt{1-\beta^2}}$ (qui est relié au paramètre λ de la rotation R_λ définie ci-dessus par la formule $\beta = \frac{1-\lambda}{1+\lambda}$, tandis que ε est le signe de λ) est celui qui intervient dans les formules de Lorentz en relativité (la vitesse de la lumière est ici égale à 1 ; voir exerc. 11.6).

3° Lorsque $\mathbf{K} = \mathbf{F}_q$, on est dans ce cas pour la forme $\langle 1, -1 \rangle$. Avec les notations de la note 11 et de l'ex. 5.6.3°, on a $SO_2^+(\mathbf{F}_q) \simeq \mathbf{F}_q^\times$, cyclique d'ordre $q - 1$. On vérifie que $O_2^+(\mathbf{F}_q)$ est isomorphe au groupe diédral D_{q-1} (*cf.* ex. I.1.4.4°).

Cas où α n'est pas un carré. La forme f est alors anisotrope et on vérifie par un calcul direct qu'on a

$$\begin{aligned} \mathrm{SO}(\mathrm{V},f) &\simeq \left\{ \mathrm{R}_{a,c} := \begin{pmatrix} a & c\alpha \\ c & a \end{pmatrix} \mid a^2 - \alpha c^2 = 1 \right\}, \\ \mathrm{O}(\mathrm{V},f) &\simeq \left\{ \mathrm{R}_{a,c},\ \mathrm{S}_{a,c} := \begin{pmatrix} a & -c\alpha \\ c & -a \end{pmatrix} \mid a^2 - \alpha c^2 = 1 \right\} \\ &= \mathrm{SO}(\mathrm{V},f) \sqcup \mathrm{S}_{1,0} \cdot \mathrm{SO}(\mathrm{V},f). \end{aligned}$$

À nouveau, le groupe $\mathrm{SO}(\mathrm{V},f)$ est abélien. Ses éléments sont appelés *rotations* et $\mathrm{O}(\mathrm{V},f) - \mathrm{SO}(\mathrm{V},f)$ est constitué de réflexions : l'isométrie de matrice $\mathrm{S}_{a,c}$ dans la base (e_1,e_2) est la symétrie orthogonale par rapport à la droite engendrée par $(1+a)e_1 + ce_2$.

Le groupe $\mathrm{O}(\mathrm{V},f)$ s'interprète en terme du corps $\mathbf{K}[\sqrt{\alpha}] = \{a + c\sqrt{\alpha} \mid a, c \in \mathbf{K}\}$. Si $x = a + c\sqrt{\alpha} \in \mathbf{K}$, son « conjugué » est $\bar{x} = a - c\sqrt{\alpha}$ et le morphisme « norme » $\mathrm{N} : \mathbf{K}[\sqrt{\alpha}] \to \mathbf{K}$ défini par $\mathrm{N}(x) = x\bar{x}$ vérifie $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$ et $(\mathrm{N}(x) = 0) \Leftrightarrow (x = 0)$.

Si $x \in \mathbf{K}[\sqrt{\alpha}]^\times$, il opère sur le $\mathbf{K}$-espace vectoriel $\mathbf{K}[\sqrt{\alpha}]$, de dimension 2, par la multiplication par x, ce qui donne un morphisme de groupes injectif

$$\rho : \mathbf{K}[\sqrt{\alpha}]^\times \to \mathrm{GL}_2(\mathbf{K}).$$

Si $x = a + c\sqrt{\alpha}$, la matrice de $\rho(x)$ dans la base $\{1, \sqrt{\alpha}\}$ de $\mathbf{K}[\sqrt{\alpha}]$ est $\begin{pmatrix} a & c\alpha \\ c & a \end{pmatrix}$. Il s'ensuit que ρ induit un isomorphisme entre le groupe (abélien) des éléments de $\mathbf{K}[\sqrt{\alpha}]$ de norme 1 et le groupe $\mathrm{SO}(\mathrm{V},f)$.

La conjugaison peut aussi être vue comme un élément de $\mathrm{GL}_2(\mathbf{K})$, dont la matrice dans la base $\{1, \sqrt{\alpha}\}$ de $\mathbf{K}[\sqrt{\alpha}]$ est $\mathrm{S}_{1,0}$. Le groupe $\mathrm{O}(\mathrm{V},f)$ est donc isomorphe au sous-groupe des automorphismes de $\mathbf{K}[\sqrt{\alpha}]$ engendré par la multiplication par les éléments de norme 1 et la conjugaison.

Le centre de $\mathrm{O}(\mathrm{V},f)$ est $\{\pm \mathrm{Id}_\mathrm{V}\}$: si la multiplication par $x \in \mathbf{K}[\sqrt{\alpha}]$ est dans le centre, elle commute à la conjugaison, c'est-à-dire qu'on a pour tout $y \in \mathbf{K}[\sqrt{\alpha}]$ de norme 1,

$$\overline{xy} = x\overline{y}.$$

On en déduit $\overline{x} = x$, donc $x \in \mathbf{K}$. Comme $\mathrm{N}(x) = 1$, on a $x = \pm 1$. On fait le même raisonnement pour la multiplication par x composée avec la conjugaison.

Dans le cas $\mathbf{K} = \mathbf{R}$, le corps $\mathbf{R}[\sqrt{\alpha}]$ est $\mathbf{C}$, la conjugaison est la conjugaison complexe et le groupe des éléments de norme 1 est le groupe des complexes de module 1.

Exemples 8.2. — 1° Lorsque $\mathbf{K} = \mathbf{R}$, on est dans ce cas uniquement lorsque la signature est $(2,0)$ (forme définie positive) ou $(0,2)$ (forme définie négative) ; les deux cas donnent le même groupe spécial orthogonal $\mathrm{SO}_2(\mathbf{R})$, qui est donc isomorphe au groupe multiplicatif des nombres complexes de module 1. On retrouve la description usuelle du groupe des isométries du plan euclidien :

$$\begin{aligned} \mathrm{SO}_2(\mathbf{R}) &= \left\{ \mathrm{R}_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mid \theta \in \mathbf{R} \right\}, \\ \mathrm{O}_2(\mathbf{R}) &= \left\{ \mathrm{R}_\theta,\ \mathrm{S}_\theta := \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} \mid \theta \in \mathbf{R} \right\}. \end{aligned}$$

2° Lorsque $\mathbf{K} = \mathbf{F}_q$, avec les notations de la note 11 et de l'ex. 5.6.3°, le corps $\mathbf{F}_q[\sqrt{\alpha}]$ est $\mathbf{F}_{q^2}$, la conjugaison est $x \mapsto x^q$ (*cf.* ex. 9.1), donc $\mathrm{N}(x) = x^{q+1}$ et le groupe $\mathrm{SO}^-(2, \mathbf{F}_q)$ est isomorphe au groupe multiplicatif $\{x \in \mathbf{F}_{q^2}^\times \mid x^{q+1} = 1\}$, cyclique d'ordre $q+1$ (*cf.* (27)). De plus, comme $\mathrm{S}_{1,0}\mathrm{R}_{a,c}\mathrm{S}_{1,0}^{-1} = \mathrm{R}_{a,-c} = \mathrm{R}_{a,c}^{-1}$, on voit que le groupe $\mathrm{O}_2^-(\mathbf{F}_q)$ est isomorphe au groupe diédral D_{q+1} (*cf.* ex. I.1.4.4°).

8.2. Le groupe $\mathrm{SO}_3(\mathbf{R})$. — Commençons par un petit résultat plus général que ce dont nous aurons besoin.

Lemme 8.3. — *Soit $\mathbf{K}$ un corps et soit f la forme quadratique sur $\mathbf{K}^n$ donnée par*

$$f(x_1, \dots, x_n) = x_1^2 + \cdots + x_n^2.$$

Alors, 1 est valeur propre pour toute isométrie qui est directe si n est impair, indirecte si n est pair.

Démonstration. — Soit M la matrice d'une telle isométrie u dans la base canonique de $\mathbf{K}^n$. On a alors ${}^t\mathrm{MM} = \mathrm{I}_n$ et

$$\begin{aligned}\det(\mathrm{I}_n - \mathrm{M}) = \det({}^t\mathrm{MM} - \mathrm{M}) &= \det({}^t\mathrm{M} - \mathrm{I}_n)\det(\mathrm{M}) \\ &= \det(\mathrm{M} - \mathrm{I}_n)\det(\mathrm{M}) = (-1)^n \det(\mathrm{M})\det(\mathrm{I}_n - \mathrm{M}).\end{aligned}$$

Si $(-1)^n \det(\mathrm{M}) = -1$, comme la caractéristique de $\mathbf{K}$ n'est pas 2, on en déduit $\det(\mathrm{I}_n - \mathrm{M}) = 0$. □

En particulier, pour toute isométrie directe u de l'espace euclidien $\mathbf{R}^3$, il existe x de norme 1 tel que $u(x) = x$. L'isométrie u laisse alors stable le plan $x^\perp$ sur lequel u est une rotation. Dans n'importe quelle base orthonormale commençant par x, la matrice de u est donc

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}.$$

On peut en particulier déterminer l'angle θ au signe près par la relation

$$\mathrm{tr}(u) = 1 + 2\cos\theta.$$

Notons d'ailleurs que le signe de θ n'est bien déterminé que si on choisit une orientation de l'espace $\mathbf{R}^3$ *et* une orientation de l'axe $\mathbf{R}x$.

Soit $\mathbf{B}^3$ la boule unité fermée dans $\mathbf{R}^3$ de centre 0. À tout $y \in \mathbf{B}^3$ non nul, on associe la rotation d'axe $\mathbf{R}y$ et d'angle $\|y\|\pi$; à 0, on associe $\mathrm{Id}_{\mathbf{R}^3}$. On obtient ainsi une surjection

$$\mathbf{B}^3 \to \mathrm{SO}_3(\mathbf{R})$$

qui est continue, qui est injective sur l'intérieur de $\mathbf{B}^3$ et qui identifie tout vecteur y de sa frontière $\mathbf{S}^3$ avec son opposé. Or, topologiquement, cette sphère n'est rien d'autre que la demi-sphère unité $\mathbf{S}'^4 \subseteq \mathbf{R}^4$. On en déduit que $\mathrm{SO}_3(\mathbf{R})$ est homéomorphe au quotient de $\mathbf{S}^4$ par la relation d'équivalence $y \sim -y$. Ce dernier espace n'est autre que $\mathbf{P}^3(\mathbf{R})$ (associer à une droite vectorielle de $\mathbf{R}^4$ ses deux points d'intersection avec $\mathbf{S}^4$). On a montré :

Le groupe topologique $\mathrm{SO}_3(\mathbf{R})$ est homéomorphe à $\mathbf{P}^3(\mathbf{R})$.

Revenant à l'interprétation de $\mathrm{SO}_3(\mathbf{R})$ comme $\mathbf{B}^3/\sim$, on « voit » que l'image dans $\mathrm{SO}_3(\mathbf{R})$ d'un diamètre de $\mathbf{B}^3$ est un lacet γ qui n'est pas homotope à zéro : $[\gamma] \neq 0$ dans $\pi_1(\mathrm{SO}_3(\mathbf{R}))$. En revanche, si on fait l'aller-retour le long du diamètre, il devient un lacet dans $\mathbf{B}^3$, qu'on peut donc contracter sur un point. On a donc $2[\gamma] = 0$ dans $\pi_1(\mathrm{SO}_3(\mathbf{R}))$.

On peut montrer

$$\pi_1(\mathrm{SO}_3(\mathbf{R})) = \langle[\gamma]\rangle \simeq \mathbf{Z}/2\mathbf{Z}.$$

Le revêtement universel de $\mathrm{SO}_3(\mathbf{R})$ est le groupe $\mathrm{SU}_2(\mathbf{C})$ (déf. 10.1) ou $\mathrm{Spin}_3(\mathbf{R})$ (*cf.* § III.6.4) : un morphisme $\mathrm{SU}_2(\mathbf{C}) \to \mathrm{SO}_3(\mathbf{R})$ de noyau $\{\pm \mathrm{I}_2\}$ sera étudié dans le th. 11.2 (*cf.* aussi note 29).

8.3. Le groupe de Lorentz $\mathrm{SO}_{1,3}(\mathbf{R})$. — Le groupe $\mathrm{SO}_{1,3}(\mathbf{R})$ des isométries directes de l'espace vectoriel $\mathbf{R}^4$ muni de la forme quadratique

$$f(x_0, \dots, x_3) = x_0^2 - x_1^2 - x_2^2 - x_3^2$$

(espace-temps de Minkowski) est important en physique. On l'appelle le *groupe de Lorentz*.

On note $(e_0, \dots, e_3)$ la base canonique de $\mathbf{R}^4$ et $\mathrm{H} = \langle e_1, e_2, e_3\rangle = e_0^\perp$ la partie « espace ». La paire $(\mathrm{H}, -f)$ est donc l'espace euclidien standard à trois dimensions. Si $x \in \mathrm{H}$ est unitaire ($f(x) = -1$), la restriction de f au plan $\mathrm{P}_x := \langle e_0, x\rangle$ a pour signature $(1,1)$. Une isométrie directe de P_x a donc pour matrice

$$\begin{pmatrix} \frac{\varepsilon}{\sqrt{1-\beta^2}} & \frac{-\varepsilon\beta}{\sqrt{1-\beta^2}} \\ \frac{-\varepsilon\beta}{\sqrt{1-\beta^2}} & \frac{\varepsilon}{\sqrt{1-\beta^2}} \end{pmatrix}$$

dans la base (e_0, x) (ex. 8.1.2°). On note $r_{\varepsilon,\beta,x}$ l'isométrie directe de V qui a cette matrice sur P_x et qui est l'identité sur $\mathrm{P}_x^\perp$. Elle « préserve le sens du temps » si $\varepsilon = 1$, elle l'inverse si $\varepsilon = -1$.

On appelle *rotation espace* les rotations de H (prolongées par l'identité sur $\mathbf{R}e_0$).

Proposition 8.4. *— Dans l'espace-temps de Minkowski, toute isométrie directe peut s'écrire come le produit d'un $r_{\varepsilon,\beta,x}$ et d'une rotation espace.*

On verra plus bas que ε ne dépend que de l'isométrie u, pas de la décomposition : il vaut 1 si u préserve le sens du temps, -1 sinon.

Démonstration. — On écrit $u(e_0) = ae_0 + bx$, avec $x \in \mathrm{H}$ et $f(x) = -1$. Si on exprime le fait que $f(u(e_0)) = f(e_0) = 1$, on obtient $a^2 - b^2 = 1$, donc $|a| \geqslant 1$. On choisit β du signe de b avec $\beta^2 = 1 - \frac{1}{a^2} \geqslant 0$ et on prend $\varepsilon = a/|a|$. On a alors $u(e_0) = r_{\varepsilon,\beta,x}(e_0)$. On en déduit $r_{\varepsilon,\beta,x}^{-1} u(e_0) = e_0$. L'isométrie directe $r_{\varepsilon,\beta,x}^{-1} u$ laisse donc stable H et s'y restreint en une rotation, ce qui montre la proposition. □

8.4. Centre et générateurs. — Rappelons que si D est une droite non isotrope, on dispose d'une symétrie orthogonale (réflexion) s_D (de déterminant -1) par rapport à $\mathrm{D}^\perp$. De même, si P est un plan sur lequel la forme quadratique est non dégénérée, on a $\mathrm{V} = \mathrm{P} \oplus \mathrm{P}^\perp$ et le *renversement* r_P, défini par $r_\mathrm{P} = (-1) \oplus 1$, est aussi une transformation orthogonale, élément de $\mathrm{SO}(\mathrm{V}, f)$.

Si $u \in \mathrm{O}(\mathrm{V}, f)$, on vérifie qu'on a $us_\mathrm{D}u^{-1} = s_{u(\mathrm{D})}$ et $ur_\mathrm{P}u^{-1} = r_{u(\mathrm{P})}$.

Proposition 8.5. — *Le centre de* $\mathrm{O}(\mathrm{V},f)$ *est* $\{\pm\mathrm{Id}_\mathrm{V}\}$, *sauf si* $\mathbf{K}=\mathbf{F}_3$ *et* V *est un plan hyperbolique*[17].

Si $\dim(\mathrm{V})\geqslant 3$, *le centre de* $\mathrm{SO}(\mathrm{V},f)$ *est trivial si* $\dim(\mathrm{V})$ *est impair,* $\{\pm\mathrm{Id}_\mathrm{V}\}$ *si* $\dim(\mathrm{V})$ *est pair.*

Si $\dim(\mathrm{V})=2$, on a vu (§8.1) que $\mathrm{SO}(\mathrm{V},f)$ est toujours abélien.

Démonstration. — Si $\dim(\mathrm{V})=2$, la description explicite de $\mathrm{O}(\mathrm{V},f)$ vue au § 8.1 donne le résultat. On suppose donc $\dim(\mathrm{V})\geqslant 3$.

Si $u\in\mathrm{O}(\mathrm{V},f)$ commute aux éléments de $\mathrm{SO}(\mathrm{V},f)$, on a $r_{u(\mathrm{P})}=ur_\mathrm{P}u^{-1}=r_\mathrm{P}$ pour tout plan hyperbolique P, donc $u(\mathrm{P})=\mathrm{P}$ et u préserve les plans sur lesquels la forme f est non dégénérée.

Montrons que toute droite $\mathrm{D}=\mathbf{K}x$ est intersection de deux plans P et Q de ce type.

Si D est non isotrope, on a $\mathrm{V}=\mathrm{D}\overset{\perp}{\oplus}\mathrm{D}^\perp$, donc en prenant deux éléments distincts y et z d'une base orthogonale de $\mathrm{D}^\perp$ (ce qui est possible puisque $\dim(\mathrm{V})\geqslant 3$), les plans $\mathrm{P}=\mathrm{D}\overset{\perp}{\oplus}\mathbf{K}y$ et $\mathrm{Q}=\mathrm{D}\overset{\perp}{\oplus}\mathbf{K}z$ conviennent. Si D est isotrope, on inclut D dans un plan hyperbolique P (sur lequel f est non dégénérée) et on complète x en une base (x,y) de P. Puisque $\mathrm{V}=\mathrm{P}\overset{\perp}{\oplus}\mathrm{P}^\perp$ et que $\dim(\mathrm{V})\geqslant 3$, on peut choisir $z\in\mathrm{P}^\perp$ non nul. Alors on peut prendre $\mathrm{Q}=\mathrm{D}\oplus\mathbf{K}(y+z)$.

Il s'ensuite que si $u\in\mathrm{O}(\mathrm{V},f)$ commute à tous les éléments de $\mathrm{SO}(\mathrm{V},f)$, il préserve toutes les droites ; c'est donc une homothétie (*cf.* note 2). Cela termine la preuve. □

Le quotient de $\mathrm{SO}(\mathrm{V},f)$ par son centre est le *groupe projectif orthogonal*

$$\mathrm{PSO}(\mathrm{V},f):=\mathrm{SO}(\mathrm{V},f)/\mathrm{Z}(\mathrm{SO}(\mathrm{V},f)).$$

C'est un sous-groupe de $\mathrm{PSL}(\mathrm{V})$; il opère donc fidèlement sur l'espace projectif $\mathbf{P}(\mathrm{V})$. On définit de la même façon le sous-groupe $\mathrm{PO}(\mathrm{V},f)\leq\mathrm{PGL}(\mathrm{V})$.

Exemples 8.6. — 1° Les groupes $\mathrm{O}_{s,n-s}(\mathbf{R})$, $\mathrm{SO}_{s,n-s}(\mathbf{R})$ et $\mathrm{PSO}_{s,n-s}(\mathbf{R})$ sont des *variétés différentiables* de dimension $n(n-1)/2$. Leur nature topologique est différente : pour $n\geqslant 2$, parmi les groupes SO, seul $\mathrm{SO}_n(\mathbf{R})$ est compact, et seul $\mathrm{SO}_n(\mathbf{R})$ est connexe (*cf.* ex. 8.12.3°, exerc. 8.11 ; mais il n'est pas simplement connexe pour $n\geqslant 2$ (rem. 11.4)).

2° Les groupes $\mathrm{O}_n(\mathbf{C})$, $\mathrm{SO}_n(\mathbf{C})$ et $\mathrm{PSO}_n(\mathbf{C})$ sont des *variétés complexes* de dimension $n(n-1)/2$.

Théorème 8.7. — *Les réflexions engendrent* $\mathrm{O}(\mathrm{V},f)$.

Démonstration. — On raisonne par récurrence sur la dimension. Soit $u\in\mathrm{O}(\mathrm{V},f)$ et soit $x_1\in\mathrm{V}$ non isotrope ; on pose $x_2:=u(x_1)$. Puisque $f(x_1+x_2)+f(x_1-x_2)=4f(x_1)\neq 0$, l'un au moins des éléments x_1-x_2 ou x_1+x_2 est non isotrope :

– si x_1-x_2 est non isotrope, $s_{x_1-x_2}(x_1)=x_2$, donc $s_{x_1-x_2}u(x_1)=x_1$;

– si x_1+x_2 est non isotrope, $s_{x_2}s_{x_1+x_2}(x_1)=s_{x_2}(-x_2)=x_2$, donc $s_{x_1+x_2}s_{x_2}u(x_1)=x_1$.

Dans les deux cas, on est ramené au cas où u fixe un vecteur non isotrope x_1, et on applique l'hypothèse de récurrence dans $x_1^\perp$. □

17. On a vu que dans ce cas, $\mathrm{O}(\mathrm{V},f)$ est abélien de cardinal 4.

Remarque 8.8. — Cette démonstration montre que toute isométrie est produit d'au plus $2n$ réflexions ($n = \dim(\mathrm{V})$). Le théorème de Cartan-Dieudonné affirme qu'il suffit d'au plus n réflexions.

Théorème 8.9. — *Si* $\dim(\mathrm{V}) \geqslant 3$, *les renversements engendrent* $\mathrm{SO}(\mathrm{V}, f)$.

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

Si $\dim(\mathrm{V}) = 3$, on a $s_{x_1} s_{x_2} = (-s_{x_1})(-s_{x_2})$ et l'opposé d'une réflexion est un renversement (puisque la dimension de V est impaire), d'où le résultat.

Si $\dim(\mathrm{V}) > 3$, on peut supposer x_1 et x_2 non colinéaires (et toujours non isotropes). Considérons le plan $\mathrm{P} := \langle x_1, x_2 \rangle$. On va construire un espace vectoriel $\mathrm{W} \supseteq \mathrm{P}$, de dimension 3, sur lequel f est non dégénérée.

Si $\mathrm{P} \cap \mathrm{P}^\perp = \{0\}$, on prend $y \in \mathrm{P}^\perp$ non isotrope et $\mathrm{W} := \langle x_1, x_2, y \rangle$.

Si $z \in \mathrm{P} \cap \mathrm{P}^\perp$ est non nul, on prend $y \notin z^\perp$ et $\mathrm{W} := \langle x_1, x_2, y \rangle$. Comme x_1 n'est pas isotrope, z ne l'est pas non plus. Un vecteur de $\mathrm{W} \cap \mathrm{W}^\perp$ est orthogonal à z, donc est dans P ; comme il est orthogonal à P, il est colinéaire à z. Enfin, comme il est orthogonal à y, il est nul.

Alors $s_{x_1} s_{x_2}$ agit par l'identité sur $\mathrm{W}^\perp$. On est ainsi ramené au cas de la dimension 3 : sur W, l'isométrie $s_{x_1}|_{\mathrm{W}} s_{x_2}|_{\mathrm{W}}$ est le produit des renversements $-s_{x_1}|_{\mathrm{W}}$ et $-s_{x_2}|_{\mathrm{W}}$; on obtient alors $s_{x_1} s_{x_2}$ comme produit de leurs extensions sur V par l'identité sur $\mathrm{W}^\perp$, qui sont encore des renversements. □

Exercice 8.10. — Montrer que $\mathrm{O}_n(\mathbf{Q})$ est dense dans $\mathrm{O}_n(\mathbf{R})$ et que $\mathrm{SO}_n(\mathbf{Q})$ est dense dans $\mathrm{SO}_n(\mathbf{R})$ (*Indication :* on pourra utiliser le th. 8.7).

Exercice 8.11. — Lorsque $n \geqslant 2$, montrer que $\mathrm{SO}_n(\mathbf{R})$ est connexe et que $\mathrm{O}_n(\mathbf{R})$ a deux composantes connexes (*Indication :* on pourra utiliser le th. 8.9).

8.5. Norme spinorielle et groupe dérivé. — La situation pour le groupe orthogonal est beaucoup plus compliquée que pour le groupe symplectique et nous ne donnerons pas toutes les démonstrations ni tous les détails. Une des raisons en est l'existence d'un morphisme

$$\theta : \mathrm{O}(\mathrm{V}, f) \to \mathbf{K}^\times / \mathbf{K}^{\times 2}$$

appelé *norme spinorielle,* qui vérifie la propriété

$$\theta(s_x) = f(x) \in \mathbf{K}^\times / \mathbf{K}^{\times 2}, \tag{26}$$

pour tout $x \in \mathrm{V}$ non isotrope. Nous ne démontrerons que plus tard (§ III.6.3, cor. 6.8) l'existence de ce morphisme [18]. Notons cependant que comme $\mathbf{K}^\times / \mathbf{K}^{\times 2}$ est abélien, son noyau, noté $\mathrm{O}'(\mathrm{V}, f)$, contient le groupe dérivé $\mathrm{D}(\mathrm{O}(\mathrm{V}, f))$, et le noyau $\mathrm{SO}'(\mathrm{V}, f) := \mathrm{O}'(\mathrm{V}, f) \cap \mathrm{SO}(\mathrm{V}, f)$ de sa restriction à $\mathrm{SO}(\mathrm{V}, f)$ contient $\mathrm{D}(\mathrm{SO}(\mathrm{V}, f))$.

18. Comme les réflexions engendrent $\mathrm{O}(\mathrm{V}, f)$, la relation (26) définit uniquement θ ; cependant, il faut vérifier que cette définition a un sens, c'est-à-dire que si $u \in \mathrm{O}(\mathrm{V}, f)$ se décompose en $u = s_{x_1} \circ \cdots \circ s_{x_r}$, alors $f(x_1) \cdots f(x_r) \in \mathbf{K}^\times / \mathbf{K}^{\times 2}$ est indépendant de la décomposition de u choisie.

Exemples 8.12. — 1° Lorsque $\mathbf{K}$ est quadratiquement clos, $\mathbf{K}^\times/\mathbf{K}^{\times 2}$ est trivial, donc aussi θ.

2° Si $\mathbf{K}=\mathbf{R}$, le groupe $\mathbf{R}^\times/\mathbf{R}^{\times 2}$ a deux éléments, à savoir les classes de 1 et de -1.

Si f est définie positive, θ prend ses valeurs dans $\mathbf{R}^{\times +}/\mathbf{R}^{\times 2}$, donc θ est trivial et $\mathrm{SO}'_n(\mathbf{R})=\mathrm{SO}_n(\mathbf{R})$.

Si f est définie négative, toute réflexion a pour image -1 dans $\mathbf{R}^\times/\mathbf{R}^{\times 2}$, donc θ est le morphisme déterminant et est trivial sur $\mathrm{SO}_n(\mathbf{R})$.

Pour avoir un morphisme θ intéressant, il faut donc regarder les groupes $\mathrm{O}_{s,t}(\mathbf{R})$ avec s et t non nuls (c'est-à-dire les cas où l'indice est $\geqslant 1$). Dans le cas de $\mathrm{O}_{1,m}(\mathbf{R})$, la forme f est donnée sur $\mathbf{R}^{m+1}$ par

$$f(x_0,\dots,x_m)=x_0^2-x_1^2-\cdots-x_m^2.$$

Ce groupe agit sur la quadrique affine $\mathrm{Q}:=\{x\in\mathbf{R}^{m+1}\mid f(x)=1\}$. Or celle-ci a deux composantes connexes Q^+ et Q^- selon que x_0 est positif ou négatif. On peut donc définir un morphisme de groupes

$$\theta':\mathrm{O}_{1,m}(\mathbf{R})\longrightarrow\mathfrak{S}_{\{\mathrm{Q}^+,\mathrm{Q}^-\}}\simeq\mathbf{Z}/2\mathbf{Z}.$$

Si x n'est pas isotrope, on vérifie que $\theta'(s_x)=\mathrm{Id}$ si et seulement si $f(x)<0$ (on voit bien ce qui se passe sur un dessin en dimension 2). Cela signifie que le morphisme θ' n'est autre que le produit dét$\cdot\theta$, donc que [19]

$$\mathrm{SO}'_{1,m}(\mathbf{R})=\{u\in\mathrm{SO}_{1,m}(\mathbf{R})\mid u(\mathrm{Q}^+)=\mathrm{Q}^+\},$$

d'indice 2 dans $\mathrm{SO}_{1,m}(\mathbf{R})$.

En relativité, on travaille dans l'espace-temps de Minkowski, qui correspond au cas $m=3$; le groupe $\mathrm{SO}_{1,3}(\mathbf{R})$ est le groupe de Lorentz (§8.3) et le groupe $\mathrm{SO}'_{1,3}(\mathbf{R})$ des transformations qui préservent le sens du temps, le *groupe de Lorentz restreint* (*cf.* exerc. 11.6).

La situation est analogue si $s,t\geqslant 2$, mais la quadrique Q définie ci-dessus est maintenant connexe. Il faut regarder à la place les sous-espaces vectoriels maximaux $\mathrm{W}\subseteq\mathbf{R}^{s+t}$ sur lesquels la forme f est définie positive, comme par exemple $\langle e_1,\dots,e_s\rangle$. On voit facilement qu'ils sont tous de dimension s et on vérifie qu'ils forment une « famille connexe » (dans le cas $s=1$, ce sont les droites engendrées par les points de Q, qui sont paramétrées par une de ses composantes connexes). On peut alors définir de manière continue une orientation o_{W} sur chacun de ces sous-espaces vectoriels W. L'image de W par une isométrie u est encore un sous-espace du même type et on obtient

$$\mathrm{SO}'_{s,t}(\mathbf{R})=\{u\in\mathrm{SO}_{s,t}(\mathbf{R})\mid u(o_{\mathrm{W}})=o_{u(\mathrm{W})}\}.$$

De façon plus « concrète », dans une base où la forme quadratique s'écrit

$$f(x_1,\dots,x_{s+t})=x_1^2+\cdots+x_s^2-x_{s+1}^2-\cdots-x_{s+t}^2,$$

la matrice M d'un élément de $\mathrm{SO}_{s,t}(\mathbf{R})$ s'écrit sous forme de blocs

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

19. Le groupe $\mathrm{SO}'_{1,m}(\mathbf{R})$ est le groupe de la géométrie hyperbolique, il agit transitivement sur Q^+, qui est un modèle de l'espace hyperbolique de dimension m. Le stabilisateur de e_0 est isomorphe à $\mathrm{SO}_m(\mathbf{R})$, qui est connexe par l'exerc. 8.11. Cela permet de montrer que $\mathrm{SO}'_{1,m}(\mathbf{R})$ est connexe.

où la matrice A est carrée d'ordre s. On voit que la matrice A est inversible [20]. On a alors

$$\mathrm{SO}'_{s,t}(\mathbf{R}) = \{\mathrm{M} \in \mathrm{SO}_{s,t}(\mathbf{R}) \mid \det(\mathrm{A}) > 0\} = \{\mathrm{M} \in \mathrm{SO}_{s,t}(\mathbf{R}) \mid \det(\mathrm{D}) > 0\}.$$

On peut montrer que ce groupe est connexe [21].

3° Lorsque (V, f) est un plan hyperbolique, on note r_λ la « rotation » de matrice R_λ dans une base hyperbolique (e_1, e_2) de V (*cf.* § 8.1). On a

$$r_\lambda = s_{\lambda e_1 - e_2} s_{e_1 - e_2},$$

donc $\theta(r_\lambda) = f(\lambda e_1 - e_2) f(e_1 - e_2) = 4\lambda \equiv \lambda$ dans $\mathbf{K}^\times/\mathbf{K}^{\times 2}$ et le morphisme $\theta|_{\mathrm{SO}(\mathrm{V},f)} : \mathrm{SO}(\mathrm{V}, f) \to \mathbf{K}^\times/\mathbf{K}^{\times 2}$ est surjectif.

Si l'indice ν de f est $\geqslant 1$, c'est-à-dire qu'il existe un vecteur isotrope non nul, V contient un plan hyperbolique. L'exemple 3° ci-dessus montre que le morphisme

$$\theta|_{\mathrm{SO}(\mathrm{V},f)} : \mathrm{SO}(\mathrm{V}, f) \to \mathbf{K}^\times/\mathbf{K}^{\times 2}$$

est alors surjectif. En particulier, si $\nu \geqslant 1$ et que $\mathbf{K}$ n'est pas quadratiquement clos ($\mathbf{K}^{\times 2} \neq \mathbf{K}^\times$), on a $\mathrm{D}(\mathrm{O}(\mathrm{V}, f)) \subseteq \mathrm{SO}'(\mathrm{V}, f) \subsetneq \mathrm{SO}(\mathrm{V}, f)$.

On a en fait un résultat plus précis [22].

***Théorème 8.13* (Eichler).** — *Soit f une forme quadratique non dégénérée sur un espace vectoriel* V *de dimension* $\geqslant 3$. *Si l'indice* ν *de f est* $\geqslant 1$ *(c'est-à-dire si f a un vecteur isotrope non nul), on a*

$$\mathrm{SO}'(\mathrm{V}, f) = \mathrm{D}(\mathrm{O}(\mathrm{V}, f)) = \mathrm{D}(\mathrm{SO}(\mathrm{V}, f))$$

et $\mathrm{SO}(\mathrm{V}, f)/\mathrm{D}(\mathrm{SO}(\mathrm{V}, f)) \simeq \mathbf{K}^\times/\mathbf{K}^{\times 2}$.

Exemples 8.14. — 1° Si $\mathbf{K} = \mathbf{R}$ et que f est définie positive ou négative, on peut montrer qu'on a encore $\mathrm{D}(\mathrm{O}_n(\mathbf{R})) = \mathrm{D}(\mathrm{SO}_n(\mathbf{R})) = \mathrm{SO}_n(\mathbf{R})$.

Si $st > 0$ et $s + t \geqslant 3$ (de sorte que f est d'indice $\geqslant 1$), le théorème montre que $\mathrm{D}(\mathrm{SO}_{s,t}(\mathbf{R}))$ est d'indice 2 dans $\mathrm{SO}_{s,t}(\mathbf{R})$.

3° Lorsque $\mathbf{K} = \mathbf{F}_q$, le groupe $\mathbf{F}_q^\times/\mathbf{F}_q^{\times 2}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$ et l'indice est toujours $\geqslant 1$ dès que $n \geqslant 3$ (ex. 5.6.3°) ; le groupe $\mathrm{D}(\mathrm{SO}(\mathbf{F}_q^n, f))$ est alors d'indice 2 dans $\mathrm{SO}(\mathbf{F}_q^n, f)$.

4° Supposons $\mathbf{K} = \mathbf{Q}$. Si $\nu(f) \geqslant 1$ et $n \geqslant 3$, le th. 8.13 donne $\mathrm{SO}(\mathbf{Q}^n, f)/\mathrm{D}(\mathrm{O}(\mathbf{Q}^n, f)) \simeq \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ qui est un groupe infini (dans lequel tout élément est d'ordre 2).

Le cas où l'indice est nul est beaucoup moins bien connu. Lorsque $\mathbf{K} = \mathbf{Q}$, Meyer a montré qu'une forme quadratique f d'indice nul sur $\mathbf{Q}^n$, avec $n \geqslant 5$, est nécessairement définie négative ou définie positive vue comme forme quadratique sur $\mathbf{R}^n$. Dans ce cas, Kneser a montré que l'image de $\theta|_{\mathrm{SO}(\mathbf{Q}^n,f)}$ est $\mathbf{Q}^{\times +}/\mathbf{Q}^{\times 2}$ et que son noyau $\mathrm{SO}'(\mathbf{Q}^n, f)$ est encore

---

20. En effet, en développant la relation ${}^t\mathrm{M}\begin{pmatrix} \mathrm{I}_s & 0 \\ 0 & -\mathrm{I}_t \end{pmatrix}\mathrm{M} = \begin{pmatrix} \mathrm{I}_s & 0 \\ 0 & -\mathrm{I}_t \end{pmatrix}$, on obtient entre autres ${}^t\mathrm{AA} = \mathrm{I}_s + {}^t\mathrm{CC}$, ce qui entraîne que la matrice ${}^t\mathrm{AA}$ est définie positive, donc que A est inversible (on obtient en fait même $|\det(\mathrm{A})| \geqslant 1$). Il en est de même pour D.

21. Comme dans la note 19, qui explique ces faits lorsque $s = 1$, la deuxième égalité et la connexité de $\mathrm{SO}'_{s,t}(\mathbf{R})$ résultent, lorsque $s, t \geqslant 2$, du fait que $\mathrm{SO}'_{s,t}(\mathbf{R})$ opère transitivement sur la quadrique connexe Q, et que le stabilisateur de e_0 est isomorphe à $\mathrm{SO}'_{s-1,t}(\mathbf{R})$.

22. *Cf.* Dieudonné, J., *La géométrie des groupes classiques*, Springer Verlag, 1955, chap. II, § 6.5. Ce n'est plus vrai pour $\dim(\mathrm{V}) = 2$, puisque $\mathrm{SO}(\mathrm{V}, f)$ est alors abélien (§ 8.1), mais on a encore $\mathrm{SO}'(\mathrm{V}, f) = \mathrm{D}(\mathrm{O}(\mathrm{V}, f))$.

$\mathrm{D}(\mathrm{SO}(\mathbf{Q}^n, f))$. On n'est donc pas très loin du cas $\nu \geqslant 1$: le groupe dérivé $\mathrm{D}(\mathrm{SO}(\mathbf{Q}^n, f))$ est encore d'indice infini dans $\mathrm{SO}(\mathbf{Q}^n, f)$.

La structure des groupes $\mathrm{O}(\mathbf{Q}^3, f)$ et $\mathrm{O}(\mathbf{Q}^4, f)$ est beaucoup moins bien connue dans ce cas.

8.6. Centre. — On peut montrer que pour $\dim(\mathrm{V}) \geqslant 3$, le centre du groupe $\mathrm{D}(\mathrm{SO}(\mathrm{V}, f))$ consiste en les homothéties de ce groupe, c'est-à-dire Id_V et, éventuellement, $-\mathrm{Id}_\mathrm{V}$.

On a d'autre part la formule

$$\theta(-\mathrm{Id}_\mathrm{V}) = \mathrm{disc}(f).$$

En effet, dans une base $(e_1, \ldots, e_n)$ de V où $f(x) = \sum_{i=1}^n \alpha_i x_i^2$, on écrit $-\mathrm{Id}_\mathrm{V} = s_{e_1} \cdots s_{e_n}$, d'où $\theta(-\mathrm{Id}_\mathrm{V}) = f(e_1) \cdots f(e_n) = \prod_{i=1}^n \alpha_i = \mathrm{disc}(f)$.

On en déduit que pour $\dim(\mathrm{V}) \geqslant 3$ et $\nu \geqslant 1$, le centre de $\mathrm{D}(\mathrm{SO}(\mathrm{V}, f)) = \mathrm{SO}'(\mathrm{V}, f)$ est d'ordre 2 si $\mathrm{disc}(f) = 1$ et $\dim(\mathrm{V})$ pair, trivial sinon.

8.7. Simplicité. — Vu les résultats de la section précédente, le seul groupe qui a des chances d'être simple est le quotient $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathrm{V}, f)))$ du groupe dérivé $\mathrm{D}(\mathrm{SO}(\mathrm{V}, f))$ par son centre.

Nous nous contenterons de passer en revue quelques résultats connus, en renvoyant au livre de Dieudonné, J., *La géométrie des groupes classiques,* pour les preuves et des discussions plus approfondies.

Cas $\nu(f) = 0$ (forme anisotrope).— Il n'y a pas de résultat général, mais certains cas particuliers sont complètement décrits.

Lorsque $\mathbf{K} = \mathbf{R}$ (où $\mathrm{D}(\mathrm{SO}_n(\mathbf{R})) = \mathrm{SO}_n(\mathbf{R})$), on a

– le groupe $\mathrm{PSO}_4(\mathbf{R})$ n'est pas simple [23] (th. 11.3) ;
– le groupe $\mathrm{PSO}_n(\mathbf{R})$ est simple pour $n = 3$ ou $n \geqslant 5$.

Lorsque $\mathbf{K} = \mathbf{Q}$, on a :

– le groupe $\mathrm{O}(\mathbf{Q}^3, f)$ admet une suite décroissante de sous-groupes distingués dont l'intersection est $\{\mathrm{Id}\}$;
– pour $n \geqslant 5$, le groupe $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{Q}^n, f))) = \mathrm{PSO}'(\mathbf{Q}^n, f)$ est simple.

Cas $\nu(f) \geqslant 1$.— La situation est plus claire : *lorsque $n \geqslant 3$, le groupe* $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{K}^n, f))) = \mathrm{PSO}'(\mathbf{K}^n, f)$ *est simple,* avec deux exceptions [24].

Ce cas inclut celui des corps finis $\mathbf{F}_q$ dès que $n \geqslant 3$. Rappelons qu'en dimension impaire, on a un seul groupe orthogonal, noté $\mathrm{O}_{2m+1}(\mathbf{F}_q)$ alors qu'en dimension paire, on en a deux,

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

24. On a plus précisément :
– si $n = 3$, le groupe $\mathrm{D}(\mathrm{SO}(\mathbf{K}^3, f))$ est isomorphe à $\mathrm{PSL}_2(\mathbf{K})$, donc il est simple pour $\mathbf{K} \neq \mathbf{F}_3$ (th. 2.15) ;
– si $n = 4$ et $\mathrm{disc}(f) \neq 1$ dans $\mathbf{K}^\times/\mathbf{K}^{\times 2}$, le groupe $\mathrm{D}(\mathrm{SO}(\mathbf{K}^4, f)) = \mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{K}^4, f)))$ est isomorphe à $\mathrm{PGL}_2(\mathbf{K}[\sqrt{\mathrm{disc}(f)}])$ et il est donc simple (th. 2.15) ;
– si $n = 4$ et $\mathrm{disc}(f) = 1$ dans $\mathbf{K}^\times/\mathbf{K}^{\times 2}$, le groupe $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{K}^4, f)))$ est isomorphe à $\mathrm{PSL}_2(\mathbf{K}) \times \mathrm{PSL}_2(\mathbf{K})$ et il est donc simple pour $\mathbf{K} \neq \mathbf{F}_3$ (th. 2.15) ;
– le groupe $\mathrm{P}(\mathrm{D}(\mathrm{SO}(\mathbf{K}^n, f)))$ est simple pour $n \geqslant 5$.

notés $\mathrm{O}^+_{2m}(\mathbf{F}_q)$ (discriminant $(-1)^m$, indice m) et $\mathrm{O}^-_{2m}(\mathbf{F}_q)$ (discriminant $\neq (-1)^m$, indice $m-1$) (ex. 5.6.3°).

Donnons les cardinaux. On a tout d'abord :

$$\begin{aligned} |\mathrm{SO}_{2m+1}(\mathbf{F}_q)| &= q^{m^2}(q^{2m}-1)(q^{2m-2}-1)\cdots(q^2-1), \\ |\mathrm{SO}^\varepsilon_{2m}(\mathbf{F}_q)| &= (q^m-\varepsilon)q^{m(m-1)}(q^{2m-2}-1)\cdots(q^2-1), \end{aligned} \tag{27}$$

où $\varepsilon = \pm 1$ ($\varepsilon = 1$ si $(-1)^m \operatorname{disc}(f)$ est un carré dans $\mathbf{F}_q$ et -1 sinon).

Par le th. 8.13, le groupe dérivé est d'indice 2 dans tous les cas. Dans le cas de la dimension impaire, son centre est trivial et

$$|\mathrm{P}(\mathrm{D}(\mathrm{SO}_{2m+1}(\mathbf{F}_q)))| = \frac{1}{2}q^{m^2}(q^{2m}-1)(q^{2m-2}-1)\cdots(q^2-1).$$

Dans le cas de la dimension paire, le centre est trivial si et seulement si $\operatorname{disc}(f) \neq 1$. Tous calculs faits, on arrive à

$$\begin{aligned} |\mathrm{P}(\mathrm{D}(\mathrm{SO}^+_{2m}(\mathbf{F}_q)))| &= \frac{q^m-1}{\operatorname{pgcd}(4,q^m-1)}q^{m(m-1)}(q^{2m-2}-1)\cdots(q^2-1), \\ |\mathrm{P}(\mathrm{D}(\mathrm{SO}^-_{2m}(\mathbf{F}_q)))| &= \frac{q^m+1}{\operatorname{pgcd}(4,q^m+1)}q^{m(m-1)}(q^{2m-2}-1)\cdots(q^2-1). \end{aligned}$$

On peut définir aussi ces groupes en caractéristique 2. On obtient ainsi trois autres séries infinies de groupes finis simples, à savoir [25]

$$\mathrm{P}(\mathrm{D}(\mathrm{SO}_{2m+1}(\mathbf{F}_q))),\ \mathrm{P}(\mathrm{D}(\mathrm{SO}^+_{2m}(\mathbf{F}_q)))\text{ et }\mathrm{P}(\mathrm{D}(\mathrm{SO}^-_{2m}(\mathbf{F}_q))).$$

9. Formes sesquilinéaires et hermitiennes

9.1. Formes sesquilinéaires. — Il y a une variante des formes bilinéaires quand le corps $\mathbf{K}$ (qu'on supposera toujours de caractéristique $\neq 2$) est équipé d'une involution de corps σ. L'exemple principal sera $\mathbf{K} = \mathbf{C}$ avec $\sigma(z) = \bar{z}$ et, pour simplifier les notations, on notera toujours l'involution σ de $\mathbf{K}$ sous la forme $\sigma(\lambda) = \bar{\lambda}$, quel que soit le corps.

La décomposition $\mathbf{C} = \mathbf{R} \oplus i\mathbf{R}$ s'étend de la manière suivante à tout corps muni d'une involution : comme $\operatorname{car}(\mathbf{K}) \neq 2$, on a une décomposition $\mathbf{K} = \mathbf{K}_0 \oplus \mathbf{K}_1$, où $\mathbf{K}_0$ et $\mathbf{K}_1$ sont les espaces propres de σ pour les valeurs propres 1 et -1, et $\mathbf{K}_0$ est un sous-corps de $\mathbf{K}$. Si $\sigma \neq \mathrm{Id}_\mathbf{K}$, on peut choisir $\mathrm{I} \in \mathbf{K}_1 - \{0\}$; on a alors

$$\mathbf{K} = \mathbf{K}_0 \oplus \mathrm{I}\mathbf{K}_0 \quad \text{avec } \mathrm{I}^2 \in \mathbf{K}_0^\times.$$

Exemple 9.1. — Si q est une puissance de nombre premier impair, le morphisme $\sigma : x \mapsto x^q$ est une involution du corps $\mathbf{K} = \mathbf{F}_{q^2}$. Le corps fixe $\mathbf{K}_0$ est le sous-corps $\mathbf{F}_q$ de $\mathbf{F}_{q^2}$.

On dit qu'un morphisme de groupes additifs u entre $\mathbf{K}$-espaces vectoriels est σ-linéaire si $u(\lambda x) = \bar{\lambda}u(x)$ pour tout vecteur x et tout $\lambda \in \mathbf{K}$. Une *forme σ-sesquilinéaire* est une application $b : \mathrm{V} \times \mathrm{V} \to \mathbf{K}$ telle que pour tout $y \in \mathrm{V}$, l'application $x \mapsto b(x,y)$ soit σ-linéaire et l'application $y \mapsto b(x,y)$ soit linéaire. Pour tous x et y dans V et tout $\lambda \in \mathbf{K}$, on a donc

$$b(x,\lambda y) = \lambda b(x,y) \quad \text{et} \quad b(\lambda x, y) = \bar{\lambda} b(x,y).$$

25. Pour des raisons que vous comprendrez plus tard, ces groupes sont aussi notés $\mathrm{B}_m(q)$, $\mathrm{D}_m(q)$ et ${}^2\mathrm{D}_m(q)$, respectivement.

Dans une base (e_i) de V, la matrice M de b est donnée par $M_{ij} = b(e_i, e_j)$. Sur des vecteurs colonnes, on a alors $b(X,Y) = X^*MY$ et la matrice de b dans une autre base est P^*MP, où P est la matrice de passage (on note, pour toute matrice N, $N^* := {}^t\bar{N}$).

La forme sesquilinéaire b est *hermitienne* si en outre

$$b(y,x) = \overline{b(x,y)}$$

pour tous $x, y \in V$. C'est le cas si et seulement si sa matrice M satisfait $M^* = M$ (on dit aussi que M est une matrice hermitienne)

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

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

On récupère, puisque $\mathrm{car}(\mathbf{K}) \neq 2$, la forme sesquilinéaire à partir de h par la formule

$$b(x,y) = \frac{1}{4}\big(h(x+y) - h(x-y) + \frac{1}{I}(h(x+Iy) - h(x-Iy))\big).$$

On définit comme dans le cas symétrique le rang d'une forme sesquilinéaire hermitienne, la notion de forme sesquilinéaire hermitienne non dégénérée, d'isométrie, de vecteurs orthogonaux, de sous-espace totalement isotrope, de plan hyperbolique.

La réduction de Gauss (*cf.* § 4.2) décompose une forme hermitienne sous la forme

$$h(x) = \alpha_1 \bar{x}_1 x_1 + \cdots + \alpha_r \bar{x}_r x_r.$$

avec $\alpha_1, \ldots, \alpha_r \in \mathbf{K}_0^\times$.

Le théorème de Witt reste valable (avec des modifications dans la démonstration, en particulier dans celle du lemme 5.3) et on peut définir de la même façon l'indice d'une forme hermitienne.

10. Groupe unitaire

10.1. Définition. — On définit le *groupe unitaire* $U(V,h)$ d'une forme hermitienne h non dégénérée sur un espace vectoriel V comme le groupe des isométries de (V,h). Si M est la matrice (inversible) dans une base de V de la forme sesquilinéaire hermitienne b associée, ce groupe est isomorphe au groupe

$$\{U \in GL(V) \mid U^*MU = M\}.$$

Le *groupe spécial unitaire* est défini comme d'habitude par

$$SU(V,h) := U(V,h) \cap SL(V).$$

Exemple 10.1. — 1° Si $\mathbf{K} = \mathbf{C}$ et σ est la conjugaison complexe, on peut trouver $a_i \in \mathbf{C}$ tel que $\bar{a}_i a_i = \pm\alpha_i$. Ainsi, pour toute forme hermitienne h non dégénérée sur $\mathbf{C}^n$, il existe une base dans laquelle elle s'écrit

$$h(x) = \bar{x}_1 x_1 + \cdots + \bar{x}_s x_s - \bar{x}_{s+1} x_{s+1} - \cdots - \bar{x}_n x_n.$$

L'indice est $\inf(s, n-s)$. Le groupe unitaire associé est noté $U_{s,n-s}(\mathbf{C})$. Il est isomorphe à

$$\left\{ U \in GL_n(\mathbf{C}) \;\middle|\; U^* \begin{pmatrix} I_s & 0 \\ 0 & -I_{n-s} \end{pmatrix} U = \begin{pmatrix} I_s & 0 \\ 0 & -I_{n-s} \end{pmatrix} \right\}.$$

On note $\mathrm{U}_n(\mathbf{C})$ lorsque $s = n$. Les groupes $\mathrm{U}_{s,n-s}(\mathbf{C})$ (resp. $\mathrm{SU}_{s,n-s}(\mathbf{C})$) sont des *variétés différentiables* de dimension n^2 (resp. n^2-1).

2° Si $\mathbf{K} = \mathbf{F}_{q^2}$ (avec q puissance de nombre premier impair) et $\sigma(\lambda) = \lambda^q$, le morphisme

$$\begin{array}{ccc} \mathbf{F}_{q^2}^\times & \longrightarrow & \mathbf{F}_q^\times \\ \lambda & \longmapsto & \bar\lambda\lambda = \lambda^{q+1} \end{array}$$

est surjectif. En effet, un générateur du groupe cyclique $\mathbf{F}_{q^2}^\times$ est d'ordre $q^2-1 = (q-1)(q+1)$; il est donc envoyé sur un élément d'ordre $q-1$, c'est-à-dire un générateur de $\mathbf{F}_q^\times$. Il en résulte que tout élément α_i de $\mathbf{F}_q^\times$ peut s'écrire $\bar a_i a_i$, et donc, pour toute forme hermitienne h non dégénérée sur $\mathbf{F}_{q^2}^n$, il existe une base dans laquelle elle s'écrit

$$h(x) = \bar x_1 x_1 + \cdots + \bar x_n x_n = x_1^{q+1} + \cdots + x_n^{q+1}.$$

Toutes les formes non dégénérées sur $\mathbf{F}_{q^2}^n$ sont donc équivalentes et iI existe aussi une base dans laquelle la forme s'écrit $h(x) = \bar x_1 x_1 - \bar x_2 x_2 + \cdots + (-1)^{n+1}\bar x_n x_n$. L'indice est donc $\lfloor n/2 \rfloor$. En particulier, tout plan est hyperbolique.

Le groupe unitaire est noté $\mathrm{U}_n(\mathbf{F}_{q^2})$. Il est isomorphe au groupe

$$\{\mathrm{U} \in \mathrm{GL}_n(\mathbf{F}_{q^2}) \mid {}^t\mathrm{U}^{(q)}\mathrm{U} = \mathrm{I}_n\},$$

où $\mathrm{U}^{(q)}$ est la matrice obtenue à partir de U en élevant tous ses coefficients à la puissance q. On a

$$|\mathrm{U}_n(\mathbf{F}_{q^2})| = (q^n - (-1)^n)q^{n-1}(q^{n-1} - (-1)^{n-1})q^{n-2}\cdots(q^2-1)q(q+1).$$

Exercice 10.2. — Soit $\mathrm{M} \in \mathrm{GL}_n(\mathbf{F}_{q^2})$ une matrice telle que ${}^t\mathrm{M} = \mathrm{M}^{(q)}$. Montrer qu'il existe une matrice $\mathrm{P} \in \mathrm{GL}_n(\mathbf{F}_{q^2})$ tel que $\mathrm{M} = {}^t\mathrm{P}^{(q)}\mathrm{P}$.

10.2. La dimension 2. — Comme dans le cas orthogonal, le cas de la dimension 2 peut être décrit par calcul direct. Nous envisageons les deux types de formes qui peuvent intervenir dans les cas $\mathbf{K} = \mathbf{C}$ ou $\mathbf{F}_{q^2}$.

Cas de la forme hermitienne $\bar x_1 x_1 + \bar x_2 x_2$.

Proposition 10.3. — *Supposons* $\dim(\mathrm{V}) = 2$ *et* $h(x_1, x_2) = \bar x_1 x_1 + \bar x_2 x_2$. *Alors*

$$\mathrm{SU}(\mathrm{V}, h) \simeq \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar\beta & \bar\alpha \end{pmatrix} \,\middle|\, \alpha, \beta \in \mathbf{K},\ \bar\alpha\alpha + \bar\beta\beta = 1 \right\}.$$

En particulier, $\mathrm{SU}_2(\mathbf{C})$ est un groupe non commutatif.

Démonstration. — La matrice $\mathrm{U} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est dans $\mathrm{SU}(\mathrm{V}, h)$ si $\det(\mathrm{U}) = 1$ et $\mathrm{U}^*\mathrm{U} = \mathrm{I}_2$, ce qui mène aux équations

$$\alpha\delta - \beta\gamma = 1, \quad \bar\alpha\alpha + \bar\gamma\gamma = \bar\beta\beta + \bar\delta\delta = 1, \quad \bar\alpha\beta + \bar\gamma\delta = 0.$$

Le système $\begin{cases} \alpha\delta - \gamma\beta = 1 \\ \bar\gamma\delta + \bar\alpha\beta = 0 \end{cases}$ d'inconnues δ et β est de déterminant 1 donc a une unique solution, qui est $\beta = -\bar\gamma$ et $\delta = \bar\alpha$. □

Cas d'un plan hyperbolique. Dans une base hyperbolique, la forme hermitienne est donnée par $h(x_1, x_2) = \bar{x}_1 x_2 + \bar{x}_2 x_1$.

Proposition 10.4. — *Supposons* $\dim(\mathrm{V}) = 2$ *et* V *hyperbolique pour la forme hermitienne* h. *Alors* $\mathrm{SU}(\mathrm{V}, h) \simeq \mathrm{SL}_2(\mathbf{K}_0)$.

Exemple 10.5. — On a donc $\mathrm{SU}_{1,1}(\mathbf{C}) \simeq \mathrm{SL}_2(\mathbf{R})$ et $\mathrm{SU}_2(\mathbf{F}_{q^2}) \simeq \mathrm{SL}_2(\mathbf{F}_q)$.

Démonstration. — Dans une base hyperbolique, la matrice de la forme hermitienne h est $\mathrm{H} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Alors, $\mathrm{U} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est dans $\mathrm{SU}(\mathrm{V}, h)$ si $\det(\mathrm{U}) = 1$ et $\mathrm{U}^* \mathrm{H} \mathrm{U} = \mathrm{H}$, ce qui mène aux équations

$$\alpha\delta - \beta\gamma = 1, \quad \alpha\bar{\gamma} + \bar{\alpha}\gamma = 0, \quad \beta\bar{\gamma} + \bar{\alpha}\delta = 1, \quad \beta\bar{\delta} + \bar{\beta}\delta = 0.$$

Elles se résolvent en $\bar{\alpha} = \alpha$, $\bar{\delta} = \delta$, $\bar{\beta} = -\beta$, $\bar{\gamma} = -\gamma$ et $\alpha\delta - \beta\gamma = 1$. On obtient $\alpha, \delta, \mathrm{I}\beta, \mathrm{I}\gamma \in \mathbf{K}_0$ et $\alpha\delta - \beta\gamma = 1$, soit encore $v = \begin{pmatrix} \alpha & \mathrm{I}\beta \\ \mathrm{I}^{-1}\gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{K}_0)$. On vérifie que l'application $u \mapsto v$ est bien un morphisme de groupes [(26)]. □

10.3. Produit scalaire hermitien. — Dans cette section uniquement, on suppose $\mathbf{K} = \mathbf{C}$ et on considère une forme hermitienne h définie positive sur un $\mathbf{C}$-espace vectoriel V de dimension n, c'est-à-dire satisfaisant $h(x) \geqslant 0$ pour tout $x \in \mathrm{V}$, avec égalité si et seulement si $x = 0$. Une telle forme est en particulier non dégénérée ; on l'appelle un *produit scalaire hermitien*. On a vu qu'il existe alors une base orthonormale, c'est-à-dire une base dans laquelle la forme h s'écrit

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

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

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

$$b(x, u(y)) = b(u^*(x), y)$$

pour tous $x, y \in \mathrm{V}$. En particulier, $u \in \mathrm{U}(\mathrm{V}, h)$ si et seulement si $u^* = u^{-1}$.

Dans une base orthonormale, si u a pour matrice U, alors u^* a pour matrice U^*.

---

26. On peut décrire plus intrinsèquement le morphisme $\mathrm{SL}_2(\mathbf{K}_0) \to \mathrm{SU}(\mathrm{V}, h)$ comme suit. On considère $\mathbf{K}$ comme un $\mathbf{K}_0$-espace vectoriel de dimension 2. L'espace vectoriel $\mathrm{V} := \mathrm{End}_{\mathbf{K}_0} \mathbf{K}$ des endomorphismes $\mathbf{K}_0$-linéaires de $\mathbf{K}$ est naturellement un $\mathbf{K}$-espace vectoriel de dimension 2, puisque (Id, σ) en est une base. Si $\alpha = a + \mathrm{I}a'$ et $\beta = b + \mathrm{I}b'$ sont dans $\mathbf{K}$, la matrice de l'endomorphisme $\alpha\mathrm{Id} + \beta\sigma$ de $\mathbf{K}$ dans la base $(1, \mathrm{I})$ est $\begin{pmatrix} a+b & (a'-b')\mathrm{I}^2 \\ a'+b' & a-b \end{pmatrix}$, dont le déterminant est $\bar{\alpha}\alpha - \bar{\beta}\beta$. C'est donc une forme hermitienne sur V, hyperbolique puisque le vecteur $(1, 1)$ est isotrope.

On dispose d'autre part d'une application $\mathbf{K}$-linéaire $\phi : \mathrm{V} = \mathrm{End}_{\mathbf{K}_0} \mathbf{K} \to \mathrm{End}_{\mathbf{K}}(\mathrm{V})$ qui envoie $u \in \mathrm{V}$ sur l'endomorphisme ϕ_u de V donné par $v \mapsto u \circ v$. Comme $\det(\phi_u(v)) = \det(u)\det(v)$, on voit que ϕ_u est unitaire pour la forme hermitienne dét si et seulement si $\det(u) = 1$. L'application ϕ induit donc un morphisme de groupes $\mathrm{SL}(\mathbf{K}) \to \mathrm{U}(\mathrm{V}, \det)$. On vérifie ensuite que ce morphisme est à valeurs dans $\mathrm{SU}(\mathrm{V}, \det)$ (c'est-à-dire que $\det(\phi_u) = 1$ si $\det(u) = 1$) et qu'il est surjectif.

Plus généralement, on dit qu'un endomorphisme u de V est *normal* si $u^* u = u u^*$. Cette notion inclut les endomorphismes unitaires ($u^* = u^{-1}$), autoadoints ($u^* = u$) et antiautoadjoints ($u^* = -u$).

Proposition 10.6. — *Tout endomorphisme normal pour un produit scalaire hermitien se diagonalise dans une base orthonormale.*

Les valeurs propres sont de module 1 pour les endomorphismes unitaires, réelles pour les endomorphismes autoadjoints et imaginaires pures pour les endomorphismes antiautoadjoints.

Démonstration de la proposition. — Soit u un endomorphisme normal de V. Soit λ une valeur propre (complexe) de u et soit V_λ l'espace propre associé. Si $x \in V_\lambda$, on a

$$u(u^*(x)) = u^*(u(x)) = u^*(\lambda x) = \lambda u^*(x),$$

donc $u^*(x) \in V_\lambda$. Ainsi $u^*(V_\lambda) \subseteq V_\lambda$.

Si $y \in V_\lambda^\perp$ et $x \in V_\lambda$, on obtient $b(x, u(y)) = b(u^*(x), y) = 0$, donc $u(V_\lambda^\perp) \subseteq V_\lambda^\perp$. Une récurrence sur la dimension de V montre alors que V est somme directe orthogonale des espaces propres de u. □

Si l'on dispose d'une seconde forme hermitienne h', on peut lui associer, puisque h est non dégénérée, un endomorphisme u de V qui vérifie

$$\forall x, y \in V \qquad b'(x, y) = b(x, u(y)).$$

On a aussi

$$b(u(x), y) = \overline{b(y, u(x)} = \overline{b'(y, x)} = b'(x, y) = b(x, u(y)),$$

de sorte que $u^* = u$. D'après la proposition, u se diagonalise dans une base h-orthonormale, ce qui signifie que dans cette base, la forme b' a une matrice diagonale

$$\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}, \quad \text{avec } \lambda_1, \ldots, \lambda_n \in \mathbf{R}.$$

La forme h' est définie positive si et seulement si les λ_i sont tous strictement positifs.

10.4. Propriétés des groupes unitaires. — On énonce sans démonstration quelques propriétés des groupes unitaires pour une forme hermitienne h sur un $\mathbf{K}$-espace vectoriel de dimension $n \geqslant 2$.

Centre : Le centre de $U(\mathbf{K}^n, h)$ est constitué des homothéties de rapport λ tel que $\bar{\lambda}\lambda = 1$.

Le centre de $SU(\mathbf{K}^n, h)$ est constitué des homothéties de rapport satisfaisant en outre $\lambda^n = 1$. Pour $\mathbf{K} = \mathbf{C}$, c'est donc le groupe des racines n-ièmes de l'unité. Pour $\mathbf{K} = \mathbf{F}_{q^2}$, c'est le groupe des racines $\mathrm{pgcd}(q+1, n)$-ièmes de l'unité.

On notera

$$PSU(\mathbf{K}^n, h) := SU(\mathbf{K}^n, h)/Z(SU(\mathbf{K}^n, h)).$$

Simplicité : Si la forme hermitienne h est d'indice $\geqslant 1$, le groupe $\mathrm{PSU}(\mathbf{K}^n, h)$ est simple (c'est donc le cas pour les groupes $\mathrm{PSU}_{s,t}(\mathbf{C})$ avec $s, t > 0$, et $\mathrm{PSU}_n(\mathbf{F}_{q^2})$ pour $n \geqslant 2$), à l'exception du groupe $\mathrm{PSU}_2(\mathbf{F}_9) \simeq \mathrm{PSL}_2(\mathbf{F}_3)$ (prop. 10.4).

Si l'indice est nul, donc la forme anisotrope, il n'y a pas de résultat général. Néanmoins $\mathrm{PSU}_n(\mathbf{C})$ est simple dès que $n \geqslant 2$: en fait, comme on le verra dans le § 11, $\mathrm{PSU}_2(\mathbf{C}) \simeq \mathrm{SO}_3(\mathbf{R})$, qui est simple, et l'énoncé pour $n > 2$ s'en déduit.

On peut définir les groupes unitaires aussi en caractéristique 2. On obtient ainsi une autre série de groupes finis simples, à savoir $\mathrm{PSU}_n(\mathbf{F}_{q^2})$ pour q puissance de nombre premier et $n \geqslant 3$ [27].

11. Quaternions

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

$$\mathbf{H} := \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbf{C} \right\}. \tag{28}$$

L'addition et la multiplication dans $\mathbf{H}$ sont celles des matrices. Puisque le déterminant est $|\alpha|^2 + |\beta|^2$, seule la matrice nulle n'est pas inversible et on obtient un corps.

On distingue les éléments suivants de $\mathbf{H}$:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathrm{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathrm{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathrm{K} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Les multiples réels de 1 fournissent le sous-corps $\mathbf{R}$ de $\mathbf{H}$. La famille $(1, \mathrm{I}, \mathrm{J}, \mathrm{K})$ est une base de $\mathbf{H}$ vu comme espace vectoriel sur $\mathbf{R}$. On observe que

$$\mathrm{I}^2 = \mathrm{J}^2 = \mathrm{K}^2 = -1, \quad \mathrm{IJK} = -1,$$

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

$$\mathrm{IJ} = -\mathrm{JI} = \mathrm{K}, \quad \mathrm{JK} = -\mathrm{KJ} = \mathrm{I}, \quad \mathrm{KI} = -\mathrm{IK} = \mathrm{J}.$$

On définit le *conjugué* d'un quaternion $q = x_0 + x_1\mathrm{I} + x_2\mathrm{J} + x_3\mathrm{K}$, où $x_0, \ldots, x_3 \in \mathbf{R}$, en posant

$$\bar{q} = x_0 - x_1\mathrm{I} - x_2\mathrm{J} - x_3\mathrm{K}.$$

La conjugaison a les propriétés suivantes :

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

2° $\mathrm{N}(q) := q\bar{q} = \bar{q}q = x_0^2 + x_1^2 + x_2^2 + x_3^2 \in \mathbf{R}$, en particulier, $\mathrm{N}(q) = 0$ si et seulement si $q = 0$, et si $q \neq 0$, on a $q^{-1} = \frac{\bar{q}}{\mathrm{N}(q)}$.

Un quaternion est
- réel si $\bar{q} = q$;
- *imaginaire pur* si $\bar{q} = -q$.

27. Ces groupes sont aussi notés ${}^2\mathrm{A}_{n-1}(q^2)$.

L'ensemble des quaternions imaginaires purs est $\mathrm{Im}(\mathbf{H}) = \{x_1\mathrm{I} + x_2\mathrm{J} + x_3\mathrm{K}\}$ et on a

$$\mathbf{H} = \mathbf{R} \oplus \mathrm{Im}(\mathbf{H}).$$

L'ensemble $\{x_0 + x_1\mathrm{I} \mid x_0, x_1 \in \mathbf{R}\}$ est un sous-corps de $\mathbf{H}$ isomorphe à $\mathbf{C}$ (ce n'est pas le seul car les rôles de I, J et K sont interchangeables dans $\mathbf{H}$ [28]). La famille $(1, \mathrm{J})$ est une base de $\mathbf{H}$ vu comme espace vectoriel sur $\mathbf{C}$. Plus précisément, on a

$$\begin{aligned} q &= x_0 + x_1\mathrm{I} + x_2\mathrm{J} + x_3\mathrm{K}, \qquad \text{où } x_0, \dots, x_3 \in \mathbf{R}, \\ &= (x_0 + x_1\mathrm{I})1 + (x_2 + x_3\mathrm{I})\mathrm{J}. \end{aligned}$$

Dans cette écriture, on fera attention que $\beta = x_2 + x_3\mathrm{I}$ et J ne commutent pas en général (on a $\mathrm{J}\beta = \bar{\beta}\mathrm{J}$).

Le centre $\mathrm{Z}(\mathbf{H})$ de $\mathbf{H}$ est $\mathbf{R}$: en effet, si $q \in \mathrm{Z}(\mathbf{H})$, écrivons comme ci-dessus $q = \alpha + \beta\mathrm{J}$, avec $\alpha, \beta \in \mathbf{C}$. De $q\mathrm{I} = \mathrm{I}q$, on déduit $\beta = 0$, et de $\alpha\mathrm{J} = \mathrm{J}\alpha = \bar{\alpha}\mathrm{J}$, on déduit $\alpha \in \mathbf{R}$.

Lemme 11.1. — *La norme* $\mathrm{N} : \mathbf{H}^\times \to \mathbf{R}^\times$ *est un morphisme de groupes multiplicatifs. Son noyau* $\ker(\mathrm{N}) = \{q \in \mathbf{H} \mid \mathrm{N}(q) = 1\}$ *est un groupe isomorphe à* $\mathrm{SU}_2(\mathbf{C})$.

Démonstration. — On a

$$\mathrm{N}(q_1 q_2) = \bar{q}_2 \bar{q}_1 q_1 q_2 = \bar{q}_2 \mathrm{N}(q_1) q_2 = \mathrm{N}(q_1)\mathrm{N}(q_2),$$

la dernière égalité étant vraie car $\mathrm{N}(q_1) \in \mathbf{R} = \mathrm{Z}(\mathbf{H})$.

La description matricielle (28) donne l'interprétation du noyau comme le groupe $\mathrm{SU}_2(\mathbf{C})$ (prop. 10.3). □

Bien sûr, N s'identifie à la norme euclidienne usuelle dans $\mathbf{H} = \mathbf{R}^4$, donc le groupe $\mathrm{SU}_2(\mathbf{C})$ est homéomorphe à la sphère de $\mathbf{R}^4$.

Soit q un quaternion tel que $\mathrm{N}(q) = 1$. Considérons la conjugaison (au sens du groupe multiplicatif (non abélien) $(\mathbf{H}^\times, \times)$)

$$\begin{aligned} \phi_q : \mathbf{H} &\longrightarrow \mathbf{H} \\ x &\longmapsto qxq^{-1} \end{aligned}$$

Puisque $q^{-1} = \bar{q}$, on a

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

donc ϕ_q agit par l'identité sur $\mathbf{R}$ et préserve la décomposition $\mathbf{H} = \mathbf{R} \oplus \mathrm{Im}(\mathbf{H})$. En outre,

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

donc ϕ_q agit par isométries sur $\mathbf{R}^4$. En restreignant ϕ_q à $\mathrm{Im}(\mathbf{H})$, on obtient ainsi un morphisme de groupes

$$\begin{aligned} \phi : \mathrm{SU}_2(\mathbf{C}) &\longrightarrow \mathrm{O}_3(\mathbf{R}) \\ q &\longmapsto \phi_q|_{\mathrm{Im}(\mathbf{H})}. \end{aligned}$$

Comme le groupe $\mathrm{SU}_2(\mathbf{C})$, homéomorphe à la sphère de $\mathbf{R}^4$, est connexe, l'image de ϕ est connexe donc incluse dans $\mathrm{SO}_3(\mathbf{R})$.

---

28. En faisant agir les automorphismes ϕ_q définis plus bas, on voit qu'on peut même changer le triplet $(\mathrm{I}, \mathrm{J}, \mathrm{K})$ en son image par n'importe quelle rotation de $\mathbf{R}^3$, donc en particulier I en $q_1\mathrm{I} + q_2\mathrm{J} + q_3\mathrm{K}$ pour $q_1, q_2, q_3 \in \mathbf{R}$ tels que $q_1^2 + q_2^2 + q_3^2 = 1$, ce qui donne une famille de sous-corps de $\mathbf{H}$ isomorphes à $\mathbf{C}$ paramétrée par la sphère $\mathbf{S}^2$.

Théorème 11.2. — *Le morphisme* ϕ *ainsi défini est surjectif, de noyau* $\{\pm 1\}$. *Par conséquent,*

$$\mathrm{SO}_3(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C})/\{\pm 1\} = \mathrm{PSU}_2(\mathbf{C}).$$

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

Montrons que ϕ est surjectif. Soit $q \in \mathrm{Im}(\mathbf{H})$ tel que $q\bar{q} = 1$. Alors $q^2 = -q\bar{q} = -1$ et

$$\begin{aligned} \phi_q(q) &= q, \\ \phi_q^2(x) &= \phi_{q^2}(x) = x \quad \text{pour tout } x \in \mathrm{Im}(\mathbf{H}), \end{aligned}$$

donc $\phi_q|_{\mathrm{Im}(\mathbf{H})}$, qui est une rotation autre que l'identité, est obligatoirement le renversement d'axe $\mathbf{R}q \subseteq \mathrm{Im}(\mathbf{H})$. L'image de ϕ contient ainsi les renversements et ϕ est surjective par le th. 8.9. □

L'isomorphisme entre $\mathrm{PSU}_2(\mathbf{C})$ et $\mathrm{SO}_3(\mathbf{R})$ a été montré en trouvant, grâce aux quaternions, une action de $\mathrm{SU}_2(\mathbf{C})$, identifié au groupe des quaternions de norme 1, sur $\mathbf{R}^3$. On peut aussi regarder l'action de $\mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C})$ sur $\mathbf{R}^4 = \mathbf{H}$, définie en associant à un couple de quaternions (q_1, q_2), chacun de norme 1, l'endomorphisme

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

de $\mathbf{H}$.

Théorème 11.3. — *1° On définit ainsi un morphisme*

$$\psi : \mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C}) \to \mathrm{SO}_4(\mathbf{R})$$

qui est surjectif, de noyau $\{\pm(1,1)\}$.

2° On a un isomorphisme $\mathrm{PSO}_4(\mathbf{R}) \simeq \mathrm{SO}_3(\mathbf{R}) \times \mathrm{SO}_3(\mathbf{R})$.

En particulier, le groupe $\mathrm{PSO}_4(\mathbf{R})$ n'est pas simple.

Démonstration. — 1° À nouveau, on a $\mathrm{N}(\phi_{q_1,q_2}(x)) = q_1 x q_2^{-1} q_2 \bar{x} q_1^{-1} = \mathrm{N}(x)$ donc l'image de ψ est bien contenue dans $\mathrm{O}_4(\mathbf{R})$ et même, par connexité de l'image, dans $\mathrm{SO}_4(\mathbf{R})$.

On vérifie facilement l'égalité

$$\psi_{q_1,q_2} \circ \psi_{q_1',q_2'} = \psi_{q_1 q_1', q_2 q_2'},$$

qui montre que ψ est un morphisme de groupes.

Le noyau de ψ est constitué des (q_1, q_2) tels que $q_1 x q_2^{-1} = x$ pour tout $x \in \mathbf{H}$ donc $q_1 x = xq_2$. Faisant $x = 1$ on déduit $q_1 = q_2$, forcément élément de $\mathrm{Z}(\mathbf{H})$, donc $q_1 = q_2 = \pm 1$.

Pour montrer que ψ est surjective, on prend $u \in \mathrm{SO}_4(\mathbf{R})$. Le quaternion $q := u(1)$ vérifie $\mathrm{N}(q) = 1$. On a $\psi_{\bar{q},1} \circ u(1) = \bar{q}q = 1$, donc l'isométrie $\psi_{\bar{q},1} \circ u$ laisse $\mathbf{R}$, donc aussi $\mathbf{R}^\perp = \mathrm{Im}(\mathbf{H})$, stable. Par le théorème précédent, il existe q' de norme 1 tel que $\psi_{\bar{q},1} \circ u = \phi_{q'} = \psi_{q',q'}$, c'est-à-dire $u = \psi_{\bar{q},1}^{-1} \circ \psi_{q',q'} = \psi_{qq',q'}$. Ceci montre que ψ est surjectif.

2° En composant ψ par la surjection sur $\mathrm{PSO}_4(\mathbf{R}) = \mathrm{SO}_4(\mathbf{R})/\{\pm \mathrm{I}_4\}$, on obtient un morphisme surjectif

$$\tilde{\psi} : \mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C}) \longrightarrow \mathrm{PSO}_4(\mathbf{R}).$$

Son noyau est constitué des (q_1, q_2) tels que $q_1 x = \varepsilon x q_2$ pour tout $x \in \mathbf{H}$, où $\varepsilon = \pm 1$. Pour $\varepsilon = 1$, on récupère le noyau de ψ ; pour $\varepsilon = -1$, on obtient (en faisant $x = -1$) $q_2 = -q_1$ puis $q_1 x = x q_1$ pour tout $x \in \mathbf{H}$, donc $q_1 = \pm 1$, ce qui rajoute au noyau les éléments $(1,-1)$ et $(-1,1)$. Le noyau de $\tilde{\psi}$ est donc constitué des quatre éléments $(\pm 1, \pm 1)$, donc $\mathrm{PSO}_4(\mathbf{R}) \simeq \mathrm{PSU}_2(\mathbf{C}) \times \mathrm{PSU}_2(\mathbf{C}) \simeq \mathrm{SO}_3(\mathbf{R}) \times \mathrm{SO}_3(\mathbf{R})$. □

Remarque 11.4. — Pour tout n, on peut construire (*cf.* § III.6.4) un groupe $\mathrm{Spin}_n(\mathbf{R})$ connexe, muni d'un morphisme de groupes surjectif $\mathrm{Spin}_n(\mathbf{R}) \to \mathrm{SO}_n(\mathbf{R})$ dont le noyau a deux éléments [29]. Il est unique à isomorphisme (de groupes) près.

On a vu $\mathrm{SO}_2(\mathbf{R}) \simeq \mathrm{U}_1(\mathbf{C})$ (ex. 8.2.1°). Le groupe $\mathrm{Spin}_2(\mathbf{R})$ est le groupe $\mathrm{U}_1(\mathbf{C})$ des nombres complexes de module 1, mais le morphisme $\mathrm{Spin}_2(\mathbf{R}) \to \mathrm{SO}_2(\mathbf{R})$ est l'élévation au carré.

Le th. 11.2 entraîne $\mathrm{Spin}_3(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C})$, et le th. 11.3 entraîne $\mathrm{Spin}_4(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C})$.

On peut montrer $\mathrm{Spin}_6(\mathbf{R}) \simeq \mathrm{SU}_4(\mathbf{C})$, c'est-à-dire qu'on a un morphisme surjectif $\mathrm{SU}_4(\mathbf{C}) \to \mathrm{SO}_6(\mathbf{R})$ dont le noyau est d'ordre 2 (exerc. III.4.11).

Cette construction peut aussi être effectuée dans le cas d'une forme quadratique (non dégénérée) quelconque sur $\mathbf{R}^n$ (rem. III.6.11). On obtient alors un groupe $\mathrm{Spin}'_{s,t}(\mathbf{R})$ qui est un revêtement (connexe) de degré 2 du groupe connexe $\mathrm{SO}'_{s,t}(\mathbf{R})$ (d'indice 2 dans $\mathrm{SO}_{s,t}(\mathbf{R})$) défini dans l'ex. 8.12.3° (*cf.* exerc. III.4.10).

Exercice 11.5. — Soit $\mathbf{K}$ un corps de caractéristique différente de 2 et soit V l'espace vectoriel (de dimension 4) des matrices 2×2 à coefficients dans $\mathbf{K}$.
a) Montrer que $f : \mathrm{M} \mapsto \mathrm{tr}(\mathrm{M}^2)$ est une forme quadratique sur V.
b) Montrer que $\mathrm{SL}_2(\mathbf{K})$ agit par isométries sur V par $\mathrm{P} \cdot \mathrm{M} := \mathrm{PMP}^{-1}$ et que ces isométries laissent toutes stable l'espace vectoriel $\mathrm{W} := \mathrm{I}_2^{\perp}$ (de dimension 3).
c) Montrer que la restriction de f à W est de type $\langle 1, -1, 2 \rangle$.
d) On en déduit un morphisme $\mathrm{SL}_2(\mathbf{K}) \to \mathrm{O}(\mathrm{W}, f|_{\mathrm{W}})$. Montrer qu'il est surjectif et déterminer son noyau.
e) En déduire que le groupe $\mathrm{Spin}'_{2,1}(\mathbf{R})$ est isomorphe à $\mathrm{SL}_2(\mathbf{R})$.

Exercice 11.6. — Le but de cet exercice est de montrer que le groupe $\mathrm{SO}'_{1,3}(\mathbf{R})$ défini dans l'ex. 8.12.3° est isomorphe à $\mathrm{PSL}_2(\mathbf{C})$. En particulier, $\mathrm{Spin}'_{1,3}(\mathbf{R}) \simeq \mathrm{SL}_2(\mathbf{C})$.

Soit V l'espace vectoriel réel des matrices hermitiennes 2×2.
a) Quelle est la dimension de V ?
b) Montrer que $\mathrm{GL}_2(\mathbf{C})$ agit linéairement sur V par la relation $\mathrm{P} \cdot \mathrm{M} = \mathrm{PMP}^*$.
c) Montrer que $\mathrm{SL}_2(\mathbf{C})$ agit par isométries sur V pour la forme quadratique de Lorentz de signature $(1,3)$. On en déduit un morphisme $\phi : \mathrm{SL}_2(\mathbf{C}) \to \mathrm{O}_{1,3}(\mathbf{R})$.
d) Déterminer le noyau de ϕ.
e) Montrer que l'image de ϕ est exactement $\mathrm{SO}'_{1,3}(\mathbf{R})$ et conclure.

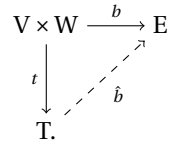
29. On dit que c'est un revêtement de degré 2 de $\mathrm{SO}_n(\mathbf{R})$ et c'est en fait, pour $n \geqslant 3$, le revêtement universel de l'espace topologique $\mathrm{SO}_n(\mathbf{R})$.

CHAPITRE III

ALGÈBRE TENSORIELLE

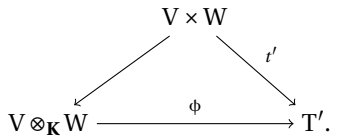
1. Produit tensoriel

Soit **K** un corps et soient V et W des **K**-espaces vectoriels. Un *produit tensoriel* de V et W est la donnée d'un **K**-espace vectoriel T et d'une application bilinéaire $t : V \times W \to T$ satisfaisant la propriété universelle suivante : si $b : V \times W \to E$ est une application bilinéaire, il existe une *unique* application *linéaire* $\hat{b} : T \to E$ telle que $b = \hat{b} \circ t$. Cela se traduit par le fait que le diagramme suivant est commutatif :



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

Théorème 1.1* (Existence et unicité).** — *Étant donnés des* **K-espaces vectoriels* V *et* W*, il existe un produit tensoriel* $(V \otimes_{\mathbf{K}} W, t)$*, unique au sens suivant : si* (T', t') *est un autre produit tensoriel de* V *et* W*, ils sont isomorphes, c'est-à-dire qu'il existe un isomorphisme* $\phi : V \otimes_{\mathbf{K}} W \to T'$ *unique tel que le diagramme suivant soit commutatif :*



On parle ainsi du *produit tensoriel de* V *et* W*. L'application bilinéaire* $t : V \times W \to V \otimes_{\mathbf{K}} W$ *est notée* $(v, w) \mapsto v \otimes w$*. Un élément de* $V \otimes_{\mathbf{K}} W$ *du type* $v \otimes w$ *est appelé* tenseur décomposable *; les tenseurs décomposables engendrent* $V \otimes_{\mathbf{K}} W$*.*

On notera la plupart du temps $V \otimes W$ au lieu de $V \otimes_{\mathbf{K}} W$.

Démonstration. — Commençons par l'unicité. On applique la propriété universelle pour $V \otimes_{\mathbf{K}} W$ à $t' : V \times W \to T'$, pour déduire l'existence d'une application linéaire $\phi : V \otimes_{\mathbf{K}} W \to T'$ unique telle que $t' = \phi \circ t$. La propriété universelle pour T' fabrique aussi $\psi : T' \to T$ tel que $t = \psi \circ t'$. Appliquant l'unicité dans la propriété universelle à l'application bilinéaire $t : V \times W \to V \otimes_{\mathbf{K}} W$, on déduit $\psi \circ \phi = \mathrm{Id}_{V \otimes_{\mathbf{K}} W}$. De manière analogue, on a $\phi \circ \psi = \mathrm{Id}_{T'}$.

Reste à construire $V \otimes_{\mathbf{K}} W$. Soit $\mathbf{K}^{(V \times W)}$ le $\mathbf{K}$-espace vectoriel de base $(e_{v,w})_{(v,w) \in V \times W}$. Un élément de $\mathbf{K}^{(V \times W)}$ est donc une somme (finie) $\sum \lambda_{v,w} e_{v,w}$ pour des scalaires $\lambda_{v,w}$ presque tous nuls. L'application $V \times W \to \mathbf{K}^{(V \times W)}$ donnée par $(v, w) \mapsto e_{v,w}$ n'est pas bilinéaire, mais elle va le devenir si on compose par la surjection sur un certain quotient $\mathbf{K}^{(V \times W)} \to S$. Pour trouver S, écrivons les relations dont nous avons besoin : pour $v, v' \in V$, $w, w' \in W$, $\lambda, \lambda' \in \mathbf{K}$, les quantités suivantes doivent êtres nulles

$$e_{\lambda v + \lambda' v', w} - \lambda e_{v,w} - \lambda' e_{v',w}, \tag{29}$$

$$e_{v, \lambda w + \lambda' w'} - \lambda e_{v,w} - \lambda' e_{v,w'}. \tag{30}$$

Il est donc naturel de définir S comme le sous-espace vectoriel de $\mathbf{K}^{(V \times W)}$ engendré par toutes les expressions (29) et (30) et de poser

$$T := \mathbf{K}^{(V \times W)} / S.$$

On définit maintenant l'application bilinéaire $t : V \times W \to T$ comme la composée

$$V \times W \longrightarrow \mathbf{K}^{(V \times W)} \twoheadrightarrow \mathbf{K}^{(V \times W)} / S = T.$$

Elle associe à (v, w) la classe, qu'on note $v \otimes w$, de $e_{v,w}$ dans le quotient T. Puisque $\mathbf{K}^{(V \times W)}$ est engendré par les $e_{v,w}$, son quotient T est engendré par les éléments de type $v \otimes w$, c'est-à-dire par les tenseurs décomposables.

Pour montrer qu'on a ainsi obtenu le produit tensoriel de V et W, il reste à montrer la propriété universelle : si on a une application bilinéaire $b : V \times W \to E$, on peut définir une application linéaire $g : \mathbf{K}^{(V \times W)} \to E$ en posant $g(e_{v,w}) = b(v, w)$. Puisque b est bilinéaire, g s'annule sur le sous-espace S et passe donc au quotient pour donner une application linéaire $\hat{b} : T \to E$. L'identité $b = \hat{b} \circ t$ est claire et l'unicité de $\hat{b}$ provient du fait que T est engendré par les $v \otimes w$; or l'image de $v \otimes w$ par $\hat{b}$ est déterminée, puisque ce doit être $b(v, w)$. □

Corollaire 1.2. — *Soient* V, W *et* E *des* $\mathbf{K}$*-espaces vectoriels. L'espace vectoriel des applications bilinéaires* $V \times W \to E$ *est isomorphe à* $\mathrm{Hom}(V \otimes W, E)$. *En particulier, l'espace des formes bilinéaires sur* $V \times W$ *est isomorphe à* $(V \otimes W)^*$.

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

***Proposition 1.3* (Fonctorialité).** — *Si on a des applications linéaires* $f : V_1 \to V_2$ *et* $g : W_1 \to W_2$, *il existe une et une seule application linéaire* $f \otimes g : V_1 \otimes W_1 \to V_2 \otimes W_2$ *telle que* $(f \otimes g)(v \otimes w) = f(v) \otimes g(w)$ *pour tous* v, w.

En outre, $(f_2 \otimes g_2) \circ (f_1 \otimes g_1) = (f_2 \circ f_1) \otimes (g_2 \circ g_1)$.

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

$$\begin{array}{ccc} \mathrm{V}_1 \times \mathrm{W}_1 & \xrightarrow{f \times g} & \mathrm{V}_2 \times \mathrm{W}_2 \\ \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle t'} \\ \mathrm{V}_1 \otimes \mathrm{W}_1 & \overset{f \otimes g}{\dashrightarrow} & \mathrm{V}_2 \otimes \mathrm{W}_2. \end{array}$$

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

La seconde assertion résulte de la propriété d'unicité de la première assertion appliquée à $(f_2 \circ f_1) \otimes (g_2 \circ g_1)$. Les détails sont laissés au lecteur. □

Propriétés du produit tensoriel 1.4. — *Soient* U, V *et* W *des* **K***-espaces vectoriels. On a*

$$\begin{aligned} \mathbf{K} \otimes \mathrm{V} &\xrightarrow{\sim} \mathrm{V} & \lambda \otimes v &\longmapsto \lambda v, \\ (\mathrm{U} \oplus \mathrm{V}) \otimes \mathrm{W} &\xrightarrow{\sim} (\mathrm{U} \otimes \mathrm{W}) \oplus (\mathrm{V} \otimes \mathrm{W}) & (u+v) \otimes w &\longmapsto u \otimes w + v \otimes w, \\ \mathrm{U} \otimes \mathrm{V} &\xrightarrow{\sim} \mathrm{V} \otimes \mathrm{U} & u \otimes v &\longmapsto v \otimes u, \\ \mathrm{U} \otimes (\mathrm{V} \otimes \mathrm{W}) &\xrightarrow{\sim} (\mathrm{U} \otimes \mathrm{V}) \otimes \mathrm{W} & u \otimes (v \otimes w) &\longmapsto (u \otimes v) \otimes w. \end{aligned}$$

Attention : la colonne de droite ne définit les isomorphismes que sur les tenseurs décomposables, alors que tous les tenseurs ne le sont pas. Mais ces applications sont linéaires, donc elles sont uniquement déterminées par leur valeur sur ces tenseurs particuliers.

Démonstration. — L'application $\mathbf{K} \times \mathrm{V} \to \mathrm{V}$ donnée par $(\lambda, v) \mapsto \lambda v$ est bilinéaire, donc il y a une application linéaire induite $\mathbf{K} \otimes \mathrm{V} \to \mathrm{V}$, qui envoie $\lambda \otimes v$ sur λv. L'inverse est $v \mapsto 1 \otimes v$, d'où le premier l'isomorphisme.

Pour le deuxième isomorphisme, montrons la généralisation suivante : soit $(\mathrm{V}_i)_{i \in \mathrm{I}}$ une famille d'espaces vectoriels ; l'application

$$\begin{aligned} \Big(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\Big) \times \mathrm{W} &\longrightarrow \bigoplus_{i \in \mathrm{I}} (\mathrm{V}_i \otimes \mathrm{W}) \\ \Big(\sum_{i \in \mathrm{I}} v_i, w\Big) &\longmapsto \sum_{i \in \mathrm{I}} v_i \otimes w \end{aligned}$$

est bilinéaire. Elle se factorise donc en

$$\Big(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\Big) \times \mathrm{W} \longrightarrow \Big(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\Big) \otimes \mathrm{W} \xrightarrow{\phi} \bigoplus_{i \in \mathrm{I}} (\mathrm{V}_i \otimes \mathrm{W}).$$

Inversement, les injections canoniques $\iota_i : \mathrm{V}_i \longrightarrow \bigoplus_{i \in \mathrm{I}} \mathrm{V}_i$ induisent par la prop. 1.3 des applications linéaires $\iota_i \otimes \mathrm{Id}_\mathrm{W} : \mathrm{V}_i \otimes \mathrm{W} \longrightarrow \Big(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\Big) \otimes \mathrm{W}$, donc une application linéaire

$$\bigoplus_{i \in \mathrm{I}} (\iota_i \otimes \mathrm{Id}_\mathrm{W}) : \bigoplus_{i \in \mathrm{I}} (\mathrm{V}_i \otimes \mathrm{W}) \longrightarrow \Big(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\Big) \otimes \mathrm{W}$$

qui est un inverse de ϕ. On a donc un isomorphisme canonique

$$\Big(\bigoplus_{i \in \mathrm{I}} \mathrm{V}_i\Big) \otimes \mathrm{W} \xrightarrow{\sim} \bigoplus_{i \in \mathrm{I}} (\mathrm{V}_i \otimes \mathrm{W}). \tag{31}$$

Les autres isomorphismes se démontrent de façon similaire. □

Si $(v_i)_{i\in \mathrm{I}}$ est une base de V, on a $\mathrm{V} \simeq \bigoplus_{i\in \mathrm{I}} \mathbf{K} v_i$ et on déduit de (31) un isomorphisme

$$\mathrm{V}\otimes \mathrm{W} \simeq \bigoplus_{i\in \mathrm{I}} \mathbf{K} v_i \otimes \mathrm{W}.$$

Tout élément de $\mathrm{V}\otimes \mathrm{W}$ s'écrit donc de manière unique $\sum_{i\in \mathrm{I}} v_i \otimes w'_i$, où $(w'_i)_{i\in \mathrm{I}}$ est une famille presque nulle d'éléments de W.

De même, si $(w_j)_{j\in \mathrm{J}}$ est une base de W, on a $\mathrm{V} \simeq \bigoplus_{i\in \mathrm{I}} \mathbf{K} v_i$ et on déduit de (31) un isomorphisme

$$\mathrm{V}\otimes \mathrm{W} \simeq \bigoplus_{j\in \mathrm{J}} \mathbf{K} v'_j \otimes \mathrm{W}.$$

Tout élément de $\mathrm{V}\otimes \mathrm{W}$ s'écrit donc de manière unique $\sum_{j\in \mathrm{J}} v'_j \otimes w_j$, où $(v'_j)_{j\in \mathrm{J}}$ est une famille presque nulle d'éléments de V.

On a aussi un isomorphisme

$$\mathrm{V}\otimes \mathrm{W} \simeq \bigoplus_{i\in \mathrm{I},\, j\in \mathrm{J}} \mathbf{K} v_i \otimes w_j,$$

ce qui signifie que $(v_i \otimes w_j)_{(i,j)\in \mathrm{I}\times \mathrm{J}}$ est une base de $\mathrm{V}\otimes \mathrm{W}$. En particulier, on a

$$\dim(\mathrm{V}\otimes \mathrm{W}) = \dim(\mathrm{V})\dim(\mathrm{W}).$$

Si V_1 a pour base $(v_{1,j})_{j\in \mathrm{I}_1}$, V_2 a pour base $(v_{2,i})_{i\in \mathrm{I}_2}$, W_1 a pour base $(w_{1,l})_{l\in \mathrm{J}_1}$ et W_2 a pour base $(w_{2,k})_{k\in \mathrm{J}_2}$ et qu'on a des applications linéaires $f : \mathrm{V}_1 \to \mathrm{V}_2$ et $g : \mathrm{W}_1 \to \mathrm{W}_2$ de matrices respectives $\mathrm{A} = (a_{ij})_{i\in \mathrm{I}_2,\, j\in \mathrm{I}_1}$ et $\mathrm{B} = (b_{kl})_{k\in \mathrm{J}_2,\, l\in \mathrm{J}_1}$ dans ces bases, alors

$$(f\otimes g)(v_{1,j}\otimes w_{1,l}) = \sum_{i\in \mathrm{I}_2,\, k\in \mathrm{J}_2} a_{ij} b_{kl}\, v_{2,i}\otimes w_{2,k},$$

de sorte que la matrice de $f\otimes g$ dans les bases $(v_{1,j}\otimes w_{1,l})_{(j,l)\in \mathrm{I}_1\times \mathrm{J}_1}$ de $\mathrm{V}_1\otimes \mathrm{W}_1$ et $(v_{2,i}\otimes w_{2,k})_{(i,k)\in \mathrm{I}_2\times \mathrm{J}_2}$ de $\mathrm{V}_2\otimes \mathrm{W}_2$ est

$$\mathrm{A}\otimes \mathrm{B} := (a_{ij} b_{kl})_{(i,k)\in \mathrm{I}_2\times \mathrm{J}_2,\,(j,l)\in \mathrm{I}_1\times \mathrm{J}_1}.$$

Par exemple, si $\mathrm{V}_1, \mathrm{V}_2, \mathrm{W}_1, \mathrm{W}_2$ sont tous de dimension 2 et qu'on choisit sur $\{1,2\}\times\{1,2\}$ l'ordre $(1,1),(1,2),(2,1),(2,2)$, la matrice est

$$\mathrm{A}\otimes \mathrm{B} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}\mathrm{B} & a_{12}\mathrm{B} \\ a_{21}\mathrm{B} & a_{22}\mathrm{B} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{12}b_{11} & a_{12}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{12}b_{21} & a_{12}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

On appelle aussi cette matrice le *produit de Kronecker* des matrices A et B (on le définit de façon analogue pour des matrices de taille quelconque). Noter qu'il n'est pas commutatif (parce que l'ordre sur $\{1,2\}\times\{1,2\}$ n'est pas invariant par permutation des deux facteurs), mais que la matrice $\mathrm{B}\otimes \mathrm{A}$ est simplement obtenue à partir de $\mathrm{A}\otimes \mathrm{B}$ en faisant des permutations de lignes et de colonnes.

Exercice 1.5. — Montrer les relations

$$\mathrm{rg}(\mathrm{A}\otimes \mathrm{B}) = \mathrm{rg}(\mathrm{A})\,\mathrm{rg}(\mathrm{B}), \quad \mathrm{tr}(\mathrm{A}\otimes \mathrm{B}) = \mathrm{tr}(\mathrm{A})\,\mathrm{tr}(\mathrm{B}), \quad \det(\mathrm{A}\otimes \mathrm{B}) = \det(\mathrm{A})^b \det(\mathrm{B})^a$$

où, dans les deux dernières égalités, A est carrée d'ordre a et B carrée d'ordre b.

Exemples 1.6. — 1° L'application

$$\begin{aligned} \psi : V^* \otimes W &\longrightarrow \mathrm{Hom}(V,W) \\ \alpha \otimes w &\longmapsto (v \mapsto \alpha(v)w) \end{aligned} \tag{32}$$

est linéaire. Elle est injective : en effet, si $(w_j)_{j\in J}$ est une base de W, on a vu que tout élément de $V^* \otimes W$ s'écrit $\sum_{j\in J} \alpha_j \otimes w_j$, où $(\alpha_j)_{j\in J}$ est une famille presque nulle d'éléments de V^*. Si son image est nulle, c'est que $\sum_{j\in J} \alpha_j(v)w_j = 0$ pour tout $v \in V$, ce qui entraîne $\alpha_j(v) = 0$ pour tout $j \in J$, pusique $(w_j)_{j\in J}$ est une base de W. On a donc $\alpha_j = 0$ pour tout $j \in J$.

L'application ψ n'est pas toujours surjective : son image consiste en fait en les applications linéaires de rang fini. Elle est donc surjective si et seulement si V ou W est de dimension finie. Concrètement, si par exemple V est dimension finie et que $(v_i)_{1\leqslant i\leqslant n}$ en est une base, de base duale $(v^i)_{1\leqslant i\leqslant n}$, on a pour $f \in \mathrm{Hom}(V,W)$ la formule

$$\psi^{-1}(f) = \sum_{i=1}^{n} v^i \otimes f(v_i).$$

2° Le produit tensoriel $\mathbf{K}[X] \otimes \mathbf{K}[Y]$ est isomorphe à $\mathbf{K}[X,Y]$, par l'application $X^i \otimes Y^j \mapsto X^i Y^j$ [1].

3° On peut définir plus généralement le produit tensoriel de modules sur un anneau commutatif A. La construction est la même que sur un corps, mais son comportement est plus compliqué. Si $A = \mathbf{Z}$, les A-modules sont les groupes abéliens et on a par exemple $\mathbf{Z}^k \otimes_{\mathbf{Z}} \mathbf{Z}^l = \mathbf{Z}^{kl}$, mais aussi $(\mathbf{Z}/n\mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{Q} = 0$, $(\mathbf{Z}/3\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/2\mathbf{Z}) = 0$ et $(\mathbf{Z}/3\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/3\mathbf{Z}) = \mathbf{Z}/3\mathbf{Z}$ (pourquoi ?).

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

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

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

Un endomorphisme $u \in \mathrm{End}_{\mathbf{K}}(V)$ s'étend en $u^{\mathbf{L}} = \mathrm{Id}_{\mathbf{L}} \otimes u \in \mathrm{End}_{\mathbf{L}}(V^{\mathbf{L}})$. Si u a comme matrice A dans une $\mathbf{K}$-base (v_i) de V, alors $u^{\mathbf{L}}$ a la même matrice A dans la $\mathbf{L}$-base $(1 \otimes v_i)$ de $V^{\mathbf{L}}$.

Par exemple, si $\mathbf{K} = \mathbf{R}$ et $\mathbf{L} = \mathbf{C}$, alors $V^{\mathbf{C}} = \mathbf{C} \otimes_{\mathbf{R}} V$ est la *complexification* de l'espace vectoriel réel V.

Exercice 1.7. — Soient V et W des espaces vectoriels de dimension finie.
a) Quelle est l'image de l'ensemble des tenseurs décomposables par l'application (32) de l'ex. 1.6 ?
b) On sait que tout élément de $V \otimes W$ peut s'écrire comme somme de tenseurs décomposables. Quel est le nombre maximal de tenseurs décomposables dont on a besoin ?

1. Mais attention : $\mathbf{K}(X) \otimes \mathbf{K}(Y)$ n'est pas isomorphe à $\mathbf{K}(X,Y)$ (pourquoi ?) !

Exercice 1.8. — Soit f_1 (resp. f_2) une forme quadratique sur un $\mathbf{K}$-espace vectoriel V_1 (resp. V_2) de dimension finie .
a) Montrer qu'il existe une unique forme quadratique $f_1 \otimes f_2$ sur $V_1 \otimes V_2$ qui vérifie

$$\forall v_1, v_2 \in V \qquad (f_1 \otimes f_2)(v_1 \otimes v_2) = f_1(v_1) f_2(v_2).$$

b) Montrer que si f_1 et f_2 sont non dégénérées, il en est de même de $f_1 \otimes f_2$.
c) Avec les notations de § II.4.2, montrer que

$$\langle \alpha_1, \dots, \alpha_m \rangle \otimes \langle \beta_1, \dots, \beta_n \rangle = \langle \alpha_i \beta_j, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n \rangle.$$

d) Si (V_2, f_2) est somme de plans hyperboliques, montrer qu'il en est de même pour $(V_1 \otimes V_2, f_1 \otimes f_2)$.
e) En déduire que le produit tensoriel des formes quadratiques définit une structure d'anneau sur le groupe de Witt $W(\mathbf{K})$ (§ II.6).

Exercice 1.9. — a) Rappeler la structure de $\mathbf{R}$-algèbre de $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}$.
b) Montrer qu'il y a deux structures de $\mathbf{C}$-algèbre non isomorphes sur $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}$.
c) Montrer que les $\mathbf{C}$-algèbres $\mathscr{M}_2(\mathbf{C})$ et $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{C}$ sont isomorphes ($\mathbf{H}$ est le corps des quaternions, *cf.* § II.11).
d) Montrer que les $\mathbf{R}$-algèbres $\mathbf{H} \otimes_{\mathbf{R}} \mathbf{H}$ et $\mathscr{M}_4(\mathbf{R})$ sont isomorphes.

2. Algèbre tensorielle

2.1. Applications d-linéaires. — Soient $V_1, \dots, V_d, E$ des $\mathbf{K}$-espaces vectoriels. Une application *d-linéaire* $V_1 \times \cdots \times V_d \to E$ est une application qui est linéaire par rapport à chacun des facteurs V_i. On peut construire comme dans le th. 1.1 un $\mathbf{K}$-espace vectoriel $V_1 \otimes \cdots \otimes V_d$ et une application d-linéaire universelle

$$V_1 \times \cdots \times V_d \to V_1 \otimes \cdots \otimes V_d.$$

L'espace vectoriel $\mathrm{Mult}^d(V_1 \times \cdots \times V_d, E)$ des applications d-linéaires de $V_1 \times \cdots \times V_d$ vers E est alors isomorphe à l'espace vectoriel $\mathrm{Hom}(V_1 \otimes \cdots \otimes V_d, E)$.

On a vu dans la section précédente (prop. 1.4) que $(V_1 \otimes V_2) \otimes V_3$ et $V_1 \otimes (V_2 \otimes V_3)$ sont canoniquement isomorphes. On vérifie facilement qu'ils le sont aussi à $V_1 \otimes V_2 \otimes V_3$.

De la même manière que pour le produit tensoriel, si on a des applications linéaires $f_i : V_i \to W_i$, on obtient une application linéaire unique

$$f_1 \otimes \cdots \otimes f_d : V_1 \otimes \cdots \otimes V_d \longrightarrow W_1 \otimes \cdots \otimes W_d$$

qui vérifie sur les tenseurs décomposables la relation

$$(f_1 \otimes \cdots \otimes f_d)(v_1 \otimes \cdots \otimes v_d) = f_1(v_1) \otimes \cdots \otimes f_d(v_d).$$

Remarque 2.1. — Soient $V_1, \dots, V_d$ des espaces vectoriels de dimension finie. Tout élément de $V_1 \otimes \cdots \otimes V_d$ peut donc s'écrire comme somme de tenseurs décomposables. On peut se poser la question de savoir le nombre maximal de tenseurs décomposables dont on a besoin. Lorsque $d = 2$, c'est l'objet de l'exerc. 1.7. En général, on ne connaît la réponse à cette importante question que dans certains cas.

2.2. Algèbres graduées. — Rappelons qu'une **K**-*algèbre* est un **K**-espace vectoriel A muni d'un produit $A \times A \to A$ qui est une application bilinéaire et qui fait de A un anneau. Elle est donc associative, mais pas nécessairement commutative. Toutes les algèbres que nous considérerons seront munies d'une unité, c'est-à-dire d'un élément 1 tel que $a \cdot 1 = 1 \cdot a = a$ pour tout $a \in A$. On a $1 = 0$ si et seulement si $A = 0$.

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

$$A = \bigoplus_{d \in \mathbf{N}} A_d$$

en somme directe d'espaces vectoriels telle que

$$\forall d, e \in \mathbf{N} \qquad A_d \cdot A_e \subseteq A_{d+e}.$$

Si A a une unité, on a $1 \in A_0$.

Par exemple, l'algèbre $\mathbf{K}[X]$ des polynômes à une indéterminée est graduée par $\mathbf{K}[X] = \bigoplus \mathbf{K}X^d$. L'algèbre (commutative) $A = \mathbf{K}[X_1, \dots, X_r]$ des polynômes à plusieurs indéterminés est également graduée si on définit A_d comme le sous-espace vectoriel des polynômes nuls ou homogènes de degré total d, donc engendré par les $X_1^{i_1} \cdots X_r^{i_r}$ pour $i_1 + \cdots + i_r = d$.

Un élément non nul $x \in A$ est dit *homogène* s'il existe d tel que $x \in A_d$; on dit alors que x est de degré d.

Un *morphisme d'algèbres graduées* est un morphisme d'algèbres $f : A \to B$ qui préserve la graduation : $f(A_d) \subseteq B_d$ pour tout $d \in \mathbf{N}$.

2.3. Algèbre tensorielle. — On définit les *puissances tensorielles* d'un espace vectoriel V par $T^0V = \mathbf{K}$ et, pour $d \geqslant 1$,

$$T^dV := \underbrace{V \otimes \cdots \otimes V}_{d \text{ fois}} =: V^{\otimes d}.$$

On peut voir aussi (canoniquement et par définition) T^dV comme le dual de $\mathrm{Mult}^d(V^d, \mathbf{K})$, l'espace vectoriel des formes d-linéaires sur V.

L'*algèbre tensorielle* de V est définie par

$$TV = \bigoplus_{n \in \mathbf{N}} T^dV. \tag{33}$$

Pour en faire une algèbre, nous devons définir un produit sur TV. C'est

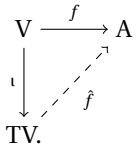
$$\begin{array}{ccc} T^dV \times T^eV & \longrightarrow & T^{d+e}V \\ (v_1 \otimes \cdots \otimes v_d, w_1 \otimes \cdots \otimes w_e) & \longmapsto & v_1 \otimes \cdots \otimes v_d \otimes w_1 \otimes \cdots \otimes w_e. \end{array}$$

Compte tenu des propriétés du produit tensoriel vues plus haut, ce produit est associatif et fait de TV une algèbre, munie de l'unité $1 \in \mathbf{K} = T^0V$. Cette algèbre n'est pas commutative dès que $\dim(V) \geqslant 2$: on a $v_1 \otimes v_2 \neq v_2 \otimes v_1$ dès que v_1 et v_2 ne sont pas proportionnels.

La décomposition (33) en fait une algèbre graduée. Noter la présence d'une injection canonique $\iota : V \hookrightarrow TV$ puisque T^1V s'identifie à V.

Si V a pour base $(e_i)_{i \in I}$, alors TV a pour base les $e_{i_1} \otimes \cdots \otimes e_{i_d}$ pour $d \in \mathbf{N}$ et $i_1, \dots, i_d \in I$. Même si l'espace vectoriel V est de dimension finie, l'espace vectoriel TV est toujours de dimension infinie dès que $V \neq 0$.

***Proposition 2.2* (Propriété universelle).** — *L'algèbre tensorielle* TV *satisfait la propriété universelle suivante : si* $f : \mathrm{V} \to \mathrm{A}$ *est une application linéaire vers une algèbre avec unité* A*, il existe un morphisme d'algèbres* $\hat{f} : \mathrm{TV} \to \mathrm{A}$ *unique tel que* $f = \hat{f} \circ \iota$*, c'est-à-dire que le diagramme suivant est commutatif :*



Démonstration. — Comme l'application

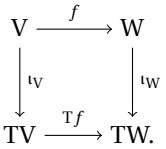
$$\begin{aligned} \mathrm{V}^d &\longrightarrow \mathrm{A} \\ (v_1, \dots, v_d) &\longmapsto f(v_1) \cdots f(v_d) \end{aligned}$$

est d-linéaire, la propriété universelle de $\mathrm{T}^d\mathrm{V}$ permet de définir l'application linéaire $\hat{f} : \mathrm{T}^d\mathrm{V} \to \mathrm{A}$. Reste à montrer que c'est bien un morphisme d'algèbres. Il suffit de le vérifier sur les tenseurs décomposables, qui engendrent TV ; or on a

$$\begin{aligned} \hat{f}((v_1 \otimes \cdots \otimes v_d) \otimes (w_1 \otimes \cdots \otimes w_e)) &= f(v_1) \cdots f(v_d) f(w_1) \cdots f(w_e) \\ &= \hat{f}(v_1 \otimes \cdots \otimes v_d) \hat{f}(w_1 \otimes \cdots \otimes w_e), \end{aligned}$$

ce qui montre ce qu'on veut. □

Comme dans tous les cas précédents, la propriété universelle implique la fonctorialité de la construction : si on a une application linéaire $f : \mathrm{V} \to \mathrm{W}$, il y a un morphisme d'algèbres, 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 $\bigoplus \mathrm{T}^d f$, où $\mathrm{T}^d f = f^{\otimes d}$ est $\underbrace{f \otimes \cdots \otimes f}_{d \text{ fois}}$, défini plus haut. En outre, on a la propriété

$$\mathrm{T}(f \circ g) = \mathrm{T}f \circ \mathrm{T}g.$$

2.4. Tenseurs covariants et contravariants. — Ce paragraphe une tentative pour expliquer le language et les notations utilisés en physique (et parfois aussi en géométrie différentielle). Soit V un espace vectoriel et soit V^* son espace vectoriel dual, c'est-à-dire $\mathrm{Hom}(\mathrm{V}, \mathbf{K})$. Les « tenseurs » considérés par les physiciens sont en général des éléments d'un produit tensoriel

$$\underbrace{\mathrm{V}^* \otimes \cdots \otimes \mathrm{V}^*}_{p \text{ fois}} \otimes \underbrace{\mathrm{V} \otimes \cdots \otimes \mathrm{V}}_{q \text{ fois}} = \mathrm{T}^p\mathrm{V}^* \otimes \mathrm{T}^q\mathrm{V}.$$

Un tel tenseur T est dit « p fois covariant et q fois contravariant ». Si on choisit une base $(e_1,\dots,e_n)$ de V, de base duale $(e^1,\dots,e^n)$ de V^*, on écrit les coordonnées de T comme $T^{i_1\dots i_q}_{j_1\dots j_p}$. Dans notre language, cela signifie

$$T = \sum_{i_1,\dots,i_q,j_1,\dots,j_p} T^{i_1\dots i_q}_{j_1\dots j_p}\, e^{j_1}\otimes\cdots\otimes e^{j_p}\otimes e_{i_1}\otimes\cdots\otimes e_{i_q}$$

(on remarque que la famille des $e^{j_1}\otimes\cdots\otimes e^{j_p}\otimes e_{i_1}\otimes\cdots\otimes e_{i_q}$ est une base de $T^pV^*\otimes T^qV$). En physique, on utilise la convention de sommation d'Einstein et on écrit simplement

$$T = T^{i_1\dots i_q}_{j_1\dots j_p}\, e^{j_1}\otimes\cdots\otimes e^{j_p}\otimes e_{i_1}\otimes\cdots\otimes e_{i_q}$$

(il est entendu qu'on somme sur les indices répétés en haut et en bas). On dit que les $T^{i_1\dots i_q}_{j_1\dots j_p}$ sont les coordonnées du tenseur T.

Soit $v = v^j e_j$ un élément de V. Dans une autre base $(e'_1,\dots,e'_n)$, définie par la matrice de passage $P = (P^j_i)$ et $e'_i = P^j_i e_j$, on a $v = v'^i e'_i$, avec

$$v = v'^i e'_i = v'^i P^j_i e_j,$$

d'où $v^j = P^j_i v'^i$, ou encore

$$v'^i = (P^{-1})^i_j v^j.$$

On dit que les coordonnées de v se transforment en sens inverse des vecteurs de base (d'où la terminologie « contravariant »). Inversement, pour une forme linéaire $\alpha = \alpha_j e^j = \alpha'_i e'^i$, on a

$$\alpha'_i = \alpha(e'_i) = \alpha(P^j_i e_j) = P^j_i \alpha_j.$$

Les composantes de α se transforment donc dans le même sens que les vecteurs de base (d'où la terminologie « covariant »). Pour un tenseur général $T = (T^{i_1\dots i_q}_{j_1\dots j_p})$ qui est p fois covariant et q fois contravariant, on vérifie que ses coordonnées dans la base $(e'_1,\dots,e'_d)$ sont

$$(T')^{i'_1\dots i'_q}_{j'_1\dots j'_p} = (P^{-1})^{i'_1}_{i_1}\cdots(P^{-1})^{i'_q}_{i_q} P^{j_1}_{j'_1}\cdots P^{j_p}_{j'_p} T^{i_1\dots i_q}_{j_1\dots j_p}.$$

Tout cela a en général lieu en présence d'une « métrique », c'est-à-dire d'une forme bilinéaire B non dégénérée sur V (produit scalaire ou forme de Lorentz ; *cf.* exerc. II.11.6).

On appelle B le *tenseur métrique* (par le cor. 1.2, on peut voir B comme un élément de $(V\otimes V)^*\simeq V^*\otimes V^*$, donc comme un tenseur 2 fois covariant) et on le note par sa matrice $g_{ij} = B(e_i,e_j)$ dans la base $(e_1,\dots,e_n)$ de V. Comme la forme B est non dégénérée, elle induit un isomorphisme $\hat{B} : V \xrightarrow{\sim} V^*$ (prop. II.3.2) qui identifie les vecteurs (contravariants) aux formes linéaires (covariantes). En coordonnées, on a $\hat{B}(e_j)(e_i) = B(e_j,e_i) = g_{ji}$, d'où

$$\hat{B}(v^j e_j) = v^j g_{ji} e^i.$$

On passe donc des coordonnées contravariantes (v^j) aux coordonnées covariantes (v_i) par la formule $v_i = v^j g_{ji}$. On peut faire le même genre de manipulations avec les tenseurs. L'exercice est laissé au lecteur.

L'isomorphisme $\hat{B}$ permet aussi de transporter la métrique B en une métrique B^* sur V^*. On vérifie que la matrice $g^{ij} := B^*(e^i,e^j)$ de B^* dans la base duale $(e^1,\dots,e^d)$ de V^* est la matrice inverse de la matrice (g_{ij}), c'est-à-dire $g_{ij}g^{jk} = \delta^k_i$. Ce « tenseur métrique

dual » permet de passer des coordonnées covariantes aux coordonnées contravariantes par la formule $v^j = v_i g^{ij}$. Finalement, le produit scalaire s'écrit

$$\mathrm{B}(u,v) = u^i v_i = u_i v^i = g_{ij} u^i v^j = g^{ij} u_i v_j.$$

3. Algèbre extérieure

On a introduit dans la section précédente l'algèbre tensorielle $\mathrm{TV} = \bigoplus \mathrm{T}^d\mathrm{V}$, où $\mathrm{T}^d\mathrm{V}$ est canoniquement le dual de $\mathrm{Mult}^d(\mathrm{V}^d, \mathbf{K})$ (les formes d-linéaires sur V). Dans cette section, nous faisons une construction analogue pour l'espace vectoriel $\mathrm{Alt}^d(\mathrm{V})$ des *formes d-linéaires alternées* sur V, c'est-à-dire satisfaisant $a(v_1,\dots,v_d) = 0$ dès qu'au moins deux des vecteurs $v_1,\dots,v_d$ sont égaux.

L'algèbre extérieure $\bigwedge \mathrm{V}$, avec une inclusion $\iota : \mathrm{V} \hookrightarrow \bigwedge \mathrm{V}$, sera la solution du problème universel pour les applications linéaires $f : \mathrm{V} \to \mathrm{A}$ de V vers une algèbre avec unité A, satisfaisant l'identité

$$f(v)^2 = 0. \tag{34}$$

Compte tenu de la propriété universelle de l'algèbre TV, l'injection ι doit se factoriser via TV ; en même temps, comme dans les cas précédents, $\bigwedge \mathrm{V}$ sera engendrée par les images des tenseurs décomposables. Il est donc légitime de chercher $\bigwedge \mathrm{V}$ comme quotient de TV, sous la forme [2]

$$\bigwedge \mathrm{V} := \mathrm{TV}/\mathrm{I}.$$

Il faut mettre dans l'idéal I tout ce dont on a besoin pour factoriser les applications satisfaisant (34). Les éléments de la forme $v \otimes v$, pour $v \in \mathrm{V}$ sont de ce type, puisqu'ils sont envoyés sur 0. Il est alors naturel de définir $\mathrm{I} \subseteq \mathrm{TV}$ comme l'idéal bilatère engendré par les éléments de type $v \otimes v$, pour $v \in \mathrm{V}$, c'est-à-dire l'ensemble des sommes finies d'éléments de TV du type

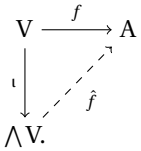
$$a \otimes v \otimes v \otimes b,$$

pour $v \in \mathrm{V}$ et $a, b \in \mathrm{TV}$, et l'*algèbre extérieure* par

$$\bigwedge \mathrm{V} = \mathrm{TV}/\mathrm{I}.$$

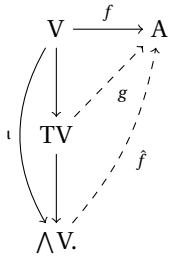
La composition $\mathrm{V} \hookrightarrow \mathrm{TV} \to \mathrm{TV}/\mathrm{I}$ fournit l'application $\iota : \mathrm{V} \to \bigwedge \mathrm{V}$.

Proposition 3.1. — *L'algèbre extérieure satisfait la propriété universelle suivante : si $f : \mathrm{V} \to \mathrm{A}$ est une application linéaire vers une algèbre avec unité, telle que $f(v)^2 = 0$ pour tout v, alors f se factorise de manière unique en $f = \hat{f} \circ \iota$, où $\hat{f} : \bigwedge \mathrm{V} \to \mathrm{A}$ est un morphisme d'algèbres :*



2. Comme pour les anneaux, on peut définir le quotient d'une algèbre A par un idéal bilatère I, c'est-à-dire un sous-espace vectoriel $\mathrm{I} \subseteq \mathrm{A}$ satisfaisant $\mathrm{AI} \subseteq \mathrm{I}$ et $\mathrm{IA} \subseteq \mathrm{I}$. On forme alors le quotient comme espace vectoriel A/I et les propriétés $\mathrm{AI} \subseteq \mathrm{I}$ et $\mathrm{IA} \subseteq \mathrm{A}$ sont exactement ce qu'il faut pour que la multiplication passe au quotient.

Démonstration. — Par la propriété universelle de TV (prop. 2.2), on a une factorisation de f par une application linéaire $g : \mathrm{TV} \to \mathrm{A}$. Puisque $g(v \otimes v) = f(v)^2 = 0$, l'application g s'annule sur l'idéal I donc g passe au quotient pour fournir un morphisme d'algèbres $\hat{f} : \bigwedge \mathrm{V} = \mathrm{TV}/\mathrm{I} \to \mathrm{A}$. Il est manifestement unique puisque $\bigwedge \mathrm{V}$ est engendré par les tenseurs décomposables. La démonstration se résume ainsi par le diagramme



□

Comme conséquence de la prop. 3.1 ou du même énoncé pour le produit tensoriel, on obtient le résultat suivant.

Proposition 3.2. — *Si $f : \mathrm{V} \to \mathrm{W}$ est une application linéaire, elle induit un morphisme d'algèbres $\bigwedge f : \bigwedge \mathrm{V} \to \bigwedge \mathrm{W}$ tel que $\iota_\mathrm{W} \circ f = \bigwedge f \circ \iota_\mathrm{V}$. En outre, $\bigwedge(f \circ g) = \bigwedge f \circ \bigwedge g$.*

Décrivons maintenant de manière plus concrète l'algèbre $\bigwedge \mathrm{V}$. Pour cela, remarquons que I est un *idéal homogène* de TV, c'est-à-dire qu'on a

$$\mathrm{I} = \bigoplus_d (\mathrm{I} \cap \mathrm{T}^d \mathrm{V}).$$

En effet, un élément de I est une somme finie d'éléments de type $a \otimes v \otimes v \otimes b$, pour $a, b \in \mathrm{TV}$ et $v \in \mathrm{V}$. En écrivant a et b comme somme d'éléments homogènes, on voit que chaque $a \otimes v \otimes v \otimes b$ est somme d'éléments homogènes qui sont dans I [3].

Il en résulte que le quotient $\bigwedge \mathrm{V} = \mathrm{TV}/\mathrm{I}$ est encore une algèbre graduée :

$$\bigwedge \mathrm{V} = \bigoplus_d \mathrm{T}^d \mathrm{V} / (\mathrm{T}^d \mathrm{V} \cap \mathrm{I}) =: \bigoplus_d \overset{d}{\bigwedge} \mathrm{V},$$

où $\bigwedge^d \mathrm{V}$ est appelée la *puissance extérieure d-ième* de V.

Puisque l'idéal I est engendré par les éléments $v \otimes v$, il ne rencontre $\mathrm{T}^0\mathrm{V}$ et $\mathrm{T}^1\mathrm{V} = \mathrm{V}$ qu'en 0, donc

$$\overset{0}{\bigwedge} \mathrm{V} = \mathbf{K}, \quad \overset{1}{\bigwedge} \mathrm{V} = \mathrm{V}$$

et le morphisme $\iota : \mathrm{V} \to \bigwedge \mathrm{V}$ est une injection.

3. Plus généralement, un idéal d'une algèbre graduée qui est engendré par des éléments homogènes (comme c'est le cas pour I) est homogène.

Le produit dans $\bigwedge \mathrm{V}$ est appelé *produit extérieur* et noté $\wedge$. Le $\mathbf{K}$-espace vectoriel $\bigwedge \mathrm{V}$ est engendré par les $v_1 \wedge \cdots \wedge v_d$ pour $d \in \mathbf{N}$ et $v_1, \ldots, v_d \in \mathrm{V}$. Le fait que l'algèbre $\bigwedge \mathrm{V}$ soit graduée s'écrit

$$\bigwedge^d \mathrm{V} \wedge \bigwedge^e \mathrm{V} \subseteq \bigwedge^{d+e} \mathrm{V}.$$

Si $f : \mathrm{V} \to \mathrm{W}$ est une application linéaire, il s'ensuit qu'on a

$$\bigwedge f = \bigoplus_d \bigwedge^d f, \quad \text{avec } \bigwedge^d f : \bigwedge^d \mathrm{V} \longrightarrow \bigwedge^d \mathrm{W}.$$

Proposition 3.3. — *L'application d-linéaire*

$$\begin{array}{rcl} \mathrm{V}^d & \longrightarrow & \bigwedge^d \mathrm{V} \\ (v_1, \ldots, v_d) & \longmapsto & v_1 \wedge \cdots \wedge v_d \end{array}$$

est alternée. En particulier, pour tout $\sigma \in \mathfrak{S}_d$ et $v_1, \ldots, v_d \in \mathrm{V}$, on a

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(n)} = \varepsilon(\sigma) v_1 \wedge \cdots \wedge v_d. \tag{35}$$

Démonstration. — Par définition de I et de $\bigwedge \mathrm{V}$, l'expression $v_1 \wedge \cdots \wedge v_d$ est nulle dès que deux consécutifs des vecteurs $v_1, \ldots, v_d$ sont égaux. De $v \wedge v = w \wedge w = (v+w) \wedge (v+w) = 0$, on déduit l'identité $w \wedge v = -v \wedge w$. Cela entraîne que la relation (35) est vérifiée lorsque σ est une transposition du type $(i \ i+1)$. Or, si cette relation est vérifiée pour des transpositions σ et τ et tous $v_1, \ldots, v_d \in \mathrm{V}$, on a

$$\begin{array}{rcl} v_{\tau\sigma(1)} \wedge \cdots \wedge v_{\tau\sigma(n)} & = & \varepsilon(\tau) v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(n)} \\ & = & \varepsilon(\tau)\varepsilon(\sigma) v_1 \wedge \cdots \wedge v_d, \end{array}$$

c'est-à-dire qu'elle est vérifiée pour le produit $\tau\sigma$. Comme les transpositions $(12), (23), \ldots, ((n-1) \ n)$ engendrent $\mathfrak{S}_d$ (ex. I.1.8.2°), cela démontre (35).

Si deux des vecteurs $v_1, \ldots, v_d$ sont égaux, on se ramène par une permutation adéquate au cas où ils sont consécutifs, d'où on déduit (en utilisant (35)) $v_1 \wedge \cdots \wedge v_d = 0$; l'application $(v_1, \ldots, v_d) \mapsto v_1 \wedge \cdots \wedge v_d$ est donc bien alternée. □

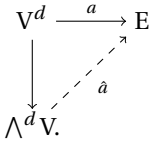
Proposition 3.4. — *L'algèbre graduée $\bigwedge \mathrm{V}$ est* anticommutative, *c'est-à-dire que si $\alpha \in \bigwedge^d \mathrm{V}$ et $\beta \in \bigwedge^e \mathrm{V}$, on a $\beta \wedge \alpha = (-1)^{de} \alpha \wedge \beta$.*

Démonstration. — Il suffit de le montrer lorsque α et β sont des produits extérieurs d'éléments de V. Cela se déduit de l'identité $w \wedge v = -v \wedge w$. □

Proposition 3.5 **(Propriétés de $\bigwedge^d \mathrm{V}$).** — *1° L'application d-linéaire alternée*

$$\begin{array}{rcl} \mathrm{V}^d & \longrightarrow & \bigwedge^d \mathrm{V} \\ (v_1, \ldots, v_d) & \longmapsto & v_1 \wedge \cdots \wedge v_d \end{array}$$

satisfait la propriété universelle suivante : si on a une application d-linéaire alternée $a : \mathrm{V}^d \to \mathrm{E}$, il existe une unique application linéaire $\hat{a} : \bigwedge^d \mathrm{V} \to \mathrm{E}$ telle que le diagramme suivant soit commutatif :



En particulier, $\mathrm{Alt}^d(V) \simeq (\bigwedge^d V)^*$.

2° Si $(e_1, \dots, e_n)$ *est une base de* V, *alors* $(e_{i_1} \wedge \cdots \wedge e_{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$ *est une base de* $\bigwedge^d V$. *En particulier, on a* $\bigwedge^d V = 0$ *pour* $d > n$, *et*

$$\dim(\bigwedge^d V) = \binom{n}{d}.$$

3° Si V *est de dimension finie* n *et* $0 \leqslant d \leqslant n$, *la forme bilinéaire*

$$\begin{array}{ccc} \bigwedge^d V \times \bigwedge^{n-d} V & \longrightarrow & \bigwedge^n V \simeq \mathbf{K} \\ (\alpha, \beta) & \longmapsto & \alpha \wedge \beta \end{array}$$

est non dégénérée. En particulier, on a un isomorphisme non canonique[4]

$$(\bigwedge^d V)^* \simeq \bigwedge^{n-d} V.$$

4° Il existe une application bilinéaire

$$\begin{array}{ccc} \bigwedge^d (V^*) \times \bigwedge^d V & \longrightarrow & \mathbf{K} \\ (\alpha_1 \wedge \cdots \wedge \alpha_d, v_1 \wedge \cdots \wedge v_d) & \longmapsto & \det(\alpha_i(v_j))_{1 \leqslant i,j \leqslant d} \end{array}$$

et elle est non dégénérée. Si V *est de dimension finie, on en déduit un isomorphisme canonique*

$$\bigwedge^d (V^*) \simeq \big(\bigwedge^d V\big)^*.$$

5° Si V *est de dimension finie* n, *on a* $\dim(\bigwedge^n V) = 1$ *par le point 2°. Si* $f \in \mathrm{End}(V)$, *l'endomorphisme* $\bigwedge^n f$ *de* $\bigwedge^n V$ *est donc la multiplication par un scalaire, qui est* $\det(f)$.

Le point 4° est utile notamment en géométrie différentielle : les applications de $\mathbf{R}^n$ dans $\bigwedge^d (\mathbf{R}^n)^*$ sont en effet les d-formes différentielles sur $\mathbf{R}^n$.

Démonstration. — 1° Par la propriété universelle de $T^d V$, l'application d-linéaire a se factorise en $a = g \circ i$, où $g \in \mathrm{Hom}(T^d V, E)$ et i est l'application d-linéaire canonique $V^d \to T^d V$. Mais, parce que a est alternée, g s'annule sur $I \cap T^d V$, donc se factorise à travers le quotient $\bigwedge^d V$ en une application linéaire $\hat{a} \in \mathrm{Hom}(\bigwedge^d V, E)$. L'unicité de $\hat{a}$ provient du fait que $\bigwedge^d V$ est engendré par les $v_1 \wedge \cdots \wedge v_d$.

2° et 3° Par (35), les $(e_{i_1} \wedge \cdots \wedge e_{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$ engendrent $\bigwedge^d V$ et il reste à voir qu'ils sont linéairement indépendants. C'est le cas lorsque $d = n$: il existe en effet une forme n-linéaire alternée non nulle, à savoir le déterminant (dans une base donnée), donc $\bigwedge^n V$

4. Il dépend du choix d'un isomorphisme $\bigwedge^n V \simeq \mathbf{K}$. L'isomorphisme $\bigwedge^n V \otimes (\bigwedge^d V)^* \simeq \bigwedge^{n-d} V$ est lui canonique (l'espace vectoriel $\bigwedge^n V$ est de dimension 1, mais n'est pas canoniquement isomorphe à $\mathbf{K}$).

n'est pas nul. Comme il est engendré par $e_1 \wedge \cdots \wedge e_n$, il est de dimension 1 et ce vecteur n'est pas nul.

Fixons $1 \leqslant j_1 < \cdots < j_{n-d} \leqslant n$; le seul cas où le produit extérieur de $e_{i_1} \wedge \cdots \wedge e_{i_d}$ avec $e_{j_1} \wedge \cdots \wedge e_{j_{n-d}}$ est non nul est lorsque $\{j_1, \ldots, j_{n-d}\}$ est le complémentaire de $\{i_1, \ldots, i_d\}$ dans $\{1, \ldots, n\}$. On en déduit que les $(e_{i_1} \wedge \cdots \wedge e_{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$ sont linéairement indépendants, ce qui montre le point 2°, ainsi que le point 3°.

4° Compte tenu des propriétés d'antisymétrie du déterminant, la formule proposée est alternée en les α_i et en les v_j et fournit donc bien une application bilinéaire $b : \bigwedge^d (\mathrm{V}^*) \times \bigwedge^d \mathrm{V} \to \mathbf{K}$. Si (e_i) est une base de V et (e^i) la base duale, et que $1 \leqslant i_1 < \cdots < i_d \leqslant n$ et $1 \leqslant j_1 < \cdots < j_d \leqslant n$, on a $b(e^{i_1} \wedge \cdots \wedge e^{i_d}, e_{j_1} \wedge \cdots \wedge e_{j_d}) = 1$ ou 0 suivant que $i_k = j_k$ pour tout k ou non. Ainsi la forme b est non dégénérée et on obtient une dualité dans laquelle $(e^{i_1} \wedge \cdots \wedge e^{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$ est la base duale de $(e_{i_1} \wedge \cdots \wedge e_{i_d})_{1 \leqslant i_1 < \cdots < i_d \leqslant n}$.

4° On a $\bigwedge^n f(e_1 \wedge \cdots \wedge e_n) = f(e_1) \wedge \cdots \wedge f(e_n) = (\sum_i f_{i1} e_i) \wedge \cdots \wedge (\sum_i f_{in} e_i) = \det(f) e_1 \wedge \cdots \wedge e_n$ après développement. □

***Remarque 3.6* (Produit vectoriel).** — Vous avez peut-être déjà rencontré le produit vectoriel de deux vecteurs dans l'espace vectoriel euclidien orienté $\mathbf{R}^3$, ou plus généralement le produit vectoriel de $n-1$ vecteurs dans l'espace vectoriel euclidien orienté $\mathrm{V} = \mathbf{R}^n$, qu'on note $v_1 \wedge \cdots \wedge v_{n-1}$ en France, mais $v_1 \times \cdots \times v_{n-1}$ dans le monde anglo-saxon ; adoptons cette dernière notation pour faire la différence avec le produit extérieur. Ce vecteur est défini par la propriété

$$\forall v \in \mathrm{V} \qquad \langle v_1 \times \cdots \times v_{n-1}, v \rangle = \det(v_1, \ldots, v_{n-1}, v),$$

le déterminant étant pris dans une base orthonormale directe (il ne dépend alors pas du choix de cette base).

D'autre part, le produit extérieur des n vecteurs d'une telle base fournissent un générateur canonique de $\bigwedge^n \mathrm{V}$ donc, par prop. 3.5.4° (et surtout la note 4), un isomorphisme canonique $\bigwedge^{n-1} \mathrm{V} \simeq \mathrm{V}^*$. Si on le compose avec l'isomorphisme $\mathrm{V}^* \simeq \mathrm{V}$ donné par le produit scalaire, on peut voir l'élément $v_1 \wedge \cdots \wedge v_{n-1}$ de $\bigwedge^{n-1} \mathrm{V}$ comme un élément de V. Le lecteur vérifiera que ce n'est autre que le produit vectoriel $v_1 \times \cdots \times v_{n-1}$.

***Exemple 3.7* (Grassmanniennes).** — Soit V un espace vectoriel de dimension n. Pour tout sous-espace vectoriel $\mathrm{W} \subseteq \mathrm{V}$ de dimension d, la droite vectorielle $\bigwedge^d \mathrm{W}$ est un sous-espace vectoriel de $\bigwedge^d \mathrm{V}$ engendré par un tenseur décomposable. On peut donc la considérer comme un point de l'espace projectif $\mathbf{P}(\bigwedge^d \mathrm{V})$. Inversement, tout point de $\mathbf{P}(\bigwedge^d \mathrm{V})$ qui correspond à une droite engendrée par un tenseur décomposable (non nul) $v_1 \wedge \cdots \wedge v_d$ définit un sous-espace vectoriel $\mathrm{W} \subseteq \mathrm{V}$ de dimension d, à savoir $\langle v_1, \ldots, v_d \rangle$.

On a ainsi identifié l'ensemble des sous-espaces vectoriels de V de dimension fixée d à un sous-ensemble (dit « grassmannienne ») de l'espace projectif $\mathbf{P}(\bigwedge^d \mathrm{V})$; on le note $\mathrm{G}(d, \mathrm{V})$ (lorsque $d = 1$, ce n'est autre que l'espace projectif $\mathbf{P}(\mathrm{V})$!).

Lorsque $\mathbf{K} = \mathbf{R}$, c'est une variété différentiable de dimension $d(n-d)$.

Exercice 3.8. — a) Montrer que dans $\mathbf{P}(\bigwedge^2 \mathbf{K}^4)$, la grassmannienne $\mathrm{G}(2, \mathbf{K}^4)$ est la quadrique projective définie par l'« équation » $\omega \wedge \omega = 0$.

b) Montrer que toute grassmannienne $\mathrm{G}(d, \mathrm{V}) \subseteq \mathbf{P}(\bigwedge^d \mathrm{V})$ est intersection de quadriques projectives.

Exercice 3.9. — Soit **K** un corps et soit V un **K**-espace vectoriel de dimension n. On a défini (prop. 3.2) un morphisme de groupes

$$\begin{array}{rcl} \phi_{\mathrm{GL}} : \mathrm{GL}(\mathrm{V}) & \longrightarrow & \mathrm{GL}\big(\bigwedge^2 \mathrm{V}\big) \\ f & \longmapsto & \bigwedge^2 f. \end{array}$$

a) Déterminer le noyau de ϕ_{GL} (*Indication :* on pourra distinguer le cas $n = 2$).
b) Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de V. Soit $a \in \mathbf{K}$ et soit u l'endomorphisme de V défini par $u(e_i) = e_i + a\delta_{1i}e_2$, pour tout $i \in \{1, \dots, n\}$. Calculer $\det\big(\bigwedge^2 u\big)$.
c) Exprimer $\det(\bigwedge^2 f)$ en fonction de $\det(f)$ (*Indication :* on pourra commencer par le cas $\det(f) = 1$).
d) Pour tout entier $d \geqslant 0$, exprimer $\det(\bigwedge^d f)$ en fonction de $\det(f)$.

3.1. Tenseurs antisymétriques. — Supposons $\mathrm{car}(\mathbf{K}) = 0$. Dans ce cas, on peut réaliser $\bigwedge^d \mathrm{V}$ comme sous-espace vectoriel de $\mathrm{T}^d\mathrm{V}$ de la manière suivante. Chaque $\sigma \in \mathfrak{S}_d$ induit un endomorphisme **K**-linéaire $\bar{\sigma}$ de $\mathrm{T}^d\mathrm{V}$ défini sur les tenseurs décomposables par

$$\bar{\sigma}(v_1 \otimes \cdots \otimes v_d) = v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(d)}.$$

Un tenseur $t \in \mathrm{T}^d\mathrm{V}$ est dit *antisymétrique* si $\bar{\sigma}(t) = \varepsilon(\sigma)t$ pour toute permutation $\sigma \in \mathfrak{S}_d$. On notera $a^d\mathrm{V} \subseteq \mathrm{T}^d\mathrm{V}$ le sous-espace vectoriel des tenseurs antisymétriques.

Considérons l'application linéaire d'*antisymétrisation*

$$\begin{array}{rcl} p : \mathrm{T}^d\mathrm{V} & \longrightarrow & \mathrm{T}^d\mathrm{V} \\ t & \longmapsto & \dfrac{1}{d!}\displaystyle\sum_{\sigma \in \mathfrak{S}_d} \varepsilon(\sigma)\bar{\sigma}(t). \end{array}$$

On a par exemple $p(v_1 \otimes v_2) = \frac{1}{2}(v_1 \otimes v_2 - v_2 \otimes v_1)$.

Proposition 3.10. — *L'application linéaire p est un projecteur ($p^2 = p$), de noyau $\mathrm{I} \cap \mathrm{T}^d\mathrm{V}$ et d'image $a^d\mathrm{V}$. Elle induit donc un isomorphisme $a^d\mathrm{V} \simeq \bigwedge^d \mathrm{V}$.*

On prendra garde que $\bigoplus_d a^d\mathrm{V}$ n'est pas une sous-algèbre de TV : le produit

$$\begin{array}{rl} & (v_1 \otimes v_2 - v_2 \otimes v_1) \otimes (w_1 \otimes w_2 - w_2 \otimes w_1) \\ = & v_1 \otimes v_2 \otimes w_1 \otimes w_2 - v_1 \otimes v_2 \otimes w_2 \otimes w_1 - v_2 \otimes v_1 \otimes w_1 \otimes w_2 + v_2 \otimes v_1 \otimes w_2 \otimes w_1 \end{array}$$

de deux éléments de $a^2\mathrm{V}$ n'est en général pas dans $a^4\mathrm{V}$. On ne peut donc pas décrire la structure d'algèbre de $\bigwedge \mathrm{V}$ ainsi.

Démonstration. — Pour tout $\tau \in \mathfrak{S}_d$, on a

$$p(\bar{\tau}(t)) = \frac{1}{d!}\sum_{\sigma \in \mathfrak{S}_d} \varepsilon(\sigma)\bar{\sigma}\bar{\tau}(t) = \frac{1}{d!}\sum_{\sigma' \in \mathfrak{S}_d} \varepsilon(\sigma'\tau^{-1})\bar{\sigma}'(t) = \varepsilon(\tau)p(t), \tag{36}$$

et de la même façon

$$\bar{\tau}(p(t)) = \frac{1}{d!}\sum_{\sigma \in \mathfrak{S}_d} \varepsilon(\sigma)\bar{\tau}\bar{\sigma}(t) = \frac{1}{d!}\sum_{\sigma' \in \mathfrak{S}_d} \varepsilon(\tau^{-1}\sigma')\bar{\sigma}'(t) = \varepsilon(\tau)p(t),$$

de sorte que

$$p(p(t)) = \frac{1}{d!}\sum_{\tau \in \mathfrak{S}_d} \varepsilon(\tau)\bar{\tau}(p(t)) = \frac{1}{d!}\sum_{\tau \in \mathfrak{S}_d} \varepsilon(\tau)^2 p(t) = p(t).$$

L'image de p est donc contenue dans $a^d\mathrm{V}$.

Si $t \in a^d\mathrm{V}$, on a $p(t) = \frac{1}{d!}\sum_{\sigma\in\mathfrak{S}_d}\varepsilon(\sigma)\varepsilon(\sigma)t = t$. Donc p est l'identité sur $a^d\mathrm{V}$ et $p^2 = p$: c'est un projecteur d'image $a^d\mathrm{V}$.

Montrons maintenant que $\mathrm{I}\cap\mathrm{T}^d\mathrm{V}$ est contenu dans le noyau de p. L'espace vectoriel $\mathrm{I}\cap\mathrm{T}^d\mathrm{V}$ est engendré par les $t = v_1\otimes\cdots\otimes v_d$, où $v_i = v_{i+1}$ pour un $i \in \{1,\dots,d-1\}$. Prenons pour τ la transposition $(i\ i+1)$. On a alors $\bar{\tau}(t) = t$, donc, par (36), $p(t) = p(\bar{\tau}(t)) = \varepsilon(\tau)p(t) = -p(t)$. Comme on est en caractéristique nulle, on a bien $p(t) = 0$.

L'application p se factorise ainsi en une application linéaire surjective $\hat{p} : \bigwedge^d\mathrm{V} \twoheadrightarrow a^d\mathrm{V}$. Si π est la surjection canonique $\mathrm{T}^d\mathrm{V} \twoheadrightarrow \bigwedge^d\mathrm{V}$, on a

$$\begin{aligned}
\pi\circ\hat{p}(v_1\wedge\cdots\wedge v_d) &= \pi\circ p(v_1\otimes\cdots\otimes v_d)\\
&= \pi\Big(\frac{1}{d!}\sum_{\sigma\in\mathfrak{S}_d}\varepsilon(\sigma)\,v_{\sigma(1)}\otimes\cdots\otimes v_{\sigma(d)}\Big)\\
&= \frac{1}{d!}\sum_{\sigma\in\mathfrak{S}_d}\varepsilon(\sigma)\,v_{\sigma(1)}\wedge\cdots\wedge v_{\sigma(d)}\\
&= \frac{1}{d!}\sum_{\sigma\in\mathfrak{S}_d}\varepsilon(\sigma)^2\,v_1\wedge\cdots\wedge v_d\\
&= v_1\wedge\cdots\wedge v_d.
\end{aligned}$$

On a donc $\pi\circ\hat{p} = \mathrm{Id}_{\bigwedge^d\mathrm{V}}$. Donc $\hat{p}$ est injective et $\mathrm{I}\cap\mathrm{T}^d\mathrm{V} = \ker(p)$. □

4. Pfaffien

Soit $\mathrm{A} = (a_{ij})$ une matrice $2n\times 2n$ alternée à coefficients dans un corps $\mathbf{K}$ de caractéristique quelconque [5]. Soit $(e_1,\dots,e_{2n})$ la base canonique de l'espace vectoriel $\mathbf{K}^{2n}$. On pose

$$\rho(\mathrm{A}) := \sum_{1\leqslant i<j\leqslant 2n} a_{ij}e_i\wedge e_j \quad \in \bigwedge^2\mathbf{K}^{2n}.$$

Alors $\rho(\mathrm{A})^n \in \bigwedge^{2n}\mathbf{K}^{2n}$; on définit le *pfaffien* de A par la formule :

$$\rho(\mathrm{A})^n = n!\,\mathrm{Pf}(\mathrm{A})\,e_1\wedge\cdots\wedge e_{2n}. \tag{37}$$

A priori, cette formule ne définit $\mathrm{Pf}(\mathrm{A})$ que si $\mathrm{car}(\mathbf{K}) = 0$. Néanmoins, en développant $\rho(\mathrm{A})^n$, on s'aperçoit que, pour $\mathrm{car}(\mathbf{K}) = 0$, le pfaffien $\mathrm{Pf}(\mathrm{A})$ est un polynôme en les coefficients de la matrice A, indépendant de $\mathbf{K}$, à coefficients entiers :

$$\mathrm{Pf} \in \mathbf{Z}[a_{ij}]. \tag{38}$$

Pour un corps $\mathbf{K}$ quelconque, on utilise le morphisme d'anneaux canonique $\phi : \mathbf{Z}\to\mathbf{K}$ pour définir à partir de (38) le pfaffien $\mathrm{Pf}\in\mathbf{K}[a_{ij}]$.

5. Cela signifie $a_{ji} = -a_{ij}$ pour tous i, j ; en caractéristique 2, il faut ajouter la condition $a_{ii} = 0$.

Exemple 4.1. — Considérons la matrice

$$A = \begin{pmatrix} 0 & \lambda_1 & & & \\ -\lambda_1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & \lambda_n \\ & & & -\lambda_n & 0 \end{pmatrix}. \tag{39}$$

Alors $\rho(A) = \sum_{i=1}^{n} \lambda_i e_{2i-1} \wedge e_{2i}$ et $\mathrm{Pf}(A) = \lambda_1 \cdots \lambda_n$.

Exemple 4.2. — Considérons la matrice alternée

$$A = \begin{pmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & a_{23} & a_{24} \\ -a_{13} & -a_{23} & 0 & a_{34} \\ -a_{14} & -a_{24} & -a_{34} & 0 \end{pmatrix}.$$

Alors

$$\begin{aligned} \rho(A)^2 &= (a_{12}e_1 \wedge e_2 + a_{13}e_1 \wedge e_3 + a_{14}e_1 \wedge e_4 + a_{23}e_2 \wedge e_3 + a_{24}e_2 \wedge e_4 + a_{34}e_3 \wedge e_4)^2 \\ &= (a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23})e_1 \wedge e_2 \wedge e_3 \wedge e_4 \end{aligned}$$

donc $\mathrm{Pf}(A) = a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}$.

Exercice 4.3. — Montrer la formule suivante, pour toute matrice $A = (a_{ij})$ alternée d'ordre $2n$:

$$\begin{aligned} \mathrm{Pf}(A) &= \frac{1}{2^n n!} \sum_{\sigma \in \mathfrak{S}_{2n}} \varepsilon(\sigma) a_{\sigma(1),\sigma(2)} \cdots a_{\sigma(2n-1),\sigma(2n)} \\ &= \sum_{\substack{\sigma \in \mathfrak{S}_{2n},\ \sigma(1)<\sigma(3)<\cdots<\sigma(2n-1) \\ \sigma(1)<\sigma(2),\ldots,\sigma(2n-1)<\sigma(2n)}} \varepsilon(\sigma) a_{\sigma(1),\sigma(2)} \cdots a_{\sigma(2n-1),\sigma(2n)}. \end{aligned}$$

Lemme 4.4. — *Si* $\mathrm{car}(\mathbf{K}) \neq 2$, *pour toute matrice antisymétrique* A *et tout* $P \in \mathrm{M}_n(\mathbf{K})$, *on a* $\rho(PA^tP) = (\bigwedge^2 P)(\rho(A))$ *dans* $\bigwedge^2 \mathbf{K}^{2n}$.

Démonstration. — Par calcul direct : si $P = (p_{ij})$ et $A = (a_{kl})$, on a $PA^tP = (\sum_{k,l} p_{ik}a_{kl}p_{jl})_{i,j}$ et

$$\begin{aligned} \rho(PA^tP) &= \sum_{i<j} \sum_{k,l} p_{ik}a_{kl}p_{jl} e_i \wedge e_j = \frac{1}{2} \sum_{i,j,k,l} p_{ik}a_{kl}p_{jl} e_i \wedge e_j \\ &= \frac{1}{2} \sum_{k,l} a_{kl} P(e_k) \wedge P(e_l) = \sum_{k<l} a_{kl} P(e_k) \wedge P(e_l) \\ &= (\bigwedge^2 P)(\rho(A)). \end{aligned}$$

□

Lemme 4.5. — *Pour toute matrice* P, *on a l'identité* $\mathrm{Pf}(PA^tP) = \det(P)\,\mathrm{Pf}(A)$.

Démonstration. — Il s'agit d'une identité entre polynômes à coefficients entiers en les coefficients de A et P, qu'il suffit de tester pour $\mathbf{K} = \mathbf{Q}$. Mettant l'égalité du lemme 4.4 à la puissance extérieure n-ième, on obtient

$$\begin{aligned} n!\,\mathrm{Pf}(\mathrm{PA}^t\mathrm{P})\,e_1\wedge\cdots\wedge e_{2n} &= \big((\textstyle\bigwedge^2\mathrm{P})(\rho(\mathrm{A}))\big)^n = \big((\textstyle\bigwedge\mathrm{P})(\rho(\mathrm{A}))\big)^n \\ &= (\textstyle\bigwedge\mathrm{P})(\rho(\mathrm{A})^n) = (\textstyle\bigwedge^{2n}\mathrm{P})(\rho(\mathrm{A})^n) \\ &= \det(\mathrm{P})\,n!\,\mathrm{Pf}(\mathrm{A})\,e_1\wedge\cdots\wedge e_{2n}, \end{aligned}$$

où la troisième égalité utilise que $\bigwedge\mathrm{P}$ est un morphisme d'algèbres. □

Théorème 4.6. — *On a l'identité* $\mathrm{Pf}(\mathrm{A})^2 = \det(\mathrm{A})$.

Démonstration. — De nouveau, il s'agit d'une identité entre polynômes à coefficients entiers en les coefficients de A, donc il suffit de la tester pour $\mathbf{K} = \mathbf{Q}$. Le théorème est vrai sur les matrices de type (39), puisque le pfaffien est $\prod_i \lambda_i$ et le déterminant $\prod_i \lambda_i^2$. Or, par la théorie des formes alternées (sur un corps de caractéristique $\neq 2$; *cf.* §4.4), toute matrice antisymétrique s'écrit sous la forme ${}^t\mathrm{PAP}$, où P est inversible et A de la forme (39), avec $\lambda_i = 1$ ou 0 (il suffit de décomposer $\mathbf{K}^{2n} = \ker(\mathrm{A}) \oplus \mathrm{E}$ et de choisir une base hyperbolique de E). Le théorème découle alors du lemme 4.5. □

Exercice 4.7. — Vérifier directement avec l'exerc. 4.2 la conclusion du théorème pour les matrices alternées d'ordre 4.

Comme conséquence, on obtient une seconde démonstration (valable aussi en caractéristique 2 !) du fait que les transformations symplectiques sont de déterminant 1.

Corollaire 4.8. — *Pour tout corps* $\mathbf{K}$*, on a l'inclusion* $\mathrm{Sp}_{2n}(\mathbf{K}) \subseteq \mathrm{SL}_{2n}(\mathbf{K})$.

Démonstration. — On a

$$\mathrm{Sp}_{2n}(\mathbf{K}) = \{\mathrm{P} \in \mathrm{GL}_{2n}(\mathbf{K}) \mid {}^t\mathrm{P}\,\mathrm{J}_{2n}\,\mathrm{P} = \mathrm{J}_{2n}\},$$

où J_{2n} est la matrice alternée définie en (20). Par le lemme 4.5, un élément P de $\mathrm{Sp}_{2n}(\mathbf{K})$ satisfait $\det({}^t\mathrm{P})\,\mathrm{Pf}(\mathrm{J}_{2n}) = \mathrm{Pf}(\mathrm{J}_{2n})$, ce qui implique $\det(\mathrm{P}) = 1$ puisque J_{2n} est inversible. □

Exercice 4.9. — Soit $\mathbf{K}$ un corps ; on pose $\mathrm{V} := \mathbf{K}^4$, muni de la base canonique (e_1, e_2, e_3, e_4).
a) L'espace vectoriel $\bigwedge^4\mathrm{V}$ est de dimension 1, donc isomorphe à $\mathbf{K}$ en envoyant le générateur $e_1\wedge e_2\wedge e_3\wedge e_4$ sur 1. Montrer que le produit

$$\textstyle\bigwedge^2\mathrm{V}\times\bigwedge^2\mathrm{V}\to\bigwedge^4\mathrm{V}\xrightarrow{\sim}\mathbf{K}$$

provenant de la structure d'algèbre extérieure est une forme bilinéaire symétrique non dégénérée sur $\bigwedge^2\mathrm{V}$. On note f la forme quadratique associée.
b) Soit W' l'espace vectoriel des matrices alternées d'ordre 4 à coefficients dans $\mathbf{K}$. Montrer que le pfaffien définit une forme quadratique f' non dégénérée sur W'.
c) Le groupe $\mathrm{GL}_4(\mathbf{K})$ agit
– d'une part sur l'espace vectoriel $\mathrm{W} := \bigwedge^2\mathrm{V}$ par $\mathrm{P}\cdot(v_1\wedge v_2) = \mathrm{P}v_1\wedge\mathrm{P}v_2$;
– d'autre part sur l'espace vectoriel W' par $\mathrm{P}\cdot\mathrm{M} = \mathrm{P}\,\mathrm{M}\,{}^t\mathrm{P}$.

Montrer qu'il existe un isomorphisme $\phi : W \xrightarrow{\sim} W'$ tel que

$$\begin{array}{lll} \forall\, w \in W & f'(\phi(w)) = f(w) & (\phi \text{ est une isométrie}) ; \\ \forall P \in GL_4(\mathbf{K}) & \phi(P \cdot w) = P \cdot \phi(w) & (\phi \text{ est un morphisme de représentations (\textit{cf.} § IV.1.1)}). \end{array}$$

d) Montrer que la première de ces actions définit un morphisme de groupes $\psi : GL_4(\mathbf{K}) \to O(W, f)$, qui induit un morphisme injectif $\bar{\psi} : SL_4(\mathbf{K})/\{\pm I_4\} \hookrightarrow SO(W, f)$ (*cf.* exerc. 3.9).
e) Montrer que l'image de ψ est contenue dans le groupe $O'(W, f)$ défini dans le § II.8.5, puis que ni ψ, ni $\bar{\psi}$ ne sont surjectifs si $\mathbf{K}$ n'est pas quadratiquement clos ($\mathbf{K}^{\times 2} \neq \mathbf{K}^{\times}$) (*Indication :* on pourra utiliser le th. II.2.6).
On peut montrer que $\bar{\psi}$ *induit en fait un isomorphisme* $SL_4(\mathbf{K})/\{\pm I_4\} \xrightarrow{\sim} SO'(W, f)$.

Exercice 4.10. — Le but de cet exercice est d'expliquer pourquoi le groupe $\mathrm{Spin}'_{3,3}(\mathbf{R})$ mentionné dans la rem. II.11.4 est isomorphe à $SL_4(\mathbf{R})$ et pourquoi $\mathrm{Spin}'_{3,2}(\mathbf{R})$ est isomorphe à $Sp_4(\mathbf{R})$. On se place dans la situation de l'exercice précédent, dont on garde les notations, avec $\mathbf{K} = \mathbf{R}$.
a) Déterminer la signature de la forme quadratique f' sur W' et en déduire que l'image de $\bar{\psi} : SL_4(\mathbf{R})/\{\pm I_4\} \to SO(W, f)$ est contenue dans le groupe $SO'_{3,3}(\mathbf{R})$ défini dans l'ex. II.8.12.2° (c'est un cas particulier de l'exerc. 4.9.e)).
On peut montrer que $\bar{\psi}$ *induit en fait un isomorphisme* $SL_4(\mathbf{R})/\{\pm I_4\} \xrightarrow{\sim} SO'_{3,3}(\mathbf{R})$, *donc que* $SL_4(\mathbf{R})$ *est bien le groupe* $\mathrm{Spin}'_{3,3}(\mathbf{R})$.

b) On pose $J := \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}$ et on note $H \subseteq W'$ l'hyperplan orthogonal à J pour la forme quadratique f'. Quelle est la signature de la restriction de la forme quadratique f' à H ?
f) Montrer que le groupe $\psi(Sp_4(\mathbf{R}))$ est contenu dans $SO'_{2,3}(\mathbf{R})$.
De nouveau, on peut montrer que $\bar{\psi}$ *induit en fait un isomorphisme* $Sp_4(\mathbf{R})/\{\pm I_4\} \xrightarrow{\sim} SO'_{2,3}(\mathbf{R})$, *donc que* $Sp_4(\mathbf{R})$ *est bien le groupe* $\mathrm{Spin}'_{2,3}(\mathbf{R}) = \mathrm{Spin}'_{3,2}(\mathbf{R})$.

Exercice 4.11. — Le but de cet exercice est d'expliquer pourquoi le groupe $\mathrm{Spin}_6(\mathbf{R})$ mentionné dans la rem. II.11.4 est isomorphe à $SU_4(\mathbf{C})$. On se place dans la situation de l'exerc. 4.9, dont on garde les notations, avec $\mathbf{K} = \mathbf{C}$. On a donc un morphisme injectif $\bar{\psi} : SL_4(\mathbf{C})/\{\pm I_4\} \hookrightarrow SO_6(\mathbf{C})$.

On note $\langle \cdot, \cdot \rangle$ la forme sesquilinéaire hermitienne définie positive standard sur $V = \mathbf{C}^4$.
a) Montrer que la formule

$$B(v_1 \wedge v_2, w_1 \wedge w_2) := \langle v_1, w_1 \rangle \langle v_2, w_2 \rangle - \langle v_1, w_2 \rangle \langle v_2, w_1 \rangle$$

définit une forme sesquilinéaire hermitienne définie positive sur $W = \bigwedge^2 \mathbf{C}^4$.
b) Montrer que le groupe $\psi(SU_4(\mathbf{C}))$ est contenu dans le groupe d'isométries $U(W, B) \simeq U_6(\mathbf{C})$.
Le morphisme ϕ *induit donc un morphisme injectif* $\bar{\phi} : SU_4(\mathbf{C})/\{\pm I_4\} \to U_6(\mathbf{C}) \cap SO_6(\mathbf{C})$ *dont on peut montrer qu'il est surjectif. D'autre part, on peut aussi montrer que le groupe* $U_6(\mathbf{C}) \cap SO_6(\mathbf{C})$ *est isomorphe à* $SO_6(\mathbf{R})$. *Donc* $SU_4(\mathbf{C})$ *est bien le groupe* $\mathrm{Spin}_6(\mathbf{R})$.

5. Algèbre symétrique

On sera ici très bref car la construction est entièrement parallèle à celle de l'algèbre extérieure. Le problème universel à résoudre ici est celui pour les morphismes $V \to A$ où A est une algèbre *commutative* avec unité. L'algèbre solution de ce problème est l'*algèbre*

symétrique SV, obtenue comme le quotient

$$\mathrm{SV} := \mathrm{TV}/\mathrm{J},$$

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 $\mathrm{J} = \bigoplus_d (\mathrm{J} \cap \mathrm{T}^d\mathrm{V})$, et on a

$$\mathrm{SV} = \bigoplus \mathrm{S}^d\mathrm{V}, \quad \mathrm{S}^d\mathrm{V} = \mathrm{T}^d\mathrm{V}/(\mathrm{J} \cap \mathrm{T}^d\mathrm{V}).$$

En particulier, $\mathrm{S}^0\mathrm{V} = \mathbf{K}$ 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 $v_1 v_2 = v_2 v_1$.

Une application linéaire $f : \mathrm{V} \to \mathrm{W}$ donne une application linéaire $\mathrm{S}f : \mathrm{SV} \to \mathrm{SW}$, avec $\mathrm{S}f = \bigoplus_d \mathrm{S}^d f$. On a bien sûr la propriété $\mathrm{S}(f \circ g) = \mathrm{S}f \circ \mathrm{S}g$.

Les propriétés de $\mathrm{S}^d\mathrm{V}$ sont les suivantes.

1° L'application d-linéaire

$$\begin{array}{ccc} \mathrm{V}^d & \longrightarrow & \mathrm{S}^d\mathrm{V} \\ (v_1, \dots, v_d) & \longmapsto & v_1 \cdots v_d \end{array}$$

est symétrique [6] et elle est universelle pour cette propriété ; en particulier $(\mathrm{S}^d\mathrm{V})^*$ est l'espace vectoriel des formes d-linéaires symétriques sur V.

2° Si $(e_1, \dots, e_n)$ est une base de V, une base de $\mathrm{S}^d\mathrm{V}$ est donnée par les $(e_{i_1}^{k_1} \cdots e_{i_r}^{k_r})$ pour tout r-uplet $1 \leqslant i_1 < \cdots < i_r \leqslant n$ et entiers k_i tels que $k_1 + \cdots + k_r = d$; on a donc

$$\dim(\mathrm{S}^d\mathrm{V}) = \binom{n+d-1}{n-1}.$$

En particulier, si $\mathrm{V} \neq 0$, l'espace vectoriel SV est toujours de dimension infinie, contrairement à $\bigwedge \mathrm{V}$.

3° Si V est de dimension n, l'algèbre SV est isomorphe à l'algèbre de polynômes $\mathbf{K}[\mathrm{X}_1, \dots, \mathrm{X}_n]$: si $(e_1, \dots, e_n)$ est une base de V, un isomorphisme est obtenu en envoyant e_i sur X_i.

4° Si $\mathrm{car}(\mathbf{K}) = 0$, on peut réaliser $\mathrm{S}^d\mathrm{V}$ à l'intérieur de $\mathrm{T}^d\mathrm{V}$ comme le sous-espace $s^d\mathrm{V}$ des *tenseurs symétriques*, c'est-à-dire des tenseurs t satisfaisant $\bar{\sigma}(t) = t$ pour tout $\sigma \in \mathfrak{S}_n$; en effet, on dispose alors d'une *symétrisation*

$$\begin{array}{ccc} q : \mathrm{T}^d\mathrm{V} & \longrightarrow & \mathrm{T}^d\mathrm{V} \\ v_1 \otimes \cdots \otimes v_d & \longmapsto & \dfrac{1}{d!} \displaystyle\sum_{\sigma \in \mathfrak{S}_d} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(d)} \end{array}$$

qui est une surjection d'image $s^d\mathrm{V}$ et de noyau $\mathrm{J} \cap \mathrm{T}^d\mathrm{V}$. Elle induit ainsi un isomorphisme $s^d\mathrm{V} \simeq \mathrm{S}^d\mathrm{V}$.

---

6. Une application d-linéaire f est *symétrique* si $f(v_{\sigma(1)}, \dots, v_{\sigma(d)}) = f(v_1, \dots, v_d)$ pour tout $\sigma \in \mathfrak{S}_d$. De nouveau, on sait par définition de J que cette propriété est vraie lorsque σ est une transposition $(i\ i+1)$ et il faut un petit argument pour l'étendre à toutes les permutations.

5° Pour $d = 2$, si $\mathrm{car}(\mathbf{K}) \neq 2$, on peut toujours écrire

$$v \otimes w = \frac{1}{2}(v \otimes w - w \otimes v) + \frac{1}{2}(v \otimes w + w \otimes v) = p(v \otimes w) + q(v \otimes w),$$

donc on obtient une décomposition de tout 2-tenseur en somme d'un tenseur antisymétrique et d'un tenseur symétrique :

$$\mathrm{T}^2\mathrm{V} = a^2\mathrm{V} \oplus s^2\mathrm{V}. \tag{40}$$

Remarque 5.1 **(Foncteurs de Schur).** — Supposons $\mathrm{car}(\mathbf{K}) = 0$. La décomposition (40) n'est plus valable pour $\mathrm{T}^d\mathrm{V}$ lorsque $d \geqslant 3$; on a bien une inclusion [7]

$$\mathrm{T}^d\mathrm{V} \supseteq a^d\mathrm{V} \oplus s^d\mathrm{V}$$

mais elle est stricte pour $d \geqslant 3$. Il suffit pour s'en convaincre de calculer les dimensions pour $d = 3$:

$$\dim(\mathrm{T}^3\mathrm{V}) = n^3 > \dim(a^3\mathrm{V}) + \dim(s^3\mathrm{V}) = \binom{n}{3} + \binom{n+2}{3} = \frac{n(n-1)(n-2)}{6} + \frac{n(n+1)(n+2)}{6}.$$

Le bout manquant est un sous-espace vectoriel de $\mathrm{T}^3\mathrm{V}$ de dimension $2\frac{n(n^2-1)}{3}$. Il est somme directe de deux copies d'un espace vectoriel canonique noté $\mathbf{S}_{(2,1)}\mathrm{V}$ (voir exerc. 5.2).

En général, on a une décomposition canonique

$$\mathrm{V}^{\otimes d} = \bigoplus_{\substack{\lambda_1 \geqslant \cdots \geqslant \lambda_n \geqslant 0 \\ \lambda_1 + \cdots + \lambda_n = d}} \left(\mathbf{S}_{(\lambda_1,\ldots,\lambda_n)}\mathrm{V}\right)^{m_\lambda}$$

où les m_λ sont des entiers strictement positifs et les $\mathbf{S}_{(\lambda_1,\ldots,\lambda_n)}$ sont les *foncteurs* [8] *de Schur,* avec (on ne note pas les λ_i nuls)

- $\mathbf{S}_{(\underbrace{1,\ldots,1}_{d \text{ fois}})}\mathrm{V} \simeq a^d\mathrm{V}$;
- $\mathbf{S}_{(d)}\mathrm{V} \simeq s^d\mathrm{V}$;
- $\mathbf{S}_{(\lambda_1,\ldots,\lambda_n)}\mathrm{V}$ est une représentation irréductible de $\mathrm{GL}(\mathrm{V})$ (*cf.* déf. IV.1.3) de dimension

$$\prod_{1 \leqslant i < j \leqslant n} \frac{\lambda_i - \lambda_j + j - i}{j - i}.$$

Exercice 5.2. — Soit $\mathbf{K}$ corps de caractéristique nulle et soit V un $\mathbf{K}$-espace vectoriel.
a) Montrer que le sous-espace vectoriel S de $\mathrm{V}^{\otimes 3}$ engendré par les $v_1 \otimes v_2 \otimes v_3 + v_2 \otimes v_1 \otimes v_3 - v_1 \otimes v_3 \otimes v_2 - v_2 \otimes v_3 \otimes v_1$ est à la fois dans le noyau de l'antisymétrisation p et dans celui de la symétrisation q.
b) En déduire $\mathrm{V}^{\otimes 3} \supseteq a^3\mathrm{V} \oplus s^3\mathrm{V} \oplus \mathrm{S}$.
c) Montrer que S est dans l'image de l'application linéaire injective $f : \mathrm{V} \otimes \bigwedge^2 \mathrm{V} \to \mathrm{V}^{\otimes 3}$ donnée par $v_1 \otimes (v_2 \wedge v_3) \mapsto v_1 \otimes v_2 \otimes v_3 - v_1 \otimes v_3 \otimes v_2$.

---

7. La somme est bien directe puisque le projecteur p est l'identité sur $a^d\mathrm{V}$ mais est nul sur $s^d\mathrm{V}$.

8. La fonctorialité signifie que pour tout $\lambda = (\lambda_1, \ldots, \lambda_n)$ et toute application linéaire $f : \mathrm{V} \to \mathrm{W}$, il existe une application linéaire canoniquement définie $\mathbf{S}_\lambda(f) : \mathbf{S}_\lambda(\mathrm{V}) \to \mathbf{S}_\lambda(\mathrm{W})$, avec $\mathbf{S}_\lambda(\mathrm{Id}) = \mathrm{Id}$ et $\mathbf{S}_\lambda(f \circ g) = \mathbf{S}_\lambda(f) \circ \mathbf{S}_\lambda(g)$ (*cf.* prop. 3.2 et § 5).

d) On considère l'application linéaire $g : \mathrm{V} \otimes \bigwedge^2 \mathrm{V} \to \bigwedge^3 \mathrm{V}$ donnée par la structure d'algèbre de $\bigwedge \mathrm{V}$ (avec le fait que $\bigwedge^1 \mathrm{V} = \mathrm{V}$). Montrer que g est surjective et que $\mathrm{S} = f(\ker(g))$. En déduire la dimension de S.
e) Soit S' le sous-espace vectoriel de $\mathrm{V}^{\otimes 3}$ engendré par les $v_1 \otimes v_2 \otimes v_3 + v_2 \otimes v_1 \otimes v_3 - v_3 \otimes v_2 \otimes v_1 - v_3 \otimes v_1 \otimes v_2$. Montrer que S' est isomorphe à S et que

$$\mathrm{V}^{\otimes 3} = a^3\mathrm{V} \oplus s^3\mathrm{V} \oplus \mathrm{S} \oplus \mathrm{S}' \simeq \bigwedge^3 \mathrm{V} \oplus \mathrm{S}^3\mathrm{V} \oplus \mathrm{S}^2.$$

Les espaces S et S' sont des copies de $\mathbf{S}_{(2,1)}\mathrm{V}$, qui est donc isomorphe au noyau de $g : \mathrm{V} \otimes \bigwedge^2 \mathrm{V} \to \bigwedge^3 \mathrm{V}$.

Remarque 5.3. — Soit V un $\mathbf{C}$-espace vectoriel de dimension finie n. Tout élément de $\mathrm{S}^d\mathrm{V}$ peut s'écrire comme somme de tenseurs décomposables du type $v \cdots v$ (*cf.* rem. 2.1). On peut se poser la question de savoir le nombre maximal de tenseurs décomposables dont on a besoin (« problème de Waring »).

Lorsque $d = 2$, on peut interpréter un élément de $\mathrm{S}^2\mathrm{V}$ comme une forme bilinéaire symétrique sur V^* ; une telle décomposition consiste alors à écrire la forme quadratique associée comme somme de carrés de formes linéaires. La réduction de Gauss nous dit qu'une forme quadratique est somme d'au plus n tels carrés. Dans ce cas, la réponse à la question est donc n.

Pour d et n quelconques, on connaît la réponse à cette importante question lorsque le tenseur à décomposer est « général » (travaux de Alexander et Hirschowitz dans les années 90) mais pas pour tous les tenseurs.

6. Algèbre de Clifford et groupe spinoriel

Dans le § II.11, on avait utilisé $\mathbf{H}$, le corps des quaternions (une $\mathbf{R}$-algèbre de dimension 4) et le groupe de ses éléments de norme 1 (isomorphe à $\mathrm{SU}_2(\mathbf{C})$) agissant par conjugaison, pour construire un morphisme de groupes surjectif de $\mathrm{SU}_2(\mathbf{C})$ vers le groupe orthogonal $\mathrm{O}_3(\mathbf{R})$ pour la forme quadratique définie positive standard sur $\mathbf{R}^3$.

Cette construction est un cas particulier d'une construction très générale, celle de l'algèbre de Clifford d'un espace vectoriel muni d'une forme quadratique, qui nous permettra de définir le groupe et la norme spinoriels déjà mentionnés dans la rem. II.11.4 et le § II.8.5.

6.1. Algèbre de Clifford d'une forme quadratique. — On part maintenant d'un espace vectoriel V sur un corps $\mathbf{K}$ de caractéristique différente de 2, muni d'une forme quadratique f. On cherche à résoudre le problème universel pour les morphismes $g : \mathrm{V} \to \mathrm{A}$, où A est une $\mathbf{K}$-algèbre avec unité, qui vérifient $g(v)^2 = f(v)1_\mathrm{A}$ pour tout $v \in \mathrm{V}$. L'algèbre solution de ce problème est l'*algèbre de Clifford* $\mathrm{C}(\mathrm{V}, f)$ (notée parfois simplement $\mathrm{C}(f)$), obtenue comme le quotient

$$\mathrm{C}(\mathrm{V}, f) = \mathrm{TV}/\mathrm{I}(f),$$

où $\mathrm{I}(f)$ est l'idéal bilatère de TV engendré par les éléments du type $v \otimes v - f(v)$. Contrairement aux cas des algèbres extérieure et symétrique, l'idéal $\mathrm{I}(f)$ n'est pas engendré par des éléments homogènes ($v \otimes v$ est de degré 2 et $f(v)$ est de degré 0), donc $\mathrm{I}(f)$ n'est pas une

algèbre graduée au sens précédent [9]. On peut néanmoins la décomposer en

$$\mathrm{C}(f) = \mathrm{C}(f)^+ \oplus \mathrm{C}(f)^-,$$

où $\mathrm{C}(f)^+$ est l'ensemble des images des éléments de TV de degré pair et $\mathrm{C}(f)^-$ l'ensemble des images des éléments de TV de degré impair. La multiplication par un élément de $\mathrm{C}(f)^+$ laisse stable ces deux morceaux, tandis que la multiplication par un élément de $\mathrm{C}(f)^-$ les échange. En particulier, $\mathrm{C}(f)^+$ est une sous-algèbre de $\mathrm{C}(f)$.

On a dans $\mathrm{C}(f)$, pour tous $v, w \in \mathrm{V}$, les égalités

$$v \cdot v = f(v) \tag{41}$$

$$v \cdot w + w \cdot v = 2\mathrm{B}(v, w), \tag{42}$$

où B est la forme bilinéaire associée à f.

Si $(e_1, \ldots, e_n)$ est une base de V, on peut montrer que les produits $e_{i_1} \cdot \ldots \cdot e_{i_k}$, avec $k \geqslant 0$ et $1 \leqslant i_1 < \cdots < i_k \leqslant n$ forment une base du $\mathbf{K}$-espace vectoriel $\mathrm{C}(f)$, qui est donc de dimension 2^d. Un tel produit est dans $\mathrm{C}(f)^+$ ou $\mathrm{C}(f)^-$ selon que k est pair ou impair, donc chacun des morceaux est de dimension 2^{n-1}. En particulier, s'il est de dimension finie, V s'injecte canoniquement dans $\mathrm{C}(f)^-$.

Exemples 6.1. — 1° Considérons l'espace vectoriel $\mathrm{V} = \mathbf{R}$ et sa base canonique $(e_1 = 1)$, muni de la forme quadratique $f(x) = -x^2$. Une base de $\mathrm{C}(f)$ est alors $(1, e_1)$ avec les relations $e_1^2 = f(e_1) = -1$. L'algèbre $\mathrm{C}(f)$ est donc isomorphe au corps $\mathbf{C}$ des nombres complexes.

2° Considérons l'espace vectoriel $\mathrm{V} = \mathbf{R}^2$ et sa base canonique (e_1, e_2), muni de la forme quadratique $f(x_1, x_2) = -x_1^2 - x_2^2$. Une base de $\mathrm{C}(f)$ est alors $(1, e_1, e_2, e_1 e_2)$ avec les relations

$$e_1^2 = f(e_1) = -1 \quad , \quad e_2^2 = f(e_2) = -1 \quad , \quad e_1 \cdot e_2 = -e_2 \cdot e_1.$$

Si on pose $\mathrm{I} := e_1$, $\mathrm{J} := e_2$ et $\mathrm{K} := e_1 \cdot e_2 = \mathrm{IJ}$, on vérifie les relations des quaternions (§ II.11)

$$\mathrm{IJK} = \mathrm{K}^2 = e_1 \cdot e_2 \cdot e_1 \cdot e_2 = -e_1^2 \cdot e_2^2 = -1.$$

L'algèbre $\mathrm{C}(f)$ est donc isomorphe au corps non commutatif $\mathbf{H}$ des quaternions.

Exercice 6.2. — Déterminer la $\mathbf{R}$-algèbre $\mathrm{C}(\mathrm{V}, f)$ dans les cas suivants :
– $\mathrm{V} = \mathbf{R}$ et $f(x) = x^2$;
– $\mathrm{V} = \mathbf{R}^2$ et $f(x_1, x_2) = x_1^2 + x_2^2$;
– $\mathrm{V} = \mathbf{R}^2$ et $f(x_1, x_2) = x_1^2 - x_2^2$.

Exercice 6.3. — Pour tous $s, t \geqslant 0$, on note $\mathrm{C}(s, t)$ l'algèbre de Clifford de la forme quadratique de signature (s, t) sur $\mathrm{V} = \mathbf{R}^{s+t}$.
a) Pour tout $n \geqslant 0$, montrer qu'on a un isomorphisme de $\mathbf{R}$-algèbres

$$\mathrm{C}(0, n+2) \simeq \mathrm{C}(n, 0) \otimes_{\mathbf{R}} \mathrm{C}(0, 2)$$

(*Indication :* si $(e_1, \ldots, e_{n+2})$ est une base orthonormale de $\mathbf{R}^{n+2}$, $(e'_1, \ldots, e'_n)$ une base orthonormale de $\mathbf{R}^n$ et (e''_1, e''_2) une base orthonormale de $\mathbf{R}^2$, on pourra considérer l'application linéaire $\mathbf{R}^{n+2} \to \mathrm{C}(n, 0) \otimes_{\mathbf{R}} \mathrm{C}(0, 2)$ qui envoie e_i sur $e'_i \otimes e''_1 \cdot e''_2$ si $i \in \{1, \ldots, n\}$ et sur $1 \otimes e''_{i-n}$ si $i \in \{n+1, n+2\}$).

9. Sauf si $f = 0$, auquel cas $\mathrm{C}(f)$ est simplement $\bigwedge \mathrm{V}$.

b) Pour tous $s, t \geqslant 0$, montrer qu'on a un isomorphisme de $\mathbf{R}$-algèbres

$$\mathrm{C}(s+1, t+1) \simeq \mathrm{C}(s,t) \otimes_{\mathbf{R}} \mathrm{C}(1,1).$$

c) Pour tout $n \geqslant 0$, montrer qu'on a des isomorphismes de $\mathbf{R}$-algèbres

$$\begin{aligned} \mathrm{C}(0, n+8) &\simeq \mathrm{C}(0,n) \otimes_{\mathbf{R}} \mathrm{C}(0,8) \\ \mathrm{C}(n+8, 0) &\simeq \mathrm{C}(n,0) \otimes_{\mathbf{R}} \mathrm{C}(8,0) \end{aligned}$$

et

$$\mathrm{C}(0,8) \simeq \mathrm{C}(8,0) \simeq \mathscr{M}_{16}(\mathbf{R})$$

(*Indication :* on pourra utiliser les exerc. 6.2 et 1.9).

6.2. Groupe de Clifford. — On note $\alpha : \mathrm{C}(f) \to \mathrm{C}(f)$ l'involution qui vaut Id sur $\mathrm{C}(f)^+$ et $-\mathrm{Id}$ sur $\mathrm{C}(f)^-$. Elle vérifie $\alpha(x \cdot y) = \alpha(x) \cdot \alpha(y)$, pour tous $x, y \in \mathrm{C}(f)$.

Pour tout x dans le groupe des unités $\mathrm{C}(f)^\times$, on considère l'endomorphisme

$$\rho_x : z \mapsto \alpha(x) \cdot z \cdot x^{-1}$$

de $\mathrm{C}(f)$. On a $\rho_1 = \mathrm{Id}_{\mathrm{C}(f)}$ et, pour tous $x, y \in \mathrm{C}(f)^\times$,

$$\rho_{x\cdot y}(z) = \alpha(x \cdot y) \cdot z \cdot (x \cdot y)^{-1} = \alpha(x) \cdot \alpha(y) \cdot z \cdot y^{-1} x^{-1} = \rho_x \circ \rho_y(z).$$

L'endomorphisme ρ_x est donc inversible (d'inverse $\rho_{x^{-1}}$) et

$$\Gamma(f) := \{x \in \mathrm{C}(f)^\times \mid \forall v \in \mathrm{V} \quad \alpha(x) \cdot v \cdot x^{-1} \in \mathrm{V}\}.$$

est un sous-groupe de $\mathrm{C}(f)^\times$ stable par α appelé *groupe de Clifford* de f. On a par construction un morphisme de groupes

$$\begin{aligned} \rho : \Gamma(f) &\longrightarrow \mathrm{GL(V)} \\ x &\longmapsto \rho_x. \end{aligned}$$

Remarquons que tout élément non isotrope v de V (c'est-à-dire qui vérifie $f(v) \neq 0$) est inversible dans $\mathrm{C}(f)$, avec $v^{-1} = \frac{1}{f(v)} v$.

Proposition 6.4. *— Tout $v \in \mathrm{V}$ non isotrope est dans $\Gamma(f)$ et ρ_v est la réflexion par rapport à l'hyperplan $v^\perp$ (ex. III.5.2).*

Démonstration. — Si B est la forme bilinéaire associée à f et que s_v est la réflexion en question, on a (ex. III.5.2)

$$\forall w \in \mathrm{V} \qquad s_v(w) = w - 2\frac{\mathrm{B}(v,w)}{\mathrm{B}(v,v)} v.$$

Comme V est un sous-espace vectoriel de $\mathrm{C}(f)$, on peut voir cette égalité entre éléments de V comme une égalité dans $\mathrm{C}(f)$. Elle s'écrit alors, en utilisant (41) et (42),

$$\forall w \in \mathrm{V} \qquad s_v(w) = w - (v \cdot w + w \cdot v) \cdot v^{-2} \cdot v = -v \cdot w \cdot v^{-1} = \alpha(v) \cdot w \cdot v^{-1},$$

puisque α est $-\mathrm{Id}$ sur V. □

Lemme 6.5. *— Si f est non dégénérée et* V *de dimension finie, le noyau de ρ est $\mathbf{K}^\times$.*

Démonstration. — Soit x un élément du noyau de ρ, qu'on écrit $x = x^+ + x^-$, avec $x^\pm \in C(f)^\pm$. On a alors $\alpha(x)\cdot v = v\cdot x$ pour tout $v \in V$, d'où $\pm x^\pm \cdot v = v \cdot x^\pm$. Choisissons une base orthogonale $(e_1,\dots,e_n)$ de V. On a alors, par (42),

$$e_i \cdot e_j = -e_j \cdot e_i \quad \text{si } i \neq j.$$

On rappelle que les $e_{i_1}\cdot\ldots\cdot e_{i_k}$, avec $1 \leqslant i_1 < \cdots < i_k \leqslant n$ forment une base du $\mathbf{K}$-espace vectoriel $C(f)$. On peut donc écrire $x^+ = x_0^+ + e_1 \cdot x_1^+$, où ni $x_0^+ \in C(f)^+$, ni $x_1^+ \in C(f)^-$, ne contient de facteur e_1 dans sa décomposition sur cette base. On a alors

$$e_1\cdot x_0^+ + f(e_1)x_1^+ = e_1\cdot x^+ = x^+\cdot e_1 = x_0^+\cdot e_1 + e_1\cdot x_1^+\cdot e_1 = e_1\cdot x_0^+ - f(e_1)x_1^+.$$

Puisque f est non dégénérée, on a $f(e_1)\neq 0$, d'où on déduit $x_1^+ = 0$, c'est-à-dire que x^+ ne contient aucun facteur e_1. On appliquant ce raisonnement avec les autres e_i, on voit que x^+ ne contient aucun facteur e_i, c'est-à-dire $x^+ \in \mathbf{K}$.

Si on écrit de la même façon $x^- = x_0^- + e_1\cdot x_1^-$, on obtient $x_1^- = 0$, c'est-à-dire $x^- \in \mathbf{K}$. Mais on a alors $x^- \in \mathbf{K}\cap C(f)^- = \{0\}$.

Tout cela montre $x = x^+ \in \mathbf{K}\cap C(f)^\times = \mathbf{K}^\times$. □

6.3. Norme et groupe spinoriels. — On définit une deuxième involution $t : C(f)\to C(f)$ de la façon suivante. Soit $C(f)^0$ l'*algèbre opposée* à $C(f)$, c'est-à-dire le même espace vectoriel, mais où la multiplication $x \overset{0}{\cdot} y$ est donnée par $y\cdot x$. Comme le problème universel dont l'application linéaire $V\to C(f)$ est la solution a une unique solution à isomorphisme près, il existe un isomorphisme d'algèbres $t : C(f)\to C(f)^0$. Cet isomorphisme vérifie donc $t(x\cdot y) = t(y)\cdot t(x)$, pour tous $x, y \in C(f)$. De nouveau, par unicité, t est une involution.

Lorsque V est de dimension finie, de base $(e_1,\dots,e_n)$, on peut décrire l'action de t sur une base de $C(f)$:

$$t(e_{i_1}\cdot\ldots\cdot e_{i_k}) = e_{i_k}\cdot\ldots\cdot e_{i_1}.$$

On remarque que $t\circ\alpha = \alpha\circ t$. Il s'ensuite que l'application

$$x \mapsto \bar{x} := t\circ\alpha(x) = \alpha\circ t(x)$$

est une involution de $C(f)$ qui commute avec α et t et vérifie $\overline{x\cdot y} = \bar{y}\cdot\bar{x}$. On définit enfin la *norme spinorielle*

$$\begin{array}{rccc} N : C(f) & \longrightarrow & C(f) \\ x & \longmapsto & x\cdot\bar{x}. \end{array}$$

On a en particulier

$$\forall v \in V \qquad N(v) = -f(v). \tag{43}$$

Proposition 6.6. — *Supposons f non dégénérée et* V *de dimension finie. Par restriction, la norme spinorielle définit un morphisme de groupes* $N : \Gamma(f)\to\mathbf{K}^\times$.

Démonstration. — Si $x \in \Gamma(f)$, nous allons montrer que $N(x)$ est dans le noyau de ρ. Appliquons t, qui renverse l'ordre des produits et qui est l'identité sur V, à la relation $\alpha(x)\cdot v\cdot x^{-1} \in V$; on obtient

$$\alpha(x)\cdot v\cdot x^{-1} = t(x^{-1})\cdot v\cdot t(\alpha(x)),$$

d'où

$$v = t(x)\cdot\alpha(x)\cdot v\cdot x^{-1}\cdot\bar{x}^{-1} = \alpha(\bar{x}\cdot x)\cdot v\cdot(\bar{x}\cdot x)^{-1}.$$

Puisque $\bar{x} \in \mathrm{C}(f)^\times$, cela signifie $\bar{x}\cdot x \in \Gamma(f)$ et $\bar{x}\cdot x \in \ker(\rho)$, c'est-à-dire $\bar{x}\cdot x \in \mathbf{K}^\times$ par le lemme 6.5. De plus, on a $\bar{x} \in \Gamma(f)$ puisque $\Gamma(f)$ est un groupe. Appliquant ce résultat à $\bar{x}$, on obtient que $\bar{\bar{x}}\cdot\bar{x} = \mathrm{N}(x)$ est dans $\mathbf{K}^\times$.

Si $x, y \in \Gamma(f)$, on a

$$\mathrm{N}(xy) = x\cdot y\cdot\bar{y}\cdot\bar{x} = x\cdot\mathrm{N}(y)\cdot\bar{x} = x\cdot\bar{x}\mathrm{N}(y) = \mathrm{N}(x)\mathrm{N}(y),$$

où la troisième égalité a lieu puisque $\mathrm{N}(y)$ est dans $\mathbf{K}^\times$, donc commute avec tous les éléments de $\mathrm{C}(f)$. On a donc bien un morphisme de groupes. □

Proposition 6.7. — *Supposons f non dégénérée et* V *de dimension finie. L'image du morphisme de groupes $\rho : \Gamma(f) \to \mathrm{GL(V)}$ est le groupe orthogonal* $\mathrm{O(V}, f)$.

Démonstration. — Soit $x \in \Gamma(f)$. Montrons tout d'abord que ρ_x est bien une isométrie, c'est-à-dire qu'on a $f(\rho_x(v)) = f(v)$ pour tout $v \in \mathrm{V}$. On a, avec la prop. 6.6 et (43),

$$\begin{aligned} f(\rho_x(v)) &= -\mathrm{N}(\rho_x(v)) = -\alpha(x)\cdot v\cdot x^{-1}\cdot\bar{x}^{-1}\cdot(-v)\cdot\alpha(\bar{x}) = -\alpha(x)\cdot v\cdot\mathrm{N}(x^{-1})\cdot v\cdot\alpha(\bar{x}) \\ &= f(v)\mathrm{N}(x^{-1})\alpha(\mathrm{N}(x)) = f(v)\mathrm{N}(x^{-1})\mathrm{N}(x) = f(v). \end{aligned}$$

L'image de $\rho : \Gamma(f) \to \mathrm{GL(V)}$ est donc contenue dans le groupe orthogonal $\mathrm{O(V}, f)$.

Mais d'autre part, par la prop. 6.4, cette image contient toutes les réflexions. Comme celles-ci engendrent $\mathrm{O(V}, f)$ (th. II.8.7), on a $\rho(\Gamma(f)) = \mathrm{O(V}, f)$. □

Corollaire 6.8. — *Sous les mêmes hypothèses, on a un isomorphisme de groupes $\hat{\rho} : \Gamma(f)/\mathbf{K}^\times \xrightarrow{\sim} \mathrm{O(V}, f)$ et la norme spinorielle induit un morphisme de groupes*

$$\theta : \mathrm{O(V}, f) \to \mathbf{K}^\times/\mathbf{K}^{\times 2}$$

qui vérifie, pour tout $v \in \mathrm{V}$ non isotrope, $\theta(s_v) = f(v)$.

Démonstration. — Le morphisme $\hat{\rho}$ est fourni par la factorisation canonique de ρ. L'image de $\mathbf{K}^\times \subseteq \Gamma(f)$ par la norme spinorielle $\mathrm{N} : \Gamma(f) \to \mathbf{K}^\times$ est le sous-groupe $\mathbf{K}^{\times 2}$ des carrés non nuls. On a donc un morphisme induit $\hat{\mathrm{N}} : \Gamma(f)/\mathbf{K}^\times \to \mathbf{K}^\times/\mathbf{K}^{\times 2}$. Il suffit de poser $\theta := \hat{\mathrm{N}}\circ\hat{\rho}^{-1}$. □

6.4. Groupe Spin_n. — On se place ici dans le cas où $\mathbf{K} = \mathbf{R}$, $\mathrm{V} = \mathbf{R}^n$ et f est (le carré de) la norme euclidienne usuelle :

$$f(x_1, \ldots, x_n) = x_1^2 + \cdots + x_n^2.$$

On pose alors

$$\mathrm{Spin}_n(\mathbf{R}) := \ker(\mathrm{N}) \cap \Gamma(f) \cap \mathrm{C}(f)^+ = \{x \in \mathrm{C}(f)^+ \mid x\cdot\bar{x} = 1,\ x\cdot\mathrm{V}\cdot x^{-1} \subseteq \mathrm{V}\}$$

puisque α est l'identité sur $\mathrm{C}(f)^+$. C'est un sous-groupe de $\Gamma(f)$.

Théorème 6.9. — *L'image du morphisme de groupes $\rho|_{\mathrm{Spin}_n(\mathbf{R})} : \mathrm{Spin}_n(\mathbf{R}) \to \mathrm{O(V}, f)$ est le groupe $\mathrm{SO(V}, f)$ et son noyau est $\{\pm 1\}$.*

Démonstration. — Vu le lemme 6.5, le noyau de la restriction de ρ à $\mathrm{Spin}_n(\mathbf{R})$ est l'intersection de $\mathbf{R}^\times$ avec $\ker(\mathrm{N})$. Mais sur $\mathbf{R}^\times$, la norme spinorielle est juste le carré, donc le noyau est $\{\pm 1\}$.

Soit $x \in \mathrm{Spin}_n(\mathbf{R})$. On décompose l'isométrie ρ_x en produit de réflexions $s_{v_1}\circ\cdots\circ s_{v_r}$, où on peut supposer les vecteurs $v_1, \ldots, v_r$ de V unitaires. On a alors (prop. 6.4) $s_{v_i} = \rho_{v_i}$,

donc $\rho(x) = \rho(v_1 \cdot \ldots \cdot v_r)$. Comme le noyau de ρ est $\mathbf{R}^\times$ (lemme 6.5), il existe $\lambda \in \mathbf{R}^\times$ tel que $x = \lambda v_1 \cdot \ldots \cdot v_r$ dans $\Gamma(f)$. En prenant les normes spinorielles, on obtient (en utilisant la prop. 6.6 et (43))

$$1 = \mathrm{N}(x) = \lambda^2 \mathrm{N}(v_1 \cdot \ldots \cdot v_r) = \lambda^2 \mathrm{N}(v_1) \cdots \mathrm{N}(v_r) = \lambda^2 (-1)^r f(v_1) \cdots f(v_r) = \lambda^2 (-1)^r.$$

Ceci n'est possible que si r est pair, ce qui entraîne

$$\det(\rho_x) = \det(s_{v_1}) \cdots \det(s_{v_r}) = (-1)^r = 1.$$

Le groupe $\rho(\mathrm{Spin}_n(\mathbf{R}))$ est donc bien contenu dans $\mathrm{SO}(\mathrm{V}, f)$.

Inversement, tout élément u de $\mathrm{SO}(\mathrm{V}, f)$ se décompose en un produit de réflexions $s_{v_1} \circ \cdots \circ s_{v_r}$, avec $v_1, \ldots, v_r$ dans V de norme 1 et r pair. Comme $s_{v_i} = \rho(v_i)$, on a $u = \rho(v_1 \cdot \ldots \cdot v_r)$ avec $v_1 \cdot \ldots \cdot v_r \in \ker(\mathrm{N}) \cap \Gamma(f) \cap \mathrm{C}(f)^+ = \mathrm{Spin}_n(\mathbf{R})$. L'image $\rho(\mathrm{Spin}_n(\mathbf{R}))$ est donc égale à $\mathrm{SO}(\mathrm{V}, f)$. □

Les groupes $\mathrm{Spin}_n(\mathbf{R})$ ont déjà été identifiés pour n petit (rem. II.11.4) : on a $\mathrm{Spin}_2(\mathbf{R}) \simeq \mathrm{U}_1(\mathbf{C})$, $\mathrm{Spin}_3(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C})$, $\mathrm{Spin}_4(\mathbf{R}) \simeq \mathrm{SU}_2(\mathbf{C}) \times \mathrm{SU}_2(\mathbf{C})$ et $\mathrm{Spin}_6(\mathbf{R}) \simeq \mathrm{SU}_4(\mathbf{C})$.

Exercice 6.10. — Montrer que $\mathrm{Spin}_n(\mathbf{R})$ est connexe pour $n \geqslant 2$ (*Indication :* on pourra utiliser le th. 8.7 et, pour tous $v, w \in \mathrm{V}$ unitaires et orthogonaux, le chemin $t \mapsto (v \cos t - w \sin t)(v \sin t + w \cos t)$, pour $t \in [0, \pi/2]$, dans $\mathrm{Spin}_n(\mathbf{R})$).

Remarque 6.11. — Si f est une forme quadratique de signature (s, t) sur $\mathbf{R}^{s+t}$, on pose de la même façon

$$\mathrm{Spin}_{s,t}(\mathbf{R}) := \ker(\mathrm{N}) \cap \Gamma(f) \cap \mathrm{C}(f)^+.$$

Une preuve analogue à celle du th. 6.9 montre que le morphisme ρ induit par restriction un morphisme surjectif $\mathrm{Spin}_{s,t}(\mathbf{R}) \to \mathrm{SO}_{s,t}(\mathbf{R})$ de noyau $\{\pm 1\}$. Lorsque $st > 0$, ces groupes ne sont pas connexes (ex. II.8.12.2°) et on définit $\mathrm{Spin}'_{s,t}(\mathbf{R})$ comme l'image inverse du groupe connexe $\mathrm{SO}'_{s,t}(\mathbf{R})$.

CHAPITRE IV

REPRÉSENTATIONS DES GROUPES FINIS

1. Représentations

Soit G un groupe et soit V un **K**-espace vectoriel. Une *représentation linéaire* de G dans V est un morphisme de groupes

$$\rho : G \longrightarrow GL(V).$$

En d'autres termes, on représente les éléments de G comme des automorphismes de V ou plus simplement, si V est de dimension finie et qu'on en choisit une base, comme des matrices (inversibles).

On notera la représentation (V,ρ), ou simplement, en l'absence d'ambiguïté, ρ ou V. L'action d'un élément $g \in G$ sur V sera souvent notée $g \cdot v$ $(= \rho(g)(v))$. C'est une action du groupe G sur V au sens de la déf. du § I.2.1.

Exemples 1.1. — 1° Une représentation de G dans un espace vectoriel de dimension 1 est un morphisme $\rho : G \to \mathbf{K}^\times$. Si G est fini, l'image est un groupe cyclique (exerc. I.1.28).

2° Si G est défini comme un sous-groupe de GL(V) (ce qui est le cas de tous les groupes classiques), l'inclusion $G \hookrightarrow GL(V)$ est appelée la *représentation standard*.

3° Si $(e_1,\dots,e_n)$ est une base de $\mathbf{K}^n$, on obtient une représentation de $\mathfrak{S}_n$ dans $\mathbf{K}^n$ en posant $\rho(\sigma)(e_i) = e_{\sigma(i)}$. Une telle représentation est appelée *représentation de permutation*. Les $\rho(\sigma)$ sont des matrices de permutation.

4° Si G est un groupe fini, on peut composer le morphisme de groupes de Cayley (ex. I.2.3)

$$\begin{array}{ccc} G & \hookrightarrow & \mathrm{Bij}(G) \\ g & \mapsto & (x \mapsto gx) \end{array}$$

avec la construction du 3° ci-dessus pour obtenir une représentation

$$\rho_R : G \to \mathrm{Bij}(G) \to GL(\mathbf{K}^G),$$

où $\mathbf{K}^G$ est l'espace vectoriel des fonctions de G dans **K**. Si $\varepsilon_h : G \to \mathbf{K}$ est la fonction caractéristique d'un élément h de G, la famille $(\varepsilon_h)_{h\in G}$ forme une base de $\mathbf{K}^G$. On a $\rho_R(g)(\varepsilon_h) = \varepsilon_{gh}$ et, pour tout $u \in \mathbf{K}^G$, on a $\rho_R(g)(u) : g' \mapsto u(g^{-1}g')$ pour tout $g' \in G$.

Cette représentation s'appelle la *représentation régulière* de G.

1.1. Vocabulaire et propriétés. — Soit (V,ρ) une représentation de G.

La *dimension* (on dit aussi le *degré*) de la représentation est $\dim(V)$.

Une *sous-représentation* est un sous-espace vectoriel $W \subseteq V$ stable sous l'action de G ; on parle de sous-espace G-invariant. Dans ce cas, on a des représentations induites sur W et sur le quotient V/W.

Exemples 1.2. — 1° Le sous-espace vectoriel

$$V^G = \{v \in V \mid \forall g \in G \quad g \cdot v = v\}$$

des vecteurs fixes sous G est un sous-espace G-invariant.

2° Si $V = \mathbf{K}^n$ est la représentation de permutation du groupe $\mathfrak{S}_n$, l'hyperplan

$$V_0 = \left\{(x_1,\dots,x_n) \in V \,\middle|\, \sum_{i=1}^{n} x_i = 0\right\}$$

est une sous-représentation de V, ainsi que la droite supplémentaire

$$V_1 = \mathbf{K}(1,\dots,1).$$

Un *morphisme* entre des représentations (V,ρ_V) et (W,ρ_W) d'un groupe G est une application linéaire $f : V \to W$ telle que

$$\forall g \in G \qquad f \circ \rho_V(g) = \rho_W(g) \circ f.$$

Dans ce cas, $\ker f$ et $\mathrm{im}(f)$ sont des sous-représentations de V et W, et f induit un isomorphisme de représentations

$$f : V/\ker(f) \xrightarrow{\sim} \mathrm{im}(f).$$

L'espace vectoriel des morphismes entre les représentations V et W est noté $\mathrm{Hom}_G(V,W)$, ou $\mathrm{Hom}(\rho_V,\rho_W)$. Des représentations ρ_V et ρ_W de dimension finie d'un groupe G sont isomorphes si et seulement si il existe une base de V et une base de W dans lesquelles, pour tout $g \in G$, les matrices de $\rho_V(g)$ et de $\rho_W(g)$ sont les mêmes.

Si V et W sont des représentations de G, on peut former les représentations suivantes :

- $V \oplus W$ pour $\rho(g) = (\rho_V(g),\rho_W(g))$;
- $V \otimes W$ pour $\rho(g) = \rho_V(g) \otimes \rho_W(g)$;
- V^* pour $\rho^*(g) = {}^t\rho(g^{-1})$;
- $\mathrm{Hom}_{\mathbf{K}}(V,W) = V^* \otimes W$ pour $\rho(g)(f) = \rho_W(g) \circ f \circ \rho_V(g)^{-1}$; en particulier l'espace des morphismes de représentations de V vers W est

$$\mathrm{Hom}_G(V,W) = \mathrm{Hom}_{\mathbf{K}}(V,W)^G;$$

- T^kV, $\bigwedge^k V$, S^kV sont aussi des représentations de G. Si $\mathrm{car}(\mathbf{K}) \neq 2$, on a par (40) un isomorphisme de représentations

$$V \otimes V \simeq \bigwedge^2 V \oplus S^2V.$$

1.2. Représentations irréductibles. —

Définition 1.3. — Une représentation V est *irréductible* si elle est non nulle et que ses seules sous-représentations sont 0 et V.

Toute représentation de dimension 1 est bien sûr irréductible.

Exemples 1.4. — 1° Si G est abélien et que **K** est algébriquement clos, les seules représentations irréductibles V de dimension finie de G sont de dimension 1. Soit $g \in G$ et soit $W \subseteq V$ un sous-espace propre (non nul) de $\rho(g)$, pour la valeur propre $\lambda \in \mathbf{K}$. On a, puisque G est abélien,

$$\forall h \in G\ \forall x \in W \qquad \rho(g)(\rho(h)(x)) = \rho(h)(\rho(g)(x)) = \rho(h)(\lambda x) = \lambda\rho(h)(x),$$

donc $\rho(h)(x) \in W$. Le sous-espace vectoriel W de V est donc stable par tous les $\rho(h)$: c'est une sous-représentation non nulle de V. Comme V est irréductible, elle est égale à V. Ceci entraîne que tous les $\rho(g)$ sont des homothéties. Toute droite $D \subseteq V$ est alors une sous-représentation, donc D = V.

Les représentations de $\mathbf{Z}/n\mathbf{Z}$ dans **C** sont données par l'image d'un générateur, qui doit être une racine n-ième de l'unité dans **C**. On obtient ainsi les n représentations irréductibles $\rho_0, \dots, \rho_{n-1}$ de $\mathbf{Z}/n\mathbf{Z}$, données par

$$\forall k \in \mathbf{Z}/n\mathbf{Z} \qquad \rho_j(k) = \exp\left(\frac{2kj\pi i}{n}\right).$$

Notons que tout cela n'est plus vrai lorsque $\mathbf{K} = \mathbf{R}$: la représentation de $\mathbf{Z}/n\mathbf{Z}$ dans $\mathbf{R}^2$ qui fait correspondre à $k \in \mathbf{Z}/n\mathbf{Z}$ la rotation d'angle $2k\pi/n$ est irréductible lorsque $n \geqslant 3$ puisqu'aucune droite n'est laissée stable par toutes ces rotations.

2° Pour $n \geqslant 3$, la représentation standard du groupe diédral D_n dans $\mathbf{R}^2$ (ou dans $\mathbf{C}^2$) est irréductible, puisqu'aucune droite n'est laissée stable par tous les éléments de D_n.

3° Si $\dim(V) \geqslant 2$, les représentations standard de SL(V), GL(V) et Sp(V) sont irréductibles puisque ces groupes opèrent transitivement sur $V - \{0\}$. C'est aussi le cas pour $O_n(\mathbf{R})$, qui opère transitivement sur la sphère unité $\mathbf{S}^{n-1}$, qui engendre l'espace vectoriel $\mathbf{R}^n$.

Exercice 1.5. — Soit G un groupe fini.
a) Montrer que toute représentation irréductible de G est de dimension finie $\leqslant |G|$.
b) Supposons **K** algébriquement clos. Soit $A \leq G$ un sous-groupe abélien. Montrer que toute représentation irréductible de G est de dimension $\leqslant \frac{|G|}{|A|}$.

Exercice 1.6. — Soit V un espace vectoriel réel de dimension finie $n > 0$ et soit d un entier positif.
a) Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de V. Donner une base naturelle $\mathscr{B}_d$ de l'espace vectoriel $S^d V$.
b) Montrer qu'il existe des réels $\lambda_1, \dots, \lambda_n$ tels que, si P et Q sont des monômes unitaires de degré d en n variables, alors $P(\lambda_1, \dots, \lambda_n) = Q(\lambda_1, \dots, \lambda_n)$ si et seulement si P = Q.
c) Montrer que GL(V) agit naturellement sur l'espace vectoriel $S^d V$. On en déduit une représentation ρ_d de GL(V) dans $S^d V$.
d) Soit W un sous-espace vectoriel non nul de $S^d V$ stable par l'action de GL(V). Montrer qu'il existe un sous-ensemble de la base $\mathscr{B}_d$ qui engendre W (*Indication :* on pourra considérer l'automorphisme g de V qui envoie e_i sur $\lambda_i e_i$).
e) En déduire que la représentation ρ_d est irréductible.

f) Montrer qu'il existe, pour tout entier $d \in \{1, \dots, n\}$, une représentation irréductible de GL(V) dans $\bigwedge^d V$.
g) Que se passe-t-il si on remplace le corps **R** par un corps quelconque ?

1.3. Supplémentaire G-invariant. — Si W est une sous-représentation de V, il n'existe pas en général de supplémentaire G-invariant de W dans V.

Exemple 1.7. — Le groupe $G \leq GL_2(\mathbf{K})$ des matrices triangulaires supérieures se représente dans $V = \mathbf{K}^2$ par la représentation standard. La droite $W = \mathbf{K}e_1$ est une sous-représentation dépourvue de supplémentaire T-invariant.

Si **K** est le corps $\mathbf{F}_p$, on a ainsi un exemple avec un groupe G fini de cardinal $p(p-1)^2$.

Néanmoins, il y a quand même un résultat général d'existence de supplémentaire G-invariant pour certains groupes finis.

Théorème 1.8. — *Si* G *est un groupe fini tel que* $\mathrm{car}(\mathbf{K}) \nmid |G|$ *et que* V *est une représentation de* G*, tout sous-espace* G*-invariant de* V *admet un supplémentaire* G*-invariant.*

Corollaire 1.9. — *Soit* G *un groupe fini tel que* $\mathrm{car}(\mathbf{K}) \nmid |G|$. *Toute représentation de* G *de dimension finie est somme directe de représentations irréductibles.*

On va donner deux démonstrations du théorème, une première particulière à $\mathbf{K} = \mathbf{R}$ ou **C**, mais qui est valable aussi pour certains groupes infinis ; une seconde traitant tous les corps.

Première démonstration. — Supposons $\mathbf{K} = \mathbf{R}$ ou **C** et V de dimension finie. On choisit un produit scalaire ou un produit scalaire hermitien sur V, noté $\langle\ ,\ \rangle_0$. Puis on définit un autre produit scalaire par

$$\langle v, w\rangle = \frac{1}{|G|}\sum_{g\in G}\langle g\cdot v, g\cdot w\rangle_0. \tag{44}$$

Ce nouveau produit scalaire est G-invariant : pour tout $g \in G$, on a

$$\langle g\cdot v, g\cdot w\rangle = \langle v, w\rangle,$$

si bien que ρ est à valeurs dans O(V) ou U(V). En particulier, si W est un sous-espace G-invariant, $W^\perp$ est aussi G-invariant et fournit le supplémentaire voulu. □

L'ingrédient essentiel de cette démonstration consiste à fabriquer un produit scalaire G-invariant par moyennisation d'un produit scalaire quelconque donné. Si G est un groupe topologique compact, il est muni d'une mesure de probabilité G-invariante, la mesure de Haar : en remplaçant (44) par l'intégration sur le groupe, la démonstration s'étend à ce cas.

Seconde démonstration. — On applique encore un procédé de moyennisation. Choisissons un projecteur quelconque $p_0 : V \to V$ d'image un sous-espace G-invariant W et posons

$$p := \frac{1}{|G|}\sum_{g\in G}\rho(g)\circ p_0\circ\rho(g)^{-1} \in \mathrm{End}(V). \tag{45}$$

Comme $\rho(g)$ préserve W, l'image de cet endomorphisme est contenue dans W. Si $v \in W$, on a $\rho(g)^{-1}(v) \in W$, donc $p_0 \circ \rho(g)^{-1}(v) = \rho(g)^{-1}(v)$ et $p(v) = v$. Ceci montre que p est un projecteur d'image W.

Montrons que son noyau W' (supplémentaire de W) est invariant par G. Commençons par noter que, pour tout $h \in G$, on a

$$\begin{aligned}\rho(h) \circ p \circ \rho(h)^{-1} &= \frac{1}{|G|} \sum_{g \in G} \rho(h) \circ \rho(g) \circ p_0 \circ \rho(g)^{-1} \circ \rho(h)^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} \rho(hg) \circ p_0 \circ \rho(hg)^{-1} = p,\end{aligned}$$

c'est-à-dire $\rho(h) \circ p = p \circ \rho(h)$. Si $p(x) = 0$, alors $p \circ \rho(h)(x) = \rho(h) \circ p(x) = 0$, donc $\rho(h)(x) \in W'$. On a donc bien trouvé un supplémentaire G-invariant de W dans V. □

Lemme de Schur 1.10. — *Soit* G *un groupe fini tel que* $\mathrm{car}(\mathbf{K}) \nmid |G|$, *soient* (V, ρ_V) *et* (W, ρ_W) *des représentations irréductibles*[1] *de* G *et soit* $f : V \to W$ *un morphisme de représentations.*

1° Soit f est nul, soit c'est un isomorphisme.

2° Si $\rho_V = \rho_W$ et que $\mathbf{K}$ *est algébriquement clos, l'application f est une homothétie.*

Démonstration. — 1° Les sous-espaces $\ker(f)$ et $\mathrm{im}(f)$ sont G-invariants, donc triviaux.

2° Si λ est une valeur propre de f, alors $\ker(f - \lambda \mathrm{Id}_V)$ est G-invariant et non nul, donc égal à V, et f est une homothétie. □

Par le cor. 1.9, on peut décomposer la représentation régulière $\mathbf{K}^G$ (ex. 1.1.4°) en somme

$$\mathbf{K}^G = \bigoplus R_i$$

de représentations irréductibles. Soit (V, ρ) une représentation de G et soit $v_0 \in V$. L'application linéaire

$$\begin{aligned} f : \mathbf{K}^G &\longrightarrow V \\ (u : G \to \mathbf{K}) &\longmapsto \sum_{g \in G} u(g)\, \rho(g)(v_0)\end{aligned}$$

est un morphisme de représentations. En effet, pour tout $h \in G$ et tout $u \in \mathbf{K}^G$, on a (*cf.* ex. 1.1.4°)

$$\begin{aligned} f(\rho_R(h)(u)) &= \sum_{g \in G} \rho_R(h)(u)(g)\, \rho(g)(v_0) \\ &= \sum_{g \in G} u(h^{-1}g)\, \rho(g)(v_0) \\ &= \sum_{g' \in G} u(g')\, \rho(hg')(v_0) \\ &= \rho(h)(f(u)).\end{aligned}$$

Si $v_0 \neq 0$, l'application f n'est pas nulle (car $f(\varepsilon_e) = v_0$), et si de plus V est irréductible, f est surjective, donc il y a au moins un i tel que $f|_{R_i}$ soit non nul ; par le lemme de Schur, c'est un isomorphisme et V est isomorphe à la représentation R_i.

1. Donc de dimension finie par l'exerc. 1.5.

On en déduit le résultat suivant [2].

Proposition 1.11. — *Soit* G *un groupe fini tel que* $\mathrm{car}(\mathbf{K}) \nmid |\mathrm{G}|$. *Il n'y a à isomorphisme près qu'un nombre fini de représentations irréductibles de* G *et chacune est de dimension* $\leqslant |\mathrm{G}|$.

Lorsque **K** est algébriquement clos, ces résultats seront précisés dans le cor. 2.6.1° et, si de plus $\mathrm{car}(\mathbf{K}) = 0$, dans la prop. 2.8, où on montre que la dimension d'une représentation irréductible est $\leqslant \sqrt{|\mathrm{G}|}$.

Exercice 1.12. — Si $\mathrm{car}(\mathbf{K}) \nmid |\mathrm{G}|$, montrer que l'intersection des noyaux des représentations irréductibles de G est $\{e\}$.

Proposition 1.13. — *Soit* G *un groupe fini tel que* $\mathrm{car}(\mathbf{K}) \nmid |\mathrm{G}|$ *et soient* $\rho_1, \ldots, \rho_\ell$ *les représentations irréductibles de* G. *Toute représentation de* G *de dimension finie se décompose en* $\bigoplus \rho_i^{n_i}$, *où les entiers naturels* n_i *sont uniquement déterminés par la représentation.*

Démonstration. — L'existence d'une telle décomposition est le cor. 1.9. Montrons l'unicité des n_i par récurrence sur la dimension de la représentation. Supposons $\mathrm{V} := \bigoplus \mathrm{V}_i$ isomorphe à $\mathrm{W} := \bigoplus \mathrm{W}_j$, où les V_i et les W_j sont des représentations irréductibles, éventuellement répétées. On va montrer qu'à permutation près, les (V_i) et les (W_j) sont la même collection de représentations. On dispose d'un automorphisme de représentations

$$f : \bigoplus_i \mathrm{V}_i \xrightarrow{\sim} \bigoplus_j \mathrm{W}_j$$

dont on notera l'inverse g. Notons $p_i : \mathrm{V} \to \mathrm{V}_i$ et $q_j : \mathrm{W} \to \mathrm{W}_j$ les projections et considérons le morphisme de représentations

$$u_j := \mathrm{V}_1 \xrightarrow{f|_{\mathrm{V}_1}} \mathrm{W} \xrightarrow{q_j} \mathrm{W}_j \xrightarrow{g|_{\mathrm{W}_j}} \mathrm{V} \xrightarrow{p_1} \mathrm{V}_1.$$

On a

$$\sum_j u_j = \sum_j p_1 \circ g|_{\mathrm{W}_j} \circ q_j \circ f|_{\mathrm{V}_1} = p_1 \circ \Big(\sum_j g|_{\mathrm{W}_j} \circ q_j\Big) \circ f|_{\mathrm{V}_1} = p_1 \circ g \circ f|_{\mathrm{V}_1} = \mathrm{Id}_{\mathrm{V}_1}.$$

Au moins un des u_j est donc non nul et, quitte à rénuméroter les W_j, on peut supposer que c'est u_1. Les morphismes de représentations $q_1 \circ f|_{\mathrm{V}_1} : \mathrm{V}_1 \to \mathrm{W}_1$ et $p_1 \circ g|_{\mathrm{W}_1} : \mathrm{W}_1 \to \mathrm{V}_1$ sont alors non nuls. Par le lemme de Schur, ce sont des isomorphismes.

Pour appliquer l'hypothèse de récurrence, il suffit de montrer que le morphisme de représentations

$$(\mathrm{Id}_{\mathrm{W}} - q_1) f|_{\bigoplus_{i\geqslant 2} \mathrm{V}_i} : \bigoplus_{i\geqslant 2} \mathrm{V}_i \longrightarrow \bigoplus_{j\geqslant 2} \mathrm{W}_j$$

entre représentations de même dimension est encore un isomorphisme. C'est en effet le cas : si $x \in \bigoplus_{i\geqslant 2} \mathrm{V}_i$ est dans le noyau, $f(x) \in \mathrm{W}_1$ et $p_1 g(f(x)) = p_1(x) = 0$, donc, $p_1 \circ g|_{\mathrm{W}_1}$

2. Comme on l'a vu dans l'exerc. 1.5, la seconde partie est valable sans hypothèse sur la caractéristique du corps. Il en est de même de la première partie, mais il faut prendre garde que lorsque $\mathrm{car}(\mathbf{K}) \mid |\mathrm{G}|$, il existe des représentations (de dimension finie) qui ne sont pas sommes de représentations irréductibles, donc il y a des représentations indécomposables qui ne sont pas irréductibles. Et malheureusement, pour certains groupes finis, le nombre de classes d'isomorphisme de représentations indécomposables est infini (en caractéristique p, Higman a démontré que c'est le cas si les p-Sylow ne sont pas cycliques).

étant un isomorphisme, $f(x) = 0$ et $x = 0$. Ce morphisme est donc injectif. Comme source et but ont même dimension, c'est un isomorphisme. □

Sous les hypothèses de la proposition, on peut donc décomposer une représentation (V, ρ) de dimension finie du groupe G en somme directe $V = \bigoplus_i V_i$ de représentations irréductibles. *Cette décomposition n'est en général pas unique!* Dans le cas par exemple où tous les $\rho(g)$ sont l'identité (donc la seule représentation irréductible qui intervient est la représentation triviale, de dimension 1) , il s'agit simplement de décomposer V en somme directe de droites, ce qu'on peut faire de bien des façons.

2. Caractères

Dans cette section, on suppose G *fini,* **K** *algébriquement clos et* $\mathrm{car}(\mathbf{K}) \nmid |G|$.

Si (V, ρ) est une représentation de dimension finie de G, on appelle *caractère* de ρ la fonction

$$\begin{array}{rcl} \chi_\rho : G & \longrightarrow & \mathbf{K} \\ g & \longmapsto & \mathrm{tr}(\rho(g)). \end{array}$$

On a $\chi_\rho(e) = \dim(V)$, donc le caractère détermine la dimension de la représentation (on verra dans la prop. 2.8 que si **K** est algébriquement clos, le caractère détermine ρ complètement).

On calcule

$$\forall g, h \in G \qquad \chi_\rho(hgh^{-1}) = \mathrm{tr}\big(\rho(h)\rho(g)\rho(h)^{-1}\big) = \mathrm{tr}\big(\rho(g)\big) = \chi_\rho(g).$$

On dit que χ_ρ est une *fonction centrale,* ou encore *invariante par conjugaison.* Elle est constante sur chaque classe de conjugaison de G. Le **K**-espace vectoriel de toutes les fonctions centrales sur le groupe G sera noté $\mathscr{C}(G)$.

Rappelons (§ I.2.3) que les classes de conjugaisons de G sont les orbites sous l'action définie par $g \cdot x = gxg^{-1}$. Lorsque G est abélien, ces classes sont des singletons. Une fonction $f : G \to \mathbf{K}$ est centrale si et seulement si elle est constante sur chaque classe de conjugaison C de G ; on notera alors $f(C)$ sa valeur sur la classe C. La dimension du **K**-espace vectoriel $\mathscr{C}(G)$ est donc le nombre de classes de conjugaison.

Exemples 2.1. — 1° Le caractère de la représentation régulière est

$$\chi_R(g) = \begin{cases} |G| & \text{si } g = e, \\ 0 & \text{si } g \neq e. \end{cases}$$

C'est donc $|G|$ fois la fonction caractéristique $\mathbf{1}_{C_e}$ de la classe de conjugaison $C_e = \{e\}$.

2° Le caractère de la représentation standard de D_n dans $\mathbf{C}^2$ est donné par

$$\chi(r^k) = 2\cos\frac{2k\pi}{n}, \quad \chi(r^k s) = 0.$$

Il vaut donc 0 sur $\{s, rs, \ldots, r^{n-1}s\}$ (qui est la réunion de 1 ou 2 classes de conjugaison selon que n est impair ou non) et $2\cos\frac{2k\pi}{n}$ sur chaque classe de conjugaison $\{r^k, r^{-k}\}$.

3° Le groupe $\mathfrak{S}_3$ possède trois classes de conjugaison, celle de l'élément neutre e, celle à 3 éléments d'une transposition τ, et celle à 2 éléments d'un 3-cycle σ. Le caractère de

la représentation standard de $\mathfrak{S}_3$ dans $\mathbf{C}^3$ vaut 3 sur e, 1 sur les transpositions et 0 sur les 3-cycles.

Plus généralement, on a vu dans la prop. I.2.8 que les classes de conjugaison de $\mathfrak{S}_n$ sont en bijection avec les partitions de n :

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

une telle partition correspondant aux produits de cycles à supports disjoints d'ordre $k_1, \ldots, k_r$. Sur la classe de conjugaison correspondante, le caractère de la représentation standard de $\mathfrak{S}_n$ dans $\mathbf{C}^n$ vaut $\max\{i \mid k_i = 1\}$ (c'est le nombre de points fixes de la permutation).

Propriétés 2.2. — *1° Des représentations de dimension finie isomorphes ont même caractère.*

2° On a $\chi_{V^*}(g) = \chi_V(g^{-1})$.

3° On a $\chi_{V\oplus W} = \chi_V + \chi_W$.

4° Si $W \subseteq V$ *est une sous-représentation,* $\chi_V = \chi_W + \chi_{V/W}$.

5° On a $\chi_{V\otimes W} = \chi_V \chi_W$.

Démonstration. — Tout est évident, sauf la quatrième propriété qui découle de l'identité $\mathrm{tr}(u \otimes v) = \mathrm{tr}(u)\,\mathrm{tr}(v)$, qu'on peut vérifier dans une base (exerc. III.1.5). □

On introduit sur le $\mathbf{K}$-espace vectoriel $\mathbf{K}^G = \{f : G \to \mathbf{K}\}$ la forme bilinéaire symétrique

$$\langle f, f' \rangle = \frac{1}{|G|} \sum_{g\in G} f(g^{-1}) f'(g).$$

En particulier, $\langle f, \varepsilon_g \rangle = \frac{1}{|G|} f(g^{-1})$, donc cette forme est non dégénérée.

Théorème 2.3. — *Les caractères des représentations irréductibles de dimension finie forment une base orthonormale du* $\mathbf{K}$*-espace vectoriel* $\mathscr{C}(G)$ *des fonctions centrales sur* G.

Démonstration. — La démonstration du théorème va utiliser deux lemmes. Soient (V, ρ_V) et (W, ρ_W) des représentations de G et soit $u \in \mathrm{Hom}(V, W)$. Comme dans (45), on pose

$$\pi(u) = \frac{1}{|G|} \sum_{g\in G} \rho_W(g) \circ u \circ \rho_V(g)^{-1} \in \mathrm{Hom}(V, W).$$

Lemme 2.4. — *L'endomorphisme* π *de* $\mathrm{Hom}(V, W)$ *ainsi défini est un projecteur d'image* $\mathrm{Hom}_G(V, W)$ *et*

$$\mathrm{tr}(\pi) = \langle \chi_V, \chi_W \rangle.$$

Démonstration. — On rappelle que

$$\mathrm{Hom}_G(V, W) := \{u \in \mathrm{Hom}(V, W) \mid \forall h \in G \quad u \circ \rho_V(h) = \rho_W(h) \circ u\}.$$

Pour tout $h \in G$, on a bien

$$\begin{aligned}\rho_W(h)\circ\pi(u)\circ\rho_V(h)^{-1} &= \frac{1}{|G|}\sum_{g\in G}\rho_W(h)\circ\rho_W(g)\circ u\circ\rho_V(g)^{-1}\circ\rho_V(h)^{-1}\\ &= \frac{1}{|G|}\sum_{g\in G}\rho_W(hg)\circ u\circ\rho_V(g^{-1}h^{-1})\\ &= \frac{1}{|G|}\sum_{g'\in G}\rho_W(g')\circ u\circ\rho_V(g'^{-1})\\ &= \pi(u).\end{aligned}$$

De plus, si $u \in \mathrm{Hom}_G(V,W)$, on a $\pi(u) = u$, de sorte que π est bien un projecteur d'image $\mathrm{Hom}_G(V,W)$.

Choisissons des bases de V et W et notons e_{ij} l'élément de $\mathrm{Hom}(V,W)$ dont la matrice dans ces bases a tous ses coefficients sont nuls, sauf celui situé à la i-ème ligne et la j-ème colonne, qui vaut 1. Les (e_{ij}) forment une base de $\mathrm{Hom}(V,W)$. On a

$$\big(\rho_W(g)\circ e_{ij}\circ\rho_V(g)^{-1}\big)_{kl} = \rho_W(g)_{ki}\rho_V(g^{-1})_{jl}.$$

Appliquant ceci au cas particulier $i = k$ et $j = l$, on calcule

$$\begin{aligned}\mathrm{tr}(\pi) = \sum_{i,j}\pi(e_{ij})_{ij} &= \sum_{i,j}\frac{1}{|G|}\sum_{g\in G}\rho_W(g)_{ii}\rho_V(g^{-1})_{jj}\\ &= \frac{1}{|G|}\sum_{g\in G}\Big(\sum_i\rho_W(g)_{ii}\Big)\Big(\sum_j\rho_V(g^{-1})_{jj}\Big)\\ &= \frac{1}{|G|}\sum_{g\in G}\chi_W(g)\chi_V(g^{-1}).\end{aligned}$$

Ceci démontre le lemme. □

Si V et W sont irréductibles, on a par le lemme de Schur

$$\mathrm{Hom}_G(V,W) = \begin{cases}0 & \text{si V et W ne sont pas isomorphes,}\\ \mathbf{K} & \text{si V et W sont isomorphes.}\end{cases}$$

Comme le rang d'un projecteur est sa trace, le lemme 2.4 entraîne que $\langle\chi_V,\chi_W\rangle = \mathrm{tr}(\pi)$ vaut 0 dans le premier cas, 1 dans le second. Donc la famille des (χ_V), pour V irréductible (ou plus exactement, pour V décrivant l'ensemble des classes d'isomorphisme de représentations irréductibles de G), est orthonormale ; il reste à voir qu'elle engendre tout $\mathscr{C}(G)$.

Lemme 2.5. — *Soit* (V,ρ) *une représentation de* G. *Si* $f : G \to \mathbf{K}$ *est une fonction centrale, posons*

$$f_\rho := \frac{1}{|G|}\sum_{g\in G} f(g)\rho(g^{-1}) \in \mathrm{End}(V).$$

1° On a $f_\rho \in \mathrm{End}_G(V)$ *et* $\mathrm{tr}(f_\rho) = \langle f,\chi_\rho\rangle$.

2° Si (V,ρ) *est irréductible,* $\dim(V)\cdot 1_{\mathbf{K}}$ *est inversible dans* $\mathbf{K}$ *et* f_ρ *est l'homothétie de* V *de rapport* $\frac{\langle f,\chi_\rho\rangle}{\dim(V)}$.

Démonstration. — On calcule, puisque f est centrale,

$$\forall h \in \mathrm{G} \qquad \rho(h) \circ f_\rho \circ \rho(h)^{-1} = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\rho(hg^{-1}h^{-1})$$
$$= \frac{1}{|\mathrm{G}|} \sum_{g' \in \mathrm{G}} f(h^{-1}g'h)\rho(g'^{-1}) = \frac{1}{|\mathrm{G}|} \sum_{g' \in \mathrm{G}} f(g')\rho(g'^{-1}) = f_\rho.$$

Donc $f_\rho \in \mathrm{End}_{\mathrm{G}}(\mathrm{V})$ et sa trace est

$$\mathrm{tr}(f_\rho) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\chi_\rho(g^{-1}) = \langle f, \chi_\rho \rangle.$$

Ceci montre le premier point.

Si ρ est irréductible, on déduit du lemme de Schur 1.10 et du premier point appliqué à la fonction centrale $f = \chi_\rho$ que $(\chi_\rho)_\rho$ est une homothétie. Si λ est son rapport, on a $\mathrm{tr}((\chi_\rho)_\rho) = \dim(\mathrm{V})\lambda = \langle \chi_\rho, \chi_\rho \rangle = 1_{\mathbf{K}}$. En particulier, $\dim(\mathrm{V}) \cdot 1_{\mathbf{K}}$ est inversible dans $\mathbf{K}$.

Pour f fonction centrale quelconque, f_ρ est de nouveau une homothétie par le lemme de Schur 1.10. Comme sa trace est $\langle f, \chi_\rho \rangle$, son rapport est $\frac{\langle f, \chi_\rho \rangle}{\dim(\mathrm{V})}$. Cela montre le second point. □

Si une fonction centrale $f \in \mathscr{C}(\mathrm{G})$ est orthogonale à tous les caractères χ_ρ, on a, par le lemme, $f_\rho = 0$ pour toute représentation ρ irréductible, et donc pour toute représentation puisque $f_{\rho \oplus \rho'} = f_\rho \oplus f_{\rho'}$. Appliquant cela à la représentation régulière, on obtient $f_{\rho_{\mathrm{R}}} = 0$ donc

$$0 = f_{\rho_{\mathrm{R}}}(\varepsilon_e) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\rho_{\mathrm{R}}(g^{-1})(\varepsilon_e) = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} f(g)\varepsilon_{g^{-1}}$$

dans $\mathbf{K}^{\mathrm{G}}$, ce qui entraîne $f = 0$, puisque les $\varepsilon_{g^{-1}}$ forment une base de $\mathbf{K}^{\mathrm{G}}$.

Cela termine la preuve du th. 2.3 : tout $f \in \mathscr{C}(\mathrm{G})$ s'écrit $f = \sum_{\rho \text{ irr}} \langle f, \chi_\rho \rangle \chi_\rho$. □

Corollaire 2.6. — *1° Le nombre de représentations irréductibles de* G *est égal au nombre de classes de conjugaison de* G.

2° Soient $\chi_1, \ldots, \chi_\ell$ *les caractères des représentations irréductibles de* G. *Soient* C *et* C′ *des classes de conjugaison dans* G. *On a*

$$\sum_{i=1}^{\ell} \chi_i(\mathrm{C}^{-1})\chi_i(\mathrm{C}') = \begin{cases} \frac{|\mathrm{G}|}{|\mathrm{C}|} \cdot 1_{\mathbf{K}} & \textit{si } \mathrm{C} = \mathrm{C}', \\ 0 & \textit{sinon.} \end{cases}$$

L'entier $|\mathrm{C}|$ divise l'ordre de G puisque c'est le cardinal d'une orbite pour l'action de G sur lui-même par conjugaison (*cf.* § I.2.2).

Lorsque la caractéristique de $\mathbf{K}$ divise l'ordre de G, le premier énoncé n'est plus nécessairement vrai (*cf.* rem. 2.13).

Démonstration. — La dimension de $\mathscr{C}(\mathrm{G})$ est égale au nombre de classes de conjugaison dans G, d'où le premier énoncé. Pour le second, soit $\mathbf{1}_{\mathrm{C}}$ la fonction caractéristique de C. Alors $f = \mathbf{1}_{\mathrm{C}}$ est une fonction centrale qui se décompose sur la base orthonormale des caractères χ_i des représentations irréductibles :

$$\mathbf{1}_{\mathrm{C}} = \sum_{i=1}^{\ell} \langle \mathbf{1}_{\mathrm{C}}, \chi_i \rangle \chi_i, \quad \text{avec } \langle \mathbf{1}_{\mathrm{C}}, \chi_i \rangle = \frac{1}{|\mathrm{G}|} |\mathrm{C}| \chi_i(\mathrm{C}^{-1}).$$

Il en résulte

$$\mathbf{1}_{\mathrm{C}} = \frac{|\mathrm{C}|}{|\mathrm{G}|} \sum_{i=1}^{\ell} \chi_i(\mathrm{C}^{-1})\chi_i,$$

ce qui est exactement le résultat voulu. □

On a déjà remarqué que la décomposition $\mathrm{V} = \bigoplus_i \mathrm{V}_i$ d'une représentation en somme directe de représentations irréductibles n'est pas unique. En revanche, si on regroupe tous les V_i isomorphes à la même représentation irréductible, on obtient une décomposition $\mathrm{V} = \bigoplus_j \mathrm{W}_j$ *en composantes isotypiques* indépendante des choix.

Théorème 2.7. — *Soit* (V,ρ) *une représentation de dimension finie du groupe fini* G. *La projection de* V *sur la composante isotypique correspondant à une représentation irréductible* (U,ψ) *est donnée par*

$$p_{\mathrm{U}} = \frac{\dim(\mathrm{U})}{|\mathrm{G}|} \sum_{g\in\mathrm{G}} \chi_\psi(g)\rho(g^{-1}).$$

En particulier, la décomposition en composantes isotypiques ne dépend que de la représentation (V,ρ).

Démonstration. — Soit f une fonction centrale sur G. Par sa définition même, l'endomorphisme f_ρ de V laisse stable toute sous-représentation (V_i,ρ_i) de (V,ρ) et se restreint à V_i en f_{ρ_i}. Si V_i est de plus irréductible, f_{ρ_i} est l'homothétie de V_i de rapport $\frac{\langle f,\chi_i\rangle}{\dim(\mathrm{V}_i)}$ (lemme 2.5.2°).

Par le th. 2.3, si f est le caractère χ_ψ d'une représentation irréductible (U,ψ), l'endomorphisme $(\chi_\psi)_\rho|_{\mathrm{V}_i}$ est donc $\frac{1}{\dim(\mathrm{V}_i)}\mathrm{Id}_{\mathrm{V}_i}$ si V_i est isomorphe à U et 0 sinon. Comme $p_{\mathrm{U}} = \dim(\mathrm{U})(\chi_\psi)_\rho$, sa restriction à V_i est donc l'identité de V_i si V_i est isomorphe à U et 0 sinon. Ceci démontre le théorème. □

On peut maintenant montrer qu'en caractéristique 0, une représentation est déterminée par son caractère. On identifie aussi les représentations irréductibles comme étant celles dont le caractère est de norme 1.

Proposition 2.8. — *Notons* $\rho_1,\dots,\rho_\ell$ *les représentations irréductibles du groupe fini* G. *Soit* ρ *une représentation de* G, *qu'on décompose en* $\rho = \bigoplus_{i=1}^{\ell} \rho_i^{n_i}$ *(prop. 1.13). On a*

$$\langle\chi_\rho,\chi_{\rho_i}\rangle = n_i\cdot 1_{\mathbf{K}} \quad , \quad \langle\chi_\rho,\chi_\rho\rangle = \Big(\sum_{i=1}^{\ell} n_i^2\Big)\cdot 1_{\mathbf{K}}.$$

Si $\mathrm{car}(\mathbf{K}) = 0$,

- *des représentations* ρ *et* ρ' *de* G *sont isomorphes si et seulement si* $\chi_\rho = \chi_{\rho'}$;
- ρ *est irréductible si et seulement si* $\langle\chi_\rho,\chi_\rho\rangle = 1_{\mathbf{K}}$;
- *la représentation régulière se décompose en* $\mathbf{K}^{\mathrm{G}} = \bigoplus_{i=1}^{\ell} \rho_i^{\dim(\rho_i)}$; *en particulier,* $\sum_{i=1}^{\ell} \dim(\rho_i)^2 = |\mathrm{G}|$.

Si $\mathrm{car}(\mathbf{K}) = p \neq 0$, il est faux que le caractère détermine la représentation ; par exemple, pour toute représentation V, le caractère de V^p est nul.

Une autre contrainte importante sur les dimensions des représentations irréductibles est qu'elles divisent l'ordre du groupe. Ce théorème plus difficile (th. 3.6) sera vu dans le § 3.2 en caractéristique nulle.

Démonstration. — On a $\chi_\rho = \sum_{i=1}^{\ell} n_i \chi_{\rho_i}$, donc $\langle \chi_\rho, \chi_{\rho_i} \rangle = n_i \cdot 1_{\mathbf{K}}$ et $\langle \chi_\rho, \chi_\rho \rangle = (\sum_{i=1}^{\ell} n_i^2) \cdot 1_{\mathbf{K}}$.

Ainsi, en caractéristique nulle, χ_ρ détermine les entiers n_i et donc toute la représentation ρ, et ρ est irréductible si et seulement si $\langle \chi_\rho, \chi_\rho \rangle = 1_{\mathbf{K}}$.

Appliquons cela à la représentation régulière : puisque $\chi_R = |G| \mathbf{1}_{\{e\}}$, on obtient $\langle \chi_R, \chi_{\rho_i} \rangle = \chi_{\rho_i}(e) = \dim(\rho_i)$, d'où il résulte que la représentation régulière est isomorphe à $\bigoplus_{i=1}^{\ell} \rho_i^{\dim(\rho_i)}$. □

Proposition 2.9. — *Supposons* $\mathrm{car}(\mathbf{K}) = 0$. *Le groupe* G *est abélien si et seulement si toutes ses représentations irréductibles sont de dimension* 1.

Démonstration. — Un groupe G est abélien si et seulement si il a exactement |G| classes de conjugaison, donc |G| représentations irréductibles. Or $|G| = \sum_{i=1}^{\ell} \dim(\rho_i)^2$, donc $\ell \leqslant |G|$ avec égalité si et seulement si toutes les représentations irréductibles sont de dimension 1. □

Exercice 2.10. — Soit p un nombre premier, soit G un p-groupe (c'est-à-dire un groupe fini de cardinal une puissance de p ; *cf.* prop. I.2.13) et soit $\mathbf{K}$ un corps de caractéristique p. Montrer que la seule représentation irréductible ρ de G dans un $\mathbf{K}$-espace vectoriel est la représentation triviale (*Indication :* si V est une telle représentation et $v \in V - \{0\}$, on pourra considérer le sous-groupe additif de V engendré par les $\rho(g)(v)$, pour g décrivant G, montrer que c'est un p-groupe, et appliquer la prop. I.2.13).

2.1. Table des caractères. — On prend $\mathbf{K} = \mathbf{C}$. Pour toute représentation (V, ρ) d'un groupe fini G, on a $\rho(g)^{|G|} = \mathrm{Id}_V$, donc les valeurs propres de $\rho(g)$ sont des racines de l'unité, et celles de $\rho(g^{-1})$ sont leurs conjugués. On a donc

$$\chi_\rho(g^{-1}) = \mathrm{tr}(\rho(g^{-1})) = \overline{\mathrm{tr}(\rho(g))} = \overline{\chi_\rho(g)}.$$

On a ainsi

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_\rho(g)} \chi_{\rho'}(g) \tag{46}$$

et, si $\chi_1, \ldots, \chi_\ell$ sont les caractères des représentations irréductibles de G, le cor. 2.6.2° donne

$$\sum_{i=1}^{\ell} \overline{\chi_i(C)} \chi_i(C') = \begin{cases} \frac{|G|}{|C|} & \text{si } C = C', \\ 0 & \text{sinon.} \end{cases} \tag{47}$$

Comme $\chi_\rho(g)$ est la somme des valeurs propres, on a aussi

$$\forall g \in G \qquad |\chi_\rho(g)| \leqslant \chi_\rho(e) = \dim(V).$$

De plus, $\chi_\rho(g) = \chi_\rho(e)$ si et seulement si $\rho(g) = \mathrm{Id}_V$. On a donc

$$\{g \in G \mid \chi_\rho(g) = \chi_\rho(e)\} = \ker(\rho) \trianglelefteq G.$$

De même, on a $|\chi_\rho(g)| = \chi_\rho(e)$ si et seulement si $\rho(g)$ est une homothétie.

La *table des caractères* de G donne la valeur de chaque caractère sur chaque classe de conjugaison ; les lignes correspondent aux caractères et les colonnes aux classes de conjugaison. C'est une table carrée (cor. 2.6.1°). Les relations obtenues se traduisent par le fait que

- les colonnes sont orthogonales (pour le produit scalaire hermitien standard) ;
- la colonne correspondant à la classe de conjugaison C est de norme hermitienne (au carré) $|G|/|C|$ (*cf.* (47)) ;
- les lignes sont orthogonales et de norme (au carré) $|G|$ pour le produit scalaire hermitien pondéré par le cardinal des classes de conjugaison (*cf.* (46)) ;
- la somme des lignes pondérées par les dimensions $\chi(e)$ est la ligne $|G|\ 0\ \cdots\ 0$.

Exercice 2.11. — Montrer qu'une table des caractères est une matrice inversible.

On peut utiliser cette table pour obtenir des informations sur les sous-groupes distingués de G. Un tel sous-groupe est réunion de classes de conjugaisons. Pour chaque caractère χ, la réunion des classes sur lesquelles χ prend la valeur $\chi(e)$ est un sous-groupe $G_\chi \trianglelefteq G$ et tout sous-groupe distingué de G est obtenu comme intersection de G_χ (utiliser l'exerc. 1.12).

En particulier, G est simple si et seulement si tous les G_χ à part $G_{\chi_{\text{triv}}} = G$ sont triviaux, c'est-à-dire si et seulement si dans chaque ligne excepté celle correspondant à la représentation triviale (qui est la seule composée uniquement de 1), la valeur $\chi(e)$ n'apparaît qu'une seule fois (dans la colonne correspondant à la classe $\{e\}$).

Les représentations de dimension 1 sont des morphismes $G \to \mathbf{C}^\times$ donc elles se factorisent par $G/D(G)$. Par le même raisonnement, le groupe dérivé $D(G)$ est l'intersection des G_χ pour tous les caractères χ de représentations de dimension 1.

On s'intéresse maintenant au centre $Z(G)$ de G. Si $g \in Z(G)$, alors $\rho_i(g)$ commute avec tous les $\rho_i(h)$ donc, par le lemme de Schur 1.10, c'est une homothétie de rapport une racine de l'unité et $|\chi_i(g)| = \chi_i(e)$ pour tout i. Inversement, si $|\chi_i(g)| = \chi_i(e)$, on a vu plus haut que $\rho_i(g)$ est une homothétie, donc commute avec tous les $\rho_i(h)$. Si c'est vrai pour tout i, alors $\rho(g)$ commute avec tous les $\rho(h)$ pour toute représentation ρ. En appliquant cela à une représentaiton fidèle (c'est-à-dire pour laquelle ρ est injective) comme la représentation régulière, on obtient $g \in Z(G)$.

Le centre de G est donc la réunion des classes de conjugaison C pour lesquelles $|\chi_i(C)| = \chi_i(e)$ pour tout i.

Les contraintes obtenues sur les caractères sont suffisantes pour obtenir une description complète des représentation irréductibles du groupe G dans certains cas. On traite ici quelques exemples.

Le groupe $\mathfrak{S}_3 = D_3$. — On a vu qu'il y a trois classes de conjugaison : celle de l'élément neutre e, celle des transpositions τ, et celles des 3-cycles σ. Il y a donc trois représentations irréductibles de $\mathfrak{S}_3$.

Les représentations de dimension 1 sont les morphismes $G \to G/D(G) \to \mathbf{C}^\times$. Dans notre cas, le groupe dérivé est $\mathfrak{A}_3$ et $\mathfrak{S}_3/\mathfrak{A}_3 \simeq \mathbf{Z}/2\mathbf{Z}$. Il y a donc deux représentations de dimension 1, facilement identifiées : la représentation triviale $\mathbf{C}_{\text{triv}}$ (de caractère χ_{triv}) et la signature $\mathbf{C}_{\text{sign}}$ (de caractère χ_{sign}). Par la prop. 2.8, la somme des carrés des dimensions

des représentations est $|\mathfrak{S}_3| = 6$, soit $1+1+4=6$ donc la dimension de la dernière représentation irréductible est 2. On peut alors dresser la table des caractères, en indiquant au-dessus de chaque classe de conjugaison son cardinal :

$\mathfrak{S}_3$	1	3	2
	e	τ	σ
χ_{triv}	1	1	1
χ_{sign}	1	-1	1
χ	2	0	-1

La première colonne donne la dimension des représentations. La troisième ligne, *a priori* inconnue, est obtenue en utilisant le fait que les colonnes sont orthogonales ; une autre méthode est d'écrire (prop. 2.8) $\chi_{\text{triv}} + \chi_{\text{sign}} + 2\chi = \chi_R = 6 \cdot \mathbf{1}_{\{e\}}$ d'où on déduit également le dernier caractère χ.

On a ainsi déterminé le caractère de la troisième représentation sans la connaître, mais on peut aussi la décrire explicitement : d'après l'ex. 1.2.2°, $\mathfrak{S}_3$ a une représentation ρ dans le plan complexe $V_0 = \{(x_1,x_2,x_3) \in \mathbf{C}^3 \mid x_1+x_2+x_3 = 0\}$ dont la somme directe avec la représentation triviale de dimension 1 est la représentation de permutation, de caractère (ex. 2.1.3°) de valeurs 3,1 et 0, qui est bien la somme $\chi_{\text{triv}} + \chi$.

On reconnaît les sous-groupes distingués de $\mathfrak{S}_3$: ce sont $\mathfrak{S}_3$ (noyau de χ_{triv}), $\mathfrak{A}_3 = \{e\} \cup \{\sigma\}$ (noyau de χ_{sign}) et $\{e\}$ (noyau de χ). Le groupe dérivé est $\mathfrak{A}_3$ (noyau de χ_{sign}) et le centre est trivial.

La table des caractères peut aussi être utilisée pour calculer la décomposition en composantes irréductibles d'une représentation donnée, grâce à la prop. 2.8. Par exemple, décomposons le produit tensoriel $V_0 \otimes V_0$, où V_0 est la représentation irréductible d'ordre 2. Son caractère est χ^2, de valeurs 4, 0, 1 ; c'est donc $\chi_{\text{triv}} + \chi_{\text{sign}} + \chi$. On a ainsi

$$V_0 \otimes V_0 \simeq \mathbf{C}_{\text{triv}} \oplus \mathbf{C}_{\text{sign}} \oplus V_0.$$

Remarquons qu'on connaissait déjà, par (40), la décomposition $V_0 \otimes V_0 = S^2V_0 \oplus \bigwedge^2 V_0$. Le morceau $\bigwedge^2 V_0$, de dimension 1, est $\mathbf{C}_{\text{sign}}$ (c'est le déterminant), tandis que le morceau S^2V_0 se décompose en deux.

Exercice 2.12. — Soit V une représentation réelle d'un groupe fini G. Montrer que la représentation S^2V contient une sous-représentation de dimension 1 (*Indication :* on pourra utiliser la construction de la première démonstration du th. 1.8).

Le groupe D_4. — Le groupe de symétrie du carré est engendré par une rotation r d'angle $\frac{\pi}{2}$ et une symétrie s. On a $sr^k s = r^{-k}$ et $rsr^{-1} = sr^2$, ce qui donne 5 classes de conjugaison : $\{\text{Id}\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, r^2 s\}$ et $\{rs, r^3 s\}$. Le sous-groupe $\mathbf{Z}/2\mathbf{Z} = \{\text{Id}, -\text{Id} = r^2\}$ est distingué et dans le quotient les trois éléments distincts r, s et rs sont d'ordre 2, donc

$$D_4/(\mathbf{Z}/2\mathbf{Z}) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

Cela nous donne donc quatre représentations de dimension 1 correspondant aux quatre morphismes $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \to \mathbf{C}^\times$; la cinquième doit donc être de dimension 2. Appliquant

la même méthode que précédemment, on obtient la table des caractères :

D_4	1	1	2	2	2
	e	r^2	$\{r, r^3\}$	$\{s, r^2 s\}$	$\{rs, r^3 s\}$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
$\chi_1\chi_2$	1	1	-1	-1	1
χ_ρ	2	-2	0	0	0

La représentation de dimension 2 ici n'est autre que la représentation standard ρ dans $\mathbf{C}^2$ (ex. 2.1.3°).

Les sous-groupes distingués de D_4 sont D_4, $\{e, r^2, s, r^2 s\}$ (noyau de χ_1), $\{e, r, r^2, r^3\}$ (noyau de χ_2), $\{e, r^2, rs, r^3 s\}$ (noyau de $\chi_1\chi_2$), $\{e\}$ et leurs intersections. Le groupe dérivé est $\{e, r^2\}$ ($\ker(\chi_1) \cap \ker(\chi_2)$) et c'est aussi le centre $\{g \in D_4 \mid \forall i \ \ |\chi_i(g)| = \chi_i(e)\}$.

Le groupe $\mathfrak{S}_4$. — On a (prop. I.2.8) 5 classes de conjugaison, correspondant aux partitions (1111) (classe de Id), (112) (classe d'une transposition, de cardinal 6), (13) (classe d'un 3-cycle, de cardinal 8), (4) (classe d'un 4-cycle, de cardinal 6) et (22) (classe d'une double transposition, de cardinal 3) de 4, donc 5 représentations irréductibles. D'autre part, on a $D(\mathfrak{S}_4) = \mathfrak{A}_4$ (prop. I.5.8), donc deux représentations irréductibles de dimension 1, la représentation triviale $\mathbf{C}_{\text{triv}}$ et la signature $\mathbf{C}_{\text{sign}}$.

On a aussi la représentation de dimension 3 de $\mathfrak{S}_4$ dans $V_0 = \{(x_1, x_2, x_3, x_4) \in \mathbf{C}^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}$. Le caractère de $V_0 \oplus \mathbf{C}_{\text{triv}}$ a été calculé dans l'ex. 2.1.3° : il prend les valeurs 4, 2, 1, 0, 0. Le caractère de V_0 prend donc les valeurs 3, 1, 0, -1, -1. On a

$$\langle \chi_{V_0}, \chi_{V_0} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)^2 = \frac{1}{24}(9 \times 1 + 1 \times 6 + 1 \times 6 + 1 \times 3) = 1,$$

de sorte que V_0 est irréductible (prop. 2.8).

Il nous reste deux représentations irréductibles à trouver, dont la somme des carrés des dimensions est $24 - 1 - 1 - 9 = 13$. Elles sont donc de dimension 2 et 3. L'une d'elles est $V_0 \otimes \mathbf{C}_{\text{sign}}$, dont le caractère prend les valeurs 3, -1, 0, 1, -1. Elle est irréductible (on peut voir ça soit en calculant $\langle \chi_{V_0 \otimes \mathbf{C}_{\text{sign}}}, \chi_{V_0 \otimes \mathbf{C}_{\text{sign}}} \rangle$, soit en remarquant que le produit tensoriel d'une représentation irréductible et d'une représentation de dimension 1 est encore irréductible).

On a donc déjà la table de caractères partielle

$\mathfrak{S}_4$	1	6	8	6	3
	Id	(12)	(123)	(1234)	(12)(34)
χ_{triv}	1	1	1	1	1
χ_{sign}	1	-1	1	-1	1
χ_{V_0}	3	1	0	-1	-1
$\chi_{V_0}\chi_{\text{sign}}$	3	-1	0	1	-1
χ_V	2	$\star$	$\star$	$\star$	$\star$

dont on peut compléter la dernière ligne en utilisant le fait que les colonnes sont orthogonales :

$\mathfrak{S}_4$	1	6	8	6	3
	Id	(12)	(123)	(1234)	(12)(34)
χ_{triv}	1	1	1	1	1
χ_{sign}	1	−1	1	−1	1
χ_{V_0}	3	1	0	−1	−1
$\chi_{V_0}\chi_{\text{sign}}$	3	−1	0	1	−1
χ_V	2	0	−1	0	2

Comment déterminer cette dernière représentation irréductible (V,ρ) ? L'astuce est de noter que $\rho((12)(34))$ est de trace 2, donc c'est l'identité. La représentation ρ se factorise donc par la surjection $\mathfrak{S}_4 \twoheadrightarrow \mathfrak{S}_4/K$, où $K \lhd \mathfrak{S}_4$ est d'ordre 4 (ex. I.5.3.3°). Le groupe $\mathfrak{S}_4/K$ est isomorphe à $\mathfrak{S}_3$. Il y a donc une représentation irréductible de degré 2 (comme on l'a vu plus haut).

Les sous-groupes distingués de $\mathfrak{S}_4$ sont $\mathfrak{S}_4$, $\mathfrak{A}_4$ (noyau de χ_{sign}), K (noyau de χ_V) et $\{e\}$. Le groupe dérivé est $\mathfrak{A}_4$ (noyau de χ_{sign}) et le centre est trivial puisque par exemple $\{\sigma \in \mathfrak{S}_4 \mid |\chi_{V_0}(\sigma)| = \chi_{V_0}(\text{Id}) = 3\} = \{\text{Id}\}$.

Remarque 2.13. — Cette discussion reste valable sur tout corps $\mathbf{K}$ de caractéristique autre que 2 et 3 : $\mathfrak{S}_4$ a encore, à isomorphisme près, 5 classes de représentations irréductibles. Sur un corps de caractéristique 2, il n'y en a plus que 2, à savoir $\mathbf{K}_{\text{triv}}$ et V ; en caractéristique 3, il y en a 4, à savoir toutes celles de la table ci-dessus à l'exception de V (qui devient isomorphe à $\mathbf{K}_{\text{triv}} \oplus \mathbf{K}_{\text{sign}}$).

Le groupe $\mathfrak{S}_5$. — On a (prop. I.2.8) 7 classes de conjugaison, correspondant aux partitions (11111) (classe de Id), (1112) (classe d'une transposition, de cardinal 10), (113) (classe d'un 3-cycle, de cardinal 20), (14) (classe d'un 4-cycle, de cardinal 30), (5) (classe d'un 5-cycle, de cardinal 24), (122) (classe d'une double transposition, de cardinal 15) et (23) (de cardinal 20) de 5, donc 7 représentations irréductibles. D'autre part, on a $D(\mathfrak{S}_5) = \mathfrak{A}_5$ (prop. I.5.8), donc il y a exactement deux représentations irréductibles de dimension 1, la représentation triviale $\mathbf{C}_{\text{triv}}$ et la signature $\mathbf{C}_{\text{sign}}$.

On a aussi la représentation de dimension 4 de $\mathfrak{S}_5$ dans $V_0 = \{(x_1,\dots,x_5) \in \mathbf{C}^5 \mid x_1+\cdots+x_5 = 0\}$ dont le caractère prend les valeurs 4, 2, 1, 0, −1, 0, −1. On calcule $\langle \chi_{V_0}, \chi_{V_0}\rangle = 1$, de sorte que V_0 est irréductible (prop. 2.8). La représentation $V_0 \otimes \mathbf{C}_{\text{sign}}$ est aussi irréductible.

Si V est une représentation de G, on a vu que la représentation $V \otimes V$ se scinde en $S^2V \oplus \bigwedge^2 V$. Le lemme suivant nous permet de calculer les caractères.

Lemme 2.14. — *On a* $\chi_{\bigwedge^2 V}(g) = \frac{1}{2}\big(\chi_V(g)^2 - \chi_V(g^2)\big)$ *et* $\chi_{S^2V}(g) = \frac{1}{2}\big(\chi_V(g)^2 + \chi_V(g^2)\big)$.

Démonstration. — Les $\rho(g)$ étant d'ordre fini, ils sont diagonalisables (leur polynôme minimal est à racines simples). Soit $g \in G$; il existe une base $(e_1,\dots,e_n)$ de V formée de vecteurs propres de $\rho(g)$, avec valeurs propres $\lambda_1,\dots,\lambda_n$. Une base de $\bigwedge^2 V$ est donnée par les $(e_i \wedge e_j)_{1\leqslant i<j\leqslant n}$ et ce sont des vecteurs propres pour $\bigwedge^2 \rho(g)$, avec valeurs propres

$(\lambda_i\lambda_j)_{1\leqslant i<j\leqslant n}$. On a donc

$$\chi_{\wedge^2 V}(g)=\sum_{1\leqslant i<j\leqslant n}\lambda_i\lambda_j=\frac{1}{2}\Big(\sum_{1\leqslant i\leqslant n}\lambda_i\Big)^2-\frac{1}{2}\sum_{1\leqslant i\leqslant n}\lambda_i^2.$$

De même, les valeurs propres de $S^2\rho(g)$ sont les $(\lambda_i\lambda_j)_{1\leqslant i\leqslant j\leqslant n}$ et

$$\chi_{S^2 V}(g)=\sum_{1\leqslant i\leqslant j\leqslant n}\lambda_i\lambda_j=\frac{1}{2}\Big(\sum_{1\leqslant i\leqslant n}\lambda_i\Big)^2+\frac{1}{2}\sum_{1\leqslant i\leqslant n}\lambda_i^2.$$

Le lemme en résulte. □

On en déduit les valeurs du caractère $\chi_{\wedge^2 V_0}$ et on vérifie que cette représentation est irréductible.

On a donc déjà la table de caractères partielle (on note l'isomorphisme de représentations $\wedge^2 V_0\simeq\wedge^2 V_0\otimes\mathbf{C}_{\text{sign}}$)

$\mathfrak{S}_5$	1	10	20	30	24	15	20
	Id	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
χ_{triv}	1	1	1	1	1	1	1
χ_{sign}	1	−1	1	−1	1	1	−1
χ_{V_0}	4	2	1	0	−1	0	−1
$\chi_{V_0}\chi_{\text{sign}}$	4	−2	1	0	−1	0	1
$\chi_{\wedge^2 V_0}$	6	0	0	0	1	−2	0

Il nous reste deux représentations irréductibles à trouver, dont la somme des carrés des dimensions est $120-1-1-16-16-36=50$. Elles sont de dimension >1, donc toutes les deux de dimension 5. Notons l'une d'elles V et soient 5, a_1, a_2, a_3, a_4, a_5, a_6 les valeurs de son caractère. Le caractère de $V\otimes\mathbf{C}_{\text{sign}}$ prend alors les valeurs 5, $-a_1$, a_2, $-a_3$, a_4, a_5, $-a_6$. De deux choses l'une :

- soit les deux représentations manquantes ont $a_1=a_3=a_6=0$ (et chacune est isomorphe à son produit tensoriel avec $\mathbf{C}_{\text{sign}}$) ;
- soit les deux représentations manquantes sont V et $V\otimes\mathbf{C}_{\text{sign}}$.

Dans le premier cas, les colonnes 2 et 4 ne peuvent être orthogonales, donc on est dans le second cas. Les relations d'orthogonalité permettent alors de compléter la table (les calculs sont laissés au lecteur) ; on obtient

$\mathfrak{S}_5$	1	10	20	30	24	15	20
	Id	(12)	(123)	(1234)	(12345)	(12)(34)	(12)(345)
χ_{triv}	1	1	1	1	1	1	1
χ_{sign}	1	−1	1	−1	1	1	−1
χ_{V_0}	4	2	1	0	−1	0	−1
$\chi_{V_0}\chi_{\text{sign}}$	4	−2	1	0	−1	0	1
$\chi_{\wedge^2 V_0}$	6	0	0	0	1	−2	0
χ_V	5	1	−1	−1	0	1	1
$\chi_V\chi_{\text{sign}}$	5	−1	−1	1	0	1	−1

Une autre façon de compléter la table est de s'intéresser au caractère χ de la représentation S^2V_0. Il prend les valeurs (lemme 2.14) 10, 4, 1, 0, 0, 2, 1 donc

$$\langle\chi,\chi\rangle = \frac{1}{120}(100\times 1+16\times 10+4\times 15+1\times 20) = 3.$$

Cette représentation est donc somme de 3 représentations irréductibles. Comme elle est de dimension 10, ces représentations sont nécessairement de dimension 1, 4 et 5 ; on note cette dernière V. Sans même calculer $\langle\chi,\chi_{\text{triv}}\rangle$, on voit que c'est strictement positif, donc $\mathbf{C}_{\text{triv}}$ intervient dans S^2V_0 (cela résulte aussi de l'exerc. 2.12, puisque V_0 est en fait une représentation réelle). On calcule aussi $\langle\chi,\chi_{V_0}\rangle = 1$, donc $\chi = \chi_{\text{triv}}+\chi_{V_0}+\chi_V$, d'où on déduit χ_V. On voit ensuite $\chi_V \neq \chi_V\chi_{\text{sign}}$ et on complète la table.

Les sous-groupes distingués de $\mathfrak{S}_5$ sont $\mathfrak{S}_5$, $\mathfrak{A}_5$ (noyau de χ_{sign}) et $\{e\}$. Le groupe dérivé est $\mathfrak{A}_5$ (noyau de χ_{sign}) et le centre est trivial puisque par exemple $\{\sigma\in\mathfrak{S}_5 \mid |\chi_{V_0}(\sigma)| = \chi_{V_0}(\text{Id}) = 4\} = \{\text{Id}\}$.

Remarques 2.15. — 1° Il reste vrai que pour tout $n\geqslant 1$, la table des caractères du groupe $\mathfrak{S}_n$ est à coefficients entiers (mais ce n'est pas le cas pour $\mathfrak{A}_n$; *cf.* exerc. 2.17 et 2.18).

2° Dans les exemples précédents, on remarque que la dimension d'une représentation irréductible divise toujours l'ordre du groupe. C'est un fait général qui sera démontré dans le th. 3.6. On voit aussi que le caractère d'une représentation irréductible de dimension $\geqslant 2$ prend toujours la valeur 0. C'est un fait général qui sera (presque) démontré dans l'exerc. 3.9.

4° On trouve ces tables de caractères dans la littérature scientifique pour les chimistes. Les notations sont différentes : le groupe D_n est noté C_{nv} et la table des caractères de $D_3 = \mathfrak{S}_3$ apparaît ainsi

	E	$3s_v$	$2C_3$
A_1	1	1	1
A_2	1	−1	1
E	2	0	−1

La notation $3s_v$ indique qu'il y a 3 éléments dans la classe de conjugaison et s_v signifie qu'elle contient des symétries par rapport à un plan vertical (les éléments de $D_3 = \mathfrak{S}_3$ sont interprétés comme les symétries d'un triangle équilatéral situé dans un plan horizontal). La notation $2C_3$ indique qu'il y a 2 éléments dans la classe de conjugaison et C_m correspond à des rotations d'angle $2\pi/m$.

Les lettres A et B indiquent des représentations (irréductibles) de dimension 1, E des représentations de dimension 2 et T des représentations de dimension 3.

Terminons avec la preuve d'une propriété vue dans des cas particuliers dans les exemples.

Proposition 2.16. — *La représentation de $\mathfrak{S}_n$ sur l'espace vectoriel*

$$V_0 = \{(x_1,\dots,x_n)\in\mathbf{C}^n \mid x_1+\cdots+x_n = 0\}$$

est irréductible.

Démonstration. — Par la prop. 2.8, cette représentation est irréductible si et seulement si $\langle \chi_{V_0}, \chi_{V_0} \rangle = 1$. Comme la représentation de permutation $\mathbf{C}^n$ est somme de V_0 et de la représentation triviale de dimension 1, il suffit de montrer que le caractère χ de la représentation de permutation vérifie $\langle \chi, \chi \rangle = 2$.

On a vu dans l'ex. 2.1.3° que $\chi(g)$ est le nombre de points fixes de la permutation $g \in \mathfrak{S}_n$. Pour tout $a \in \{1, \dots, n\}$, posons $g_a = 0$ si $g(a) \neq a$, et $g_a = 1$ si $g(a) = a$. On a donc

$$\begin{aligned} \langle \chi, \chi \rangle &= \frac{1}{n!} \sum_{g \in \mathfrak{S}_n} \Big(\sum_{a=1}^{n} g_a \Big)^2 \\ &= \frac{1}{n!} \sum_{1 \leqslant a,b \leqslant n} \sum_{g \in \mathfrak{S}_n} g_a g_b \\ &= \frac{1}{n!} \sum_{1 \leqslant a \leqslant n} \sum_{g \in \mathfrak{S}_n} g_a + \frac{2}{n!} \sum_{1 \leqslant a < b \leqslant n} \sum_{g \in \mathfrak{S}_n} g_a g_b. \end{aligned}$$

Le premier terme de la somme vaut $\frac{1}{n!} \sum_{1 \leqslant a \leqslant n} (n-1)! = 1$ et le second vaut $\frac{2}{n!} \sum_{1 \leqslant a < b \leqslant n} (n-2)! = 1$. La proposition en résulte. □

Exercice 2.17. — Montrer que la table des caractères du groupe alterné $\mathfrak{A}_4$ est donnée par

	1	4	4	3
	Id	(123)	(132)	(12)(34)
χ_{triv}	1	1	1	1
χ	1	ω	ω^2	1
χ^2	1	ω^2	ω	1
χ_{V_0}	3	0	0	-1

où $\omega := \exp(2i\pi/3)$.

Exercice 2.18. — Montrer que la table des caractères du groupe alterné $\mathfrak{A}_5$ est donnée par

	1	20	15	12	12
	Id	(123)	(12)(34)	(12345)	(21345)
χ_{triv}	1	1	1	1	1
χ_1	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_2	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_{V_0}	4	1	0	-1	-1
χ_V	5	-1	1	0	0

Exercice 2.19. — Déterminer la table des caractères du sous-groupe $H_8 := \{\pm 1, \pm I, \pm J, \pm K\}$ du groupe multiplicatif $\mathbf{H}^\times$ des quaternions (*cf.* § II.11). Remarquer que c'est la même que celle du groupe D_4.

Exercice 2.20. — Déterminer la table des caractères du groupe $SL_2(\mathbf{F}_3)$ (*cf.* exerc. I.2.12) (*Indication :* les 7 classes de conjugaison sont celles de $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (cardinal 1), de $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ (cardinal 1), de $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (cardinal 6), de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (cardinal 4), de $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ (cardinal 4), de $\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$ (cardinal 4) et de $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$ (cardinal 4)).

Exercice 2.21. — Déterminer la table des caractères du groupe $T_3(\mathbf{F}_3)$ des matrices 3×3 triangulaires supérieures, avec des 1 sur la diagonale, à coefficients dans $\mathbf{Z}/3\mathbf{Z}$ (*cf.* ex. I.2.19).

Exercice 2.22. — On rappelle que le groupe $SL_2(\mathbf{F}_3)$ est de cardinal 24 et qu'il y a 7 classes de conjugaison (exerc. I.2.10) : celle de $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ (cardinal 1), celle de $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$ (cardinal 1), celle de $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ (cardinal 4), celle de $\begin{pmatrix}1&-1\\0&1\end{pmatrix}$ (cardinal 4), celle de $\begin{pmatrix}-1&-1\\0&-1\end{pmatrix}$ (cardinal 4), celle de $\begin{pmatrix}-1&1\\0&-1\end{pmatrix}$ (cardinal 4) et celle de $\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ (cardinal 6)).

Déterminer la table des caractères du groupe $SL_2(\mathbf{F}_3)$.

Exercice 2.23. — Soit $\mathbf{F}_q$ un corps fini et soit G le groupe des bijections de $\mathbf{F}_q$ de la forme $x\mapsto ax+b$, avec $a\in\mathbf{F}_q^\times$ et $b\in\mathbf{F}_q$. Il est donc de cardinal $q(q-1)$.
a) Montrer que G a $q-1$ représentations complexes de dimension 1 (*Indication :* utiliser le morphisme de groupes de G vers $\mathbf{F}_q^\times$ donné par a).
b) Montrer que G a q classes de conjugaison. En déduire que G a exactement q représentations complexes irréductibles.
c) En déduire que G a exactement une autre représentation complexe irréductible que celles décrites en a) et que cette représentation est de dimension $q-1$. Décrire explicitement cette représentation (*Indication :* on pourra composer l'action de G sur $\mathbf{F}_q$ avec la représentation de permutation de $\mathfrak{S}_q=\mathrm{Bij}(\mathbf{F}_q)$ sur $\mathbf{C}^q$).

Exercice 2.24. — Considérons la représentation de permutation de $\mathfrak{S}_n$ sur l'espace vectoriel $V=\mathbf{C}^n$ et sa sous-représentation irréductible (prop. 2.16)

$$V_0=\{(x_1,\dots,x_n)\in\mathbf{C}^n \mid x_1+\cdots+x_n=0\}.$$

a) Montrer qu'on a un isomorphisme de représentations $\bigwedge^k V\simeq\bigwedge^k V_0\oplus\bigwedge^{k-1}V_0$.
b) Montrer que chaque représentation $\bigwedge^k V_0$, pour $1\leqslant k\leqslant n-1$, est irréductible (*Indication :* on pourra calculer $\langle\chi_{\bigwedge^k V},\chi_{\bigwedge^k V}\rangle$).

Exercice 2.25. — On fixe un entier $n\geqslant 4$. Pour tout $g\in\mathfrak{S}_n$, on note $\phi(g)$ le nombre de points fixes de la permutation g et on pose, pour tout entier $m\geqslant 0$,

$$\varpi(n,m):=\sum_{g\in\mathfrak{S}_n}\phi(g)^m.$$

a) Calculer $\varpi(n,1)$, $\varpi(n,2)$, $\varpi(n,3)$ et $\varpi(n,4)$ (*Indication :* on pourra s'inspirer de la preuve de la prop. 2.16).
b) Le groupe $\mathfrak{S}_n$ opère sur l'espace vectoriel $V=\mathbf{C}^n$ par permutation des coordonnées. Il opère aussi sur $V\otimes V$ par

$$\forall g\in G\ \ \forall v,w\in V\qquad g\cdot(v\otimes w)=g(v)\otimes g(w).$$

Décomposer cette représentation $V\otimes V$ de $\mathfrak{S}_n$ en somme de représentations irréductibles.
c) Montrer que pour tout m, le quotient $B(n,m):=\varpi(n,m)/n!$ est un entier.
d) Pour $m<n$, montrer la relation $B(n,m+1):=\sum_{i=0}^m\binom{m}{i}B(n,i)$, avec $B(n,0):=1$. En particulier, $B(n,m)$ est indépendant de n.

3. Propriétés d'intégralité

Dans cette section, on suppose G *fini et* **K** *algébriquement clos de caractéristique 0.* Il contient alors **Q** comme sous-corps.

Dans cette section on démontre que la dimension d'une représentation irréductible (de dimension finie) divise l'ordre du groupe. La démonstration nécessite de connaître quelques propriétés des entiers algébriques, que nous allons maintenant définir.

3.1. Entiers algébriques. —

Définition 3.1. — Un élément de **K** est un entier algébrique s'il est racine d'un polynôme unitaire à coefficients dans **Z**.

Par exemple, toute racine de l'unité est un entier algébrique.

Remarque 3.2. — Si $x \in \mathbf{Q} \subseteq \mathbf{K}$ est un entier algébrique, $x \in \mathbf{Z}$. En effet, si $x = \frac{r}{s}$ avec $\mathrm{pgcd}(r,s) = 1$, alors $r^n + a_1 r^{n-1} s + \cdots + a_n s^n = 0$ qui implique $s \mid r^n$ donc $s = \pm 1$.

Si $x \in \mathbf{K}$, on note $\mathbf{Z}[x]$ le sous-anneau de **K** engendré par x, c'est-à-dire l'ensemble des $\mathrm{P}(x)$, pour $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$, ou encore le sous-groupe additif de **K** engendré par les puissances positives de x.

Proposition 3.3. — *Soit $x \in \mathbf{K}$. Les propriétés suivantes sont équivalentes :*
(i) *x est un entier algébrique ;*
(ii) *le groupe abélien $\mathbf{Z}[x]$ est de type fini ;*
(iii) *il existe un sous-groupe abélien de type fini de* **K** *contenant* $\mathbf{Z}[x]$.

Démonstration. — L'énoncé (i) implique (ii) : si $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, le groupe abélien $\mathbf{Z}[x]$ est engendré par $1, x, x^2, \ldots, x^{n-1}$.

Le passage de (ii) à (iii) est évident. Montrons que (iii) implique (i). Par la prop. I.3.2.2°, $\mathbf{Z}[x]$, qui est un sous-groupe d'un groupe abélien de type fini, est encore un groupe de type fini. Soit $\{\mathrm{P}_1(x), \ldots, \mathrm{P}_r(x)\}$ un ensemble de générateurs. Si $d := \max_{1 \leqslant i \leqslant r} \deg(\mathrm{P}_i)$, l'ensemble $\{1, x, \ldots, x^d\}$ engendre aussi $\mathbf{Z}[x]$. Comme $x^{d+1} \in \mathbf{Z}[x]$, on peut l'écrire comme combinaison linéaire à coefficients entiers de $1, x, \ldots, x^d$. Cela donne un polynôme unitaire de degrés $d+1$ à coefficients entiers qui annule x, de sorte que x est un entier algébrique. □

Corollaire 3.4. — *L'ensemble des entiers algébriques de* **K** *est un sous-anneau de* **K**.

Démonstration. — Si x et y sont des entiers algébriques, $\mathbf{Z}[x]$ est engendré (comme groupe abélien) par $1, x, \ldots, x^r$, et $\mathbf{Z}[y]$ par $1, y, \ldots, y^s$. Alors le groupe (abélien) $\mathbf{Z}[x,y]$ est engendré par les $x^i y^j$ pour $0 \leqslant i \leqslant r$ et $0 \leqslant j \leqslant s$, donc est de type fini. Or il contient $\mathbf{Z}[x-y]$ et $\mathbf{Z}[xy]$, donc $x-y$ et xy sont aussi des entiers algébriques par la proposition. □

Par exemple, les valeurs des caractères des représentations (de dimension finie) de G sont des entiers algébriques, puisque ce sont des sommes de racines de l'unité.

3.2. Propriété de la dimension des représentations. — On peut maintenant passer à la démonstration que la dimension d'une représentation irréductible (de dimension finie) divise l'ordre du groupe.

Lemme 3.5. *— Soit* C *une classe de conjugaison de* G *et soit* (V,ρ) *une représentation irréductible de* G. *Alors* $\frac{|C|\chi_\rho(C)}{\dim(V)}$ *est un entier algébrique.*

Démonstration. — Le lemme 2.5.2° appliqué à la fonction caractéristique $f = \mathbf{1}_{C^{-1}}$ de la classe $C^{-1} := \{g^{-1} \mid g \in C\}$ fournit un endomorphisme $v := |G|(\mathbf{1}_{C^{-1}})_\rho = \sum_{g\in C}\rho(g)$ qui est l'homothétie de V de rapport

$$\lambda := \frac{|G|\langle \mathbf{1}_{C^{-1}}, \chi_\rho\rangle}{\dim(V)} = \frac{|C|\chi_\rho(C)}{\dim(V)}.$$

Considérons maintenant la représentation régulière $\rho_R : G \to GL(\mathbf{K}^G)$. Dans la base canonique $(\varepsilon_g)_{g\in G}$ de $\mathbf{K}^G$, la matrice de chaque endomorphisme $\rho_R(g)$ est une matrice de permutation, donc elle est en particulier à coefficients entiers. Il en est de même pour l'endomorphisme $u = \sum_{g\in C}\rho_R(g)$ de $\mathbf{K}^G$. Mais $\mathbf{K}^G$ contient comme sous-représentation toutes les représentations irréductibles de G, donc en particulier V.

La restriction de u à V est alors l'endomorphisme v défini plus haut, qui est une homothétie de rapport λ. On en déduit que λ est valeur propre de u, donc est racine de son polynôme caractéristique, qui est unitaire à coefficients entiers. C'est donc un entier algébrique. □

Théorème 3.6. *— On suppose* G *fini et* **K** *algébriquement clos de caractéristique 0. Si* V *est une représentation irréductible de* G, *on a* $\dim(V) \mid |G|$.

Démonstration. — Si χ est le caractère de V, on a $1 = \langle\chi,\chi\rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g^{-1})\chi(g)$ (th. 2.3). Notons $C_1,\dots,C_\ell$ les classes de conjugaison de G. On a alors

$$\begin{aligned}\frac{|G|}{\dim(V)} &= \frac{1}{\dim(V)}\sum_{g\in G}\chi(g^{-1})\chi(g)\\ &= \frac{1}{\dim(V)}\sum_{i=1}^{\ell}|C_i|\chi(C_i^{-1})\chi(C_i)\\ &= \sum_{i=1}^{\ell}\frac{|C_i|\chi(C_i)}{\dim(V)}\chi(C_i^{-1}).\end{aligned}$$

Comme les $\chi(C_i^{-1})$ sont des entiers algébriques, on conclut par le lemme 3.5 et le cor. 3.4 que le rationnel $\frac{|G|}{\dim(V)}$ est un entier algébrique, donc un entier (rem. 3.2 ; c'est ici que sert l'hypothèse $\mathrm{car}(\mathbf{K}) = 0$). □

Remarque 3.7. *—* La conclusion du théorème n'est plus vraie en général si le corps **K** n'est pas algébriquement clos : si $\mathbf{K} = \mathbf{R}$, la représentation de $\mathbf{Z}/3\mathbf{Z}$ comme groupe des rotations de $\mathbf{R}^2$ préservant un triangle équilatéral centré à l'origine, donc envoyant 1 sur la matrice $\begin{pmatrix}-1/2 & -\sqrt{3}/2\\ \sqrt{3}/2 & -1/2\end{pmatrix}$, est irréductible mais sa dimension, 2, ne divise pas l'ordre du groupe, 3. Sur **C**, cette représentation se scinde en somme directe de deux représentations de dimension 1.

En revanche, elle reste vraie en caractéristique $p > 0$ si $p \nmid |G|$. Mais il existe une représentation irréductible dans $\bar{\mathbf{F}}_{13}^5$ (où $\bar{\mathbf{F}}_{13}$ est une clôture algébrique de $\mathbf{F}_{13}$) du groupe $SL_2(\mathbf{F}_{13})$, d'ordre $2^3 \cdot 3 \cdot 7 \cdot 13 = 2184$ divisible par la caractéristique, 13, mais pas par la dimension, 5.

La contrainte donnée par le théorème est très forte. Par exemple, en combinant avec la prop. 2.8, on déduit qu'un groupe d'ordre p^2 ne peut avoir que des représentations irréductibles de dimension 1, donc est abélien (prop. 2.9). On retrouve ainsi le cor. I.2.15.1°.

On peut raffiner un peu le th. 3.6.

Théorème 3.8. — *On suppose* G *fini et* $\mathbf{K}$ *algébriquement clos de caractéristique 0. Si* V *est une représentation irréductible de* G*, on a* $\dim(V) \mid [G : Z(G)]$.

Démonstration (J. Tate). — Le groupe $G^m = G \times \cdots \times G$ a une représentation ρ_m dans $V^{\otimes m}$ donnée par

$$\rho_m(g_1, \ldots, g_m) = \rho(g_1) \otimes \cdots \otimes \rho(g_m).$$

Son caractère est (exerc. III.1.5)

$$\chi_m(g_1, \ldots, g_m) = \chi(g_1) \cdots \chi(g_m),$$

donc $\langle \chi_m, \chi_m \rangle = 1$ et ρ_m *est irréductible* (prop. 2.8).

Si $g_i \in Z(G)$, alors $\rho(g_i)$ commute à tous les $\rho(g)$. C'est donc un endomorphisme de la représentation (V, ρ), c'est-à-dire une homothétie $\lambda_i \mathrm{Id}_V$ (lemme de Schur 1.10). Si en outre $g_1 \cdots g_m = e$, alors $\mathrm{Id}_V = \rho(e) = \rho(g_1) \cdots \rho(g_m) = \lambda_1 \cdots \lambda_m \mathrm{Id}_V$ et $\lambda_1 \cdots \lambda_m = 1_{\mathbf{K}}$, d'où $\rho_m(g_1, \ldots, g_m) = \mathrm{Id}_{V^{\otimes m}}$. Soit

$$S = \{(g_1, \ldots, g_m) \in Z(G)^m \mid g_1 \cdots g_m = e\}.$$

C'est un sous-groupe distingué de G^m et on peut factoriser la représentation ρ_m en

$$\begin{array}{ccc} G^m & \xrightarrow{\rho_m} & GL(V^{\otimes m}) \\ \downarrow & \nearrow_{\hat{\rho}_m} & \\ G^m/S, & & \end{array}$$

où $\hat{\rho}_m$ est encore irréductible. Par le th. 3.6, $\dim(V^{\otimes m}) = (\dim(V))^m$ divise $|G^m/S| = \frac{|G|^m}{|Z(G)|^{m-1}}$, donc pour tout $m \geqslant 1$,

$$|Z(G)|^{m-1} \left| \left(\frac{|G|}{\dim(V)} \right)^m, \quad \text{qui implique} \quad |Z(G)| \left| \frac{|G|}{\dim(V)} \right. . \right.$$

□

On peut généraliser ce résultat en montrant que le degré de toute représentation irréductible divise l'indice de tout sous-groupe abélien distingué dans G.

Exercice 3.9. — Soit G un groupe fini et soit χ le caractère d'une représentation irréductible complexe ρ de G. On pose

$$N(\chi) := \prod_{g \in G} |\chi(g)|^2.$$

On admettra que $N(\chi)$ est un entier [3].
a) Montrer $N(\chi) \leqslant 1$, avec égalité si et seulement si $\dim(\rho) = 1$ (*Indication :* on pourra comparer moyenne géométrique et moyenne arithmétique).
b) En déduire que si $\dim(\rho) \geqslant 2$, il existe $g \in G$ tel que $\chi(g) = 0$.

3. La théorie de Galois nous dit $N(\chi) \in \mathbf{Q}$. D'autre part, $N(\chi) := \prod_{g\in G} \chi(g)\chi(g^{-1})$ est un entier algébrique. C'est donc un entier.

TD1 : Généralités sur les groupes

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Soit E un ensemble muni d'une loi de composition, associative, avec élément neutre e, et telle que tout élément de E possède un inverse à gauche. Montrer que tout élément de E possède un inverse à droite qui coïncide avec son inverse à gauche. En déduire que E est un groupe.

Solution de l'exercice 1. Soit $g \in E$. Par hypothèse, il existe $h \in E$ tel que $h \cdot g = e$.
De même, il existe $k \in E$ tel que $k \cdot h = e$. L'associativité assure alors que $g = (k \cdot h) \cdot g = k \cdot (h \cdot g) = k$, donc $g \cdot h = e$, donc h est aussi inverse à droite de g.
Par conséquent, tout élément de E admet un inverse (à droite et à gauche), donc E est un groupe.

Exercice 2 : ⋆
Soit G un groupe tel que $g^2 = e$ pour tout $g \in G$. Montrer que G est abélien.

Solution de l'exercice 2. Pour tous $g, h \in G$, on a $(g \cdot h)^2 = e$, i.e. $g \cdot h \cdot g \cdot h = e$, donc en multipliant à droite par $h \cdot g$, on a $g \cdot h = h \cdot g$, i.e. G est commutatif.

Exercice 3 : ⋆
Soit G un groupe et soit H un sous-ensemble fini non vide de G stable pour la loi de composition du groupe G.

a) Montrer que H est un sous-groupe de G.
b) Trouver un exemple d'un groupe G et d'un sous-ensemble non vide de G stable pour la loi de composition du groupe G qui ne soit pas un sous-groupe de G.

Solution de l'exercice 3.

a) Soit $h \in H$. Comme H est fini et $h^n \in H$ pour tout $n \in \mathbb{N}$, il existe deux entiers $n > m \geq 0$ tels que $h^n = h^m$. Or h admet un inverse dans G, donc on en déduit l'égalité suivante de G : $h^{n-m} = e$. Or H est stable par multiplication, donc $e \in H$ et $h^{-1} = h^{n-m-1} \in H$, donc H est stable par inverse. Cela assure que H est un sous-groupe de G.
b) On peut prendre $G = (\mathbb{Z}, +)$ et $H = \mathbb{N}$.

Exercice 4 : ⋆
Soit G un groupe et soit H un sous-groupe de G d'indice 2. Montrer que H est distingué dans G.

Solution de l'exercice 4. Les classes à gauche de G modulo H sont $\{H, G \setminus H\}$. Donc les classes à droite de G modulo H sont $\{H, G \setminus H\}$. Si $g \notin H$, on a donc $g \cdot H = G \setminus H = H \cdot g$, ce qui assure le résultat.

Exercice 5 :
Soit G un groupe fini.

a) Montrer que des éléments conjugués dans G sont de même ordre.
b) Deux éléments de même ordre dans G sont-ils toujours conjugués ?
c) Trouver tous les groupes abéliens finis G pour lesquels la question précédente a une réponse positive. Un exemple non abélien ?

Solution de l'exercice 5.

a) Si $g, h \in G$ et $n \in \mathbb{N}$, on a $(h \cdot g \cdot h^{-1})^n = h \cdot g^n \cdot h^{-1}$, donc $(h \cdot g \cdot h^{-1})^n = e$ si et seulement si $g^n = e$, ce qui assure le résultat.

b) Non. Par exemple, dans le groupe commutatif $G = \mathbb{Z}/3\mathbb{Z}$, on a deux éléments d'ordre 3 qui ne sont pas conjugués.

c) Dans un groupe abélien fini, les classes de conjugaison sont réduites à un élément. Donc la question précédente a une réponse positive dans un groupe abélien fini G si et seulement si tous les éléments de G ont des ordres distincts. Or si un groupe admet un élément g d'ordre $n \geq 3$, alors il admet d'autres éléments d'ordre n, par exemple g^{-1}. Donc les seuls groupes abéliens convenables sont le groupe trivial et le groupe $\mathbb{Z}/2\mathbb{Z}$.

Si $G = \mathfrak{S}_3$, alors les éléments d'ordre 2 dans G sont les transpositions $(12), (13), (23)$ qui sont bien conjuguées, et les éléments d'ordre 3 sont les 3-cycles (123) et (132), qui sont également conjugués. Donc G est un exemple de groupe non abélien convenable.

Exercice 6 :
Soit $f : G_1 \to G_2$ un morphisme de groupes et soit x un élément de G_1 d'ordre fini. Montrer que l'ordre de $f(x)$ divise l'ordre de x.

Solution de l'exercice 6. On note n l'ordre de x. On a $x^n = e$, donc $f(x)^n = f(x^n) = e$, donc l'ordre de $f(x)$ divise n.

Exercice 7 : $\star$
Montrer qu'il n'existe pas de morphisme de groupes surjectif de $(\mathbb{Q}, +)$ dans $(\mathbb{Q}_+^*, \times)$.

Solution de l'exercice 7. Soit $\phi : (\mathbb{Q}, +) \to (\mathbb{Q}_+^*, \times)$ un morphisme surjectif. Alors $2 \in \mathbb{Q}_+^*$ admet un antécédent x par φ. Alors $y := \frac{x}{2} \in \mathbb{Q}$ vérifie que $2y = x$, donc $\varphi(y)^2 = \varphi(x) = 2$. Par conséquent, on a construit un rationnel $\varphi(y) \in \mathbb{Q}_+^*$ tel que $\varphi(y)^2 = 2$, ce qui contredit l'irrationnalité de $\sqrt{2}$.

Exercice 8 :
Donner la liste de tous les groupes (à isomorphisme près) de cardinal inférieur ou égal à 7.

Solution de l'exercice 8.
- le seul groupe de cardinal 1 est le groupe trivial.
- si p est un nombre premier et si G est de cardinal p, alors tout élément $g \in G$ distinct de l'élément neutre est d'ordre p, ce qui assure que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Il y a donc un unique groupe de cardinal p (qui est $\mathbb{Z}/p\mathbb{Z}$) pour $p = 2, 3, 5, 7$.
- Soit G un groupe d'ordre 4. Si G admet un élément d'ordre 4, G est isomorphe à $Z/4\mathbb{Z}$. Sinon, tous ses éléments sont d'ordre 1 ou 2. Donc G est abélien, et le choix de deux éléments distincts (non neutres) g et h de G fournit un isomorphisme entre G et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il y a donc exactement deux groupes d'ordre 4.
- Soit G un groupe d'ordre 6. Si G est commutatif, G admet nécessairement un élément d'ordre 2 et un élément d'ordre 3 (sinon tous les éléments de G sont d'ordre divisant 2, auquel cas G contient $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ce qui n'est pas possible, ou tous les élélléments de G sont d'ordre divisant 3, auquel cas G contient $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, ce qui n'est pas possible non plus). Alors le produit de ces deux éléments est d'ordre 6, ce qui assure que G est isomorphe à $\mathbb{Z}/6\mathbb{Z}$.
  Si G n'est pas commutatif : alors G contient un élément d'ordre 3, noté a, et aussi un élément b d'ordre 2 (sinon on montre que G aurait au moins 7 éléments). Nécessairement, a et b ne commutent pas, et ils engendrent G. Les éléments de G sont donc $e, a, a^2, b, a \cdot b, b \cdot a$. Donc néssairement on a $a^2 \cdot b = b \cdot a$ et $b \cdot a^2 = a \cdot b$, ce qui détermine complétement la table de multiplication de G. Il y a donc au plus un groupe non commutatif d'ordre 6. Or $\mathfrak{S}_3$ en est un, donc c'est le seul.
  Il y a donc exactement deux groupes d'ordre 6 : $\mathbb{Z}/6\mathbb{Z}$ et $\mathfrak{S}_3$.

Exercice 9 : $\star\star$
Soit G un groupe tel que le quotient par son centre est monogène. Prouver que G est abélien.

Solution de l'exercice 9. On rappelle que le centre $Z(G)$ de G est distingué. On considère le morphisme quotient $\pi : G \to G/Z(G)$. Par hypothèse, $G/Z(G)$ est engendré par un élément $\overline{g_0}$. Comme π est surjective, il existe $g_0 \in G$ tel que $\pi(g_0) = \overline{g_0}$. Soient alors $g, h \in G$. Il existe des entiers $n, m \in \mathbb{Z}$ tels que $\pi(g) = \overline{g_0}^n$ et $\pi(h) = \overline{g_0}^m$. Donc $\pi(g \cdot g_0^{-n}) = \pi(h \cdot g_0^{-m}) = e$, donc $y = g \cdot g_0^{-n}$ et $z = h \cdot g_0^{-m}$ sont dans $Z(G)$.
Alors

$$g \cdot h = y \cdot g_0^n \cdot z \cdot g_0^m = y \cdot z \cdot g_0^{n+m} = z \cdot g_0^m \cdot y \cdot g_0^n = h \cdot g\,,$$

donc G est commutatif.

Exercice 10 : ⋆⋆
Soit G un groupe. Vrai ou faux ?

a) Si tout sous-groupe H de G est distingué dans G, alors G est abélien.

b) Si $H \triangleleft G$ et $K \triangleleft H$, alors $K \triangleleft G$.

c) Soient x et $y \in G$ d'ordre fini. Alors xy est nécessairement d'ordre fini.

d) Si G a un nombre fini de sous-groupes, alors G est fini.

e) Si H et K sont des sous-groupes de G, alors $\langle H \cup K \rangle = HK$.

Solution de l'exercice 10.

a) Faux. On considère par exemple le groupe H des quaternions, d'ordre 8. Ce groupe est définit de la façon suivante : l'ensemble H est

$$H = \{\pm 1, \pm i, \pm j, \pm k\}\,,$$

et la loi de groupe est définie par

$$\begin{array}{l}(-1)^2 = 1\,,\ i^2 = j^2 = k^2 = -1\,,\\ (-1) \cdot i = i \cdot (-1) = -i\,,\ (-1) \cdot j = j \cdot (-1) = -j\,,\ (-1) \cdot k = k \cdot (-1) = -k\,,\\ i \cdot j = -j \cdot i = k\,.\end{array}$$

On voit que les sous-groupes de H sont les suivants :
– le sous-groupe trivial $\{1\}$, qui est distingué.
– le sous-groupes de cardinal 2 engendré par -1, qui est distingué car contenu dans le centre de H.
– les sous-groupes de cardinal 4 sont d'indice 2 dans H, donc distingué.
– le sous-groupe H entier, qui est distingué.
Donc les sous-groupes de H sont tous distingués, alors que H n'est pas commutatif.

b) Faux. On peut prendre $G = \mathfrak{S}_4$ ou $\mathfrak{A}_4$, $H = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $K = \{\mathrm{id}, (12)(34)\} \cong \mathbb{Z}/2\mathbb{Z}$.

c) Faux. Pour avoir un contre-exemple, il faut nécessairement que le groupe G soit infini et non commutatif. On peut prendre par exemple le groupe libre sur deux générateurs a et b d'ordre 2, i.e. l'ensemble des mots finis formés des lettres a et b sans répétition, avec la loi de concaténation des mots (avec simplification éventuelle des mots aa et bb apparaissant). Dans ce groupe, les éléments a et b sont d'ordre 2, alors que leur produit $a \cdot b = ab$ est d'ordre infini.
Pour un exemple plus concret, on peut prendre $G = \mathrm{GL}_2(\mathbb{Q})$, $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$.
Alors x est d'ordre 2, y est d'ordre 3 et $x \cdot y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.

d) Vrai. Il est clair que tout élément de G est d'ordre fini : si $g \in G$ est d'ordre infini, alors le sous-groupe engendré par g est isomorphe à $\mathbb{Z}$, et il contient donc une infinité de sous-groupes distincts. Or G a un nombre fini de sous-groupes cycliques, noté $\langle g_1 \rangle, \ldots, \langle g_n \rangle$. Donc pour tout $g \in G$, il existe i tel que $\langle g \rangle = \langle g_i \rangle$, donc g est une puissance de g_i, ce qui assure que le cardinal de G est borné par la somme des ordres des g_i, donc G est fini.

e) Faux. Il est clair que l'inclusion $HK \subset \langle H \cup K \rangle$ est toujours vérifiée. En revanche, le sous-ensemble HK n'est en général pas un sous-groupe de G, au contraire de $\langle H \cup K \rangle$: par exemple, si on prend $G = \mathfrak{S}_3$, $H = \{\mathrm{id}, (12)\}$ et $K = \{\mathrm{id}, (13)\}$, alors on a $\langle H \cup K \rangle = G$ (de cardinal 6), alors que $HK = \{\mathrm{id}, (12), (13), (132)\}$ (de cardinal 4) n'est pas un sous-groupe de G. La réponse est en revanche affirmative si H ou K est distingué dans G.

Exercice 11 :
Soit S un sous-ensemble non vide d'un groupe fini G. Soient $N(S) := \{g \in G \mid gSg^{-1} = S\}$ et $C(S) := \{g \in G \mid \forall s \in S\,, gsg^{-1} = s\}$ le normalisateur et le centralisateur de S dans G. Montrer que :

a) $N(S) < G$ et $C(S) \triangleleft N(S)$.

b) $N(S) = G$ si et seulement si $S = \bigcup_{g \in G} gSg^{-1}$.

c) Si $H \triangleleft G$, alors $C(H) \triangleleft G$.

d) Si $H < G$, alors $N(H)$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Solution de l'exercice 11.

a) On a $e \in N(S)$. Soient $g, h \in N(S)$. Alors on a $(gh)S(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S$, donc $gh \in N(S)$. Si $g \in N(S)$, on a $gSg^{-1} = S$, donc en multipliant à gauche et à droite par g^{-1} et g respectivement, on a $S = g^{-1}Sg$, donc $g^{-1} \in N(S)$. Donc $N(S)$ est un sous-groupe de G. De même, il est clair que $C(S)$ est un sous-groupe de G contenu dans $N(S)$. Montrons qu'il est distingué dans $N(S)$. Soit $g \in C(S)$ et $h \in N(S)$. Soit $s \in S$. Alors

$$(hgh^{-1})s(hgh^{-1})^{-1} = hg(h^{-1}sh)g^{-1}h^{-1}\,,$$

et comme $h \in N(S)$, on a $h^{-1}sh \in S$, donc comme $g \in C(S)$, $g(h^{-1}sh)g^{-1} = h^{-1}sh$, donc finalement $(hgh^{-1})s(hgh^{-1})^{-1} = h(h^{-1}sh)h^{-1} = s$, donc $hgh^{-1} \in C(S)$, donc $C(S) \triangleleft N(S)$.

b) On suppose $N(S) = G$. Alors pour tout $g \in G$, on a $gSg^{-1} = S$, donc $S = \bigcup_{g \in G} gSg^{-1}$. Réciproquement, si on suppose $S = \bigcup_{g \in G} gSg^{-1}$, pour tout $g \in G$, on a donc $g^{-1}Sg \subset S$, donc en multipliant par g et g^{-1} à gauche et à droite respectivement, on a $S \subset gSg^{-1} \subset S$, ce qui assure que $gSg^{-1} = S$, donc $g \in N(S)$, donc $G = N(S)$.

c) On suppose H distingué dans G. Soit $g \in G$ et $c \in C(H)$. Soit enfin $h \in H$. On calcule $(gcg^{-1})h(gcg^{-1})^{-1} = gc(g^{-1}hg)c^{-1}g^{-1}$: puisque H est distingué dans G, on sait que $g^{-1}hg \in H$. Or $c \in C(H)$, donc $c(g^{-1}hg)c^{-1} = g^{-1}hg$, donc finalement $(gcg^{-1})h(gcg^{-1})^{-1} = g(g^{-1}hg)g^{-1} = h$, ce qui assure que $gcg^{-1} \in C(H)$. Donc $C(H)$ est distingué dans G.

d) Par définition et via la question a), il est clair que $N(H)$ est un sous-groupe de G contenant H, et que H est distingué dans $N(H)$. Soit maintenant K un sous-groupe de G contenant H tel que $H \triangleleft K$. Alors par définition, pour tout $k \in K$, on a $kHk^{-1} = H$, donc $k \in N(H)$, donc $K \subset N(H)$, ce qui assure la maximalité de $N(H)$ parmi les sous-groupes de G concernés.

Exercice 12 : $\star\star$
Soit G un groupe et soit $H \triangleleft G$ un sous-groupe distingué.

a) Décrire les sous-groupes distingués de G/H en fonction de ceux de G.

b) Soit K un sous-groupe de G.

i) Si K est distingué dans G et contient H, montrer que l'on a un isomorphisme $(G/H)/(K/H) \cong G/K$.

ii) Montrer que HK est un sous-groupe de G égal à KH.

iii) Montrer que H est distingué dans HK.

iv) Montrer que l'on a un isomorphisme $K/(K \cap H) \cong (HK)/H$.

Solution de l'exercice 12.

a) On note $\pi : G \to G/H$ la projection canonique. On sait que la correspondance $K \mapsto \pi(K)$ établit une bijection entre l'ensemble des sous-groupes de G contenant H est l'ensemble des sous-groupes de G/H, dont la réciproque est donnée par $\overline{K} \mapsto \pi^{-1}(\overline{K})$. On vérifie immédiatemment que cette bijection induit une bijection entre les sous-groupes distingués de G contenant H et les sous-groupes distingués de G/H.

b) i) Le morphisme $\pi : G \to G/H$, composé avec la projection $\pi' : G/H \to (G/H)/(K/H)$, induit un morphisme surjectif $q : G \to (G/H)/(K/H)$. Par construction, un élément $g \in G$ est dans $\mathrm{Ker}(q)$ si et seulement si $\pi(g) \in \mathrm{Ker}(\pi') = K/H$ si et seulement si $g \in K$. Donc $\mathrm{Ker}(q) = K$. Le théorème de factorisation assure alors que q induit un isomorphisme $\overline{q} : G/K \xrightarrow{\simeq} (G/H)/(K/H)$.

ii) Soient $h, h' \in H$ et $k, k' \in K$. Comme H est distingué dans G, il existe $h'' \in H$ tel qu'on ait $k \cdot h' = h'' \cdot k$, donc $(h \cdot k) \cdot (h' \cdot k') = (h \cdot h'') \cdot (k \cdot k') \in HK$, donc HK est un sous-groupe de G.

Puisque pour tous $h \in H$ et $k \in K$, il existe $h' \in H$ tel que $h \cdot k = k \cdot h'$, on voit que $HK \subset KH$. De même, pour tous $h \in H$ et $k \in K$, il existe $h' \in H$ tel que $k \cdot h = h' \cdot k$, donc $HK = KH$.

iii) C'est évident.

iv) L'inclusion $K \to HK$ induit un morphisme $p : K \to (HK)/H$. Montrons que p est surjectif : si $h \in H$ et $k \in K$, on voit que la classe $(h \cdot k)H = kH$ est l'image de k par p, donc p est surjectif. En outre, un élément $k \in K$ est dans $\mathrm{Ker}(p)$ si et seulement si il est dans H, donc $\mathrm{Ker}(p) = K \cap H$. Le théorème de factorisation permet de conclure.

Exercice 13 :
Quel est le nombre minimal de transpositions nécessaires pour engendrer le groupe $\mathfrak{S}_n$.

Solution de l'exercice 13. Montrons que ce nombre vaut $n-1$. Il est clair qu'il existe une famille de $n-1$ transpositions engendrant $\mathfrak{S}_n$ (par exemple les transpositions de la forme $(1i)$, avec $2 \leq i \leq n$). Montrons que l'on ne peut pas faire mieux. Soit $E \subset \mathfrak{S}_n$ un ensemble de transpositions. On considère le graphe fini Γ dont les sommets sont les entiers $1, 2, \ldots, n$, de sorte que deux sommets distincts i et j sont reliés par une arête si et seulement si $(ij) \in E$. Supposons la partie E génératrice. Alors il est clair que le graphe Γ est connexe.
Il suffit donc de montrer, par récurrence sur n, qu'un graphe connexe à n sommets possède au moins $n-1$ arêtes : le cas $n = 2$ est évident. Montrons l'hérédité : soit donc un tel graphe Γ, connexe à $n+1$ sommets. On a l'alternative suivante :
– soit chaque sommet a au moins deux voisins. Alors le nombre total d'arêtes est au moins égal à $\frac{1}{2}(n+1) \cdot 2 = n+1$.
– soit il existe un sommet s ayant un unique voisin. On considère alors le graphe Γ' dont les sommets sont les sommets de Γ autres que s et les arêtes celles de Γ autres que celle contenant s. Alors il est clair que Γ' est un grpahe connexe à n sommets, donc il admet au moins $n-1$ arêtes, donc Γ a au moins n arêtes.
Cela conclut la preuve par récurrence.

Exercice 14 : $\star\star\star$
Soit G un groupe de type fini

a) Un sous-groupe H de G est-il nécessairement de type fini ?

b) Même question en supposant de plus que le cardinal de G/H est fini.

Solution de l'exercice 14.

a) Non. Un contre-exemple est donné par le groupe libre G sur deux générateurs a et b, et H le sous-groupe engendré par tous les éléments de la forme ab^n, avec $n \in \mathbb{N}$. Supposons que H soit de type fini. Alors il existe un entier N tel que dans tout mot de H, le nombre de b consécutifs est toujours strictement inférieur à N. Or il est clair que $ab^N \in H$, ce qui est contradictoire. Donc H n'est pas de type fini, alors que G l'est.

Un autre exemple est donné par le sous-groupe G de $\mathrm{GL}_2(\mathbb{Q})$ engendré par les matrices $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, et le sous-groupe H de G formé des matrices de G avec des 1 sur la diagonale. Supposons que H soit de type fini. Alors il existe un entier $N \geq 1$ tel que H soit contenu dans le sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$ formé des matrices de la forme $\begin{pmatrix} 1 & \frac{a}{N} \\ 0 & 1 \end{pmatrix}$. Or $A^{-N} \cdot B \cdot A^N = \begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix}$ est dans H, ce qui est contradictoire puisque $2^N > N$, donc H n'est pas de type fini, alors que G l'est

b) On suppose G/H fini. Alors on peut trouver un nombre fini déléments $g_1 = e, \ldots, g_n$ de G tels que $G/H = \{g_1 H, \ldots, g_n H\}$. Puisque G est de type fini, on dispose de $h_1, \ldots, h_m \in G$ tels que tout éléments de G est produit des h_i. Alors pour tout i, j, il existe $1 \leq k \leq n$ et $h_{i,j} \in H$ tels que $h_i \cdot g_j = g_k \cdot h_{i,j}$.
Montons alors que les $h_{i,j}$ engendrent H. Soit $h \in H$. On sait qu'il existe des entiers $i_1, \ldots, i_r$ tels que $h = h_{i_1} \ldots h_{i_r}$. On a donc $h_{i_r} = h_{i_r} \cdot e = h_{i_r} \cdot g_1 = g_{k_r} \cdot h_{i_r,1}$, donc finalement

$$h = h_{i_1} \cdot \cdots \cdot h_{i_{r-1}} \cdot g_{k_r} \cdot h_{i_r,1} \,.$$

De même, $h_{i_{r-1}} \cdot g_{k_r} = g_{k_{r-1}} \cdot h_{i_{r-1},k_r}$, donc

$$h = h_{i_1} \cdot \cdots \cdot h_{i_{r-2}} \cdot g_{k_{r-1}} \cdot h_{i_{r-1},k_r} \cdot h_{i_r,1} \,.$$

Donc par récurrence, on trouve

$$h = g_{k_1} \cdot h_{i_1,k_2} \cdot \cdots \cdot h_{i_{r-1},k_r} \cdot h_{i_r,1} \,.$$

Enfin, h et les $h_{i,j}$ sont dans H, donc $g_{k_1} \in H$, donc $k_1 = 1$ et donc

$$h = h_{i_1,k_2} \cdot \cdots \cdot h_{i_{r-1},k_r} \cdot h_{i_r,1} \,,$$

ce qui conclut la preuve.

Exercice 15 : $\star\star$
On dit qu'un groupe G est d'exposant e si e est le plus petit entier $n \geq 1$ tel que pour tout $g \in G$, on a $g^n = 1$. Pour quels entiers e un groupe d'exposant e est-il nécessairement commutatif ?

Solution de l'exercice 15. On a déjà vu que $e = 2$ convenait. Et $e = 1$ aussi évidemment. Montrons que ce sont les entiers convenables. Supposons que e soit divisible par 4. Alors le groupe $G = \mathbb{Z}/e\mathbb{Z} \times H$, où H est le groupe des quaternions d'ordre 8, est d'exposant e et n'est pas commutatif (car H ne l'est pas).
Supposons $e \geq 3$ non divisible par 4. Alors e admet un facteur premier impair p. On considère alors le groupe $G = \mathbb{Z}/e\mathbb{Z} \times U(p)$, où $U(p)$ est le sous-groupe de $\mathrm{GL}_p(\mathbb{F}_p)$ formés des matrices triangulaires supérieures avec des 1 sur la diagonale. On voit facilement que G est d'exposant e et n'est pas commutatif, car $U(p)$ n'est pas commutatif.

Exercice 16 :

a) Prouver que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.

b) Prouver que les sous-groupes non denses de $\mathbb{R}$ sont les $a\mathbb{Z}$, avec $a \in \mathbb{R}$.

Solution de l'exercice 16.

a) Soit G un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$. Alors $G \cap \mathbb{N}^*$ admet un plus petit élément noté n. Soit alors $x \in G$. Écrivons la divisions euclidienne de x par n : il existe $q, r \in \mathbb{N}$ tel que $x = nq + r$, avec $0 \leq r < n$. Comme $x, n \in G$ et $r = x - nq$, on a $r \in G \cap \mathbb{N}$ et $r < n$. Donc la minimalité de n assure que $r = 0$, donc $x = nq \in n\mathbb{Z}$. Cela prouve que $G = n\mathbb{Z}$.

b) Soit G un sous-groupe de $\mathbb{R}$ distinct de $\{0\}$ et non dense. Montrons que 0 est un point isolé de G : supposons par l'absurde que tout intervalle ouvert contenant 0 contienne un élément non nul de G. Soit $x \in G$ et I un intervalle ouvert contenant x. Alors $I - x$ est un intervalle ouvert contenant 0. Donc par hypothèse, il existe $y \neq 0 \in G \cap (I - x)$. Alors $y + x \in G \cap I$ et $y + x \neq x$. Donc G est dense dans $\mathbb{R}$, ce qui est exclu. Donc 0 est un point isolé de G. Notons alors $a := \inf G \cap \mathbb{R}_+^*$. On sait donc que $a > 0$. Montrons que $a \in G$. Par définition, il existe une suite (x_n) dans $G \cap \mathbb{R}_+^*$ convergeant vers a. Comme 0 est un point isolé de G, la suite $(x_{n+1} - x_n)$ (à valeurs dans G et convergeant vers 0) est stationnaire à 0, donc la suite (x_n) est stationnaire, donc $a \in G$.
Soit alors $x \in G \cap \mathbb{R}_+^*$. En considérant la partie entière n de $\frac{x}{a}$, on voit que $na \leq x < (n+1)a$. Alors $0 \leq x - na < a$ et $x - na \in G$, donc la minimalité de a assure que $x - na = 0$, donc $x = na$. Cela assure que $G = a\mathbb{Z}$.

Exercice 17 : $\star\star$
Soit G un groupe fini.

a) Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathfrak{S}_n$.

b) Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathfrak{A}_n$.

c) Montrer qu'il existe $n \in \mathbb{N}$ tel que G soit un sous-groupe de $\mathrm{GL}_n(k)$, pour tout corps k.

Solution de l'exercice 17.

a) On considère l'action de G sur lui-même par translation à gauche. Autrement dit, on regarde le morphisme de groupes $\varphi : G \to \mathfrak{S}(G)$ défini par $\varphi(g)(h) := g \cdot h$. Comme G est de cardinal n, on sait que $\mathfrak{S}(G)$ est isomorphe à $\mathfrak{S}_n$. Il suffit donc de montrer que le morphisme φ est injectif. Soit $g \in \mathrm{Ker}(\varphi)$. Alors pour tout $h \in G$, on a $g \cdot h = h$, ce qui assure (en prenant $h = e$ par exemple) que $g = e$. Donc φ st injective.

b) Au vu de la question précédente, il suffit de plonger $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$. Remarquons d'abord que l'on dispose d'un morphisme injectif naturel $\iota : \mathfrak{S}_n \to \mathfrak{S}_{n+2}$ obtenu en prolongeant une bijection de $\{1, \ldots, n\}$ en une bijection de $\{1, \ldots, n+2\}$ par l'identité sur les éléments $n+1$ et $n+2$. On définit alors l'application $\psi : \mathfrak{S}_n \to \mathfrak{A}_{n+2}$ de la façon suivante : si $\sigma \in \mathfrak{A}_n$, on pose $\psi(\sigma) := \iota(\sigma)$, et si $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$, on pose $\psi(\sigma) := \iota(\sigma) \circ (n, n+1)$. On vérifie facilement que ψ est un morphisme de groupes injectif, ce qui conclut la preuve.

c) Au vu de la première question, il suffit de construire un morphisme de groupes injectif de $\mathfrak{S}_n$ dans $\mathrm{GL}_n(k)$. On utilise pour cela les matrices de permutations. On a en effet une application

$$\varphi : \mathfrak{S}_n \to \mathrm{GL}_n(k)$$

définie par $\varphi(\sigma) := P_\sigma$. Il est classique que φ est un morphisme de groupes, et il est clair que celui-ci est injectif. Cela conclut la preuve.

Exercice 18 : $\star\star\star$
Déterminer les classes de conjugaison dans $\mathfrak{S}_n$. Et dans $\mathfrak{A}_n$?

Solution de l'exercice 18. Soit $c = (a_1, \ldots, a_k)$ un k-cycle dans $\mathfrak{S}_n$. Il est clair que pour tout $\sigma \in \mathfrak{S}_n$, on a

$$\sigma \circ c \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k)) .$$

Comme toute permutation se décompose de façon unique en produit de cycles à supports disjoints, on trouve immédiatemment que les classes de conjugaisons dans $\mathfrak{S}_n$ sont paramétrée par les partitions de l'entiers n. On rappelle qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que $m_1 \leq \cdots \leq m_r$ et $\sum m_i = n$. La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.
La description des classes de conjugaison dans $\mathfrak{A}_n$ est un peu plus subtile. On remarque d'abord que puisque $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$, la classe de conjugaison dans $\mathfrak{S}_n$ d'un élément de $\mathfrak{A}_n$ est contenue

dans $\mathfrak{A}_n$. Comme $\mathfrak{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$, pour tout $\sigma \in \mathfrak{A}_n$, la classe de conjugaison de σ dans $\mathfrak{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathfrak{A}_n$, soit réunion de deux classes de conjugaison dans $\mathfrak{A}_n$ (celle de σ et une autre).
Montrons alors que l'on est dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition.
En effet, si σ admet un cycle c de longueur paire, pour tout $\tau \in \mathfrak{S}_n$, on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$, ce qui assure que les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathfrak{A}_n$ coïncident. Si σ admet deux cycles $c = (a_1, \dots, a_{2k+1})$ et $c' = (a'_1, \dots, a'_{2k+1})$ de même longueur impaire, alors si on note $d := (a_1 a'_1) \dots (a_{2k+1} a'_{2k+1})$ (permutation impaire), on a pour tout $\tau \in \mathfrak{S}_n$, $\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$, ce qui assure que les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathfrak{A}_n$ coïncident.
Réciproquement, si σ n'a que des cycles de longueurs impaires deux-à-deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ, et on voit facilement que $(ij) \circ \sigma \circ (ij)$ n'est pas conjuguée à σ dans $\mathfrak{A}_n$ alors qu'elle l'est dans $\mathfrak{S}_n$.

Exercice 19 :
Montrer que si $n \geq 2$, $\mathfrak{S}_{n+2}$ a deux sous-groupes non conjugués isomorphes à $\mathfrak{S}_n$.

Solution de l'exercice 19. On a vu à l'exercice 17 que l'on disposait d'un morphisme injectif canonique $\iota : \mathfrak{S}_n \to \mathfrak{S}_{n+2}$ (prolongement des bijections par l'identité sur les éléments $n+1$ et $n+2$) compatible avec la signature, i.e. tel que pour tout $\sigma \in \mathfrak{S}_n$, on a $\epsilon(\iota(\sigma)) = \epsilon(\sigma)$, et d'un morphisme injectif canonique $\psi : \mathfrak{S}_n \to \mathfrak{A}_{n+2}$. Puisque deux permutations conjuguées ont même signature, et puisqu'il existe dans $\mathfrak{S}_n$ des permutations impaires, on voit donc que les deux sous-groupes $\iota(\mathfrak{S}_n)$ et $\psi(\mathfrak{S}_\mathfrak{n})$ de $\mathfrak{S}_{n+2}$ sont isomorphes à $\mathfrak{S}_n$ et ne sont pas conjugués.

Exercice 20 : $\star\star\star$
Montrer que tout sous-groupe d'indice n dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Solution de l'exercice 20.
– On suppose $n \geq 5$. On note $G = \mathfrak{S}_n$ et H un sous-groupe de G d'indice n. On note enfin $X := G/H$ l'ensemble quotient de cardinal n. On dispose de l'action naturelle de G sur X par multiplication à droite, qui induit un morphisme de groupes

$$\psi : G \to \mathfrak{S}(X) \cong \mathfrak{S}_n \,.$$

Montrons que c'est un isomorphisme : son noyau est un sous-groupe distingué de $G = \mathfrak{S}_n$, non égal à $\mathfrak{S}_n$ (car l'action est transitive). La simplicité de $\mathfrak{A}_n$ assure que ce noyau est $\mathfrak{A}_n$ ou $\{\mathrm{id}\}$. Le premier cas est impossible car l'action est transitive et $|X| > 2$. Donc ψ est injective, donc par cardinalité, c'est un isomorphisme.
On peut restreindre l'action au sous-groupe H. D'où une action de H sur X. Or le point $x := H \in X$ est clairement un point fixe pour l'action de H, donc on en déduit une action de H sur $X' := X \setminus \{x\}$. D'où un morphisme

$$\varphi : H \to \mathfrak{S}(X') \cong \mathfrak{S}_{n-1} \,.$$

Ce morphisme φ est injectif car ψ l'est, donc par cardinalité, c'est un isomorphisme, d'où la conclusion.
– Si $2 \leq n \leq 4$, on montre le résultat à la main : si $n = 2$ ou 3, le résultat est évident. Si $n = 4$, on utilise l'exercice 8 pour savoir qu'un sous-groupe d'indice 4 dans $\mathfrak{S}_4$ est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou $\mathfrak{S}_3$. Or $\mathfrak{S}_4$ ne contient aucun élément d'ordre 6, donc ce sous-groupe est bien isomorphe à $\mathfrak{S}_3$.

TD2 : Actions de groupes et théorèmes de Sylow

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Soit p un nombre premier.

a) Montrer qu'un groupe de cardinal p^2 est commutatif.

b) Combien d'éléments d'ordre p y a-t-il dans un groupe de cardinal p ? Et dans un groupe de cardinal p^2 ?

Solution de l'exercice 1.

a) Soit G un groupe d'ordre p^2. L'équation aux classes pour l'action de G sur lui-même par conjugaison assure que le centre Z de G n'est pas réduit à l'élément neutre. Donc G/Z est de cardinal 1 ou p. Dans le second cas, le groupe G/Z est donc cyclique, ce qui assure que G est commutatif (voir la feuille de TD1, exercice 9). En outre, si G admet un élément d'ordre p^2, alors G est cyclique et isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Si G n'admet pas de tel élément, alors tous ses éléments autres que le neutre sont d'ordre p. En choisissant $x \in G \setminus \{e\}$ et $y \in G \setminus \langle x \rangle$, on voit que $G = \langle x, y \rangle$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

b) Dans un groupe de cardinal p, tout élément autre que le neutre est d'ordre p (1 et p sont les seuls diviseurs positifs de p). Donc un tel groupe admet $p-1$ éléments d'ordre p.
Soit G un groupe d'ordre p^2. Si G est cyclique engendré par x, on voit que x^n est d'ordre p si et seulement si p divise n et p^2 ne divise pas n. Cela assure que les éléments d'ordre p sont exactement les x^{pr}, avec $r = 1, \ldots, p-1$. Ils sont donc en nombre de $p-1$. Si G n'est pas cyclique, tous les éléments autres que le neutre sont d'ordre p, donc G contient $p^2 - 1$ éléments d'ordre p.

Exercice 2 : ⋆
Soit G un groupe fini agissant sur un ensemble fini X. En considérant l'ensemble

$$E := \{(g, x) \in G \times X : g \cdot x = x\},$$

calculer le nombre moyen de point fixes d'un élément de G.
Que dire en particulier si l'action est transitive ? Que dire de la moyenne du nombre de points fixes d'une permutation aléatoire ?

Solution de l'exercice 2. On calcule le cardinal de E de deux façons différentes :

$$|E| = \sum_{g \in G} |\mathrm{Fix}(g)|$$

et

$$\begin{aligned} |E| &= \textstyle\sum_{x \in X} |\mathrm{Stab}_G(x)| \\ &= \textstyle\sum_{\overline{x} \in X/G} \sum_{y \in \overline{x}} |\mathrm{Stab}_G(y)| \\ &= \textstyle\sum_{\overline{x} \in X/G} |\overline{x}|.|\mathrm{Stab}_G(\overline{x})| = |G|.|X/G|, \end{aligned}$$

où on note $\mathrm{Fix}(g) := \{x \in X : g \cdot x = x\}$ l'ensemble des points fixes de g dans X. On en déduit donc l'égalité

$$\sum_{g \in G} |\mathrm{Fix}(g) = |G|.|X/G|,$$

i.e.

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| = |X/G|\,.$$

Cela signifie que le nombre moyen de points fixes d'un élément de G est exactement $|X/G|$, i.e. le nombre d'orbites de l'action.
En particulier, si l'action est transitive, ce nombre vaut 1.
Par exemple, si $G = \mathfrak{S}_n$ agit (via l'action évidente) sur $X = \{1, \dots, n\}$, alors on voit que le nombre moyen de points fixes d'une permutation est exactement 1.

Exercice 3 : (Lemme de Cauchy) ⋆
Soit G un groupe fini et soit p un nombre premier divisant le cardinal de G. En utilisant une action convenable de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble

$$X = \{(g_1, \dots, g_p) \in G^p \mid g_1 \cdots g_p = 1\}$$

prouver que G admet un élément d'ordre p (sans utiliser les théorèmes de Sylow !).

Solution de l'exercice 3. On peut indicer un élément de X (qui est un p-uplets d'éléments de G) par les éléments de $\mathbb{Z}/p\mathbb{Z}$.
On considère l'action de $H = \mathbb{Z}/p\mathbb{Z}$ sur l'ensemble X définie, pour $k \in H$ et $x = (g_1, \dots, g_p) \in X$, par

$$h \cdot x := (g_{1+k}, \dots, g_{p+k})\,,$$

où les indices des g_i sont pris dans le groupe $H = \mathbb{Z}/p\mathbb{Z}$.
Vérifions que pour tout $k \in H$ et $x \in X$, $h \cdot x \in X$. Pour cela, on doit vérifier que si $g_1 \dots g_p = 1$ implique que $g_{1+k} \dots g_{p+k} = 1$. Ceci est clair via le calcul suivant : si $g_1 \dots g_p = 1$, on a $g_2 \dots g_p = g_1^{-1}$, donc $g_2 \dots g_p g_1 = 1$, et donc par récurrence, on a $g_{k+1} \dots g_p g_1 \dots g_k = 1$.
Donc la formule précédente définit bien une action de H sur X.
Léquation aux classes s'écrit alors

$$|X| = |X^H| + \sum_{\overline{x}\in X/H x\notin X^H} [H : H_x]\,.$$

Or H est de cardinal p, donc H_x est nécessairement le groupe trivial si $x \notin X^H$. D'où

$$|X| = |X^H| + p|X/H \setminus X^H|\,.$$

Or il est clair que $|X| = |G|^{p-1}$, donc $|X|$ est divisible par p.
L'équation aux classes assure donc que p divise $|X^H|$. Or $X^H \neq \emptyset$ car $(1, \dots, 1) \in X^H$, donc il existe un élément de X^H distinct de $(1, \dots, 1)$. Un tel élément est de la forme $(g, \dots, g) \in G^p$ pour un certain $g \in G \setminus \{1\}$. Par définition de X, on a donc $g^p = 1$ et $g \neq 1$, ce qui assure que g est d'ordre p dans G.

Exercice 4 : ⋆
Combien y a-t-il de colliers différents formés de 9 perles dont 4 bleues, 3 blanches et 2 rouges ?

Solution de l'exercice 4. On représente un collier par un cercle du plan euclidien orienté $\mathbb{R}^2$ (de centre 0 et rayon 1) muni de neuf points $A_1, \dots, A_9$ disposés à intervalles réguliers.
On choisit de dire que deux colliers sont équivalents (ce sont les "mêmes" colliers) si et seulement si on peut obtenir l'un à partir de l'autre en effectuant une rotation plane du collier ou en le retournant (comme une crêpe) dans l'espace de dimension 3.
Autrement dit, l'ensemble X de tous les colliers possibles à 9 perles dont 4 bleues, 3 blanches et 2 rouges, est muni d'une action du groupe diédral $G = \mathrm{D}_9$ des isométries d'un polygône régulier à neuf côtés. Ce groupe G est donc un sous-groupe de $\mathrm{SO}_2(\mathbb{R})$, il est de cardinal 18 et ses éléments sont les suivants :

$$G = \{\mathrm{id}, r, r^2, r^3, r^4, r^5, r^6, r^7, r^8, s, r\circ s, r^2\circ s, r^3\circ s, r^4\circ s, r^5\circ s, r^6\circ s, r^7\circ s, r^8\circ s\}\,,$$

où r est la rotation de centre O et d'angle $\frac{2\pi}{9}$ et s est la symétrie orthogonale d'axe $\Delta = (OA_1)$. En particulier, G contient 9 rotations et 9 symétries orthogonales.
Au vu de la discussion précédente, le nombre de colliers différents est exactement le nombre d'orbites dans l'action de G sur X, i.e. $|X/G|$.
On calcule ce nombre grâce à la formule démontrée à l'exercice 2 :

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| \,.$$

Calculons maintenant $\mathrm{Fix}(g)$ pour tout $g \in G$: soit $g \in G$.
- Si $g = \mathrm{id}$, il est clair que $\mathrm{Fix}(g) = X$.
- Si $g = r, r^2, r^4, r^5, r^7, r^8$, alors le sous-groupe de G engendré par g est constitué des 9 rotations (r^k engendre ce sous-groupe si et seulement si k est premier avec 9). Donc un collier fixe par g est fixe par r, ce qui implique que toutes les perles sont de la même couleur. Ceci n'est pas possible, donc $\mathrm{Fix}(g) = \emptyset$.
- Si $g = r^3, r^6$, alors dans un collier fixe par g, le nombre de perles d'une couleur donnée doit être un multiple de 3, ce qui n'est pas le cas dans l'ensemble X, donc $\mathrm{Fix}(g) = \emptyset$.
- Si g est une symétrie, on peut supposer $g = s$, les autres cas étant identiques. Puisque l'axe Δ de g ne contient qu'une perle (A_1 en l'occurence), dans un collier fixe par g, les perles A_i, $i \neq 1$ vont par paire de même couleur. Cela assure que la perle A_1 est nécessairement blanche. Se donner un collier fixe par g revient alors à se donner les couleurs des perles A_2, A_3, A_4, A_5 de sorte que 2 soient bleues, 1 blanche et 1 rouge. Il est clair que le nombre de tels colliers vaut

$$|\mathrm{Fix}(g)| = \binom{4}{2}.\binom{2}{1} = 6.2 = 12 \,.$$

Enfin, le cardinal de X se calcule simplement via la formule suivante

$$|X| = \binom{9}{4}.\binom{5}{3} = 126.10 = 1260 \,.$$

Donc on en déduit que

$$|X/G| = \frac{1}{18}\,(1260 + 9.12) = 76 \,.$$

Il y a donc exactement 76 colliers distincts (à équivalence près) satisfaisant les contraintes de l'énoncé.

Exercice 5 : $\star\star$
Soit G un groupe.

a) On suppose que G est fini et on note p le plus petit nombre premier divisant le cardinal de G. Montrer que tout sous-groupe de G d'indice p est distingué.

b) On suppose que G est infini et qu'il admet un sous-groupe strict H d'indice fini. Montrer que G n'est pas un groupe simple.

Solution de l'exercice 5.

a) Soit H un sous-groupe de G d'indice p. On note $X := G/H$. C'est un ensemble de cardinal p, muni de l'action naturelle transitive de G. Cette action induit un morphisme de groupes finis $\varphi : G \to \mathfrak{S}(X)$. On s'intéresse à la restriction de cette action au sous-groupe H, i.e. au morphisme

$$\varphi : H \to \mathfrak{S}(X) \,.$$

Puisque H agit trivialement sur la classe x_0 de H dans $X = G/H$, l'action de H sur X induit une action de H sur $X' := X \setminus \{x_0\}$, c'est-à-dire un morphisme de groupes

$$\psi : H \to \mathfrak{S}(X') \,.$$

Or X' est de cardinal $p-1$, donc tous les facteurs premiers du cardinal de $\mathfrak{S}(X')$ sont strictement inférieur à p. Or les facteurs premiers du cardinal de H sont par hypothèse tous supérieurs ou égaux à p. Par conséquent, les cardinaux de H et $\mathfrak{S}(X')$ sont premiers entre eux, ce qui implique que le morphisme ψ est le morphisme trivial. Donc H agit trivialement sur X', donc aussi sur X.

Montrons que cela implique que H est distingué dans G. Soit $h \in H$ et $g \in G$. Puisque H agit trivialement sur X, on sait que $h \cdot (gH) = gH$, donc $(g^{-1}hg)H = H$, donc $g^{-1}hg \in H$, donc H est distingué dans G.

b) Comme en a), on considère l'action de G sur l'ensemble fini $X := G/H$, i.e. le morphisme de groupes induit

$$\varphi : G \to \mathfrak{S}(X)\,.$$

Comme l'action de G sur X est transitive et comme $H \neq G$, le morphisme φ est non trivial. Son noyau $\mathrm{Ker}(\varphi)$ est donc un sous-groupe distingué de G distinct de G. En outre, G est infini et $\mathfrak{S}(X)$ est fini, donc le morphisme φ n'est pas injectif, donc $\mathrm{Ker}(\varphi)$ n'est pas le groupe trivial. Donc $\mathrm{Ker}(\varphi)$ est un sous-groupe distingué non trivial de G, donc G n'est pas un groupe simple.

Exercice 6 :

a) Montrer que si G est un groupe fini et H un sous-groupe strict de G, alors la réunion des conjugués de H n'est pas égale à G tout entier. Que dire si le groupe G est infini et si H est d'indice fini dans G ? Et si on ne suppose plus H d'indice fini ?

b) Soit G un groupe fini agissant transitivement sur un ensemble fini X tel que $|X| \geq 2$. Montrer qu'il existe $g \in G$ ne fixant aucun point de X.

Solution de l'exercice 6.

a) Puisque pour tout $g \in G$ et $h \in H$, on a $gHg^{-1} = (gh)H(gh)^{-1}$ et $|gHg^{-1}| = |gHG^{-1}|$, on estime le cardinal de $\bigcup_{g\in G} gHg^{-1}$ de la façon suivante :

$$\begin{aligned} |\textstyle\bigcup_{g\in G} gHg^{-1} \setminus \{e\}| &= |\textstyle\bigcup_{\overline{g}\in G/H} gHg^{-1} \setminus \{e\}| \\ &\leq \textstyle\sum_{\overline{g}\in G/H} |gHg^{-1} \setminus \{e\}| \\ &\leq \textstyle\sum_{\overline{g}\in G/H} |H \setminus \{e\}| \\ &\leq |G/H|.\,(|H|-1) \\ &\leq |G| - \tfrac{|G|}{|H|}\,. \end{aligned}$$

Or on a $|G \setminus \{e\}| = |G| - 1$, donc comme $H \neq G$, on a bien

$$|\bigcup_{g\in G} gHg^{-1} \setminus \{e\}| < |G \setminus \{e\}|$$

donc

$$\bigcup_{g\in G} gHg^{-1} \neq G\,.$$

Si l'on suppose désormais le groupe G infini et le sous-groupe H d'indice fini, alors on a une action naturelle transitive de G sur l'ensemble fini $X := G/H$ par multiplication à droite, induisant un morphisme non trivial

$$\varphi : G \to \mathfrak{S}(X)\,.$$

Or $\mathfrak{S}(X)$ est un groupe fini, $\varphi(H)$ est contenu dans le sous-groupe de $\mathfrak{S}(X)$ fixant la classe de H, et la transitivité de l'action de G sur X assure que $\varphi(G)$ n'est pas contenu dans ce sous-groupe. Donc $\varphi(H)$ est un sous-groupe strict du groupe fini $\varphi(G)$. Donc la preuve précédente assure que

$$\bigcup_{g\in G} \varphi(g)\varphi(H)\varphi(g)^{-1} \neq \varphi(G)\,.$$

On en déduit immédiatement que

$$\bigcup_{g\in G} gHg^{-1} \neq G\,.$$

Enfin, si le sous-groupe H n'est plus supposé d'indice fini, la conclusion n'est plus vérifiée en général : par exemple, si $G := \mathrm{SO}_3(\mathbb{R})$ est le groupe des rotations vectorielles de $\mathbb{R}^3$ (matrices réelles 3×3 orthogonales de déterminant 1) et si $H := \mathrm{SO}_2(\mathbb{R})$ est le sous-groupe des rotations d'axe fixé Δ (par exemple $\Delta = \mathbb{R}(1,0,0)$), alors H est clairement un sous-groupe stricit de G (d'indice infini) et pourtant on a

$$\bigcup_{g\in G} gHg^{-1} = G\,,$$

puisque toute rotation de $\mathbb{R}^3$ est conjuguée dans $\mathrm{SO}_3(\mathbb{R})$ à une rotation d'axe Δ.

Un autre tel exemple est donné par le groupe $G = \mathrm{GL}_n(\mathbb{C})$ ($n \geq 2$) et le sous-groupe strict $H := \mathrm{T}_n(\mathbb{C}) \cap \mathrm{GL}_n(\mathbb{C})$ des matrices triangulaires supérieures inversibles : un résultat classique d'algèbre linéaire assure que tout élément de g est trigonalisable, i.e. conjugué dans G à un élément de H, ce qui assure que

$$\bigcup_{g\in G} gHg^{-1} = G\,.$$

b) On choisit un point $x_0 \in X$ et on note $H := \mathrm{Stab}_G(x_0)$. Alors H est un sous-groupe de G, et $H \neq G$ (sinon on aurait $X = \{x_0\}$). Donc la question a) assure qu'il existe $g_0 \in G$ tel que $g_0 \notin \bigcup_{g\in G} gHg^{-1}$. Soit alors $x \in X$. On sait qu'il existe $g \in G$ tel que $x = g\cdot x_0$. Alors $\mathrm{Stab}_G(x) = gHg^{-1}$, donc par construction on sait que $g_0 \notin \mathrm{Stab}_G(x)$, ce qui signifie que $g_0\cdot x \neq x$. Cela conclut la preuve.

Exercice 7 :
Soit G un groupe fini non trivial agissant sur un ensemble fini X. On suppose que pour tout $g \neq e \in G$, il existe un unique $x \in X$ tel que $g\cdot x = x$. On souhaite montrer que X admet un point fixe sous G (nécessairement unique).

a) On note $Y := \{x \in X : \mathrm{Stab}_G(x) \neq \{e\}\}$. Montrer que Y est stable par G.

b) On note $n = |Y/G|$ et $y_1, \ldots, y_n$ un système de représentants de Y/G. Pour tout i, on note m_i le cardinal de $\mathrm{Stab}_G(y_i)$. En considérant l'ensemble $Z := \{(g,x) \in (G\setminus\{e\}) \times X : g\cdot x = x\}$, montrer que

$$1 - \frac{1}{|G|} = \sum_{i=1}^{n}\left(1 - \frac{1}{m_i}\right)\,.$$

c) En déduire que $n = 1$.

d) Conclure.

Solution de l'exercice 7.

a) Soit $x \in Y$ et $g \in G$. On sait que $\mathrm{Stab}_G(g\cdot x) = g\mathrm{Stab}_G(x)g^{-1}$, donc comme $\mathrm{Stab}_G(x) \neq \{e\}$, on a $\mathrm{Stab}_G(g\cdot x) \neq \{e\}$, donc $g\cdot x \in Y$. Donc Y est stable par G.

b) On calcule le cardinal de Z de deux façons différents comme dans l'exercice 2 et on obtient, puisque pour tout $x \in X\setminus Y$, $\mathrm{Stab}_G(x)\setminus\{e\} = \emptyset$:

$$|G| - 1 = \sum_{y\in Y}\left(|\mathrm{Stab}_G(y)| - 1\right)\,.$$

On peut alors regrouper les éléments de Y par orbites, et on obtient

$$|G| - 1 = \sum_{i=1}^{n}|O_{y_i}|\left(|\mathrm{Stab}_G(y_i)| - 1\right) = \sum_{i=1}^{n}|G|\left(1 - \frac{1}{m_i}\right)\,.$$

On divise par $|G|$ et on obtient le résultat.

c) Par définition, on a pour tout i, $m_i \geq 2$. Donc on en déduit que

$$1 > 1 - \frac{1}{|G|} = \sum_{i=1}^{n} \left(1 - \frac{1}{m_i}\right) \geq \frac{n}{2},$$

donc $n < 2$, donc $n = 1$ (le cas $n = 0$ est impossible car G est non trivial).

d) On choisit donc $y_1 \in Y$. Alors par les questions b) et c), on a $|\mathrm{Stab}_G(y_1)| = |G|$, donc $\mathrm{Stab}_G(y_1) = G$, donc y_1 est fixe par G.

Exercice 8 : $\star\star$

a) Soit G un p-groupe fini agissant sur un ensemble fini X. On note X^G l'ensemble des points fixes de X sous G. Montrer que

$$|X^G| \equiv |X| \pmod{p}.$$

b) Soit G un p-groupe agissant sur un ensemble fini X dont le cardinal n'est pas divisible par p. Montrer que X admet un point fixe sous G.

c) Soit G un p-groupe fini et $H \neq \{e\}$ un sous-groupe distingué de G. Montrer que l'intersection de H avec le centre de G n'est pas réduite à l'élément neutre.

d) Montrer qu'un groupe d'ordre p^n admet des sous-groupes d'ordre p^i pour tout $0 \leq i \leq n$.

e) Soit p un nombre premier congru à 1 modulo 4. On souhaite montrer que p est somme de deux carrés d'entiers. On note

$$X := \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}.$$

i) On définit $i : X \to X$ par les formules suivantes

$$i : (x, y, z) \mapsto \begin{array}{l} (x + 2z, z, y - x - z) \text{ si } x < y - z, \\ (2y - x, y, x - y + z) \text{ si } y - z < x < 2y, \\ (x - 2y, x - y + z, y) \text{ si } x > 2y. \end{array}$$

Vérifier que i est bien définie.

ii) Montrer que i est une involution.

iii) Montrer que i a un unique point fixe.

iv) Montrer que $|X|$ est impair.

v) Montrer que l'application $j : X \to X$ définie par $j(x, y, z) := (x, z, y)$ admet un point fixe.

vi) Conclure.

Solution de l'exercice 8.

a) On note p^n le cardinal de G. On écrit l'équation aux classes :

$$|X| = \sum_{\overline{x} \in X/G} |O_x| = \sum_{x \in X^G} 1 + \sum_{\overline{x} \in X/G,\, x \notin X^G} \frac{|G|}{|\mathrm{Stab}_G(x)|} = |X^G| + \sum_{\overline{x} \in X/G,\, x \notin X^G} \frac{|G|}{|\mathrm{Stab}_G(x)|}.$$

Or, pour tout $x \notin X^G$, $\mathrm{Stab}_G(x)$ est un sous-groupe strict de G, son cardinal est donc de la forme p^i, avec $0 \leq i < n$. Donc $\frac{|G|}{|\mathrm{Stab}_G(x)|} = p^{n-i}$ est divisible par p, donc la formule précédente assure que

$$|X^G| \equiv |X| \pmod{p}.$$

b) Par hypothèse, on a $|X| \not\equiv 0 \pmod{p}$, donc par la question a), on a $|X^G| \not\equiv 0 \pmod{p}$, donc en particulier $|X^G| \neq 0$, donc $X^G \neq \emptyset$.

c) On considère l'ensemble $X := H$ et l'action de G sur X par conjugaison. Alors la question a) assure que l'on a $|H^G| \equiv |H| \equiv 0 \pmod{p}$. Or $e \in H^G$, donc $|H^G| \neq 0$, donc $|H^G| \geq p$, donc H^G n'est pas réduit à l'élement neutre. Enfin, il est clair que H^G est l'intersection de H avec le centre de G.

d) On raisonne par récurrence sur n. Pour $n = 0$, la propriété est évidente. Supposons la propriété connue pour un entier n et montrons-la pour l'entier $n+1$. Soit G un groupe d'ordre p^{n+1}. Si $i = 0$, la réponse est évidente. On peut donc supposer $i \geq 1$. La question c) assure que le centre de G est non trivial, et comme ce centre est un p-groupe, il admet un élément d'ordre p, donc un sous-groupe Z d'ordre p. Comme Z est central dans G, il est distingué. On note $\pi : G \to G/Z$ le morphisme quotient. Par hypothèse de récurrence, comme G/Z est de cardinal p^n, il existe un sous-groupe H' de G/Z de cardinal p^{i-1}. Alors il est clair que $H := \pi^{-1}(H')$ est un sous-groupe de G de cardinal p^i. Cela conclut la preuve.

e) i) Il suffit de vérifier que pour tout $(x, y, z) \in X$, on a $x \neq y - z$, $x \neq 2y$ et $i(x, y, z) \in X$. Tout cela est évident (les deux premières vérifications utilisent le fait que p est premier).

ii) Il s'agit de vérifier que pour tout $(x, y, z) \in X$, on a $i(i(x, y, z)) = (x, y, z)$. Pour cela, il y a trois cas à considérer :
- Si $x < y - z$: alors $i(x, y, z) = (x', y', z')$ avec $x' = x + 2z$, $y' = z$ et $z' = y - x - z$. On voit immédiatemment que $x' > 2y'$, ce qui assure que $i(x', y', z') = (x' - 2y', x' - y' + z', y') = (x, y, z)$.
- Si $y - z < x < 2y$: alors $i(x, y, z) = (x', y', z')$ avec $x' = 2y - x$, $y' = y$ et $z' = x - y + z$. On voit immédiatemment que $y' - z' < x' < 2y'$, ce qui assure que $i(x', y', z') = (2y' - x', y', x' - y' + z') = (x, y, z)$.
- Si $x > 2y$: alors $i(x, y, z) = (x', y', z')$ avec $x' = x - 2y$, $y' = x - y + z$ et $z' = y$. On voit immédiatemment que $x' < y' - z'$, ce qui assure que $i(x', y', z') = (x' + 2z', z', y' - x' - z') = (x, y, z)$.

Donc $i \circ i = \mathrm{id}_X$.

Enfin, il est clair que cela définit une action de $G = \mathbb{Z}/2\mathbb{Z}$ sur X via la formule $g \cdot x := i^g(x)$ pour $g \in G$ et $x \in X$.

iii) Soit $(x, y, z) \in X$. La question e)ii) assure que $i(x, y, z) = (x, y, z)$ si et seulement si $y - z < x < 2y$, $x = 2y - x$, $y = y$ et $z = x - y + z$ si et seulement si $x = y$. En outre, pour tout $(x, z) \in \mathbb{N}^2$, on a $(x, x, z) \in X$ si et seulement si $x^2 + 4xz = p$ si et seulement si $x(x + 4z) = p$ si et seulement si $x = 1$ et $p = 4z + 1$ (car p est premier). Or par hypothèse, p est congru à 1 modulo 4, donc il existe un unique $k \in \mathbb{N}$ tel que $p = 4k + 1$. Finalement, on a montré que i admettait le point $(1, 1, k)$ comme unique point fixe.

iv) Comme G est un 2-groupe, la question a) assure que l'on a

$$|X^G| \equiv |X| \ (\text{mod. } 2)\,.$$

Or $|X^G| = 1$, donc $|X| \equiv 1 (\text{mod. } 2)$, i.e. $|X|$ est impair.

v) L'application j est clairement une involution de X, donc elle définit une nouvelle action de G sur X. Par la question a), le nombre de points fixes pour cette action (qui est le nombre de points fixes de j) est congru à $|X|$ modulo 2. Or la question e)iv) assure que $|X|$ est impair, donc j a un nombre impair de points fixes, donc j a (au moins) un point fixe.

vi) Notons (x_0, y_0, y_0) un point fixe de j (qui existe par la question précédente). Alors on a $x_0^2 + 4y_0^2 = p$, i.e.

$$p = x_0^2 + (2y_0)^2\,,$$

ce qui conclut la preuve.

Exercice 9 :
Soit $n \geq 1$ un entier. Montrer qu'il n'existe qu'un nombre fini de classes d'isomorphisme de groupes finis admettant exactement n classes de conjugaison.

Solution de l'exercice 9. Soit G un tel groupe. On considère l'action de G sur lui-même par conjugaison : si $g \in G$ et $x \in G$, on pose $g \cdot x := gxg^{-1}$. Les classes de conjugaison dans G sont exactement les orbites pour cette action, donc on sait que cette action admet exactement n orbites. Si on note

$g_1, \dots, g_n$ un ensemble de représentants dans G pour l'action par conjugaison, et si $m_i := |\mathrm{Stab}_G(g_i)|$, alors l'équation aux classes assure que

$$\sum_{i=1}^{n} \frac{1}{m_i} = 1\,. \tag{1}$$

Comme il est clair que les m_i déterminent le cardinal de G (le plus grand des m_i est égal à $|G|$, puisque l'élément neutre commute à tous les éléments de G), il suffit de montrer que l'équation (1) d'inconnues $(m_1, \dots, m_n)$ admet un nombre fini de solutions dans $\mathbb{N}^n$.
Pour cela, on peut raisonner comme suit : pour $A \in \mathbb{Q}$, on note $N(n, A)$ le nombre de solutions (éventuellement infini) dans $\mathbb{N}^n$ de l'équation

$$\sum_{i=1}^{n} \frac{1}{m_i} = A\,. \tag{2}$$

Soit $n \geq 2$. Il est clair que si $(m_1, \dots, m_n)$ est solution de (2), si on choisit $1 \leq j \leq n$ tel que $m_j = \min_i m_i$, alors $\frac{1}{A} < m_j \leq \frac{n}{A}$ et $(m_i)_{i \neq j}$ est solution de l'équation

$$\sum_{i \neq j} \frac{1}{m_i} = A - \frac{1}{m_j}\,. \tag{3}$$

Donc on en déduit que

$$N(n, A) \leq n \sum_{\frac{1}{A} < k \leq \frac{n}{A}} N\left(n-1, A - \frac{1}{k}\right)\,.$$

Comme $N(1, A) \leq 1$ pour tout $A \in \mathbb{Q}$, une récurrence simple assure que $N(n, A)$ est fini pour tout $A \in \mathbb{Q}$.
Cela assure que $N(n, 1)$ est fini pour tout n, et donc que si G a exactement n classes de conjugaison, son cardinal est borné par une constante ne dépendant que de n. Comme il n'y a qu'un nombre fini de (classes d'isomorphisme de) groupes de cardinal donné, cela assure qu'il n'y a qu'un nombre fini de (classes d'isomorphisme de) groupes finis ayant n classes de conjugaison.

Exercice 10 : $\star\star$
On suppose qu'il existe un groupe simple G d'ordre 180.

a) Montrer que G contient trente-six 5-Sylow.

b) Montrer que G contient dix 3-Sylow, puis que deux 3-Sylow distincts ne peuvent pas contenir un même élément $g \neq e_G$. (Indication : on pourra considérer les ordres possibles pour le centralisateur de g ; on observera qu'un groupe d'ordre 18 admet un unique 3-Sylow.)

c) Conclure.

Solution de l'exercice 10.

a) Pour tout p premier divisant $|G|$, on note n_p le nombre de p-Sylow de G. Les théorèmes de Sylow assurent que n_5 divise 36 et $n_5 \equiv 1$ [5]. Cela implique que $n_5 = 1, 6, \text{ou } 36$. Comme G est simple, le cas $n_5 = 1$ est impossible (sinon le 5-Sylow serait distingué dans G), donc $n_5 = 6$ ou $n_5 = 36$. Supposons $n_5 = 6$, alors l'action transitive de G par conjugaison sur l'ensemble de ses 5-Sylow induit un morphisme non trivial $G \to \mathfrak{S}_6$. Comme G est simple, ce morphisme est injectif. Comme le morphisme $G \to \mathbb{Z}/2\mathbb{Z}$ donné par la signature a nécessairement un noyau trivial, on voit que G est un sous-groupe de $\mathfrak{A}_6$. En calculant les cardinaux, on voit que G est un sous-groupe d'indice 2 dans $\mathfrak{A}_6$, il est donc distingué et non trivial, ce qui contredit la simplicité de $\mathfrak{A}_6$. Cela assure donc que $n_5 = 36$.

b) Comme auparavant, on sait que n_3 divise 20 et que $n_3 \equiv 1$ [3]. Cela implique, comme G est simple, que $n_3 = 4$ ou $n_3 = 10$. Si on avait $n_3 = 4$, on en déduirait comme en a) un morphisme injectif de G dans $\mathfrak{S}_4$, ce qui est impossible car le cardinal de G est strictement supérieur à celui de $\mathfrak{S}_4$. Donc $n_3 = 10$.

Soient S et T deux 3-Sylow de G distincts, et soit $g \in S \cap T$. On suppose $g \neq e_G$ et on note $Z := \{x \in G : xg = g = x\}$ le centralisateur de g dans G. Puisqu'un groupe d'ordre 9 est abélien, on voit que Z contient S et T. Donc nécessairement, on a $|Z| \in \{18, 36, 45, 90\}$. Or l'action (transitive) de G sur G/Z induit un morphisme injectif de G vers $\mathfrak{S}(G/Z)$, donc par cardinalité, on a nécessairement $|Z| = 18$. Alors S et T sont des 3-Sylow de Z, et un groupe d'ordre 18 admet un unique 3-Sylow, donc $S = T$, ce qui est contradictoire. Donc finalement $S \cap T = \{e_G\}$.

Finalement, G admet dix 3-Sylow dont les intersections deux-à-deux sont triviales. Par conséquent, il y a dans G exactement $10.8 = 80$ éléments $\neq e_G$ d'ordre divisant 9.

c) La question a) assure que G contient exactement $36.4 = 144$ éléments d'ordre 5. Donc G possède au moins $144 + 80$ éléments, ce qui est contradictoire.

Donc il n'existe pas de groupe simple d'ordre 180.

Exercice 11 : ⋆⋆

Soient p et q deux nombres premiers distincts.

a) Montrer qu'un groupe d'ordre pq n'est pas simple.

b) Montrer que si $p < q$ et p ne divise pas $q - 1$, alors tout groupe d'ordre pq est cyclique.

c) Soit G un groupe simple d'ordre $p^\alpha m$, avec $\alpha \geq 1$ et m non divisible par p. On note n_p le nombre de p-Sylow de G. Montrer que $|G|$ divise $n_p!$.

d) Montrer qu'un groupe d'ordre $p^m q^n$, avec $p < q$, $1 \leq m \leq 2$ et $n \geq 1$, n'est pas simple.

e) Montrer qu'un groupe d'ordre $p^2 q$ ou $p^3 q$ n'est pas simple.

Solution de l'exercice 11.

a) Soit G un groupe d'ordre pq. On peut supposer $p < q$. On sait que le nombre de q-Sylow n_q divise p et est congru à 1 modulo q. Comme $p < q$, cela assure que $n_q = 1$, donc l'unique q-Sylow de G est distingué dans G, donc G n'est pas simple.

b) La question précédente assure que G admet un sous-groupe distingué H d'ordre q, engendré par un élément x. Le quotient G/H est cyclique d'ordre p. L'action de G par conjugaison sur H induit une action de G/H sur H, i.e. un morphisme de groupes $G/H \to \mathrm{Aut}(H) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Par hypothèse, comme p ne divise pas $q - 1$, ce morphisme est nécessairement trivial. Donc le sous-groupe H est contenu dans le centre de G. Or G admet un élément y d'ordre p, qui commute donc avec x. Donc l'élément $xy \in G$ est d'ordre pq, donc G est cyclique.

c) On regarde l'action transitive de G par conjugaison sur l'ensemble S_p de ses p-Sylow. Comme G est simple, $n_p > 1$, donc cela fournit un morphisme de groupes non trivial $G \to \mathfrak{S}(S_p) \cong \mathfrak{S}_{n_p}$. Par simplicité de G, ce morphisme est injectif, donc $|G|$ divise $|\mathfrak{S}_{n_p}| = n_p!$.

d) Par la question a), on peut supposer $m = 2$. Soit G un tel groupe, que l'on suppose simple. On sait que $n_q \equiv 1 \ [q]$ et n_q divise p^2. Donc $n_q = p^2$ et q divise $p^2 - 1 = (p-1)(p+1)$, donc $q \leq p + 1$, donc $q = p + 1$, donc $p = 2$ et $q = 3$, donc $|G| = 4.3^n$. La question c) assure alors que 4.3^n divise $4!$, donc 3^n divise 6, donc $n = 1$ et G est de cardinal 12. Alors $n_2 = 3$, et donc $|G|$ divise $3! = 6$, ce qui est contradictoire. Cela conclut la preuve.

e) On suppose G simple. La question d) assure que l'on peut supposer $|G| = p^3 q$, avec $p < q$. Alors nécessairement $n_q \equiv 1 \ [q]$ et $n_q = p$, p^2 ou p^3. Comme $p < q$, on a $n_q = p^2$ ou p^3. Comptons les éléments d'ordre q dans G : il y en a exactement $n_q(q-1)$.

Si $n_q = p^3$, alors G contient exactement $|G| - p^3$ éléments d'ordre q. Le complémentaire de l'ensemble de ces éléments d'ordre q est donc un ensemble de cardinal p^3. Or tout p-Sylow de G est de cardinal p^3 et ne contient aucun élément d'ordre q, donc il coïncide avec le complémentaire de l'ensemble des éléments d'ordre q. Cela assure que G admet unique p-Sylow, qui est donc distingué, donc G n'est pas simple, ce qui est une contradiction.

Si $n_q = p^2$, alors la condition $n_q \equiv 1 \ [q]$ assure que q divise $p^2 - 1$, donc $q = p + 1$, donc $p = 2$ et $q = 3$ et $|G| = 24$. Alors $n_2 = 3$, donc $|G| = 24$ divise $3! = 6$, ce qui est contradictoire.

Cela conclut la preuve.

Exercice 12 : $\star$

Montrer qu'un groupe non commutatif d'ordre < 60 n'est pas simple.

Solution de l'exercice 12. On utilise les exercices 8 et 11 pour réduire le problème : il reste à traiter le cas des groupes de cardinal 30, 42 et 48.

- Soit G un groupe d'ordre $30 = 2.3.5$. Supposons G simple. Alors les théorèmes de Sylow assurent que $n_3 = 10$ et $n_5 = 6$. Or l'intersection de deux 3-Sylow (resp. de deux 5-Sylow) distincts de G est réduite à l'élément neutre, donc G admet $10.2 = 20$ éléments d'ordre 3 et $6.4 = 24$ éléments d'ordre 5. Comme $20 + 24 > 30$, on a une contradiction.
- Soit G un groupe d'ordre $42 = 2.3.7$. Les théorèmes de Sylow assurent que $n_7 = 1$, donc G admet un unique 7-Sylow, qui est donc distingué dans G, donc G n'est pas simple.
- Soit G un groupe d'ordre $38 = 2^4.3$. Supposons G simple. Alors les théorèmes de Sylow assurent que $n_2 = 3$. Par conséquent, l'exercice 11, question c), assure que le cardinal de G divise $n_2! = 6$, ce qui est une contradiction.

Cela termine la preuve.

Exercice 13 : $\star\star$

On cherche à montrer que $\mathfrak{A}_5$ est le seul groupe simple d'ordre 60.

a) Faire la liste des éléments de $\mathfrak{A}_5$ avec leur ordre respectif. Décrire les classes de conjugaison dans $\mathfrak{A}_5$.

b) Montrer que $\mathfrak{A}_5$ est simple.

c) Soit G un groupe simple d'ordre 60. Montrer que le nombre de 2-Sylow de G est égal à 5 ou à 15.

d) En déduire que G contient un sous-groupe d'ordre 12.

e) Conclure.

Solution de l'exercice 13.

a) Les 60 éléments de $\mathfrak{A}_5$ sont les suivants :
   - l'identité, d'ordre 1, qui forme une classe de conjugaison.
   - les bitranspositions $(ab)(cd)$, avec $\{a, b, c, d\}$ de cardinal 4. Elles sont au nombre de 15, elles sont d'ordre 2, et elles forment une classe de conjugaison.
   - les 3-cycles (abc), avec $\{a, b, c\}$ de cardinal 3. Ils sont au nombre de 20, ils sont d'ordre 3, et forment une classe de conjugaison.
   - les 5-cycles $(abcde)$, avec $\{a, b, c, d, e\}$ de cardinal 5. Ils sont au nombre de 24, ils sont d'ordre 5, et ils forment exactement deux classes de conjugaison : celle de (12345) et celle de (21345) (voir par exemple la feuille de TD1, exercice 18).

   On vérifie que l'on a bien énuméré tous les éléments en calculant $1 + 15 + 20 + 24 = 60$.

b) Soit $H \neq \{e\}$ un sous-groupe distingué de $G = \mathfrak{A}_5$. Comme H est distingué, H est réunion de classes de conjugaison dans G. Puisque $1 + 15 = 16$, $1 + 12 = 13$, $1 + 24 = 25$, $1 + 15 + 12 = 28$, $1 + 15 + 24 = 40$, $1 + 20 = 21$, $1 + 2015 = 36$, $1 + 20 + 12 = 33$, $1 + 20 + 24 = 45$, et qu'aucun des ces entiers ne divise 60, le théorème de Lagrange assure que H contient nécessairement toutes les classes de conjugaison dans G, donc $H = G$.

c) Les théorèmes de Sylow assure que n_2 est impair et divise 15, ce qui assure que $n_2 = 1$, 3, 5 ou 15. Comme G est simple, on a $n_2 \neq 1$. Si $n_2 = 3$, alors l'exercice 11, question c), assure que 60 divise $3! = 6$, ce qui est contradictoire. Donc $n_2 = 5$ ou 15.

d) – Supposons d'abord $n_2 = 5$. Alors le normalisateur d'un 2-Sylow de G est de cardinal $60/5 = 12$ d'où le résultat.
   – Supposons maintenant $n_2 = 15$. Montrons qu'il existe deux 2-Sylow distincts S et T tels que $|S \cap T| = 2$. Dans le cas contraire, on aurait exactement $15.3+1 = 46$ éléments d'ordre divisant 4 ; les théorèmes de Sylow assurent que $n_5 = 6$, donc G contient $6.4 = 24$ éléments d'ordre 5. Mais ceci est contradictoire car $46 + 24 = 70 > |G|$. On dispose donc de deux 2-Sylow distincts S et T tels que $S \cap T = \{e, x\}$, avec x d'ordre 2. Notons H le centralisateur de x

dans G. Alors H contient S et T donc son cardinal est multiple de 4 et > 6, donc $|H| = 12$, 20 ou 60. Dans le deuxième cas, l'action transitive de G sur G/H induit un morphisme injectif $G \to \mathfrak{S}(G/H) \cong \mathfrak{S}_3$, ce qui est contradictoire. Dans le troisième cas, x est dans le centre de G, ce qui assure $Z(G)$ est non trivial, ce qui contredit le fait que G soit simple. Donc finalement on a bien $|H| = 12$.

– On note $H \subset G$ le sous-groupe d'ordre 12 construit en d). L'action transitive de G sur G/H induit un morphisme injectif $\varphi : G \to \mathfrak{S}(G/H) \cong \mathfrak{S}_5$. Alors $\varphi(G) \cap \mathfrak{A}_5$ est un sous-groupe distingué de $\varphi(G)$ (qui est simple), donc $\varphi(G) \cap \mathfrak{A}_5 = \{\mathrm{id}\}$ ou $\mathfrak{A}_5$. Dans le premier cas, on en déduit que $|\varphi(G)| \leq 2$ (en composant avec la signature), ce qui est contradictoire. Donc $\varphi(G)$ contient $\mathfrak{A}_5$, donc par cardinalité, φ induit bien un isomorphisme $G \cong \mathfrak{A}_5$.

Exercice 14 : $\star\star\star$

Soit G un groupe fini.

a) Soit H un sous-groupe de G d'indice n. On note $x_1, \ldots, x_n \in G$ un ensemble de représentants de G modulo H. L'action de G sur G/H induit une action de G sur $\{1, \ldots, n\}$, et pour tout $g \in G$ et $1 \leq i \leq n$, il existe $h_{i,g\cdot i} \in H$ tel que $gx_i = x_{g\cdot i} h_{i,g\cdot i}$. On note enfin $\pi : H \to H/D(H)$ la projection canonique. Montrer que la formule

$$V(g) := \pi\left(\prod_{i=1}^{n} h_{i,g\cdot i}\right)$$

définit un morphisme de groupes $G \to H/D(H)$ indépendant du choix des x_i.

b) Avec les notations précédentes, soit $h \in H$. On considère l'action de $\langle h \rangle$ sur $X = G/H$ et on note $g_1, \ldots, g_r$ des éléments de G tels que les classes $[g_i]$ des g_i dans X forment un ensemble de représentants pour cette action. Pour tout i, on note n_i l'entier minimal non nul tel que $h^{n_i} \cdot [g_i] = [g_i]$. Montrer que

$$V(h) = \pi\left(\prod_{i=1}^{r} g_i^{-1} h^{n_i} g_i\right).$$

c) Soient S un p-Sylow de G et $A, B \subset S$ des parties stables par conjugaison dans S. Montrer que si A et B sont conjuguées dans G, alors elles le sont dans $N_G(S)$ (on pourra considérer deux p-Sylow de $N_G(A)$).

d) Soit S un p-Sylow de G tel que $S \subset Z(N_G(S))$. Montrer que le morphisme $V : G \to S$ défini à la question a) est surjectif. En déduire qu'il existe un sous-groupe distingué H de G tel que S soit isomorphe à G/H.

e) En déduire que si G est simple non cyclique, alors le cardinal de G est divisible par 12 ou son plus petit facteur premier apparaît au moins au cube dans sa décomposition en facteurs premiers.

Solution de l'exercice 14.

a) On rappelle que le groupe $H/D(H)$ est commutatif, donc l'ordre des produits effectués dans ce groupe n'importe pas. Soient $g, g' \in G$. On a par définition

$$V(gg') = \pi\left(\prod_{i=1}^{n} h_{i,(gg')\cdot i}\right),$$

où les $h_{i,(gg')\cdot i} \in H$ sont définis par la formule

$$(gg')x_i = x_{(gg')\cdot i} h_{i,(gg')\cdot i}\,.$$

Or on a

$$(gg')x_i = g(g'x_i) = g(x_{g'\cdot i} h_{i,g'\cdot i}) = x_{g\cdot(g'\cdot i)} h_{g'\cdot i, g\cdot(g'\cdot i)} h_{i,g'\cdot i}\,,$$

donc

$$h_{i,(gg')\cdot i} = h_{g'\cdot i, g\cdot(g'\cdot i)} h_{i,g'\cdot i}\,.$$

Donc, puisque $H/D(H)$ est commutatif, on a

$$V(gg') = \pi\left(\prod_{i=1}^{n} h_{g'\cdot i, g\cdot(g'\cdot i)}\right)\pi\left(\prod_{i=1}^{n} h_{i,g'\cdot i}\right) = V(g)V(g')\,,$$

car l'application de $\{1,\dots,n\}$ dans lui-même donnée par $i \mapsto g'\cdot i$ est une bijection.
En outre, il est clair que $V(1) = 1$, donc cela assure que V est un morphisme de groupes.
Montrons maintenant que V est indépendant du choix des x_i : la commutativité de $H/D(H)$ assure que V reste le même si l'on permute les x_i. Si x_i' est un autre ensemble de représentants de G modulo H (définissant un morphisme $V' : G \to H/D(H)$), alors quitte à permuter les x_i', on peut supposer que x_i' est congru à x_i modulo H, i.e. qu'il existe $k_i \in H$ tel que $x_i' = x_i k_i$. Par conséquent, on voit (avec les notations naturelles) que l'on a

$$h_{i,g\cdot i} = k_{g\cdot i} h'_{i,g\cdot i} k_i^{-1}\,.$$

Donc, en utilisant à nouveau la commutativité de $H/D(H)$, on voit que pour tout $g \in G$,

$$V(g) = \pi\left(\prod_i h_{i,g\cdot i}\right) = \pi\left(\prod_i k_{g\cdot i} h'_{i,g\cdot i} k_i^{-1}\right) = \pi\left(\prod_i h'_{i,g\cdot i}\right) = V'(g)\,,$$

donc $V = V'$, ce qui assure que V ne dépend pas du choix des x_i.

b) Il est clair qu'un ensemble de représentants de G modulo H est donné par

$$g_1, hg_1, \dots, h^{n_1-1}g_1, g_2, hg_2, \dots, h^{n_2-1}g_2, g_3, \dots, g_r, hg_r, \dots h^{n_r-1}g_r\,.$$

Avec ce choix pour les x_i, on voit facilement que l'on a

$$V(h) = \pi\left(\prod_{i=1}^{r} g_i^{-1} h^{n_i} g_i\right)\,.$$

c) On suppose qu'il existe $g \in G$ tel que $B = gAg^{-1}$. Alors les hypothèses assurent que l'on a les inclusions suivantes :

$$S \subset N_G(A) \text{ et } g^{-1}Sg \subset N_G(A)\,.$$

Or S et $g^{-1}Sg$ sont deux p-Sylow du groupe $N_G(A)$, donc ils sont conjugués dans $N_G(A)$: il existe donc $h \in N_G(A)$ tel que

$$g^{-1}Sg = hSh^{-1}\,,$$

donc $gh \in N_G(S)$. Enfin, on a

$$(gh)A(gh)^{-1} = g(hAh^{-1})g^{-1} = gAg^{-1} = B$$

car h normalise A. Cela conclut la preuve.

d) Soit $s \in S$. En conservant les mêmes notations, la question b) assure que

$$V(s) = \pi\left(\prod_{i=1}^{r} g_i^{-1} s^{n_i} g_i\right)\,.$$

On pose alors $A = \{g_i^{-1}s^{n_i}g_i\}$ et $B = \{s^{n_i}\}$. Comme S est commutatif, A et B sont deux parties de S stables par conjugaison dans S, et conjuguées par l'élément g_i de G. Alors la question c) assure qu'il existe $y_i \in N_G(S)$ tel que $g_i^{-1}s^{n_i}g_i = y_i s^{n_i} y_i^{-1}$. Or par hypothèse S est contenu dans le centre de $N_G(S)$, ce qui assure que

$$g_i^{-1}s^{n_i}g_i = y_i s^{n_i} y_i^{-1} = s^{n_i}\,,$$

donc

$$V(s) = \prod_i s^{n_i} = s^{\sum_i n_i} = s^{[G:S]}\,.$$

Enfin, S est un p-Sylow de G, donc $[G : S]$ est premier au cardinal de S (qui est un groupe commutatif), ce qui assure que le morphisme $S \to S$ défini par $s \mapsto s^{[G:S]}$ est un isomorphisme (Lagrange assure que ce morphisme est injectif, donc bijectif. On peut aussi utiliser une relation de Bézout).

On a donc montré que la restriction de V à S était un isomorphisme, ce qui assure que $V : G \to S$ est surjectif. Donc $H = \mathrm{Ker}(V)$ est un sous-groupe distingué de G tel que S soit isomorphe à G/H via V.

e) Soit G un groupe non cyclique. On note p le plus petit facteur premier de $|G|$, et on suppose que p^3 ne divise pas $|G|$. Soit S un p-Sylow de G. Alors S est de cardinal p ou p^2, donc S est commutatif et comme plus haut, l'action par conjugaison induit un morphisme de groupes

$$\overline{\phi} : N_G(S)/S \to \mathrm{Aut}(S)\,,$$

dont la trivialité équivaut au fait que $S \subset Z(N_G(S))$.

Or tous les facteurs premiers du cardinal de $N_G(S)/S$ sont $> p$, alors que $\mathrm{Aut}(S)$ est l'un des trois groupes suivants : $\mathbb{Z}/p-1\mathbb{Z}$ (si S est d'ordre p), $\mathbb{Z}/p(p-1)\mathbb{Z}$ (si S est cyclique d'ordre p^2), $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ (si S est non cyclique d'ordre p^2). Les cardinaux de ces trois groupes sont respectivement $p-1$, $p(p-1)$ et $(p^2-1)(p^2-p) = (p-1)^2p(p+1)$. Par conséquent, dans les trois cas, les facteurs premiers du cardinal de $\mathrm{Aut}(S)$ sont tous $\leq p+1$. On a donc deux cas :

– si $p > 2$, alors $p+1$ n'est pas premier, donc le morphisme $\overline{\phi}$ est trivial dans tous les cas.
– si $p = 2$, alors $p+1 = 3$ est premier, et le morphisme $\overline{\phi}$ trivial, sauf éventuellement si $p^2 = 4$ et $p+1 = 3$ divisent le cardinal de G.

Finalement, on a $S \subset Z(N_G(S))$ dans tous les cas, sauf si $p = 2$ et $|G|$ est multiple de 12. Donc la question d) assure que G admet un sous-groupe distingué d'indice $|S|$, sauf si 12 divise $|G|$.

On en déduit immédiatemment que G n'est pas simple, sauf si éventuellement 12 divise $|G|$.

Cela conclut la preuve.

Exercice 15 : $\star\star\star$

a) Montrer qu'un groupe d'ordre $60 < n < 168$ avec n non premier n'est jamais simple.

b) Montrer que $\mathrm{SL}_3(\mathbb{F}_2)$ et $\mathrm{PSL}_2(\mathbb{F}_7)$ sont d'ordre 168.

c) Montrer que $\mathrm{SL}_3(\mathbb{F}_2)$ est simple.

d) Soit G simple d'ordre 168. Montrer que G est isomorphe à $\mathrm{PSL}_2(\mathbb{F}_7)$.

e) Montrer que l'on a un isomorphisme entre $\mathrm{SL}_3(\mathbb{F}_2)$ et $\mathrm{PSL}_2(\mathbb{F}_7)$.

Solution de l'exercice 15.

a) On fait les listes des entiers entre 61 et 167, et on utilise les exercices 8, 11 et 14 pour voir que les seuls cardinaux possibles pour un groupe simple dans cet intervalle sont

$$72 = 2^3.3^2, 80 = 2^4.5, 88 = 2^3.11, 96 = 2^5.3, 104 = 2^3.13, 112 = 2^4.7, 120 = 2^3.3.5, 135 = 3^3.5,$$
$$136 = 2^3.17, 144 = 2^4.3^2, 152 = 2^3.19, 156 = 2^2.3.13, 160 = 2^5.5\,.$$

Puis on étudie séparément les cas restants en utilisant les théorèmes de Sylow.

b) Le calcul du cardinal de $\mathrm{GL}_n(\mathbb{F})$, où $\mathbb{F}$ est un corps fini de cardinal q, est classique. On trouve $|\mathrm{GL}_n(\mathbb{F})| = (q^n-1)(q^n-q)\dots(q^n-q^{n-1})$. Donc ici, comme $\mathrm{SL}_3(\mathbb{F}_2) = \mathrm{GL}_3(\mathbb{F}_2)$, on obtient $|\mathrm{SL}_3(\mathbb{F}_2)| = 7.6.4 = 168$.

c) Les éléments de $\mathrm{SL}_2(\mathbb{F}_3)$ ont un polynôme minimal dans la liste suivante : $X+1$, X^2+1, X^2+X+1, X^3+1, X^3+X+1, X^3+X^2+1, X^3+X^2+X+1. Montrons que le polynôme minimal d'une matrice de $\mathrm{SL}_3(\mathbb{F}_2)$ caractérise sa classe de conjugaison, que presque tous ces polynômes apparaissent effectivement et comptons au passage le nombre d'éléments dans chaque classe de conjugaison et l'ordre de ces éléments.

– La seule matrice de polynôme minimal $X+1$ est la matrice I_3.

– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. Le polynôme minimal de A est $X^2+1=(X+1)^2$ si et seulement si $A \neq I_3$ et $\mathrm{Im}\,(A-I_3) \subset \mathrm{Ker}(A-I_3)$, si et seulement si $\mathrm{Ker}(A-I_3)$ est un plan contenant la droite $\mathrm{Im}\,(A-I_3)$. Donc se donner une telle matrice équivaut à se donner un plan P et une droite $D \subset P$ dans $\mathbb{F}_2^3$, et il y a exactement 7 choix pour P et 3 pour $D \subset P$, donc 21 matrices de polynôme minimal X^2+1. Ces matrices sont clairement d'ordre 2 et deux-à-deux conjuguées).
– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. Si le polynôme minimal de A est X^2+X+1, son polynôme caractéristique est nécessairement X^3+1 (car A est inversible), donc 1 est valeur propre de A, mais 1 n'est pas racine de X^2+X+1, ce qui est contradictoire. Donc le polynôme X^2+X+1 n'apparaît pas comme polynôme minimal d'une matrice de $\mathrm{SL}_3(\mathbb{F}_2)$.
– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. On voit que le polynôme minimal de A est $X^3+1=(X+1)(X^2+X+1)$ si et seulement si $\mathbb{F}_2^3$ est somme directe de la droite $\mathrm{Ker}(A+1)$ et du plan $\mathrm{Ker}(A^2+A+1)$. Une telle matrice est complétement caractérisée par la donnée d'une droite et d'un plan supplémentaire, ainsi que celle d'un vecteur quelconque du plan dont l'image par A n'est pas colinéaire à lui-même. Il y a donc exactement $7.4.2 = 56$ telles matrices, qui sont toutes d'ordre 3, et bien deux-à-deux conjuguées.
– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. Le polynôme minimal de A est irréductible de degré 3 si et seulement si pour tout vecteur non nul x, (x, Ax, A^2x) est une base de $\mathbb{F}_2^3$. Comme X^3+X+1 et X^3+X^2+1 sont les seuls polynômes irréductibles de degré 3, on en déduit facilement qu'il y a exactement $6.4 = 24$ matrices de polynôme minimal X^3+X+1 et 24 matrices de polynôme minimal X^3+X^2+1. Toutes ces matrices sont clairement d'ordre 7 et deux telles matrices de même polynôme minimal sont bien conjuguées. Notons enfin que si A a pour polynôme minimal X^3+X+1, alors A^{-1} a pour polynôme minimal X^3+X^2+1 (et vice-versa).
– Soit $A \in \mathrm{SL}_3(\mathbb{F}_2)$. Le polynôme minimal de A est $X^3+X^2+X+1=(X+1)^3$ si et seulement si $\mathrm{Ker}(A+I_3)$ est une droite contenue dans le plan $\mathrm{Ker}((A+I_3)^2)$ et pour tout vecteur hors de ce plan, son image est dans le plan mais pas dans la droite. On voit donc qu'il y a exactement $7.3.2 = 42$ telles matrices, que leur ordre est 4 et qu'elles sont bien toutes conjuguées.

Finalement, on vérifie que l'on a bien $1+21+56+24+24+42=168$. On a donc ainsi décrit les 6 classes de conjugaison dans $\mathrm{SL}_3(\mathbb{F}_2)$.

Soit maintenant $H \lhd \mathrm{SL}_3(\mathbb{F}_2)$ un sous-groupe distingué $\neq \{I_3\}$. Supposons que H ne contienne aucun élément d'ordre 3 ou 7. Alors le cardinal de H est un diviseur de 8, donc H contient un élément d'ordre 2, donc H contient les 21 éléments d'ordre 2 (on a vu qu'ils étaient tous conjugués), donc H contient au moins 22 éléments, ce qui est contradictoire. Donc H contient soit un élément d'ordre 3 soit un d'ordre 7. Dans le premier cas, H contient 56 éléments d'ordre 7, donc $|H| \geq 57$, donc $|H| = 84$ ou 168, donc H contient un élément d'ordre 2 et un élément d'ordre 7, donc au moins 21 éléments d'ordre 2 et 24 d'ordre 7, donc $|H| \geq 57+21+24 = 102$, donc $|H| = 168$. Dans le second cas, H contient au moins 24 éléments d'ordre 7, et en fait H contient tous les 48 éléments d'ordre 7, car les deux classes de conjugaison sont échangées par l'inversion. Donc $|H| \geq 49$, donc $|H| = 56$, 84 ou 168. Donc H a un élément d'ordre 7 et on conclut par le premier cas que $|H| = 168$.

Finalement, on a $H = \mathrm{SL}_3(\mathbb{F}_2)$, ce qui assure la simplicité de $\mathrm{SL}_3(\mathbb{F}_2)$.

d) Les théorèmes de Sylow assurent que G admet exactement huit 7-Sylow. Si on note X l'ensemble des 7-Sylow de G, l'action transitive par conjugaison de G sur X induit un morphisme de groupes injectif

$$\varphi : G \hookrightarrow \mathfrak{S}(X) \cong \mathfrak{S}_8 .$$

Or les éléments de $\mathfrak{S}_8$ sont d'ordre 1, 2, 3, 4, 5, 6, 7, 8, 10, 12 et 15. Or G n'admet aucun élément d'ordre 15, donc tous les éléments de G sont d'ordre ≤ 12.

En outre, on voit que pour tout 7-Sylow S de G, $|N_G(S)| = \frac{|G|}{|X|} = 21$. Donc en particulier, le groupe $N_G(S)$ n'est pas cyclique.

Montrons que $N_G(S)$ agit transitivement sur $X' := X \setminus \{S\}$. Comme $N_G(S)$ agit trivialement sur S, on voit que la restriction de φ à S induit un morphisme

$$\widetilde{\varphi} : S \to \mathfrak{S}(X') \cong \mathfrak{S}_7 .$$

Si $T \in X'$, alors S n'est pas contenu dans $N_G(T)$ (sinon on aurait $S = T$), donc $S \cap N_G(T) = \{e\}$ et pour tous $g, g' \in S$, on a $gTg^{-1} = g'Tg'^{-1}$ si et seulement si $g = g'$. Par conséquent, l'orbite

de T sous l'action de S dans X' est de cardinal $|S| = 7 = |X'|$, donc S agit transitivement sur X'.

Soit $T \in X'$. On a vu que le groupe $N_G(S)$ de cardinal 21 agissait transitivement sur l'ensemble X' de cardinal 7, et le stabilisateur de T pour cette action n'est autre que $N_G(S) \cap N_G(T)$. Donc en calculant les cardainaux, on voit que $|N_G(S) \cap N_G(T)| = 3$.

On a $n_3 \neq 1$, congru à 1 modulo 3 et diviseur de 56, donc $n_3 \in \{4, 7, 28\}$. Le cas $n_3 = 4$ est impossible par 168 ne divise pas $4! = 24$. Supposons que $n_3 = 7$. Le sous-groupe $N_G(S)$ est d'ordre 21, il contient donc un ou sept 3-Sylow. Comme $N_G(S)$ n'est pas cyclique et d'ordre 21, on voit que cela implique que $N_G(S)$ possède exactement sept 3-Sylow, donc que $N_G(S)$ contient tous les 3-Sylow de G. Ceci étant valable pour tout 7-Sylow S, on aurait donc pour $T \neq S$ dans X, $|N_G(S) \cap N_G(T)| \geq 7.2 + 1 = 15$, ce qui contredit un calcul précédent. Donc finalement $n_3 = 28$.

On pose $H := N_G(N_G(S) \cap N_G(T))$. Comme $N_G(S) \cap N_G(T)$ est un 3-Sylow de G, H est de cardinal $\frac{168}{28} = 6$. Si H est cyclique, alors G contient au moins un élément x d'ordre 6. Alors $\langle x^2 \rangle$ est un 3-Sylow de G, et comme les 3-Sylow de G sont conjugués, on voit que tout 3-Sylow est engendré par le carré d'un élément d'ordre 6. Donc G contient au moins $2.28 = 56$ éléments d'ordre 6. Le groupe G contiendrait donc finalement $28.2 = 56$ éléments d'ordre 3, au moins 56 éléments d'ordre 6 et $8.6 = 48$ éléments d'ordre 7. Or $56 + 56 + 48 = 160$, et G possède en outre également au moins deux 2-Sylow, donc au moins 9 éléments d'ordre divisant 8, on trouve que G contiendrait au moins 169 éléments, ce qui est contradictoire. Donc H n'est pas cyclique, donc $H \cong \mathfrak{S}_3$.

Fixons maintenant un générateur s du 7-Sylow S. Alors l'application

$$\tau : \{0, \ldots, 6\} \to X'$$

définie par $\tau(k) := s^k T s^{-k}$ est bijective (car S agit transitivement sur X'). En posant $\tau(\infty) := S$, on obtient ainsi une bijection

$$\tau : \mathbb{P}^1(\mathbb{F}_7) = \mathbb{F}_7 \cup \{\infty\} \xrightarrow{\simeq} X\,.$$

On vérifie qu'avec ces identifications, l'action de s sur $X \cong \mathbb{P}^1(\mathbb{F}_7)$ définie par la formule suivante

$$\forall x \in \mathbb{P}^1(\mathbb{F}_7)\,,\ s \cdot x = x + 1$$

avec la convention naturelle que $\infty + 1 = \infty$. Autrement dit, l'action de s sur X est donnée par l'homographie de $\mathbb{P}^1(\mathbb{F}_7)$ définie par la matrice

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{F}_7)\,.$$

Choisissons $t \in N_G(S) \cap N_G(T)$ non trivial (donc d'ordre 3). Le morphisme $c : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(S) \cong \mathbb{Z}/6/Z$ donné par la conjugaison par les puissances de t est non trivial (sinon $N_G(S)$ serait cyclique engendré par st), il est donc égal à $k \mapsto 2k$ ou $k \mapsto 4k$, ce qui signifie que tst^{-1} est égal à s^2 ou s^4. Alors quitte à remplacer t par $t^2 = t^{-1}$, on peut supposer que $tst^{-1} = s^2$. Alors on voit facilement que l'action de t sur X correspond à la bijection de $\mathbb{P}^1(\mathbb{F}_7)$ donnée par la formule

$$\forall x \in \mathbb{P}^1(\mathbb{F}_7)\,,\ t \cdot x = 2.x$$

avec la convention naturelle que $2.\infty = \infty$. Autrement dit, l'action de t sur X est donnée par l'homographie de $\mathbb{P}^1(\mathbb{F}_7)$ définie par la matrice

$$\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{F}_7)\,.$$

Soient maintenant $u \in H \setminus (N_G(S) \cap N_G(T))$. Comme $H \cong \mathfrak{S}_3$, on voit que u correspond à une transposition, alors que t correspond à un 3-cycle. il est donc clair que $utu^{-1} = t^{-1}$. On en déduit

que pour tout $x \in \mathbb{P}^1(\mathbb{F}_7)$, on a $u \cdot (2.x) = 4.u \cdot x$. Montrons que $G = \langle s, t, u \rangle$. Il est clair que le groupe de droite est de cardinal > 21 et divisible par 21, donc son cardinal vaut 42, 84 ou 168. S'il vaut 84, c'est un sous-groupe d'indice 2 de G, il est distingué, ce qui contredit la simplicité de G. S'il vaut 42, c'est un sous-groupe d'indice 4, ce qui permet de construire un morphisme non trivial, donc injectif $G \to \mathfrak{S}(G/\langle s, t, u, \rangle \cong \mathfrak{S}_4$, ce qui est impossible par cardinalité. Donc on a bien $G = \langle s, t, u \rangle$. Comme G agit transitivement sur X, on voit que nécessairement $u(0) = \infty$ et $u(\infty) = 0$ (on rappelle que s et t fixent 0 et ∞). Supposons maintenant que $u(1) \in \{1, 2, 4\}$. Alors la relation $u \cdot (2.x) = 4.u \cdot x$ assure que vu comme permutation d'ordre 2 de $\mathbb{P}^1(\mathbb{F}_7)$, u a au moins deux points fixes, donc u est dans le normalisateur d'un 7-Sylow de G, ce qui est exclu puisque u est d'ordre 2 et ce normalisateur est d'ordre 21. Donc $u(1) \in \{3, 5, 6\}$. Alors la formule $u \cdot (2.x) = 4.u \cdot x$ assure que si l'on note $a := u(1) \in \{3, 5, 6\}$, l'action de u sur X correspond à la bijection de $\mathbb{P}^1(\mathbb{F}_7)$ donnée par la formule

$$\forall x \in \mathbb{P}^1(\mathbb{F}_7)\,,\ u \cdot x = \frac{a}{x}$$

avec les conventions naturelles. Autrement dit, l'action de t sur X est donnée par l'homographie de $\mathbb{P}^1(\mathbb{F}_7)$ définie par la matrice

$$\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_7)\,.$$

Or $a \in \{3, 5, 6\}$, donc $\frac{-1}{a} \in \{1, 2, 4\}$ est un carré dans $\mathbb{F}_7$, donc il existe $c \in \mathbb{F}_7^*$ tel que $\frac{-1}{a} = c^2$, et alors on voit que l'action de t sur X est donnée par l'homographie définie par la matrice

$$\begin{pmatrix} 0 & ac \\ c & 0 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{F}_7)\,.$$

Finalement, comme $G = \langle s, t, u \rangle$, on voit que $\varphi(G) \subset \mathfrak{S}_8$ est contenu dans le sous-groupe $\mathrm{PSL}_2(\mathbb{F}_7)$ de $\mathfrak{S}_8$ (en identifiant X et $\mathbb{P}^1(\mathbb{F}_7)$ via l'application τ). Or ces deux groupes ont pour cardinal 168, donc φ induit un isomorphisme entre G et $\mathrm{PSL}_2(\mathbb{F}_7)$.

e) Les questions c) et d) assurent le résultat. Le lecteur curieux pourra chercher à construire un isomorphisme explcite entre ces deux groupes.

TD3 : Groupes abéliens de type fini

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Montrer que les groupes $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ sont isomorphes.

Solution de l'exercice 1. On utilise le lemme chinois pour voir que les deux groupes sont isomorphes au groupe

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z} \times /Z/9\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z})\,.$$

Cette écriture est la décomposition en composantes p-primaire. On peut aussi écrire la décomposition en facteurs invariants de ces deux groupes, et l'on trouve :

$$\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/900\mathbb{Z}\,.$$

Exercice 2 : ⋆
Montrer qu'un groupe abélien fini non cyclique possède un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ pour un certain nombre premier p.

Solution de l'exercice 2. Le théorème du cours assure qu'un tel groupe G est isomorphe à un produit $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$, avec $d_i \geq 2$ et $d_i | d_{i+1}$. Comme G n'est pas cyclique, on a $r \geq 2$. Il existe un facteur premier p de d_1, alors p divise tous les d_i, et $\mathbb{Z}/p\mathbb{Z}$ est isomorphe à un sous-groupe de chacun des $\mathbb{Z}/d_i\mathbb{Z}$ (c'est le sous-groupe de p-torsion). Alors le sous-groupe de p-torsion de G est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^r$, qui contient clairement un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 3 : ⋆

a) Combien y a-t-il de groupes abéliens de cardinal 360 ? Faire la liste complète de ces groupes.
b) Plus généralement, pour tout entier n, combien y a-t-il de groupes abéliens de cardinal n ?

Solution de l'exercice 3.

a) On écrit la décomposition en facteurs premiers de $360 = 2^3.3^2.5$. Alors si G est un groupe de cardinal 360, $T_2(G)$ est un groupe abélien de cardinal 2^3, il y a donc 3 classes d'isomorphisme de tels groupes, à savoir $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$. De même, il y a exactement deux classes d'isomorphisme possibles pour $T_3(G)$, à savoir $\mathbb{Z}/9\mathbb{Z}$ et $(\mathbb{Z}/3\mathbb{Z})^2$, et $T_5(G)$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Par conséquent, il y a exactement $3.2 = 6$ classes d'isomorphisme de groupes abéliens d'ordre 360, dont les décompositions p-primaires et en facteurs invariants sont les suivantes :

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/360\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$$

$$\mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}$$

$$(\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}\,.$$

b) On utilise la classification des classes d'isomorphisme de groupes abéliens finis. Notons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. Alors on sait que la classe d'isomorphisme d'un groupe abélien d'ordre n est caractérisée par ses facteurs invariants $(d_1, \dots, d_s)$ qui sont des entiers > 1 tels que $d_i | d_{i+1}$ et $d_1 \dots d_s = n$. Par conséquent, chaque d_i se décompose $d_i = p_1^{\alpha_{i,1}} \dots p_1^{\alpha_{i,r}}$, avec les contraintes suivantes : pour tout j, $\alpha_{i,j} \leq \alpha_{i+1,j}$ (pour tout i) et $\sum_{i=1}^{s} \alpha_{i,j} = \alpha_j$.
Par conséquent, le nombre de choix possibles pour les a_i est exactement $\prod_{j=1}^{r} p(\alpha_j)$, où $p(\alpha)$ désigne le nombre de partitions de α, i.e. le nombre de façons d'écrire l'entier α comme une somme croissante d'entiers strictement positifs.

Exercice 4 :

a) Le nombre de classes de conjugaison dans $\mathfrak{S}_5$ est le même que le nombre de groupes abéliens de cardinal 32 à isomorphisme près. Pourquoi ?

b) Généraliser au nombre de classes de conjugaison dans $\mathfrak{S}_n$.

Solution de l'exercice 4.

a) Les deux ensembles en question sont naturellement en bijection avec l'ensemble des partitions de 5.

b) Soit p un nombre premier. Notons G_n l'ensemble des classes d'isomorphisme de groupes abéliens de cardinal p^n, P_n l'ensemble des partitions de l'entier n et C_n l'ensemble des classes de conjugaison dans $\mathfrak{S}_n$. On dispose des applications suivantes

$$\varphi : P_n \to G_n$$

et

$$\psi : P_n \to C_n$$

où pour toute partition $(n_1, \dots, n_r)$ de n, $\varphi((n_1, \dots, n_r))$ est la classe d'isomorphisme de $\prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$ et $\psi((n_1, \dots, n_r))$ est la classe de conjugaison de la permutation $(1, 2, \dots, n_1)(n_1 + 1, \dots, n_1 + n_2) \dots (n_1 + \dots + n_{r-1} + 1, \dots, n)$. On voit alors facilement que φ et ψ sont des bijections, donc $|C_n| = |G_n|$, i.e. il y a autant de classes de conjugaison dans $\mathfrak{S}_n$ que de classes d'isomorphisme de groupes abéliens d'ordre p^n.

Exercice 5 : $\star$
Soit G un groupe abélien fini. Montrer qu'il existe dans G un élément d'ordre égal à l'*exposant de G* (c'est-à-dire au ppcm des ordres des éléments de G).

Solution de l'exercice 5.

— On commence par une preuve "élémentaire" : montrons d'abord que pour tous $x, y \in G$ d'ordres respectifs m et n premiers entre eux, le produit xy est d'ordre $m.n$. Il est clair que $(xy)^{mn} = 1$ donc l'ordre de xy divise mn. Soit maintenant $k \geq 1$ tel que $(xy)^k = 1$. En élevant à la puissance n, on obtient $x^{kn} = 1$, donc m divise kn. Or m et n sont premiers entre eux, donc m divise k. Par symétrie, on a aussi que n divise k, donc mn divise k, donc xy est d'ordre mn.
On décompose l'exposant de G en facteurs premiers : $\exp(G) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, avec les p_i premiers distincts. Par définition de l'exposant de G, pour tout $1 \leq i \leq r$, il existe $g_i \in G$ dont l'ordre est divisible par $p_i^{\alpha_i}$, disons égal à $p_i^{\alpha_i}.m_i$. Alors $g_i^{m_i}$ est d'ordre $p_i^{\alpha_i}$, et on a vu qu'alors l'élément $g := g_1^{m_1} \dots g_r^{m_r} \in G$ est d'ordre exactement $p_1^{\alpha_1} \dots p_r^{\alpha_r} = \exp(G)$.
— Une preuve moins élémentaire : le théorème de classification des groupes abéliens finis assure qu'il existe des entiers $2 \leq d_1 | \dots | d_s$ tels que G soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$. Il est alors clair que $\exp(G) = d_r$ et que l'élément $(0, \dots, 0, 1) \in \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$ est d'ordre d_r.

Exercice 6 : $\star$
Soit G un groupe et soient H et K des sous-groupes de G. On suppose que :

a) $H \triangleleft G$ et $K \triangleleft G$;

b) $HK = G$;

c) $H \cap K = e$.

Montrer que G est isomorphe à $H \times K$.

Solution de l'exercice 6. Montrons d'abord que H et K commutent. Soient $h \in H$ et $k \in K$. Comme H est distingué dans G, on a $kh^{-1}k^{-1} \in H$, donc $hkh^{-1}k^{-1} \in H$. De même, K est distingué dans G, donc $hkh^{-1} \in K$, donc $hkh^{-1}k^{-1} \in K$. Donc $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, donc $hk = kh$.
Montrons maintenant que pour tout $g \in G$, il existe un unique couple $(h, k) \in H \times K$ tel que $g = hk$. L'existence est assurée par l'hypothèse b). Pour l'unicité, soient $h, h' \in H$ et $k, k' \in K$ tels que $hk = h'k'$. Alors $kk'^{-1} = h^{-1}h'$ est dans $H \cap K$, donc l'hypothèse c) assure que $kk'^{-1} = h^{-1}h' = e$, donc $h = h'$ et $k = k'$, d'où l'unicité.
On considère alors l'application $\varphi : H \times K \to G$ définie par $\varphi(h, k) := hk$. Le fait que H et K commutent assure que φ est un morphisme de groupes. L'existence et l'unicité prouvée plus haut assurent que φ est une bijection. Donc G est bien isomorphe au groupe $H \times K$.

Exercice 7 : ⋆⋆
Soit K un corps et soit $G \subset K^*$ un sous-groupe fini d'ordre n. On va montrer que G est un groupe cyclique.

a) Montrer que l'ordre de tout élément de G divise n.

b) Soit d un diviseur de n et $x \in G$ d'ordre d. Soit H le sous-groupe cyclique de G engendré par x. Montrer que tout élément d'ordre d est dans H.

c) On note $N(d)$ le nombre d'éléments de G d'ordre d. Montrer que $N(d) = 0$ ou $\varphi(d)$, et que $\sum_{d|n,\ d>0} N(d) = n$.

d) Conclure.

En particulier, si p est un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, et si K est un corps fini, K^* est un groupe cyclique.

Solution de l'exercice 7.

a) C'est le théorème de Lagrange.

b) Considérons le polynôme $P = X^d - 1 \in K[X]$. Comme K est un corps, le polynôme P a au plus d racines dans K. Or tout élément du groupe H est d'ordre divisant d, donc tous les éléments de H sont des racines de P. Or le cardinal de H est égal à l'ordre de x, c'est-à-dire à d. Donc H contient toutes les racines de P dans K.

Soit maintenant $y \in G$ d'ordre d. Alors y est racine de P, donc y est dans H.

c) Supposons $N(d) \neq 0$. Alors il existe $x \in G$ d'ordre d. La question b) assure que tout les éléments d'ordre d dans G sont exactement les éléments d'ordre d dans $\langle x \rangle$ qui est un groupe cyclique d'ordre d. Or un groupe cyclique d'ordre d a exactement $\varphi(d)$ éléments d'ordre d, donc $N(d) = \varphi(d)$.

En outre, on peut partitionner G selon l'ordre des éléments, i.e. G est la réunion disjointe, pour d divisant n (par la question a)), des ensembles G_d formés des éléments d'ordre d. En calculant les cardinaux, on trouve donc $|G| = \sum_{d|n} |G_g|$, i.e. $n = \sum_{d|n} N(d)$.

d) La question c) assure que $n = \sum_{d|n} N(d)$. Or on sait que $n = \sum_{d|n} \varphi(d)$. Donc $\sum_{d|n} N(d) = \sum_{d|n} \varphi(d)$. Or pour tout $d|n$, $N(d) \leq \varphi(d)$, donc on a bien pour tout $d|n$, $N(d) = \varphi(d)$. En particulier, $N(n) = \varphi(n) > 0$, donc il existe un élément d'ordre n dans G, i.e. G est cyclique.

Exercice 8 : ⋆⋆
Si A est un anneau, on note $A^\times$ le groupe (multiplicatif) des éléments inversibles de A.

a) Soit G un groupe monogène. Montrer que le groupe des automorphismes de G est en bijection avec l'ensemble des générateurs de G.

b) Montrer que pour tout $n \in \mathbb{N}$, on a un isomorphisme de groupes $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

c) Soit p un nombre premier impair et soit $\alpha \geq 1$. Quel est l'ordre de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$? En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

d) Expliciter $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ pour $\alpha \geq 1$.

e) En déduire $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n \in \mathbb{N}$.

Solution de l'exercice 8.

a) Soit G_0 l'ensemble des générateurs de G et soit g_0 un élément de G_0. Alors si φ est un automorphisme de G, l'image de φ est engendrée par $\varphi(g_0)$; ce qui veut dire que $\varphi(g_0)$ est un générateur de G. On définit alors une application (ensembliste) $\begin{array}{ccc} \operatorname{Aut} G & \to & G_0 \\ \varphi & \mapsto & \varphi(g_0) \end{array}$. Comme g_0 est générateur, l'application est bijective.

b) Dans $\mathbb{Z}$, montrons par récurrence sur $k \geq 1$ qu'il existe λ_k premier à p vérifiant $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$. L'étape d'initialisation pour $k=1$ est claire via la formule du binôme, puisque p divise $\binom{p}{2}$. Montrons l'hérédité : soit $k \geq 1$, on a $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$ par hypothèse de récurrence, donc on obtient $(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda_k + \sum_{i=2}^{p} \binom{p}{i} \lambda_k^i p^{(i-1)(k+1)-1})$ et le résultat est montré par récurrence.

En particulier, $1+p$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

En utilisant l'exercice 7, on sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, d'ordre $p-1$. Notons x_0 un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ et prenons un relèvement x_1 de x_0 dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. L'ordre de x_1 est le la forme $(p-1)p^s$ pour un certain $s \leq \alpha$, de sorte que $x := x_1^{p^s}$ est d'ordre $p-1$. Comme x et $1+p$ ont des ordres premiers entre eux et comme le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est abélien, on a vu que $x(1+p)$ est donc d'ordre $p^{\alpha-1}(p-1) = \varphi(p)$ et $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est donc cyclique.

c) Remarquons d'abord que $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ et $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$. Supposons maintenant $\alpha \geq 2$. Par une récurrence semblable à celle effectuée au b), on montre que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. Observons maintenant le morphisme surjectif $\pi : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$: son noyau est exactement $\langle 5 \rangle$, et $\pi(-1) = -1$. Par conséquent, les sous-groupes $\langle 5 \rangle$ et $\langle -1 \rangle$ vérifient les hypothèses de l'exercice 6, donc $\langle 5 \rangle \times \langle -1 \rangle \cong (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. On obtient donc finalement $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

d) Si $n = \prod_p p^{\alpha_p}$ est la décomposition en facteurs premiers de n, alors le lemme chinois nous donne

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/2^{\alpha_2}\mathbb{Z})^\times \times \prod_{p \neq 2,\, \alpha_p \geq 1} \big(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{\alpha_p - 1}\mathbb{Z}\big).$$

Exercice 9 :
Déterminer les entiers $n \in \mathbb{Z}$ pour lesquels $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

Solution de l'exercice 9. Si $n = \prod_p p^{\alpha_p}$ est la décomposition en facteurs premiers de n, la question d) de l'exercice 8 assure que

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/2^{\alpha_2}\mathbb{Z})^\times \times \prod_{p \neq 2,\, \alpha_p \geq 1} \big(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{\alpha_p - 1}\mathbb{Z}\big).$$

En remarquant qu'un groupe cyclique ne peut pas contenir plus d'un élément d'ordre 2, on conclut que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = p^\alpha$ ou $2p^\alpha$ avec p un nombre premier impair et $\alpha \geq 0$ ou $n = 4$.

Exercice 10 : $\star\star$
Décomposer le groupe $G = (\mathbb{Z}/187\mathbb{Z})^\times$ sous la forme donnée par le théorème de structure des groupes abéliens de type fini.

Solution de l'exercice 10. Comme $187 = 11.17$, l'exercice 8 assure que

$$G \cong (\mathbb{Z}/11\mathbb{Z})^\times \times (\mathbb{Z}/17\mathbb{Z})^\times \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/80\mathbb{Z}\,.$$

Les facteurs invariants de G sont donc 2 et 80.

Exercice 11 : $\star\star$

a) On considère $H := \{(a,b) \in \mathbb{Z}^2 : a-b \text{ est divisible par } 10\}$. Montrer que H est un sous-groupe de $\mathbb{Z}^2$, calculer son rang, en donner une base et décrire le quotient $\mathbb{Z}^2/H$.

b) On note H le sous-groupe de $\mathbb{Z}^2$ engendré par $(2,5)$, $(5,-1)$ et $(1,-2)$. Déterminer une base de H et décrire le quotient $\mathbb{Z}^2/H$.

c) On note H le quotient de $\mathbb{Z}^3$ par le sous-groupe engendré par les vecteurs $(4,8,10)$ et $(6,2,0)$. Déterminer la structure du groupe H.

Solution de l'exercice 11.

a) Il est clair que H est un sous-groupe de $\mathbb{Z}^2$. Soit $(a,b) \in \mathbb{Z}^2$. Alors $(a,b) \in H$ si et seulement s'il existe $k \in \mathbb{Z}$ tel que $b = a + 10k$. Cela assure que $H = \{(a, a+10k) : (a,k) \in \mathbb{Z}^2\} = \mathbb{Z}(1,1) \oplus \mathbb{Z}(0,10)$, donc que H est de rang 2, de base $(1,1)$ et $(0,10)$. Alors $(1,1)$ et $(0,1)$ forment une base de $\mathbb{Z}^2$ adaptée à l'inclusion $H \subset \mathbb{Z}^2$, ce qui assure que $\mathbb{Z}^2/H \cong \mathbb{Z}/10\mathbb{Z}$.

b) On applique l'algorithme de réduction des matrices à coefficients entiers pour montrer que des opérations élémentaires sur les colonnes de la matrice obtenue en inscrivant les trois vecteurs donnés en colonne, à savoir

$$\begin{pmatrix} 2 & 5 & 1 \\ 5 & -1 & -2 \end{pmatrix},$$

aboutissent à la matrice

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 9 & -2 \end{pmatrix}.$$

Cela assure que $(1,-2)$ et $(0,9)$ forment une base de H. Donc H est de rang 2, et $((1,-2);(0,1))$ est une base adaptée à l'inclusion $H \subset \mathbb{Z}^2$, ce qui assure que $\mathbb{Z}^2/H \cong \mathbb{Z}/9\mathbb{Z}$.

c) En réduisant la matrice correspondante, on voit qu'une base du sous-groupe $\mathbb{Z}(4,8,10) + \mathbb{Z}(6,2,0)$ est donnée par $(-20,0,10)$ et $(6,2,0)$. Cela assure qu'une base adaptée à l'inclusion de ce groupe dans $\mathbb{Z}^3$ est donnée par les trois vecteurs $(-2,0,1)$, $(3,1,0)$ et $(1,0,0)$. Donc le quotient H est isomorphe à $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Exercice 12 :
Soit $n \geq 1$. Constuire dans $\mathbb{R}$ un sous-groupe isomorphe à $\mathbb{Z}^n$.

Solution de l'exercice 12. Soient $p_1, \ldots, p_n$ des nombres premiers distincts. Considrons le sous-groupe additif de $\mathbb{R}$ engendr par $\log(p_1), \ldots, \log(p_n)$. Si $a_1, \ldots, a_n \in \mathbb{Z}$ sont tels que $a_1 \log(p_1) + \cdots + a_n \log(p_n) = 0$, alors en prenant l'exponentielle on trouve $p_1^{a_1} \ldots p_n^{a_n} = 1$ donc $a_1 = \cdots = a_n = 0$. Donc ce sous-groupe est isomorphe à $\mathbb{Z}^n$.
Autre exemple : le groupe engendré par $2^{(2^{-i})}$, $1 \leq i \leq n$ convient aussi.
Autre exemple : le groupe engendré par les racines carrées des n premiers entiers positifs sans facteurs carrés $1, \sqrt{2}, \ldots, \sqrt{m}$ convient aussi.
Encore un autre exemple : si $\theta \in \mathbb{R}$ est un nombre transcendant (il en existe, par cardinalité), alors le sous-groupe engendré par $1, \theta, \ldots, \theta^{n-1}$ convient également (pour un exemple explicite, on pourra prendre $\theta = \pi$, mais la preuve de la transcendance est difficile, ou plus directement un nombre de Liouville comme $\theta = \sum_{k=0}^{+\infty} 10^{-k!}$).

Exercice 13 :
Soit $n \geq 1$ est un entier. Montrer que tout système libre maximal dans $\mathbb{Z}^n$ est de cardinal n.
Donner un exemple où un tel système n'est pas une base.

Solution de l'exercice 13. On peut voir $G = \mathbb{Z}^n$ comme un sous-groupe de $\mathbb{Q}^n$. Soit $e_1, \ldots, e_r$ un système libre maximal de G.

— Supposons $r > n$. Alors $e_1, \ldots, e_r$ n'est pas libre sur $\mathbb{Q}$ donc il existe $q_1, \ldots, q_r \in \mathbb{Q}$ tels que $q_1 e_1 + \cdots + q_r e_r = 0$. Quitte à multiplier par le PPCM des dénominateurs des $q_1, \ldots, q_r$, on peut supposer que $q_1, \ldots, q_r \in \mathbb{Z}$. Donc $e_1, \ldots, e_r$ n'est pas libre sur $\mathbb{Z}$.

— Supposons $r < n$. On vient de voir que $e_1, \dots, e_r$ est libre sur $\mathbb{Z}$ si et seulement si $e_1, \dots, e_r$ est libre sur $\mathbb{Q}$. Or si $r < n$, alors $e_1, \dots, e_r$ n'est pas une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^n$, donc il existe $e_{r+1} \in G$ tel que $e_1, \dots, e_r, e_{r+1}$ soit libre sur $\mathbb{Q}$ donc sur $\mathbb{Z}$, et alors $e_1, \dots, e_r$ n'est pas maximal.

Enfin, le système $(2, 0, \dots, 0)$, $(0, 2, \dots, 0)$, …, $(0, \dots, 0, 2)$ est libre de cardinal n, donc maximal, mais ce n'est pas une base de $\mathbb{Z}^n$ puisque $(1, 0, \dots, 0)$ n'est pas dans le sous-groupe engendré (la somme des coordonnées d'un vecteurs du sous-groupe engendré est toujours paire).

Exercice 14 :

Soit $e_1 = (a_1, \dots, a_n) \in \mathbb{Z}^n$ un vecteur tel que le pgcd de ses coordonnées vaut 1. Montrer que l'on peut compléter e_1 en une base $(e_1, \dots, e_n)$ de $\mathbb{Z}^n$.

Solution de l'exercice 14. L'exercice équivaut à trouver une matrice dans $\mathrm{GL}_n(\mathbb{Z})$ dont la première ligne est formée des entiers $a_1, \dots, a_n$. On le montre par récurrence sur n. Soit d le pgcd de $a_1, \dots, a_{n-1}$ et notons $a'_i = a_i/d$ pour tout $1 \leq i \leq n-1$. Alors, par hypothèse de récurrence, il existe une matrice D de taille $(n-1) \times (n-2)$ telle que la matrice

$$\left(\begin{array}{ccc} a'_1 & \dots & a'_{n-1} \\ \hline & & \\ & D & \\ & & \end{array}\right)$$

appartienne à $\mathrm{GL}_{n-1}(\mathbb{Z})$. Par hypothèse, $\mathrm{pgcd}(a_n, d) = 1$ donc il existe $v, w \in \mathbb{Z}$ tels que $a_n v + dw = 1$. Alors la matrice

$$\left(\begin{array}{ccccc} da'_1 & \dots & da'_{n-1} & a_n \\ \hline & & & 0 \\ & & & 0 \\ & D & & 0 \\ & & & \vdots \\ & & & 0 \\ -va'_1 & \dots & -va'_{n-1} & w \end{array}\right)$$

convient.

Exercice 15 : $\star\star$

Déterminer les facteurs invariants des matrices suivantes à coefficients dans $\mathbb{Z}$:

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix}, \begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix}, \begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix}.$$

Solution de l'exercice 15. On peut le faire de deux façons différentes a priori : soit en calculant le PGCD des coefficients de la matrices, puis le PGCD des mineurs de taille 2, etc..., soit en appliquant l'algorithme de réduction des matrices à coefficients entiers via des opérations élémentaires sur les lignes et les colonnes (cette second méthode est sans doute la plus rapide dans le troisième exemple). Dans les deux cas, on trouve les résultats suivants, où $\sim$ désigne l'équivalence des matrices à coefficients entiers :

$$\begin{pmatrix} 2 & 4 \\ 4 & 11 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix},$$

$$\begin{pmatrix} 69 & -153 \\ 12 & -27 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix},$$

$$\begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 16 \end{pmatrix}.$$

Les facteurs invariants sont donc respectivement $(1, 6)$, $(3, 9)$ et $(1, 2, 16)$.

Exercice 16 :

a) Soit G un groupe abélien de type fini et soit $f : G \to G$ un morphisme surjectif. Montrer que f est un isomorphisme. Ceci est-il nécessairement vrai si l'on remplace surjectif par injectif ?

b) Soit G un groupe abélien libre de type fini et soit $f : G \to G$ un morphisme. Définir le déterminant $\det(f) \in \mathbb{Z}$ de f et montrer que f est injectif si et seulement si $\det(f) \neq 0$. Dans ce cas, montrer que l'on a $|\mathrm{Coker}(f)| = |\det(f)|$.

Solution de l'exercice 16.

a) Notons F le sous-groupe de torsion de G, de sorte que $\overline{G} := G/F$ est un groupe abélien libre de type fini, i.e. isomorphe à $\mathbb{Z}^n$. On voit alors que f induit un morphisme $f_{\mathrm{tors}} : F \to F$ et un morphisme surjectif $\overline{f} : \overline{G} \to \overline{G}$. On choisit une base $(e_1, \dots, e_n)$ de $\overline{G}$. Comme $\overline{f}$ est surjectif, pour tout $1 \leq i \leq n$, il existe $d_i \in \overline{G}$ tel que $f(d_i) = e_i$. On considère alors le morphisme $\overline{g} : \overline{G} \to \overline{G}$ défini par $\overline{g}(e_i) := d_i$ pour tout i. On voit alors que (d_i) est une base de $\overline{G}$. Par construction, on a $\overline{f} \circ \overline{g} = \mathrm{id}_{\overline{G}}$. Alors le calcul matriciel assure que l'on a aussi $\overline{g} \circ \overline{f} = \mathrm{id}_{\overline{G}}$, donc $\overline{f}$ est un isomorphisme. Comme $\overline{f}$ est injectif, on en déduit que $f_{\mathrm{tors}} : F \to F$ est surjectif, et comme F est fini, f_{tors} est un isomorphisme de F. Il est alors facile de conclure que f est un isomorphisme de G.

Variante : pour tout $n \geq 1$, on a une inclusion $\mathrm{Ker}(f^n) \subset \mathrm{Ker}(f^{n+1})$ et un isomorphisme $\mathrm{Ker}(f^{n+1})/\mathrm{Ker}(f^n) \cong \mathrm{Ker}(f)$. On peut montrer que la suite des noyaux $\mathrm{Ker}(f^n)$ est une suite croissante de sous-groupes de G. Or on voit facilement que $G \cong F \times \mathbb{Z}^n$ n'admet pas de suite croissante non stationnaire de sous-groupes, donc la suite des $\mathrm{Ker}(f^n)$ est stationnaire : il existe $n \geq 1$ tel que $\mathrm{Ker}(f^n) = \mathrm{Ker}(f^{n+1})$. On en déduit donc que $\mathrm{Ker}(f) = 0$, ce qui conclut la preuve.

La conclusion n'est plus valable si l'on remplace surjectif par injectif. Par exemple, le morphisme de multiplication par 2 dans $\mathbb{Z}$ est injectif, mais son image est le sous-groupe strict $2\mathbb{Z} \subset \mathbb{Z}$, donc ce n'est pas un isomorphisme.

b) On définit $\det(f)$ comme le déterminant de la matrice de f (à coefficents dans $\mathbb{Z}$) dans une base quelconque de G sur $\mathbb{Z}$. En effet, la formule classique de changement de bases assure que ce déterminant est bien défini (il ne dépend pas de la base choisie). Cela revient à définir $\det(f)$ comme le déterminant de l'endomorphisme $\widetilde{f}$ de $\mathbb{Q}^n$ induit par f via un isomorphisme $G \cong \mathbb{Z}^n$ (correspondant au choix d'une base de G).

Supposons $\det(f) \neq 0$. Alors l'application linéaire correspondante $\widetilde{f} : \mathbb{Q}^n \to \mathbb{Q}^n$ est de déterminant non nul, donc elle est injective, ce qui assure que sa restriction à $\mathbb{Z}^n$ est injective, donc f est injective.

Réciproquement, supposons que $\det(f) = 0$. Alors il existe $x \in \mathbb{Q}^n$ non nul tel que $\widetilde{f}(x) = 0$. Or il existe $m \in \mathbb{Z} \setminus \{0\}$ tel que $mx \in \mathbb{Z}^n$. On a alors $f(mx) = m\widetilde{f}(x) = 0$, et $mx \neq 0$, donc f n'est pas injective sur $\mathbb{Z}^n$.

On suppose désormais que $\det(f) \neq 0$. Le théorème de réduction des matrices à coefficients entiers assure qu'il existe deux bases (x_i) et (y_i) de G et $(d_1, \dots, d_n)$ des entiers positifs tels que $\mathrm{Mat}_{\underline{x},\underline{y}}(f) = \mathrm{diag}(d_1, \dots, d_n)$. En particulier, on a $\det(f) = \pm d_1 \dots d_n$ et l'image de f est engendrée par les vecteurs $(d_1 y_1, \dots, d_n y_n)$. Comme $(y_1, \dots, y_n)$ est une base de G, on voit que $\mathrm{Coker}(f) := G/\mathrm{Im}\,(f) \cong \prod_{i=1}^n \mathbb{Z}/d_i\mathbb{Z}$. Donc en particulier, on a $|\mathrm{Coker}(f)| = |d_1 \dots d_n|$, d'où le résultat.

Exercice 17 : $\star\star\star$

Soient $A_1, \dots, A_n$ des groupes abéliens de type fini et $f_i : A_i \to A_{i+1}$ des morphismes de groupes. On dit que la suite

$$0 \to A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \dots \xrightarrow{f_{n-1}} A_n \to 0$$

est exacte si f_1 est injectif, f_{n-1} est surjectif, et pour tout $1 \leq i \leq n-2$, $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$.
Montrer que si la suite est exacte, alors $\sum_{i=1}^n (-1)^i \mathrm{rang}(A_i) = 0$.

Solution de l'exercice 17. On remarque qu'une telle suite exacte se découpe en des suites exactes courtes de la forme

$$0 \to \mathrm{Im}\,(f_{i-1}) = \mathrm{Ker}(f_i) \to A_i \xrightarrow{f_i} \mathrm{Im}\,(f_i) = \mathrm{Ker}(f_{i+1}) \to 0\,,$$

et qu'il suffit donc de démontrer la formule souhaitée pour un telle suite exacte courte. On suppose donc $n = 3$.
On sait que le rang d'un groupe abélien G de type fini est le cardinal maximal d'une famille libre de G, i.e. le plus grand entier n tel que G admette un sous-groupe (ou un quotient) isomorphe à $\mathbb{Z}^n$.
On note r_i le rang de A_i. Il existe donc un sous-groupe de B_i de A_i isomorphe à $\mathbb{Z}^{n_i}$. Si $(e_1, \dots, e_{n_3})$ est une base de B_3, on peut trouver pour tout $1 \leq j \leq n_3$ un élément $d_j \in A_2$ tel que $f_2(d_j) = e_j$. Alors le sous-groupe de A_2 engendré par $f_1(B_1)$ et par les d_j est isomorpheà $\mathbb{Z}^{r_1+r_3}$: en effet, si $(c_1, \dots, c_{n_1})$ est une base de B_1, pour tous $(\lambda_1, \dots, \lambda_{n_1}, \mu_1, \dots, \mu_{n_3}) \in \mathbb{Z}^{n_1+n_3}$ tels que $\sum_i \lambda_i f_1(c_i) + \sum_j \mu_j d_j = 0$, on a (après application de f_2) $\sum_j \mu_j e_j = 0$ dans A_3, donc tous les μ_j sont nuls, donc $\sum_i \lambda_i f_1(c_i) = 0$, donc par injectivité de f_1, $\sum_i \lambda_i c_i = 0$, donc tous les λ_i sont nuls, donc la famille $(f_1(c_1, \dots, f_1(c_{n_1}), d_1, \dots, d_{n_3})$ est bien libre. On a donc $r_2 \geq r_1 + r_3$. Le théorème de la base adaptée assure que $f_1(A_1) \cap B_2$ est un sous-groupe abélien libre de rang s_1, tel que le quotient soit de rand $r_2 - s_1$ (pas forcément libre). Donc $s_1 \leq r_1$ et $r_2 - s_1 \leq r_3$, donc $r_2 \leq r_1 + r_3$. Donc finalement $r_2 = r_1 + r_3$, ce qui conclut la preuve.

Exercice 18 : $\star\star\star$
On se propose de redémontrer le théorème de structure des groupes abéliens finis.
On appelle caractère d'un groupe abélien fini G tout morphisme $G \to \mathbb{C}^*$.

a) Si H est un sous-groupe d'un groupe abélien fini G, montrer que tout caractère de H se prolonge en un caractère de G.

b) Soit G un groupe abélien fini. On note H un sous-groupe de G engendré par un élément de G d'ordre maximal. Montrer que l'on a un isomorphisme $G \cong H \times G/H$.

c) Conclure.

Solution de l'exercice 18.

a) On monter le résultat par récurrence sur $n := [G : H]$. C'est clair si $n = 1$. Supposons donc $n > 1$ et le résultat vrai pour tous les sous-groupes H' de G tels que $[G : H'] < n$. Soit $\chi : H \to \mathbb{C}^*$ un caractère de H. Choisissons $x \in G \setminus H$, et notons $m \geq 2$ l'entier minimal tel que $x^m \in H$. On note enfin $H' := \langle H, x \rangle$. Comme $x^m \in H$, $a := \chi(x^m) \in \mathbb{C}^*$ a bien un sens. On sait que a admet (au moins) une racine m-ième, choisissons-en une que l'on note a_0. On pose alors $\chi' : H' \to \mathbb{C}^*$ défini par $\chi'(hx^k) := \chi(h)a_0^k$. Vérifions que χ' est bien défini et que c'est un caractère de H'. Tout d'abord, supposons que $hx^k = h'x^{k'}$, avec $h, h' \in H$ et $k, k' \in \mathbb{Z}$. Alors $h^{-1}h' = x^{k-k'}$, donc $k - k'$ est multiple de m. Notons par exemple $k - k' = mr$. Alors on a

$$\chi(h')a_O^{k'} = \chi(hx^{mr})a_0^{k'} = \chi(h)\chi(x^{mr})a_0^{k'} = \chi(h)a_0^{k'+mr} = \chi(h)a_0^k\,,$$

ce qui assure que χ' est bien défini. Montrons maitenant que c'est un morphisme de groupes : soient $h, h\text{“} \in H$ et $k, k' \in \mathbb{Z}$. On a alors

$$\chi'(hx^k h'x^{k'}) = \chi'(hh'x^{k+k'}) = \chi(hh')a_0^{k+k'} = \chi(h)\chi(h')a_0^{k+k'} = \chi(h)a_0^k\chi(h')a_0^{k'} = \chi'(hx^k)\chi'(h'x^{k'})\,,$$

donc χ' est un caractère de H'.
Enfin, il est clair par construction que $\chi'_{|H} = \chi$.
L'hypothèse de récurrence assure alors que χ' se prolonge en un caractère de G, car $[G : H'] < [G : H]$, donc χ se prolonge bien en un caractère de G.

b) Notons d l'ordre du sous-groupe cyclique H et $\pi : G \to G/H$ la projection canonique. Il est clair qu'il existe un caractère surjectif (et même un isomorphisme) $\chi : H \to \mu_d(\mathbb{C})$, où $\mu_d(\mathbb{C})$ désigne le sous-groupe de $\mathbb{C}^*$ formé des racines d-ièmes de l'unité. La question a) assure alors que χ se prolonge en un caractère $\chi' : G \to \mathbb{C}^*$. Remarquons que par définition de H, l'exposant de G est égal à d, ce qui assure que χ' est un morphisme à valeurs dans $\mu_d(\mathbb{C})$. En particulier, on dispose d'un morphisme de groupes surjectif

$$\varphi := \chi^{-1} \circ \chi' : G \to H\,.$$

Alors le morphisme

$$\psi : G \to H \times G/H$$

défini par $\psi(g) := (\varphi(g), \pi(g))$. Alors $\mathrm{Ker}(\psi) = \mathrm{Ker}(\varphi) \cap \mathrm{Ker}(\pi) = \mathrm{Ker}(\chi') \cap H$. Or $\chi'_{|H} = \chi$ est injectif, donc $\mathrm{Ker}(\psi) = \{e\}$, donc ψ est injectif, donc par cardinalité, ψ est un isomorphisme.

c) La question b) jointe à une récurrence simple sur $|G|$ assure que tout groupe abélien fini G est isomorphe à un produit de groupes cycliques de la forme

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots, \mathbb{Z}/d_r\mathbb{Z}$$

avec $d_1 \geq 2$ et $d_i | d_{i+1}$ pour tout i.
Il reste à montrer l'unicité d'une telle écriture. Cela peut se faire assez facilement avec une récurrence sur r, ou alors en suivant la preuve du cours.

TD4 : Produit semi-direct

Exercices $\star$: à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices $\star\star$: seront traités en classe en priorité.
Exercices $\star\star\star$: plus difficiles.

Exercice 1 : $\star$
Soient N et H des groupes et soit $\phi : H \to \mathrm{Aut}(N)$ un morphisme de groupes. Notons $N \underset{\phi}{\rtimes} H$ l'ensemble $N \times H$ muni de la loi de composition définie par $(n_1, h_1) \underset{\phi}{\rtimes} (n_2, h_2) = (n_1\phi(h_1)(n_2), h_1h_2)$.

a) Montrer que $N \underset{\phi}{\rtimes} H$ est un groupe, appelé *produit semi-direct* de H par N relativement à ϕ.

b) Montrer que $N \times \{e_H\} \lhd N \underset{\phi}{\rtimes} H$ et $\{e_N\} \times H < N \underset{\phi}{\rtimes} H$.

c) Identifier le quotient de $N \underset{\phi}{\rtimes} H$ par $N \times \{e_H\}$.

Solution de l'exercice 1.

a) Montrons d'abord que la loi est associative. Soient $n_1, n_2, n_3 \in N$ et $h_1, h_2, h_3 \in H$. Par définition du produit, on a

$$((n_1, h_1) \underset{\phi}{\rtimes} (n_2, h_2)) \underset{\phi}{\rtimes} (n_3, h_3) = (n_1\phi(h_1)(n_2), h_1h_2) \underset{\phi}{\rtimes} (n_3, h_3) = (n_1\phi(h_1)(n_2)\phi(h_1h_2)(n_3), h_1h_2h_3)\,.$$

De même, on a

$$(n_1, h_1) \underset{\phi}{\rtimes} ((n_2, h_2) \underset{\phi}{\rtimes} (n_3, h_3)) = (n_1, h_1) \underset{\phi}{\rtimes} (n_2\phi(h_2)(n_3), h_2h_3) = (n_1\phi(h_1)(n_2\phi(h_2)(n_3)), h_1h_2h_3)\,.$$

Or par définition de ϕ, $\phi(_1)$ est un morphisme de groupes, et ϕ est lui-même un morphisme, donc on a

$$\phi(h_1)(n_2\phi(h_2)(n_3)) = \phi(h_1)(n_2)(\phi(h_1) \circ \phi(h_2))(n_3) = \phi(h_1)(n_2)\phi(h_1h_2)(n_3)\,,$$

dont on déduit que

$$((n_1, h_1) \underset{\phi}{\rtimes} (n_2, h_2)) \underset{\phi}{\rtimes} (n_3, h_3) = (n_1, h_1) \underset{\phi}{\rtimes} ((n_2, h_2) \underset{\phi}{\rtimes} (n_3, h_3))\,,$$

donc le produit $\underset{\phi}{\rtimes}$ est associatif.
On voit tout de suite que l'élément (e_N, e_H) est neutre pour la loi $\underset{\phi}{\rtimes}$.
Montrons que tout élément admet un inverse. Soit $n \in N$ et $h \in H$. Pour tous $n' \in N$, $h' \in H$, on a

$$(n, h) \underset{\phi}{\rtimes} (n', h') = (e_N, e_H)$$

si et seulement si

$$(n\phi(n')(h'), hh') = (e_N, e_H)\,,$$

si et seulement si $h' = h^{-1}$ et $n' = \phi(h^{-1})(n^{-1})$. Le calcul de $(n', h') \underset{\phi}{\rtimes} (n, h)$ est exactement similaire, ce qui assure que (n, h) est inversible et que son inverse est $(n, h)^{-1} = (\phi(h^{-1})(n^{-1}), h^{-1})$.
On a donc bien montré que $N \underset{\phi}{\rtimes} H$ est un groupe.

b) Les formules définissant le produit assurent que $N \times \{e_H\}$ et $\{e_N\} \times H$ sont bien des sous-groupes de $N \underset{\phi}{\rtimes} H$, car $\phi(h)(e_N) = e_N$ pour tout $h \in H$. Montrons que le premier est distingué : soit $n, n' \in N$ et $h' \in H$. On a alors

$$\begin{aligned}(n,h) \underset{\phi}{\rtimes} (n',e_H) \underset{\phi}{\rtimes} (n,h)^{-1} &= (n,h) \underset{\phi}{\rtimes} (n',e_H) \underset{\phi}{\rtimes} (\phi(h^{-1})(n^{-1}),h^{-1}) \\ &= (n\phi(h)(n'),h) \underset{\phi}{\rtimes} (\phi(h^{-1}(n^{-1}),h^{-1}) \\ &= (n\phi(h)(n')\phi(h)(\phi(h^{-1})(n^{-1})),e_H) \\ &= (n\phi(h)(n')n^{-1},e_H) \in N \times \{e_H\}\,.\end{aligned}$$

Cela montre bien que $N \times \{e_H\}$ est distingué.

On remarque en revanche qu'en général, $\{e_N\} \times H$ n'est pas distingué (faire le calcul).

c) On dispose d'une application naturelle $\pi : N \underset{\phi}{\rtimes} H \to H$ donné par la seconde projection, à savoir $\pi(n,h) := h$. Il est clair que π est surjective, et la définition de la loi de groupes assure que π est un morphisme de groupes. Calculons son noyau : soient $n \in N$ et $h \in H$. On a $\pi(n,h) = e_H$ si et seulement si $h = e_H$, donc $\mathrm{Ker}(\pi) = N \times \{e_H\}$. Finalement, l'application π passe au quotient par son noyau et induit un isomorphisme de groupes

$$\overline{\pi} : \left(N \underset{\phi}{\rtimes} H\right) / \left(N \underset{\phi}{\rtimes} \{e_H\}\right) \xrightarrow{\sim} H\,.$$

Exercice 2 : $\star$

Soit G un groupe et soient N et H des sous-groupes de G tels que $N \cap H = \{e\}$, $NH = G$ et $N \lhd G$. Montrer que :

a) l'application $i : H \to \mathrm{Aut}(N)$ définie par $h \mapsto i_h$, où $i_h(n) = hnh^{-1}$, est un morphisme de groupes.

b) l'application

$$\begin{aligned} f : N \underset{i}{\rtimes} H &\to G \\ (n,h) &\mapsto nh \end{aligned}$$

est un isomorphisme de groupes.

On dit alors que G est le *produit semi-direct* de H par N.

Solution de l'exercice 2.

a) C'est évident (i est bien définie car N est distingué dans G).

b) Montrons que f est un morphisme de groupes. Soient $n, n' \in N$ et $h, h' \in H$. On a

$$f(n,h)f(n',h') = nhn'h'$$

et

$$f((n,h) \underset{i}{\rtimes} (n',h')) = f(ni(h)(n'),hh') = f(nhn'h^{-1},hh') = nhn'h^{-1}hh' = nhn'h'\,,$$

ce qui assure que $f((n,h) \underset{i}{\rtimes} (n',h')) = f(n,h)f(n',h')$, donc f est bien un morphisme de groupes.

Montrons maintenant que f est un isomorphisme de groupes : l'hypothèse $NH = G$ assure que f est surjectif, et l'hypothèse $N \cap H = \{e\}$ assure que le noyau de f est trivial. Donc f est bien un isomorphisme.

Exercice 3 : $\star$

Montrer que le produit semi-direct $N \underset{\phi}{\rtimes} H$ est direct si et seulement si ϕ est le morphisme trivial si et seulement si $\{e_N\} \times H \lhd N \underset{\phi}{\rtimes} H$.

Solution de l'exercice 3. Le produit semi-direct $N \underset{\phi}{\rtimes} H$ est direct si et seulement si pour tous $n, n' \in N$ et $h, h' \in H$, on a

$$(n, h) \underset{\phi}{\rtimes} (n', h') = (n', hh')$$

si et seulement si pour tous $n, n' \in N$ et $h \in H$, $n\phi(h)(n') = nn'$ si et seulement si pour tous $n' \in N$ et $h \in H$, $\phi(h)(n') = n'$ si et seulement si ϕ est le morphisme trivial.
Pour tout $n \in N$ et $h, h' \in H$, on a

$$(n, h) \underset{\phi}{\rtimes} (e_N, h') \underset{\phi}{\rtimes} (n, h)^{-1} = (n\phi(hh'h^{-1})(n^{-1}), hh'h^{-1}) .$$

On en déduit immédiatement que le morphisme ϕ est trivial si et seulement si $\{e_N\} \times H$ est distingué dans $N \underset{\phi}{\rtimes} H$.

Exercice 4 : $\star\star$
Une suite de morphismes $\ldots \to A \xrightarrow{u} B \xrightarrow{v} C \to \ldots$ est dit exacte en B si $\mathrm{Im}(u) = \mathrm{Ker}(v)$, et elle est dite *exacte* si elle est exacte en tous ses termes.
Soit

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

une suite exacte (courte). On dit alors que G est une *extension* de H par N.

a) Montrer que, si G est le produit direct de H et N ou bien un produit semi-direct de H par N, alors on a une telle suite exacte.

b) Réciproquement soit une telle suite exacte. Si p possède une *section*, c'est-à-dire s'il existe un morphisme de groupes $s : H \to G$ tel que $p \circ s = \mathrm{id}_H$, montrer que G est le produit semi-direct de H par N pour l'opération $h \cdot n = s(h)ns(h)^{-1}$.

c) Donner un exemple de suite exacte courte qui n'est pas un produit semi-direct.

Solution de l'exercice 4.

a) On suppose que $G = N \underset{\phi}{\rtimes} H$. On a vu dans l'exercice 1, question c), que l'on disposait d'un morphisme surjectif $\pi : G \to H$ dont le noyau est le sous-groupe $N \underset{\phi}{\rtimes} \{e_H\}$, qui est isomorphe à N. Donc on a bien une suite exacte

$$1 \to N \xrightarrow{i} G \xrightarrow{\pi} H \to 1 ,$$

où $i : N \to G$ est défini par $i(n) := (n, e_H)$.
On vérifie en outre que l'application $H \to G$ définie par $h \mapsto (e_N, h)$ est une section de π.

b) C'est une conséquence de l'exercice 2 appliqué aux sous-groupes $N' := i(N)$ et $H' := s(H)$ de G. Vérifons seulement que ces deux sous-groupes satisfont les hypothèses de l'exercice 2 : il est clair que N' est distingué dans G car $N' = \mathrm{Ker}(p)$. Soit $g \in G$, posons $h := s(\pi(g)) \in H'$. Alors on a

$$\pi(h) = \pi(s(\pi(g)) = \pi(g) ,$$

donc $n := gh^{-1} \in \mathrm{Ker}(\pi) = N'$, donc finalement on a bien $g = nh$, ce qui assure que $G = N'H'$.
Soit $g \in N' \cap H'$. Comme $g \in H'$, il existe $h \in H$ tel que $g = s(h)$. Comme $g \in N'$, $\pi(g) = e_H$. Donc $\pi(s(h)) = e_H$, i.e. $h = e_H$, donc $g = s(e_H) = e_G$. Donc $N' \cap H' = \{e_G\}$.
On peut donc bien appliquer l'exercice 2 pour conclure.

c) On peut par exemple considérer la suite exacte

$$1 \to \mathbb{Z}/2\mathbb{Z} \to Z/4\mathbb{Z} \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \to 1$$

où p est la réduction modulo 2. C'est bien une suite exacte, en revanche p n'admet pas de section, puisque l'élément non trivial du quotient $\mathbb{Z}/2\mathbb{Z}$ est d'ordre 2, alors que tous ses antécédents par p sont d'ordre 4. Donc $\mathbb{Z}/4\mathbb{Z}$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Un autre exemple est donné par le groupe des quaternions $\mathbf{H}_8$ dont le centre Z est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et le quotient correspondant est $G/Z \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ce qui fournit une suite exacte

$$1 \to Z/2\mathbb{Z} \to \mathbf{H}_8 \xrightarrow{p} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to 1\,,$$

telle que p n'admet pas de section (on le voit en listant les éléments d'ordre 2 dans $\mathbf{H}_8$). Donc $\mathbf{H}_8$ n'est pas produit semi-direct de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$.

Exercice 5 : $\star\star$

a) Montrer que l'on peut écrire $\mathfrak{S}_n$ comme un produit semi-direct naturel.

b) Montrer que l'on peut écrire le groupe diédral D_n comme un produit semi-direct naturel.

c) Montrer que l'on peut écrire $\mathrm{GL}_n(k)$ comme un produit semi-direct naturel (k est un corps).

d) Ces produits semi-directs sont-ils directs ?

Solution de l'exercice 5.

a) On considère la suite exacte suivante

$$1 \to \mathfrak{A}_n \to \mathfrak{S}_n \xrightarrow{\varepsilon} \{\pm 1\} \to 1\,,$$

ce qui est une traduction du fait que la signature est un morphisme de groupes surjectif dans $\{\pm 1\}$ à noyau $\mathfrak{A}_n$.
La donnée d'une section du morphisme ε équivaut à la donnée d'une permutation $\sigma \in \mathfrak{S}_n$ d'ordre 2 et de signature -1. On peut prendre par exemple $\sigma = (12)$. L'exercice 4 assure alors que cette section induit un isomorphisme de groupes

$$\mathfrak{S}_n \cong \mathfrak{A}_n \underset{\phi}{\rtimes} \{\pm 1\}$$

où l'action de $\{\pm 1\}$ sur $\mathfrak{A}_n$ est donnée par la conjugaison par σ, i.e. $\phi(-1) : \tau \mapsto \sigma\tau\sigma^{-1}$.

b) On rappelle que le groupe diédral D_n est le groupe des isométries du plan préservant un polygone régulier à n côtés. Ce groupe est constitué de n isométries directes qui forment un sous-groupe, engendré par la rotation r de centre O et d'angle $\frac{2\pi}{n}$ (une fois qu'on a choisi pour origine O l'isobarycentre des sommets de polygone), et n isométries indirectes qui sont de la forme $r^k \circ s$, où $k \in \mathbb{Z}$ et s est une symétrie axiale (fixée) préservant le polygone. On dispose alors des sous-groupes $\langle r \rangle$ et $\langle s \rangle$ qui vérifient les hypothèses de l'exercice 2, ce qui assure que l'on a un isomorphisme $D_n \cong \langle r \rangle \underset{\phi}{\rtimes} \langle s \rangle$ où l'action ϕ est donnée par conjugaison dans D_n. Comme les groupes $\langle r \rangle$ et $\langle s \rangle$ sont cycliques d'ordre respectifs n et 2, on a donc un isomorphisme

$$D_n \cong \mathbb{Z}/n\mathbb{Z} \underset{\phi}{\rtimes} \mathbb{Z}/2\mathbb{Z}\,,$$

où l'action ϕ est donnée par $\phi(-1) : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $x \mapsto -x$.

c) On a une suite exacte naturelle

$$1 \to \mathrm{SL}_n(k) \to \mathrm{GL}_n(k) \xrightarrow{\det} k^* \to 1\,,$$

et on dispose d'une section $s : k^* \to \mathrm{GL}_n(k)$ du morphisme déterminant donnée par exemple par $s(\lambda) := \mathrm{diag}(\lambda, 1, \ldots, 1)$. Alors l'exercice 4 assure que cela fournit un isomorphisme

$$\mathrm{GL}_n(k) \cong \mathrm{SL}_n(k) \underset{\phi}{\rtimes} k^*\,.$$

d) On voit facilement que dans les cas a) et b), les produits ne sont pas directs (sauf pour $n = 2$), quelle que soit la section choisie. Et mieux, on vérifie facilement qu'il n'existe pas d'isomorphisme (quelconque) entre ces groupes et les produits directs correspondants.

En revanche, le cas c) est moins évident pour $n \geq 2$. Si $x \mapsto x^n$ est un automorphisme de k^*, notons $a : k^\times \to k^\times$ son inverse. Alors l'application

$$\begin{aligned} \alpha : \mathrm{SL}_n(k) \times k^* &\simeq \mathrm{GL}_n(k) \\ (A, t) &\mapsto A.\mathrm{diag}(a(t), \ldots, a(t)) \end{aligned}$$

est un isomorphisme.

Réciproquement, supposons qu'il existe un isomorphisme de groupes

$$\begin{aligned} \alpha : \mathrm{SL}_n(k) \times k^* &\simeq \mathrm{GL}_n(k) \\ (A, t) &\mapsto \phi(A)s(t)\,. \end{aligned}$$

Le sous-groupe dérivé de $\mathrm{SL}_n(k) \times k^*$ est $\mathrm{SL}_n(k) \times \{1\}$ et celui de $\mathrm{GL}_n(k)$ est aussi $\mathrm{SL}_n(k)$ [1]. On en déduit que ϕ est un automorphisme de $\mathrm{SL}_n(k)$.

En outre, $\alpha(k^*) = s(k^*)$ commute avec tout élément de $\mathrm{GL}_n(k)$ et est donc composé uniquement d'homothéties (le centre de $\mathrm{GL}_n(k)$ est formé des homothéties). On a donc que l'application $t \mapsto s(t)$ est un morphisme injectif de la forme $t \mapsto \mathrm{diag}(a(t), \ldots, a(t))$ de k^* vers $\mathrm{GL}_n(k)$.

Puisque le noyau de det est $\mathrm{SL}_n(k)$, on en déduit que $a(t)^n = 1$ si, et seulement si, $a(t) = 1$. Puisque $t \mapsto a(t)$ est injectif, on déduit que $t \mapsto a(t)^n$ est injectif. Or det est surjectif sur k^*, donc $t \mapsto a(t)^n = a(t^n)$ est bijectif, et donc $x \mapsto x^n$ est bijectif et donc un automorphisme de k^*.

Finalement, $\mathrm{GL}_n(k)$ est isomorphe au produit direct de $\mathrm{SL}_n(k)$ par k^* si et seulement si le morphisme $(.)^n : k^* \to k^*$ est un automorphisme. C'est le cas par exemple si $k = \mathbb{R}$ et n est impair, ou si k est un corps fini (ou plus généralement un corps dit parfait) de caractéristique p avec n égal à une puissance de p.

Exercice 6 :
Soit $G = N \rtimes H$ et soit K un sous-groupe de G contenant N. Montrer que l'on a $K = N \rtimes (K \cap H)$.

Solution de l'exercice 6. C'est immédiat en applicant par exemple l'exercice 2 :

a) On a $N \lhd G$ et $N < K$, donc $N \lhd K$.

b) On a $H < G$ et $K < G$, donc $H \cap K < K$.

c) On a $N \cap H = \{e\}$, donc $N \cap (K \cap H) = \{e\}$.

d) On a $NH = G$, donc si $k \in K$, alors $k = nh$ avec $n \in N$ et $h \in H$. Puisque $N \subset K$, on en déduit que $h \in H \cap K$. D'où $N(H \cap K) = K$.

Exercice 7 :
Montrer que tout groupe d'ordre 255 est cyclique.

Solution de l'exercice 7. Soit G un groupe d'ordre $255 = 3 \cdot 5 \cdot 17$. D'après les théorèmes de Sylow, le nombre n_3 de 3-Sylow vaut 1 ou 85, le nombre n_5 de 5-Sylow vaut 1 ou 51 et on n'a qu'un seul 17-Sylow. On ne peut pas avoir $n_3 = 85$ et $n_5 = 51$ car on aurait trop d'éléments dans G. Donc $n_3 = 1$ ou $n_5 = 1$. Supposons $n_3 = 1$ (l'autre cas se résoud de la même façon). Notons S_3 le seul 3-Sylow, S_{17} le seul 17-Sylow et S_5 un 5-Sylow quelconque. On a :

a) $S_3 S_{17} \simeq S_3 \times S_{17} \lhd G$.

b) $S_3 S_{17} \cap S_5 = \{e\}$.

c) $S_3 S_{17} S_5 = G$

1. Sauf dans le cas $n = 2$ et $k = \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$. On peut faire l'exercice à la main dans ces deux cas (si $k = \mathbb{Z}/2\mathbb{Z}$, on a un produit direct et si $k = \mathbb{Z}/3\mathbb{Z}$ ce n'est pas un produit direct).

On déduit de l'exercice 2 que $G = S_3S_{17} \rtimes S_5$. Soit $\phi : S_5 \to \mathrm{Aut}(S_3S_{17})$ le morphisme correspondant. On sait que $\mathrm{Aut}(S_3S_{17}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, donc ϕ est trivial et le produit semi-direct est direct. On conclut par le lemme chinois.

Exercice 8 : ⋆⋆
Soient H et N des groupes et soient ϕ et $\psi : H \to \mathrm{Aut}(N)$ des morphismes. On veut trouver des conditions nécessaires et suffisantes pour que $N \rtimes_\phi H$ et $N \rtimes_\psi H$ soient isomorphes.

a) S'il existe un automorphisme α de H tel que $\psi = \phi \circ \alpha$, montrer que l'on a la conclusion attendue.

b) S'il existe un automorphisme u de N tel que

$$\forall h \in H \qquad \phi(h) = u\psi(h)u^{-1},$$

montrer que la conclusion attendue vaut encore.

c) Si H est cyclique et que ϕ et $\psi : H \to \mathrm{Aut}(N)$ sont tels que $\phi(H) = \psi(H)$, montrer que $N \rtimes_\phi H$ et $N \rtimes_\psi H$ sont isomorphes.

Solution de l'exercice 8.

a) Le morphisme $\begin{array}{ccc} N \rtimes_\psi H & \to & N \rtimes_\phi H \\ (n,h) & \mapsto & (n, \alpha(h)) \end{array}$ est un isomorphisme.

b) Le morphisme $\begin{array}{ccc} N \rtimes_\psi H & \to & N \rtimes_\phi H \\ (n,h) & \mapsto & (u(n), h) \end{array}$ est l'isomorphisme recherché.

c) H est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et $\mathrm{Im}\,(\phi) = \mathrm{Im}\,(\psi)$ est isomorphe à $\mathbb{Z}/m\mathbb{Z}$ avec m diviseur de n. Il existe donc d premier à m tel que $\phi(1) = d\psi(1)$ dans $\mathbb{Z}/m\mathbb{Z}$. Puisque l'application $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$ est surjective, il existe $d' \in (\mathbb{Z}/n\mathbb{Z})^\times$ qui s'envoie vers d.
La multiplication par d' est un automorphisme α de $\mathbb{Z}/n\mathbb{Z}$ qui satisfait aux conditions de a), d'où le résultat.

Exercice 9 : ⋆⋆
Soient $p < q$ des nombres premiers.

a) Déterminer à isomorphisme près tous les groupes de cardinal pq.

b) Si $q \geq 3$, en déduire que tout groupe de cardinal $2q$ est isomorphe à $\mathbb{Z}/2q\mathbb{Z}$ ou au groupe diédral D_q.

Solution de l'exercice 9.

a) Soit G un groupe de cardinal pq. Le théorème de Sylow assure que G admet un unique q-Sylow N qui est donc distingué dans G. Par cardinalité, on a $N \cong \mathbb{Z}/q\mathbb{Z}$. On sait aussi que G admet un p-Sylow $H \cong \mathbb{Z}/p\mathbb{Z}$. Alors $N \cap H = \{e\}$, et $NH = G$ par cardinalité. Donc G est un produit semi-direct de G par H. Donc

$$G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}\,.$$

Ce produit semi-direct est défini via un morphisme $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ (voir TD3, exercice 7). On a alors deux cas :
— Si p ne divise pas $q-1$, alors le morphisme ϕ est trivial, donc G est isomorphe au produit direct $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$. Il y a donc une unique classe d'isomorphisme de groupes d'ordre pq, à savoir celle de $\mathbb{Z}/pq\mathbb{Z}$.
— Si p divise $q-1$, alors il existe un morphisme non trivial $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z}$ et tout tel morphisme est injectif. Alors la question c) de l'exercice 8 assure que si ϕ et ϕ' sont deux tels morphismes non triviaux, alors les produits semi-directs $\mathbb{Z}/q\mathbb{Z} \underset{\phi}{\rtimes} \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \underset{\phi'}{\rtimes} \mathbb{Z}/p\mathbb{Z}$ sont isomorphes. Il existe donc exactement deux classes d'isomorphisme de groupes de cardinal pq, à savoir $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ (produit semi-direct non trivial).

b) C'est le cas particulier de la question précédente avec $p = 2$. Comme $q - 1$ est pair, on est dans le second cas : il existe exactement deux classes d'isomorphisme de groupes d'ordre $2q$, qui sont $\mathbb{Z}/2q\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Or on a vu à l'exercice 5, question b), que ce dernier groupe est isomorphe à D_q (c'est l'unique groupe non abélien d'ordre $2q$).

Exercice 10 : $\star\star\star$

a) Montrer qu'un groupe d'ordre 8 est isomorphe à l'un des groupes suivants :

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4,\ \mathbf{H}_8.$$

Justifier que $\mathbf{H}_8$ n'est pas un produit semi-direct et que les cinq groupes cités sont deux-à-deux non isomorphes.

b) Montrer que $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ possède un unique 2-Sylow que l'on identifiera.

c) Donner la liste des classes d'isomorphisme de groupes finis de cardinal ≤ 15.

Solution de l'exercice 10.

a) Soit G un groupe d'ordre 8.

i) Si G possède un élément d'ordre 8, alors G est cyclique, isomorphe $\mathbb{Z}/8\mathbb{Z}$.

ii) Si G est d'exposant 2, alors G est abélien et isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

iii) Si G est d'exposant 4 et est abélien, alors G est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

iv) On suppose maintenant G d'exposant 4 et non abélien. Il existe $r \in G$ d'ordre 4. Alors $R\langle r\rangle$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Soit $s \in G \setminus \langle r\rangle$ d'ordre minimal.

i. Si s est d'ordre 2, alors le sous-groupe engendré $S = \langle s\rangle$ intersecte R trivialement, et G est engendré par R et S (puisque ces derniers contiennent au moins 5 éléments). De plus, R est distingué car d'indice 2, et G est donc isomorphe au produit semi-direct $R \rtimes S \cong \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq D_4$.

ii. Si s est d'ordre 4, renommons r et s respectivement par i et j. Reste à établir la table de G et voir qu'elle coïncide avec celle de $\mathbf{H}_8$: pour cela, on note $k := ij \in G$. Comme $j \notin R$ et j est d'ordre 4, on voit que $k \notin R \cup S$. Donc k est d'ordre 4 également. Si $R \cap S = \{1\}$, alors $k^3 \in R \cup S$, donc $k \in R \cup S$, ce qui est contradictoire. Donc $R \cap S$ est d'ordre 2, engendré par $i^2 = j^2$. Cela assure que $i^2 = j^2$ est central dans G. Comme G est de cardinal 8 et comme les éléments $1, i, j, i^2 = j^2, i^3, j^3, k, k^3$ sont deux-à-deux distincts, l'élément k^2 qui est d'ordre 2, est nécessairement égal à $i^2 = j^2$. On a donc i, j, k d'ordre 4, avec $k = ij$ et $i^2 = j^2 = k^2$ central. Calculons ji : comme $ji \notin R \cup S$, on a $ji = k$ ou $ji = k^3$. Or G n'est pas commutatif, donc $ji = k^3 = i^2(ij)$. Finalement, on a bien montré que la table de multiplication de G est celle du groupe des quaternions, donc $G \cong \mathbf{H}_8$.

On a donc bien montré qu'il y avait exactement cinq groupes d'ordre 8 à isomorphisme près.

Supposons maintenant que $\mathbf{H}_8 = N \rtimes H$ soit un produit semi-direct non trivial. Alors l'un des sous-groupes N ou H est d'ordre 2, donc est exactement $\{\pm 1\}$ (-1 est l'unique élément d'ordre 2 dans $\mathbf{H}_8$). Si c'était H, H serait distingué car -1 est central, et le produit semi-direct serait direct. Comme tout groupe d'ordre 4 est abélien, $\mathbf{H}_8$ serait abélien, ce qui n'est pas le cas. On peut donc supposer $N = \{\pm 1\}$. Mais alors $\mathrm{Aut}(N)$ est réduit à un élément et tout morphisme $H \to \mathrm{Aut}(N)$ est trivial. Le produit semi-direct serait encore direct et $\mathbf{H}_8$ à nouveau abélien. C'est donc que l'hypothèse initiale est fausse, donc $\mathbf{H}_8$ n'est pas un produit semi-direct non trivial.

b) En passant en revue les éléments de $\mathrm{SL}_2(\mathbb{F}_3)$, il y en a uniquement 8 d'ordre une puissance de 2. Ce sont :

— ordre 1 : $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;

— ordre 2 : $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$;
— ordre 4 : $\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$.

Il y a donc un unique 2-Sylow dans $\mathrm{SL}_2(\mathbb{F}_3)$, et il est clairement isomorphe à $\mathbf{H}_8$.

c) On a déjà classifié les groupes d'ordre ≤ 7 dans l'exercice 8 de la feuille de TD1. Les groupes d'ordre 8 sont classifiés à la question a). Les groupes d'ordre 9, 11 et 13 sont abéliens. Les groupes d'ordre 10, 13, 14 et 15 sont classifiés à l'exercice 9. Il reste donc à traiter les groupes d'ordre $12 = 2^2.3$. Soit G un groupe d'ordre 12. Les théorèmes de Sylow assure que G admet un ou quatre 3-Sylow :
— Dans le premier cas, G admet donc un sous-groupe distingué N isomorphe à $\mathbb{Z}/3\mathbb{Z}$, tel que $H = G/N$ soit un groupe d'ordre 4. Alors par cardinalité, G est produit semi-direct de H par $N \cong \mathbb{Z}/3\mathbb{Z}$. Un tel produit est défini par un morphisme $\phi : H \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Si H est cyclique d'ordre 4, il existe un unique tel morphisme ϕ non trivial, qui définit le produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, en plus du produit direct $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Sinon, $H \cong (\mathbb{Z}/2\mathbb{Z})^2$, et il y a exactement trois morphismes ϕ non triviaux dont on constate qu'ils diffèrent deux-à-deux d'un automorphisme de H, et donc l'exercice 8, question a), assure que les produits semi-directs associés sont isomorphes ; par conséquent, dans ce cas, on a un unique produit semi-direct non trivial $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2$ en plus du produit direct $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.
— Dans le second cas, G admet $4.2 = 8$ éléments d'ordre 3, ce qui assure que le complémentaire de l'ensemble de ces éléments est l'unique 2-Sylow N de G. Alors G est produit semi-direct de $\mathbb{Z}/3\mathbb{Z}$ par N. Un tel produit est donné par un un morphisme de groupes $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(N)$. Si N est cyclique, alors $\mathrm{Aut}(N)$ est d'ordre 2 et ϕ est trivial. Si $N \cong (\mathbb{Z}/2\mathbb{Z})^2$, alors $\mathrm{Aut}(N) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$, donc il existe un morphisme non trivial $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(N)$, et deux tels morphismes définissent des produits semi-directs isomorphes par l'exercice 8, question c). Donc finalement, donc ce cas, G est soit $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, soit $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$, soit $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$.

On a donc la liste suivante des classes d'isomorphisme de groupes d'ordre 12 (il est facile de vérifier que ces groupes ne sont pas deux-à-deux isomorphes) :

$$\mathbb{Z}/12\mathbb{Z}\,,\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}\,,\ \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}\,,\ \mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2 \cong D_6\,,\ (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z} \cong \mathfrak{A}_4\,.$$

Finalement, on a la classification complète des groupes d'ordre ≤ 15 :
— ordre 1 : le groupe trivial $\{1\}$.
— ordre 2 : le groupe cyclique d'ordre 2, à savoir $\mathbb{Z}/2\mathbb{Z}$.
— ordre 3 : le groupe cyclique d'ordre 3, à savoir $\mathbb{Z}/3\mathbb{Z}$.
— ordre 4 : les groupes abéliens d'ordre 4, à savoir $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$.
— ordre 5 : le groupe cyclique d'ordre 5, à savoir $\mathbb{Z}/5\mathbb{Z}$.
— ordre 6 : le groupe cyclique d'ordre 6, i.e. $\mathbb{Z}/6\mathbb{Z}$, et le groupe symétrique $\mathfrak{S}_3$.
— ordre 7 : le groupe cyclique d'ordre 7, i.e. $\mathbb{Z}/7\mathbb{Z}$.
— ordre 8 : les groupes abéliens d'ordre 8, i.e $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^3$, le groupe diédral D_4 et le groupe des quaternions $\mathbf{H}_8$.
— ordre 9 : les groupes abéliens d'ordre 9, à savoir $\mathbb{Z}/9\mathbb{Z}$ et $(\mathbb{Z}/3\mathbb{Z})^2$.
— ordre 10 : le groupe cyclique d'ordre 10, i.e. $\mathbb{Z}/10\mathbb{Z}$ et le groupe diédral D_5.
— ordre 11 : le groupe cyclique d'ordre 11, à savoir $\mathbb{Z}/11\mathbb{Z}$.
— ordre 12 : les groupes abéliens d'ordre 12, i.e. $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, le groupe alterné $\mathfrak{A}_4 \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$, le groupe diédral D_6 et le groupe $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.
— ordre 13 : le groupe cyclique d'ordre 13, à savoir $\mathbb{Z}/13\mathbb{Z}$.
— ordre 14 : le groupe cyclique d'ordre 14, i.e $\mathbb{Z}/14\mathbb{Z}$, et le groupe diédral D_7.
— ordre 15 : le groupe cyclique d'ordre 15, à savoir $\mathbb{Z}/15\mathbb{Z}$.

Exercice 11 : $\star\star\star$

Soit p un nombre premier impair.

a) Déterminer les p-Sylow de $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

b) Soient ϕ et ψ des morphismes non triviaux de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. En notant pour tout entier k, ϕ_k le morphisme défini par $\phi_k(x) = \phi(kx)$, montrer qu'il existe un entier k et une matrice $P \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ tels que $\psi = P\phi_k P^{-1}$.

c) En déduire qu'il existe, à isomorphisme près, un unique produit semi-direct non trivial $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.

d) Montrer que le centre de ce dernier groupe est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

e) Soit G un groupe d'ordre p^3 non cyclique, contenant un élément x d'ordre p^2. Monter que $\langle x\rangle$ est distingué dans G et que G est un produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $\langle x\rangle \cong \mathbb{Z}/p^2\mathbb{Z}$.

f) Décrire les classes d'isomorphisme de groupes de cardinal p^3 : on raisonnera par exemple suivant l'ordre maximal d'un élément du groupe.

Solution de l'exercice 11.

a) Les p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$ sont d'ordre p. Soit $\mathcal{S}$ l'ensemble des p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$. Comme le sous-groupe $U := \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} : * \in \mathbb{F}_p \right\}$ des matrices unipotentes supérieures est un p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$, en faisant agir $\mathrm{GL}_2(\mathbb{F}_p)$ sur $\mathcal{S}$ par conjugaison, on voit que $\mathcal{S}$ est isomorphe à $\mathrm{GL}_2(\mathbb{F}_p)/\mathrm{Stab}(U) = \mathrm{GL}_2(\mathbb{F}_p)/B$, où $B := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \right\}$ désigne le sous-groupe de Borel standard de $\mathrm{GL}_2(\mathbb{F}_p)$. Cela donne directement la liste qui suit dans a') :

a') Une variante : les p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$ sont d'ordre p. Comme le sous-groupe U des matrices unipotentes supérieures est un p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$ et que tous sont conjugués, on voit qu'une matrice de $\mathrm{GL}_2(\mathbb{F}_p)$ est dans un p-Sylow si et seulement si son polynôme caractéristique est $(X-1)^2$. On dénombre (à la main) p^2 telles matrices et donc $(p+1)$ p-Sylow distincts (car deux p-Sylow distincts ne s'intersectent qu'en l'élément neutre). On remarque que ce sont les conjugués de U par les $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, $a \in \mathbb{F}_p$, et par $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

b) Comme les images de ψ et φ sont des p-Sylow de $\mathrm{GL}_2(\mathbb{F}_p)$, elles sont conjuguées par une matrice $P \in \mathrm{GL}_2(\mathbb{F}_p)$. Notons $\begin{array}{rccc} \varphi^{(P)} : & \mathbb{Z}/p\mathbb{Z} & \to & \psi(\mathbb{Z}/p\mathbb{Z}) \\ & x & \mapsto & P\varphi(x)P^{-1} \end{array}$; c'est un isomorphisme. Dès lors, $(\varphi^{(P)})^{-1} \circ \psi$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$, donc de la forme $x \mapsto kx$ pour un certain $k \in \mathbb{Z}$ premier avec p.

c) Comme on a $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{F}_p)$, la question a) nous donne l'existence d'un tel produit semi-direct non trivial. L'unicité résulte de b) et de l'exercice 8.

d) Comme le centre d'un p-groupe est non trivial, le centre de $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$, ne peut être que d'ordre p, p^2 ou p^3. Mais s'il était d'ordre p^2 ou p^3, l'exercice 9 du TD1 nous dirait que $(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$ est abélien. Ce n'est pas le cas puisque le produit semi-direct est non trivial, et donc le centre est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

e) Le sous-groupe $\langle x\rangle$ est d'indice p dans un groupe d'ordre p^3, donc on a vu à l'exercice 5, question a), du TD2, que $\langle x\rangle$ est distingué dans G. En outre, le quotient $G/\langle x\rangle$ est d'ordre p, donc isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Soit alors $y \in G \setminus \langle x\rangle$. Alors $y^p \in \langle x\rangle$ et $y^{p^2} = e$, donc il existe $k \in \mathbb{Z}$ tel que $y^p = x^{pk}$. Comme $\langle x\rangle$ est distingué, il existe un entier $r \geq 0$ tel que $y^{-1}xy = x^r$. On voit alors facilement que pour tous $\alpha \in \mathbb{N}$, on a $x^\alpha y = yx^{\alpha r}$. On cherche à trouver $z \in G \setminus \langle x\rangle$ d'ordre p. On cherche z sous la forme $z = yx^n$. Alors $z^p = (yx^n)^p = yx^nyx^n \dots yx^n$, et une récurrence simple assure que

$$z^p = y^p x^{n(r^{p-1}+\cdots+r+1)} = x^{pk+n(r^{p-1}+\cdots+r+1)}\,.$$

Donc z est d'ordre p si et seulement si

$$pk + n(r^{p-1} + \cdots + r + 1) \equiv 0\ [p^2]\,. \tag{1}$$

On cherche donc à résoudre l'équation (1) d'inconnue $n \in \mathbb{Z}$. Notons $S := r^{p-1} + \cdots + r + 1$. Alors on a $(r-1)S \equiv r - 1\ [p]$, donc soit $r \not\equiv 1\ [p]$ et $S \equiv 1\ [p]$, soit $r \equiv 1\ [p]$ et on vérifie

que dans ce cas $S \equiv p\ [p^2]$ (remarquons que l'hypothèse p impair est utilisée ici). Donc dans les deux cas, cela assure que l'équation (1) admet toujours une solution $n_0 \in \mathbb{Z}$. Au vu de la discussion précédente, on sait donc que $z_0 := yx^{n_0} \in G \setminus \langle x \rangle$ est d'ordre p. Par conséquent, les deux sous-groupe $N := \langle x \rangle$ et $H := \langle z \rangle$ vérifient les hypothèses de l'exercice 2, ce qui asssure que G est produit semi-direct de $H \cong \mathbb{Z}/p\mathbb{Z}$ par $N \cong \mathbb{Z}/p^2\mathbb{Z}$.

f) Soit G un groupe d'ordre p^3. On note p^r l'ordre maximal d'un élément de G.
   — Si $r = 3$, G est cyclique et $G \cong \mathbb{Z}/p^3\mathbb{Z}$.
   — Si $r = 2$, alors la question e) assure que $G \cong \mathbb{Z}/p^2\mathbb{Z} \underset{\phi}{\rtimes} \mathbb{Z}/p\mathbb{Z}$. Ce produit semi-direct est défini par un morphisme $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong \mathbb{Z}/p(p-1)\mathbb{Z}$. Comme le groupe $\mathbb{Z}/p(p-1)\mathbb{Z}$ admet un unique sous-groupe d'ordre p, l'exercice 8, question c), assure qu'il existe un unique produit semi-direct non trivial $\mathbb{Z}/p^2\mathbb{Z} \underset{\phi}{\rtimes} \mathbb{Z}/p\mathbb{Z}$.
   — Si $r = 1$, alors tout sous-groupe de G d'ordre p^2 est distingué et isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ (on rappelle qu'un tel sous-groupe existe effectivement), et tout élément du complémentaire de ce sous-groupe est d'ordre p, ce qui assure que G est produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $(\mathbb{Z}/p\mathbb{Z})^2$. Par conséquent, la question c) assure que $G \cong (\mathbb{Z}/p\mathbb{Z})^3$ ou G est isomorphe à l'unique produit semi-direct non trivial $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}$.

   Finalement, on aboutit à la conclusion qu'il y a exactement cinq classes d'isomorphisme de groupes d'ordre p^3, à savoir

$$\mathbb{Z}/p^3\mathbb{Z}\,,\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}\,,\ (\mathbb{Z}/p\mathbb{Z})^3\,,\ (\mathbb{Z}/p^2\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}\,,\ (\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/p\mathbb{Z}\,.$$

   On remarquera que contrairement au cas $p = 2$ (voir exercice 10, question c)), tous les groupes d'ordre p^3 sont des produits semi-directs de groupes abéliens.

   Le lecteur curieux pourra essayer de réaliser les deux classes d'isomorphisme non abéliennes comme des groupes de matrices sur $\mathbb{F}_p$.

Exercice 12 : $\star\star\star$

Soient $p \neq q$ deux nombres premiers. Classifier les groupes d'ordre p^2q.

Solution de l'exercice 12. Soit G un groupe d'ordre p^2q. On note n_p (resp. n_q) le nombre de p-Sylow (resp. q-Sylow) de G. Les théorèmes de Sylow assurent que $n_p = 1$ ou q et $n_q = 1, p$ ou p^2.
Supposons que $n_q = p^2$. Cela implique que $q|p^2 - 1$. Alors G possède exactement $p^2(q-1) = p^2q - p^2$ éléments d'ordre r. Donc le complémentaire de l'ensemble de ces éléments est l'unique p-Sylow de G. Donc on a $n_p = 1$.
Supposons $n_q = p$. Il est clair qu'alors $n_p = q$ est impossible. Donc $n_p = 1$.
Finalement, on donc dans l'un des cas suivants :
— $q|p^2 - 1$, $n_p = 1$ et $n_q = p^2$. Dans ce cas, G est produit semi-direct non trivial de $\mathbb{Z}/q\mathbb{Z}$ par son p-Sylow, lequel est soit $(\mathbb{Z}/p\mathbb{Z})^2$, soit $\mathbb{Z}/p^2\mathbb{Z}$.
— $q|p - 1$, $n_p = 1$ et $n_q = p$. Dans ce cas, G est produit semi-direct non trivial de $\mathbb{Z}/q\mathbb{Z}$ par son p-Sylow, lequel est soit $(\mathbb{Z}/p\mathbb{Z})^2$, soit $\mathbb{Z}/p^2\mathbb{Z}$.
— $p|q - 1$, $n_p = q$ et $n_q = 1$. Dans ce cas, G est produit semi-direct non trivial de soit $(\mathbb{Z}/p\mathbb{Z})^2$, soit $\mathbb{Z}/p^2\mathbb{Z}$, par son q-Sylow $\mathbb{Z}/q\mathbb{Z}$.
— $n_p = n_q = 1$. Dans ce cas, G est abélien, isomorphe à $\mathbb{Z}/p^2q\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$.

On est donc amené à classifier les produits semi-directs d'un groupe d'ordre p^2 par un groupe d'ordre q, et d'un groupe d'ordre q par un groupe d'ordre p^2. On obtient que :

a) Il existe un produit semi-direct non trivial $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ si et seulement si $q|p - 1$ (car $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ est cyclique d'ordre $p(p-1)$), et dans ce cas, il existe une unique classe d'isomorphisme de tels groupes, grâce à l'exercice 8, question c).

b) Il existe un produit semi-direct non trivial $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$ si et seulement si $q|p^2-1$ (on rappelle que $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2) \cong \mathrm{GL}_2(\mathbb{F}_p)$). Dénombrons maintenant, sous cette hypothèse, le nombre de classes d'isomorphisme de tels groupes. On voit facilement que deux produits semi-directs de cette forme, définis par deux morphismes non triviaux $\phi, \psi : \mathbb{Z}/q\mathbb{Z} \to \mathrm{GL}_2(\mathbb{F}_p)$, sont isomorphes si et seulement si $\phi(\mathbb{Z}/q\mathbb{Z})$ et $\psi(\mathbb{Z}/q\mathbb{Z})$ sont des sous-groupes conjugués de $\mathrm{GL}_2(\mathbb{F}_p)$. On voit

facilement que deux matrices non scalaires de $\mathrm{GL}_2(\mathbb{F}_p)$ sont conjuguées si et seulement si elles ont les mêmes valeurs propres (c'est valable sur un corps quelconque). Or deux matrices d'ordre q dans $\mathrm{GL}_2(\mathbb{F}_p)$ ont pour valeurs propres des racines q-ièmes de l'unité. Si les deux valeurs propres sont 1, la matrice est semblable à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ qui est d'ordre p, ce qui est contradictoire. On est alors amené à distinguer les cas suivants :

i) $q = 2$. La discussion précédente assure qu'il y a exactement deux classes de conjugaison de matrices d'ordre 2, à savoir $-I_2$ et $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. On en déduit donc deux classes d'isomorphisme de produits semi-directs non triviaux $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

ii) $q|p-1$ et $q \not| p+1$. Comme $q|p-1$, $\mathbb{F}_p^*$ contient exactement q racines q-ièmes de l'unité. Soit $\zeta \in \mathbb{F}_p^*$ une telle racine primitive. Alors on voit que tout sous-groupe d'ordre q de $\mathrm{GL}_2(\mathbb{F}_p)$ est engendré par une matrice dont les valeurs propres sont ζ et ζ^r avec $0 \leq r < q$. Deux tels sous-groupes (caractérisé par des entiers r et r' comme précédemment) sont conjugués si et seulement s'il existe $1 \leq s < q$ tel que $(1, r) = (s, r's)$ ou $(1, r) = (r's, s)$, si et seulement si $r = r'$ ou ($r \neq 0$ et $r' = r^{-1}$ mod. q). Donc dans ce cas, le nombre de produits semi-directs $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$ non triviaux non isomorphes est de $\frac{q+3}{2}$.

iii) $q \not| p-1$ et $q|p+1$. Alors $\mathbb{F}_p^*$ ne contient aucun élément d'ordre q. Donc toute matrice d'ordre q est de déterminant 1, donc les valeurs propres d'une telle matrice sont des racines primitives q-ièmes de l'unité $\neq 1$ inverses l'une de l'autre. Par conséquent, si A et B sont deux matrices quelconques d'ordre q, B est conjuguée à une puissance de A première à q (et vice-versa). Cela assure que le produit semi-direct non-trivial $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$ est unique (à isomorphisme près) dans ce cas.

c) Il existe un produit semi-direct non trivial $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$ si et seulement si $p|q-1$ (car $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est cyclique d'ordre $q-1$), et dans ce cas, l'exercice 8, question c), assure qu'il existe une unique classe d'isomorphisme de tels groupes si p divise exactement $q-1$, et deux telles classes si $p^2|q-1$.

d) Il existe un produit semi-direct non trivial $\mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^2$ si et seulement si $p|q-1$ (car $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est cyclique d'ordre $q-1$). Or dans ce cas, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ admet un unique sous-groupe d'ordre p, et deux morphismes non triviaux de $(\mathbb{Z}/p\mathbb{Z})^2$ vers ce sous-groupe diffèrent par un automorphisme de $(\mathbb{Z}/p\mathbb{Z})^2$, ce qui assure que tous les produits semi-directs non triviaux $\mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^2$ sont isomorphes.

Finalement, on obtient la classification suivante :

a) Si $p \not| q-1$ et $q \not| p^2-1$. Deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$.

b) Si $p|q-1$, $p^2 \not| q-1$ et $q \not| p^2-1$. Quatre groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^2$.

c) Si $p^2|q-1$ et $q \not| p^2-1$. Cinq groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; deux produits semi-directs $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^2$.

d) Si $q|p-1$ et $q \neq 2$. $\frac{q+9}{2}$ groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$; $\frac{q+3}{2}$ produits semi-directs $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$.

e) Si $q|p+1$ et $q \neq 2$ et $p \neq 2$. Trois groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; un produit semi-direct $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$.

f) $q = 2$. Cinq groupes : deux groupes abéliens $\mathbb{Z}/p^2q\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/pq\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$; deux produits semi-directs $(\mathbb{Z}/p\mathbb{Z})^2 \rtimes \mathbb{Z}/q\mathbb{Z}$.

g) $p = 2$ et $q = 3$. Cinq groupes : deux groupes abéliens $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$; un produit semi-direct $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2$; un produit semi-direct $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z}$.

TD5 : groupes résolubles et nilpotents, croissance des groupes

Exercices $\star$: à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices $\star\star$: seront traités en classe en priorité.
Exercices $\star\star\star$: plus difficiles.

Certaines questions de cette feuille sont résolues dans le polycopié de cours, mais ces notions ne seront pas traitées en cours. Il est recommandé de chercher ces exercices sans l'aide du polycopié.

Si G est un groupe, on note $C^0(G) := G$ et $C^{n+1}(G) := [G, C^n(G)]$, à savoir le sous-groupe de G engendré par les commutateurs $ghg^{-1}h^{-1}$, avec $g \in G$ et $h \in C^n(G)$. On dit que G est nilpotent s'il existe $N \geq 0$ tel que $C^N(G) = \{e\}$. Dans ce cas, l'entier $N \geq 0$ minimal tel que $C^N(G) = \{e\}$ est appelé classe de nilpotence de G.

Exercice 1 : $\star$
Soit G un groupe.

a) Montrer qu'un groupe nilpotent est résoluble.

b) Que dire de la réciproque ?

c) Montrer que le centre d'un groupe nilpotent est non trivial.

d) Montrer que si G est nilpotent et H est un sous-groupe de G, alors H est nilpotent.

e) On suppose désormais dans la suite que H est un sous-groupe distingué de G. Montrer que si G est nilpotent, G/H est nilpotent.

f) On suppose H et G/H nilpotents. Le groupe G est-il nilpotent ?

g) Les groupes résolubles $\mathfrak{S}_3$ et $\mathfrak{S}_4$ sont-ils nilpotents ?

h) Soit p un nombre premier. Montrer que tout p-groupe est nilpotent.

i) Soient p, q, r trois nombres premiers. Montrer que tout groupe d'ordre pqr est résoluble. Un tel groupe est-il nilpotent ?

j) On suppose G fini. Montrer que G est nilpotent si et seulement si tout sous-groupe maximal de G est distingué si et seulement si G est produit direct de ses p-Sylow.

Solution de l'exercice 1.

a) On montre facilement par récurrence que pour tout $n \in \mathbb{N}$, on a $D^n(G) \subset C^n(G)$. Cela assure l'implication demandée.

b) La réciproque est fausse : le groupe $G = \mathfrak{S}_3$ est résoluble puisque sont groupe dérivé est le groupe abélien $\mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$, donc $D^2(G) = \{\mathrm{id}\}$ (G est extension d'un groupe abélien par un autre groupe abélien). En revanche, G n'est pas nilpotent puisque $C^1(G) = \mathfrak{A}_3$ n'est pas central dans G (le 3-cycle (123) ne commute pas avec (12) par exemple), donc $C^2(G) = [\mathfrak{S}_3, \mathfrak{A}_3]$ est un sous-groupe non trivial de $\mathfrak{A}_3 \cong \mathbb{Z}/3$, donc $C^2(G) = \mathfrak{A}_3 = C^1(G)$, donc $C^n(G) = \mathfrak{A}_3$ pour tout $n \geq 1$.

c) Soit G un groupe nilpotent. Il existe un entier $n \geq 0$ maximal tel que $C^n(G) \neq \{e\}$. Alors $C^{n+1}(G) = \{e\}$, donc $[G, C^n(G)] = \{e\}$, ce qui signifie que le sous-groupe non trivial $C^n(G)$ est contenu dans le centre de G. Donc $Z(G) \neq \{e\}$.

d) Une récurrence simple assure que pour tout $n \geq 0$, $C^n(H) \subset C^n(G)$, d'où le résultat.

e) La projection canonique $\pi : G \to G/H$ est un morphisme de groupes, donc une récurrence assure que $\pi(C^n(G)) \subset C^n(G/H)$ pour tout n. Or π est surjectif, donc une nouvelle récurrence assure que $\pi(C^n(G)) = C^n(G/H)$ (un commutateur dans G/H se relève en un commutateur dans G...). Cette égalité assure le résultat.

f) Non. Si $G = \mathfrak{S}_3$, $H = \mathfrak{A}_3$ et $G/H = \{\pm 1\}$, alors H et G/H sont abéliens donc nilpotents, alors que G n'est pas nilpotent par la question b).

En revanche, on a le résultat plus faible suivant : si $H \subset G$ est un sous-groupe central, alors G/H nilpotent implique G nilpotent. En effet, la question précédente assure que si $C^n(G/H) = \{e\}$, alors $C^n(G) \subset H$, donc $C^{n+1}(G) = [G, C^n(G)] \subset [G, H] \subset [G, Z(G)] = \{e\}$, donc G est nilpotent.

g) Non et non. Pour $\mathfrak{S}_3$, voir la question b). Et $\mathfrak{S}_3$ est isomorphe à un sous-groupe de $\mathfrak{S}_4$, donc la question d) assure que $\mathfrak{S}_4$ n'est pas nilpotent.

h) Soit G un groupe de cardinal p^n. On montre par récurrence sur n que G est nilpotent. Si $n = 1$, c'est évident car un groupe d'ordre p est commutatif. On suppose $n \geq 2$. Alors on sait que le centre de G n'est pas réduit à $\{e\}$, donc $G/Z(G)$ est de cardinal p^i avec $0 \leq i < n$. Par hypothèse de récurrence, $G/Z(G)$ est nilpotent, donc la remarque dans la réponse à la question f) assure que G est nilpotent.

i) — On suppose d'abord que $p = q = r$. Alors G est nilpotent par la question h), donc G est résoluble.

— On suppose maintenant $p = q \neq r$. Les théorèmes de Sylow assurent que $n_p = 1$ ou r et $n_r = 1$, p ou p^2. Supposons que $n_r = p^2$. Alors G contient exactement $p^2(r-1) = p^2 r - p^2 = |G| - p^2$ éléments d'ordre r, et un p-Sylow de G est de cardinal p^2, ce qui assure que G admet un unique p-Sylow, i.e. $n_p = 1$. Si l'on supose que $n_r = p$, alors nécessairement $n_p \neq r$ (sinon on aurait $p|r-1$ et $r|p-1$, ce qui est absurde), donc $n_p = 1$. Finalement, dans tous les cas, on a soit $n_r = 1$, soit $n_p = 1$. On a donc dans G un sous-groupe distingué d'ordre r ou d'ordre p^2, donc abélien, tel que le groupe quotient soit d'ordre p^2 ou r, donc abélien également. Cela assure que G est résoluble. En outre, G n'est pas nécessairement nilpotent (cf par exemple $G = \mathfrak{S}_3 \times \mathbb{Z}/2\mathbb{Z}$).

— On suppose maintenant que $p < q < r$. Alors $n_r = 1$ ou $n_r = pq$, et $n_q = 1$, r ou pr. Supposons que $n_r \neq 1$ et $n_q \neq 1$. Alors G admet exactement $pq(r-1)$ élḿeent d'ordre r, et au moins $r(q-1)$ éléments d'ordre q. Donc on a

$$|G| \geq pq(r-1) + r(q-1) = pqr + (q-1)r - pq \geq pqr + pr - pq = |G| + p(r-q) > |G|\,,$$

ce qui est contradictoire. Donc $n_1 = 1$ ou $n_q = 1$, donc G admet un sous-groupe distingué d'ordre premier (donc abélien), tel que le quotient soit un groupe dont le cardinal est produit de deux nombres premiers distincts. En particulier, ce quotient est résoluble (voir TD2, exercice 11 a)), donc G est résoluble. En revanche, G n'est pas toujours nilpotent, voir par exemple $G = \mathfrak{S}_3 \times \mathbb{Z}/5\mathbb{Z}$.

j) — On suppose que G est le produit direct de ses sous-groupes de Sylow. Alors G est un produit de p-groupes, ces p-groupes sont nilpotents (voir h)), et il est clair qu'un produit direct de groupes nilpotents est nilpotent. Donc G est nilpotent.

— On suppose maintenant G nilpotent. Soit $M \subset G$ un sous-groupe maximal. Il existe un entier $n \geq 1$ minimal tel que $C^n(G) \subset M$. Par minimalité de n, il existe $g \in C^{n-1}(G) \setminus M$. Alors on a $[g, M] \subset [C^{n-1}(G), G] \subset C^n(G) \subset M$, ce qui assure que $gMg^{-1} \subset M$, donc $g \in N_G(M) \setminus M$. Donc $N_G(M)$ est un sous-groupe de G contenant strictement M. Par maximalité de M, cela implique que $N_G(M) = G$, donc M est distingué dans G.

— On suppose maintenant que tout sous-groupe maximal de G est distingué dans G. Soit S un p-Sylow de G. Supposons que $N_G(S) \neq G$. Alors $N_G(S)$ est contenu dans un sous-groupe maximal M de G. Par hypothèse, M est distingué dans G. Donc pour tout $g \in G$, $gSg^{-1} \subset gMg^{-1} = M$, donc S et gSg^{-1} sont deux p-Sylow du groupe M. Donc il existe

$h \in M$ tel que $gSg^{-1} = hSh^{-1}$, donc $h^{-1}g \in N_G(S) \subset M$, donc $g \in M$, donc $G = M$, ce qui est contradictoire. Par conséquent, $N_G(S) = G$ et S est donc distingué dans G. On considère alors l'application $\varphi : \prod_{p||G|} S_p \to G$ (où S_p désigne l'unique p-Sylow de G) définie par le produit dans G. Comme les sous-groupes de Sylow ont des cardinaux premiers entre eux, on voit que les éléments d'un sous-groupe de Sylow commutent avec ceux d'un autre, ce qui assure que l'application φ est un morphisme de groupes, clairement injectif. Par cardinalité, c'est un isomorphisme.

Exercice 2 :
Soit G un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$. On note $T_n(\mathbb{C})$ le sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ formé des matrices triangulaires supérieures.

a) Montrer que si G est connexe, alors $D(G)$ l'est aussi.

b) Montrer que si G est abélien, alors G est conjugué à un sous-groupe de $T_n(\mathbb{C})$.

c) On suppose G résoluble connexe. Montrer que G est conjugué à un sous-groupe de $T_n(\mathbb{C})$.

Solution de l'exercice 2.

a) Par définition, $D(G) = \bigcup_{n\in\mathbb{N}^*} G_n$, où G_n désigne l'ensemble des éléments de G qui s'écrivement comme produits de n commutateurs dans G. Montrons que pour tout n, G_n est connexe : l'application $c_n : G^{2n} \to G$ définie par $c_n(g_1, \dots, g_{2n}) := [g_1, g_2] \dots [g_{2n-1}, g_{2n}]$ est continue, et son image est exactement G_n. Cela assure que G_n est connexe car G^{2n} l'est. Or pour tout $n \geq 1$, G_n contient l'élément neutre de G, donc $D(G)$ admet un recouvrement par des parties connexes de G ayant toutes un point de G en commun, donc $D(G)$ est connexe.

b) Tout élément de $\mathrm{GL}_n(\mathbb{C})$ est trigonalisable, donc tout élément de G est trigonalisable. Or G est abélien, donc les éléments de G sont cotrigonalisables, i.e. il existe $P \in \mathrm{GL}_n(\mathbb{C})$ telle que $PGP^{-1} \subset T_n(\mathbb{C})$.

c) Soit G un groupe résoluble. On note V le $\mathbb{C}$-espace vectoriel $\mathbb{C}^n$. Montrons que si $n > 1$, V admet un sous-espace vectoriel strict non nul stable par tous les éléments de G. Pour ce faire, on raisonne par l'absurde, i.e. on suppose qu'aucun sous-espace vectoriel strict non nul de V n'est stable par G, et on va montrer que $n = 1$. On raisonne alors par récurrence sur la "classe de résolubilité" du groupe G, i.e. sur l'entier minimal $r \geq 1$ tel que $D^r(G) = \{I_n\}$.
— Si $r = 1$, alors G est abélien, donc la question b) assure que V admet une droite stable par G, donc l'hypothèse implique que $n = 1$.
— On suppose $r > 1$. Alors $H := D^{r-1}(G)$ est un sous-groupe commutatif distingué dans G, non trivial. La question b) assure que quitte à conjuguer, on peut supposer que H est un sous-groupe de $T_n(\mathbb{C})$. On définit

$$W := \{v \in V : v \text{ est vecteur propre de tout élément de } H\}.$$

On sait que W contient une droite, donc $W \neq \{0\}$. Montrons que W est stable par G. Soit $w \in W$ et $g \in G$. Alors pour tout $h \in H$, on a $h(g(w)) = g(g^{-1}hg(w))$, et $g^{-1}hg \in H$ puisque H est distingué, donc $g^{-1}hg(w)$ est proportionnel à w, donc $h(g(w))$ est proportionnel à $g(w)$, donc $g(w) \in W$. Donc W est bien stable par G. Par hypothèse, on a donc $W = V$. Cela signifie que V admet une base de vecteurs propres pour tous les éléments de H, i.e. que quitte à conjuguer, on peut supposer que $H \subset D_n(\mathbb{C})$, où $D_n(\mathbb{C})$ désigne l'ensemble des matrices diagonales de $\mathrm{GL}_n(\mathbb{C})$.
Montrons maintenant que $H \subset Z(G)$: pour tout $h \in H$ et tout $g \in G$, h et ghg^{-1} ont les mêmes valeurs propres. Or il n'existe qu'un nombre fini de matrices diagonales à valeurs propres fixées. Donc cela assure que l'application $c_h : G \to H$ définie par $c_h(g) := ghg^{-1}$ est d'image finie. Or cette application est continue et G est connexe, donc $c_h(G) = \{h\}$. Cela assure que h est dans le centre de G, donc $H \subset Z(G)$.

Soit $h \in H \setminus \{I_n\}$. Soit U un espace propre de h. Puisque h commute avec tous les éléments de G, on voit que U est stable par G. Or U est non trivial, donc l'hypothèse initiale assure que $U = V$. Donc h est une homothétie (matrice scalaire). Or $h \in D(G) \subset \mathrm{SL}_n(\mathbb{C})$, donc $\det(h) = 1$, donc H est fini. Or la question a) assure que H est connexe, donc $H = \{I_n\}$, ce qui est contradictoire avec le fait que $H = D^{r-1}(G) \neq \{I_n\}$.

On a donc montré que si $n \geq 2$ (ce qui est le cas si G n'est pas abélien), V admet un sous-espace vectoriel W strict non nul stable par G. On note W' un supplémentaire de W. La décomposition $V = W \oplus W'$ assure alors que quitte à conjuguer, G est contenu dans le sous-groupe des matrices "triangulaires supérieures par blocs", avec des blocs de taille $\dim(W)$ et $\dim(W')$: tout élément $g \in G$ s'écrit $g = \begin{pmatrix} g_W & * \\ 0 & g_{W'} \end{pmatrix}$. Donc l'image de G par le morphisme $g \mapsto g_W$ est un sous-groupe résoluble connexe de $\mathrm{GL}_{\dim(W)}(\mathbb{C})$, donc par récurrence, comme $\dim(W) < n$, quitte à conjuguer encore, on peut supposer que les matrices g_W sont triangulaires supérieures pour tout $g \in G$. De même, quitte à choisir une bonne base de V/W, on peut supposer que les matrices $g_{W'}$ sont triangulaires supérieures pour tout $g \in G$. Alors il est clair que G est un sous-groupe de $T_n(\mathbb{C})$.

Exercice 3 : $\star\star$

Soit G un groupe de type fini. On définit le sous-groupe de Frattini de G (noté $\phi(G)$) comme l'intersection des sous-groupes maximaux de G.

a) Montrer que $\mathbb{Q}$ ne possède pas de sous-groupe maximal.

b) Montrer que G admet au moins un sous-groupe maximal. La preuve est-elle plus simple si G est fini ?

c) Montrer que $\phi(G)$ est distingué dans G et même qu'il est stable par tout automorphisme de G (on dit qu'il est caractéristique). On note $\pi : G \to G/\phi(G)$ la projection canonique.

d) Soit $S \subset G$ une partie de G. Montrer que S engendre G si et seulement si $\pi(S)$ engendre $G/\phi(G)$.

e) Montrer que $\phi(G)$ est exactement l'ensemble des éléments $g \in G$ tels que pour toute partie $S \subset G$, on a : $\langle S, g\rangle = G \implies \langle S\rangle = G$.

f) Montrer que si G est fini, alors $\phi(G)$ est nilpotent.

g) On suppose G fini. Montrer que G est nilpotent si et seulement si $D(G) \subset \phi(G)$.

h) On suppose que G est un p-groupe.

i) Montrer que tout sous-groupe maximal de G contient $D(G)$ et le sous-groupe G^p engendré par les puissances p-ièmes dans G.

ii) Montrer que $G/\phi(G)$ est le plus grand quotient abélien de G d'exposant p.

iii) Que peut-on en déduire sur le nombre minimal de générateurs de G ?

iv) Montrer que $\phi(G) = D(G).G^p$.

Solution de l'exercice 3.

a) Soit H un sous-groupe strict de $\mathbb{Q}/\mathbb{Z}$. Il existe donc $x \in \mathbb{Q}/\mathbb{Z}$ tel que $x \notin H$. Notons $H' := \langle H, x\rangle$. C'est un sous-groupe de $\mathbb{Q}/\mathbb{Z}$ contenant strictement H. Or $x \in \mathbb{Q}/\mathbb{Z}$ est d'ordre fini n. On considère l'élément $\frac{x}{n} \in \mathbb{Q}/\mathbb{Z}$: si $\frac{x}{n} \in H'$, alors il existe $m \in \mathbb{Z}$ et $h \in H$ tel que $\frac{x}{n} = h + mx$. Donc $x = nh + 0 = nh$, donc $x \in H$, ce qui est contradictoire. Donc $\frac{x}{n} \notin H'$, donc $H' \neq \mathbb{Q}/\mathbb{Z}$, donc H n'est pas maximal dans $\mathbb{Q}/\mathbb{Z}$. Cela assure que $\mathbb{Q}/\mathbb{Z}$ n'admet pas de sous-groupe maximal.

b) On suppose $G \neq \{e\}$ et on écrit $G = \langle a_1, \ldots, a_n\rangle$. On considère l'ensemble $\mathcal{E}$ des sous-groupes stricts de G. C'est un ensemble non vide, muni de la relation d'ordre donnée par l'inclusion. Montrons que toute partie non vide totalement ordonnée $\mathcal{F}$ de $\mathcal{E}$ admet un majorant dans $\mathcal{E}$. Soit $\mathcal{F}$ une telle partie. On définit alors

$$M := \langle H; H \in \mathcal{F}\rangle = \bigcup_{H \in \mathcal{F}} H\,.$$

Il est clair que M est un sous-groupe de G contenant chacun des $H \in \mathcal{F}$. Montrons que $M \neq G$. Si on avait $M = G$, alors pour tout i, $a_i \in M$, donc pour tout i, il existe $H_i \in \mathcal{F}$ tel que $a_i \in H_i$. Or $\mathcal{F}$ est totalement ordonné, donc il existe $H \in \mathcal{F}$ tel que $a_i \in H$ pour tout $1 \leq i \leq n$. Alors $H = G$ puisque les a_i engendrent G. Ceci est une contradiction car $H \in \mathcal{F}$ est un sous-groupe strict de G. Cela assure donc que $M \neq G$, i.e. que $M \in \mathcal{E}$.

On peut alors appliquer le lemme de Zorn pour déduire que l'ensemble $\mathcal{E}$ admet un élément maximal, ce qui revient à dire que G admet un sous-groupe maximal.

Si le groupe G est fini, l'ensemble des sous-groupes de G est fini également, on peut se passer du lemme de Zorn en considérant un sous-groupe strict de G de cardinal maximum.

c) Soit $\varphi \in \mathrm{Aut}(G)$. Alors pour tout sous-groupe maximal $H \subset G$, $\varphi(H)$ est un sous-groupe maximal de G, et l'application $H \mapsto \varphi(H)$ est une permutation de l'ensemble des sous-groupes maximaux de G. Par conséquent, on a

$$\varphi(\phi(G)) = \bigcap_{H \subset G \text{ maximal}} \varphi(H) = \bigcap_{H \subset G \text{ maximal}} H = \phi(G)\,,$$

donc $\phi(G)$ est un sous-groupe caractéristique de G.

d) Le sens direct est clair puisque π est surjective. Montrons le sens réciproque : on suppose que $H = \langle S \rangle$ n'est pas égal à G. Alors H est contenu dans un sous-groupe maximal M de G. Comme H contient $\phi(G)$, $\pi(H)$ s'identifie à $H/\phi(G)$, qui est un sous-groupe strict de $G/\phi(G)$. Cela assure que $\langle \pi(S) \rangle \subset H/\phi(G)$ est un sous-groupe strict de $G/\phi(G)$, donc $\pi(S)$ n'engendre pas $G/\phi(G)$.

e) La question précédente assure que si $g \in \phi(G)$, alors pour tout $S \subset G$, on a $\langle S, g \rangle = G \implies \langle S \rangle = G$. Soit maintenant $g \in G \setminus \phi(G)$. Alors il existe un sous-groupe maximal H de G tel que $g \notin H$. On considère alors $S := H \subset G$. il est clair que $\langle S \rangle = H \neq G$ alors que $\langle S, g \rangle = G$ par maximalité de H. D'où la description de $\phi(G)$ recherchée.

f) Soit P un p-Sylow de $\phi(G)$. Comme $\phi(G)$ est distingué dans G, on en déduit que $G = \phi(G)N_G(P)$. La question d) assure alors que $G = N_G(P)$, donc P est distingué dans G, donc dans $\phi(G)$. Donc tout sous-groupe de Sylow de $\phi(G)$ est distingué dans $\phi(G)$, ce qui assure que $\phi(G)$ est produit de ses groupes de Sylow, donc $\phi(G)$ est nilpotent (voir exercice 1, j)).

g) On suppose G nilpotent. Alors l'exercice 1 assure que pour tout sous-groupe maximal H de G, H est distingué, donc G/H est un groupe simple nilpotent, donc G/H est cyclique d'ordre premier, donc abélien, donc $D(G) \subset H$. Donc $D(G) \subset \phi(G)$. Réciproquement, si $D(G) \subset \phi(G)$, alors tout sous-groupe maximal H de G contient $D(G)$, donc H est distingué dans G, donc G est nilpotent par l'exercice 1.

h) i) Soit H un sous-groupe maximal de G. La preuve de la question précédente assure que H est distingué dans G et G/H est cyclique d'ordre p, ce qui assure que H contient $D(G)$ et G^p.

ii) La question précédente assure que $G/\phi(G)$ est un groupe abélien d'exposant p. Soit maintenant H un sous-groupe distingué de G tel que G/H soit abélien d'exposant p. Notons $\pi_H : G \to G/H$ la projection. On a donc un isomorphisme $G/H \cong (\mathbb{Z}/p\mathbb{Z})^r$. On considère alors les r-projections $\pi_i : (\mathbb{Z}/p\mathbb{Z})^r \to \mathbb{Z}/p\mathbb{Z}$: il est clair que $H = \bigcap_{i=1}^n H_i$, où $H_i := \mathrm{Ker}(\pi_i \circ \pi_H : G \to \mathbb{Z}/p\mathbb{Z})$, et que les H_i sont des sous-groupes maximaux de G (car d'indice p). Donc $H \subset \phi(G)$, ce qui assure l'existence d'un morphisme surjectif $\pi' : G/\phi(G) \to G/H$ tel que $\pi' \circ \pi = \pi_H$. Donc $G/\phi(G)$ est bien le plus grand quotient abélien d'exposant p de G.

iii) Soit $g_1, \ldots, g_m$ une famille génératrice de G. Alors $\pi(g_1), \ldots, \pi(g_m)$ engendrent $G/\phi(G)$, donc $m \geq \dim_{\mathbb{F}_p}(G/\phi(G))$. Or $G/\phi(G)$ admet une partie génératrice minimale de cardinal $\dim_{\mathbb{F}_p}(G/\phi(G))$, et en choisissant des relevés de ces générateurs dans G, on obtient une famille génératrice (voir question d)) de G de cardinal $\dim_{\mathbb{F}_p}(G/\phi(G))$. Cela assure que le nombre minimal de générateurs de G est égal à $\dim_{\mathbb{F}_p}(G/\phi(G))$.

iv) La question h)i) assure que $D(G).G^p \subset \phi(G)$. Or $G/D(G).G^p$ est clairement un groupe abélien d'exposant p, donc la question h)ii) assure que $\phi(G) \subset D(G).G^p$, ce qui conclut.

Exercice 4 : $\star\star$

Soit G un groupe de type fini. Pour toute partie génératrice finie A de G, pour tout $m \in \mathbb{N}$, on note $B_{G,A}(m)$ l'ensemble des éléments de G qui s'écrivent comme produits d'au plus m éléments de $A \cup A^{-1}$. On pose $\beta_{G,A}(m) := |B_{G,A}(m)|$. Si β et β' sont deux fonctions $\mathbb{N} \to \mathbb{R}^+$, on notera $\beta \preceq \beta'$ s'il existe $c > 0$ et $a \in \mathbb{N}^*$ tels que pour tout n, $\beta(n) \leq c\beta'(an)$, et $\beta \sim \beta'$ si $\beta \preceq \beta'$ et $\beta' \preceq \beta$.

a) Montrer que $B_{G,A}(m)$ est une boule dans l'espace métrique (G, d), où d est une distance que l'on précisera.

b) Soient A et A' deux parties génératrices finies de G. Montrer que $\beta_{G,A} \sim \beta_{G,A'}$. On notera donc abusivement $\beta_G = \beta_{G,A}$.

c) Calculer β_G si G est un groupe fini, si $G = \mathbb{Z}$, si $G = \mathbb{Z}^n$, si G est le groupe libre à n générateurs (i.e. le groupe des mots finis sur un alphabet de n lettres, avec leurs inverses, pour la loi de concaténation des mots).

d) Montrer que $\beta_G(n) \preceq e^n$.

e) Si G' est un groupe de type fini, calculer $\beta_{G\times G'}$.

f) Montrer que si $H \subset G$ est un sous-groupe de type fini, alors $\beta_H \preceq \beta_G$, et si H est d'indice fini, alors $\beta_H \sim \beta_G$.

g) Soit H un quotient de G. Comparer β_H et β_G.

h) Montrer que si $G = \mathrm{SL}_2(\mathbb{Z})$, alors G est de type fini et $\beta_G(n) \sim e^n$.

i) Montrer que si G est nilpotent de classe 2, alors il existe $d \geq 0$ tel que $\beta_G(n) \preceq n^d$.

j) Montrer que si G est nilpotent, alors il existe $d \geq 0$ tel que $\beta_G(n) \preceq n^d$.

k) Montrer que le groupe $G = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$, où le produit semi-direct est défini via la matrice $A := \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, est un groupe résoluble tel que $\beta_G(n) \sim e^n$.

Solution de l'exercice 4.

a) Soient $g, h \in G$. On définit $d(g, h)$ comme le nombre minimal de termes dans une écriture de gh^{-1} comme produit d'éléments de $A \cup A^{-1}$. Il est clair que cela définit une application $d : G \times G \to \mathbb{N}$ telle que
— pour tous $g, h \in G$, $d(g, h) = d(h, g)$ (car l'ensemble $A \cup A^{-1}$ est stable par inverse).
— pour tous $g, h \in G$, $d(g, h) = 0$ si et seulement si $g = h$.
— pour tous $g, h, k \in G$, $d(g, k) \leq d(g, h) + d(h, k)$.
Donc (G, d) est un espace métrique, et $B_{G,A}(m)$ est la boule fermée de centre e et de rayon m pour cette distance d.

b) Il suffit de le montrer pour $A' = A \cup \{\alpha\}$ avec $\alpha \in G$. Il est clair que pour tout $m \geq 0$, on a $B_{G,A}(m) \subset B_{G,A'}(m)$, donc $\beta_{G,A} \preceq \beta_{G,A'}$. Or $\alpha \in G$ s'écrit $\alpha = a_1 \dots a_r$ avec $a_i \in A$ pour tout i. Soit $g \in B_{G,A'}(m)$. Alors $g = a'_1 \dots a'_k$ s'écrit comme un produit de $k \leq m$ éléments de A'. Pour tout $1 \leq i \leq k$, soit $a'_i \in A$, soit $a'_i = \alpha$ et a'_i est produit de r éléments de A. Cela assure que g est produit d'au plus kr éléments de A. Donc $B_{G,A'}(m) \subset B_{G,A}(km)$, donc $\beta_{G,A'} \preceq \beta_{G,A}$. Donc finalement $\beta_{G,A} \sim \beta_{G,A'}$.

c) — Si G est un groupe fini, alors on peut prendre $A = G$ et on voit que $\beta_{G,A}(m) = |G|$ pour tout $m \geq 1$, donc $\beta_G \sim 1$.
— Si $G = \mathbb{Z}$, on peut prendre $A = \{1\}$, et on voit que $B_{G,A}(m) = \{-m, -(m-1), \dots, 0 \dots, m-1, m\}$, donc $\beta_{G,A}(m) = 2m + 1$, donc $\beta_G(m) \sim m$.
— Si $G = \mathbb{Z}^n$, on peut prendre $A = \{-1, 0, 1\}^n$, et on voit que $B_{G,A}(m) = \mathbb{Z}^n \cap [-m; m]^n$, donc $\beta_{G,A}(m) = (2m + 1)^n$, donc $\beta_G(m) \sim m^n$.

— Si G est le groupe libre à $n \geq 2$ générateurs, notés $a_1, \ldots, a_n$, on peut considérer $A = \{a_1, \ldots, a_n\}$, où ϵ est l'élément neutre (mot vide). Alors on a $\beta_{G,A}(m) \geq n^m$ en considérant uniquement les mots de m lettres parmi $a_1, \ldots, a_n$, et on a $\beta_{G,A}(m) \leq (2n+1)^m$ de façon évidente. Donc $\beta_G(m) \sim n^m \sim e^m$.

d) En considérant le nombre de mots possibles de longueur m sur un alphabet à $2|A|+1$ lettres, il est clair que $\beta_{G,A}(m) \leq (2|A|+1)^m$, donc $\beta_G(m) \preceq e^m$.

e) On choisit une partie génératrice finie A (resp. A') de G (resp. G') stable par inverse et contenant l'élément neutre. Alors $A \times A'$ est une partie génératrice de $G \times G'$, et on a une bijection naturelle $B_{G,A}(m) \times B_{G',A'}(m) \cong B_{G\times G', A\times A'}(m)$, ce qui assure que $\beta_{G\times G'} \sim \beta_G \beta_{G'}$.

f) Il existe une partie génératrice finie A de H. On choisit une partie génératrice finie $B = A \cup A'$ de G. Il est alors clair que $B_{H,A}(m) \subset B_{G,B}(m)$, ce qui assure que $\beta_H \preceq \beta_G$.

On suppose maintenant que H est d'indice fini dans G. On munit G de la distance d_G définie par une partie génératrice finie (fixée) de G. Il est clair que l'action de G sur lui-même par translation est une action par isométries. On note $E \subset G$ un ensemble (fini) de représentants de G modulo H. On note $R := \max\{d_G(e,x) : x \in E\}$. Alors $E \subset B_G(R)$ et $G = \bigcup_{h\in H} B_G(h,R)$, i.e. $G = H.B_G(R)$.

On définit alors l'ensemble fini suivant :

$$S := \{h \in H : B_G(R+1) \cap B_G(h, R+1) \neq \emptyset\}\,.$$

On va montrer que S engendre H et comparer $\beta_{H,S}(m)$ à $\beta_G(m)$.

Pour cela, on pose $r := \min\{d_G(B_G(R), B_G(h,R)) : h \in H \setminus S\}$. Par construction, on a $r > 1$.

Soit $h \in H$. On peut trouver $g_0, \ldots, g_m \in G$ tels que $g_0 = e$, $g_m = h$ et $d_G(g_i, g_{i+1}) = 1$, avec m minimal, i.e. $m = d_G(e,h)$.

Comme $G = \bigcup_{h\in H} B_G(h,R)$, pour tout i, il existe $h_i \in H$ tel que $g_i \in B_G(h_i, R)$, et on peut supposer $h_0 = e$ et $h_m = h$. On a alors

$$d_G(B_G(R), B_G(h_i^{-1}h_{i+1}, R)) = d(B_G(h_I, R), B_G(h_{i+1}, R)) \leq d_G(g_i, g_{i+1}) = 1 < r\,.$$

Cela assure que $s_i := h_i^{-1}h_{i+1} \in S$. On en déduit via une récurrence simple que

$$h = h_m = h_{m-1}h_{m-1}^{-1}h_m = h_{m-1}s_m = s_1 \ldots s_m\,.$$

Cela montre en particulier que $H = \langle S \rangle$, et que $d_{H,S}(e,h) \leq m = d_G(e,h)$

Soit alors $m \in \mathbb{N}$ et $g \in B_G(m)$. On sait qu'il existe alors $h \in H$ tel que $d_G(g,h) \leq R$. Alors $d_G(e,h) \leq R + m$ par inégalité triangulaire. On a montré en outre que $d_{H,S}(e,h) \leq d_G(e,h)$, donc $d_{H,S}(e,h) \leq R+m$. Cela assure que

$$B_G(m) \subset \bigcup_{h\in B_{H,S}(R+m)} B_G(h,R)\,.$$

En calculant les cardinaux, on en déduit que

$$\beta_G(m) \leq |B_G(R)|\beta_{H,S}(R+m)\,,$$

ce qui assure que $\beta_G \preceq \beta_H$, d'où finalement

$$\beta_H \sim \beta_G\,.$$

g) Si A est une partie génératrice finie de G, et si $\pi : G \to H$ est la projection canonique, alors $\pi(A)$ est une partie génératrice finie de H. Il est alors clair que $\pi : B_{G,A}(m) \to B_{H,\pi(A)}(m)$ est une application surjective, ce qui assure que $\beta_H \preceq \beta_G$.

h) C'est un résultat classique que $\mathrm{SL}_2(\mathbb{Z})$ est de type fini. On considère le sous-groupe H de $\mathrm{SL}_2(\mathbb{Z})$ engendré par les matrices $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. Soient alors $r \geq 1$ et $k_1, l_1, \ldots, k_r, l_r \in \mathbb{Z}$ des entiers tous non nuls.
Montrons que $A^{k_1}B^{l_1}\ldots A^{k_r}B^{l_r} \neq I_2$.
Pour cela, on définit par récurrence $M_0 = I_2$, $M_{2i+1} = M_{2i}A^{k_i}$ et $M_{2i+2} = M_{2i+1}B^{r_i}$, et on note $M_{2i} = \begin{pmatrix} m(2i) & * \\ * & * \end{pmatrix}$ et $M_{2i+1} = \begin{pmatrix} * & m(2i+1) \\ * & * \end{pmatrix}$. Une récurrence simple assure que $|m(i)| \geq i+1$ pour tout i. Cela assure immédiatement que le produit $A^{k_1}B^{l_1}\ldots A^{k_r}B^{l_r} \neq I_2$.
Par conséquent, H est isomorphe au groupe libre à deux générateurs A et B (il faut pour cela également regarder des produits de la forme précédente avec $k_1 = 0$ ou $l_r = 0$). Donc $\beta_H(m) \sim e^m$ par la question c). Cela assure que $\beta_G(m) \sim e^m$ grâce aux questions d) et f).

i) voir le polycopié de cours, chaptire I, section 8. Ou alors la preuve de la question j) dans le cas d'un groupe de classe 2.

j) Si G est abélien de type fini et de rang r, alors $\beta_G(m) \sim m^r$ grâce au théorème de classification des groupes abéliens de type fini et au cas de $\mathbb{Z}^r$.
On suppose G nilpotent de classe $c \geq 2$. On considère le sous-groupe $H = D(G)$ de G. Il est clair que H est de type fini, nilpotent de classe $\leq c-1$. Par récurrence, on peut supposer que $\beta_H(m) \preceq m^r$. On prend une partie génératrice finie $A = \{g_1, \ldots g_n\}$ (stable par inverse et contenant e) de G. Soit alors $g \in B_G(m)$. L'élément g s'écrit comme un produit d'au plus m éléments de A. On cherche à regrouper ces éléments pour écrire g sous la forme $g = g_1^{k_1}\ldots g_n^{k_n}d$, avec $d \in H$. Pour ce faire, on constate que $g_ig_j = g_jg_i[g_i^{-1}, g_j^{-1}]$, donc tout échange de deux générateurs produit un commutateur "à droite". On est ensuite amené à échanger ce commutateur avec un autre générateur g_k, ce qui produit un élément de la forme $[g_k^{-1}, [g_i^{-1}, g_j^{-1}]] \in C^2(G)$. On poursuit de cette façon jusqu'à obtenir une écriture de g de la forme $g = g_1^{k_1}\ldots g_n^{k_n}d$ avec $d \in H$: on voit que d est produit d'au plus m^2 éléments $[g_i, g_j]$, d'au plus m^3 éléments $[g_i, [g_j, g_k]]$, etc... finalement, on peut écrire $g = g_1^{k_1}\ldots g_n^{k_n}d$ avec $d \in H$ produit d'au plus $m^2 + \cdots + m^c \leq m^{c+1}$ commutateurs de la forme précédente (commutateurs des g_i). Or tous ces commutateurs sont des mots de longueur bornée k sur un ensemble fini de générateurs de $D(G)$, ce qui assure que $\beta_G(m) = \mathcal{O}(m^n\beta_H(km^{c+1}))$, donc $\beta_G(m) \preceq m^{n+r(c+1)}$. Cela assure donc le résultat.

k) Il est clair que A admet deux valeurs propres réelles λ et λ^{-1}, avec $\lambda > 2$.
Montrons d'abord qu'il existe un vecteur $v \in \mathbb{Z}^2$ tel que pour tout $n \in \mathbb{N}$, les vecteurs $\sum_{i=0}^n \epsilon_i A^i v$ sont deux-à-deux distincts si $(\epsilon_0, \ldots, \epsilon_n)$ décrivent $\{0,1\}^{n+1}$. La matrice transposée de A admet aussi λ pour valeur propre. Donc il existe une forme linéaire $f : \mathbb{R}^2 \to \mathbb{R}$ telle que ${}^tAf = \lambda f$. Il suffit alors de prendre $v \in \mathbb{Z}^2 \setminus \mathrm{Ker}(f)$ (la vérification est laissée au lecteur).
On voit v comme un élément de G, et on note $t = (0,0,1) \in G$. On fixe un ensemble S de générateurs de G contenant v et t. En particulier, pour tout $\underline{\epsilon} \in \{0,1\}^{n+1}$, les éléments $g_{\underline{\epsilon}} := v^{\epsilon_0}(tvt^{-1})^{\epsilon_1}\ldots(t^nvt^{-n})^{\epsilon_n}$ sont des éléments deux-à-deux distincts de G. Donc l'application $\underline{\epsilon} \mapsto g_{\underline{\epsilon}}$ définit une injection de $\{0,1\}^{n+1}$ dans G telle que pour tout $\underline{\epsilon}$, $d_{G,S}(e, g_{\underline{\epsilon}}) \leq 3n+1$. On en déduit donc que pour tout n, $\beta_{G,S}(3n+1) \geq 2^{n+1}$, ce qui implique que $\beta_{G,S}(n) \sim e^n$ grâce à la question d).

Exercice 5 : $\star\star\star$
On note Σ^* l'ensemble des mots (finis) sur l'alphabet $\Sigma = \{0;1\}$, i.e. $\Sigma^* := \bigcup_{n\in\mathbb{N}} \Sigma^n$. On note G le groupe $\mathfrak{S}(\Sigma^*)$. On note $a \in G$ l'élément défini par $a(1m) := 0m$ et $a(0m) := 1m$ pour tout $m \in \Sigma^*$.

a) Montrer que les formules suivantes définissent des éléments b, c et d de G : $b(0m) = 0a(m)$, $c(0m) = 0a(m)$, $d(0m) = 0m$, $b(1m) = 1c(m)$, $c(1m) = 1d(m)$ et $d(1m) = 1b(m)$. On note $\Gamma := \langle a, b, c, d\rangle \subset G$.

b) Montrer que $a^2 = b^2 = c^2 = d^2 = \mathrm{id}$ et que $bc = cb = d$, $cd = dc = b$, $bd = db = c$.

c) Montrer que tout élément de Γ s'écrit comme produit des éléments a, b, c, d, avec un terme du produit sur deux égal à a.

d) Pour tout $n \geq 1$, on note $\Gamma_n := \{\gamma \in \Gamma : \gamma_{|\Sigma^n} = \mathrm{id}\}$. Montrer que Γ_n est un sous-groupe distingué strict d'indice fini de Γ.

e) On définit $\varphi_1 : \Gamma_1 \to G \times G$ par $\varphi_1(\gamma) := (\gamma_0, \gamma_1)$, où $\gamma_\epsilon(w)$ est le mot tel que $\gamma(\epsilon w) = \epsilon\gamma_\epsilon(w)$. Montrer que φ_1 est un morphisme de groupes injectif.

f) Montrer que les morphismes $\varphi^\epsilon : \Gamma_1 \to \Gamma$ définis par $\gamma \mapsto \gamma_\epsilon$ sont surjectifs. En déduire que Γ est infini.

g) Montrer que $\varphi_1(\Gamma_1)$ est un sous-groupe d'indice fini de $\Gamma \times \Gamma$.

h) Montrer que Γ n'est pas à croissance polynomiale, i.e. pour tout $d \geq 0$, $n^d \prec \beta_\Gamma(n)$.

i) Montrer que pour tout $\gamma \in \Gamma_1$, $l(\gamma_0) + l(\gamma_1) \leq l(\gamma) + 1$, où $l(g)$ désigne le nombre minimal de symboles a, b, c, d nécessaires pour écrire g.

j) Pour tout $n \geq 1$, généraliser les contructions précédentes pour obtenir un morphisme injectif $\varphi_n : \Gamma_n \to \Gamma^{\Sigma_n}$ tel que $\varphi_n(\Gamma_n)$ est un sous-groupe d'indice fini de Γ^{X_n}.

k) Montrer que pour tout $\gamma \in \Gamma_3$, si on note $\varphi_3(\gamma) = (\gamma_\epsilon)_{\epsilon\in\Sigma_3}$, alors

$$\sum_{\epsilon\in\Sigma_3} l(\gamma_\epsilon) \leq \frac{5}{6} l(\gamma) + 8\,.$$

l) Montrer que Γ n'est pas à croissance exponentielle, i.e. $\beta_\Gamma(n) \prec e^n$. On dit que Γ est à croissance intermédiaire.

Solution de l'exercice 5.

a) Une récurrence simple sur la longueur des mots de Σ^* assure que les formules indiquées définissent des applications $b, c, d : \Sigma^* \to \Sigma^*$. On vérifie maintenant que ce sont des bijections. Pour cela, on montre que $b^2 = c^2 = d^2 = \mathrm{id}$. On raisonne par récurrence sur la longueur des mots de Σ^*. Il est clair que $b^2(\varepsilon) = c^2(\varepsilon) = d^2(\varepsilon) = \varepsilon$, où ε désigne le mot vide. Soit $m \in \Sigma^*$ un mot de longueur $n \geq 0$. Alors $b^2(0m) = b(0a(m)) = 0a^2(m) = 0m$, $c^2(0m) = c(0a(m)) = 0a^2(m) = 0m$, $d^2(0m) = d(0m) = 0m$. Et on a, par récurrence sur n, $b^2(1m) = b(1c(m)) = 1c^2(m) = 1m$, $c^2(1m) = c(1d(m)) = 1d^2(m) = 1m$ et $d^2(1m) = d(1b(m)) = 1b^2(m) = 1m$. Donc $b^2 = c^2 = d^2 = \mathrm{id}$. Donc $b, c, d \in G$.

b) On a déjà vu que $a^2 = b^2 = c^2 = d^2 = \mathrm{id}$. Montrons les autres relations par récurrence sur la longueur d'un mot $m \in \Sigma^*$. On a en effet

$$bc(0m) = b(0a(m)) = 0a^2(m) = 0m\,,\ cb(0m) = c(0a(m)) = 0a^2(m) = 0m\,,\ d(0m) = 0m\,,$$

et

$$bc(1m) = b(1d(m)) = 1cd(m) = 1b(m)\,,\ cb(1m) = c(1c(m)) = 1dc(m) = 1b(m)\,,\ d(1m) = 1b(m)\,.$$

De même,

$$cd(0m) = c(0m) = 0a(m)\,,\ dc(0m) = d(0a(m)) = 0a(m)\,,\ b(0m) = 0a(m)\,,$$

et

$$cd(1m) = c(1b(m)) = 1db(m) = 1c(m)\,,\ dc(1m) = d(1d(m)) = 1bd(m) = 1c(m)\,,\ b(1m) = 1c(m)\,.$$

Enfin,

$$bd(0m) = b(0m) = 0a(m)\,,\ db(0m) = d(0a(m)) = 0a(m)\,,\ c(0m) = 0a(m)\,,$$

et

$$bd(1m) = b(1b(m)) = 1cb(m) = 1d(m)\,,\ db(1m) = d(1c(m)) = 1bc(m) = 1d(m)\,,\ c(1m) = 1d(m)\,.$$

On conclut donc que $bc = cb = d$, $cd = dc = b$ et $cd = db = c$.

c) C'est une conséquence simple de la question b), via une récurrence (on peut diminuer la longueur d'une écriture d'un élément de Γ comme produit de a, b, c, d dès que deux éléments consécutifs dans ce produit sont distincts de a).

d) On considère l'application $\psi_n : \Gamma \to \mathrm{Aut}(\Sigma^n)$ définie par $\gamma \mapsto \gamma_{|\Sigma^n}$: celle-ci est bien définie car tout élément de Γ envoie Σ^n dans Σ^n car c'est le cas des générateurs de Γ. En outre, ψ_n est un morphisme de groupes, et $\mathrm{Aut}(\Sigma^n)$ est un groupe fini de cardinal $(2^n)!$. Donc $\Gamma_n = \mathrm{Ker}(\psi_n)$ est un sous-groupe distingué de Γ d'indice divisant $(2^n)!$. Et c'est un sous-groupe strict car $a \notin \Gamma_n$.

e) Vérifions que φ_1 est un morphisme de groupes : soient $\gamma, \gamma' \in \Gamma_1$.
Alors $\varphi_1(\gamma \circ \gamma') = ((\gamma \circ \gamma')_0, (\gamma \circ \gamma')_1)$. Et par définition, on a pour tout $m \in \Sigma^*$ et $x \in \{0; 1\}$,

$$(\gamma \circ \gamma')(xm) = \gamma(\gamma'(xm)) = \gamma(x\gamma'_x(m)) = x\gamma_x(\gamma'_x(m)),$$

ce qui assure que $(\gamma \circ \gamma')_x(m) = (\gamma_x \circ \gamma'_x)(m)$, donc φ_1 est un morphisme de groupes.
Montrons son injectivité : soit $\gamma \in \mathrm{Ker}(\varphi_1)$. Alors pour tout $m \in \Sigma^*$ et $x \in \{0; 1\}$, $\gamma(xm) = x\gamma_x(m) = xm$, donc $\gamma = \mathrm{id}$. Donc φ_1 est injectif.

f) On calcule $\varphi_1(b) = (a, c)$, $\varphi_1(c) = (a, d)$ et $\varphi_1(d) = (\mathrm{id}, b)$, puis $\varphi_1(aba) = (c, a)$, $\varphi_1(aca) = (d, a)$ et $\varphi_1(ada) = (b, \mathrm{id})$. Cela assure immédiatement que φ^0 et φ^1 sont surjectifs. Comme Γ_1 est un sous-groupe strict de Γ, cela assure que Γ est infini.

g) On note B le plus petit sous-groupe distingué de Γ contenant b. Alors on vérifie que $\langle a, d\rangle$ se surjecte sur Γ/B via la projection $\Gamma \to \Gamma/B$. Or il est clair que $\langle a, d\rangle \cong D_4$, donc $[\Gamma : B]$ divise 8.
Pour $\gamma \in \Gamma$, la question précédente assure qu'il existe $g, g' \in \Gamma_1$ tels que $\varphi^0(g) = \varphi^1(g') = \gamma$. Alors un calcul simple assure que $\varphi_1(gadag^{-1}) = (\gamma b\gamma^{-1}, \mathrm{id})$ et $\varphi_1(g'dg'^{-1}) = (\mathrm{id}, \gamma b\gamma^{-1})$. Donc $B \times \{\mathrm{id}\}$ et $\{\mathrm{id}\} \times B$ sont contenus dans $\varphi_1(\Gamma_1)$. Donc $B \times B \subset \varphi_1(\Gamma_1)$. Donc $[\Gamma \times \Gamma : \varphi_1(\Gamma_1)]$ divise $[\Gamma \times \Gamma : B \times B] = [\Gamma : B]^2 = 64$, donc $\varphi_1(\Gamma_1)$ est un sous-groupe d'indice fini (divisant 64) de $\Gamma \times \Gamma$.

h) Les questions d) et g) assurent que Γ et $\Gamma \times \Gamma$ admettent des sous-groupes d'indice fini isomorphes (à Γ_1), donc l'exercice 4, question f) assure que $\beta_\Gamma \sim \beta_{\Gamma\times\Gamma} \sim {\beta_\Gamma}^2$. Supposons alors qu'il existe $k \in \mathbb{N}^*$ (que l'on peut supposer minimal) tel que $\beta_\Gamma(m) \preceq m^k$. Alors on aurait $\beta_\Gamma(m)^2 \sim \beta_\Gamma(m) \preceq m^k$, donc $\beta_\Gamma(m) \preceq m^{\frac{k}{2}}$, donc par minimalité, on aurait $k = 1$ et $\beta_\Gamma(m) \sim m$ (car Γ est infini). Alors $\beta_\Gamma(m) \sim {\beta_\Gamma}^2(m) \sim m^2$, ce qui est contradictoire. Donc Γ n'est pas à croissance polynomiale.

i) Soit $\gamma \in \Gamma_1$. La question c) assure que γ s'écrit sous l'une des quatre formes suivantes (et on peut supposer cette écriture minimale) :

$$\gamma = a * a * \cdots * a * a,$$

$$\gamma = a * a * \cdots * a*,$$

$$\gamma = *a * \cdots * a * a$$

ou

$$\gamma = *a * \cdots * a*,$$

où les symboles $*$ désignent des éléments de l'ensemble $\{b, c, d\}$.
Alors les morphismes φ^ϵ appliqués à ces décompositions s'écrivent explicitement via les règles suivantes (que l'on démontre par récurrence sur la longueur de γ) :

(I) $\varphi^0(\gamma) = \gamma_0$ s'obtient en remplaçant les a par id et en remplaçant chaque symbole $*$ suivant la règle : si $*$ vient après un nombre impair de symboles a, alors $* = b$ est remplacé par a, $* = c$ par a et $* = d$ par id ; si $*$ vient après un nombre pair de symboles a, alors $* = b$ est remplacé par c, $* = c$ par d et $* = d$ par b.

(II) $\varphi^1(\gamma) = \gamma_1$ s'obtient en remplaçant les a par id et en remplaçant chaque symbole $*$ suivant la règle : si $*$ vient après un nombre pair de symboles a, alors $* = b$ est remplacé par a, $* = c$ par a et $* = d$ par id ; si $*$ vient après un nombre impair de symboles a, alors $* = b$ est remplacé par c, $* = c$ par d et $* = d$ par b.

En appliquant ces règles, on voit facilement que dans chacun des quatre types de décomposition mentionnés, on a toujours

$$l(\gamma_0) + l(\gamma_1) \leq l(\gamma) + 1\,.$$

j) Il suffit de considérer l'application $\varphi_n : \Gamma_n \to \Gamma^{\Sigma_n}$ définie de la façon suivante : pour tout $\gamma \in \Gamma_n$, pour tout $\epsilon \in \Sigma^n$, pour tout $m \in \Sigma^*$, $\gamma(\epsilon m)$ est un mot de la forme $\epsilon\gamma_\epsilon(m)$, et on pose alors $\varphi_n(\gamma) = (\gamma_\epsilon)_{\epsilon\in\Sigma^n}$. On adapte alors la preuve de la question g) pour montrer que $\varphi_n(\Gamma_n)$ est d'indice fini dans Γ^{Σ^n}.

k) Il s'agit de raffiner l'argument de la question i). Étant donné $\gamma \in \Gamma_3$, le calcul de $\varphi_3(\gamma) = (\gamma_\epsilon)$ se fait en appliquant, à une écriture minimale de γ, trois fois les règles (I) et (II) énoncées dans la réponse à la question i). À chaque application de l'une de ces règles, on constate que la longueur de γ est diminuée de $l_d(\gamma) - 1$, où $l_d(\gamma)$ est le nombre de symboles d dans l'écriture de γ considérée ; et en outre, chaque lettre c de γ produit une lettre d après application de la règle (I) ou (II), laquelle lettre sera supprimée à l'application suivante d'une des deux règles. Et chaque lettre b de γ fournit une lettre c après la première application d'une des deux règles, laquelle lettre c fournit une lettre d à la deuxième application, laquelle lettre d disparaît à la troisième application. Or l'une des lettre b, c, d apparaît strictement plus que $\frac{l(\gamma)}{6} - 1$ fois dans l'écriture de γ, donc la conjonction de la question i) avec les remarques précédentes aboutit à l'estimation souhaitée :

$$\sum_{\epsilon\in\Sigma_3} l(\gamma_\epsilon) \leq \frac{5}{6} l(\gamma) + 8\,.$$

l) On a donc montré que pour tout $\gamma \in \Gamma_3$, on a

$$\sum_{\epsilon\in\Sigma_3} l(\gamma_\epsilon) \leq \frac{5}{6} l(\gamma) + 8\,.$$

Cela implique que

$$\beta_{\Gamma_3}(m) \leq \sum_{\substack{(n_1,\ldots,n_8)\in\mathbb{N}^8 \\ \sum_i n_i \leq \frac{5}{6}m+8}} \beta_\Gamma(n_1)\ldots\beta_\Gamma(n_8)\,.$$

On pose alors $\lambda := \lim_{n\to+\infty} \sqrt[n]{\beta_\Gamma(n)}$ (on vérifiera que cette limite existe). Supposant $\lambda > 1$, l'inégalité précédente implique après quelques calculs que $\lambda \leq \lambda^{\frac{5}{6}}$, ce qui est contradictoire. Donc $\lambda \leq 1$, ce qui assure que $\beta_\Gamma(n) \prec e^n$.

TD6 : groupe linéaire, homographies, simplicité

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆

a) Soit K un corps et soit E un K-espace vectoriel de dimension finie. Rappeler pourquoi $\mathrm{PGL}(E)$ agit fidèlement sur $\mathbb{P}(E)$.

b) Soit q une puissance d'un nombre premier et $n \geq 2$. Construire un morphisme de groupes injectif canonique $\mathrm{PGL}_n(\mathbb{F}_q) \to \mathfrak{S}_N$ avec $N := \frac{q^n-1}{q-1}$.

c) Identifier les groupes $\mathrm{PGL}_n(\mathbb{F}_q)$ et $\mathrm{PSL}_n(\mathbb{F}_q)$ pour $n = 2$ et $q = 2, 3, 4, 5$.

d) Montrer que $\mathrm{PSL}_2(\mathbb{F}_5)$ est isomorphe à $\mathrm{PGL}_2(\mathbb{F}_4)$.

Solution de l'exercice 1.

a) voir cours.

b) La question a) assure que l'on a un morphisme de groupes injectif $\varphi : \mathrm{PGL}(\mathbb{F}_q^n) \to \mathfrak{S}(\mathbb{P}^{n-1}(\mathbb{F}_q))$. Or par définition on a $\mathbb{P}^{n-1}(\mathbb{F}_q) = (\mathbb{F}_q^n \setminus \{0\})/\mathbb{F}_q^*$, donc on déduit facilement que $|\mathbb{P}^{n-1}(\mathbb{F}_q)| = \frac{|\mathbb{F}_q^n|}{|\mathbb{F}_q^*|} = \frac{q^n-1}{q-1} =: N$. Par conséquent, on a bien un morphisme de groupes injectif

$$\varphi : \mathrm{PGL}_n(\mathbb{F}_q) \to \mathfrak{S}_N \,.$$

On peut donner une autre preuve, plus géométrique, par récurrence sur n : on sait que l'espace projectif $\mathbb{P}^{n-1}(K)$ est réunion disjointe d'un espace affine de dimension $n-1$ sur K (disons K^n) et d'un hyperplan projectif de dimension $n-2$ (i.e. isomorphe à $\mathbb{P}^{n-2}(K)$), appelé hyperplan à l'infini. On a donc $\mathbb{P}^{n-1}(K) = K^{n-1} \sqcup \mathbb{P}^{n-2}(K)$, dont on déduit par récurrence la formule suivante :

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

c) Pour $n = 2$, le morphisme φ de la question précédente est de la forme

$$\varphi : \mathrm{PGL}_2(\mathbb{F}_q) \to \mathfrak{S}_{q+1} \,,$$

avec $|\mathrm{PGL}_2(\mathbb{F}_q)| = (q-1)q(q+1)$ et $|\mathfrak{S}_{q+1}| = (q+1)!$.

i) Si $q = 2$ ou 3, les deux cardinaux sont égaux, ce qui assure que φ est un isomorphisme. Donc $\mathrm{PGL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$ et $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$. En outre, $\mathrm{PSL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2)$, donc $\mathrm{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$. On vérifie aussi que $\mathrm{PSL}_2(\mathbb{F}_3) \subset \mathrm{PGL}_2(\mathbb{F}_3)$ est un sous-groupe d'indice 2, donc $\mathrm{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$.

ii) Si $q = 4$, on a $\mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{PGL}_2(\mathbb{F}_4) \subset \mathfrak{S}_5$ est un sous-groupe d'indice 2, ce qui assure que $\mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{PGL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$, l'unique groupe simple d'ordre 60.

iii) Si $q = 5$, les cardinaux assurent que $\mathrm{PGL}_2(\mathbb{F}_5) \subset \mathfrak{S}_6$ est un sous-groupe d'indice 6. Or un résultat classique assure qu'un tel sous-groupe est isomorphe à $\mathfrak{S}_5$ (voir TD1, exercice 20). Et $\mathrm{PSL}_2(\mathbb{F}_5) \subset \mathrm{PGL}_2(\mathbb{F}_5)$ est un sous-groupe d'indice 2, ce qui assure que $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$ et $\mathrm{PSL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$.

d) On a vu à la question précédente que ces deux groupes sont isomorphes à $\mathfrak{A}_5$. C'est l'unique groupe (à isomorphisme près) simple d'ordre 60.

Exercice 2 : ⋆

a) Soit p un nombre premier. Montrer que la réduction modulo p des coefficients d'une matrice induit un morphisme de groupes $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ qui est surjectif.

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

c) Soit $N \geq 3$. Montrer que le noyau du morphisme de réduction $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/N\mathbb{Z})$ est sans torsion.

Solution de l'exercice 2.

a) Si $M \in \mathrm{SL}_n(\mathbb{Z})$, le déterminant de sa réduction modulo p est encore 1 car l'expression du déterminant est la même quel que soit le corps. La réduction modulo p d'un produit est bien le produit des réductions car l'expression du produit de deux matrices est la même quel que soit le corps. Donc $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ est bien défini et c'est un morphisme de groupes.
Toute matrice élémentaire $I_n + E_{ij}$ de $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ est l'image de la matrice $I_n + E_{ij} \in \mathrm{SL}_n(\mathbb{Z})$. Comme les matrices élémentaires engendrent $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z}) = \mathrm{SL}_n(\mathbb{F}_p)$, le morphisme de réduction est surjectif.

b) Soit $N \geq 2$. On décompose N en facteurs premiers : $N = \prod_{i=1}^n p_i^{\alpha_i}$, avec les p_i premiers deux-à-deux distincts. Alors le lemme chinois assure que l'application naturelle de réduction

$$\mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z}) \to \prod_i^n \mathrm{SL}_n(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$$

est un isomorphisme de groupes, compatible aux morphismes naturels $\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{SL}_n(\mathbb{Z}/N\mathbb{Z})$ et $\mathrm{SL}_n(\mathbb{Z}) \to \prod_i^n \mathrm{SL}_n(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$. Cela assure, via la preuve de la question précédente, qu'il suffit de montrer que pour p premier et $\alpha \geq 1$, $\mathrm{SL}_n(\mathbb{Z}/p^\alpha\mathbb{Z})$ est engendré par les matrices élémentaires. Pour cela, on adapte la démonstration du cas de $\mathrm{SL}_n(K)$, où K est un corps. Soit en effet $M \in \mathrm{SL}_n(\mathbb{Z}/p^\alpha\mathbb{Z})$. Puisque le déterminant de M vaut 1 modulo p^α, le développement par rapport à la première ligne assure qu'il existe un coefficient de la première ligne de M qui n'est pas divisible par p, donc qui est inversible dans $\mathbb{Z}/p^\alpha\mathbb{Z}$. On utilise cet élément inversible comme pivot, et la preuve du cas des corps fonctionne (récurrence sur la taille de la matrice).

c) Soit $A \in \mathrm{GL}_n(\mathbb{Z})$ d'ordre fini r dans le noyau de ce morphisme. Alors $A^r = I_n$, ce qui assure que A est annulée par le polynôme $X^r - 1$. Comme ce polynôme est scindé à racines simples dans $\mathbb{C}$, A est diagonalisable dans $\mathbb{C}$, et ses valeurs propres $\lambda_1, \ldots, \lambda_n$ sont des racines de l'unité dans $\mathbb{C}$. Et par hypothèse, il existe une matrice $B \in \mathrm{Mat}_n(\mathbb{Z})$ telle que $A = I_n + N.B$. Un calcul simple assure que $\chi_A(X) = N^n \chi_B\left(\frac{X-1}{N}\right)$.
Donc $\chi_A(1) = N^n \chi_B(0)$, avec $\chi_B(0) \in \mathbb{Z}$. Et $\chi_A(X) = \prod_{i=1}^n (X - \lambda_i)$, donc $|\chi_A(1)| = \prod_{i=1}^n |1 - \lambda_i| \leq 2^n$. On a donc $\chi_B(0) \in \mathbb{Z}$ et $|\chi_B(0)| N^n \leq 2^n$, avec $N \geq 3$. Donc nécessairement $\chi_B(0) = 0$, donc $\chi_A(1) = 0$. Donc on peut supposer que $\lambda_1 = 1$. Donc A admet un vecteur propre dans $\mathbb{Q}^n$ pour la valeur propre $\lambda_1 = 1$. Quitte à multiplier par un rationnel bien choisi, on peut supposer ce vecteur propre dans $\mathbb{Z}^n$, avec les coordonnées premières entre elles. Alors A est semblable dans $\mathrm{GL}_n(\mathbb{Z})$ à une matrice de la forme

$$A \sim \begin{pmatrix} 1 & * \\ 0 & A' \end{pmatrix}$$

avec $A' \in \mathrm{GL}_{n-1}(\mathbb{Z})$. Par construction, A' vérifie les mêmes hypothèses que A, donc A' admet également 1 pour valeur propre, et on conclut par récurrence sur n que $A = I_n$.

Exercice 3 : $\star$
On note $G := \mathrm{PSL}_3(\mathbb{F}_4)$ et $H := \mathrm{PSL}_4(\mathbb{F}_2)$.

a) Montrer que G et H ont même cardinal.

b) Montrer que H contient deux classes de conjugaison distinctes formées d'éléments d'ordre 2.

c) Montrer que tout élément d'ordre 2 dans G est la classe d'une transvection de $\mathbb{F}_4^3$.

d) Montrer que G et H ne sont pas isomorphes.

Solution de l'exercice 3.

a) On voit facilement que G et H sont de cardinal 20160.

b) On considère les deux matrices suivantes dans H :

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Il est clair que A et B sont des élément de H d'ordre 2. Or $A - I_4$ est de rang 1 alors que $B - I_4$ est de rang 2, donc A et B ne sont pas conjugués dans H.

c) Soit $\overline{A} \in G$ d'ordre 2. On note $A \in \mathrm{SL}_3(\mathbb{F}_3)$ un relevé de A. Alors $A^2 = \alpha I_3$, avec $\alpha \in \mathbb{F}_4^*$. Donc A est annulée par $X^2 - \alpha = (X - \alpha^2)^2 \in \mathbb{F}_4[X]$, ce qui assure que A est trigonalisable, donc A est semblable à une matrice de la forme

$$A' = \begin{pmatrix} \alpha^2 & a & b \\ 0 & \alpha^2 & c \\ 0 & 0 & \alpha^2 \end{pmatrix},$$

avec $a, b, c \in \mathbb{F}_4$ non tous nuls. On peut en outre supposer que $\alpha = 1$. La condition $A^2 = I_3$ équivaut à $ac = 0$, ce qui assure que $a = 0$ ou $c = 0$. Donc A est semblable à l'une des deux matrices suivantes

$$A' = \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Donc on voit facilement qu'une telle matrice A est une matrice de transvection dans $\mathrm{SL}_3(\mathbb{F}_4)$. Or en dimension $n \geq 3$, les transvections sont toutes conjuguées dans $\mathrm{SL}_n(K)$. Cela assure que G admet une unique classe de conjugaison formée d'éléments d'ordre 2.

d) Puisqu'un isomorphisme de groupes envoie les classes de conjugaison sur les classes de conjugaison et respecte l'ordre des éléments, les questions b) et c) assurent que G et H ne sont pas isomorphes. Ce sont donc deux groupes simples non isomorphes de même cardinal. On peut montrer que 2160 est le plus petit entier n tel qu'il existe deux groupes simples non isomorphes de cardinal n.

Exercice 4 : $\star\star$

Soit K un corps et soit E un K-espace vectoriel de dimension 2. Soit $\mathcal{T}$ l'ensemble des classes de conjugaisons sous $\mathrm{SL}(E)$ des transvections de E. On fixe une base de E et, pour $a \in K^*$, on note T_a la transvection de matrice $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ dans cette base.

a) Montrer que T_a et T_b sont conjuguées si et seulement si ab^{-1} est un élément de K^{*2}.

b) En déduire une bijection entre K^*/K^{*2} et $\mathcal{T}$.

c) Que dire de plus si $K = \mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{F}_p$?

Solution de l'exercice 4.

a) Pour toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K)$, pour tout $x \in K^*$, on a

$$AT_xA^{-1} = \begin{pmatrix} 1 - acx & a^2x \\ -c^2x & 1 - bc \end{pmatrix}.$$

Donc pour $x, y \in K^*$, les matrices T_x et T_y sont conjuguées dans $\mathrm{SL}_2(K)$ si et seulement s'il existe $a, b, d \in K$ tels que $ad = 1$ et $y = a^2x$ si et seulement s'il existe $a \in K^*$ tel que $y = a^2x$ si et seulement si $yx^{-1} \in (K^*)^2$.

b) On définit l'application $\begin{array}{ccc} \psi : K^\times & \to & \mathcal{T} \\ x & \mapsto & [T_x] \end{array}$, où $[T]$ désigne la classe de similitude de l'endomorphisme T. Elle est surjective car toute transvection de E a pour matrice T_y pour un certain $y \in K^*$, dans une base (e_1, e_2) bien choisie. La question a) assure que ψ passe au quotient par $(K^*)^2$ et induit la bijection souhaitée.

c) Pour $\mathbb{C}$, $\mathcal{T}$ est un singleton car tout élément est un carré ; donc toutes les transvections sont conjuguées dans $\mathrm{SL}_2(\mathbb{C})$. Pour $\mathbb{R}$ ou $\mathbb{F}_p$, $\mathcal{T}$ est un ensemble à 2 éléments. Pour $\mathbb{Q}$, $\mathcal{T}$ est infini, puisque $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ est en bijection avec l'ensemble des entiers relatifs sans facteur carré.

Exercice 5 : $\star\star$

Soit $n \geq 1$. On note $\mathrm{Int}(\mathfrak{S}_n)$ le sous-groupe des automorphismes intérieurs de $\mathrm{Aut}(\mathfrak{S}_n)$.

a) Soit $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$ tel que ϕ transforme toute transposition en une transposition. Montrer que ϕ est intérieur.

b) Soit $\sigma \in \mathfrak{S}_n$. Déterminer le cardinal du commutant $Z(\sigma) := \{\tau \in \mathfrak{S}_n \mid \tau\sigma\tau^{-1} = \sigma\}$ de σ.

c) En déduire que si $n \neq 6$, on a $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$.

d) Soit $n \geq 5$ tel que $\mathrm{Int}(\mathfrak{S}_n) = \mathrm{Aut}(\mathfrak{S}_n)$. Montrer que tous les sous-groupes d'indice n de $\mathfrak{S}_n$ sont conjugués.

e) En utilisant les 5-Sylow de $\mathfrak{S}_5$, montrer qu'il existe un sous-groupe H d'indice 6 de $\mathfrak{S}_6$ opérant transitivement sur $\{1, \ldots, 6\}$.

f) Construire géométriquement un sous-groupe H' d'indice 6 dans $\mathfrak{S}_6$ vérifiant les mêmes propriétés que H.

g) En déduire que $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Solution de l'exercice 5.

a) On peut supposer $n \geq 4$, puisque tout automorphisme de $\mathfrak{S}_i$ pour $i \leq 3$ étant intérieur (le vérifier). Le groupe symétrique $\mathfrak{S}_n$ est engendré par les transpositions $\tau_i = (1\, i)$ pour $i \geq 2$. Puisque τ_i et τ_j ne commutent pas si $i \neq j$, les supports des transpositions $\varphi(\tau_i)$ et $\varphi(\tau_j)$ ont exactement un point en commun, que l'on notera α_1. Comme $\varphi(\tau_i)$ a un point commun avec $\varphi(\tau_1)$, $\varphi(\tau_2)$ et $\varphi(\tau_3)$, il ne peut en tre autrement : tous ont α_1 en commun. On écrit alors $\varphi(\tau_i) = (\alpha_1\ \alpha_i)$. On a ensuite $\{\alpha_1, \ldots, \alpha_n\} = \{1, \ldots, n\}$ par injectivité de φ. On définit alors la permutation $\alpha \in \mathfrak{S}_n$ par $\alpha(i) = \alpha_i$ pour tout i : il est alors clair que φ est la conjugaison par α, donc $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$.

b) Décomposons σ en produit de cycles à supports disjoints, k_1 cycles de longueur 1, ..., k_n cycles de longueur n, avec $n = \sum_i i k_i$. Un élément qui commute à σ doit préserver la décomposition en cycles de σ, et donc envoyer le support d'un k-cycle sur celui d'un autre k-cycle, en respectant l'ordre cyclique du support de ces cycles, pour tout k. Ainsi le commutant d'un n-cycle de $\mathfrak{S}_n$ est-il par exemple composé des puissances de ce dernier. En mettant ceci bout à bout, on prouve que l'on a

$$|Z(\sigma)| = \prod_i k_i! i^{k_i}.$$

c) Soit φ un automorphisme de $\mathfrak{S}_n$. Si τ est une transposition de $\mathfrak{S}_n$, $\varphi(\tau)$ est aussi d'ordre 2 et est donc un produit de k transpositions à supports disjoints. Or on a $|Z(\tau)| = |Z(\varphi(\tau))|$, ce qui se réécrit $2(n-2)! = 2^k k!(n-2k)!$. Comme on a $n \neq 6$, on voit que ceci impose $k = 1$. Par la question b), φ est alors intérieur.

d) Soit $H \subset \mathfrak{S}_n$ un sous-groupe d'indice n. L'action transitive de $\mathfrak{S}_n$ sur $\mathfrak{S}_n/H$ induit un morphisme de groupes $\phi : \mathfrak{S}_n \to \mathfrak{S}(\mathfrak{S}_n/H) \cong \mathfrak{S}_n$. Alors $\mathrm{Ker}(\phi)$ est un sous-groupe distingué de $\mathfrak{S}_n$, c'est donc $\{\mathrm{id}\}$, $\mathfrak{A}_n$ ou $\mathfrak{S}_n$. Puisque $\mathrm{Ker}(\phi)$ agit trivialement sur la classe de H dans $\mathfrak{S}_n/H$, on a $\mathrm{Ker}(\phi) \subset H$, donc $\mathrm{Ker}(\phi) = \{\mathrm{id}\}$, i.e. ϕ est injective. Donc $\phi \in \mathrm{Aut}(\mathfrak{S}_n)$. Par hypothèse, il existe $\sigma \in \mathfrak{S}_n$ tel que ϕ soit la conjugaison par σ. Or par construction ϕ envoie H sur le stabilisateur d'un point (la classe de H) dans $\mathfrak{S}(\mathfrak{S}_n/H) \cong \mathfrak{S}_n$. Enfin, dans $\mathfrak{S}_n$, il est clair que les stabilisateurs d'un point de $\{1, \ldots, n\}$ sont tous conjugués.

e) Les théorèmes de Sylow assurent que $\mathfrak{S}_5$ admet un ou six 5-Sylow. La simplicité de $\mathfrak{A}_5$ assure que $\mathfrak{S}_5$ n'admet pas de sous-groupe distingué d'ordre 5, donc $\mathfrak{S}_5$ admet exactement six 5-Sylow. Notons X l'ensemble des 5-Sylow de $\mathfrak{S}_5$. L'action de $\mathfrak{S}_5$ sur X par conjugaison est transitive, et induit un morphisme de groupes $\mu : \mathfrak{S}_5 \to \mathfrak{S}(X) \cong \mathfrak{S}_6$ dont le noyau est trivial (car on connaît les sous-groupes distingués de $\mathfrak{S}_5$). On note alors $H := \mu(\mathfrak{S}_5) \subset \mathfrak{S}_6$.

f) Le groupe $H' = \mathrm{PGL}_2(\mathbb{F}_5)$, vu comme sous-groupe de $\mathfrak{S}_6$ par action sur $\mathbb{P}^1(\mathbb{F}_5)$ (voir exercice 1), n'est pas conjugué à $\mathfrak{S}_5 = \mathrm{Stab}(6) \subset \mathfrak{S}_6$ puisqu'il ne fixe aucun point.

g) Les questions d) et e) (ou f)) assurent que le groupe $\mathfrak{S}_6$ possède au moins un automorphisme extérieur.

Exercice 6 : $\star\star$

Soit K un corps.

a) Montrer que l'action de $\mathrm{PGL}_2(K)$ sur $\mathbb{P}^1(K)$ est 3-transitive. Est-elle 4-transitive ?

b) Pour $n = 1, 2, 3$, décrire le quotient $\mathbb{P}^1(K)^{[n]}/\mathrm{PGL}_2(K)$ (i.e. l'ensemble des orbites) où $\mathbb{P}^1(K)^{[n]}$ désigne l'ensemble des n-uplets de points deux-à-deux distincts de $\mathbb{P}^1(K)$.

c) Montrer que l'on a une bijection naturelle $(\mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K))/\mathrm{PGL}_2(K) \to \mathbb{P}^1(K)$. Cette bijection est notée $(a, b, c, d) \mapsto [a, b, c, d]$ et $[a, b, c, d]$ est appelé le birapport des points a, b, c, d.

d) Expliciter la bijection précédente via l'identification $\mathbb{P}^1(K) \cong K \cup \{\infty\}$.

Solution de l'exercice 6.

a) Soient $(x_1, x_2, x_3) \in \mathbb{P}^1(K)^3$ et $(y_1, y_2, y_3) \in \mathbb{P}^1(K)^3$ deux triplets de points de $\mathbb{P}^1(K)$ deux-à-deux distincts. Par définition, il existe des vecteurs non nuls $u_i \in K^2$ et $v_i \in K^2$, définis à un scalaire près, tels que x_i est la classe de u_i et y_i celle de v_i dans $\mathbb{P}^1(K)$. Les points initiaux étant deux-à-deux distincts, cela assure que les vecteurs u_i (resp. v_i) sont deux-à-deux non proportionnels. En particulier, il existe des scalaires λ_i et μ_i non nuls tels que $u_3 = \lambda_1 u_1 + \lambda_2 u_2$ et $v_3 = \mu_1 v_1 + \mu_2 v_2$. Quitte à remplacer u_i par $\lambda_i u_i$ et v_i par $\mu_i v_i$, on peut supposer que $\lambda_i = \mu_i = 1$. Comme (u_1, u_2) et (v_1, v_2) sont des bases de K^2, il existe $g \in \mathrm{GL}(K^2)$ telle que $g(u_i) = v_i$ pour $i = 1$ et 2. Alors par linéarité, on a $g(u_3) = v_3$. Si on note h l'image de g dans $\mathrm{PGL}_2(K)$, on a $h(x_i) = y_i$ pour $i = 1, 2, 3$. Cela assure que l'action de $\mathrm{PGL}_2(K)$ sur $\mathbb{P}^1(K)$ est 3-transitive.

En revanche, elle n'est pas 4-transitive si $K \neq \mathbb{F}_2, \mathbb{F}_3$: on voit facilement qu'un élément de $\mathrm{PGL}_2(K)$ est complétement déterminé par les images de trois points distincts de $\mathbb{P}^1(K)$: une application linéaire de K^2 qui a trois droites propres distinctes est une homothétie.

b) La question a) assure que $\mathbb{P}^1(K)^{[n]}/\mathrm{PGL}_2(K)$ est réduit à un point si $n = 1, 2, 3$, i.e. l'action de $\mathrm{PGL}_2(K)$ sur $\mathbb{P}^1(K)^{[n]}$ a une seule orbite.

c) On définit une application $\varphi : \mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ par $\varphi(x_1, x_2, x_3, x_4) := h(x_4)$, où $h \in \mathrm{PGL}_2(K)$ est l'unique homographie de $\mathbb{P}^1(K)$ telle que $h(x_1) = \infty$, $h(x_2) = 0$ et $h(x_3) = 1$. Cette application est bien définie (voir solution de la question a)). Elle est surjective car $\varphi(\infty, 0, 1, x) = x$ pour tout $x \in \mathbb{P}^1(K)$.

Soient $(x_i) \in \mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K)$ et $g \in \mathrm{PGL}_2(K)$. Si $h \in \mathrm{PGL}_2(K)$ est définie par $h(x_1) = \infty$, $h(x_2) = 0$ et $h(x_3) = 1$, alors $\varphi(x_i) = h(x_4)$, et on voit que $h \circ g^{-1}$ envoie le triplet $(g(x_1), g(x_2), g(x_3))$ sur le triplet $(\infty, 0, 1)$, ce qui assure que $\varphi(g(x_i)) = h \circ g^{-1}(g(x_4)) = h(x_4) = \varphi(x_i)$. Donc φ passe au quotient par $\mathrm{PGL}_2(K)$ et induit une application surjective $\overline{\varphi} : (\mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K))/\mathrm{PGL}_2(K) \to \mathbb{P}^1(K)$.

Soient (x_i) et (y_i) dans $\mathbb{P}^1(K)^{[3]} \times \mathbb{P}^1(K)$. On a $\varphi(x_1, x_2, x_3, x_4) = \varphi(y_1, y_2, y_3, y_4)$ si et seulement $h(x_4) = g(y_4)$ où h (resp. g) est l'unique élément de $\mathrm{PGL}_2(K)$ tel que $h(x_1) = \infty$, $h(x_2) = 0$ et $h(x_3) = 1$ (resp. $g(y_1) = \infty$, $g(y_2) = 0$ et $g(y_3) = 1$). Alors l'homographie $g^{-1} \circ h$ envoie x_i sur y_i pour $i = 1, 2, 3, 4$. Cela assure que l'application $\overline{\varphi}$ est une bijection.

d) On identifie $\mathbb{P}^1(K)$ avec $K \cup \infty$. Soient $x_i \in K \cup \{\infty\}$ tels que x_1, x_2, x_3 sont deux-à-deux distincts. Si $x_1, x_2, x_3 \neq \infty$, on vérifie que l'application $h : K \cup \infty \to K \cup \infty$ définie par $x \mapsto \frac{x_3 - x_1}{x_2 - x_1} \frac{x - x_2}{x - x_1}$ (avec les conventions usuelles) envoie le triplet (x_1, x_2, x_3) sur le triplet $(\infty, 0, 1)$, et

que h coïncide avec l'homographie $h' \in \mathrm{PGL}_2(K)$ définie par la matrice $\begin{pmatrix} x_3-x_1 & -x_2(x_3-x_1) \\ x_2-x_1 & -x_1(x_2-x_1) \end{pmatrix} \in \mathrm{GL}_2(K)$, ce qui assure que $\varphi(x_i) = h(x_4)$, i.e.

$$\varphi(x_i) = \frac{x_3-x_1}{x_2-x_1}\frac{x_4-x_2}{x_4-x_1}\,.$$

Si $x_1 = \infty$, on considère $h : x \mapsto \frac{x-x_2}{x_3-x_2}$ et on vérifie que c'est une homographie envoyant (x_i) sur $(\infty, 0, 1)$, ce qui redonne la même formule pour $\varphi(x_i)$ avec les convientions usuelles. De même, si $x_2 = \infty$, on considère $h : x \mapsto \frac{x_3-x_1}{x-x_1}$, qui redonne la même formule, et si $x_3 = \infty$, on considère $h : x \mapsto \frac{x-x_2}{x-x_1}$, qui redonne encore une fois la même formule.
Finalement, dans tous les cas, on a bien

$$\varphi(x_i) = \frac{x_3-x_1}{x_2-x_1}\frac{x_4-x_2}{x_4-x_1}\,.$$

Exercice 7 :

a) Montrer que le groupe $\mathrm{PSL}_2(\mathbb{Z})$ agit naturellement sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

b) Montrer que cette action est fidèle. Identifier le stabilisateur de $i \in \mathcal{H}$.

c) Soit G un groupe agissant sur un espace topologique X. Une partie F de X est appelée *domaine fondamental* pour l'action de G sur X si elle vérifie :

$$\text{(i) } \overline{F^\circ} = F, \quad \text{(ii) } X = \bigcup_{h\in G} hF, \quad \text{(iii) } \forall g \in G\setminus\{1\},\ F^\circ \cap (gF)^\circ = \emptyset.$$

Soit $D = \{z \in \mathcal{H} \ : \ |\mathrm{Re}(z)| \le \frac{1}{2}, |z| \ge 1\}$.

i) En maximisant la partie imaginaire des éléments d'une orbite $\mathrm{PSL}_2(\mathbb{Z})\cdot z$, montrer que D vérifie la propriété (ii).

ii) Montrer que D est un domaine fondamental pour l'action de $\mathrm{PSL}_2(\mathbb{Z})$ sur $\mathcal{H}$.

iii) En déduire que les matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ engendrent $\mathrm{SL}_2(\mathbb{Z})$.

Solution de l'exercice 7.

a) On considère l'action usuelle de $\mathrm{PGL}_2(\mathbb{C})$ sur $\mathbb{C}\cup\{\infty\} = \mathbb{P}^1(\mathbb{C})$ par homographie, via la formule

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

On vérifie facilement que pour tout $z \in \mathcal{H}$, et tout $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$, on a $A\cdot z \in \mathbb{C}$ et

$$\mathrm{Im}\,(A\cdot z) = \frac{\mathrm{Im}\,(z)}{|cz+d|^2}\,,$$

ce qui assure que $A\cdot z \in \mathcal{H}$. D'où l'action recherchée.

b) Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$. On a

$$A\cdot i = i \Leftrightarrow a = d \text{ et } b = -c \Leftrightarrow A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ ou } A = I_2\,.$$

On note $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Alors $\mathrm{Stab}(i) = \{I_2, S\} \cong \mathbb{Z}/2\mathbb{Z}$.

En outre, comme pour tout $z \in \mathcal{H}$, on a $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\cdot z = \frac{-1}{z}$, on voit que la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ne fixe pas le point $z = 1+i \in \mathcal{H}$, ce qui assure que l'action de $\mathrm{PSL}_2(\mathbb{Z})$ sur $\mathcal{H}$ est fidèle.

c) i) Soit $z \in \mathcal{H}$. On considère l'orbite $\mathrm{PSL}_2(\mathbb{Z}) \cdot z$ de z, et on note $X := \{z' \in \mathrm{PSL}_2(\mathbb{Z}) \cdot z : \mathrm{Im}\,(z') \geq \mathrm{Im}\,(z)\}$. On a vu que pour tout $A \in \mathrm{PSL}_2(\mathbb{Z})$, on a $\mathrm{Im}\,(A \cdot z) = \frac{\mathrm{Im}\,(z)}{|cz+d|^2}$, donc pour tout $z' = A \cdot z \in X$, on a $|cz + d|^2 \leq 1$, ce qui n'arrive que pour un nombre fini d'entiers c et d. Par conséquent, il existe $z' \in X$ tel que $\mathrm{Im}\,(z')$ soit maximal.
Comme la matrice $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est dans $\mathrm{PSL}_2(\mathbb{Z})$, et que pour tout $n \in \mathbb{Z}$, $T^n \cdot z' = z' + n$, on peut supposer que $|\mathrm{Re}\,(z)| \leq \frac{1}{2}$. Or $S \cdot z' = \frac{-1}{z'}$ et $\mathrm{Im}\,(\frac{-1}{z'}) = \frac{\mathrm{Im}\,(z')}{|z'|^2} \leq \mathrm{Im}\,(z')$ par maximalité de z', donc $|z'| \geq 1$. Donc $z' \in D$ et D vérifie la propriété (ii).

ii) La propriété (i) est clairement vérifiée par D. Vérifions la propriété (iii) : soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$. Soit $z \in D^\circ$ tel que $A \cdot z \in D$. Par symétrie, on peut supposer quer $\mathrm{Im}\,(A \cdot z) \geq \mathrm{Im}\,(z)$. Alors on a vu que $|cz + d|^2 \leq 1$, donc $|c| \leq \frac{2}{\sqrt{3}}$, donc $c = -1$, 0 ou 1.
— si $c = 0$, alors $a = d = 1$ et A est une translation de vecteur $(b, 0)$ ($b \in \mathbb{Z}$) dans $\mathcal{H}$, donc $b = 0$ (sinon $A \cdot z \notin D^\circ$).
— si $c = \pm 1$, alors on vérifie que $a = d = 0$ et $b = -1$, ce qui est impossible.
Donc $A = I_2$.
Donc D est bien un domaine fondamental pour cette action.

iii) Soient $A \in PSL_2(\mathbb{Z})$ et $z \in D^\circ$, on a $A \cdot z \in \mathcal{H}$, donc en adaptant la preuve de la question c)i) en remplaçant le groupe $\mathrm{PSL}_2(\mathbb{Z})$ par son sous-groupe $\langle S, T\rangle$, on voit qu'il existe $B \in \langle S, T\rangle$ tel que $B \cdot (A \cdot z) \in D$. Alors $z \in D^\circ$ et $(BA) \cdot z \in D$. On a vu à la question c)i) qu'alors $BA = \pm I_2$, ce qui assure que $A = B^{-1}$ dans $\mathrm{PSL}_2(\mathbb{Z})$, donc $A \in \langle S, T\rangle$, donc $\mathrm{PSL}_2(\mathbb{Z}) = \langle S, T\rangle$, et comme $S^2 = -I_2$, on a $\mathrm{SL}_2(\mathbb{Z}) = \langle S, T\rangle$.

Exercice 8 :
Soit K un corps.
Montrer que les homographies sont exactement les K-automorphismes du corps $K(T)$ (les automorphismes de $K(T)$ dont la restriction à K est l'identité), i.e. que $\mathrm{Aut}_K(K(T)) \cong \mathrm{PGL}_2(K)$.

Solution de l'exercice 8. On dispose d'un morphisme de groupes évident $\varphi : \mathrm{PGL}_2(K) \to \mathrm{Aut}_K(K(T))$ défini de la façon suivante : si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ représente un élément de $\mathrm{PGL}_2(K)$, on note $\varphi(A)$ le K-automorphisme de $K(T)$ défini par $\varphi(A) : T \mapsto \frac{aT+b}{cT+d}$. Il est clair que φ est un morphisme de groupes. Montrons que φ est injectif : si $\varphi(A) = \mathrm{id}$, cela signifie que $\frac{aT+b}{cT+d} = T$, ce qui implique $aT+b = cT^2+dT$, donc $b = c = 0$ et $a = d$, donc A est une homothétie. Donc φ est injectif. Montrons que φ est surjectif : soit $\sigma \in \mathrm{Aut}_K(K(T))$. La fraction rationnelle $\sigma(T)$ s'écrit $\frac{P}{Q}$, avec $P, Q \in K[T]$ premiers entre eux. Comme σ est une bijection de $K(T)$, on peut écrire T comme une fraction rationnelle en $\frac{P}{Q}$, donc il existe des polynômes R et S, premiers entre eux, tels que $T = \frac{R(\sigma(T))}{S(\sigma(T))}$.
En écrivant r_0 et s_0 les coefficients constants de R et S, et $n := \max(\deg R, \deg S)$, on déduit de cette égalité que $(s_0T - r_0)Q^n = PU$, pour un certain polynôme $U \in K[T]$. Comme P et Q sont premiers entre eux, on en déduit que P divise $s_0T - r_0$. Or r_0 ou s_0 est non nul, donc cela implique que $\deg P \leq 1$. Symétriquement, on montre que $\deg Q \leq 1$ en utilisant les coefficients s_n et r_n. Donc finalement $\sigma(T)$ est de la forme $\frac{aT+b}{cT+d}$. Enfin, pour que σ soit bijective, on constate que l'on doit avoir $ad - bc \neq 0$, ce qui assure que σ est bien une homographie, i.e. que φ est surjectif.

Exercice 9 : $\star\star\star$
Soit G un groupe simple d'ordre 360.

a) Montrer que G admet dix 3-Sylow.

b) Montrer que G est isomorphe à un sous-groupe de $\mathfrak{A}_{10}$. On supposera désormais que G est un sous-groupe de $\mathfrak{A}_{10}$.

c) Soit S un 3-Sylow de G. Montrer que S n'est pas cyclique, et que l'on peut supposer que $N_G(S)$ est le stabilisateur de 10 dans $G \subset \mathfrak{A}_{10}$.

d) Montrer que tout élément non trivial de S ne fixe aucun point de $\{1, 2, \ldots, 9\}$.

e) Montrer que l'on peut supposer que S est engendré par les éléments $x = (1\,2\,3)(4\,5\,6)(7\,8\,9)$ et $y = (1\,4\,7)(2\,5\,8)(3\,6\,9)$.

f) Montrer que le stabilisateur P de 1 dans $N_G(S)$ est cyclique d'ordre 4 et est un 2-Sylow de $N_G(S)$. On note z un générateur de P.

g) Montrer qu'on peut supposer que $z = (2\,4\,3\,7)(5\,6\,9\,8)$.

h) Soit T un 2-Sylow de G contenant z. Montrer que $T = \langle z, t\rangle$, avec t d'ordre 2.

i) Montrer que l'on peut supposer que $t = (1\,10)(2\,3)(5\,6)(8\,9)$.

j) Montrer que $G = \langle x, y, z, t\rangle$.

k) Que peut-on en conclure pour les groupes simples d'ordre 360 ?

l) Montrer que $\mathrm{PSL}_2(\mathbb{F}_9) \cong \mathfrak{A}_6$.

Solution de l'exercice 9.

a) On note n_3 le nombre de 3-Sylow. Les théorèmes de Sylow assurent que $n_3 \in \{1, 4, 10, 40\}$. Alors la simplicité de G assure que $n_3 = 10$ ou 40. Montrons que $n_3 = 40$ est impossible.

Première solution : supposons $n_3 = 40$. Alors pour tout 3-Sylow S, le normalisateur $N_G(S) \subset G$ est d'indice 40, donc $N_G(S)$ est de cardinal 9. Donc $N_G(S) = S$. Et $|S| = 9$ assure que S est abélien. Par conséquent, $S = Z(N_G(S))$. Alors le théorème de transfert de Burnside (voir TD1, exercice 14) assure que G n'est pas simple, ce qui est contradictoire.

Seconde solution : on voit qu'il existe deux 3-Sylow S et T tels que $I := S \cap T$ est non trivial, i.e. est d'ordre 3. Alors $N_G(I)$ contient S et T, donc $|N_G(I)|$ est multiple de 9, divise 360 et est distinct de 9. Or $|N_G(I)| \neq 18, 45$ car un groupe d'ordre 18 (resp. 45) a un unique 3-Sylow. Si $|N_G(I)| \geq 72$, alors $N_G(I)$ est un sous-groupe strict de G d'indice ≤ 5, donc G se plonge dans un groupe symétrique $\mathfrak{S}_d$ avec $d \leq 5$, ce qui est contradictoire car 360 ne divise pas 5!. Donc $|N_G(I)| = 36$. Donc $N_G(I)$ a un unique 2-Sylow P, qui est donc distingué dans $N_G(I)$. Alors $N_G(P)$ contient $N_G(I)$, et P est contenu comme sous-groupe d'indice 2 dans un 2-Sylow Q de G, donc $Q \subset N_G(P)$, donc $|N_G(P)|$ est multiple de 8, donc $|N_G(P)|$ est multiple de 72, et distinct de 360, donc $|N_G(P)| = 72$, donc G admet un sous-groupe d'indice 5, ce qui est contradictoire à nouveau.

b) Puisque $n_3 = 10$, l'action de G sur l'ensemble X des 3-Sylow de G fournit un morphisme de groupes, injectif par simplicité de G, $\varphi : G \to \mathfrak{S}(X) \cong \mathfrak{S}_{10}$. Alors $\varphi(G) \cap \mathfrak{A}_{10}$ est distingué non trivial dans $\varphi(G)$, donc par simplicité, $\varphi(G) \subset \mathfrak{A}_{10}$, d'où le résultat.

c) Comme $N_G(S)$ fixe $S \in X$, le groupe $N_G(S)$ s'identifie bien au stabilisateur du point $S \in X$ dans G.

Supposons S cyclique. Alors un générateur de S est un élément d'ordre 9 dans $\mathfrak{A}_{10}$, donc un 9-cycle. Donc $N_G(S)$ est formé d'éléments de $\mathfrak{A}_9$ (on a vu que $N_G(S)$ fixe un point) normalisant un 9-cycle. Or le centralisateur d'u 9-cycle dans $\mathfrak{A}_9$ est exactement le sous-groupe engendré par ce cycle, donc cela assure que le morphisme naturel $N_G(S)/S \to \mathrm{Aut}(S)$ est injectif. Or $|N_G(S)/S|4$ et $|\mathrm{Aut}(S)| = 6$, ce qui est contradictoire.

Donc S n'est pas cyclique.

d) Supposons qu'il existe $s \in S \setminus \{\mathrm{id}\}$ fixant un point $i \in \{1, \ldots, 9\}$. Alors s est d'ordre 3, et $s \in S \cap T$, où T est le 3-Sylow de G correspondant au point $i \in \{1, \ldots, 9\}$. Alors on est exactement dans la situation de la seconde solution de la question a), et on arrive donc à la même contradiction. D'où le résultat.

e) Les questions c) et d) assurent que S est engendré par deux éléments x et y de $\mathfrak{A}_9$ d'ordre 3, qui commutent et qui ne fixent aucun point de $\{1, \ldots, 9\}$. Cela implique que chacun de ces deux générateurs est un produit de trois 3-cycles à supports disjoints. Notons $x = (a\,b\,c)(d\,e\,f)(g\,h\,i)$, avec $\{a, b, c, d, e, f, g, h, i\} = \{1, \ldots, 9\}$. Comme y commute avec x, y permute les supports des trois 3-cycles de x en respectant l'ordre cyclique sur ces supports. En outre, un 3-cycle de y ne peut avoir le même support qu'un 3-cycle de x, sinon un élément non trivial de S

fixe les trois points de ce support. Donc quitte à permuter $(d\,e\,f)$ et $(g\,h\,i)$, on peut supposer que $y = (a\,d\,g)(b\,e\,h)(c\,f\,i)$. Quitte à renuméroter les éléments de $\{1,\dots,9\}$, on a le résultat souhaité.

f) La question précédente assure que S agit (librement et) transitivement sur $\{1,\dots,9\}$. Donc $|P| = 4$. Donc P est un 2-Sylow de $N_G(S)$ (qui est de cardinal 36) et $N_G(S) = S.P$. Donc P est isomorphe à $N_G(S)/S$ et on vérifie que le centralisateur de S dans $\mathfrak{A}_9$ est un 3-groupe, donc $Z_G(S) = S$, donc $P \cong N_G(S)/G$ s'injecte dans $\mathrm{Aut}(S) \cong \mathrm{GL}_2(\mathbb{F}_3)$. Et comme $N_G(S)$ est un sous-groupe de $\mathfrak{A}_9$, on vérifie que son action par conjugaison sur S se factorise en un morphisme $N_G(S) \to \mathrm{SL}_2(\mathbb{F}_3)$. Donc P s'injecte dans $\mathrm{SL}_2(\mathbb{F}_3)$. Or l'exercice 10, question b) du TD4 assure que l'unique 2-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$ est isomorphe au groupe des quaternions d'ordre 8, et tout sous-groupe d'ordre 4 du groupe des quaternions est cyclique. Donc P est cyclique.

g) L'élément $z \in P$ fixe 1 et 10, donc $z \in \mathfrak{A}(\{2,3,\dots,9\})$. Et z est d'ordre 4, donc z est un produit de deux 4-cycles à supports disjoints. Notons $a \in \{3,\dots,9\}$ l'image de 2 par z. Puisque z normalise S et est d'ordre 4, on voit que $a \in \{4,7\}$. Et si $a = 4$, nécessairement $z = (2\,4\,3\,7)(5\,6\,9\,8)$, et si $a = 7$, alors $z = (2\,7\,3\,4)(5\,8\,9\,6)$. Comme ces deux éléments sont inverses l'un de l'autre, ils engendrent le même groupe P, donc quitte à remplacer z par z^{-1}, on peut supposer que $z = (2\,4\,3\,7)(5\,6\,9\,8)$.

Remarquons que cette question implique qu'un élément non trivial de G fixe au plus deux points de $\{1,\dots,10\}$.

h) Comme $\langle z\rangle \subset T$ est d'indice 2, il existe bien $t \in T$ tel que $T = \langle z, t\rangle$. Comme G est simple, T ne peut pas être un groupe cyclique, donc t est d'ordre 2 ou 4. Or $t \notin N_G(S)$, donc $t(10) \neq 10$. Comme z fixe 1 et 10, on voit que nécessairement $t(1) = 10$ et $t(10) = 1$.

Supposons maintenant t d'ordre 4. Comme t est paire et contient le cycle $(1\,10)$ dans sa décomposition, la restriction de t à $\{1,\dots,9\}$ est soit un 4-cycle, soit le produit d'un 4-cycle par une bitransposition de supports disjoints. Dans les deux cas, t^2 est une bitransposition, or $t^2 = c^2$ et c^2 est un produit de quatre transpositions à supports disjoints. D'où une contradiction.

Donc t est d'ordre 2.

i) La question précédente assure que $T \cong D_4$. Comme t est paire, d'ordre 2 et fixe au plus deux points (voir question g)), on voit que t est produit de quatre transpositions (dont $(1\,10)$). Comme t normalise $P = \langle z\rangle$, une étude au cas par cas assure que, quitte à multiplier t par une puissance de z (ce qui est acceptable), t est bien de la forme souhaitée.

j) Par construction, $\langle x, y, z, t\rangle \subset G$ est un sous-groupe de cardinal ≥ 72. Or G n'admet pas de sous-groupe strict d'indice ≤ 5, donc $G = \langle x, y, z, t\rangle$.

k) Les questions précédentes assurent que tout groupe simple d'ordre 360 est isomorphe au sous-groupe G_0 de $\mathfrak{A}_{10}$ engendré par les éléments explicites x, y, z, t de $\mathfrak{A}_{10}$ (ces éléments ne dépendent pas de G). En particulier, cela implique que tous les groupes simples d'ordre 360 sont isomorphes.

l) Ces deux groupes sont simples d'ordre 360, donc la question précédente assure le résultat.

TD7 : formes quadratiques

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Décomposer sous forme de combinaison linéaire de carrés les formes quadratiques réelles suivantes ; en déduire leur signature et leur rang.

a) $f(x,y,z) = x^2 - 2y^2 + xz + yz$.
b) $f(x,y,z) = 2x^2 - 2y^2 - 6z^2 + 3xy - 4xz + 7yz$.
c) $f(x,y,z) = 3x^2 + 3y^2 + 3z^2 - 2xy - 2xz - 2yz$.
d) $f(x,y,z,t) = xy + yz + zt + tx$.
e) $f(x_1,\dots,x_n) = \sum_{1\le i<j\le n} x_i x_j$.
f) $f(A) = \mathrm{tr}(A^2)$, pour $A \in M_n(\mathbb{R})$.
g) $f(A) = \mathrm{tr}({}^tAA)$, pour $A \in M_n(\mathbb{R})$.
h) $f(A) = \mathrm{tr}(A)^2$, pour $A \in M_n(\mathbb{R})$.

Solution de l'exercice 1. On applique l'algorithme de Gauss pour diagonaliser la plupart de ces formes quadratiques. On obtient :

a) $f(x,y,z) = \left(x + \frac{z}{2}\right)^2 - 2\left(y - \frac{z}{4}\right)^2 - \frac{z^2}{8}$. Donc $\mathrm{sign}(f) = (1,2)$ et $\mathrm{rang}(f) = 3$.
b) $f(x,y,z) = 2\left(x + \frac{3}{4}y - z\right)^2 - \frac{25}{8}\left(y - \frac{8}{5}z\right)^2$. Donc $\mathrm{sign}(f) = (1,1)$ et $\mathrm{rang}(f) = 2$.
c) $f(x,y,z) = 3\left(x + \frac{y}{3} - \frac{z}{3}\right)^2 + \frac{8}{3}\left(y - \frac{z}{2}\right)^2 - 2z^2$. Donc $\mathrm{sign}(f) = (2,1)$ et $\mathrm{rang}(f) = 3$.
d) $f(x,y,z) = \frac{1}{4}(x+z+y+t)^2 - \frac{1}{4}(x+z-y-t)^2$. Donc $\mathrm{sign}(f) = (1,1)$ et $\mathrm{rang}(f) = 2$.
e) On peut par exemple remarquer que la matrice associée à f dans la base canonique admet pour valeurs propres $-\frac{1}{2}$ avec multiplicité $n-1$ (avec des vecteurs propres de la forme $e_i - e_1$, $2 \le i \le n$, où (e_i) est la base canonique) et $\frac{n-1}{2}$ avec mutiplicité 1 (utiliser la trace). Donc on en déduit que $\mathrm{sign}(f) = (1, n-1)$ et $\mathrm{rang}(f) = n$.
f) La forme polaire de f est la forme bilinéaire symétrique $(A,B) \mapsto \mathrm{tr}(AB)$. On remarque que la restriction de f au sous-espace $S_n(\mathbb{R})$ des matrices symétriques est définie positive, alors que la restriction de f au sous-espace $A_n(\mathbb{R})$ des matrices antisymétriques est définie négative. En outre, ces deux sous-espaces sont en somme directe et engendre $M_n(\mathbb{R})$, et ils sont orthogonaux pour q. Cela assure que $\mathrm{sign}(q) = (\dim(S_n(\mathbb{R})), \dim(A_n(\mathbb{R}))) = \left(\frac{n(n+1)}{2}, \frac{n(n-1)}{2}\right)$ et $\mathrm{rang}(f) = n^2$. On peut aussi trouver directement la décomposition en carrés en remarquant que si $A = (a_{i,j})$, on a

$$f(A) = \sum_{i,j} a_{i,j}a_{j,i} = \sum_i a_{i,i}^2 + 2\sum_{i<j} a_{i,j}a_{j,i} = \sum_i a_{i,i}^2 + \frac{1}{2}\sum_{i<j}(a_{i,j}+a_{j,i})^2 - \frac{1}{2}\sum_{i<j}(a_{i,j}-a_{j,i})^2.$$

g) Il est classique que f est la forme quadratique associée au produit scalaire canonique $(A,B) \mapsto \mathrm{tr}({}^tAB)$, donc f est définie positive, donc $\mathrm{sign}(f) = (n^2, 0)$ et $\mathrm{rang}(f) = n^2$. La décoposition en carrés est donnée par $f(A) = \sum_{i,j} a_{i,j}^2$.
h) Par définition, f est le carré d'une forme linéaire non nulle (la trace), donc $\mathrm{sign}(f) = (1,0)$ et $\mathrm{rang}(f) = 1$.

Exercice 2 :
Soit $n \geq 1$ et soit $\mathbb{R}_n[X]$ l'espace vectoriel des polynômes réels de degré inférieur ou égal à n. Pour tous $P, Q \in \mathbb{R}_n[X]$, on pose :

$$B(P,Q) = \int_0^1 tP(t)Q'(t)dt \qquad \text{et} \qquad f(P) = B(P,P).$$

a) Montrer que B est une forme bilinéaire. Est-elle symétrique ? Antisymétrique ?

b) La forme f a-t-elle des vecteurs isotropes non nuls ?

c) Calculer la matrice de f dans la base $(1, X, \ldots, X^n)$.

d) Pour $n = 2$, déterminer la signature de f. La forme f est-elle positive ? Négative ?

Solution de l'exercice 2.

a) La linéarité de l'intégrale assure que B est bilinéaire. On a $B(1,X) = 1/2$ et $B(X,1) = 0$ et donc B n'est ni symétrique ni antisymétrique.

b) On a $f(1) = 0$ et donc $1 \in \mathbb{R}_n[X]$ est un vecteur isotrope.

c) Notons que la forme polaire de f n'est pas B mais sa symétrisée, à savoir

$$B_s(P,Q) := \frac{1}{2}\left(B(P,Q) + B(Q,P)\right).$$

Un petit calcul assure que la matrice de f (i.e. de B_s) dans la base indiquée est $M_n = \left(\frac{i+j-2}{2(i+j-1)}\right)_{1\leq i,j\leq n}$.

d) La signature est $(1,2)$.

Exercice 3 : $\star$
Soit K un corps de caractéristique différente de 2. Soit P un K-espace vectoriel de dimension 2, muni d'une forme quadratique f. Quelles sont valeurs possibles pour le nombre de droites isotropes de f ? Donner un exemple dans chaque cas.

Solution de l'exercice 3.

— La forme f n'a aucune droite isotrope si et seulement si elle est anisotrope (par définition). Or il existe une forme quadratique anisotrope sur P si et seulement si le corps K n'est pas quadratiquement clos : il suffit de considérer la forme $f(x,y) = x^2 - \alpha y^2$ sur K^2, où $\alpha \in K^* \setminus (K^*)^2$. En particulier, ce cas n'arrive pas sur un corps algébriquement clos.

— La forme f a une unique droite isotrope si et seulement si $\text{rang}(f) = 1$. Ceci arrive sur tout corps K, il suffit de considérer par exemple la forme quadratique $f(x,y) = x^2$ sur K^2 (la seule droite isotrope est la droite d'équation $x = 0$).

— La forme f a exactement deux droites isotropes si et seulement si elle est hyperbolique, i.e. non dégénérée et admettant un vecteur isotrope. Une telle forme existe sur tout corps K, comme le montre l'exemple $f(x,y) = x^2 - y^2$ sur K^2 (droites isotropes d'équations $x+y=0$ et $x-y=0$).

— Supposons que la forme f ait au moins 3 droites isotropes. Notons alors v_1, v_2, v_3 trois vecteurs isotropes deux-à-deux non proportionnels. Puisque (v_1, v_2) est une base de P, il existe $\lambda, \mu \in K^*$ tels que $v_3 = \lambda v_1 + \mu v_2$. On applique la forme f, et si on note b la forme polaire de f, on obtient

$$0 = f(v_3) = f(\lambda v_1 + \mu v_2) = \lambda^2 f(v_1) + \mu^2 f(v_2) + 2\lambda\mu b(v_1, v_2) = 2\lambda\mu b(v_1, v_2).$$

Donc $b(v_1, v_2) \neq 0$, donc la matrice de f dans la base (v_1, v_2) est la matrice nulle (c'est une base orthogonale formée de vecteurs isotropes), donc $f = 0$.

Finalement, une forme quadratique sur un plan vectoriel admet soit aucune droite isotrope, soit une droite isotrope, soit deux droites isotropes, soit toutes les droites de P sont isotropes. Tous ces cas arrivent sur tout corps K, sauf le premier (aucune droite isotrope) qui existe si et seulement si K n'est pas quadratiquement clos.

Exercice 4 : $\star\star$
Soit K un corps de caractéristique différente de 2 et soit E un K-espace vectoriel de dimension finie. Soient f et f' des formes quadratiques sur E vérifiant $f^{-1}(0) = (f')^{-1}(0)$.

a) Supposons K algébriquement clos. Montrer qu'il existe $a \in K^\times$ tel que l'on ait $f' = af$.

b) Donner un contre-exemple pour $K = \mathbb{R}$ et $E = \mathbb{R}^2$.

Solution de l'exercice 4.

a) Soient b et b' les formes bilinéaires respectives de f et f'. Si f est totalement isotrope, le résultat est clair. Supposons que ce ne soit pas le cas : il existe $x \in E$ avec $f(x) \neq 0$. Posons $a = f'(x)f(x)^{-1} \in K^\times$. Soit $y \in E$. Les polynômes $af(y + \lambda x)$ et $f'(y + \lambda x)$ de $K[\lambda]$ sont de degré 2, ont mêmes racines par hypothèse, et ils ont même coefficient dominant $f'(x)$: ils sont donc égaux puisque K est algébriquement clos. En particulier, on a $f'(y) = af(y)$. Donc $f' = af$.

b) Il suffit de considérer les formes quadratiques $x^2 + y^2$ et $x^2 + 2y^2$.

Cet exercice est un cas très particulier du théorème des zéros de Hilbert (le Nullstellensatz de Hilbert) : soit K un corps algébriquement clos, $I \subset K[X_1, \ldots, X_n]$ un idéal et notons $Z(I)$ l'ensemble des zéros communs à tous les polynômes de I. Si f est un polynôme qui s'annule sur $Z(I)$, alors il existe $n \in \mathbb{N}$ tel que $f^n \in I$.

Exercice 5 : $\star\star$

Soit K un corps de caractéristique différente de 2, soit E un K-espace vectoriel de dimension finie non nulle et soit H un hyperplan de E. Soient de plus f une forme quadratique non dégénérée sur E et u un élément de $\mathcal{O}(E, f)$ vérifiant $u_{|H} = \mathrm{id}_H$.

a) Si $f_{|H}$ est non dégénérée, montrer que u est soit l'identité, soit la réflexion orthogonale d'hyperplan H.

b) Si $f_{|H}$ est dégénérée, montrer que u est l'identité.

Solution de l'exercice 5. Notons b la forme bilinéaire associée à f.

a) Si $f_{|_H}$ est non dégénérée, l'orthogonal de H pour b est un supplémentaire de H, de dimension 1, disons égal à Kx. Alors $b(u(x), u(h)) = b(x, h) = 0$ pour tout $h \in H$, ce qui assure que $u(x) \in Kx$ et $f(u(x)) = f(x)$ donne $u(x) = \pm x$ (car $f(x) \neq 0$ puisque $x \notin H \perp$). Donc $u = \mathrm{id}$ ou u est la réflexion orthogonale (i.e. parallèlement à $H^\perp$) d'hyperplan H.

b) Si $f_{|_H}$ est dégénérée, il existe $h \in H^\perp \cap H$ non nul. On peut le compléter en un plan hyperbolique (au passage, comme $H^\perp$ est de dimension 1, cela force $H^\perp \cap H$ à être égal à $H^\perp$) grâce à un $y \notin H$. Ecrivons $u(y) = \alpha y + h'$ avec $\alpha \in K$ et $h' \in H$. On a $1 = b(y, h) = b(u(y), u(h)) = \alpha$ et $b(u(y) - y, n) = 0$ pour tout $n \in H$. On peut donc écrire $u(y) = y + \beta h$. Mais alors on a $f(y) + 2\beta = f(u(y)) = f(y)$, d'où $\beta = 0$. Donc $u = \mathrm{id}$.

Exercice 6 :

Soit $n \geq 1$ et soit $E = \mathbb{R}^{n+1}$ muni de la forme quadratique

$$f(x_0, \ldots, x_n) = x_0^2 - (x_1^2 + \cdots + x_n^2),$$

de forme bilinéaire b. Un sous-espace F de E est dit *elliptique* si $f_{|F}$ est définie négative, *hyperbolique* si $f_{|F}$ est de signature $(1, m)$ avec $m \geq 1$ et *parabolique* si F est isotrope.

a) Soit F un sous-espace de dimension au moins 2 tel qu'il existe $x \in F$ avec $f(x) > 0$. Montrer que F est hyperbolique.

b) Soit F un sous-espace elliptique de dimension au plus $n-1$. Montrer que $F^\perp$ est hyperbolique.

c) Soit F un sous-espace parabolique. Montrer que $f|_F$ est de rang $\dim F - 1$.

Solution de l'exercice 6.

a) C'est évident. Montrons même que $f_{|_F}$ est non dégénérée. Supposons le contraire : il existe $t \in F \cap F^\perp$ non nul. On a alors $f(x + t) = f(x) > 0$ et la restriction de f au plan engendré par x et t est définie positive, ce qui contredit le fait que $\mathrm{sign}(f) = (1, n)$. Donc $f_{|F}$ est non dégénérée, ce qui assure que $\mathrm{sign}(f) = (1, \dim F - 1)$.

b) Supposons $f(t') \leq 0$ pour tout $t' \in F^\perp$. Comme on a $E = F \oplus F^\perp$ (pas de vecteur isotrope dans F), écrivons tout élément $e = t(e) + t'(e)$ suivant cette décomposition. On aurait alors $f(e) = f(t(e)) + f(t'(e)) \leq 0$, ce qui n'est pas vrai pour $(1, 0, \ldots, 0)$. De ce fait, il existe $x \in F^\perp$ avec $f(x) > 0$ et on applique la question a).

c) Supposons $f_{|_F}$ de rang $\leq \dim F - 2$. Alors $f_{|_F}$ possède deux vecteurs isotropes qui se complètent en deux plans hyperboliques distincts dans E. Or E ne contient pas de somme directe de deux plans hyperboliques (sinon sa signature serait (p, q) avec $p \geq 2$). L'hypothèse initiale est donc erronée.

Exercice 7 : $\star\star$

Soient $p \neq q$ deux nombres premiers impairs. On note $\left(\frac{p}{q}\right)$ l'entier qui vaut 1 si p est un carré modulo q et -1 sinon. On note $S := \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p : \sum_i x_i^2 = 1\}$.

a) Montrer que $\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}}\ [p]$.

b) En considérant une action de groupe, montrer que $|S| \equiv 1 + \left(\frac{p}{q}\right)\ [p]$.

c) Montrer qu'il existe une base de $\mathbb{F}_q^p$ dans laquelle la forme quadratique $\sum_i X_i^2$ admet pour matrice $\mathrm{diag}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, (-1)^{\frac{p-1}{2}}\right)$.

d) En déduire que $|S| = q^{\frac{p-1}{2}}(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}})$.

e) Conclure que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ (c'est la loi de réciprocité quadratique).

Solution de l'exercice 7.

a) Soit $a \in \mathbb{F}_p^*$. S'il existe $b \in \mathbb{F}_p^*$ tel que $a = b^2$, alors $a^{\frac{p-1}{2}} = b^{p-1} = 1$. Donc les $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{F}_p$ sont racines du polynôme $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[X]$. Or ce polynôme admet au plus $\frac{p-1}{2}$ racines, donc ses racines sont exactement les carrés non nuls. Or pout tout $a \in \mathbb{F}_p^*$, $\left(a^{\frac{p-1}{2}}\right)^2 = 1$, donc $a^{\frac{p-1}{2}} = \pm 1$. Cela assure que pour tout $a \in \mathbb{Z}$ non divisible par p, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}\ [p]$ (le symbole $\left(\frac{a}{p}\right)$ est défini de façon évidente). D'où le résultat.

b) Le groupe $G = \mathbb{Z}/p\mathbb{Z}$ agit sur S par permutation circulaire. L'équation aux classes assure que $|S^G| \equiv |S|\ [p]$. Or $S^G \cong \{x \in \mathbb{F}_q : (x, \ldots, x) \in S\} = \{x \in \mathbb{F}_q : px^2 = 1\}$. Donc $S^G = \emptyset$ si p n'est pas un carré modulo q, et $|S^G| = 2$ si p est u carré modulo q. D'où le résultat.

c) Les deux formes quadratiques mentionnées sont de rang p et de discriminant 1, donc elles sont équivalentes sur $\mathbb{F}_q$ (voir le théorème de classification des formes quadratiques sur un corps fini). D'où le résultat.

d) La question c) assure que

$$|S| = \left|\{(x_1, \ldots, x_p) \in \mathbb{F}_q^p : x_1x_2 + \cdots + x_{p-2}x_{p-1} + (-1)^{\frac{p-1}{2}}x_p^2 = 1\}\right|.$$

Notons $T := \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p : x_1x_2 + \cdots + x_{p-2}x_{p-1} + (-1)^{\frac{p-1}{2}}x_p^2 = 1\}$, $T_0 := \{(x_1, \ldots, x_p) \in T : x_1 = \cdots = x_{p-2} = 0\}$ et $T_1 := T \setminus T_0$. Il est clair que $|T_0| = \left(1 + \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\right) q^{\frac{p-1}{2}} = \left(1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) q^{\frac{p-1}{2}}$. Ensuite, pour tout $(x_1, \ldots, x_{p-2}) \in \mathbb{F}_q^{\frac{p-1}{2}} \setminus \{0\}$, et tout $x_p \in \mathbb{F}_q$, l'équation

$$x_1x_2 + \cdots + x_{p-2}x_{p-1} + (-1)^{\frac{p-1}{2}}x_p^2 = 1$$

définit un hyperplan affine de $\mathbb{F}_q^{\frac{p-1}{2}}$, donc l'ensemble des solutions de cette équation est de cardinal $q^{\frac{p-3}{2}}$. Cela assure que $|T_1| = \left(q^{\frac{p-1}{2}} - 1\right) qq^{\frac{p-3}{2}} = \left(q^{\frac{p-1}{2}} - 1\right) q^{\frac{p-1}{2}}$. Donc finalement

$$|S| = |T| = |T_0| + |T_1| = q^{\frac{p-1}{2}}\left(q^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right).$$

e) Les questions a), b) et d) assurent que

$$1+\left(\frac{p}{q}\right) \equiv q^{\frac{p-1}{2}}\left(q^{\frac{p-1}{2}}+(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)\,[p]\,,$$

donc en utilisant la question a),

$$\left(\frac{p}{q}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)\,[p]\,.$$

Puisque ces nombres valent ± 1, on en déduit que

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)\,.$$

Exercice 8 : $\star\star\star$

Soient $a,b,c\in\mathbb{Z}$ sans facteurs carrés. On considère la forme quadratique $f(x,y,z):=ax^2+by^2+cz^2$ sur $\mathbb{Q}^3$.

a) À quelle condition sur a,b,c la forme f est-elle isotrope sur $\mathbb{R}$?

b) On suppose $a,b>0$ et $c=-1$ et on note d le pgcd de a et b. Montrer que la forme quadratique f est isotrope sur $\mathbb{Q}$ si et seulement si les trois conditions suivantes sont satisfaites

i) a est un carré modulo b.

ii) b est un carré modulo a.

iii) $-\frac{ab}{d^2}$ est un carré modulo d.

c) On suppose désormais a,b,c deux-à-deux premiers entre eux. Montrer que f est isotrope sur $\mathbb{Q}$ si et seulement si f est isotrope sur $\mathbb{R}$ et les trois conditions suivantes sont satisfaites

i) $-ab$ est un carré modulo c.

ii) $-ac$ est un carré modulo b.

iii) $-bc$ est un carré modulo a.

d) Sous les hypothèses de la question c), montrer que f est isotrope sur $\mathbb{Q}$ si et seulement si f est isotrope sur $\mathbb{R}$ et pour tout nombre premier p, pour tout entier $m\geq 1$, il existe $(x,y,z)\in\mathbb{Z}^3$ non tous divisibles par p tels que $f(x,y,z)\equiv 0\,[p^m]$.

e) Vérifier que dans l'équivalence précédente, il suffit de prendre $p|abc$ et $m=2$.

f) Soit q une forme quadratique non dégénérée sur $\mathbb{Q}^3$. Donner un algorithme permettant de décider si q est isotrope.

Solution de l'exercice 8.

a) Il faut et il suffit que a,b,c ne soient pas tous de même signe.

b) — On suppose f isortrope sur $\mathbb{Q}$: il existe $(x,y,z)\in\mathbb{Q}^3\setminus\{(0,0,0)\}$ tel que $f(x,y,z)=0$. Quitte à multiplier x,y,z par le ppcm des dénominateurs de x,y,z, et à diviser par le pgcd des numérateurs, on peut supposer que $x,y,z\in\mathbb{N}$ sont des entiers premiers entre eux dans leur ensemble, vérfiant $ax^2+by^2=z^2$. Soit p un nombre premier divisant b et x. Alors $p|z$, donc $p^2|by^2$. Comme b est sans facteur carré, $p|y$, donc p divise x, y et z. Or x,y,z sont premiers entre eux, donc $\mathrm{pgcd}(b,x)=1$. Donc en réduisant l'égalité modulo b, on obtient que $ax^2\equiv z^2\,[b]$. Comme x et b sont premiers entre eux, x est inversible modulo b, donc a est un carré modulo b. Par symétrie, on a également que b est un carré modulo a.
Comme d divise a et b, on sait que $d|z^2$. Comme a et b sont sans facteur carré, d est sans facteur carré, ce qui assure que $d|z$, i.e. $z=dz'$ avec $z'\in\mathbb{Z}$. Écrivons de même $a=da'$ et $b=db'$. On peut donc diviser l'égalité $ax^2+by^2=z^2$ par d pour obtenir $a'x^2+b'y^2=dz'^2$. On réduit modulo d cette égalité et on obtient $a'x^2+b'y^2\equiv 0\,[d]$, ce qui assure, puisque x et y sont premiers à d, que $a'b'$ est un carré modulo d. Donc $\frac{ab}{d^2}$ est un carré modulo d.

— Réciproquement, supposons les conditions i), ii) et iii) satisfaites. On raisonne par récurrence sur a. Si $a = 1$, le résultat est évident, car $(x, y, z) = (1, 0, 1)$ est un vecteur isotrope de f. Soit alors $a > 1$. Quitte à échanger a et b, alors on peut supposer que $a \geq b$. Dans le cas où $a = b$, la condition iii) assure que -1 est un carré modulo b, donc b est somme de deux carrés dans $\mathbb{Z}$, i.e. $a = b = s^2 + t^2$, et on vérifie que $(s, t, s^2 + t^2)$ est un vecteur isotrope de f. Donc on peut supposer $a > b$.

On construit maintenant $0 < a' < a$ tel que f est isotrope si $a'x^2 + by^2 - z^2$ l'est. Pour ce faire, on sait que la propriété ii) implique l'existence de $c, k \in \mathbb{Z}$ tels que $b = c^2 - ka$. Il existe $a', m \in \mathbb{Z}$ tels que $k = a'm^2$, avec a' sans facteur carré. On peut en outre supposer que $|c| \leq \frac{a}{2}$. Montrons que $0 < a' < a$. On a $c^2 = b + aa'm^2$. Comme $c^2 > 0$ et $a > b$, on a néssairement $a' \geq 0$. Or b est sans facteur carré, donc $a \neq 0$, donc $a > 0$. La condition $|c| \leq \frac{a}{2}$ implique que $b + aa'm^2 \leq \frac{a^2}{4}$, donc $aa' < \frac{a^2}{4}$, donc $a < \frac{a}{4} < a$.

Vérifions maintenant que les propriétés i), ii) et iii) sont satisfaites pour la forme quadratique $a'x^2 + by^2 - z^2$. On écrit toujours $a = dA$ et $b = dB$, avec $d = \text{pgcd}(a, b)$. Alors $c^2 = dB + dAa'm^2$, ce qui implique, comme d est sans facteur carré, que $d|c$, i.e. $c = dC$ avec $C \in \mathbb{Z}$. On a donc $dC^2 = B + Aa'm^2$. Donc $Aa'm^2 \equiv -B\,[d]$, donc $a'A^2m^2 \equiv -AB\,[d]$. Or $\text{pgcd}(d, m) = 1$, et par iii), $-AB$ est un carré modulo d, donc a' est un carré modulo d. De même, la relation $c^2 \equiv a'am^2\,[B]$ et l'hypothèse i) assurent que a' est un carré modulo B. Donc a' est un carré modulo $Bd = b$.

Notons maintenant $r := \text{pgcd}(a', b)$, $a' = rA'$, $b = rB'$. Montrons que $-A'B'$ est un carré modulo r. Par définition, on a $c^2 = rB' + raA'm^2$, donc $r|c$ (car r est sans facteur carré), donc en notant $c = rC$, on a $rC^2 = B' + aA'm^2$. On réduit modulo r et on obtient $aA'm^2 = -B'\,[r]$. Or par i), a est un carré modulo b, donc modulo r, donc $-A'B'$ est bien un carré modulo r.

Supposons maintenant que la forme quadratique $f'(x, y, z) = a'x^2 + +by^2 - z^2$ soit isotrope sur $\mathbb{Q}^3$, et notons (x_0, y_0, z_0) un vecteur isotrope dans $\mathbb{Q}^3$. Alors $a'x_0^2 = z_0^2 - by_0^2$, et en multipliant cette égalité avec $aa'm^2 = c^2 - b$, on obtient $a(a'mx_0)^2 = (z_0^2 - by_0^2)(c^2 - b)$, i.e. $a(a'mx_0)^2 + b(cy_0 + z_0)^2 - (cz_0 + by_0)^2 = 0$, donc $f(a'mx_0, cy_0 + z_0, cz_0 + by_0) = 0$, donc f est isotrope sur $\mathbb{Q}^3$.

Cela conclut la preuve par récurrence sur a.

c) On suppose que a et b sont de même signe et c de signe opposé. On pose $a' := -ac$, $b' := -bc$. En multipliant f par $-c$, on obtient que la forme quadratique f est $\mathbb{Q}$-isométrique à la forme quadratique $f'(x, y, z) = a'x^2 + b'y^2 - z^2 = 0$.

Alors la question b) assure que f est isotrope sur $\mathbb{Q}^3$ si et seulement si f' l'est si et seulement si $-ac$ est un carré modulo $-bc$, $-bc$ est un carré modulo $-ac$ et $-ab$ est un carré modulo c. On voit facilement que cela équivaut aux conditions i), ii) et iii) de l'énoncé.

Enfin, les conditions i),ii),iii) sont symétriques en a, b, c, ce qui assure que l'équivalence souhaitée : en effet, si f est isotrope sur $\mathbb{R}$, deux des coefficients de f sont de même signe et l'autre est de signe opposé, donc quitte à permuter a, b, c (ce qui n'affecte pas les conditions i),ii),iii)), on peut bien supposer a et b de même signe et c de signe opposé. D'où le résultat.

d) Le sens direct est clair. Montrons la réciproque. On suppose donc les conditions de l'énoncé vérifiées. Prenons $m = 2$ et p un facteur premier de a. Par hypothèse, il existe $x, y, z \in \mathbb{Z}^3$ non tous divisibles par p, tels que $f(x, y, z) \equiv 0\,[p^2]$. Il est clair que p ne divise pas yz (sinon $p^2|a$), donc $by^2 + cz^2 \equiv 0\,[p]$ implique que $-bc$ est un carré modulo p. Ceci étant valable pour tout $p|a$, on en déduit que $-bc$ est un carré modulo a. Par symétrie, on a également que $-ac$ est un carré modulo b et $-ab$ est un carré modulo c. La question c) assure alors que f est isotrope sur $\mathbb{Q}$.

e) C'est une conséquence immédiate de la solution à question d).

f) Montrons d'abord que q est isométrique sur $\mathbb{Q}$ à une forme quadratique $f(x, y, z) = ax^2 + by^2 + cz^2$ avec $a, b, c \in \mathbb{Z}$ deux-à-deux premiers entre eux. Pour cela, on commence d'abord par diagonaliser q, chasser les dénominateurs et diviser par le pgcd des coefficients apparaissant pour écrire q sous la forme $q(x, y, z) = a'x^2 + b'y^2 + c'z^2$, avec $a', b', c' \in \mathbb{Z}$ premiers entre eux dans leur ensemble et sans facteur carré. Notons $d := \text{pgcd}(a', b')$, avec $a' = da''$ et $b' = db''$. En multipliant

q par d, on voit que q est équivalente à la forme quadratique $(x,y,z) \mapsto a''x^2 + b''y^2 + c''z^2$, avec $c'' := dc'$. Alors a'' et b'' sont premiers entre eux et a'', b'', c'' sont sans facteur carré, et $\mathrm{pgcd}(a'', c'') = \mathrm{pgcd}(a'', c')|\mathrm{pgcd}(a', c')$ et $\mathrm{pgcd}(b'', c'') = \mathrm{pgcd}(b'', c')|\mathrm{pgcd}(b', c')$. On répète successivement cette opération avec le couple de coefficients (a'', c''), ce qui donne des nouveaux coefficients $(a^{(3)}, b^{(3)}, c^{(3)})$, puis avec $(b^{(3)}, c^{(3)})$, ce qui fournit les coefficients (a, b, c) recherchés (tels que a, b, c soient sans facteur carré et deux-à-deux premiers entre eux. On applique alors la question e) pour décider algorithmiquement si la forme quadratique q est isotrope : on décompose a, b et c en facteurs premiers, et pour chaque p premier divisant a, b ou c, on teste si l'équation $ax^2 + by^2 + cz^2 = 0$ a une solution modulo p^2 non divisible par p. Enfin, on teste si les trois entiers a, b, c sont de même signe ou non.

Remarque : cet exercice est un cas particulier du théorème de Hasse-Minkowski, qui affirme que pour toute forme quadratique non dégénérée q sur $\mathbb{Q}^n$ (que l'on peut supposer diagonale à coefficients premiers premiers entre eux dans leur ensemble), la forme q est isotrope si et seulement si elle est isotrope sur $\mathbb{R}$ et pour tout premier p et tout entier $n \geq 1$, l'équation $q = 0$ admet une solution modulo p^n formée d'entiers non tous divisibles par p (cela signifie que q est isotrope sur tous les corps p-adiques $\mathbb{Q}_p$).

Exercice 9 : $\star\star\star$

Soit K un corps. On définit son niveau $s(K) \in \mathbb{N} \cup \{\infty\}$ et, si la caractéristique de K n'est pas 2, son u-invariant $u(K) \in \mathbb{N} \cup \{\infty\}$ par

$$s(K) := \inf\{n \geq 1 \mid \exists (x_1, \ldots, x_n) \in K^n \quad x_1^2 + \cdots + x_n^2 = -1\}$$

et

$$u(K) := \sup\{\dim(q) : q \text{ forme quadratique anisotrope sur } K\},$$

avec la convention que l'infimum de l'ensemble vide est ∞.

a) Montrer que $u(K) \geq s(K)$.

b) Calculer $s(K)$ et $u(K)$ si K est algébriquement clos.

c) Donner un exemple de corps K avec $s(K) = \infty$ et un exemple avec $u(K) = \infty$ et $s(K) < \infty$.

d) Montrer que des corps isomorphes ont même niveau et même u-invariant. Les réciproques sont-elles vraies ?

e) Montrer que le niveau d'un corps fini est égal à 1 ou 2. Montrer que le u-invariant d'un corps fini vaut 2.

f) Montrer l'égalité $s(K) = s(K(X))$.

On suppose désormais que K de caractéristique différente de 2. Pour $n \geq 1$, on considère la forme quadratique

$$f_n(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^2.$$

g) Montrer que f_n admet un vecteur isotrope si et seulement si on a $s(K) \leq n - 1$.

h) Supposons $n = 2^k$ avec $k \in \mathbb{N}$. Montrer que pour tout $x = (x_1, \ldots, x_n) \in K^n$ non nul, il existe une matrice T_x de première ligne $(x_1, \ldots, x_n)$ vérifiant

$${}^tT_xT_x = T_x^tT_x = f_n(x_1, \ldots, x_n)I_n.$$

i) En déduire que l'ensemble des sommes non nulles de 2^k carrés d'éléments de K est un groupe multiplicatif.

j) Montrer que le niveau d'un corps est soit infini, soit une puissance de 2.

Solution de l'exercice 9.

a) Soit $n < s(K)$. Alors par définition la forme quadratique $x_1^2 + \cdots + x_n^2 + x_{n+1}^2$ est anisotrope sur K^{n+1} (sinon, un vecteur isotrope contredit le fait que $n < s(K)$). Donc $u(K) \geq n + 1$. En appliquant ceci à $n = s(K) - 1$, on trouve $u(K) \geq s(K)$.

b) Si K est algébriquement clos, on a clairement $s(K) = 1$, et comme toute forme quadratique de rang 2 est isotrope, on a $u(K) = 1$.

c) Si $K = \mathbb{R}$, on a $s(K) = \infty$ (et donc $u(K) = \infty$). Si $K = \mathbb{C}(T_i; i \in \mathbb{N})$, alors $s(K) = 1$ et $u(K) = \infty$; en effet, pour tout $n \geq 0$, la forme quadratique $\sum_{i=0}^{n} T_i x_i^2$ est anisotrope sur K^{n+1}.

d) Le sens direct est évident. Les réciproques sont fausses, puisqu'on voit que $s(\mathbb{F}_5) = s(\mathbb{F}_{13}) = 1$ et $u(\mathbb{F}_5) = u(\mathbb{F}_{13}) = 2$. De même, pour tout corps algébriquement clos, $s(K) = s(\mathbb{C}) = u(K) = u(\mathbb{C}) = 1$.

e) L'élément -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q = 2^r$ ou $q \equiv 1\,[4]$. Dans ce cas, on a $s(\mathbb{F}_q) = 1$, et sinon $s(\mathbb{F}_q) = 2$. Et pour tout q impair, on sait que $u(\mathbb{F}_q) = 2$.

f) On a immédiatemment $s(K) \geq s(K(X))$. Supposons donc $s(K(X))$ fini, et notons s cet entier. Il existe des fractions rationnelles $R_1(X), \ldots, R_s(X)$ telles que l'on ait $R_1(X)^2 + \cdots + R_s(X)^2 = -1$.

Supposons dans un premier temps K infini. En notant $Q(X)$ un dénominateur commun des $R_i(X)$, on obtient une identité de la forme $P_1(X)^2 + \cdots + P_s(X)^2 = -Q(X)^2$ dans $K[X]$. Comme K est infini, il existe $\alpha \in K$ tel que $Q(\alpha) \neq 0$. Pour tout i, notons $p_i^{(\alpha)} = P_i(\alpha)Q(\alpha)^{-1} \in K$. On a alors $(p_1^{(\alpha)})^2 + \cdots + (p_s^{(\alpha)})^2 = -1$. Ceci donne $s(K) \leq s(K(X))$.

Dans le cas où K est fini, par la question e), on peut supposer $s(K(X)) = 1$. Alors $R_1(X)$ s'écrit $\frac{P_1(X)}{Q(X)}$ avec $P_1(X), Q(X) \in K[X]$. En choisissant $P_1(X)$ et $Q(X)$ premiers entre eux, on voit que $R_1(X)$ est un élément de K^*. Cela donne $s(K) = 1$ aussi. Ce qui conclut la preuve.

g) Si on a $s(K) \leq n-1$, alors il existe $x_1, \ldots, x_{n-1} \in K$ tels que $x_1^2 + \cdots + x_{n-1}^2 + 1^2 = 0$. Réciproquement, si f_n a un vecteur isotrope $(x_1, \ldots, x_n)$ avec $x_i \neq 0$, alors $\sum_{j \neq i} \left(\frac{x_j}{x_i}\right)^2 = -1$.

h) Montrons le par récurrence sur $k \geq 0$. Le cas $k = 0$ est trivial. Supposons la propriété vraie au rang k et prouvons le rang $k+1$. Par hypothèse de récurrence, on a T_1 et T_2 vérifiant

$$ {}^tT_1T_1 = T_1{}^tT_1 = f_n(x_1, \ldots, x_n)I_n, \quad {}^tT_2T_2 = T_2{}^tT_2 = f_n(x_{n+1}, \ldots, x_{2n})I_n. $$

On calcule ensuite

$$ \begin{pmatrix} {}^tT_1 & {}^tA \\ {}^tT_2 & {}^tB \end{pmatrix} \begin{pmatrix} T_1 & T_2 \\ A & B \end{pmatrix} = \begin{pmatrix} {}^tT_1T_1 + {}^tAA & {}^tT_1T_2 + {}^tAB \\ {}^tT_2T_1 + {}^tBA & {}^tT_2T_2 + {}^tBB \end{pmatrix}, $$

et

$$ \begin{pmatrix} T_1 & T_2 \\ A & B \end{pmatrix} \begin{pmatrix} {}^tT_1 & {}^tA \\ {}^tT_2 & {}^tB \end{pmatrix} = \begin{pmatrix} T_1{}^tT_1 + T_2{}^tT_2 & T_1{}^tA + T_2{}^tB \\ A{}^tT_1 + B{}^tT_2 & A{}^tA + B{}^tB \end{pmatrix}. $$

Alors :

i) si $f_n(x_1, \ldots, x_n) \neq 0$, on prend $A = T_1^{-1t}T_2T_1$ et $B = -{}^tT_1$.

ii) sinon, si $f_n(x_{n+1}, \ldots, x_{2n}) \neq 0$, on prend $A = -{}^tT_2$ et $B = T_2^{-1t}T_1T_2$.

iii) enfin, si $f_n(x_1, \ldots, x_n) = f_n(x_{n+1}, \ldots, x_{2n}) = 0$, on prend $A = -T_1$ et $B = T_2$.

Les calculs précédents assurent alors que la matrice $T_x := \begin{pmatrix} T_1 & T_2 \\ A & B \end{pmatrix}$ convient.

i) Si $f_n(x)$ et $f_n(y)$ sont deux sommes non nulles de 2^k carrés d'éléments, il suffit de définir $x \cdot y$ comme étant la première ligne de T_xT_y et on a $f_n(x \cdot y) = f_n(x)f_n(y)$. De même, si $[-1].x$ désigne la première ligne de T_x^{-1}, on obtient $f_n([-1].x) = f_n(x)^{-1}$.

j) Supposons $s(K)$ fini, vérifiant $n := 2^k \leq s(K) < 2n = 2^{k+1}$ pour un certain $k \geq 0$. Alors f_{2n} possède un vecteur isotrope par la question g), disons $(x_1, \ldots, x_{2n})$. On a donc $f_n(x_1, \ldots, x_n) = -f_n(x_{n+1}, \ldots, x_{2n}) \neq 0$. Mais alors $f_n(x_1, \ldots, x_n)f_n(x_{n+1}, \ldots, x_{2n})^{-1} = -1$ est une somme de 2^k carrés par la question i).

Remarque : réciproquement, pour tout $n = 2^k$, il existe un corps K de niveau n. On peut par exemple considérer le corps $K = \mathbb{R}(X_1, \ldots, X_{n-1})[X_n]/(\sum X_i^2 + 1)$ (voir par exemple le théorème 2.8 du chapitre 11 de Lam, *Algebraic theory of quadratic forms*).

TD8 : Groupe orthogonal (et symplectique)

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Soient K un corps de caractéristique $\neq 2$ et E un K-espace vectoriel de dimension finie. Soit q une forme quadratique non dégénérée sur E. Soit $u : E \to E$ une application (pas forcément linéaire a priori) telle que $u(0) = 0$ et pour tout $x, y \in E$, $q(u(x) - u(y)) = q(x - y)$.

a) Montrer que $u \in \mathrm{O}(E, q)$ (on pourra utiliser une base orthogonale).

b) L'hypothèse $u(0) = 0$ est-elle nécessaire ?

Solution de l'exercice 1.

a) On voit d'abord que pour tout $x \in E$, on a $q(u(x)) = q(x)$ (prendre $y = 0$ dans l'hypothèse). Ensuite, si on note b la forme polaire de q, on a pour tout $x, y \in E$, on a

$$q(u(x)) + q(u(y)) - 2b(u(x), u(y)) = q(u(x) - u(y)) = q(x - y) = q(x) + q(y) - 2b(x, y)\,,$$

donc $b(u(x), u(y)) = b(x, y)$.
On munit alors E d'une base orthogonale pour q, notée $(e_1, \ldots, e_n)$. Comme q est non dégénérée, on a $q(e_i) \neq 0$ pour tout i. Alors pour tout $i \neq j$, on a $b(u(e_i), u(e_j)) = b(e_i, e_j) = 0$ si $i \neq j$ et $q(e_i)$ si $i = j$. Cela assure que $(u(e_i))$ est une base orthogonale de (E, q).
Soit $x \in E$. On décompose $x = \sum_i \lambda_i e_i$ sur la base (e_i) et $u(x) = \sum_i \mu_i u(e_i)$ sur la base $(u(e_i))$. Pour montrer que u est linéaire, il suffit de montrer que $\lambda_i = \mu_i$ pour tout i. Pour cela, on calcule en utilisant l'orthogonalité des deux bases :

$$\mu_i q(e_i) = b(u(x), u(e_i)) = b(x, e_i) = \lambda_i q(e_i)$$

ce qui assure que $\lambda_i = \mu_i$ puisque $q(e_i) \neq 0$.
Donc u est linéaire, i.e. $u \in \mathrm{O}(E, q)$.

b) Oui. En effet, si l'on enlève l'hypothèse $u(0) = 0$, les applications vérifiant l'hypothèse sont exactement les isométries affines de (E, q), et il existe de telles isométries non linéaires dès que $E \neq \{0\}$ (par exemple, les translations de vecteur $\neq 0$).

Exercice 2 : ⋆
Soit E un $\mathbb{R}$-espace vectoriel de dimension finie $n \geq 1$.

a) Montrer que tout endomorphisme de E admet un sous-espace stable de dimension 1 ou 2.

b) Soit q une forme quadratique définie positive sur E. Montrer que pour tout $u \in \mathrm{O}(E, q)$, il existe une base orthonormée e de E, des entiers positifs r, s, t tels que $n = r + s + 2t$ et des réels $\theta_1, \ldots, \theta_t \in \mathbb{R} \setminus \pi\mathbb{Z}$, tels que

$$\mathrm{Mat}_e(u) = \begin{pmatrix} I_r & 0 & 0 & \ldots & 0 \\ 0 & -I_s & 0 & \ldots & 0 \\ 0 & 0 & R_{\theta_1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \ldots & R_{\theta_t} \end{pmatrix},$$

où R_θ désigne la matrice $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

c) En déduire que sous les hypothèses précédentes, $\mathrm{SO}(E,q)$ est connexe par arcs.

Solution de l'exercice 2.

a) Soit u un endomorphisme de E. On considère un polynôme $P \in \mathbb{R}[X]$ non nul et annulateur de u (par exemple le polynôme caractéristique). Il existe des polynômes $P_1, \dots, P_r$ de degré 1 ou 2 tels que $P = P_1 \dots P_r$. Alors $P(u) = P_1(u) \circ \cdots \circ P_r(u) = 0$, donc il existe $1 \leq i \leq r$ tel que $P_i(u)$ n'est pas injectif. Donc il existe $x \in Ker(P_i(u)) \setminus \{0\}$. Alors $\mathrm{Vect}_{\mathbb{R}}(x, u(x))$ est un sous-espace de dimension 1 ou 2 de E qui est stable par u.

b) Les cas $n = 1$ et $n = 2$ sont classiques (voir le cours). Le cas général se déduit de ces deux cas par une récurrence immédiate utilisant la question a) : on rappelle que si un sous-espace $F \subset E$ est stable par u, alors $F^{\perp}$ est stable par u.

c) Soit $u \in \mathrm{SO}(E,q)$. La question b) assure qu'il existe une base e de E dans laquelle la matrice P de u est de la forme susmentionnée. Comme $\det(u) = 1$, s est pair, donc on peut écrire P sous la forme

$$P = \begin{pmatrix} I_r & 0 & \dots & 0 \\ 0 & R_{\theta_1} & \dots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & R_{\theta_t} \end{pmatrix},$$

avec $\theta_i \in \mathbb{R}$. Pour tout $x \in [0;1]$, on pose

$$P(x) := \begin{pmatrix} I_r & 0 & \dots & 0 \\ 0 & R_{x\theta_1} & \dots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \dots & R_{x\theta_t} \end{pmatrix}.$$

Alors l'application $f : [0;1] \to \mathrm{SO}_n(\mathbb{R})$ définie par $x \mapsto P(x)$ est bien définie et continue, et $P(0) = I_n$, $P(1) = P$. Cela assure la connexité par arcs de $\mathrm{SO}(E,q)$.

Exercice 3 : $\star\star$

Soit $\mathbb{F}_q$ un corps fini à q éléments, de caractéristique différente de 2. Soient $n \geq 1$, $b \in \mathbb{F}_q$ et $\varepsilon \in \mathbb{F}_q^{\times} \setminus \mathbb{F}_q^{\times 2}$. Notons $S(2n,b)$, $S(2n+1,b)$ et $S_\varepsilon(2n,b)$ les nombres respectifs de solutions des équations

$$x_1^2 - y_1^2 + \cdots + x_n^2 - y_n^2 = b, \tag{1}$$
$$x_1^2 - y_1^2 + \cdots + x_n^2 - y_n^2 + x_{n+1}^2 = b, \tag{2}$$
$$x_1^2 - y_1^2 + \cdots + x_n^2 - \varepsilon y_n^2 = b. \tag{3}$$

a) Montrer

$$S(2n,b) = \begin{cases} q^{2n-1} + q^n - q^{n-1} & \text{si } b = 0; \\ q^{2n-1} - q^{n-1} & \text{si } b \neq 0; \end{cases}$$

$$S(2n+1,b) = \begin{cases} q^{2n} & \text{si } b = 0; \\ q^{2n} - q^n & \text{si } b \notin \mathbb{F}_q^{\times 2}; \\ q^{2n} + q^n & \text{si } b \in \mathbb{F}_q^{\times 2}; \end{cases}$$

$$S_\varepsilon(2n,b) = \begin{cases} q^{2n-1} - q^n + q^{n-1} & \text{si } b = 0; \\ q^{2n-1} + q^{n-1} & \text{si } b \neq 0. \end{cases}$$

b) En déduire

$$|\mathrm{O}_{2n+1}(\mathbb{F}_q)| = 2q^{n^2}\prod_{i=1}^{n}(q^{2i}-1),$$
$$|\mathrm{O}^+_{2n}(\mathbb{F}_q)| = 2q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1),$$
$$|\mathrm{O}^-_{2n}(\mathbb{F}_q)| = 2q^{n(n-1)}(q^n+1)\prod_{i=1}^{n-1}(q^{2i}-1).$$

Solution de l'exercice 3.

a) On montre les formules (1), (2) et (3) par récurrence sur k. Soit $b \in \mathbb{F}_q$. On a clairement

$$S(1,b) = \begin{cases} 1 & \text{si } b = 0; \\ 0 & \text{si } b \notin \mathbb{F}_q^{\times 2}; \\ 2 & \text{si } -b \in \mathbb{F}_q^{\times 2}. \end{cases}$$

Calculons $S(2,b)$. Si $b=0$, l'équation $(x_1-y_1)(x_2-y_2)=0$ a $2q-1$ solutions. Si $b \neq 0$, elle a les $q-1$ solutions suivantes

$$x_1 = \frac{1}{2}\left(\frac{b}{c}+c\right), \qquad y_1 = \frac{1}{2}\left(\frac{b}{c}-c\right), \qquad c \in \mathbb{F}_q^\times.$$

Calculons enfin $S_\varepsilon(2,b)$. Soit $K = \mathbb{F}_q[\sqrt{d}]$. On a $K \simeq \mathbb{F}_{q^2}$ et les éléments de K s'écrivent sous la forme $x+y\sqrt{d}$, avec $x,y \in \mathbb{F}_q$. On définit la norme $N(x+y\sqrt{d}) = x^2-dy^2$. On constate que $S_\varepsilon(2,b)$ est le nombre d'éléments de K de norme b. Or $N : K^* \to \mathbb{F}_q^*$ est un morphisme de groupes surjectif, son noyau ayant pour cardinal $q+1$. On en déduit que $S_\varepsilon(2,b) = q+1$.
Remarque : les quantités $S(2,b)$ et $S_\varepsilon(2,b)$ s'interprètent géométriquement comme les nombres de points à coordonnées dans $\mathbb{F}_q$ de coniques (non dégénérées) définies dans le plan affine $(\mathbb{F}_q)^2$. Or il est classique que l'ensemble des points d'une conique *projective* non dégénérée et non vide sur un corps quelconque est en bijection (cette bijection étant donnée par des fractions rationnelles) avec la droite projective sur ce corps (considérer par exemple l'ensemble des droites passant par un point fixé de la conique, et regarder l'intersection de ces droites avec la conique). Cela assure qu'une conique projective non dégénérée sur $\mathbb{F}_q$ (qui est non vide : compter les carrés dans $\mathbb{F}_q$) a exactement $q+1$ points. Pour passer à une conique affine, il suffit de regarder le nombre de points de notre conique projective sur la droite à l'infini dans $\mathbb{P}^2(\mathbb{F}_q)$: dans le cas de $S(2,b)$, ce nombre vaut 2 ; dans le cas de $S_\varepsilon(2,b)$, ce nombre vaut 0. Cela explique les deux entiers obtenus.
Montrons maintenant par récurrence la formule (1) pour n quelconque. Les solutions de (1) sont exactement les solutions de l'équation

$$x_1^2 - y_1^2 + \cdots + x_{n-1}^2 - y_{n-1}^2 = a, \qquad x_n^2 - y_n^2 = b-a, \qquad a \in \mathbb{F}_q. \tag{4}$$

Si $b=0$, le nombre de solution vaut donc

$$\begin{aligned} & S(2(n-1),0)S(2,0) + \sum_{a\in\mathbb{F}_q^\times} S(2(n-1),a)S(2,b-a) \\ = \;& (q^{2n-3}+q^{n-1}-q^{n-2})(2q-1) + (q-1)(q^{2n-3}-q^{n-2})(q-1) \\ = \;& q^{2n-1}+q^n-q^{n-1} \end{aligned}$$

Si $b \neq 0$, le nombre des solutions de (1) vaut

$$\begin{aligned} & S(2(n-1),0)S(2,b) + S(2(n-1),-b)S(2,0) + \sum_{a\in\mathbb{F}_q^\times, a\neq -b} S(2(n-1),a)S(2,b-a) \\ = \;& (q^{2n-3}+q^{n-1}-q^{n-2})(2q-1) + (q^{2n-3}-q^{n-2})(2q-1) + (q-2)(q^{2n-3}-q^{n-2})(q-1) \\ = \;& q^{2n-1}-q^{n-1}. \end{aligned}$$

Les formules (2) et (3) se prouvent exactement de la même façon.

b) Montrons $|\mathrm{O}^+_{2n}(\mathbb{F}_q)| = 2q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1)$ (les autres formules se prouvent de façon analogue).

Le cas où $n=1$ a été fait en cours (et le cas $n=0$ est évident). On prouve le cas général par récurrence.

Soit $Q(x_1,y_1,\ldots,x_n,y_n) = x_1^2 - y_1^2 + \cdots + x_n^2 - y_n^2$. Alors $\mathrm{O}^+_{2n}(\mathbb{F}_q) = \mathrm{O}((\mathbb{F}_q)^{2n}, Q)$. Soit $v \in \mathbb{F}_q^{2n}$ tel que $Q(v) = 1$ (un tel v existe). Il est facile de voir que l'orbite de v sous l'action de $\mathrm{O}_{2n}(Q,\mathbb{F}_q)$ est l'ensemble des $w \in \mathbb{F}_q^{2n}$ tels que $Q(w) = 1$ (on peut par exemple compléter v et w en deux bases orthogonales et considérer la matrice de passage).

On a donc $|\mathrm{Orb}(v)| = S(2n,1) = q^{2n-1} - q^{n-1}$. D'un autre côté, puisque $\mathbb{F}_q^{2n} = \langle v\rangle \oplus \langle v\rangle^\perp$, on a $\mathrm{Stab}(v) = \mathrm{O}(\langle v\rangle^\perp) = \mathrm{O}_{2n-1}(\mathbb{F}_q)$.

On en déduit les formules suivantes en utilisant l'hypothèse de récurrence (le cardinal de $\mathrm{O}_{2n-1}(\mathbb{F}_q)$) :

$$\begin{aligned} |\mathrm{O}^+_{2n}(\mathbb{F}_q)| &= |\mathrm{Orb}(v)||\mathrm{Stab}(v)| \\ &= (q^{2n-1}-q^{n-1})2q^{(n-1)^2}\prod_{i=1}^{n-2}(q^{2i}-1) \\ &= 2q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1). \end{aligned}$$

Comme mentionné plus haut, les deux autres cas se prouvent de manière similaire.

Exercice 4 : $\star\star$

Soit V un $\mathbb{R}$-espace vectoriel de dimension 3 muni de la forme quadratique définie positive $f(x_1,x_2,x_3) = x_1^2+x_2^2+x_3^2$. Le but de cet exercice est de montrer que $\mathrm{SO}(V,f)$ est simple. Soit N un sous-groupe distingué non trivial de $\mathrm{SO}(V,f)$.

a) Montrer que si N contient un renversement, alors $N = \mathrm{SO}(V,f)$.

b) Soit N_0 la composante connexe de l'identité de N. Montrer que N_0 est un sous-groupe distingué de $\mathrm{SO}(V,f)$.

c) Montrer que $N = \{\mathrm{id}\}$ si et seulement si $N_0 = \{\mathrm{id}\}$.

d) Montrer que la fonction

$$\begin{aligned} \varphi : N_0 &\longrightarrow [-1,1] \\ g &\longmapsto \frac{\mathrm{tr}(g)-1}{2} \end{aligned}$$

est bien définie et continue.

e) Montrer qu'il existe $g \in N_0$ tel que $\varphi(g) \leq 0$.

f) Montrer qu'il existe $g \in N_0$ tel que $\varphi(g) = 0$.

g) Conclure.

Solution de l'exercice 4.

a) Le cours assure que les renversements engendrent $\mathrm{SO}(V,f)$. Montrons que tous les renversements sont conjugués dans $\mathrm{SO}(V,f)$. Remarquons d'abord qu'en dimension 3, un renversement n'est autre qu'un demi-tour autour d'une droite, i.e. une rotation d'angle π. Soient r_1 et r_2 deux renversements d'axes respectifs Δ_1 et Δ_2. Pour montrer que r_1 et r_2 sont conjugués, il suffit de montrer qu'il existe $u \in \mathrm{SO}(V,f)$ tel que $u(\Delta_1) = \Delta_2$. Et ceci est évident puisque par exemple $\mathrm{SO}(V,f)$ agit transitivement sur l'ensemble des vecteurs de V de norme 1. Donc les renversements engendrent $\mathrm{SO}(V,f)$ et sont tous conjugués, or N est distingué, donc N contient un renversement si et seulement si $N = \mathrm{SO}(V,f)$.

b) Vérifions les faits classiques suivants : tout d'abord, la multiplication $m : \mathrm{SO}(V,f)\times\mathrm{SO}(V,f) \to \mathrm{SO}(V,f)$ est continue, donc $m(N_0 \times N_0) \subset N$ est connexe et contient id, donc il est contenu dans N_0, donc N_0 est stable par composition. De même, il est stable par inverse. Or il contient id, donc N_0 est un sous-groupe de N. Pour tout $g \in \mathbb{N}$, le morphisme $c_g : \mathrm{SO}(V,f) \to \mathrm{SO}(V,f)$ défini par $c_g(x) := gxg^{-1}$ est continu, donc $c_g(N_0) \subset N$ est connexe et contient id, donc $c_g(N_0) \subset N_0$, ce qui assure que N_0 est distingué dans N.

c) Le sens direct est évident. Montrons la réciproque : on suppose donc $N_0 = \{\mathrm{id}\}$. Soit $g \in N$. L'application $\varphi_g : \mathrm{SO}(V,f) \to N$ définie par $h \mapsto [h,g]$ est continue, donc $\mathrm{Im}\,(\varphi_g) \subset N_0 = \{\mathrm{id}\}$. Cela assure que $g \in Z(\mathrm{SO}(V,f))$, donc $N \subset Z(\mathrm{SO}(V,f))$. Or le cours assure que $Z(\mathrm{SO}(V,f)) = \{\mathrm{id}\}$, donc $N = \{\mathrm{id}\}$.

d) Il est clair que φ est continue (c'est la restriction d'une application linéaire). Pour tout $r \in \mathrm{SO}(V,f)$, l'exercice 2 assure qu'il existe une base e de V et $\theta \in [0, 2\pi[$ tels que

$$\mathrm{Mat}_e(r) = \begin{pmatrix} 1 & 0 \\ 0 & R_\theta \end{pmatrix},$$

donc $\varphi(r) = \cos(\theta)$. Cela assure que φ est bien à valeurs dans $[-1;1]$.

e) Puisque $N \neq \{id\}$, la question c) assure que $N_0 \neq \{\mathrm{id}\}$. Donc il existe $g \neq \mathrm{id}$ dans N_0. Notons $\varphi(g) = \cos(\theta)$, avec $\theta \in]-\pi;\pi] \setminus \{0\}$. Or $g^{-1} \in N_0$, et $\varphi(g^{-1}) = -\theta$, donc on supposer que $\theta \in]0;\pi]$.
Si $\frac{\pi}{2} \leq \theta \leq \pi$, le résultat est démontré.
Sinon, on pose $N := E\left(\frac{\pi}{2\theta}\right)$. On a alors

$$N\theta \leq \frac{\pi}{2} < (N+1)\theta \leq \frac{\pi}{2} + \theta \leq \pi,$$

donc $s := g^{N+1} \in N_0$ convient.

f) Le groupe N_0 est connexe, et φ est clairement continue, donc $\varphi(N_0)$ est un connexe de $[-1,1]$ contenant $\varphi(g) \leq 0$ et $\varphi(\mathrm{id}) = 1$. Or, les connexes de $\mathbb{R}$ sont les intervalles, donc il existe $g \in N$ tel que $\varphi(g) = 0$, c'est-à-dire que N_0 contient une rotation d'angle $\pm\frac{\pi}{2}$. Alors l'élément $R := g^2 \in N_0$ est donc un renversement. Donc la question a) assure que $N = \mathrm{SO}(V,f)$, donc $\mathrm{SO}(V,f)$ est un groupe simple.

Exercice 5 : $\star\star$

Soit V un $\mathbb{R}$-espace vectoriel de dimension $n \geq 5$ muni de la forme quadratique définie positive $f(x_1,\ldots,x_n) = x_1^2 + \cdots + x_n^2$. Le but de cet exercice est de montrer que $\mathrm{PSO}(V,f)$ est simple. Soit $\overline{N}$ un sous-groupe distingué non trivial de $\mathrm{PSO}(V,f)$ et soit N le sous-groupe de $\mathrm{SO}(V,f)$ lui correspondant.

a) Montrer que si N contient un renversement, alors $\overline{N} = \mathrm{PSO}(V,f)$.

b) Supposons qu'il existe un sous-espace U de V de dimension 3 tel que $N \cap \mathrm{SO}(U, f|_U) \neq \{\mathrm{id}\}$. Montrer qu'alors $\overline{N} = \mathrm{PSO}(V,f)$.

c) Conclure (on pourra considérer le commutateur d'un élément $r \in N \setminus \{\pm\mathrm{id}\}$ ayant un vecteur fixe non nul avec la composée de deux réflexions bien choisies).

Solution de l'exercice 5.

a) C'est exactement le même raisonnement que la question a) de l'exercice 4 : les renversements engendrent $\mathrm{SO}(V,f)$ et sont tous conjugués dans $\mathrm{SO}(V,f)$.

b) Par hypothèse, $N' := N \cap \mathrm{SO}(U,f)$ est un sous-groupe distingué non trivial de $\mathrm{SO}(U,f)$. Donc l'exercice 4 assure que $N' = \mathrm{SO}(U,f)$, donc N' contient un renversement r de (U,f). Il suffit alors de prolonger r en $r' \in \mathrm{SO}(V,f)$ en demandant que $r'_{|_{U^\perp}} = \mathrm{id}_{U^\perp}$, ce qui fournit un renversement $r' \in N$, donc par la question a), on a $\overline{N} = \mathrm{PSO}(V,f)$.

c) On cherche à construire un sous-espace U de dimension 3 satisfaisant les hypothèses de la question précédente. Comme $N \neq \{\pm id\}$, il existe $u \in N$ tel que $u \neq \pm\mathrm{id}$. Par conséquent, il existe un plan $P \subset V$ tel que $u(P) \neq P$. Notons $r \in \mathrm{SO}(V,f)$ le renversement de plan P. On pose $\rho := [u,r]$. Alors $\rho \in N$ car N est distingué, et ρ est le produit de deux renversements, à savoir uru^{-1} renversement de plan $u(P)$, et r^{-1} renversement de plan P. Donc cela assure que la restriction de ρ à $P^\perp \cap u(P)^\perp$ est l'identité. Or $\dim(P^\perp \cap u(P)^\perp) \geq n-4 \geq 4$ (car $n \geq 5$). Donc ρ a un vecteur fixe $a \in V \setminus \{0\}$. Remarquons également que $\rho \neq \pm\mathrm{id}$ car $u(P) \neq P$.

Il existe également $b \in V$ tel que la famille $(b, \rho(b))$ soit libre. On note $c := \rho(b)$.

Définissons $\sigma := s_b \circ s_a$ (où s_x désigne la réflexion orthogonale d'hyperplan $x^\perp$), et considérons $s := [\rho, \sigma]$. Alors comme N est distingué, on voit que $s \in N$. Et on vérifie que

$$s = s_{\rho(b)} s_{\rho(a)} s_a s_b = s_c s_a s_a s_b = s_c s_b$$

est un produit de deux réflexions distinctes, donc $s \in N$ fixe un sous-espace $W \subset V$ de dimension $n-2$ et $s \neq \pm\mathrm{id}$. Alors il suffit de considérer un sous-espace $U \subset V$ de dimension 3 contenant $H^\perp$, et de considérer l'élément $s \in N \cap \mathrm{SO}(U,f)$, puis de conclure via la question b).

Exercice 6 : $\star\star$

On note $\mathbb{Z}_{(2)}$ le sous-anneau de $\mathbb{Q}$ formé des rationnels à dénominateur impair. On note $G = \mathrm{O}_3(\mathbb{Q})$.

a) Montrer que $G \subset \mathrm{Mat}_3(\mathbb{Z}_{(2)})$.

b) Pour tout $n \in \mathbb{N}^*$, on pose $G_n := \{A \in G : \exists B \in \mathrm{Mat}_3(\mathbb{Z}_{(2)}),\ A = I_3 + 2^n B\}$. Montrer que G_n est un sous-groupe distingué de G.

c) Montrer que $\bigcap_{n\in\mathbb{N}^*} G_n = \{I_3\}$.

d) Montrer que $G_1 \subsetneq G$ et que $G_1 \not\subset \mathrm{SO}_3(\mathbb{Q})$.

e) Montrer que pour tout $n \geq 1$, $G_{n+1} \subsetneq G_n$.

f) Montrer que pour tout $n \geq 2$, $G_n \subset \mathrm{SO}_3(\mathbb{Q})$.

g) Pour tout $n \geq 2$, montrer que $G_n/G_{n+1} \cong (\mathbb{Z}/2\mathbb{Z})^3$.

h) Montrer que $G/G_1 \cong \mathfrak{S}_3$.

i) Montrer que $G_1/G_2 \cong (\mathbb{Z}/2\mathbb{Z})^4$.

j) Comparer la structure de $\mathrm{O}_3(\mathbb{Q})$ avec celle de $\mathrm{O}_3(\mathbb{R})$.

Solution de l'exercice 6. Remarquons pour commencer que le quotient de l'anneau $\mathbb{Z}_{(2)}$ par l'idéal (2^n) engendré par l'élément 2^n est canoniquement isomorphe à $\mathbb{Z}/2^n\mathbb{Z}$, ce qui permet de formuler certaines démonstrations qui suivent de façon un peu plus concise. Par soucis de simplicité, on n'utilisera pas explicitement cette description dans ce corrigé.

a) Soit $A \in G$, et soit $(x,y,z) \in \mathbb{Q}^3$ un vecteur colonne de A. Alors on a $x^2+y^2+z^2 = 1$. Supposons que l'un des rationnels x,y,z ait un dénominateur pair. On multiplie alors l'égalité précédente par le ppcm des dénominateurs pour obtenir une inégalité du type

$$a^2 + b^2 + c^2 = d^2$$

avec $a,b,c,d \in \mathbb{Z}$, d pair et a, b ou c impair. Par symétrie, supposons a impair. On réduit cette égalité modulo 4. On obtient

$$1 + b^2 + c^2 \equiv 0\,[4]\,.$$

Or les seuls carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1, donc l'égalité précédente modulo 4 est contradictoire. Cela assure que tous les dénominateurs des coefficients de A sont impairs, donc $A \in \mathrm{Mat}_3(\mathbb{Z}_{(2)})$.

b) Un calcul simple assure que G_n est un sous-groupe distingué de G.

c) Soit $A = (a_{i,j}) \in \bigcap_{n\in\mathbb{N}^*} G_n$. Alors pour tout $i \neq j$, pour tout $n \geq 1$, le numérateur de $a_{i,j}$ est divisible par 2^n, donc $a_{i,j} = 0$. Et pour tout i, il existe $b \in \mathbb{Z}_{(2)}$ tel que $a_{i,i} = 1 + 4b$, et $a_{i,i} \in \{\pm 1\}$, donc $a_{i,i} = 1$. Donc $A = I_3$.

d) On considère la matrice de permutation suivante

$$A := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

Il est clair que $A \in G$ et $A \notin G_1$.
De même, la matrice

$$B := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

est dans G_1 mais pas dans $\mathrm{SO}_3(\mathbb{Q})$.

e) L'inclusion $G_{n+1} \subset G_n$ est évidente. Montrons qu'elle est stricte. Pour cela, on considère, dans le cas $n \geq 2$, la matrice

$$A_n := \begin{pmatrix} \frac{1-4^{n-1}}{1+4^{n-1}} & \frac{2^n}{1+4^{n-1}} & 0 \\ -\frac{2^n}{1+4^{n-1}} & \frac{1-4^{n-1}}{1+4^{n-1}} & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3 + 2^n \begin{pmatrix} -\frac{2^{n-1}}{1+4^{n-1}} & \frac{1}{1+4^{n-1}} & 0 \\ -\frac{1}{1+4^{n-1}} & -\frac{2^{n-1}}{1+4^{n-1}} & 0 \\ 0 & 0 & 0 \end{pmatrix} .$$

On voit donc que $A_n \in G_n \setminus G_{n+1}$.
Dans le cas $n = 1$, on considère la matrice

$$A_1 := \begin{pmatrix} \frac{1}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \\ \frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \end{pmatrix} = I_3 + 2 \begin{pmatrix} -\frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \\ \frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \end{pmatrix} .$$

Donc $A_1 \in G_1$ et $A_1 \notin G_2$. Une variante est donnée par la matrice $B_1 := \mathrm{diag}(1, 1, -1)$.

f) Soit $A \in G_n$, avec $n \geq 2$. Par définition, il existe $B \in \mathrm{Mat}_3(\mathbb{Z}_{(2)})$ tel que $A = I_3 + 4B$. La multilinéarité du déterminant assure que $\det(A) = 1 + 4d$, pour un certain $d \in \mathbb{Z}_{(2)}$. Or A est orthogonale, donc $\det(A) \in \{\pm 1\}$, et l'égalité précédente assure que $\det(A) = 1$ (car 4 ne divise pas 2 dans l'anneau $\mathbb{Z}_{(2)}$). Donc $G_n \subset \mathrm{SO}_3(\mathbb{Q})$.

g) On considère l'application $\pi_n : G_n \to \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z})$ définie par $\pi_n(I_3 + 2^n B) := \overline{B}$, où si $B = (b_{i,j})$, les coefficients $(\overline{b_{i,j}})$ de $\overline{B}$ sont définis par $\overline{b_{i,j}} = 0$ si le numérateur de $b_{i,j}$ est pair, et $\overline{b_{i,j}} = 1$ si celui-ci est impair. On vérifie que π_n est un morphisme de groupes, notamment que $\pi_n(AA') = \pi_n(A) + \pi_n(B)$. En outre, il est clair que $\mathrm{Ker}(\pi_n) = G_{n+1}$, donc le théorème de factorisation assure que π_n induit un morphisme injectif

$$\overline{pi}_n : G_n/G_{n+1} \to \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z}) .$$

Or pour tout $A = I_3 + 2^n B \in G_n$, on a $A^t A = I_3$, donc $B + {}^t B + 2^n B^t B = 0$. Par conséquent, en regardant cette égalité modulo 2, on voit que

$$\mathrm{Im}\,(\overline{\pi}_n) \subset \{B \in \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z}) : b_{i,j} = b_{j,i} \text{ et } b_{i,i} = 0 \,\forall i, j\} \cong (\mathbb{Z}/2\mathbb{Z})^3 .$$

Enfin, on voit que cette inclusion est une égalité en regardant l'image par π_n de la matrice A_n introduite à la question e), ainsi que les matrices obtenues à partir de A_n en permutant les vecteurs de la base. Donc finalement $G_n/G_{n+1} \cong (\mathbb{Z}/2\mathbb{Z})^3$

h) On considère le morphisme de groupes $\pi_0 : G \to \mathrm{O}_3(\mathbb{F}_2)$ défini par $\pi_0(A) := \overline{A}$, où $\overline{A}$ est défini comme en g) et $\mathrm{O}_3(\mathbb{F}_2)$ désigne l'ensemble des matrices A de $\mathrm{Mat}_3(\mathbb{F}_2)$ telles que ${}^t AA = A^t A = I_3$. Un calcul simple assure que $\mathrm{O}_3(\mathbb{F}_2) \cong \mathfrak{S}_3$ via les matrices de permutations. Or toute matrice de permutations dans G s'envoie par π_0 sur la matrice de permutations correspondante dans $\mathrm{O}_3(\mathbb{F}_2)$, ce qui assure que π_0 est surjectif. Enfin, par définition, on a bien $\mathrm{Ker}(\pi_0) = G_1$, donc $G/G_1 \cong \mathfrak{S}_3$.

i) On raisonne comme en g). On considère le morphisme de groupes $\pi_1 : G_1 \to \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z})$ définie par $\pi_1(I_3 + 2B) := \overline{B}$. On a toujours $\mathrm{Ker}(\pi_1) = G_2$, et l'image de π_1 se calcule en réduisant modulo 2 l'égalité déjà rencontrée $B + {}^tB + 2B{}^tB = 0$: on voit que $\mathrm{Im}\,(\pi_1)$ est contenu dans $\{B \in \mathrm{Mat}_3(\mathbb{Z}/2\mathbb{Z}) : b_{i,j} = b_{j,i} \text{ et } \sum_{k\neq i} b_{i,k} = 0\,\forall i,j\}$. Or ce dernier sous-groupe de $\mathrm{Mat}_2(\mathbb{Z}/2\mathbb{Z})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$, engendré par les trois matrices ayant un unique coefficient non nul, situé sur la diagonale, et par la matrice dont tous les coefficients valent 1. Et ces quatre matrices sont bien dans l'image de π_1, ce que l'on voit en utilisant les matrices A_1 et B_1 de la question e). Donc $G_1/G_2 \cong (\mathbb{Z}/2\mathbb{Z})^4$.

j) Il suffit de reprendre toutes les questions précédentes. Le groupe $\mathrm{O}_3(\mathbb{Q})$ n'est pas du tout un groupe simple (ni $\mathrm{SO}_3(\mathbb{Q})$), contrairement à $\mathrm{SO}_3(\mathbb{R})$. En fait, on a montré que $G = \mathrm{O}_3(\mathbb{Q})$ est un groupe pro-résoluble, au sens où la suite de sous-groupes $D^n(G)$ vérifie $\bigcap_{n\in\mathbb{N}} D^n(G) = \{\mathrm{id}\}$. Plus précisément, on peut dire que G est une limite (projective dénombrable) de groupes résolubles finis.

Exercice 7 : $\star\star\star$

Soient $K = \mathbb{F}_q$ un corps fini de caractéristique impaire et $n \in \mathbb{N}^*$. On note $\mathrm{P}\Omega_n^{\pm}(K)$ le quotient du groupe dérivé de $\mathrm{O}_n^{\pm}(K)$ par son centre.

a) Déterminer $\mathrm{O}_1(K)$, $\mathrm{SO}_1(K)$ et $\mathrm{P}\Omega_1(K)$.

b) Montrer que $\mathrm{O}_2^+(K)$ est isomorphe au groupe diédral D_{q-1}. Identifier $\mathrm{SO}_2^+(K)$ et $\mathrm{P}\Omega_2^+(K)$.

c) En considérant le corps $\mathbb{F}_{q^2}$, montrer que $\mathrm{O}_2^-(K)$ est isomorphe à D_{q+1} et identifier $\mathrm{SO}_2^-(K)$ et $\mathrm{P}\Omega_2^-(K)$.

d) On suppose $n = 3$. On note V le K-espace vectoriel des matrices 2×2 de trace nulle.

i) Exhiber une base naturelle de V comme K-espace vectoriel.

ii) Montrer que $\mathrm{GL}_2(K)$ agit naturellement sur V.

iii) En déduire un morphisme de groupes $\rho : \mathrm{GL}_2(K) \to \mathrm{GL}(V) \cong \mathrm{GL}_3(K)$ que l'on explicitera.

iv) Montrer que $Ker(\rho) = K^*I_2$.

v) Montrer que pour tout $A \in \mathrm{GL}_2(K)$, $\det(\rho(A)) = 1$.

vi) Vérifier que le déterminant définit une forme quadratique non dégénérée sur V.

vii) En déduire des isomorphismes $\mathrm{PGL}_2(K) \cong \mathrm{SO}(V, \det) \cong \mathrm{SO}_3(K)$.

viii) Montrer que l'on a des isomorphismes $\mathrm{PGL}_2(K) \times \{\pm 1\} \cong \mathrm{O}(V, \det) \cong \mathrm{O}_3(K)$.

ix) Montrer que $\mathrm{P}\Omega_3(K) \cong \mathrm{PSL}_2(K)$.

e) On suppose $n = 4$. On note $W := \mathrm{Mat}_2(K)$, et pour tout $M \in W$, on note $Q(M) := \det(M)$.

i) Montrer que Q est une forme quadratique sur W qui est somme de deux plans hyperboliques.

ii) Montrer que $\mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ agit naturellement sur W.

iii) Soit $A, B \in \mathrm{GL}_2(K)$. Montrer que l'action de (A, B) sur W préserve Q si et seulement si $\det(A) = \det(B)$, et que cette action est triviale si et seulement s'il existe $\lambda \in K^*$ tel que $A = B = \lambda I_2$.

iv) En déduire un morphisme de groupes injectif $i : ((\mathrm{SL}_2(K) \times \mathrm{SL}_2(K)) \rtimes K^*)/K^* \to \mathrm{O}(W, Q)$, où l'on explicitera le groupe de gauche.

v) Montrer que $\langle \mathrm{Im}\,(i), T\rangle = \mathrm{O}(W, Q)$, où $T : W \to W$ est défini par $T(M) := {}^tM$ et décrire $\mathrm{SO}(W, Q)$.

vi) En déduire que $\mathrm{P}\Omega_4^+(K) \cong \mathrm{PSL}_2(K) \times \mathrm{PSL}_2(K)$ si $|K| > 3$.

vii) Décrire $\mathrm{P}\Omega_4^+(\mathbb{F}_3)$.

Solution de l'exercice 7.

a) Il est clair que $\mathrm{O}_1(K) = \{\pm 1\}$, $\mathrm{SO}_1(K) = \{1\}$ et $\mathrm{P}\Omega_1(K) = \{1\}$.

b) Le cours (ou un calcul simple) assure que

$$\mathrm{O}_2^+(K) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} : \lambda \in K^* \right\} \bigcup \left\{ \begin{pmatrix} 0 & \mu \\ \mu^{-1} & 0 \end{pmatrix} : \mu \in K^* \right\}.$$

Or K^* est un groupe cyclique, donc en notant ζ un générateur de ce groupe, on pose

$$R := \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \text{ et } S := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On voit alors que $\mathrm{O}_2^+(K) = \langle R, S \rangle$, que $\mathrm{O}_2^+(K)$ est d'ordre $2(q-1)$, que R est d'ordre $q-1$, S est d'ordre 2, et $RS = SR^{-1}$, ce qui assure que $\mathrm{O}_2^+(K)$ est isomorphe au groupe diédral D_{q-1} (groupe des isométries planes réelles d'un polygone régulier à $q-1$ côtés), l'isomorphisme envoyant R sur la rotation de centre O (isobarycentre des sommets du polygone) et d'angle $\frac{2\pi}{q-1}$ et S sur une symétrie axiale d'axe joignant deux sommets du polygone. On en déduit que $\mathrm{SO}_2^+(K) = \langle R \rangle \cong \mathbb{Z}/(q-1)\mathbb{Z}$ et $\mathrm{P}\Omega_2^+(K) = \{1\}$.

c) On fixe un élément $\varepsilon \in K^* \setminus (K^*)^2$, et on définit $L := K(\sqrt{\varepsilon}) := \{x + y\sqrt{\varepsilon} : x, y \in K\}$ (que l'on peut aussi définir comme $L := K[X]/(X^2 - \varepsilon)$). Il est clair que L est un corps contenant K comme sous-corps, de sorte que L est un K-espace vectoriel de dimension 2. On munit L de l'application "norme" $N : L \to K$ définie par $N(x + y\sqrt{\varepsilon}) := x^2 - \epsilon y^2$. Il est clair que N est une form quadratique sur le K-espace vectoriel L, de sorte que $\mathrm{O}(L, N) \cong \mathrm{O}_2^-(K)$. En outre, on voit que N induit un morphisme de groupes $N : L^* \to K^*$ tel que $N(x) = x^{q+1}$ pour tout $x \in L^*$. Puisque L^* est cyclique de cardinal $q^2 - 1$, on voit que N est surjectif de noyau $A := \{x \in L^* : x^{q+1} = 1\}$ cyclique de cardinal $q+1$. Or, pour tout $x \in A$, on définit $m_x : L \to L$ par $m_x(y) := xy$. Il est clair que m_x est K-linéaire et pour tout $y \in L$, on a bien $N(m_x(y)) = N(xy) = N(x)N(y) = N(y)$, donc $m_x \in \mathrm{O}(L, N)$. On en déduit donc un morphisme de groupes injectif $A \hookrightarrow \mathrm{SO}(L, N)$ défini par $x \mapsto m_x$ (il est clair que $\det(m_x) = 1$). On dispose également de l'automorphisme de Frobenius $\mathrm{Fr} : L \to L$ défini par $\mathrm{Fr}(x) := x^q$: on voit que $\mathrm{Fr} \in \mathrm{O}(L, N) \setminus \mathrm{SO}(L, N)$ et que Fr est d'ordre 2. Par cardinalité (voir exercice 3), on en déduit que $\langle A, \mathrm{Fr} \rangle = \mathrm{O}(L, N)$. On vérifie enfin que $m_x \circ \mathrm{Fr} = \mathrm{Fr} \circ m_x^{-1}$, ce qui assure que $\mathrm{O}_2^-(K) \cong D_{q+1}$, $\mathrm{SO}_2^-(K) \cong \mathbb{Z}/(q+1)\mathbb{Z}$ et $\mathrm{P}\Omega_2^-(K) = \{1\}$.

d) i) Une base de V est donnée par les matrices suivantes :

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

ii) L'action de $\mathrm{GL}_2(K)$ sur V est définie par $A \cdot M := AMA^{-1}$ pour tout $A \in \mathrm{GL}_2(K)$ et $M \in V$.

iii) Le morphisme est induit par l'action précédente, qui est bien linéaire. Explicitement, on voit que dans la base donnée en d)i), on a :

$$\rho\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \frac{1}{ad - bc} \begin{pmatrix} a^2 & -b^2 & -2ab \\ -c^2 & d^2 & 2cd \\ -ac & bd & ad + bc \end{pmatrix}.$$

iv) La formule explicite de la question d)iii) assure que $\mathrm{Ker}(\rho) = K^* I_2$.

v) C'est un calcul avec la formule de la question d)iii).

vi) Soit $A = \begin{pmatrix} z & x \\ y & -z \end{pmatrix} \in V$. Alors $\det(A) = -z^2 - xy$ est clairement une forme quadratique non dégénérée (de rang 3) sur V.

vii) Les questions d)iii), d)iv), d)v), et le fait que l'action considérée préserve le déterminant sur V, assurent que le morphisme ρ induit un morphisme de groupes injectif

$$\overline{\rho} : \mathrm{PGL}_2(K) \hookrightarrow \mathrm{SO}(V, \det) \cong \mathrm{SO}_3(K).$$

En calculant les cardinaux des deux groupes, on voit que ceux-ci ont tous les deux pour cardinal $q(q-1)(q+1)$, donc $\overline{\rho}$ est un isomorphisme de groupes.

viii) Comme V est de dimension impaire, on voit que $-\mathrm{id}_V \in \mathrm{O}(V,\det) \setminus \mathrm{SO}(V,\det)$, ce qui permet d'obtenir l'isomorphisme $\mathrm{O}_3(K) \cong \mathrm{SO}_3(K) \times \{\pm I_3\}$. On conclut en utilisant la question d)viii).

ix) Avec les questions précédentes, il suffit de dire que le groupe de dérivé de $\mathrm{GL}_2(K)$ est $\mathrm{SL}_2(K)$ pour conclure que $\Omega_3(K) \cong \mathrm{PSL}_2(K)$. Enfin, le centre de $\mathrm{PSL}_2(K)$ est trivial, ce qui assure que $\mathrm{P}\Omega_3(K) \cong \mathrm{PSL}_2(K)$.

e) i) Soit $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in W$. On a $\det(M) = xt - yz$, donc on voit que $Q = \det$ est une forme quadratique sur W qui est somme de deux plans hyperboliques : les plans $\{x = t = 0\}$ et $\{y = z = 0\}$.

ii) Pour tout $(A, B) \in \mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ et tout $M \in W$, on pose $(A, B) \cdot M := AMB^{-1}$. Cela définit bien une action de groupe.

iii) Soient $(A, B) \in \mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ et $M \in W$. On a $Q((A, B) \cdot M) = \det(A) \det(B)^{-1} Q(M)$. Donc (A, B) préserve Q si et seulement si $\det(A) = \det(B)$.

En outre, (A, B) agit trivialement sur W si et seulement si pour tout $M \in W$, on a $AM = MB$ si et seulement si $A = B$ et pour tout $M \in W$, $AM = MA$ si et seulement si $A = B$ et $A \in Z(\mathrm{GL}_2(K)) = K^* I_2$.

iv) On note G le sous-groupe de $\mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ formé des couples de matrices $(A, B) \in \mathrm{GL}_2(K) \times \mathrm{GL}_2(K)$ tels que $\det A = \det B$. On dispose d'une action de K^* sur $\mathrm{SL}_2(K)$ donnée par une section de la suite exacte

$$A \to \mathrm{SL}_2(K) \to \mathrm{GL}_2(K) \xrightarrow{\det} K^* \to 1\,.$$

Par exemple, on peut considérer l'action donnée par $\lambda \cdot A := \mathrm{diag}(\lambda, 1) A \mathrm{diag}(\lambda^{-1}, 1)$, pour tout $\lambda \in K^*$ et $A \in \mathrm{SL}_2(K)$. Pour simplifier, on notera $s(\lambda) := \mathrm{diag}(\lambda, 1)$.

On en déduit une action diagonale de K^* sur $\mathrm{SL}_2(K) \times \mathrm{SL}_2(K)$, ce qui permet de définir un produit semi-direct $(\mathrm{SL}_2(K) \times \mathrm{SL}_2(K)) \rtimes K^*$. On voit facilement que l'on a un isomorphisme naturel $G \cong (\mathrm{SL}_2(K) \times \mathrm{SL}_2(K)) \rtimes K^*$. Considérons alors le morphisme de groupes $\varphi : G \to \mathrm{O}(W, Q)$ défini par $\varphi(A, B) : M \mapsto AMB^{-1}$.

Alors la question e)iii) assure que $\mathrm{Ker}(\varphi) = \cong K^*$, donc φ induit un morphisme de groupes injectif $i = \overline{\varphi} : G/K^* \to \mathrm{O}(W, Q)$.

v) Un calcul simple (utilisant par exemple le produit de Kronecker des matrices, i.e. le produit tensoriel des matrices) assure que le déterminant de $\varphi(A, B)$ vaut $\det(A)^2 \det(B)^{-2} = 1$. Donc φ est à valeur dans $\mathrm{SO}(W, Q)$. On a donc un morphisme de groupes injectif $i = \overline{\varphi} : G/K^* \to \mathrm{SO}(W, Q)$, et on voit que $T \in \mathrm{O}(W, Q) \setminus \mathrm{SO}(W, Q)$. Donc $\langle \mathrm{Im}\,(i), T \rangle \subset \mathrm{O}(W, Q)$.

On calcule alors les cardinaux des groupes en question (en utilisant notamment l'exercice 3) : on a $|G/K^*| = |\mathrm{SL}_2(K)|^2 = q^2(q-1)^2(q+1)^2$, $|\mathrm{SO}(W, Q)| = |\mathrm{SO}_4^+(K)| = q^2(q^2-1)(q^2-1)$, donc l'égalité des cardinaux assure que $i : G/K^* \to \mathrm{SO}(W, Q)$ est un isomorphisme.

Or $\mathrm{SO}(W, Q)$ est un sous-groupe d'indice 2 dans $\mathrm{O}(W, Q)$, donc $\langle \mathrm{Im}\,(i), T \rangle = \mathrm{O}(W, Q)$.

vi) La question précédente assure que $\Omega_4^+(K) \cong D((\mathrm{SL}_2(K) \times \mathrm{SL}_2(K))/K^*$, donc si $|K| > 3$, on a $\Omega_4^+(K) \cong (\mathrm{SL}_2(K) \times \mathrm{SL}_2(K))/K^*$. On en déduit alors $\mathrm{P}\Omega_4^+(K) \cong \mathrm{PSL}_2(K) \times \mathrm{PSL}_2(K)$ si $|K| > 3$.

vii) On a vu que $\mathrm{SO}_4^+(\mathbb{F}_3) \cong G/K^*$. Comme $D(\mathrm{SL}_2(\mathbb{F}_3)) \subset \mathrm{SL}_2(\mathbb{F}_3)$ est isomorphe au groupe $\mathbf{H}_8$ des quaternions d'ordre 8 (voir par exemple TD4, exercice 10), et comme $D(\mathrm{GL}_2(\mathbb{F}_3)) = \mathrm{SL}_2(\mathbb{F}_3)$, on constate que $\Omega_4^+(\mathbb{F}_3) \cong (\mathrm{SL}_2(\mathbb{F}_3) \times \mathrm{SL}_2(\mathbb{F}_3))/\mathbb{F}_3^*$, donc $\mathrm{P}\Omega_4^+(\mathbb{F}_3) \cong \mathrm{PSL}_2(\mathbb{F}_3) \times \mathrm{PSL}_2(\mathbb{F}_3)$.

Exercice 8 :

On considère $V = \mathbb{F}_2^6$ muni de la forme bilinéaire $x \cdot y = \sum_{i=1}^6 x_i y_i$. On note $x_0 := (1, \ldots, 1) \in V$.

a) Donner la définition des groupes $\mathrm{Sp}_n(K)$ lorsque K est un corps de caractéristique 2.

b) Montrer que $W := x_0^\perp / \mathbb{F}_2 x_0$ est naturellement muni d'une forme bilinéaire alternée non dégénérée.

c) En déduire un morphisme naturel $\mathfrak{S}_6 \to \mathrm{Sp}_4(\mathbb{F}_2)$.

d) Conclure que $\mathrm{Sp}_4(\mathbb{F}_2) \cong \mathfrak{S}_6$.

Solution de l'exercice 8.

a) voir le cours.

b) Pour tout $x \in V$, on a $x \cdot x = x \cdot x_0$. Donc pour tout $x \in x_0^\perp$, $x \cdot x = 0$. Cela assure que la restriction de la forme bilinéaire au sous-espace $x_0^\perp$ de dimension 5 est une forme bilinéaire alternée. Son noyau est exactement la droite engendré par x_0, donc cette forme alternée induit une forme alternée b non dégénérée sur $W = x_0^\perp/\mathbb{F}_2 x_0$.

c) L'action de $\mathfrak{S}_6$ sur V par permutation des coordonnées induit une action de $\mathfrak{S}_6$ sur W, dont on voit facilement qu'elle préserve la forme symplectique précédente. On en déduit donc un morphisme de groupes injectif $\mathfrak{S}_6 \to \mathrm{Sp}(W, b) \cong \mathrm{Sp}_4(\mathbb{F}_2)$.

d) On calcule les cardinaux et on voit que $|\mathfrak{S}_6| = 6! = 720$ et $|\mathrm{Sp}_4(\mathbb{F}_2)| = 15.8.3.2 = 720$ (le cardinal des groupes $\mathrm{Sp}2n(\mathbb{F}_q)$ se calcule de façon analogue à celui des groupes orthogonaux : cf exercice 3). On en déduit donc que le morphisme de la question précédente est un isomorphisme, i.e. $\mathrm{Sp}_4(\mathbb{F}_2) \cong \mathfrak{S}_6$.

Exercice 9 : $\star\star\star$

Soit K un corps de caractéristique différente de 2 et soit $m \geq 3$. On munit $V = K^{2m}$ de la forme bilinéaire alternée usuelle B ; on note $\mathrm{Sp}_{2m}(K)$ le groupe symplectique correspondant. Soient $s, t \in \mathrm{Sp}_{2m}(K)$ des involutions.

a) Montrer qu'il existe une décomposition $V = E_+(s) \overset{\perp}{\oplus} E_-(s)$, où $E_+(s)$ et $E_-(s)$ désignent les espaces propres de s associées aux valeurs propres 1 et -1, respectivement.

b) En déduire une bijection entre l'ensemble des involutions de $\mathrm{Sp}_{2m}(K)$ et l'ensemble des sous-espaces non dégénérés de V.

On dit que l'involution s est de type $(2r, 2m-2r)$ si l'espace $E_+(s)$ est de dimension $2r$. On parle d'*involution extrémale* pour une involution de type $(2, 2m-2)$ ou $(2m-2, 2)$. Dans ce cas-là, on note $E_2(s)$ l'espace $E_\pm(s)$ de dimension 2.

c) En considérant les familles commutatives maximales d'involutions conjuguées dans $\mathrm{Sp}_{2m}(K)$, montrer que tout automorphisme de $\mathrm{Sp}_{2m}(K)$ envoie une involution extrémale sur une involution extrémale.

On dit que des involutions extrémales s et t forment un *couple minimal* si on a $\dim(E_2(s) \cap E_2(t)) = 1$. Si $\mathcal{S} \subseteq \mathrm{Sp}_{2m}(K)$ est un ensemble d'involutions extrémales, on note $C(\mathcal{S})$ l'ensemble des involutions extrémales qui commutent à tout élément de $\mathcal{S}$.

d) Montrer que s et t forment un couple minimal si et seulement si ($st \neq ts$ et pour tous $s', t' \in C(C(\{s,t\}))$ avec $s't' \neq t's'$ on a $C(C(\{s,t\})) = C(C(\{s',t'\}))$).

e) Déterminer les ensembles maximaux I d'involutions extrémales tels que toute paire d'éléments de I forme un couple minimal ou commute.

Soit $n \geq 3$. Une application $\phi : K^n \to K^n$ est dite semi-linéaire s'il existe un automorphisme de corps $\theta : K \to K$ tel que ϕ soit θ-linéaire, c'est-à-dire :

- On a $\phi(v + v') = \phi(v) + \phi(v')$, pour tous $v, v' \in K^n$.
- On a $\phi(\lambda v) = \theta(\lambda)\phi(v)$, pour tout $v' \in K^n$ et tout $\lambda \in K$.

L'ensemble des applications semi-linéaires inversibles forment un groupe, noté $\Gamma\mathrm{L}_n(K)$ et appelé le groupe des transformations semi-linéaires de K^n.

On admet le théorème fondamental de la géométrie projective, qui est l'énoncé suivant : *soit* $\phi : \mathbb{P}^n(K) \to \mathbb{P}^n(K)$ *une bijection telle que trois points* A_1, A_2, A_3 *de* $\mathbb{P}^n(K)$ *sont alignés si et seulement si* $\phi(A_1), \phi(A_2), \phi(A_3)$ *le sont. Alors il existe un automorphisme de corps* $\sigma : K \to K$ *et une transformation* σ*-linéaire* $\gamma \in \Gamma\mathrm{L}_{n+1}(K)$ *telle que* ϕ *soit induite par* γ.

On définit enfin $\Gamma\mathrm{Sp}_{2m}(K)$ comme le sous-groupe de $\Gamma\mathrm{L}_{2m}(K)$ des éléments préservant la forme B.

f) Montrer que tout automorphisme de $\mathrm{Sp}_{2m}(K)$ est de la forme $x \mapsto axa^{-1}$ pour un certain élément $a \in \Gamma\mathrm{Sp}_{2m}(K)$.

Solution de l'exercice 9.

a) Une involution annule le polynôme $X^2 - 1$, d'où une décomposition $V = E_+(s) \oplus E_-(s)$. Cette dernière est B-orthogonale puisque si e_+ et e_- sont des éléments respectivement de $E_+(s)$ et $E_-(s)$, alors on a

$$-B(e_+, e_-) = B(s(e_+), s(e_-)) = B(e_+, e_-)\,,$$

donc $B(e_+, e_-) = 0$.

b) L'application $s \mapsto E_+(s)$ est la bijection souhaitée.

c) Soit $\mathcal{F}$ une telle famille. Elle est composée d'involutions de type $(2r, 2m-2r)$ pour un r fixé (puisque les éléments de $\mathcal{F}$ sont conjugués). Comme ils commutent, tous les éléments de $\mathcal{F}$ se diagonalisent dans une base symplectique commune. Aussi, il convient de remarquer que si V a pour base symplectique $(e_1, e_2, \ldots, e_{2m})$ avec $b(e_{2i-1}, e_{2i}) = -b(e_{2i}, e_{2i-1}) = 1$, et $b(e_i, e_j) = 0$ sinon, alors on a $e_{2j} \in E_+(s) \Leftrightarrow e_{2j-1} \in E_+(s)$. De ce fait, $E_+(s)$ est déterminé par un choix de r vecteurs, et on a $|\mathcal{F}| \leq \binom{m}{r}$.
En particulier si s est une involution extrémale, alors elle est incluse dans une famille maximale, à m éléments, d'involutions conjuguées commutant deux-à-deux. Parce que cette dernière propriété est conservée par un automorphisme de $\mathrm{Sp}_{2m}(K)$ et parce que l'on a $\binom{m}{r} \neq m$ pour $r \notin \{1, m-1\}$, tout automorphisme de $\mathrm{Sp}_{2m}(K)$ envoie involutions extrémales sur involutions extrémales.

d) Si s et t sont deux involutions extrémales avec $s \neq \pm t$, on a

$$C(\{s,t\}) = \{u \text{ extrémale} \mid E_2(u) \subseteq E_{2m-2}(s) \cap E_{2m-2}(t),\ E_{2m-2}(u) \supseteq E_2(s) + E_2(t)\}.$$

On en déduit

$$C(C(\{s,t\})) = \{u \text{ extrémale} \mid E_2(u) \subseteq E_2(s) + E_2(t),\ E_{2m-2}(u) \supseteq E_{2m-2}(s) \cap E_{2m-2}(t)\}.$$

Si s et t forment un couple minimal, alors on a $st \neq ts$ puisqu'on a $\dim(E_2(t) \cap E_2(s)) = 1$ non paire. De plus, si $s', t' \in C(C(\{s,t\}))$ vérifient $s't' \neq t's'$, alors $E_2(s') + E_2(t') \subseteq E_2(s) + E_2(t)$, qui est de dimension 3. Ainsi on a $\dim(E_2(s') \cap E_2(t')) = 1$ et (s', t') est un autre couple minimal avec $E_2(s') + E_2(t') = E_2(s) + E_2(t)$. Il s'ensuit $E_{2m-2}(s') \cap E_{2m-2}(t') = E_{2m-2}(s) \cap E_{2m-2}(t)$ et $C(C(\{s', t'\})) = C(C(\{s,t\}))$.
Si s et t ne sont pas un couple minimal, alors on a $\dim(E_2(s) \cap E_2(t)) \in \{0, 2\}$. Dans le cas où cette dimension vaut 2, la question (b) donne $s = \pm t$ et on a alors $st = ts$. Supposons donc $E_2(s) \cap E_2(t) = \emptyset$. Dans ce cas-là, $E_2(s) + E_2(t)$ est de dimension 4, et on peut trouver s' et t' un couple minimal avec $E_2(s') + E_2(t') \subsetneqq E_2(s) + E_2(t)$ et $E_{2m-2}(s') \cap E_{2m-2}(t') \supsetneqq E_{2m-2}(s) \cap E_{2m-2}(t)$. On a alors $C(C(\{s', t'\})) \neq C(C(\{s,t\}))$.

e) Si $\pm s, \pm t, \pm u$ sont six éléments distincts de I, l'espace $E_2(s) \cap E_2(t) \cap E_2(u)$ est de dimension 1 ou 0. Dans le premier cas, on note V_1 la droite obtenue et dans le second cas, on a $E_2(u) \subseteq E_2(s) + E_2(t) =: V_3$. Les ensembles maximaux correspondants sont alors respectivement

$$I_1(V_1) := \{v \text{ involution extrémale} \mid V_1 \subseteq E_2(v)\},$$

$$I_3(V_3) := \{v \text{ involution extrémale} \mid E_2(v) \subseteq V_3\}.$$

Et tous les ensembles maximaux I sont de l'un de ces deux types.

f) Si V_3 est de dimension 3, on peut trouver $V_4 \supseteq V_3$ de dimension 4 et non isotrope. Alors si w est une involution extrémale avec $V_4 \subseteq E_{2m-2}(w)$, tout élément v de $I_3(V_3)$ vérifie $E_2(v) \subseteq E_{2m-2}(w)$ et $E_2(w) \subseteq V_4^\perp \subseteq E_{2m-2}(v)$. De ce fait, w commute avec tout élément de $I_3(V_3)$. Or il n'existe pas d'élément non trivial de $\mathrm{Sp}_{2m}(K)$ commutant avec tout élément de $I_1(V_1)$. On en déduit que tout automorphisme de $\mathrm{Sp}_{2m}(K)$ préserve $\{I_1(x) \mid x \in \mathbb{P}^{2m-1}(K)\}$.
Soit ϕ un automorphisme de $\mathrm{Sp}_{2m}(K)$. On lui associe la bijection $\theta_\phi : \mathbb{P}^{2m-1}(K) \to \mathbb{P}^{2m-1}(K)$

via $\phi(I_1(x)) = I_1(\theta_\phi x)$. Maintenant, $x, y \in \mathbb{P}^{2m-1}(K)$ sont deux droites orthogonales si et seulement si elles engendrent un plan anisotrope ; ceci est encore équivalent à $I(x) \cap I(y) = \emptyset$. Cette dernière propriété est conservée par ϕ, de sorte que θ_ϕ préserve l'orthogonalité. On en déduit que θ_ϕ préserve l'alignement, et par le théorème fondamental de la géométrie projective, il existe $a \in \Gamma\mathrm{L}_{2m}(K)$ tel que l'on ait $\theta_\phi(Kx) = K(ax)$ pour tout $x \in K^{2m} \smallsetminus \{0\}$. Comme a préserve l'orthogonalité, on a même $a \in \Gamma\mathrm{Sp}_{2m}(K)$. Si s est une involution extrémale, on a $\{s\} = I_1(e_1) \cap I_1(e_2)$ si e_1 et e_2 sont deux droites engendrant $E_2(s)$. On en déduit que $\phi(s) = asa^{-1}$. Si g est un élément de $\mathrm{Sp}_{2m}(K)$, gsg^{-1} est une involution extrémale et on a

$$agsg^{-1}a^{-1} = \phi(gsg^{-1}) = \phi(g)\phi(s)\phi(g)^{-1} = \phi(g)asa^{-1}\phi(g)^{-1}.$$

Ceci s'écrit encore $g^{-1}a^{-1}\phi(g)as = sg^{-1}a^{-1}\phi(g)a$; autrement dit, $g^{-1}a^{-1}\phi(g)a$ commute à toute involution extrémale et préserve donc tout plan hyperbolique. Il s'ensuit que $g^{-1}a^{-1}\phi(g)a$ préserve les droites et est donc une homothétie, disons $\lambda(g)I_{2m}$. Mais alors, $g \mapsto \lambda(g)$ fournit un morphisme $\mathrm{Sp}_{2m}(K) \to K^\times$. Par simplicité de $\mathrm{PSp}_{2m}(K)$, le noyau de ce dernier est $\{1\}$, $Z(\mathrm{Sp}_{2m}(K))$ ou $\mathrm{Sp}_{2m}(K)$. Les deux premiers cas ne permettent pas de factoriser λ par l'abélianisé ; c'est donc le dernier cas qui se présente, et λ est trivial.

TD9 : Formes sesquilinéaires, groupe unitaire, quaternions

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Montrer que toute forme sesquilinéaire réelle est bilinéaire.

Solution de l'exercice 1. Il est classique que l'identité est l'unique automorphisme de corps de $\mathbb{R}$. Par conséquent, l'identité est la seule involution de corps de $\mathbb{R}$, ce qui assure le résultat.

Exercice 2 : ⋆
Soient K un corps de caractéristique différente de 2 et $\sigma \in \mathrm{Aut}(K)$ une involution distincte de id_K. Montrer que $k = K^\sigma := \{x \in K : \sigma(x) = x\}$ est un sous-corps de K, qu'il existe $a \in K \setminus k$ tel que $a^2 \in k$, $\sigma(a) = -a$ et $K = k(a) := \{\lambda a + \mu : (\lambda, \mu) \in k^2\}$.
Que dire si K est de caractéristique 2 ?

Solution de l'exercice 2.
- On vérifie facilement que $k := K^\sigma$ contient 0 et 1, qu'il est stable par somme et produit, ainsi que par opposé et par inverse. Cela assure que k est un sous-corps de K.
- On suppose que la caractéristique de K n'est pas 2. Par hypothèse, il existe $b \in K \setminus k$. Posons $a := b - \sigma(b)$. On voit que a vérifie que $\sigma(a) = -a$ et donc $a \notin k$ (puisque $a \neq 0$ et K n'est pas de caractéristique 2). On a donc $a^2 = -a\sigma(a) \in K$. En outre, il est clair que $k(a) \subset K$. Réciproquement, soit $x \in K$. Posons $\lambda := \frac{x+\sigma(x)}{2}$ et $y := \frac{x-\sigma(x)}{2}$. Alors $x = \lambda + y$ et en outre, $\lambda \in k$ et $\sigma(y) = -y$. Donc $\frac{y}{a}$ est fixe par σ, donc $\frac{y}{a} \in k$, i.e. il existe $\mu \in k$ tel que $y = \mu a$. Finalement, on a $x = \lambda + \mu a$, avec $\lambda, \mu \in k$. Cela assure que $K = k(a)$.
- On suppose maintenant que K est de caractéristique 2. On sait qu'il existe $b \in K \setminus k$. Posons $a := \frac{b}{b+\sigma(b)}$. On voit que $\sigma(a) = a + 1$, donc $a \notin k$. En outre, $\alpha := a\sigma(a)$ est un élément de k, et on a la relation suivante : $a^2 + a + \alpha = 0$ (on note en revanche que $a^2 \notin k$). On a bien $k(a) \subset K$. Réciproquement, soit $x \in K \setminus k$. Posons $y := \frac{x}{x+\sigma(x)}$. Alors $\sigma(y) = y + 1$, donc $\sigma(a + y) = a + y$, donc $a + y \in k$. Donc $y \in k(a)$, donc $x = (x + \sigma(x))y \in k(a)$ car $x + \sigma(x) \in k$. Donc $K = k(a)$.

Exercice 3 : ⋆⋆
Soient K un sous-corps de $\mathbb{R}$ et $K' = K(i) := \{x + iy : (x, y) \in K^2\}$. On munit K' de l'involution induite par la conjugaison complexe. Soient E' un K'-espace vectoriel et E le K-espace vectoriel sous-jacent. Une forme K-bilinéaire f sur $E \times E$ est dite *invariante par* i si l'on a $f(ix, iy) = f(x, y)$ pour tous $x, y \in E$.

a) Montrer que l'application $\phi \mapsto \big((x, y) \mapsto \phi(x, y) + i\phi(x, iy)\big)$ est un isomorphisme de l'espace des formes bilinéaires sur $E \times E$ invariantes par i vers celui des formes sesquilinéaires sur $E' \times E'$.

b) Montrer qu'elle induit un isomorphisme de l'espace des formes symétriques sur $E \times E$ invariantes par i vers l'espace des formes hermitiennes sur $E' \times E'$.

c) Montrer que si ϕ est symétrique invariante par i, alors $(x, y) \mapsto \phi(x, iy)$ est antisymétrique.

Solution de l'exercice 3.

a) Notons ψ_ϕ l'image de ϕ. Pour tous $x, y \in E$ et $\lambda, \mu \in k$, on vérifie que

$$\psi_\phi((\lambda + i\mu)x, y) = \lambda\phi(x, y) + i\lambda\phi(x, iy) - \mu\phi(x, iy) + i\mu\phi(x, y) = (\lambda + i\mu)\psi_\phi(x, y)$$

et

$$\psi_\phi(x,(\lambda+i\mu)y) = \lambda\phi(x,y) + i\lambda\phi(x,iy) + \mu\phi(x,iy) - i\mu\phi(x,y) = (\lambda - i\mu)\psi_\phi(x,y)\,.$$

Donc ψ_ϕ est bien une forme sesquilinéaire sur $E' \times E'$.
Et il est clair que l'application $\phi \mapsto \psi_\phi$ est k-linéaire.
Réciproquement, tout forme sesquilinéaire ψ sur $E' \times E'$ s'écrit $\psi = \phi_1 + i\phi_2$ où ϕ_1 et ϕ_2 sont des formes k-bilinéaires sur $E \times E$. On a, pour tous $x, y \in E \times E$, les égalités

$$\phi_1(ix,iy) + i\phi_2(ix,iy) = \psi(ix,iy) = \psi(x,y) = \phi_1(x,y) + i\phi_2(x,y)\,.$$

Autrement dit, ϕ_1 et ϕ_2 sont invariantes par i. Aussi, on a l'égalité

$$\phi_1(x,iy) + i\phi_2(x,iy) = \psi(x,iy) = -i\psi(x,y) = \phi_2(x,y) - i\phi_1(x,y)\,,$$

de sorte que l'on a $\phi_2(x,y) = \phi_1(x,iy)$.
Cela assure que l'application $\psi \mapsto \phi_\psi := \phi_1$ est la réciproque de l'application précédente, i.e. que pour toute forme sesquilinéaire ψ, on a $\psi_{\phi_\psi} = \psi$, et pour toute forme bilinéaire ϕ, on a $\phi_{\psi_\phi} = \phi$.
D'où l'isomorphisme souhaité.

b) On a $\psi_\phi(y,x) = \phi(y,x) - i\phi(iy,x)$, ce qui assure le résultat souhaité.

c) Si ϕ est symétrique invariante par i, on a $\phi(x,iy) + \phi(y,ix) = \phi(x,iy) + \phi(iy,-x) = 0$.

Exercice 4 :
Soient K un corps, E un espace vectoriel sur K, ϕ une forme sesquilinéaire sur $E \times E$ et u un endomorphisme de E.
Si $v : E \to F$ est une application linéaire entre deux espaces vectoriels, on définit sa *transposée* comme étant l'application $\begin{array}{rccc} {}^tv : & F^* & \to & E^* \\ & f & \mapsto & f \circ v \end{array}$.

a) Montrer que les deux conditions suivantes sont équivalentes :
   i) il existe un unique endomorphisme u^* de E vérifiant $\phi(u(x),y) = \phi(x,u^*(y))$ pour tous $x, y \in E$;
   ii) l'application $d_\phi : E \to E^*$ induite par ϕ est injective et ${}^tu(d_\phi(E)) \subseteq d_\phi(E)$.

b) Donner un exemple où E est de dimension infinie, d_ϕ est injective, mais où ${}^tu(d_\phi(E))$ n'est pas contenu dans $d_\phi(E)$.

Solution de l'exercice 4.

a) Supposons (i). Alors u^* stabilise $\ker d_\phi$. Soit S un supplémentaire de $\ker d_\phi$ dans E ; si $u_0^* : E \to E$ désigne l'identité de $\ker d_\phi$ prolongée par 0 sur S, $u^* + u_0^*$ est un endomorphisme satisfaisant aussi l'égalité voulue. Par unicité, on a donc $u_0^* = 0$ et $\ker d_\phi = 0$. Aussi, on a ${}^tu(d_\phi(y)) = d_\phi(y) \circ u = d_\phi(u^*(y))$ pour tout $y \in E$.
   Réciproquement, supposons (ii). L'inclusion ${}^tu(d_\phi(E)) \subseteq d_\phi(E)$ nous permet de définir une application ensembliste $u^* : E \to E$ vérifiant $\phi(u(x),y) = \phi(x,u^*(y))$ pour tous $x, y \in E$. L'injectivité de d_ϕ nous assure l'unicité d'un tel u^*, et sa linéarité en découle.

b) Soient k un corps et E un espace vectoriel sur k possédant une base dénombrable $(e_n)_{n\geq 1}$ (par exemple $E = k[X] = k^{(\mathbb{N})}$). On définit une forme bilinéaire ϕ sur $E \times E$ en posant $\phi(e_i,e_j) = \delta_{i,j+1}$ pour tous $i, j \geq 1$. Soit u l'application linéaire définie par $e_i \mapsto \delta_{1,i}e_2$. Alors d_ϕ est injective et on a ${}^tu(e_2^*) = e_1^* \notin d_\phi(E)$ alors que $e_2^* = d_\phi(e_1) \in d_\phi(E)$.

Exercice 5 :
Soient K un corps, E_0 et E_1 deux espaces vectoriels sur K et ϕ_0, ϕ_1 des formes sesquilinéaires respectivement sur $E_0 \times E_0$ et $E_1 \times E_1$. On suppose que ϕ_1 est non dégénérée et qu'il existe un élément $\alpha \in K$ et une bijection $v : E_0 \to E_1$ tels que l'on ait $\phi_1(v(x),v(y)) = \phi_0(x,y)\alpha$ pour tous $x, y \in E_0$.

a) Montrer que ϕ_0 est non dégénérée et que v est linéaire.

Soient E_2 un espace vectoriel sur K et ϕ_2 une forme sesquilinéaire non dégénérée sur $E_2 \times E_2$. On suppose l'existence d'une application linéaire surjective $u : E_1 \to E_2$ qui vérifie

$$\phi_2(u(x), u(y)) = 0 \Rightarrow \phi_1(x, y) = 0 \quad \text{pour tous } x, y \in E_1.$$

b) Montrer que u est un isomorphisme de E_1 sur E_2.

c) Montrer que pour tout $y \in E_1$, il existe un élément $m(y) \in K$ tel que l'on ait $\phi_2(u(x), u(y)) = \phi_1(x, y)m(y)$ pour tout $x \in E_1$.

d) En déduire qu'il existe $\beta \in K^*$ tel que l'on ait $\phi_2(u(x), u(y)) = \phi_1(x, y)\beta$ pour tous $x, y \in E_1$.

Solution de l'exercice 5.

a) Comme ϕ_1 est non dégénérée, on voit que $v(0) = 0$. Soit $x \in E_0$ tel que $\phi_0(., x) = 0$. Alors $\phi_1(., v(x)) = 0$, donc $v(x) = 0 = v(0)$. Or v est injective, donc $x = 0$, donc ϕ_0 est non dégénérée. Un raisonnement analogue utilisant la non-dégénérescence de ϕ_1 assure la linéarité de v.

b) Soit b un élément du noyau de u. La condition implique alors $\phi_1(., b) = 0$, et comme ϕ_1 est non dégénérée, on a $b = 0$. Donc u est injective, donc un isomorphisme.

c) D'après a) et les hypothèses de non dégénérescence, pour tout $y \in E_1$, $d_{\phi_1}(y)$ et $d_{\phi_2}(u(y))$ sont deux éléments non nuls de E_1^* possédant le même hyperplan. Alors, il existe $m(y) \in k^*$ vérifiant $\phi_2(u(x), u(y)) = \phi_1(x, y)m(y)$ pour tout $x \in E_1$.

d) On voit tout d'abord que $m : E_1 \to k^*$ est constante sur les droites. Maintenant, si y et y' sont deux éléments non colinéaires de E_1 (qui est alors de dimension supérieure à 2), on a

$$\phi_1(x, y + y')m(y + y') = \phi_1(x, y)m(y) + \phi_1(x, y')m(y').$$

En prenant successivement x dans $\ker d_{\phi_1}(y) \setminus \ker d_{\phi_1}(y')$ et $\ker d_{\phi_1}(y) \setminus \ker d_{\phi_1}(y')$ (c'est possible parce que ϕ_1 est non dégénérée), on obtient $m(y) = m(y')$ et le résultat voulu.

Exercice 6 :
Déterminer les groupes unitaires, orthogonaux et symplectiques en dimension 1 et 2.

Solution de l'exercice 6. Voir cours.

Exercice 7 : $\star\star$
Soient p un nombre premier impair et $q = p^r$ une puissance d'un tel nombre premier, avec $r \geq 1$.

a) Montrer qu'il existe une involution non triviale sur $\mathbb{F}_q$ si et seulement si r est pair.

b) Vérifier que $\sigma : x \mapsto x^q$ est l'unique involution non triviale de $\mathbb{F}_{q^2}$ et que son corps des invariants est $\mathbb{F}_q$.

c) On note $E_n := \mathbb{F}_{q^2}^n$. Montrer qu'il y a sur (E_n, σ) une unique classe d'équivalence de formes hermitiennes non dégénérées. Montrer qu'une telle forme admet dans une base convenable la matrice identité.

d) Soit z_n (resp. y_n) le nombre de vecteurs non triviaux de E_n de norme 0 (resp. 1). Par récurrence, montrer que l'on a pour tout entier $n \geq 1$,

$$z_n = (q^n - (-1)^n)(q^{n-1} + (-1)^n) \quad \text{et} \quad y_n = q^{n-1}(q^n - (-1)^n).$$

e) Calculer l'ordre de $\mathrm{U}_n(\mathbb{F}_{q^2})$.

f) En déduire l'ordre de $\mathrm{SU}_n(\mathbb{F}_{q^2})$ et de $\mathrm{PSU}_n(\mathbb{F}_{q^2})$.

Solution de l'exercice 7.

a) L'exercice 2 assure que si $\mathbb{F}_q$ admet une involution non triviale σ, alors $\mathbb{F}_q$ est un $\mathbb{F}_q^\sigma$-espace vectoriel de dimension 2, ce qui assure que $|\mathbb{F}_q|$ est un carré, donc $q = p^r$ est un carré, donc r est pair.

Réciproquement, si $r = 2s$ est pair, alors l'application $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ définie par $x \mapsto x^{p^s}$ est une involution non triviale de $\mathbb{F}_q$ (c'est un morphisme de corps car c'est une puissance de l'automorphisme de Frobenius, c'est une involution par le théorème de Lagrange, et ce n'est pas l'identité car les points fixes de σ sont les racines de $X^{p^s} - X$ dans $\mathbb{F}_q$, qui sont au plus $p^s < q = |\mathbb{F}_q|$).

b) On a vu à la question a) que σ était une involution non triviale, et que son corps des invariants était un corps de cardinal q. Il reste à montrer l'unicité de σ. Soit τ une involution non triviale de $\mathbb{F}_{q^2}$. Alors $\mathbb{F}_{q^2}^\sigma$ et $\mathbb{F}_{q^2}^\tau$ sont deux sous-corps de $\mathbb{F}_{q^2}$ de cardinal q. Donc $\left(\mathbb{F}_{q^2}^\sigma\right)^*$ et $\left(\mathbb{F}_{q^2}^\tau\right)^*$ sont deux sous-groupes de même cardinal du groupe cyclique $\mathbb{F}_{q^2}^*$, donc ils sont égaux, donc $\mathbb{F}_{q^2}^\sigma = \mathbb{F}_{q^2}^\tau \subset \mathbb{F}_{q^2}$. On notera $k := \mathbb{F}_{q^2}^\sigma$. L'exercice 2 assure qu'il existe $a \in \mathbb{F}_{q^2}^*$ tel que $\sigma(a) = -a$, $\mathbb{F}_{q^2} = k(a)$ et $a^2 \in k$. Alors $\tau(a)^2 = \tau(a^2) = a^2$, donc $\tau(a) = \pm a$. Si $\tau(a) = a$, alors $\tau = \mathrm{id}$, ce qui est exclu. Donc $\tau(a) = -a = \sigma(a)$. Cela suffit pour conclure que $\tau = \sigma$. D'où l'unicité recherchée.

c) L'application $N : \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ définie par $x \mapsto x\sigma(x) = x^{q+1}$ est un morphisme de groupes surjectif, dont le noyau est de cardinal $q+1$. Soit f une forme hermitienne non dégénérée sur (E_n, σ). Alors il existe une base orthogonale $(e_1, \dots, e_n)$ de E_n pour f. Puisque f est non dégénérée, pour tout i, $f(e_i) \in \mathbb{F}_q^*$. Donc pour tout i, il existe $\lambda_i \in \mathbb{F}_{q^2}^*$ tel que $f(e_i) = N(\lambda_i)$. Alors $f\left(\frac{e_i}{\lambda_i}\right) = 1$ pour tout i, ce qui assure que la matrice de f dans la base $\left(\frac{e_i}{\lambda_i}\right)$ est bien l'identité.

d) La surjectivité du morphisme $N : \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ défini plus haut assure que pour tout $\alpha \in \mathbb{F}_q^*$, l'ensemble des vecteurs $x \in E_n$ de norme α est de cardinal exactement y_n. Or E_n est la réunion disjointe des sous-ensembles formés des vecteurs de norme α, pour α décrivant $\mathbb{F}_q$, donc $|E_n| = 1 + z_n + (q-1)y_n$. On a donc $q^{2n} = 1 + z_n + (q-1)y_n$.

En écrivant l'ensemble des vecteurs $\neq 0$ de E_{n+1} de norme nulle comme réunion disjointe de l'ensemble des vecteurs $\neq 0$ dont la dernière coordonée est nulle et de celui des vecteurs de norme nulle dont la dernière coordonnée n'est pas nulle, on obtient que $z_{n+1} = z_n + (q^2-1)y_n$. On en déduit grâce à la relation précédente que $z_{n+1} = (q^{2n}-1)(q+1) - qz_n$. Comme z_1 vaut 0, on prouve la formule voulue par récurrence sur n.

e) La question c) assure que les éléments de $\mathrm{U}_n(\mathbb{F}_{q^2})$ sont en bijection avec les bases orthonormales de $\mathbb{F}_{q^2}^n$. On en déduit donc que

$$|\mathrm{U}_n(\mathbb{F}_{q^2})| = \prod_{i=1}^n y_i = \prod_{i=1}^n q^{i-1}(q^i - (-1)^i) = q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q^i - (-1)^i)\,.$$

f) La condition ${}^t u^{(q)} u = 1$, où $u^{(q)}$ désigne la matrice de coefficients les puissances q-ième des coefficients de la matrice $u \in \mathrm{U}_n(\mathbb{F}_{q^2})$, assure que $\det\left(\mathrm{U}_n(\mathbb{F}_{q^2})\right) = \{x^{q+1} \mid x \in \mathbb{F}_{q^2}^*\}$. Comme ce dernier ensemble est de cardinal $q-1$, on a

$$|\mathrm{SU}_n(\mathbb{F}_{q^2}/\mathbb{F}_q)| = \frac{|\mathrm{U}_n(\mathbb{F}_{q^2})|}{q-1} = q^{\frac{n(n-1)}{2}} \prod_{i=2}^n (q^i - (-1)^i)\,,$$

et comme le centre de $\mathrm{SU}_n(\mathbb{F}_{q^2})$ est réduit aux homothéties unitaires, on a $Z(\mathrm{SU}_n(\mathbb{F}_{q^2})) = \{\lambda I_n : \lambda^{q+1} = 1 \text{ et } \lambda^n = 1\}$, donc

$$|\mathrm{PSU}_n(\mathbb{F}_{q^2}/\mathbb{F}_q)| = \frac{|\mathrm{SU}_n(\mathbb{F}_{q^2})|}{n \wedge (q+1)} = \frac{q^{\frac{n(n-1)}{2}}}{n \wedge (q+1)} \prod_{i=2}^n (q^i - (-1)^i)\,.$$

Exercice 8 : ⋆⋆⋆

Soient p un nombre premier impair, $f \geq 1$ et $q = p^f$. Soit b la forme sur $(\mathbb{F}_{q^2})^3 \times (\mathbb{F}_{q^2})^3$ définie par $b(u, v) = u_1 v_3^q + u_2 v_2^q + u_3 v_1^q$

a) Déterminer l'ensemble Δ des droites isotropes de b. Quel est le cardinal de Δ ?

b) Notons (e_1, e_2, e_3) la base canonique de $(\mathbb{F}_{q^2})^3$. On définit aussi les éléments $t_{\alpha,\beta}$ et $h_{\gamma,\delta}$ de $\mathrm{PU}_3(\mathbb{F}_{q^2})$ correspondant respectivement aux matrices

$$\begin{pmatrix} 1 & -\beta^q & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \gamma & 0 & 0 \\ 0 & \delta & 0 \\ 0 & 0 & \gamma^{-q} \end{pmatrix}$$

avec les conditions $\delta^{1+q} = 1$, $\gamma \neq 0$, $\alpha + \alpha^q + \beta^{1+q} = 0$. Déterminer le stabilisateur de e_1 dans $\mathrm{PU}_3(\mathbb{F}_{q^2})$ et montrer que $T := \{t_{\alpha,\beta} \mid \alpha + \alpha^q + \beta^{1+q} = 0\}$ en est un sous-groupe distingué.

c) Montrer que l'action de $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ sur Δ est 2-transitive.

d) Calculer le sous-groupe dérivé T_{e_1} de T.

e) On appelle transvection unitaire de $(\mathbb{F}_{q^2})^3$ toute transvection de $(\mathbb{F}_{q^2})^3$ préservant la forme b. Montrer que $u \in \mathrm{U}_3(\mathbb{F}_{q^2})$ est une transvection unitaire si et seulement si il existe $\alpha \in \mathbb{F}_{q^2}$ vérifiant $\alpha + \alpha^q = 0$ et $a \in (\mathbb{F}_{q^2})^3$ isotrope tels que pour tout $x \in (\mathbb{F}_{q^2})^3$, on ait $u(x) = x + \alpha b(a, x)a$ (on dit que u est une transvection unitaire de vecteur a).

f) Pour tout vecteur isotrope a, montrer que l'ensemble T_a des transvections unitaires de vecteur a forme un sous-groupe abélien distingué dans le stabilisateur de a sous $\mathrm{SU}_3(\mathbb{F}_{q^2})$.

g) Montrer que toute transvection unitaire est un commutateur dans $\mathrm{SU}_3(\mathbb{F}_{q^2})$.

h) Montrer que le sous-groupe de $\mathrm{SU}_3(\mathbb{F}_{q^2})$ engendré par les transvections unitaires agit transitivement sur $\{x \in (\mathbb{F}_{q^2})^3 : b(x, x) = 1\}$.

i) Montrer que $\mathrm{SU}_3(\mathbb{F}_{q^2})$ est engendré par les transvections unitaires.

j) Montrer que $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ est un groupe simple.

Solution de l'exercice 8.

a) Un petit calcul montre que les droites isotropes sont $ke_1 = k(1, 0, 0)$ et les $k(\alpha, \beta, 1)$ avec $\alpha + \alpha^q + \beta^{1+q} = 0$. Le nombre de solutions de cette équation est $q^2 \cdot q = q^3$ (car l'application $\mathbb{F}_{q^2} \to \mathbb{F}_q$ définie par $x \mapsto x^{1+q}$ est surjective et l'application $\begin{array}{ccc} \mathbb{F}_{q^2} & \to & \mathbb{F}_q \\ x & \mapsto & x + x^q \end{array}$ est $\mathbb{F}_q$-linéaire).
Le cardinal de Δ est donc $q^3 + 1$.

b) On vérifie d'abord que les $t_{\alpha,\beta}$ et $h_{\gamma,\delta}$ stabilisent bien ke_1. Notons respectivement T et H les sous-groupes de $\mathrm{PU}_3(\mathbb{F}_{q^2})$ engendrés par les $t_{\alpha,\beta}$ et les $h_{\gamma,\delta}$: ils forment un produit semi-direct $T \rtimes H$ (la vérification est laissée au lecteur).
L'image réciproque de $T \rtimes H$ dans $\mathrm{U}_3(\mathbb{F}_{q^2})$ est de cardinal $q^3 \cdot (q^2 - 1)(q + 1)$. De plus, l'action de $\mathrm{U}_3(\mathbb{F}_{q^2})$ sur Δ étant transitive, on a

$$|\mathrm{Stab}_{\mathrm{U}_3}(ke_1)| = |\mathrm{U}_3(\mathbb{F}_{q^2})| \cdot |\Delta|^{-1} = q^3(q^2 - 1)(q + 1)\,.$$

Ceci montre que le stabilisateur de ke_1 dans $\mathrm{PU}_3(\mathbb{F}_{q^2})$ est exactement le groupe $T \rtimes H$.

c) Un petit calcul montre que l'action de $T \subset \mathrm{PSU}_3(\mathbb{F}_{q^2})$ est transitive sur $\Delta \setminus \{ke_1\}$. Or $\mathrm{SU}_3(\mathbb{F}_{q^2})$ agit transitivement sur Δ, donc on en déduit facilement que $\mathrm{PSU}_3(\mathbb{F}_q^2)$ agit 2 fois transitivement sur Δ.

d) On calcule que $t_{\alpha,\beta} \cdot t_{\alpha',\beta'} = t_{\alpha+\alpha'-\beta^q\beta',\beta+\beta'}$. Donc $[t_{\alpha,\beta}, t_{\alpha',\beta'}] = t_{\beta\beta'^q-\beta'\beta^q,0}$. On en déduit que $T_{e_1} := D(T)$ est le groupe formé des matrices

$$\begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

avec $\alpha \in \mathbb{F}_{q^2}$ tel que $\alpha^q = -\alpha$. C'est le groupe des transvections unitaires de T.

e) Soit $u \in \mathrm{U}_3(\mathbb{F}_{q^2})$ une transvection de vecteur $a \in (\mathbb{F}_{q^2})^3$. Alors il existe une forme linéaire f non nulle telle que pour tout $x \in (\mathbb{F}_{q^2})^3$, $u(x) = x + f(x)a$, avec $f(a) = 0$. Puisque u est unitaire, on a, pour tous $x, y \in (\mathbb{F}_{q^2})^3$, $b(u(x), u(y)) = b(x, y)$, i.e.

$$\overline{b(a,x)}f(y) + b(a,y)\overline{f(x)} + b(a,a)f(y)\overline{f(x)} = 0\,.$$

Donc en prenant $y = a$ et x quelconque, on voit que $b(a, a) = 0$ (car $f \neq 0$). Et en choisissant x tel que $b(a, x) = 1$, en posant $\alpha := -\overline{f(x)}$, on obtient que pour tout y, $f(y) = \alpha b(a, y)$. En outre, pour y tel que $b(a, y) = 1$, on constate que $\alpha + \overline{\alpha} = 0$.
Par conséquent, pour toute transvection unitaire u de $(\mathbb{F}_{q^2})^3$, il existe un vecteur isotrope a et $\alpha \in \mathbb{F}_{q^2}$ tel que $\alpha + \overline{\alpha} = 0$ de sorte que pour tout $x \in (\mathbb{F}_{q^2})^3$,

$$u(x) = x + \alpha b(a, x)a\,.$$

Réciproquement, il est clair qu'une telle donnée définit une transvection unitaire.

f) On peut toujours compléter le vecteur isotrope a en un plan hyperbolique de base hyperbolique (a, c). Ensuite, on complète la famille (a, c) en une base (a, b, c) de $(\mathbb{F}_{q^2})^3$ avec un vecteur b orthogonal à a et c et de norme 1. On est alors ramené via ce changement de bases aux calculs des questions a),b),c),d). D'où le résultat souhaité.

g) Cela résulte des questions e), f), et des calculs de commutateurs de la question d).

h) Soient x et y deux vecteurs tels que $b(x, x) = b(y, y) = 1$. Si la restriction de b au sous-espace engendré par x et y est non dégénérée, alors un calcul dans $\mathrm{SU}_2(\mathbb{F}_{q^2}) \cong \mathrm{SL}_2(\mathbb{F}_q)$ assure le résultat. Si b restreinte à $\mathrm{vect}(x, y)$ est dégénérée, on peut trouver z tel que les plans $\mathrm{vect}(x, z)$ et $\mathrm{vect}(y, z)$ soient non dégénérés (prendre par exemple un vecteur isotrope $z \notin \mathrm{vect}(x, y)$, non orthogonal à x, ni à y). Alors on conclut par le cas précédent en composant deux transvections unitaires.

i) Pour tout x tel que $b(x, x) = 1$, le stabilisateur de x dans $\mathrm{SU}_3(\mathbb{F}_{q^2})$ est isomorphe à $\mathrm{SU}(x^\perp, b) \cong \mathrm{SU}_2(\mathbb{F}_{q^2})$. Or $\mathrm{SU}_2(\mathbb{F}_{q^2})$ est engendré par les transvections unitaires, donc la question h) assure que $\mathrm{SU}_3(\mathbb{F}_{q^2})$ est engendré par les transvections unitaires.

j) La question c) assure que le groupe $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ agit primitivement sur Δ. Pour tout $d \in \Delta$, on pose T_d l'image de T_a dans $\mathrm{PSU}_3(\mathbb{F}_{q^2})$, où a est un vecteur directeur de d. La question f) assure que pour tout $d \in \Delta$, T_d est un sous-groupe abélien de $\mathrm{PSU}_3(\mathbb{F}_{q^2})$, distingué dans le stabilisateur de d. Et la question i) assure que $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ est engendré par la réunion des T_d, $d \in \Delta$. Par conséquent, le théorème d'Iwasawa assure que tout sous-groupe distingué de $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ agissant non trivialement sur Δ contient $D(\mathrm{PSU}_3(\mathbb{F}_{q^2}))$. Or les questions g) et i) assurent que $D(\mathrm{PSU}_3(\mathbb{F}_{q^2})) = \mathrm{PSU}_3(\mathbb{F}_{q^2})$, donc cela démontre que le groupe $\mathrm{PSU}_3(\mathbb{F}_{q^2})$ est un groupe simple.

Exercice 9 : $\star\star$

Soit $\mathbf{H}$ la $\mathbb{R}$-algèbre des quaternions. Un élément $z \in \mathbf{H}$ est dit *pur* s'il s'écrit sous la forme $z = bi + cj + dk$ avec $a, b, c \in \mathbb{R}$.

a) Montrer que $z \in \mathbf{H}$ est pur si et seulement si $z^2 \in \mathbb{R}^-$.

b) Montrer que tout élément de $\mathbf{H}$ est produit de deux quaternions purs.

c) Montrer que tout automorphisme d'anneaux de $\mathbf{H}$ est de la forme $x \mapsto qxq^{-1}$ pour un certain $q \in \mathbf{H}$ de norme 1.

d) Vérifier que la transposée sur $\mathrm{Mat}_2(\mathbf{H})$ ne conserve pas le groupe $\mathrm{GL}_2(\mathbf{H})$.

Solution de l'exercice 9.

a) C'est un calcul immédiat.

b) Soient $z, z' \in \mathbf{H}$ deux quaternions purs, identifiés à deux vecteurs $Z, Z' \in \mathbb{R}^3$. Un calcul direct assure que $zz' \in \mathbf{H}$ est le quaternion dont la coordonnée réelle est l'opposé du produit scalaire $-Z \cdot Z'$ et les trois autres coordonnées sont les coordonnées du produit vectoriel $Z \wedge Z'$ dans $\mathbb{R}^3$. Soit alors $z_0 = \alpha + Y \in \mathbf{H}$, avec $\alpha \in \mathbb{R}$ et Y pur. L'équation vectorielle dans $\mathbb{R}^3$ donnée par $Z \wedge Z' = Y$ admet clairement une solution $Z, Z' \in \mathbb{R}^3$, avec $Z \neq 0$. Alors pour tout $\lambda \in \mathbb{R}$, $Y = Z \wedge (Z' + \lambda Z)$, et $Z \cdot (Z' + \lambda Z) = Z \cdot Z' + \lambda \|X\|^2$. Il est alors clair qu'il existe $\lambda \in \mathbb{R}$ tel que $Z \wedge (Z' + \lambda Z) = Y$ et $Z \cdot (Z' + \lambda Z) = -\alpha$, donc $z_0 = zz'$, avec $z, z' \in \mathbf{H}$ purs.

c) Soit $\varphi : \mathbf{H} \to \mathbf{H}$ un morphisme d'anneaux. Alors $\varphi(Z(\mathbf{H})) = Z(\mathbf{H})$, où $Z(\mathbf{H}) = \{x \in \mathbf{H} : \forall y \in \mathbf{H},\ xy = yx\}$. Donc $\varphi(\mathbb{R}) = \mathbb{R}$. Donc la restriction de φ à $\mathbb{R}$ est un automorphisme d'anneau de $\mathbb{R}$, donc $\varphi_{|\mathbb{R}} = \mathrm{id}_{\mathbb{R}}$.
La question a) assure qu'un quaternion z est pur si et seulement si $z^2 \in \mathbb{R}^-$, donc pour tout $z \in \mathbf{H}$, z est pur si et seulement si $z^2 \in \mathbb{R}^-$ si et seulement si $\varphi(z^2) = \varphi(z)^2 \in \mathbb{R}^-$ si et seulement si $\varphi(z)$ est pur. Donc si on note $\mathbf{P} \subset \mathbf{H}$ le sous-espace vectoriel des quaternions purs, la restriction de φ à $\mathbf{P}$ induit un isomorphisme de groupes $\varphi_{|\mathbf{P}} : \mathbf{P} \to \mathbf{P}$. Or pour tout $z \in \mathbf{P}$, on a $N(z) = -z^2$ et $N(\varphi(z)) = -z^2$, donc $\varphi_{|\mathbf{P}} \in \mathrm{O}(\mathbf{P}, N) \cong \mathrm{O}_3(\mathbb{R})$. Or (i, j, k) est une base orthonormée de $(\mathbf{P}, N)$, donc $(\varphi(i), \varphi(j), \varphi(k))$ également, donc il existe une rotation $r \in \mathrm{SO}_3(\mathbb{R})$ telle que $r(i) = \varphi(i)$, $r(j) = \varphi(j)$ et $r(k) = \pm\varphi(k)$. Or on dispose de l'isomorphisme $\psi : \{x \in \mathbf{H} : N(x) = 1\}/\{\pm 1\} \xrightarrow{\sim} \mathrm{SO}(\mathbb{P}, N) \cong \mathrm{SO}_3(\mathbb{R})$ défini par $\psi(x) : z \mapsto xzx^{-1}$, ce qui assure que la rotation r est de la forme $\psi(x)$ pour un certain $x \in \mathbf{H}$ de norme 1. Alors on a $xix^{-1} = \varphi(i)$ et $xjx^{-1} = \varphi(j)$, donc $xkx^{-1} = \varphi(i)\varphi(j) = \varphi(k)$. Cela assure que φ est la conjugaison par x sur $\mathbf{H}$.

d) On peut considérer par exemple la matrice $\begin{pmatrix} 1 & j \\ i & k \end{pmatrix}$.

Exercice 10 : $\star\star$
Soit K un corps de caractéristique différente de 2 et soient $\alpha, \beta \in K^*$. On note $(1, i, j, k)$ la base canonique de K^4, et on note $\mathbf{H}_{\alpha,\beta}$ l'unique structure de K-algèbre sur K^4 définie par

$$1 \text{ est le neutre pour la multiplication, } i^2 = \alpha\,,\ j^2 = \beta,\ ij = -ji = k\,.$$

a) Définir la norme réduite $N : \mathbf{H}_{\alpha,\beta} \to K$ et la conjugaison $\mathbf{H}_{\alpha,\beta} \to \mathbf{H}_{\alpha,\beta}$.

b) Montrer que si K est algébriquement clos, alors $\mathbf{H}_{\alpha,\beta}$ est isomorphe à $\mathrm{Mat}_2(K)$.

c) Montrer que $\mathbf{H}_{\alpha,\beta}$ est une algèbre à division (i.e. un "corps non commutatif") si et seulement si N est une forme anisotrope sur le K-espace vectoriel $\mathbf{H}_{\alpha,\beta}$.

d) Montrer que si $K = \mathbb{F}_q$, alors $\mathbf{H}_{\alpha,\beta}$ n'est pas intègre.

e) Soient $\alpha', \beta' \in K^*$. Montrer que les K-algèbres $\mathbf{H}_{\alpha,\beta}$ et $\mathbf{H}_{\alpha',\beta'}$ sont isomorphes si et seulement si les normes N et N' associées sont des formes quadratiques isométriques.

Solution de l'exercice 10.

a) Par analogie avec les quaternions de Hamilton, on définit le conjugué d'un élément $z = a + bi + cj + dk$ par $\overline{z} := a - bi - cj - dk$. De même, on définit la norme d'un élément $z = a + bi + cj + dk$ par $N(z) := z\overline{z} = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2$.

b) Soient $a, b \in K^*$ des racines carrées respectives de α et β (ces racines existent car K est algèbriquement clos). Le morphisme de K-algèbres $\mathbf{H}_{\alpha,\beta} \to \mathrm{Mat}_2(K)$ défini par $i \mapsto \begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$ et $j \mapsto \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix}$ est l'isomorphisme voulu.

c) Il est clair que N est une forme quadratique sur le K-espace vectoriel $\mathbf{H}_{\alpha,\beta}$.
Supposons que $\mathbf{H}_{\alpha,\beta}$ soit une algèbre à division. Soient $z \in \mathbf{H}_{\alpha,\beta} \setminus \{0\}$ et z' un inverse de z. On a alors $N(z)N(z') = N(zz') = N(1) = 1$ et donc $N(z) \neq 0$. Par conséquent, la forme quadratique N est anisotrope.
Réciproquement, si N est anisotrope, alors pour tout élément $z \in \mathbf{H}_{\alpha,\beta} \setminus \{0\}$, l'élément $N(z)^{-1}\overline{z}$ fournit un inverse de z, donc $\mathbf{H}_{\alpha,\beta}$ est une algèbre à division.

d) On sait que sur un corps fini, une forme quadratique de dimension ≥ 3 est isotrope. Par conséquent, la norme N est isotrope sur $\mathbf{H}_{\alpha,\beta}$, donc il existe $z \in \mathbf{H}_{\alpha,\beta} \setminus \{0\}$ tel que $z\overline{z} = N(z) = 0$, donc $\mathbf{H}_{\alpha,\beta}$ n'est pas intègre.

e) Soit $\varphi : \mathbf{H}_{\alpha,\beta} \xrightarrow{\sim} \mathbf{H}_{\alpha',\beta'}$ un isomorphisme de K-algèbres. Comme le centre de ces algèbres est réduit à K, on a nécessairement $\varphi(K) = K$. On note $\mathbf{P}_{\alpha,\beta} \subset \mathbf{H}_{\alpha,\beta}$ le sous-espace vectoriel des quaternions purs. Pour tout $z \in \mathbf{H}_{\alpha,\beta} \setminus \{0\}$, on a $z \in \mathbf{P}_{\alpha,\beta}$ si et seulement si $z \notin K$ et $z^2 \in K$ si et seulement si $\varphi(z) \notin K$ et $\varphi(z)^2 \in K$ si et seulement si $\varphi(z) \in \mathbf{P}_{\alpha',\beta'}$. Donc $\varphi_{|\mathbf{P}_{\alpha,\beta}}$ induit un isomorphisme $\mathbf{P}_{\alpha,\beta} \to \mathbf{P}_{\alpha',\beta'}$. Montrons maintenant que φ préserve la conjugaison : soit $z \in \mathbf{H}_{\alpha,\beta}$. Alors z s'écrit $z = z_0 + p$ avec $z_0 \in K$ et $p \in \mathbf{P}_{\alpha,\beta}$. On a donc $\varphi(\overline{z}) = \varphi(z_0 - p) = \varphi(z_0) - \varphi(p)$ et $\varphi(z) = \varphi(z_0) + \varphi(p)$. Or on a vu que $\varphi(z_0) \in K$ et $\varphi(p) \in \mathbf{P}_{\alpha',\beta'}$, donc les formules précédentes assurent que $\varphi(\overline{z}) = \overline{\varphi(z)}$. On en déduit que pour tout $z \in \mathbf{H}_{\alpha,\beta}$,

$$N'(\varphi(z)) = \varphi(z)\overline{\varphi(z)} = \varphi(z)\varphi(\overline{z}) = \varphi(z\overline{z}) = z\overline{z} = N(z)$$

car $z\overline{z} \in K$ et φ est un morphisme de K-algèbres.

Cela assure que les formes quadratiques N et N' sont isométriques via φ.

Réciproquement, supposons qu'il existe une isométrie (linéaire) $f : (\mathbf{H}_{\alpha,\beta}, N) \to (\mathbf{H}_{\alpha',\beta'}, N')$. Le théorème de Witt (appliqué à l'orthogonal d'un vecteur de norme 1) assure que l'on peut supposer que f envoie $\mathbf{P}_{\alpha,\beta}$ sur $\mathbf{P}_{\alpha',\beta'}$. On a alors $f(i)^2 = -N'(f(i)) = -N(i) = i^2 = \alpha$, et de même $f(j)^2 = \beta$. De plus, comme i et j sont orthogonaux pour N, $f(i)$ et $f(j)$ sont orthogonaux pour N' : ainsi on a $f(i)f(j) + f(j)f(i) = 0$. Cela implique que la sous-K-algèbre de $\mathbf{H}_{\alpha',\beta'}$ engendrée par $f(i)$ et $f(j)$ est isomorphe à $\mathbf{H}_{\alpha,\beta}$, donc par égalité des dimensions, que $\mathbf{H}_{\alpha',\beta'}$ est isomorphe comme K-algèbre à $\mathbf{H}_{\alpha,\beta}$.

Exercice 11 : $\star\star\star$

Soient A un anneau commutatif unitaire et $\mathbf{H}(A)$ la A-algèbre des éléments $a + bi + cj + dk$ avec $a, b, c, d \in A$ telle que 1 est neutre pour la multiplication et avec les relations :

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j.$$

a) Définir la norme réduite $N : \mathbf{H}(A) \to A$ et la conjugaison $\mathbf{H}(A) \to \mathbf{H}(A)$.

b) Montrer que pour tout $x, y \in \mathbf{H}(A)$, $N(xy) = N(x)N(y)$.

c) On définit les *quaternions d'Hurwitz* par

$$\mathrm{H} := \left\{ a + bi + ck + dk \in \mathbf{H}(\mathbb{Q}) \mid (a, b, c, d) \in \mathbb{Z}^4 \cup \left(\frac{1}{2} + \mathbb{Z}^4\right) \right\}.$$

Montrer que H est un sous-anneau de $\mathbf{H}(\mathbb{Q})$ contenant $\mathbf{H}(\mathbb{Z})$ et vérifiant $N(z) = 1$ si et seulement si z est inversible dans H.

d) Montrer que tout idéal à droite (respectivement à gauche) de H est principal.

e) Montrer que, pour tout nombre premier p, il existe $z \in \mathrm{H}$ tel que $N(z) = p$.

f) Montrer que tout entier naturel est somme de quatre carrés.

Solution de l'exercice 11.

a) On pose $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$, qui est bien un élément de A. De même, on définit le conjugué par $\overline{a + bi + cj + dk} = a - bi - cj - dk$.

b) On a $N(z_1 z_2) = z_1 z_2 \overline{z}_2 \overline{z}_1 = N(z_1)N(z_2)$.

c) Il est clair que $(H, +)$ forme un sous-groupe de $(\mathbf{H}(\mathbb{Q}), +)$. Il contient 1, vérifions qu'il est stable par multiplication. Pour cela, posons, $u = \dfrac{1}{2}(1 + i + j + k) \in H$. Il suffit de vérifier que $u.1$, $u.i$, $u.j$, $u.k$ et u^2 sont encore des éléments de H, ce qui est immédiat.

Lorsque z est un élément de $\mathbf{H}(\mathbb{Z})$, $N(z)$ est entier. Soit alors $z \in H \setminus \mathbf{H}(\mathbb{Z})$: un tel z s'écrit $u + a + bi + cj + dk$, avec $a, b, c, d \in \mathbb{Z}$. On a alors $N(z) = a^2 + a + b^2 + b + c^2 + c + d^2 + d + 1 \in \mathbb{Z}$. Donc pour tout $z \in H$, $N(z) \in \mathbb{Z}$.

Soit $z \in H$ de norme 1 : son inverse dans $\mathbf{H}(\mathbb{Q})$ est $\overline{z}$, qui est bien dans H. Réciproquement, si z est inversible dans H, alors il existe $z' \in H$ vérifiant $zz' = 1$. Il en résulte $N(z)N(z') = 1$, et donc $N(z) = 1$ puisque la norme sur H est à valeurs entières positives.

d) Commençons par une remarque. Si $x = a + bi + cj + dk$ est un élément de $\mathbf{H}(\mathbb{Q})$, il existe $a', b', c', d' \in \mathbb{Z}$ tels que $|a - a'| \leq \frac{1}{2}$, $|b - b'| \leq \frac{1}{2}$, $|c - c'| \leq \frac{1}{2}$ et $|d - d'| \leq \frac{1}{2}$. Pour $x' = a' + b'i + c'j + d'k$, on a alors $N(x - x') \leq 1$, avec égalité si et seulement si $x \in H \smallsetminus \mathbf{H}(\mathbb{Z})$.

Prouvons maintenant l'assertion voulue pour les idéaux à droite (le cas des idéaux à gauche est symétrique). Soient $\mathfrak{a}$ un idéal à droite propre de H et $z \in \mathfrak{a}$ un élément de norme minimale non nulle. Soit $y \in \mathfrak{a}$; par la remarque précédente, il existe $t \in H$ avec $N(z^{-1}y - t) < 1$. On a alors $N(y - zt) < N(z)$; par minimalité, on obtient que $N(y - zt) = 0$ et donc $y = zt$. Donc $\mathfrak{a}$ est principal, engendré par z.

e) Comme on a $2 = 1^2 + 1^2 + 0^2 + 0^2$, on peut supposer p impair. L'idéal pH est bilatère et on peut former l'anneau quotient H/pH. Comme p est impair, H/pH est isomorphe à $\mathbf{H}(\mathbb{Z})/p\mathbf{H}(\mathbb{Z}) \simeq \mathbf{H}(\mathbb{F}_p)$. Or l'équation $a^2 + b^2 + c^2 + d^2 = 0$ a une solution non triviale dans $\mathbb{F}_p$, et l'élément de $\mathbf{H}(\mathbb{F}_p)$ correspondant à une telle solution engendre un idéal à droite propre de $\mathbf{H}(\mathbb{F}_p)$. L'image réciproque dans H de cet idéal est un idéal principal de la forme z_0H, par la question d), et il vérifie $pH \subsetneq z_0H \subsetneq H$. En particulier, il existe un élément $z' \in H$ vérifiant $z_0z' = p$. On obtient que $p^2 = N(p) = N(z_0)N(z')$. Or $N(z_0) > 1$ et $N(z') > 1$ (sinon z_0 ou z_1 est inversible dans H), donc on a finalement $N(z_0) = p$ par primalité.

f) Il suffit de montrer que dans la question précédente, on peut trouver $z \in \mathbf{H}(\mathbb{Z})$ tel que $N(z) = p$. Supposons que ce ne soit pas le cas et regardons l'image de $\xi = 2z_0$ dans $\mathbf{H}(\mathbb{Z})/4\mathbf{H}(\mathbb{Z}) \simeq \mathbf{H}(\mathbb{Z}/4\mathbb{Z})$ (où $z_0 \in H \setminus \mathbf{H}(\mathbb{Z})$ vérifie $N(z_0) = p$). Dans $\mathbf{H}(\mathbb{Z}/4\mathbb{Z})$, la norme de ξ est nulle, c'est-à-dire que $\xi\overline{\xi} = 0$. Il suffit alors de relever $\overline{\xi}$ en un élément de $\{\varepsilon_1 1 + \varepsilon_2 i + \varepsilon_3 j + \varepsilon_4 k : \varepsilon_1, \ldots, \varepsilon_4 \in \{\pm 1\}\} \subseteq \mathbf{H}(\mathbb{Z})$, et de poser $z_1 := \frac{1}{2}\overline{\xi}$ dans H. Il en résulte que $N(z_0z_1) = p$ (puisque $N(z_1) = 1$) avec $z_0z_1 \in \mathbf{H}(\mathbb{Z})$. On peut donc supposer dans la question e) que $z \in \mathbf{H}(\mathbb{Z})$.

Le résultat pour tout entier naturel se déduit alors de la question b) et de la décomposition en facteurs premiers dans $\mathbb{Z}$.

Exercice 12 : $\star\star\star$

Soient K un corps de caractéristique $\neq 2$, $\alpha, \beta \in K^*$. On note $\mathbf{H} := \mathbf{H}_{\alpha,\beta}$ (voir l'exercice 10 pour la définition) et $\mathbf{H}^\times := \{x \in \mathbf{H} : N(x) \neq 0\}$.
Pour tout $q \in \mathbf{H}^\times$ et $x \in \mathbf{H}$, on note $S_q(x) := qxq^{-1}$. On rappelle que l'on dispose de la norme N sur $\mathbf{H}$ qui est une forme quadratique.

a) Montrer que pour tout $q \in \mathbf{H}^\times$ et tout $x \in \mathbf{H}$, $N(S_q(x)) = N(x)$.

b) Montrer que pour tout $q \in \mathbf{H}^\times$, $S_{q|_K} = \mathrm{id}_K$ et $S_q(\mathbf{P}) = \mathbf{P}$, où $\mathbf{P} \subset \mathbf{H}$ désigne l'espace des quaternions purs.

c) En déduire un morphisme de groupes $s : \mathbf{H}^\times \to \mathrm{O}(\mathbf{P}, N)$ et montrer que son noyau est K^*.

d) Montrer que pour tout $p \in \mathbf{P}^\times := \mathbf{P} \cap \mathbf{H}^\times$, $s(p)$ est le renversement d'axe p. En déduire que $s(\mathbf{H}^\times) = \mathrm{SO}(\mathbf{P}, N)$.

e) En déduire un isomorphisme $\mathbf{H}^\times/K^* \cong \mathrm{SO}(\mathbf{P}, N)$.

f) On suppose $\alpha = \beta = 1$. Montrer que N est une forme isométrique à la forme quadratique $(x, y, z) \mapsto x^2 - y^2 - z^2$ sur K^3. Montrer que $\mathrm{PGL}_2(K) \cong \mathrm{SO}_3(K, N)$ et $\mathrm{PSL}_2(K) \cong \Omega_3(K, N) := D(\mathrm{O}_3(K, N))$.

g) Montrer que pour tout $u \in \mathrm{SO}(\mathbf{H}, N)$, il existe $a, b \in \mathbf{H}^\times$ tels que $u(x) = axb$ pour tout $x \in \mathbf{H}$. Montrer en outre que $N(a)N(b) = 1$.

h) Montrer que pour tout $u \in \mathrm{O}(\mathbf{H}, N) \setminus \mathrm{SO}(\mathbf{H}, N)$, il existe $a, b \in \mathbf{H}^\times$ tels que $u(x) = a\overline{x}b$ pour tout $x \in \mathbf{H}$.

i) Notons $U := \{(a, b) \in \mathbf{H}^\times \times \mathbf{H}^\times : N(a) = N(b)\}$. Construire un morphisme de groupes surjectif $S : U \to \mathrm{SO}(\mathbf{H}, N)$ et calculer son noyau.

j) On suppose $\alpha = \beta = 1$. Montrer que N est une forme hyperbolique sur $\mathrm{Mat}_2(K)$ et que les groupes $\mathrm{P}\Omega_4(K, N) := \mathrm{P}(\mathrm{D}(\mathrm{O}_4(K, N)))$ et $\mathrm{PSL}_2(K) \times \mathrm{PSL}_2(K)$ sont isomorphes.

Solution de l'exercice 12.

a) C'est clair puisque la norme est multiplicative et $N(1) = 1$.

b) Par définition, K est contenu dans le centre de $\mathbf{H}$, ce qui assure que $S_{q|_K} = \mathrm{id}_K$. En outre, on a toujours l'équivalence, pour un $x \in \mathbf{H} \setminus \{0\}$, $x \in \mathbf{P}$ si et seulement si $x \notin K$ et $x^2 \in K$. Cette caractérisation (ou un calcul direct) assure que $S_q(\mathbf{P}) = \mathbf{P}$.

c) Les questions a) et b) assurent que si l'on pose $s(q) := S_{q|_{\mathbf{P}}}$ pour tout $q \in \mathbf{H}^\times$, on définit ainsi un élément $s(q) \in \mathrm{O}(\mathbf{P}, N)$. Or il est clair que $s(1) = \mathrm{id}_{\mathbf{P}}$ et $s(qq') = s(q)s(q')$, donc on a bien défini un morphisme de groupes $s : \mathbf{H}^\times \to \mathrm{O}(\mathbf{P}, N)$. Calculons son noyau : un élément de $\mathbf{H}$ commutant avec tous les éléments de $\mathbf{P}$ commute avec tous les éléments de $\mathbf{H}$, donc est dans K. Par conséquent, $\mathrm{Ker}(s) = K \cap \mathbf{H}^\times = K^*$.

d) Soit σ la réflexion orthogonale d'axe p. Alors on sait que pour tout $x \in \mathbb{P}$, $\sigma(x) = x - 2\frac{\langle x,p\rangle}{N(p)}p = x - \frac{x\overline{p}+p\overline{x}}{p\overline{p}}p$. Or pour tout $x \in \mathbb{P}$, on a $\overline{x} = -x$, donc $\sigma(x) = \frac{pxp}{N(p)}$, donc le renversement d'axe p est donné par $x \mapsto -\sigma(x) = -\frac{pxp}{N(p)} = pxp^{-1} = s(p)$, d'où le résultat.

En particulier, $s(p)$ est un renversement pour tout $p \in \mathbf{P}^\times$, donc $\det(s(p)) = 1$ pour tout $p \in \mathbf{P}^\times$.

Soit alors $z \in \mathbf{H}^\times$. On sait que tout élément de $\mathrm{O}(\mathbf{P}, N)$ est produit de reflexions orthogonales, donc il existe $q_1, \ldots, q_r \in \mathbf{P}^\times$ tels que $s(z)$ est la composée des reflexions orthogonales d'axe $q_1, \ldots, q_r$. Donc $s(z) = (-1)^r s(q_1) \circ \cdots \circ s(q_r)$. Supposons que $s(z) \notin \mathrm{SO}(\mathbf{P}, N)$. Alors r est impair, et pour tout $x \in \mathbf{P}$, on a $zxz^{-1} = -q_1 \ldots q_r x (q_1 \ldots q_r)^{-1}$. En notant $q := q_1 \ldots q_r$, on en déduit que pour tout $x \in \mathbf{H}$, $\overline{x} = (z^{-1}q)x(z^{-1}q)^{-1}$. Ceci est contradictoire puisque $x \mapsto \overline{x}$ est un anti-automorphisme alors que $x \mapsto (z^{-1}q)x(z^{-1}q)^{-1}$ est un automorphisme. Par conséquent, $s(z) \in \mathrm{SO}(\mathbf{P}, N)$.

On a donc montré que $s(\mathbf{H}^\times) \subset \mathrm{SO}(\mathbf{P}, N)$. Enfin, tout élément de $\mathrm{SO}(\mathbf{P}, N)$ est produit de renversements, et les renversements sont dans l'image de s (et même dans $s(\mathbf{P}^\times)$), donc $s(\mathbf{H}^\times) = \mathrm{SO}(\mathbf{P}, N)$.

e) C'est la conjonction des questions c) et d).

f) Pour tout $q = xi + yj + zk \in \mathbf{P}$, on a $N(q) = -x^2 - y^2 + z^2$, d'où la description de la classe d'isométrie de N. En outre, en adaptant la question b) de l'exercice 10, on voit facilement que dans le cas présent, on a un isomorphisme de K-algèbres $\mathbf{H} \cong \mathrm{Mat}_2(K)$, et donc un isomorphisme de groupes $\mathbf{H}^\times/K^* \cong \mathrm{PGL}_2(K)$. Par conséquent, la question e) fournit un isomorphisme $\mathrm{PGL}_2(K) \xrightarrow{\sim} \mathrm{SO}_3(K, N)$, et le calcul du groupe dérivé de $\mathrm{GL}_2(K)$ assure que cet isomorphisme induit l'isomorphisme suivant entre les sous-groupes dérivés :

$$\mathrm{PSL}_2(K) \xrightarrow{\sim} \Omega_3(K, N)$$

(noter que ce résultat généralise l'isomorphisme obtenu à l'exercice 7, question d), de la feuille de TD7, dans le cas où K était un corps fini).

g) et h) Comme à la question d), on voit facilement que pour tout $q \in \mathbf{H}^\times$, la reflexion orthogonale de droite Kq est donnée par la formule suivante : $x \mapsto \frac{-q\overline{x}q}{N(q)}$. Or tout élément de $\mathrm{SO}(\mathbf{H}, N)$ (resp. $\mathrm{O}(\mathbf{H}, N) \setminus \mathrm{SO}(\mathbf{H}, N)$) est produit d'un nombre pair (resp. impair) de reflexions orthogonales. On en déduit donc les deux formules souhaitées, en composant un nombre pair (resp. impair) de reflexions données par des formules du type $x \mapsto \frac{-q\overline{x}q}{N(q)}$, pour certains $q \in \mathbf{H}^\times$. La condition $N(a)N(b) = 1$ dans la question g) s'obtient en écrivant que $N(u(x)) = N(x)$ pour tout x.

i) Pour $(a, b) \in U$, on définit $S_{a,b} : \mathbf{H} \to \mathbf{H}$ par $S_{a,b}(q) := aqb^{-1}$. Il est clair que pour tout $(a, b) \in U$, $S_{a,b} \in \mathrm{O}(\mathbf{H}, N)$, et que l'on définit ainsi un morphisme de groupes $S : U \to \mathrm{O}(\mathbf{H}, N)$. Soit $(a, b) \in U$. Supposons que $S_{a,b} \notin \mathrm{SO}(\mathbf{H}, N)$. Alors la question h) assure qu'il existe $c, d \in \mathbf{H}^\times$ tels que pour tout $x \in H$, on ait $S_{a,b}(x) = c\overline{x}d$. On en déduit que pour tout $x \in \mathbf{H}$, on a $c^{-1}axb^{-1}d^{-1} = \overline{x}$, relation qui implique que pour tout $x \in \mathbf{H}$, $c^{-1}axa^{-1}c = \overline{x}$, ce qui aboutit à une contradiction comme à la question d). Donc S est à valeur dans $\mathrm{SO}(\mathbf{H}, N)$. La question g) assure que l'image du morphisme de groupes S contient $\mathrm{SO}(\mathbf{H}, N)$, donc S est un bien un morphisme de groupes surjectif $\mathbf{H}^\times \to \mathrm{SO}(\mathbf{H}, N)$. Son noyau est constitué de l'ensemble

des $(a,b) \in U$ tels que $axb^{-1} = x$ pour tout $x \in \mathbf{H}$, i.e. l'ensemble des $(a,b) \in U$ tels que $a = b$ (prendre $x = 1$) et a commute avec tous les éléments de $\mathbf{H}$. Donc $\mathrm{Ker}(S) = \{(\lambda,\lambda) : \lambda \in K^*\}$.

j) On voit que dans ce cas, pour tout $q = x+yi+zj+tk \in \mathbf{H}$, on a $N(q) = x^2-y^2-z^2+t^2$. Donc $(\mathbf{H}, N)$ est bien somme de deux plans hyperboliques. Comme à la question f), on sait que l'on a un isomorphisme de K-algèbres $\mathbf{H} \xrightarrow{\sim} \mathrm{Mat}_2(K)$. Cet isomorphisme induit des isomorphismes de groupes $\mathbf{H}^\times \xrightarrow{\sim} \mathrm{GL}_2(K)$ et $U \xrightarrow{\sim} \{(A,B) \in \mathrm{GL}_2(K) \times \mathrm{GL}_2(K) : \det(A) = \det(B)\}$. Donc $D(U) \cong \mathrm{SL}_2(K) \times \mathrm{SL}_2(K)$ puisque $D(\mathrm{GL}_2(K)) = \mathrm{SL}_2(K)$. On en déduit via la question i) que S induit un isomorphisme $(\mathrm{SL}_2(K) \times \mathrm{SL}_2(K))/\{\pm I_2\} \xrightarrow{\sim} \Omega_4(K,N)$. En quotientant ces deux groupes par leur centre, on obtient finalement un isomorphisme

$$\mathrm{PSL}_2(K) \times \mathrm{PSL}_2(K) \xrightarrow{\sim} \mathrm{P}\Omega_4(K,N)\,,$$

isomorphisme qui généralise le cas des corps finis traité à la question e) de l'exercice 7 de la feuille de TD7.

TD10 : Produit tensoriel

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Soit K un corps, et soient A et B des K-algèbres.

a) Définir une structure de K-algèbre sur $A \otimes_K B$.

b) Montrer que les K-algèbres $K[X] \otimes_K K[Y]$ et $K[X,Y]$ sont isomorphes.

c) Montrer que le morphisme naturel de K-algèbres de $K(X) \otimes_K K(Y)$ vers $K(X,Y)$ est injectif mais non surjectif.

Solution de l'exercice 1.

a) On sait que $A \otimes_K B$ est naturellement muni d'une structure de K-espace vectoriel. Il reste à définir la multiplication. Pour cela, on remarque par exemple que la multiplication sur A est une application bilinéaire $A \times A \to A$, donc elle induit une application linéaire $m_A : A \otimes A \to A$. On dispose donc d'une application linéaire naturelle

$$m_A \otimes m_B : (A \otimes A) \otimes (B \otimes B) \to A \otimes B$$

définie sur les tenseurs purs par $(m_A \otimes m_B)(a \otimes a' \otimes b \otimes b') = aa' \otimes bb'$. Alors la commutativité et l'associativité du produit tensoriel permettent d'identifier cette application à une application linéaire

$$m_{A\otimes B} : (A \otimes B) \otimes (A \otimes B) \to A \otimes B\,,$$

correspondant à une application bilinéaire $m : (A\otimes B)\times(A\otimes B) \to A\otimes B$ qui est la multiplication souhaitée. Par construction, elle vérifie $m(a \otimes b, a' \otimes b') = (aa') \otimes (bb')$.
En utilisant le fait que les multiplications m_A et m_B munissent A et B d'une structure de K-algèbre, il est facile de vérifier que m munit $A \otimes B$ d'une structure de K-algèbre : par exemple, on vérifie que

$$(a_1 \otimes b_1 + a_2 \otimes b_2)\, a' \otimes b' = (a_1 \otimes b_1)(a' \otimes b') + (a_2 \otimes b_2)(a' \otimes b') = a_1a' \otimes b_1b' + a_2a' \otimes b_2b'\,,$$

et que K est central dans l'algèbre $A \otimes B$ ainsi définie.
Une variante consiste à considérer, pour tout $(a,b) \in A \times B$, l'application bilinéaire $m_{a,b} : A \times B \to A \otimes B$ définie par $(a',b') \mapsto aa' \otimes bb'$. Elle induit naturellement une application linéaire $m_{a,b} : A \otimes B \to A \otimes B$. Il est facile de voir que l'application $m : (a,b) \mapsto m_{a,b}$ est une application bilinéaire $m : A \times B \to \mathrm{End}_K(A \otimes B)$, donc elle induit une application linéaire $M : A \otimes B \to \mathrm{End}_K(A \otimes B)$. Il est alors clair que M induit une application bilinéaire $M' : (A \otimes B) \times (A \otimes B) \to A \otimes B$, qui est la multiplication souhaitée.

b) L'application naturelle $K[X] \times K[Y] \to K[X,Y]$ définie par $(P(X), Q(Y)) \mapsto P(X)Q(Y)$ est clairement bilinéaire, donc elle induit une application linéaire $\varphi : K[X] \otimes_K K[Y] \to K[X,Y]$. Il est facile de voir que φ est un morphisme de K-algèbres (pour la structure de K-algèbre définie en a)).
On voit ensuite que φ envoie la base $(X^i \otimes Y^j)_{(i,j)\in\mathbb{N}^2}$ de $K[X]\otimes K[Y]$ sur la base $(X^iY^j)_{(i,j)\in\mathbb{N}^2}$ de $K[X,Y]$, donc φ est un isomorphisme.
On peut également considérer l'application linéaire $\psi : K[X,Y] \to K[X] \otimes_K K[Y]$ définie par $\sum_{m,n} \lambda_{m,n} X^m Y^n \mapsto \sum_{m,n} \lambda_{m,n}\, X^m \otimes Y^n$ (ces sommes sont finies), et vérifie que $\psi \circ \varphi$ et $\varphi \circ \psi$ sont bien les applications identité sur chacun des espaces en question.

c) On dispose comme en b) d'une application linéaire naturelle $\widetilde{\varphi} : K(X) \otimes_K K(Y) \to K(X,Y)$, définie par $\widetilde{\varphi}(f(X) \otimes f(Y)) = f(X)g(Y)$. On voit que l'image de $\widetilde{\varphi}$ est incluse dans le sous-espace strict

$$V := \left\{ R(X,Y) \in K(X,Y) : \exists (Q_1(X), Q_2(Y)) \in K[X] \times K[Y] \,,\, R(X,Y)Q_1(X)Q_2(Y) \in K[X,Y] \right\}.$$

Ceci montre bien que $\widetilde{\varphi}$ n'est pas surjective, puisque par exemple l'élément $\frac{1}{X+Y} \in K(X,Y)$ n'est pas dans V.

Définissons

$$\begin{array}{rccc} \widetilde{\psi} : & V & \to & K(X) \otimes_K K(Y) \\ & \dfrac{\sum_{m,n} \lambda_{m,n} X^m Y^n}{Q_1(X)Q_2(Y)} & \mapsto & \sum_{m,n} \lambda_{m,n} \dfrac{X^m}{Q_1(X)} \otimes \dfrac{Y^n}{Q_2(Y)} \end{array} .$$

On constate facilement que $\widetilde{\psi}$ est bien définie et que $\widetilde{\psi} \circ \widetilde{\varphi}$ est l'identité, ce qui assure l'injectivité voulue.

Exercice 2 : $\star$

a) Notons $M_2(\mathbb{C})$ la $\mathbb{C}$-algèbre des matrices 2×2 à coefficients dans $\mathbb{C}$ et $\mathbf{H}$ la $\mathbb{R}$-algèbre des quaternions. Montrer que les $\mathbb{C}$-algèbres $M_2(\mathbb{C})$ et $\mathbf{H} \otimes_{\mathbb{R}} \mathbb{C}$ sont isomorphes.

b) Montrer que $\mathbf{H} \otimes_{\mathbb{R}} \mathbf{H}$ est isomorphe à $M_4(\mathbb{R})$.

Solution de l'exercice 2.

a) On constate d'abord que $\mathbf{H} \otimes_{\mathbb{R}} \mathbb{C}$ est naturellement munie d'une structure de $\mathbb{C}$-algèbre : on a un isomorphisme naturel de $\mathbb{C}$-espaces vectoriels $\mathbf{H} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}i \oplus \mathbb{C}j \oplus \mathbb{C}k$, avec $i^2 = j^2 = k^2 = -1$, et $ij = -ji = k$.

Par conséquent, il est facile de vérifier que l'application

$$1 \otimes a + i \otimes b + j \otimes c + k \otimes d \mapsto \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

définit bien un isomorphisme de $\mathbb{C}$-algèbres $\mathbf{H} \otimes \mathbb{C} \xrightarrow{\sim} \mathrm{Mat}_2(\mathbb{C})$.

b) On va montrer que $\mathbf{H} \otimes_{\mathbb{R}} \mathbf{H}$ est isomorphe à $\mathrm{Mat}_2(\mathbb{R}) \otimes_{\mathbb{R}} \mathrm{Mat}_2(\mathbb{R})$ (qui est isomorphe à $\mathrm{Mat}_4(\mathbb{R})$, puisque pour toute K-algèbre A, on a que $\mathrm{Mat}_n(K) \otimes_K A \simeq \mathrm{Mat}_n(A)$).

On considère la sous-$\mathbb{R}$-algèbre A de dimension 4 de $\mathbf{H} \otimes_{\mathbb{R}} \mathbf{H}$ engendrée par $1 \otimes 1, i \otimes 1, j \otimes j, k \otimes j$ (on vérifie que le sous-espace vectoriel engendré par ces quatre vecteurs est bien une sous-algèbre). Alors l'application linéaire $a : A \to \mathrm{Mat}_2(\mathbb{R})$ définie par $a(1 \otimes 1) := I_2$, $a(i \otimes 1) := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $a(j \otimes j) := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $a(k \otimes j) := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ est bien un isomorphisme de $\mathbb{R}$-algèbres. De même, on définit la sous-$\mathbb{R}$-algèbre B de dimension 4 de $\mathbf{H} \otimes_{\mathbb{R}} \mathbf{H}$ engendrée par $1 \otimes 1, 1 \otimes j, i \otimes k, i \otimes i$ (on vérifie que le sous-espace vectoriel engendré par ces quatre vecteurs est bien une sous-algèbre). Alors on voit que l'isomorphisme linéaire $A \to B$ défini par $1 \otimes 1 \mapsto 1 \otimes 1$, $i \otimes 1 \mapsto 1 \otimes j$, $j \otimes j \mapsto i \otimes k$ et $k \otimes j \mapsto i \otimes i$ est un morphisme de $\mathbb{R}$-algèbres, donc $B \cong \mathrm{Mat}_2(\mathbb{R})$ comme $\mathbb{R}$-algèbres.

Enfin, les deux sous-$\mathbb{R}$-algèbres A et B commutent dans $\mathbf{H} \otimes_{\mathbb{R}} \mathbf{H}$, donc l'application linéaire naturelle $A \otimes_{\mathbb{R}} B \to \mathbf{H} \otimes_{\mathbb{R}} \mathbf{H}$ induite par la multiplication dans $\mathbf{H} \otimes_{\mathbb{R}} \mathbf{H}$ (i.e. $(a,b) \mapsto ab$) est un morphisme de $\mathbb{R}$-algèbres. On vérifie enfin que c'est un isomorphisme en calculant les dimensions et en montrant par exemple que l'image contient des générateurs de $\mathbf{H} \otimes_{\mathbb{R}} \mathbf{H}$.

Plus directement, notons $\sigma_i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\sigma_j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\sigma_k = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. On pose ensuite

$$\alpha(1 \otimes 1) = 1 \otimes 1, \quad \alpha(i \otimes 1) = \sigma_i \otimes \sigma_j, \quad \alpha(j \otimes 1) = \sigma_j \otimes 1, \quad \alpha(k \otimes 1) = \sigma_k \otimes \sigma_j \,.$$

Ces matrices vérifient les mêmes relations que les générateurs de $\mathbf{H}$. Faisons la même chose de manière symétrique :

$$\alpha(1 \otimes 1) = 1 \otimes 1, \quad \alpha(1 \otimes i) = \sigma_j \otimes \sigma_i, \quad \alpha(1 \otimes j) = 1 \otimes \sigma_j, \quad \alpha(1 \otimes k) = \sigma_j \otimes \sigma_k \,.$$

Cela suffit pour prolonger α en un morphisme d'algèbres $\mathbf{H} \otimes_{\mathbb{R}} \mathbf{H} \to \mathrm{Mat}_2(\mathbb{R}) \otimes_{\mathbb{R}} \mathrm{Mat}_2(\mathbb{R})$, dont on vérifie (en calculant les dimensions) que c'est un isomorphisme.

Exercice 3 : $\star\star$

a) Soient U et V des espaces vectoriels (sur un corps K). On note $U^* = \mathrm{Hom}_K(U, K)$ le dual de U. Expliciter une application linéaire naturelle injective $\Phi : U^* \otimes_K V \to \mathrm{Hom}_K(U, V)$. Quelles sont les images des tenseurs décomposés (c'est-à-dire les $\lambda \otimes v$ avec $\lambda \in U^*$ et $v \in V$) ? Quelle est l'image de l'application Φ ? Quand est-elle un isomorphisme ?

b) Soient E et F deux K-espaces vectoriels de dimension finie. Que vaut

$$\max_{x \in E \otimes F} \min \left\{ n \in \mathbb{N} : \exists (e_1, \dots, e_n) \in E^n \text{ et } (f_1, \dots, f_n) \in F^n \,,\, x = \sum_{i=1}^{n} e_i \otimes f_i \right\} ?$$

Solution de l'exercice 3.

a) On définit $\phi : U^* \times V \to \mathrm{Hom}_K(U, V)$ par $\phi(\varphi, v) := \varphi(.)v$. Il est clair que l'application ϕ est bilinéaire, donc elle induit une application $\Phi : U^* \otimes_K V \to \mathrm{Hom}_K(U, V)$. Il est clair que l'image de Φ est exactement le sous-espace $W \subset \mathrm{Hom}_K(U, V)$ des applications linéaires de rang fini. Par construction, les tenseurs décomposés sont envoyés sur les applications linéaires de rang 1. En outre, pour tout $f \in W$, on choisit une base $(v_i)_{1 \leq i \leq n}$ de $\mathrm{Im}\,(f)$, de sorte que $f = \sum_{i=1}^{n} f_i(.)v_i$, avec $f_i \in U^*$. La formule de changement de bases assure que l'élément $\Psi(f) := \sum_{i=1}^{n} f_i \otimes v_i \in U^* \otimes_K V$ ne dépend pas de la base (v_i) choisie. Cela permet de définir une application linéaire $\Psi : W \to U^* \otimes_K V$ telle que $\Psi \circ \Phi = \mathrm{id}$, ce qui assure que Φ est injective (d'image W).

Finalement, Φ est un isomorphisme si et seulement si tout application linéaire $U \to V$ est de rang fini si et seulement si U ou V est de dimension finie.

b) La question a) assure que l'on a un isomorphisme canonique $\Phi : E \otimes_K F \xrightarrow{\sim} \mathrm{Hom}_K(E^*, F)$, et que si pour tout $x \in E \otimes_K F$, on note

$$\mathrm{rg}(x) := \min \left\{ n \in \mathbb{N} : \exists (e_1, \dots, e_n) \in E^n \text{ et } (f_1, \dots, f_n) \in F^n \,,\, x = \sum_{i=1}^{n} e_i \otimes f_i \right\} ,$$

alors on a $\mathrm{rg}(x) = \mathrm{rg}(\Phi(x))$, où le second rang est le rang classique d'une application linéaire. Par conséquent, on voit immédiatement que l'on a

$$\max_{x \in E \otimes F} \min \left\{ n \in \mathbb{N} : \exists (e_1, \dots, e_n) \in E^n \text{ et } (f_1, \dots, f_n) \in F^n \,,\, x = \sum_{i=1}^{n} e_i \otimes f_i \right\} = \min\{\dim(E), \dim(F)\} .$$

Remarque : la question plus générale du nombre maximal de tenseurs décomposables dont on a besoin pour écrire un élément quelconque de $E_1 \otimes_K \cdots \otimes_K E_n$, où les E_i sont des K-espaces vectoriels de dimension finie, est très difficile si $n \geq 3$. Cette question est encore largement ouverte, et la réponse dépend du corps K...

Exercice 4 :
Soit K un corps et soit E un espace vectoriel de dimension finie sur K. Soit $n \geq 1$ un entier. Montrer que le dual $(\bigwedge^n E)^*$ de $\bigwedge^n E$ est canoniquement isomorphe à $\bigwedge^n E^*$.

Solution de l'exercice 4. Définissons l'application bilinéaire suivante

$$\begin{array}{rccc} b : & (E^*)^n \times E^n & \to & K \\ & ((\alpha_i)_i, (x_j)_j) & \mapsto & \det((\alpha_i(x_j))_{ij}) \end{array} .$$

Pour tout $(x_j)_j$, l'application $b(\cdot, (x_j))$ est alternée et passe donc au quotient pour définir $\bigwedge^n E^* \times E^n \to K$. De la même manière, c'est encore alterné en l'autre variable et b induit donc une application

bilinéaire $\bar{b} : \bigwedge^n E^* \times \bigwedge^n E \to K$. Cette dernière est non dégénérée : il suffit de prendre pour $(\alpha_i)_i$ la base duale de (x_i) pour obtenir 1.
L'application $(\alpha_i)_i \mapsto b((\alpha_i), \cdot)$ est l'isomorphisme $\bigwedge^n E^* \xrightarrow{\sim} \left(\bigwedge^n E\right)^*$ recherché.

Exercice 5 :
Soit $n \geq 1$ un entier, soit K un corps et soit E un espace vectoriel de dimension n sur K. Montrer que le dual $(\bigwedge^i E)^*$ de $\bigwedge^i E$ est non canoniquement isomorphe à $\bigwedge^{n-i} E$.

Solution de l'exercice 5. L'application naturelle $\bigwedge^i E \times \bigwedge^{n-i} E \to \bigwedge^n E$ composée avec l'isomorphisme non canonique (voir cours) $\bigwedge^n E \simeq K$ montrent que $(\bigwedge^i E)^*$ est non canoniquement isomorphe à $\bigwedge^{n-i} E$.

Exercice 6 : $\star\star$
Soit K un corps et soient E et F des K-espaces vectoriels de dimension finie. Soit $n \geq 1$ un entier. Montrer que l'on a une bijection entre l'ensemble des applications linéaires $\bigwedge^n E \to F$ et l'ensemble des applications n-linéaires alternées $E^n \to F$.

Solution de l'exercice 6. Si $f : \bigwedge^n E \to F$, on peut lui associer $(e_i)_i \mapsto f(e_1 \wedge \cdots \wedge e_n)$.
On peut construire l'application réciproque de la manière suivante : notons $\phi : \bigwedge^n E^* \xrightarrow{\sim} \left(\bigwedge^n E\right)^*$ l'isomorphisme de l'exercice 4. Notons $(f_1, \ldots, f_r)$ une base de F et $(f_1^*, \ldots, f_r^*)$ la base duale. Si $g : E^n \to F$ est n-linéaire alternée, on lui associe $\sum_j \phi(f_j^* \circ g) f_j$. On vérifie ensuite que c'est bien l'inverse de l'application précédente.

Exercice 7 : $\star\star$
Soit K un corps et soit E un K-espace vectoriel. Soient $u_1, \ldots, u_r$ des éléments de E.

a) Montrer que l'on a $u_1 \wedge \cdots \wedge u_r \neq 0$ dans $\bigwedge^r E$ si et seulement si la famille $(u_1, \ldots, u_r)$ est libre dans E.

b) Montrer que l'on a $u_1 \wedge \cdots \wedge u_r \neq 0$ dans $\bigwedge^r E$ si et seulement s'il existe une forme alternée f sur E telle que $f(u_1, \ldots, u_r) \neq 0$.

Solution de l'exercice 7.

a) Si on a une relation linéaire non triviale $\lambda_1 u_1 + \cdots + \lambda_r u_r = 0$ avec les λ_i dans K, on peut supposer $\lambda_{i_0} = 1$ pour un certain i_0. Alors on a

$$u_1 \wedge \cdots \wedge u_r = -\sum_{j \neq i_0} \lambda_j \, u_1 \wedge \cdots \wedge u_{i_0 - 1} \wedge u_j \wedge u_{i_0 + 1} \wedge \ldots u_r = 0 \, .$$

Si la famille $(u_i)_i$ est libre, notons F le sous-espace de E engendré par ces vecteurs : la droite $\bigwedge^r F \subseteq \bigwedge^r E$ est alors engendrée par $u_1 \wedge \cdots \wedge u_r$.

b) Si $u_1 \wedge \cdots \wedge u_r$ est non nul, notons F le sous-espace de E de base $(u_1, \ldots, u_r)$. Alors la forme linéaire $\bigwedge^r F \to K$ définie par $u_1 \wedge \cdots \wedge u_r \mapsto 1$ peut se prolonger par 0 sur un supplémentaire de $\bigwedge^r F$ dans $\bigwedge^r E$ et on obtient une forme linéaire $f : \bigwedge^r E \to K$ telle que $f(u_1 \wedge \cdots \wedge u_r) \neq 0$. La réciproque est évidente.

Exercice 8 :
Soit K un corps et soient E et F des K-espaces vectoriels. Soit $n \geq 1$ un entier et soit $u : E \to F$ une aplication linéaire.

a) Définir une application linéaire "naturelle" $\bigwedge^n u : \bigwedge^n E \to \bigwedge^n F$.

b) Supposons que le rang de u est fini égal à un entier r. Montrer que si $n \leq r$, alors le rang de $\bigwedge^n u$ est $\binom{n}{r}$, et si $n > r$, l'application $\bigwedge^n u$ est nulle.

Solution de l'exercice 8.

a) Il s'agit de $\bigwedge^n u : x_1 \wedge \cdots \wedge x_n \mapsto u(x_1) \wedge \cdots \wedge u(x_n)$.

b) On vérifie que l'image de $\bigwedge^n u$ est $\bigwedge^n \big(\mathrm{Im}\,(u)\big)$, ce qui assure le résultat.

Exercice 9 :
Soit K un corps et soient A et B des K-algèbres graduées.

a) Montrer qu'il existe sur $A \otimes_K B$ une structure naturelle de K-algèbre graduée telle que

$$(a \otimes b)(a' \otimes b') = (-1)^{(\deg b)(\deg a')}(aa' \otimes bb').$$

On note $A \otimes_K^{\mathrm{su}} B$ l'algèbre ainsi obtenue.

b) Soient V et W des espaces vectoriels sur K. Montrer que l'on a un isomorphisme de K-algèbres

$$\bigwedge(V \oplus W) \simeq \bigwedge V \otimes_K^{\mathrm{su}} \bigwedge W.$$

Solution de l'exercice 9.

a) D'abord, la multiplication ainsi définie est bien associative. Ensuite, la distributivité par rapport à l'addition permet de définir la multiplication sur $A \otimes B$ et de lui fournir la structure d'algèbre voulue (voir aussi l'exercice 1).

b) En tant que K-espaces vectoriels, l'isomorphisme est clair puisque l'on a, pour tout $n \geq 0$, un isomorphisme naturel :

$$\bigwedge^n (V \oplus W) \simeq \bigoplus_{k=0}^{n} \left(\bigwedge^k V\right) \otimes_K \left(\bigwedge^{n-k} W\right),$$

et ce dernier espace est exactement le sous-espace vectoriel de $(\bigwedge V) \otimes_K (\bigwedge W)$ formé des éléments de degré n.
Reste à vérifier la compatibilité avec la multiplication, qui se fait sur les tenseurs indécomposables. Pour cela,

soient $n, n' \in \mathbb{N}, 0 \leq k \leq n, 0 \leq k' \leq n', v_1, \ldots, v_k, v'_1, \ldots, v'_{k'} \in V, w_{k+1}, \ldots, w_n, w'_{k'+1}, \ldots, w'_{n'} \in W$.

On calcule le produit suivant dans $\bigwedge(V \oplus W)$:

$$(v_1 \wedge \cdots \wedge v_k \wedge w_{k+1} \wedge \cdots \wedge w_n) \wedge (v'_1 \wedge \cdots \wedge v'_{k'} \wedge w'_{k'+1} \wedge \cdots \wedge w'_{n'}) = (-1)^{(n-k)k'} v_I \wedge w_J,$$

où on a posé $v_I = v_1 \wedge \cdots \wedge v_k \wedge v'_1 \wedge \cdots \wedge v'_{k'}$ et $w_J = w_{k+1} \wedge \cdots \wedge w_n \wedge w'_{k'+1} \wedge \cdots \wedge w'_{n'}$.
Or par définition de $\otimes^{\mathrm{su}}$, on a dans $\bigwedge V \otimes_K^{\mathrm{su}} \bigwedge W$:

$$(v_1 \wedge \cdots \wedge v_k \otimes w_{k+1} \wedge \cdots \wedge w_n) \cdot^{\mathrm{su}} (v'_1 \wedge \cdots \wedge v'_{k'} \otimes w'_{k'+1} \wedge \cdots \wedge w'_{n'}) = (-1)^{(n-k)k'} v_I \otimes w_J,$$

ce qui assure que l'isomorphisme naturel de K-espaces vectoriels entre $\bigwedge(V \oplus W)$ et $(\bigwedge V) \otimes_K^{\mathrm{su}} (\bigwedge W)$ est bien un isomorphisme de K-algèbres.

Exercice 10 :
Soit K un corps et soit E un K-espace vectoriel.

a) Supposons E de dimension finie. On note $\bigwedge E = \bigoplus_n \bigwedge^n E$ et on écrit tout élément $z \in \bigwedge E$ sous la forme $z = \sum_{n \geq 0} z_n$. Montrer que $z \in \bigwedge E$ est inversible si et seulement si $z_0 \neq 0$.

b) Montrer que tout élément $z \in \bigwedge E$ appartient à un $\bigwedge F$ pour un certain sous-espace $F \subset E$ de dimension finie. En déduire une description des inversibles de $\bigwedge E$.

Solution de l'exercice 10.

a) Notons r la dimension de E. Si z est inversible d'inverse y, en projetant sur la composante en degré 0 de l'algèbre extérieure la relation $zy = 1$ dans $\bigwedge E$, on voit que $z_0 y_0 = 1$, donc la condition est nécessaire.

Réciproquement, supposons $z_0 \neq 0$. On vérifie que $z_0^{-1} \sum_{i=0}^{r} \big(-z_0^{-1} \sum_{n \geq 1} z_n\big)^{\wedge i}$ est une somme finie dans $\bigwedge E$ qui est l'inverse de z.

b) Seuls un nombre fini de z_n sont non nuls. Chacun s'écrit alors comme une somme finie

$$z_n = z_{n,1}^{(1)} \wedge \cdots \wedge z_{n,n}^{(1)} + \cdots + z_{n,1}^{(\alpha_n)} \wedge \cdots \wedge z_{n,n}^{(\alpha_n)} .$$

Il suffit alors de considérer pour F le sous-espace de E engendré par tous les $z_{n,i}^k$ avec $n \geq 0$ tel que $z_n \neq 0$, $1 \leq i \leq n$ et $1 \leq k \leq \alpha_n$. Alors $z \in \bigwedge F \subset \bigwedge E$.
La question a) assure alors que si $z_0 \neq 0$, alors z est inversible dans $\bigwedge F$, donc dans $\bigwedge E$. Réciproquement, si z est inversible dans $\bigwedge E$ d'inverse y, alors il existe un sous-espace vectoriel $G \subset E$ de dimension finie tel que $y, z \in \bigwedge G \subset \bigwedge E$, et la question a) assure que $z_0 \neq 0$.

Exercice 11 : ⋆⋆
Soit $n \geq 1$ un entier. Soient $F \subset E$ des corps tels que E est un F-espace vectoriel de dimension n, de base $(1, x_1, \ldots, x_{n-1})$. On suppose l'existence d'un groupe G de cardinal n, composé de F-automorphismes de E, tel que le corps $E^G = \{e \in E \mid \forall g \in G,\ ge = e\}$ est exactement F.

a) Montrer que les éléments de G sont linéairement indépendants.

b) Soit V un E-espace vectoriel, muni d'une action semi-linéaire de G. On définit le sous-F-espace vectoriel des G-invariants par $V^G := \{v \in V \mid \forall g \in G\ gv = v\}$. Prouver que l'application naturelle E-linéaire $\eta : V^G \otimes_F E \to V$ commute à l'action de G.

c) Montrer que η est un isomorphisme.

Solution de l'exercice 11.

a) On raisonne par l'absurde. Soit $\lambda_1 g_1 + \cdots + \lambda_k g_k = 0$ dans $\mathrm{End}_F(E) \subset E^E$ une relation de dépendance linéaire sur E de longueur k minimale (avec les $g_i \in G$ deux-à-deux distincts et $\lambda_i \in E^*$ pour tout i). On peut supposer $k \geq 2$. Comme les caractères g_i sont distincts, on a l'existence d'un élément $y \in E$ avec $g_1(y) \neq g_2(y)$. On a alors, pour tout $x \in E$, $g_1(y) \sum_i \lambda_i g_i(x) = 0$, et aussi $\sum_i \lambda_i g_i(xy) = \sum_i \lambda_i g_i(x) g_i(y) = 0$. En soustrayant ces deux égalités, on obtient une combinaison linéaire non triviale et strictement plus courte, à savoir

$$\lambda_2(g_2(y) - g_1(y))g_2 + \cdots + \lambda_k(g_k(y) - g_1(y))g_k = 0 ,$$

ce qui contredit la minimalité de la relation initiale.

b) Tout d'abord, on dispose bien d'une application E-linéaire $\eta : V^G \otimes_F E \to V$ puisque l'application $V^G \times E \to V$ définie par $(v, e) \mapsto ev$ est bilinéaire.
Pour tout $g \in G$, et tous $v \in V^G$ et $e \in E$, on a

$$\eta(g \cdot (v \otimes e)) = \eta(v \otimes g(e)) = \eta(g(v) \otimes g(e)) = g(e)g(v) = g(ev) ,$$

donc η est bien G-équivariante.

c) Montrons d'abord que η est surjective. Notons $g_1 = \mathrm{Id}, \ldots, g_n$ les éléments de G. On renomme aussi $x_0 := 1 \in E$. Soit v un élément non nul de V. Posons, pour tout $j \in \{0, \ldots, n-1\}$, $v_j := \sum_i g_i(x_j v) \in V^G$. Par la question a), la matrice $(g_i(x_j))_{i,j}$ est inversible, et en inversant le système précédent, on obtient les $g_i(v)$ comme combinaisons linéaires des v_j. La relation donnant $g_0(v)$ affirme alors la surjectivité souhaitée.
Montrons ensuite que η est injective. Si ce n'est pas le cas, il existe une famille $(v_1, \ldots, v_m)$ de vecteurs de V^G qui est F-libre mais non E-libre. On suppose l'entier m minimal pour cette propriété. On dispose d'une combinaison linéaire non triviale $\sum_i \lambda_i v_i = 0$ sur E. Comme les λ_i ne sont pas tous dans F, on peut supposer $\lambda_1 \notin F$ et $\lambda_m = 1$. Comme $\lambda_1 \notin F = E^G$, il existe $g \in G$ tel que $g(\lambda_1) \neq \lambda_1$. On obtient alors une relation $\sum_{i=1}^{m-1} (g(\lambda_i) - \lambda_i) v_i = 0$, qui contredit la minimalité de m. Donc η est bien injective.

Exercice 12 : ⋆⋆
Soit K un corps.

a) Définir une notion de suite exacte de K-espaces vectoriels.

b) Soit $0 \to V_1 \to V_2 \to V_3 \to 0$ une suite exacte de K-espaces vectoriels. Soit également W un K-espace vectoriel.

i) Montrer que la suite

$$0 \to \mathrm{Hom}_K(V_3, W) \to \mathrm{Hom}_K(V_2, W) \to \mathrm{Hom}_K(V_1, W) \to 0$$

est une suite exacte.

ii) Montrer que la suite

$$0 \to V_1 \otimes_K W \to V_2 \otimes_K W \to V_3 \otimes_K W \to 0$$

est une suite exacte.

Solution de l'exercice 12.

a) Soient $(E_n)_{n\in\mathbb{Z}}$ des K-espaces vectoriels et $f_n : E_n \to E_{n+1}$ des applications linéaires. On dit que la suite

$$\ldots \xrightarrow{f_{n-2}} E_{n-1} \xrightarrow{f_{n-1}} E_n \xrightarrow{f_n} E_{n+1} \xrightarrow{f_{n+1}} \ldots$$

est exacte en rang n (ou en E_n) si et seulement si $\mathrm{Im}\,(f_{n-1}) = \mathrm{Ker}(f_n)$. On dit que la suite est exacte si elle est exacte en rang n pour tout $n \in \mathbb{Z}$.

b) On note $f : V_1 \to V_2$ et $g : V_2 \to V_3$ les deux morphismes non triviaux de la suite exacte.

~~i)~~ Montrons que la composée $\mathrm{Hom}_K(V_3, W) \to \mathrm{Hom}_K(V_2, W) \to \mathrm{Hom}_K(V_1, W)$ est l'application nulle. Soit $\varphi : V_3 \to W$ une application linéaire. Alors l'image de φ dans $\mathrm{Hom}_K(V_2, W)$ est $\varphi \circ g$ et son image dans $\mathrm{Hom}_K(V_1, W)$ est $\varphi \circ g \circ f$. Or la suite initiale est exacte, donc $g \circ f = 0$, donc l'image de φ dans $\mathrm{Hom}_K(V_1, W)$ est nulle.

— Montrons maintenant que le noyau de $\mathrm{Hom}_K(V_2, W) \to \mathrm{Hom}_K(V_1, W)$ est contenu dans l'image de $\mathrm{Hom}_K(V_3, W) \to \mathrm{Hom}_K(V_2, W)$. Soit $\varphi : V_2 \to W$ dans ce noyau, i.e. tel que $\varphi \circ f = 0$. Alors $f(V_1) \subset \mathrm{Ker}(\varphi)$, donc le théorème de factorisation assure que φ se factorise en une application linéaire $V_2/f(V_1) \to W$. Or g induit un isomorphisme $V_2/f(V_1) \simeq V_3$, donc φ se factorise en $\overline{\varphi} : V_3 \to W$ de sorte que $\overline{\varphi} \circ g = \varphi$. Cela assure que φ est l'image de $\overline{\varphi}$ par l'application naturelle $\mathrm{Hom}_K(V_3, W) \to \mathrm{Hom}_K(V_2, W)$.

— Montrons que l'application $\mathrm{Hom}_K(V_3, W) \to \mathrm{Hom}_K(V_2, W)$ est injective. Soit $\varphi : V_3 \to W$ tel que $\varphi \circ g = 0$. Comme g est surjective par hypothèse, il est clair que cela implique que $\varphi = 0$, d'où l'injectivité souhaitée.

— Montrons que l'application $\mathrm{Hom}_K(V_2, W) \to \mathrm{Hom}_K(V_1, W)$ est surjective. Soit $\varphi : V_1 \to W$ une application linéaire. On choisit un supplémentaire V_1' de $f(V_1)$ dans V_2, et on définit une application linéaire $\psi : V_2 \to W$ en posant $\psi_{|_{f(V_1)}} = \varphi \circ {f_{|_{V_1}}}^{-1}$ et $\psi_{|_{V_1'}} = 0$. Il est alors clair que $\psi \circ f = \varphi$, donc φ est l'image de ψ par $\mathrm{Hom}_K(V_2, W) \to \mathrm{Hom}_K(V_1, W)$.

On a bien prouvé l'exactitude souhaitée.

ii) — Montrons que la composée $V_1 \otimes_K W \to V_2 \otimes_K W \to V_3 \otimes_K W$ est l'application nulle. Soit $v_1 \otimes w \in V_1 \otimes W$. Alors l'image de $v_1 \otimes w$ dans $V_2 \otimes W$ est $f(v_1) \otimes w$ et son image dans $V_3 \otimes W$ est $g(f(v_1)) \otimes W$. Or la suite initiale est exacte, donc $g \circ f = 0$, donc l'image de $v_1 \otimes w$ dans $V_3 \otimes W$ est nulle.

— Montrons maintenant que le noyau de $V_2 \otimes W \to V_3 \otimes W$ est contenu dans l'image de $V_1 \otimes W \to V_2 \otimes W$. Pour cela, on constate que le point précédent assure que l'application $V_2 \otimes W \to V_3 \otimes W$ se factorise en une application linéaire $\overline{f} : V_2 \otimes W/\mathrm{Im}\,(V_1 \otimes W) \to V_3 \otimes W$, définie par $\overline{f}(v_2 \otimes w) = f(v_2) \otimes w$. On définit une application $h : V_3 \times W \to V_2 \otimes W/\mathrm{Im}\,(V_1 \otimes W)$ de la façon suivante : si $(v_3, w) \in V_3 \times W$, la surjectivité de g assure qu'il existe $v_2 \in V_2$ tel que $g(v_2) = v_3$, et on définit $h(v_3, w)$ comme l'image de $v_2 \otimes w$ dans le quotient $V_2 \otimes W/\mathrm{Im}\,(V_1 \otimes W)$. Vérifions que la définition de h est correcte : si $v_2, v_2' \in V_2$ vérifient que $g(v_2) = v_3 = g(v_2')$, alors $v_2 - v_2' \in \mathrm{Ker}(g) = \mathrm{Im}\,(f)$, donc il existe $v_1 \in V_1$ tel que $v_1 - v_2' = f(v_1)$. Alors on a $v_2 \otimes w - v_2' \otimes w = (v_2 - v_2') \otimes w = f(v_1) \otimes w \in \mathrm{Im}\,(V_1 \otimes W)$. Donc h est bien définie.

En outre, il est clair que h est bilinéaire, donc h induit une application linéaire $\overline{h}$: $V_3 \otimes W \to V_2 \otimes W/\mathrm{Im}\,(V_1 \otimes W)$
Il est immédiat de vérifier que $\overline{h}$ est la réciroque de l'application $\overline{g}$. Cela assure bien que le noyau de $V_2 \otimes W \to V_3 \otimes W$ est égal à l'image de $V_1 \otimes W \to V_2 \otimes W$.

— Montrons que l'application $V_1 \otimes W \to V_2 \otimes W$ est injective. On fixe une base $(w_i)_{i\in I}$ de W. Alors $W \cong \bigoplus_{i\in I} Kw_i$, et le morphisme $V_1 \otimes W \to V_2 \otimes W$ s'identifie que morphisme $\bigoplus_{i\in I} f\otimes_{\mathrm{id}_i} : \bigoplus_{i\in I} V_1 \otimes Kw_i \to \bigoplus_{i\in I} V_2 \otimes Kw_i$, qui est bien injectif puisque chacune des composantes de ce morphisme est le morphisme injectif $f : V_1 \to V_2$.

— Montrons que l'application $V_2 \otimes W \to V_3 \otimes W$ est surjective. Soit $v_3 \otimes w \in V_3 \otimes W$. Par surjectivité de g, il existe $v_2 \in V_2$ tel que $g(v_2) = v_3$. Alors $v_3 \otimes w$ est l'image de $v_2 \otimes w$ par l'application $V_2 \otimes W \to V_3 \otimes W$. une application linéaire. On choisit un supplémentaire V_1' de $f(V_1)$ dans V_2, et on définit une application linéaire $\psi : V_2 \to W$ en posant $\psi_{|_{f(V_1)}} = \varphi \circ {f_{|_{V_1}}}^{-1}$ et $\psi_{|_{V_1'}} = 0$. Il est alors clair que $\psi \circ f = \varphi$, donc φ est l'image de ψ par $\mathrm{Hom}_K(V_2, W) \to \mathrm{Hom}_K(V_1, W)$.

On a bien prouvé l'exactitude souhaitée.

Remarque : on peut également déduire la question b) ii) de la question b) i), en montrant le fait suivant : une suite $0 \to E_1 \to E_2 \to E_3 \to 0$ de K-espaces vectoriels est exacte si et seulement si pour tout K-espace vectoriel F, la suite $0 \to \mathrm{Hom}_K(E_3, F) \to \mathrm{Hom}_K(E_2, F) \to \mathrm{Hom}_K(E_1, F) \to 0$ est une suite exacte. La preuve de ce fait est facile (du même ordre que la preuve de b)i)). Il suffit ensuite d'appliquer cela à la suite $0 \to V_1 \otimes W \to V_2 \otimes W \to V_3 \otimes W \to 0$, en utilisant les identifications $\mathrm{Hom}_K(V_i \otimes W, F) \simeq \mathrm{Hom}_K(V_i, \mathrm{Hom}_K(W, F))$...

Exercice 13 :
Soit V un espace vectoriel hermitien complexe de dimension finie n, de base $(e_1, \ldots, e_n)$. On ne suppose pas que cette base est orthonormale. Pour $1 \leq i \leq n$, soit s_i une transformation unitaire telle que $s_i(e_i) = c_i e_i$ avec $c_i \neq 1$ et telle que s_i est l'identité sur $e_i^\perp$. On appelle G le sous-groupe de $\mathrm{GL}(V)$ engendré par les s_i.

a) Soit $x \in V$. Exprimer $s_i(x)$ comme combinaison linéaire de x et de e_i.

b) Soit k un entier supérieur ou égal à 1. Montrer que tout élément de $\bigwedge^k V$ invariant par G est nul (on pourra procéder par récurrence sur n en considérant le sous-espace V' de base $(e_1, \ldots, e_{n-1})$ et en décomposant V en somme directe de V' et de son supplémentaire orthogonal).

c) On suppose que G est fini. Montrer que pour tout élément A de $\mathrm{End}(V)$ on a :

$$\sum_{g\in G} \det(A - g) = |G| \cdot \det(A) \quad \text{et} \quad \sum_{g\in G} \det(\mathrm{Id} - Ag) = |G|.$$

d) En déduire que pour tout A de $\mathrm{End}(V)$, il existe $g \in G$ tel que Ag n'a aucun point fixe non nul.

Solution de l'exercice 13.

a) La formule usuelle de projection orthogonale assure que l'on a

$$s_i(x) = (c_i - 1)\frac{\langle x, e_i\rangle}{\|e_i\|^2} e_i + x\,.$$

b) On raisonne par récurrence sur n :

— si $n = 1$, alors la seule valeur intéressante est $k = 1$, et on a $\bigwedge^k V = \bigwedge^1 V = V = Ke_1$. Or par définition, on a $s_1(e_1) = c_1 e_1 \neq e_1$, donc $\left(\bigwedge^k V\right)^G = \{0\}$.

— Soit $n > 1$ et supposons le résultat démontré si $\dim V = n - 1$. On considère le sous-espace vectoriel V' suggéré dans l'énoncé, ainsi que la décomposition en somme directe orthogonale $V = V' \oplus^\perp V'^\perp$. Alors $\dim V' = n-1$ et $\dim V'^\perp = 1$. Soit $k \geq 1$. On a alors un isomorphisme canonique

$$\bigwedge^k(V) \simeq \bigoplus_{i=0}^{k} \bigwedge^i(V') \otimes \bigwedge^{k-i}(V'^\perp) = \bigwedge^k(V') \oplus \left(\bigwedge^{k-1}(V') \otimes V'^\perp\right).$$

Supposons d'abord $k \geq 2$. Alors l'hypothèse de récurrence assure que $\bigwedge^k (V')^{G'} = \{0\}$ et $\bigwedge^{k-1}(V')^{G'} = \{0\}$, où $G' := \langle s_1, \dots, s_{n-1}\rangle \subset G$. Soit alors $x = x_1 + x_2 \otimes v \in \bigwedge^k(V)^G$, avec $x_1 \in \bigwedge^k(V')$, $x_2 \in \bigwedge^{k-1}(V')$ et $v \in V'^{\perp}$. Alors pour tout $1 \leq i \leq n-1$, on a $s_i(x) = x$, donc comme V' et $V'^{\perp}$ sont stables par s_i, on a $s_i(x_1) = x_1$ et $s_i(x_2) \otimes v = x_2 \otimes v$. Donc $x_1 \in \bigwedge^k(V')^{G'} = \{0\}$, donc $x = x_2 \otimes v$. Si $v = 0$, alors $x = 0$, sinon, on a $s_i(x_2) = x_2$ pour tout $1 \leq i \leq n-1$, donc $x_2 \in \bigwedge^{k-1}(V')^{G'} = \{0\}$, donc $x = 0$ dans tous les cas. Donc $\bigwedge^k(V)^G = \{0\}$.
Supposons maintenant $k = 1$. Alors par récurrence, on a seulement $\bigwedge^1(V')^{G'} = \{0\}$, et donc si $x = x_1 + x_2 \otimes v \in \bigwedge^1(V)^G$, on a toujours $x_1 = 0$, et donc $x = x_2 \otimes v$, avec $x_2 \in \mathbb{C}$ et $v \in V'^{\perp}$. On applique alors $s_n \in G$ à ce vecteur : $s_n(x) = x$ implique que $s_n(v) = v$. Si $v \neq 0$, Kv est un supplémentaire de V' et la restriction de s_n à V' est l'identité, alors que $s_n \neq \mathrm{id}$, donc $s_n(v) \neq v$. Par conséquent, $v = 0$ et donc $x = 0$. Donc $\bigwedge^1(V)^G = \{0\}$.
Cela conclut la preuve.

c) On considère l'endomorphisme $S := \sum_{g\in G} \bigwedge^n (A - g) : \bigwedge^n(V) \to \bigwedge^n(V)$. C'est une homothétie de rapport $\sum_{g\in G} \det(A - g)$. Soit alors $e := e_1 \wedge \cdots \wedge e_n$ un vecteur non nul de $\bigwedge^n(V)$. Alors

$$S(e) = S(e_1) \wedge \cdots \wedge S(e_n)$$

s'écrit, en développant, comme une somme finie de termes dont le premier est $\sum_{g\in G} A(e_1) \wedge \cdots \wedge A(e_n) = |G| \det(A) \cdot e$ et les suivants sont des multiples de vecteurs de la forme

$$A(e_{i_{k+1}}) \wedge \cdots \wedge A(e_{i_n}) \wedge \sum_{g\in G} g(e_{i_1}) \wedge \cdots \wedge g(e_{i_k})$$

avec $1 \leq k \leq n$ et $\{i_1, \dots, i_n\} = \{1, \dots, n\}$. Or pour tout $k \geq 1$, le vecteur $\sum_{g\in G} g(e_{i_1}) \wedge \cdots \wedge g(e_{i_k}) \in \bigwedge^k(V)$ est clairement fixe par G, donc la question b) assure que $\sum_{g\in G} g(e_{i_1}) \wedge \cdots \wedge g(e_{i_k}) = 0$, donc finalement

$$S(e) = |G| \det(A) \cdot e\,,$$

i.e.

$$\sum_{g\in G} \det(A - g) = |G| \det(A)\,.$$

De même, on obtient avec un raisonnement exactement similaire que

$$\left(\sum_{g\in G} \bigwedge{}^n (\mathrm{Id} - Ag)\right)(e) = \sum_{g\in G} e = |G| \cdot e\,,$$

puisque tous les termes restants sont nuls pour la même raison que plus haut. On en déduit donc que

$$\sum_{g\in G} \det(\mathrm{Id} - Ag) = |G|\,.$$

d) Soit $A \in \mathrm{End}(V)$. La seconde formule de la question c) assure qu'il existe $g \in G$ tel que $\det(\mathrm{Id} - Ag) \neq 0$. Donc $\mathrm{Id} - Ag$ est inversible, donc Ag n'a pas de point fixe non nul dans V.

Exercice 14 : $\star\star\star$

Soient p un nombre premier impair, $r \geq 1$ et $q = p^r$.

a) On note $V_1, V_2 := (\mathbb{F}_{q^2})^2$, et (e_i, f_i) la base canonique de V_i. On munit $V := V_1 \otimes_{\mathbb{F}_{q^2}} V_2$ de la forme bilinéaire symétrique b définie par $b(v_1 \otimes v_2, v_1' \otimes v_2') := b_1(v_1, v_1')b_2(v_2, v_2')$, où b_i est la forme bilinéaire alternée sur V_i telle que $b_i((1,0),(0,1)) = 1$. On pose enfin

$$V' := \mathrm{Vect}_{\mathbb{F}_p}\{e_1 \otimes e_2, f_1 \otimes f_2, \lambda e_1 \otimes f_2 + \overline{\lambda} f_1 \otimes e_2 : \lambda \in \mathbb{F}_{q^2}\} \subset V\,.$$

i) Montrer que $\dim_{\mathbb{F}_p} V' = 4$.

ii) Construire un morphisme de groupes $\mathrm{SL}_2(\mathbb{F}_{q^2}) \to \mathrm{O}(V', b)$.

iii) En déduire un isomorphisme de groupes $\mathrm{P}\Omega_4^-(\mathbb{F}_q) \cong \mathrm{PSL}_2(\mathbb{F}_{q^2})$.

b) On note (e_i) la base canonique de $\mathbb{F}_q^4$ et on note $W := \bigwedge^2(\mathbb{F}_q^4)$.

i) Quelle est la dimension de W comme $\mathbb{F}_q$-espace vectoriel ?

ii) Montrer que W est muni d'une forme bilinéaire symétrique non dégénérée naturelle f telle que pour tout $\sigma : \{1,2,3,4\} \to \{1,2,3,4\}$, $f(e_{\sigma(1)} \wedge e_{\sigma(2)}, e_{\sigma(3)} \wedge e_{\sigma(4)}) = \varepsilon(\sigma)$, avec par convention $\varepsilon(\sigma) = 0$ si σ n'est pas bijective.

iii) Montrer que $\mathrm{GL}_4(\mathbb{F}_q)$ agit naturellement sur W.

iv) Construire un morphisme de groupes $\mathrm{SL}_4(\mathbb{F}_q) \to \mathrm{O}(W, f)$.

v) En déduire un isomorphisme $\mathrm{P}\Omega_6^+(\mathbb{F}_q) \cong \mathrm{PSL}_4(\mathbb{F}_q)$.

c) On note (e_1, e_2, e_3, e_4) une base orthonormée pour la forme sesquilinéaire naturelle sur $X := (\mathbb{F}_{q^2})^4$, et $X' \subset \bigwedge^2 X$ le sous-$\mathbb{F}_q$-espace vectoriel engendré par les vecteurs $\lambda e_{\sigma(1)} \wedge e_{\sigma(2)} + \overline{\lambda} e_{\sigma(3)} \wedge e_{\sigma(4)}$, pour tout $\sigma \in \mathfrak{A}_4$ et $\lambda \in \mathbb{F}_{q^2}$.

i) Montrer que $\dim_{\mathbb{F}_q} X' = 6$.

ii) Montrer que X' est muni d'une forme bilinéaire symétrique f telle que pour tout $\sigma \in \mathfrak{A}_4$, $\lambda, \mu \in \mathbb{F}_{q^2}$,

$$f(\lambda e_{\sigma(1)} \wedge e_{\sigma(2)} + \overline{\lambda} e_{\sigma(3)} \wedge e_{\sigma(4)}, \mu e_{\sigma(1)} \wedge e_{\sigma(2)} + \overline{\mu} e_{\sigma(3)} \wedge e_{\sigma(4)}) = \lambda\overline{\mu} + \overline{\lambda}\mu\,.$$

iii) Construire un morphisme de groupes $\mathrm{SU}_4(\mathbb{F}_{q^2}) \to \mathrm{O}(X', f)$.

iv) En déduire un isomorphisme de groupes $\mathrm{P}\Omega_6^-(\mathbb{F}_q) \cong \mathrm{PSU}_4(\mathbb{F}_{q^2})$.

Solution de l'exercice 14.

a) i) On fixe un élément $\varepsilon \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. On vérifie facilement que V' est un $\mathbb{F}_p$-espace vectoriel de dimension 4, dont une base est $e_1 \otimes e_2, f_1 \otimes f_2, e_1 \otimes f_2 + f_1 \otimes e_2, \varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2$.

ii) On considère la représentation de $\mathrm{SL}_2(\mathbb{F}_{q^2})$ sur V définie par l'action diagonale $g \cdot (v_1 \otimes v_2) := g(v_1) \otimes \overline{g}(v_2)$. Montrons que le sous-$\mathbb{F}_p$-espace vectoriel $V' \subset V$ est stable par cette action. Comme $\mathrm{SL}_2(\mathbb{F}_{q^2})$ est engendré par les transvections, il suffit de montrer que V' est stable par les transvections. Pour cela, il suffit de considérer l'élément $g = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$ (dans la base (e_i, f_i) de V_i), avec $\lambda \in \mathbb{F}_{q^2}$. On a alors

$$g \cdot (e_1 \wedge e_2) = (e_1 + \lambda f_1) \otimes (e_2 + \overline{\lambda} f_2) = e_1 \otimes e_2 + (\lambda f_1 \otimes e_2 + \overline{\lambda} e_1 \otimes f_2) + \lambda\overline{\lambda} f_1 \otimes f_2 \in V'$$

car $\lambda\overline{\lambda} \in \mathbb{F}_q$. De même,

$$g \cdot (f_1 \otimes f_2) = f_1 \otimes f_2 \in V'\,,$$

et

$$g \cdot (\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2) = (\varepsilon\lambda + \overline{\varepsilon}\overline{\lambda}) f_1 \otimes f_2 + (\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2) \in V'$$

car $\varepsilon\lambda + \overline{\varepsilon}\overline{\lambda} \in \mathbb{F}_q$.

Donc $V' \subset V$ est stable par $\mathrm{SL}_2(\mathbb{F}_{q^2})$. On a donc un morphisme de groupes naturel $\mathrm{SL}_2(\mathbb{F}_{q^2}) \to \mathrm{GL}(V')$.

Soit alors $g = \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_{q^2})$. Si on note q la forme quadratique associée à b, on a

$$q(g \cdot (e_1 \otimes e_2)) = q(e_1 \otimes e_2 + (\lambda f_1 \otimes e_2 + \overline{\lambda} e_1 \otimes f_2) + \lambda\overline{\lambda} f_1 \otimes f_2) = -2\lambda\overline{\lambda} + 2\lambda\overline{\lambda} = 0 = q(e_1 \otimes e_2)$$

et

$$q(g \cdot (f_1 \otimes f_2)) = q(f_1 \otimes f_2)$$

et

$$q(g \cdot (\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2)) = q((\varepsilon\lambda + \overline{\varepsilon}\overline{\lambda}) f_1 \otimes f_2 + (\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2)) = -2\varepsilon\overline{\varepsilon} = q(\varepsilon e_1 \otimes f_2 + \overline{\varepsilon} f_1 \otimes e_2)\,.$$

Cela assure que les éléments de $\mathrm{SL}_2(\mathbb{F}_{q^2})$ agissant sur V' préservent la forme b, donc le morphisme précédent est en fait un morphisme $\rho : \mathrm{SL}_2(\mathbb{F}_{q^2}) \to \mathrm{O}(V', b)$, comme souhaité.

iii) Un calcul simple assure que le noyau du morphisme ρ construit à la question précédente est $\{\pm I_2\}$. Le calcul du groupe dérivé de $\mathrm{SL}_2(\mathbb{F}_{q^2})$ assure que le morphisme ρ est à valeurs dans $\Omega(V',b)$. Donc ce morphisme induit un morphisme injectif $\overline{\rho} : \mathrm{PSL}_2(\mathbb{F}_{q^2}) \to \Omega(V',b)$. Un calcul de cardinaux assure alors que ce morphisme induit un isomorphisme $\mathrm{PSL}_2(\mathbb{F}_{q^2}) \xrightarrow{\sim} \mathrm{P}\Omega(V',b)$. Enfin, on vérifie facilement que la forme bilinéaire symétrique b est de type $-$, et par conséquent le groupe $\mathrm{P}\Omega(V',b)$ s'identifie au groupe $\mathrm{P}\Omega_4^+(\mathbb{F}_q)$, ce qui conclut la preuve.

b) i) On sait que W est de dimension $\binom{4}{2} = 6$ sur $\mathbb{F}_p$.

ii) On définit la forme f sur la base $(e_i \wedge e_j)_{i<j}$ de W, de la façon suivante : on pose $f(e_i \wedge e_j, e_k \wedge e_k) := 1$ si la permutation $(i\,j\,k\,l)$ est paire, $f(e_i \wedge e_j, e_k \wedge e_k) := -1$ si cette permutation est impaire, et $f(e_i \wedge e_j, e_k \wedge e_k) := 0$ sinon. Il est clair que cela définit une forme bilinéaire symétrique non dégénérée vérifiant la propriété souhaitée.

iii) Il suffit de considérer l'action diagonale de $\mathrm{GL}_4(\mathbb{F}_q)$ sur W donnée par $g \cdot (x \wedge y) := g(x) \wedge g(y)$.

iv) On a construit à la question précédente un morphisme de groupes $\mathrm{SL}_4(\mathbb{F}_q) \to \mathrm{GL}(W)$. Montrons que les éléments de $\mathrm{SL}_4(\mathbb{F}_q)$ agissant sur W préservent la forme bilinéaire f. Pour cela, on considère la transvection $g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \lambda & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{SL}_4(\mathbb{F}_q)$. On a alors $g \cdot (e_1 \wedge e_3) = e_1 \wedge e_3 + \lambda e_2 \wedge e_3$ et $g \cdot (e_1 \wedge e_4) = e_1 \wedge e_4 + \lambda e_2 \wedge e_4$, et $g \cdot (e_i \wedge e_j) = e_i \wedge e_j$ sinon. Par conséquent, un calcul simple assure que l'on a $f(g \cdot (e_1 \wedge e_3), g \cdot (e_1 \wedge e_4)) = f(e_1 \wedge e_3 + \lambda e_2 \wedge e_3, e_1 \wedge e_4 + \lambda e_2 \wedge e_4) = \lambda - \lambda = 0 = f(e_1 \wedge e_3, e_1 \wedge e_4)$, et de même, pour tout i,j,k,l, on a $f(g \cdot (e_i \wedge e_j), g \cdot (e_k \wedge e_l)) = f(e_i \wedge e_j, e_k \wedge e_l)$. Comme les transvections engendrent $\mathrm{SL}_4(\mathbb{F}_q)$, on en déduit que l'action de $\mathrm{SL}_4(\mathbb{F}_q)$ sur W préserve la forme bilinéaire f. Par conséquent, l'action de la question précédente induit un morphisme naturel

$$\rho : \mathrm{SL}_4(\mathbb{F}_q) \to \mathrm{O}(W,f)\,.$$

v) On vérifie que $\mathrm{Ker}(\rho) = \{\pm I_4\}$, que la forme quadratique associée à f est de type $+$, et alors le calcul du groupe dérivé de $\mathrm{SL}_4(\mathbb{F}_q)$ assure que le morphisme ρ induit un morphisme de groupes injectif

$$\overline{\rho} : \mathrm{PSL}_4(\mathbb{F}_q) \to \mathrm{P}\Omega(W,f) \cong \mathrm{P}\Omega_6^+(\mathbb{F}_q)\,.$$

Un argument de cardinalité assure alors que ce morphisme est un isomorphisme.

c) i) On note ε un élément fixé de $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. On vérifie qu'une base de X' est donnée les vecteurs

$$e_1 \wedge e_2 + e_3 \wedge e_4\,,\ e_1 \wedge e_3 + e_4 \wedge e_2\,,\ e_1 \wedge e_4 + e_2 \wedge e_3\,,\ \varepsilon e_1 \wedge e_2 + \overline{\varepsilon} e_3 \wedge e_4\,,\ \varepsilon e_1 \wedge e_2 + \overline{\varepsilon} e_3 \wedge e_4\,,\ \varepsilon e_1 \wedge e_2 + \overline{\varepsilon} e_3 \wedge e_4\,.$$

Par conséquent, $\dim_{\mathbb{F}_q} X' = 6$.

ii) On introduit la forme f comme la somme orthogonale des trois formes naturelles suivantes définies sur les trois $\mathbb{F}_q$-plans en somme directe $\{\lambda e_i \wedge e_j + \overline{\lambda} e_k \wedge e_l : \lambda \in \mathbb{F}_{q^2}\}$ (pour $(i,j,k,l) = (1,2,3,4)$, $(1,3,4,2)$ et $(1,4,2,3)$), par les formules suivantes

$$f(\lambda e_i \wedge e_j + \overline{\lambda} e_k \wedge e_l, \mu e_i \wedge e_j + \overline{\mu} e_k \wedge e_l) := \lambda\overline{\mu} + \overline{\lambda}\mu\,.$$

Remarquons que la restriction de f à chacun de ces trois plans (deux-à-eux orthogonaux) est une forme quadratique non dégénérée de type $-$, donc f est une forme quadratique non dégénérée de type $-$ sur X'.

iii) On dispose de l'action naturelle de $\mathrm{SU}_4(\mathbb{F}_{q^2})$ sur $\bigwedge^2 X$ définie par $g \cdot (x \wedge y) := g(x) \wedge g(y)$. Or on vérifie que $\mathrm{SU}_4(\mathbb{F}_{q^2})$ est engendré par les matrices de permutation des vecteurs e_i, ainsi que par les matrices correspondant aux applications définies par $e_1 \mapsto \alpha e_1 + \beta e_2$, $e_2 \mapsto -\overline{\beta} e_1 + \overline{\alpha} e_2$, avec $\alpha, \beta \in \mathbb{F}_{q^2}$ tels que $\alpha\overline{\alpha} + \beta\overline{\beta} = 1$. Or un calcul élémentaire assure que ces éléments de $\mathrm{SU}_4(\mathbb{F}_{q^2})$ préservent tous le sous-espace X' de $\bigwedge^2 X$, et qu'ils laissent également la forme quadratique f invariante. Par conséquent, l'action susmentionnée de $\mathrm{SU}_4(\mathbb{F}_{q^2})$ sur $\bigwedge^2 X$ induit un morphisme de groupes

$$\rho : \mathrm{SU}_4(\mathbb{F}_{q^2}) \to \mathrm{O}(X',f)\,.$$

iv) On voit que $\mathrm{Ker}(\rho) = \{\pm I_4\}$, et le calcul du sous-groupe dérivé de $\mathrm{SU}_4(\mathbb{F}_{q^2})$ assure que le morphisme ρ induit un morphisme de groupes injectif

$$\overline{\rho} : \mathrm{PSU}_4(\mathbb{F}_{q^2}) \to \mathrm{P}\Omega(X', f) \cong \mathrm{P}\Omega_6^-(\mathbb{F}_q)\,.$$

Un calcul de cardinaux assure alors que le morphisme $\overline{\rho}$ est un isomorphisme.

Exercice 15 : $\star\star\star$

Soit K un corps de caractéristique $\neq 2$, V un K-espace vectoriel de dimension n et q une forme quadratique sur V.

a) On note $I(q)$ l'idéal bilatère de $T(V)$ engendré par les éléments de la forme $v\otimes v - q(v)$ pour $v \in V$. On pose $C(q) := T(V)/I(q)$. Montrer que $C(q)$ est une K-algèbre, canoniquement isomorphe à $\bigwedge V$ comme K-espace vectoriel, et admettant une décomposition $C(q) = C(q)^+ \oplus C(q)^-$ définie par le degré des éléments de $T(V)$.

b) Vérifier $C(q)^+$ est une sous-algèbre de $C(q)$.

c) Montrer que $\dim_K C(q) = 2^n$ et donner une base de $C(q)$ comme K-espace vectoriel.

d) Montrer que V se plonge naturellement dans $C(q)$.

e) Calculer $C(q)$ lorsque $K = \mathbb{R}$, $\dim_{\mathbb{R}}(V) \leq 2$. Généraliser au cas où K est quelconque et $\dim_K(V) \leq 1$.

f) Calculer le centre de $C(q)$.

g) On note $\alpha := \mathrm{id}_{C(q)^+} \oplus -\mathrm{id}_{C(q)^-} \in \mathrm{GL}_K(C(q))$ et pour tout $x \in C(q)^\times$, $\rho_x \in \mathrm{End}_K(C(q))$ défini par $\rho_x : z \mapsto \alpha(x) z x^{-1}$. Montrer que cela définit un morphisme de groupes $\rho : C(q)^\times \to \mathrm{GL}_K(C(q))$.

h) On note $\Gamma(V,q) := \{x \in C(q)^\times : \rho_x(V) \subset V\}$. Montrer que $\Gamma(V,q)$ contient les vecteurs non isotropes de (V,q).

i) On suppose q non dégénérée. Montrer que $\mathrm{Ker}(\rho) = K^*$.

j) Montrer qu'il existe un unique $t \in \mathrm{GL}_K(C(q))$ tel que $t_{|V} = \mathrm{id}_V$ et $t(xy) = t(y)t(x)$ pour tout $x, y \in C(q)$.

k) Pour tout $x \in C(q)$, on pose $\overline{x} := t(\alpha(x))$. Montrer que la formule $N(x) := x\overline{x}$ définit une application $N : C(q) \to C(q)$ induisant un morphisme de groupes $N : \Gamma(V,q) \to K^*$.

l) On suppose q non dégénérée. Montrer que $\mathrm{Im}\,(\rho) = \mathrm{O}(V,q)$.

m) On suppose q non dégénérée. Montrer que l'on dispose d'un morphisme naturel $\theta : \mathrm{O}(V,q) \to K^*/(K^*)^2$.

n) On suppose q non dégénérée et isotrope. Montrer que $\theta : \mathrm{SO}(V,q) \to K^*/(K^*)^2$ est surjectif.

o) On suppose q non dégénérée. On note $\mathrm{Pin}(V,q) := \mathrm{Ker}(N) = \{g \in \Gamma(V,q) : N(g) = 1\}$ et $\mathrm{Spin}(V,q) := \{g \in \mathrm{Pin}(V,q) : \det(\rho(g)) = 1\}$. Montrer que l'on a des suites exactes de groupes :

$$1 \to \{\pm 1\} \to \mathrm{Pin}(V,q) \xrightarrow{\rho} \mathrm{O}(V,q) \xrightarrow{\theta} K^*/(K^*)^2$$

et

$$1 \to \{\pm 1\} \to \mathrm{Spin}(V,q) \xrightarrow{\rho} \mathrm{SO}(V,q) \xrightarrow{\theta} K^*/(K^*)^2\,.$$

p) On suppose $K = \mathbb{R}$ et q non dégénérée et non définie. Montrer que $\theta : \mathrm{SO}(V,q) \to K^*/(K^*)^2$ est surjective.

q) Montrer les isomorphismes suivants : $\mathrm{Spin}_2(\mathbb{C}) \cong \mathbb{C}^*$, $\mathrm{Spin}_3(\mathbb{C}) \cong \mathrm{SL}_2(\mathbb{C})$, $\mathrm{Spin}_4(\mathbb{C}) \cong \mathrm{SL}_2(\mathbb{C}) \times \mathrm{SL}_2(\mathbb{C})$, $\mathrm{Spin}_5(\mathbb{C}) \cong \mathrm{Sp}_4(\mathbb{C})$, $\mathrm{Spin}_6(\mathbb{C}) \cong \mathrm{SL}_4(\mathbb{C})$, ainsi que $\mathrm{Spin}_2(\mathbb{R}) \cong \mathrm{U}_1(\mathbb{C})$, $\mathrm{Spin}_3(\mathbb{R}) \cong \mathrm{SU}_2(\mathbb{C})$, $\mathrm{Spin}_4(\mathbb{R}) \cong \mathrm{SU}_2(\mathbb{C}) \times \mathrm{SU}_2(\mathbb{C})$.

Solution de l'exercice 15.

a) Il est clair que $C(q)$ est naturellement une K-algèbre. Remarquons que contrairement à $\bigwedge(V)$ ou $S(V)$, l'algèbre $C(q)$ n'est en général pas naturellement $\mathbb{Z}$-graduée, puisque l'idéal $I(q)$ n'est pas homogène. On peut écrire un isomorphisme canonique de K-espaces vectoriels $C(q) \xrightarrow{\sim} \bigwedge V$ en toute caractéristique, mais cela demande quelques vérifications un peu longues. On donnera une autre version de cet isomorphisme (moins canonique) à la question c). La K-algèbre $T(V)$ est munie d'une décomposition en somme directe $T(V) = T(V)^+ \oplus T(V)^-$, où $T(V)^+$ (resp. $T(V)^-$) est le sous-espace vectoriel formé des éléments de degré pair (resp. impair). Or l'idéal $I(q)$ est engendré par des éléments de degré pair, donc cet idéal admet lui aussi une décomposition $I(q) = I(q)^+ \oplus I(q)^-$, où $I(q)^\pm := I(q) \cap T(q)^\pm$. Il est alors clair que le quotient $C(q) = T(V)/I(q)$ admet lui aussi une décomposition (en somme directe de sous-K-espaces vectoriels) de la forme $C(q) = C(q)^+ \oplus C(q)^-$, où $C(q)^+$ (resp. $C(q)^-$) est l'image de $T(V)^+$ (resp. $T(V)^-$) dans $C(q)$.

b) Comme $T(V)^+$ est une sous-K-algèbre de $T(V)$, on en déduit immédiatement que $C(q)^+$ est une sous-K-algèbre de $C(q)$. Remarquons également que $C(q)^-$ n'est pas une sous-algèbre de $C(q)$, mais que $C(q)^-$ est stable par multiplication par un élément de $C(q)^+$. On dit que $C(q)$ est une K-algèbre $\mathbb{Z}/2\mathbb{Z}$-graduée.

c) Soit $e_1, \dots, e_n$ une base de V. Par définition de $C(q)$, on a la relation suivante : pour tous $v, w \in C(q)$, $v \cdot w + w \cdot v = 2b(v, w)$. Par conséquent, tout produit $e_{i_1} \cdot \dots \cdot e_{i_r}$ peut se réécrire sous la forme d'une combinaison linéaire de produits $e_{j_1} \cdot \dots \cdot e_{j_s}$ avec $j_1 < \dots < j_s$. On en déduit donc que la famille $(e_{i_1} \cdot \dots \cdot e_{i_r})_{1 \leq i_1 < \dots < i_r \leq n}$ est une famille génératrice de $C(q)$ comme K-espace vectoriel. Donc $\dim_K C(q) \leq 2^n$.

Montrons que c'est une égalité. Pour cela, on démontre le fait suivant : si (V, q) et (V', q') sont deux espaces quadratiques, alors on a un isomorphisme canonique de K-algèbres graduées $C(q \oplus^\perp q') = C(q) \otimes^{\mathrm{su}} C(q')$. En effet, on dispose d'une application linéaire $\varphi : V \oplus V' \to C(V) \otimes C(q')$ définie par $\varphi(v \oplus v') := v \otimes 1 + 1 \otimes v'$. Or on a la relations suivante : pour tout $(v, v') \in V \times V'$, on a $\varphi(v \oplus v')^2 = q(v) + q(v') = (q \oplus^\perp q')(v \oplus v')$, donc la définition de $C(q \oplus^\perp q')$ assure que l'application φ se prolonge en un morphisme de K-algèbres graduées

$$\overline{\varphi} : C(q \oplus^\perp q') \to C(q) \otimes C(q') .$$

Réciproquement, les inclusions de V et V' dans $V \oplus V'$ assurent l'existence de morphismes de K-algèbres graduées $C(q), C(q') \to C(q \oplus^\perp q')$, dont on déduit (ce qui demande un petit calcul) un morphisme de K algèbres graduées $\psi : C(q) \otimes^{\mathrm{su}} C(q') \to C(q \oplus^\perp q')$. Il est alors immédiat de constater que ψ est la réciproque de $\overline{\varphi}$, ce qui conclut la preuve du fait énoncé plus haut.

Remarquons au passage que pour la calcul de la dimension et d'une base (voir ci-dessous), on a seulement besoin de la surjectivité de $\overline{\varphi}$, laquelle est évidente puisque les éléments $x \otimes 1$ et $1 \otimes x$, avec $x \in V$, $x' \in V'$, engendrent $C(q) \otimes^{\mathrm{su}} C(q')$ comme K-algèbre, et ces éléments sont clairement dans l'image de $\overline{\varphi}$.

Pour finir le calcul de la dimension, on raisonne par récurrence sur la dimension n de V. Si $n = 1$, on a $v = K$ et $q(x) = ax^2$ pour un certain $a \in K$. Si $a = 0$, on a $C(q) = \bigwedge K = K \oplus K$ qui est bien de dimension 2, et si $a \neq 0$, on voit que $T(K) \cong K[X]$ et il est évident que $C(q)$ est l'idéal de $K[X]$ engendré par $(X^2 - a)$, donc $C(q) \cong K[X]/(X^2 - a)$, qui est bien de dimension 2 sur K. Si $n > 1$, on a de nouveau deux cas : soit $q = 0$ et $C(q) \cong \bigwedge V$, auquel cas $\dim_K C(q) = 2^n$, soit $q \neq 0$, il existe $v \in V$ tel que $q(v) \neq 0$, et $V = Kv \oplus^\perp (Kv)^\perp$, donc $C(q) \cong C(q_{|Kv}) \otimes C(q_{|(Kv)^\perp})$, et l'hypothèse de récurrence assure que $\dim_K C(q) = 2.2^{n-1} = 2^n$.

Finalement, $\dim_K C(q) = 2^n$, et la famille génératrice précédente formée des $(e_{i_1} \cdot \dots \cdot e_{i_r})_{1 \leq i_1 < \dots < i_r \leq n}$ est bien une base de $C(q)$.

Remarque : il est désormais facile d'exhiber un isomorphisme de K-espaces vectoriels entre $C(q)$ et $\bigwedge V$: il suffit de faire correspondre la base $(e_{i_1} \wedge \dots \wedge e_{i_r})$ de $\bigwedge V$ avec la base $(e_{i_1} \cdot \dots \cdot e_{i_r})$ de $C(q)$...

d) On dispose du morphisme naturel $V \to T(V) \to C(q)$. On a montré à la question précédente que si (e_i) est une base de V, alors les images des vecteurs e_i dans $C(q)$ forment une famille libre. Cela assure que le morphisme naturel $V \to C(q)$ est bien injectif.

e) — On suppose d'abord $K = \mathbb{R}$. Si $n = 0$, il est clair que $C(q) \cong \mathbb{R}$. Si $n = 1$, on a montré à la question précédente que deux cas se présentaient : soit $q = 0$, et $C(q) \cong \bigwedge \mathbb{R} \cong K[X]/(X^2)$, soit $q \neq 0$ (disons $q(x) = ax^2$) et $C(q) \cong \mathbb{R}[X]/(X^2 - a)$; dans ce dernier cas, on a deux possibilités : si $a > 0$, alors $C(q) \cong \mathbb{R}^2$, et si $a > 0$, $C(q) \cong \mathbb{C}$. Enfin, si $n = 2$, limitons-nous aux formes quadratiques non dégénérées : il y a trois cas (trois signatures possibles). Si $\mathrm{sign}(q) = (2, 0)$, alors $C(q) \cong \mathrm{Mat}_2(\mathbb{R})$. Si $\mathrm{sign}(q) = (1, 1)$, alors $C(q) \cong \mathrm{Mat}_2(\mathbb{R})$. Si $\mathrm{sign}(q) = (0, 2)$, alors $C(q) \cong \mathbf{H}$, où $\mathbf{H}$ est l'algèbre des quaternions de Hamilton.
— Désormais, K est un corps quelconque. Si $n = 0$, on a $C(q) \cong K$. Si $n = 1$, on a trois possibilités : si on note $q(x) = ax^2$, soit $a = 0$ et alors $C(q) \cong \bigwedge K \cong K[X]/(X^2)$, soit $a \in (K^*)^2$ et alors $C(q) \cong K^2$, soit $a \notin (K^*)^2$ et alors $C(q) \cong K[X]/(X^2 - a) \cong K(\sqrt{(a)})$ est un corps qui est une extension quadratique de K.

f) On note $Z(q)$ le centre de l'algèbre $C(q)$. On fixe une base orthogonale (e_i) de V. Pour toute partie $I = \{i_1, \ldots, i_r\} \subset \{1, \ldots, n\}$, avec $i_1 < \cdots < i_r$, on note $e_I := e_{i_1} \cdot \cdots \cdot e_{i_r}$. Alors pour tout tel I et tout $j \in \{1, \ldots, n\}$, on a

$$e_I \cdot e_j = \varepsilon_{I,j} e_j \cdot e_I \,,$$

où $\varepsilon_{I,j} := (-1)^{|I|}$ si $j \notin I$ et $\varepsilon_{I,j} := -(-1)^{|I|}$ si $j \in I$. Soit alors $x = \sum_I x_I e_I \in C(q)$. On a clairement $a \in Z(q)$ si et seulement si $e_j \cdot x = x \cdot e_j$ pour tout $1 \leq j \leq n$. Soit alors $j \in \{1, \ldots, n\}$. En utilisant les relations de commutation susmentionnées, on obtient la caractérisation suivante : $x \cdot e_j = e_j \cdot x$ si et seulement si $x_I = 0$ pour tout I tel que ($|I|$ est pair et $j \in I$) ou ($|I|$ est impair et $j \notin I$). En faisant varier j dans $\{1, \ldots, n\}$, on en déduit la dichotomie suivante :
— si n est pair : $x \in Z(q)$ si et seulement si $x_I = 0$ pour tout $I \neq \emptyset$. Donc $Z(q) = Ke_\emptyset \cong K$.
— si n est impair : $x \in Z(q)$ si et seulement si $x_I = 0$ pour tout $I \neq \emptyset$ et $I \neq \{1, \ldots, n\}$. Donc $Z(q) = Ke_\emptyset \oplus Ke_{\{1,\ldots,n\}} \cong K^2$.

g) Tout d'abord, pour tout $x \in C(q)^\times$, l'application $\rho_x : C(q) \to C(q)$ est bien linéaire, et elle est inversible d'inverse $\rho_{x^{-1}}$. Donc $x \mapsto \rho_x$ définit bien une application $\rho : C(q)^\times \to \mathrm{GL}_K(C(q))$. On voit facilement que c'est un morphisme de groupes en montrant que pour tout $x, y \in C(q)$, on a $\alpha(x \cdot y) = \alpha(x) \cdot \alpha(y)$.

h) Voir cours, proposition III.6.4.

i) Voir cours, proposition III.6.5.

j) On définit $C'(q)$ comme la K-algèbre opposée à $C(q) : C'(q) = C(q)$ comme K-espace vectoriel, et la multiplication $\cdot'$ sur $C'(q)$ est définie par $a \cdot' b := b \cdot a$. Alors l'application naturelle $i : V \to C'(q)$ est une application linéaire telle que $i(x)^2 = q(x)$, donc par définition de $C(q)$, l'application i se prolonge en un morphisme de K-algèbres $i : C(q) \to C'(q)$ En composant ce morphisme avec l'identification $C'(q) \xrightarrow{\sim} C(q)$, on obtient une application linéaire $t : C(q) \to C(q)$ telle que $t_{|V} = \mathrm{id}_V$ et $t(x \cdot y)t(y) \cdot t(x)$. L'unicité de t résulte de la propriété universelle de $C(q)$ qui découle de sa définition. Et l'unicité implique que t est une involution.

k) voir cours, proposition III.6.6.

l) voir cours, proposition III.6.7.

m) voir cours, proposition III.6.8.

n) La forme q étant non dégénérée et isotrope, elle représente tous les éléments de K, i.e. l'application $q : V \to K$ est surjective. Par conséquent, soit $\lambda \in K^*$, il existe $v \in V$ tel que $q(v) = -\lambda$. Alors la question h) assure que $v \in \Gamma(V, q)$, et la définition de N assure que $N(v) = v \cdot (-v) = -q(v) = \lambda$. Mais $\rho(v)$ est une reflexion, donc $\rho(v) \in \mathrm{O}(V, q) \setminus \mathrm{SO}(V, q)$. Il suffit de multiplier v par un vecteur $v' \in V$ tel que $q(v') = -1$ (qui existe) pour obtenir un élément $x := v \cdot v' \in \Gamma(V, q)$ tel que $N(x) = \lambda$ et $\det(\rho(x)) = \det(\rho(v)) \det(\rho(v')) = (-1)(-1) = 1$, donc l'élément $\rho(x) \in \mathrm{SO}(V, q)$ vérifie que $\theta(\rho(x))$ est la classe de $N(x) = \lambda$ dans $K^*/(K^*)^2$. D'où la surjectivité souhaitée.

o) Le morphisme $\mathrm{Pin}(V, q) \to \mathrm{O}(V, q)$ est la composée de l'inclusion $\mathrm{Pin}(V, q) \subset \Gamma(V, q)$ avec le morphisme $\rho : \Gamma(V, q) \to \mathrm{O}(V, q)$. Par conséquent, le noyau de $\mathrm{Pin}(V, q) \to \mathrm{O}(V, q)$ est exactement

$$\mathrm{Ker}(\rho) \cap \mathrm{Pin}(V, q) = X^* \cap \mathrm{Pin}(V, q) = \{x \in K^* : N(x) = 1\} = \{x \in K^* : x^2 = 1\} = \{\pm 1\} \,.$$

Cela assure que la suite suivante (dont les morphismes sont les morphismes naturels)

$$1 \to \{\pm 1\} \to \mathrm{Pin}(V,q) \xrightarrow{\rho} \mathrm{O}(V,q)$$

est exacte. En outre, soit $y \in \mathrm{Ker}(\theta : \mathrm{O}(V,q) \to K^*/(K^*)^2)$: par surjectivité de ρ (voir question k)), il existe $x \in \Gamma(V,q)$ tel que $\rho(x) = y$. Alors par construction de θ (voir question m)), on a $\theta(y) = N(x) \bmod (K^*)^2$. Comme $\theta(y) = 1 \in K^*/(K^*)^2$, il existe $t \in K^*$ tel que $N(x) = t^2$. Alors on a $\rho(t^{-1}x) = \rho(x) = y$ car $K^* = \mathrm{Ker}(\rho)$ et $N(t^{-1}x) = 1 \in K^*$, donc $t^{-1}x \in \mathrm{Pin}(V,q)$. On a donc montré que $y = \rho(t^{-1}x) \in \rho(\mathrm{Pin}(V,q))$, donc $\mathrm{Ker}(\theta) \subset \rho(\mathrm{Pin}(V,q))$. L'inclusion inverse étant évidente, cela termine la preuve de l'exactitude de la suite

$$1 \to \{\pm 1\} \to \mathrm{Pin}(V,q) \xrightarrow{\rho} \mathrm{O}(V,q) \xrightarrow{\theta} K^*/(K^*)^2 \,.$$

La seconde suite exacte se déduit immédiatement de celle-ci, en remarquant que $\mathrm{Spin}(V,q) = \mathrm{Pin}(V,q) \cap \rho^{-1}(\mathrm{SO}(V,q))$.

p) C'est une conséquence directe de la question n).

q) Les détails sont laissés au lecteur courageux...

TD11 : Représentations des groupes finis I

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆
Montrer que tout groupe fini G admet une représentation fidèle sur tout corps K.

Solution de l'exercice 1. La représentation régulière de G sur K répond à la question.
De façon équivalence, le théorème de Cayley assure que G se plonge dans le groupe des permutations de G, et ce dernier groupe se plonge dans un groupe linéaire via les matrices de permutation.

Exercice 2 : ⋆
Soit G un groupe fini, soit H un sous-groupe distingué dans G, notons $\pi : G \to G/H$ la projection canonique. Soit ρ une représentation complexe de G/H.

a) Montrer que $\rho \circ \pi$ est une représentation de G.

b) Montrer que ρ est irréductible si et seulement si $\rho \circ \pi$ est irréductible.

Solution de l'exercice 2.

a) C'est évident : la composée de deux morphismes de groupes est un morphisme de groupes.

b) Plus généralement, si $f : G \to G'$ est un morphisme de groupe, et ρ une représentation de G', on a toujours l'implication suivante : si $\rho \circ f$ est irréductible (comme représentation de G), alors ρ est irréductible. En effet, tout sous-espace stable par G' est stable par G puisque l'action de G se factorise par G'. En revanche, la réciproque est fausse en général si f n'est pas surjective (prendre pour G le groupe trivial, pour G' un groupe non abélien et pour ρ une représentation irréductible de dimension ≥ 2).

   Dans la situation de l'exercice, en revanche, le morphisme π est surjectif. Montrons le sens réciproque : on suppose ρ irréductible. Soit W un sous-espace strict stable par G. Pour tout $x \in G/H$, il existe $g \in G$ tel que $\pi(g) = x$. Comme W est stable par g, il est stable par x, donc W est stable par tout élément de G/H. Comme ρ est irréductible, $W = 0$, donc $\rho \circ \pi$ est irréductible.

Exercice 3 : ⋆
Soit V un $\mathbb{C}$-espace vectoriel, soit G un groupe et soit (V, ρ) une représentation de G. On suppose qu'il existe $v \in V$ tel que $\{\rho(g)v \mid g \in G\}$ forme une base de V. Montrer que (V, ρ) est isomorphe à la représentation régulière de G.

Solution de l'exercice 3. Soit W un espace vectoriel de base $\{e_g\}_{g \in G}$ (par exemple, $W = K^G$ et e_g est l'indicatrice de g). Rappelons que la représentation regulière ρ_R de G opère sur W par $\rho_R(h)e_g = e_{hg}$. Considérons l'application linéaire ϕ définie sur la base (e_g) par :

$$\begin{array}{rccc} \phi : W & \longrightarrow & V \\ e_g & \mapsto & \rho(g)v \end{array}$$

Comme $(\rho(g)v)_{g \in G}$ est une base de V, ϕ est un isomorphisme de K-espaces vectoriels, et par définition, ϕ est G-équivariant, donc ϕ est un isomophisme entre ρ et ρ_R.

Exercice 4 : ⋆⋆
Soit V une représentation complexe d'un groupe fini G. On note S la représentation $S^2(V)$ et A la représentation $\bigwedge^2 V$.

a) Calculer les caractères χ_S et χ_A de S et de A en fonction du caractère χ_V de V.

b) Calculer $\chi_{V\otimes V}$ en fonction de χ_A et χ_S.

Solution de l'exercice 4.

a) Soit $g \in G$. Il existe une base $(e_i)_{i\leq i\leq n}$ de V formée de vecteurs propres de g. Pour tout i, on note λ_i la valeur propre correspondant à e_i. Alors par définition, on a $\chi_V(g) = \sum_i \lambda_i$.
Or $S^2(V)$ admet comme base $(e_i \cdot e_j)_{1\leq i\leq j\leq n}$, et pour tout $i \leq j$, $g(e_i \cdot e_j) = \lambda_i\lambda_j e_i \cdot e_j$, donc les vecteurs de cette base sont des vecteurs propres pour g, ce qui assure que $\chi_S(g) = \sum_{i\leq j} \lambda_i\lambda_j$. Donc

$$\chi_S(s) = \frac{1}{2}\left(\left(\sum_i \lambda_i\right)^2 + \sum_i \lambda_i^2\right) = \frac{\chi_V(g)^2 - \chi_V(g^2)}{2}\,.$$

De même, $\bigwedge^2(V)$ admet comme base $(e_i \wedge e_j)_{1\leq i<j\leq n}$, et pour tout $i < j$, $g(e_i \wedge e_j) = \lambda_i\lambda_j e_i \wedge e_j$, donc les vecteurs de cette base sont des vecteurs propres pour g, ce qui assure que $\chi_A(g) = \sum_{i<j} \lambda_i\lambda_j$. Donc

$$\chi_A(s) = \frac{1}{2}\left(\left(\sum_i \lambda_i\right)^2 - \sum_i \lambda_i^2\right) = \frac{\chi_V(g)^2 - \chi_V(g^2)}{2}\,.$$

Donc finalement, on a

$$\chi_S = \frac{\chi_V^2 + \chi_V(.^2)}{2}$$

et

$$\chi_A = \frac{\chi_V^2 - \chi_V(.^2)}{2}\,.$$

b) On sait que l'on a un isomorphisme de représentations $V \otimes V \simeq S^2(V) \otimes \bigwedge^2(V)$, ce qui assure que

$$\chi_{V\otimes V} = \chi_S + \chi_A\,.$$

Remarque : En combinant a) et b), on retrouve bien la formule $\chi_{V\otimes V} = \chi_V^2$.

Exercice 5 : $\star\star$
Soit $G = \mathfrak{S}_3$ et soit V un $\mathbb{C}$-espace vectoriel possédant une base indexée par les éléments de G. On considère l'application $T : G \to \mathrm{GL}(V)$ définie par $T(g)e_\tau = e_{g\tau g^{-1}}$.

a) Montrer que T est une représentation de G.

b) Soit j une racine cubique primitive de 1. Soit W le sous-espace de V dont une base est

$$\alpha = e_{(1,2)} + je_{(1,3)} + j^2 e_{(2,3)}, \qquad \beta = e_{(1,2)} + j^2 e_{(1,3)} + je_{(2,3)}.$$

Montrer que W est une sous-G-représentation de V. Est-ce que W est irréductible ?

c) Déterminer la décomposition de V en somme directe de sous-espaces irréductibles et expliciter l'action de G sur chacun de ces sous-espaces.

d) Soit U une représentation irréductible de $\mathfrak{S}_3$ de dimension 2. Décomposer $U \otimes U$, $S^2(U)$ et $\bigwedge U$ en somme de représentations irrédutibles.

Solution de l'exercice 5.

a) C'est évident.

b) Le groupe $\mathfrak{S}_3$ est engendré par $(1,2)$ et $(1,2,3)$. Il suffit donc de montrer que l'espace engendré par α et β est stable par $T((1,2))$ et $T((1,2,3))$. Un simple calcul donne $T((1,2))(\alpha) = \beta$, $T((1,2))(\beta) = \alpha$, $T((1,2,3))(\alpha) = j\alpha$ et $T((1,2,3))(\beta) = j^2\beta$. Un simple calcul montre qu'aucun sous-module de W de dimension 1 n'est stable par $\mathfrak{S}_3$ et donc W est irréductible.

c) Remarquons que si C est une classe de conjugaison dans $\mathfrak{S}_3$, alors $\sum_{g\in C} e_g$ est stable par T. On trouve ainsi trois sous-espaces stables sous $\mathfrak{S}_3$, à savoir les trois droites :

$$W_1 = \mathbb{C}_{\mathrm{Id}}, \qquad W_2 = \mathbb{C}(e_{(1,2)} + e_{(1,3)} + e_{(2,3)}), \qquad W_3 = \mathbb{C}(e_{(1,2,3)} + e_{(1,3,2)})\,.$$

Enfin, si on note ε la signature, on obtient :

$$T(g)(e_{(1,2,3)} - e_{(1,3,2)}) = \varepsilon(g)(e_{(1,2,3)} - e_{(1,3,2)})$$

(il suffit de le vérifier pour $(1,2)$ et $(1,2,3)$). Donc l'espace $W_4 = \mathbb{C}(e_{(1,2,3)} - e_{(1,3,2)})$ est stable par $\mathfrak{S}_3$. On a finalement :

$$V = W_1 \oplus W_2 \oplus W_3 \oplus W_4 \oplus W\,.$$

La représentation triviale apparaît trois fois dans cette décomposition (W_1, W_2 et W_3), la signature une fois (W_4) et l'unique représentation irréductible de dimension 2 une fois (W).

d) On sait que U est isomorphe à W. Une base de l'espace de dimension 4 $W \otimes W$ est donnée par $\alpha\otimes\alpha$, $\alpha\otimes\beta$, $\beta\otimes\alpha$ et $\beta\otimes\beta$. Or les calculs de la question b) assurent que $W_1 := \mathbb{C}(\alpha\otimes\beta+\beta\otimes\alpha)$ est une sous-représentation triviale, $W_2 := \mathbb{C}(\alpha\otimes\beta-\beta\otimes\alpha)$ est une sous-représentation donnée par la signature, et $W_3 := \mathrm{vect}(\alpha\otimes\alpha, \beta\otimes\beta)$ est une sous-représentation irréductible de dimension deux isomorphe à $U \cong W$. Donc $U \otimes U \simeq W_1 \oplus W_2 \oplus W_3$, avec W_1 triviale, W_2 la signature et $W_3 = U$. De même, $S^2(U)$ admet pour base $\alpha\cdot\alpha$, $\alpha\cdot\beta$ et $\beta\cdot\beta$, donc on voit que $S^2(U) = W_1 \oplus W$ avec les notations précédentes. Enfin, on a des ismomorphismes évidents de représentations $\bigwedge U = \bigwedge^0 U \oplus \bigwedge^1 U \oplus \bigwedge^2 U \simeq W_1 \oplus U \oplus \bigwedge^2 U$, or $\bigwedge^2 U$ est un K-espace vectoriel de dimension 1 de base $\alpha \wedge \beta$, donc c'est la représentation signature W_2.

Exercice 6 :
Soit p un nombre premier et soit K un corps algébriquement clos de caractéristique différente de p. Soit G un p-groupe. Montrer que G possède une représentation non triviale de dimension 1 sur K.

Solution de l'exercice 6. On sait que G admet un sous-groupe distingué H d'indice p. Donc $G/H \simeq \mathbb{Z}/p\mathbb{Z}$. Puisque K est algébriquement clos de caractéristique $\neq p$, le polynôme $X^p - 1$ est scindé à racines simples, donc les racines p-ièmes de l'unité dans K^* forment un sous-groupe cyclique d'ordre p, isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On obtient donc une injection de $\mathbb{Z}/p\mathbb{Z}$ dans K^*. Le morphisme composé $G \mapsto G/H \cong \mathbb{Z}/p\mathbb{Z} \mapsto K^*$ est donc un caractère non trivial de G, i.e. une représentation non triviale de dimension 1 de G sur K.

Exercice 7 :
Soit G un groupe fini et soit χ un caractère de G vérifiant

$$\forall g \in G \qquad g \neq 1 \Rightarrow \chi(g) = 0.$$

Montrer que χ est un multiple entier du caractère de la représentation régulière de G.

Solution de l'exercice 7. Il suffit de montrer que $|G|$ divise $\chi(1)$. On calcule $\langle \mathrm{triv}, \chi\rangle$, où triv désigne la représentation triviale de G. On a que $\langle \mathrm{triv}, \chi\rangle = \chi(1)/|G|$ et donc $|G|$ divise $\chi(1)$.

Exercice 8 :

a) Soit A un groupe fini abélien et χ un caractère de A sur $\mathbb{C}$. Montrer

$$\sum_{a\in A} |\chi(a)|^2 \geq |A| \cdot \chi(1).$$

b) Soit G un groupe fini et soit A un sous-groupe abélien de G d'indice $n \geq 1$. Montrer que si χ est un caractère irréductible de G, on a $\chi(1) \leq n$. Que peut-on dire si $\chi(1) = n$?

Solution de l'exercice 8.

a) On décompose le caractère χ en somme de caractères irréductibles : $\chi = \sum_i a_i\chi_i$. Il faut donc montrer que $\sum_i a_i^2 \geq \sum_i a_i$ ce qui est vrai car $a_i \in \mathbb{N}$ pour tout i.

b) Notons ψ la restriction du caractère χ à A. D'après a), on a $\sum_{x\in A}|\psi(x)|^2 \geq |A|\psi(1) = |A|\chi(1)$. D'autre part, puisque χ est irréductible, on a $\sum_{g\in G}|\chi(g)|^2 = |G|$. On a donc $|G| \geq \sum_{x\in A}|\chi(x)|^2 = |A|\chi(1)$, d'où $\chi(1) \leq n$.
Si $\chi(1) = n$, alors $\sum_{x\in G\setminus A}|\chi(x)|^2 = 0$, c'est-à-dire $\chi(x) = 0$ pour tout $x \in G \setminus A$.

Exercice 9 : $\star\star$

Soit G un groupe fini et soient ϕ et ψ des caractères de G dans $\mathbb{C}$.

a) Montrer que si ψ est de degré 1, $\phi\psi$ est irréductible si et seulement si ϕ est irréductible.

b) Montrer que si ψ est de degré strictement supérieur à 1, le caractère $\psi\bar{\psi}$ n'est pas irréductible.

c) Soit ϕ un caractère irréductible de G. On suppose que ϕ est le seul caractère irréductible de son degré. Montrer que s'il existe un caractère ψ de degré 1 et $g \in G$ tel que $\psi(g) \neq 1$, alors $\phi(g) = 0$.

Solution de l'exercice 9.

a) Calculons le produit scalaire : $\langle\phi\psi, \phi\psi\rangle = \frac{1}{|G|}\sum_{g\in G}\phi(g)\psi(g)\overline{\phi(g)\psi(g)}$. Puisque ψ est de degré 1, on a $\psi(g)\overline{\psi(g)} = 1$ pour tout $g \in G$. On a donc que $\langle\phi\psi, \phi\psi\rangle = \langle\phi, \phi\rangle$, et donc $\phi\psi$ est irréductible si et seulement si ϕ est irréductible.

b) On a $\langle\text{triv}, \psi\overline{\psi}\rangle = \langle\psi, \psi\rangle$. Si ψ est non irréductible, alors $\langle\psi, \psi\rangle > 1$ et donc triv apparaît dans $\psi\overline{\psi}$ avec multiplicité ≥ 2, donc $\psi\overline{\psi}$ est réductible. Si ψ est irréductible, alors $\langle\text{triv}, \psi\overline{\psi}\rangle = 1$, et donc $\psi\overline{\psi}$ est irréductible si et seulement si $\psi\overline{\psi} = \text{triv}$. Mais cela n'est pas possible car $\psi\overline{\psi}(1) > 1$ parce que ψ est de degré ≥ 2 et $\text{triv}(1) = 1$.

c) D'après a), $\phi\psi$ est irréductible, et donc par hypothèse, $\phi\psi = \phi$, d'où le résultat.

Exercice 10 : $\star\star$

a) Établir la table de caractère de D_4.

b) Établir la table de caractère de $\mathbf{H}_8$.

c) Que peut-on en conclure ?

Solution de l'exercice 10.

a) Voir cours.

b) On note $G = \mathbf{H}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. On vérifie que G admet cinq classes de conjugaison, à savoir $\{1\}$, $\{-1\}$, $\{\pm i\}$, $\{\pm j\}$, $\{\pm k\}$. On a $D(G) = \{\pm 1\}$, donc $G/D(G) = \langle\bar{i}, \bar{j} : \bar{i}^2 = \bar{j}^2 = 1, \bar{i}\bar{j} = \bar{j}\bar{i}\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Donc G admet quatre représentations de dimension 1 correspondant aux quatre morphismes de groupes $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{C}^*$. On en déduit que la cinquième représentation irréductible de G est de dimension 2. Et son caractère se déduit des quatre caractères précédents par orthogonalité. On obtient la table de caractères suivante :

$\mathbf{H}_8$	1	1	2	2	2
	$\{1\}$	$\{-1\}$	$\{\pm i\}$	$\{\pm j\}$	$\{\pm k\}$
χ_{triv}	1	1	1	1	1
χ_1	1	1	-1	1	-1
χ_2	1	1	1	-1	-1
$\chi_3 = \chi_1\chi_2$	1	1	-1	-1	1
χ_ρ	2	-2	0	0	0

C'est donc exactement la même table de caractères que D_4.

c) Ces exemples assurent que la table de caractères ne détermine pas la classe d'isomorphisme d'un groupe fini.

Remarque : la représentation irréductible de dimension 2 de D_4 est définie sur $\mathbb{R}$, alors que $\mathbf{H}_8$ n'admet pas de représentation irréductible de dimension 2 sur $\mathbb{R}$.

Exercice 11 :

a) En considérant la représentation naturelle de $\mathfrak{S}_4$ sur un $\mathbb{C}$-espace vectoriel de dimension 4, construire une (sous-)représentation irréductible de dimension 3, de caractère valant $(3, 1, 0, -1, -1)$ sur les différentes classes de conjugaisons.

b) Dresser les tables de caractères de $\mathfrak{S}_4$ et $\mathfrak{A}_4$ et interpréter géométriquement certaines représentations obtenues.

c) Dresser les tables de caractères de $\mathfrak{S}_5$ et $\mathfrak{A}_5$ et interpréter géométriquement certaines représentations obtenues.

Solution de l'exercice 11.

a) Voir cours.

b) — La table de caractères de $\mathfrak{S}_4$ est dans le cours. Avec les notations du cours, les deux représentations V_0 et $V_0 \otimes \mathrm{sign}$ irréductibles de dimension 3 correspondent aux l'actions de $\mathfrak{S}_4$ sur $\mathbb{R}^3$ définies respectivement par l'isomorphisme $\mathfrak{S}_4 \xleftarrow{\sim} \mathrm{Isom}^+(\mathrm{Cube}) \subset \mathrm{GL}_3(\mathbb{R})$ (une isométrie directe du cube permute les quatre grandes diagonales dudit cube) et par l'isomorphisme $\mathfrak{S}_4 \xleftarrow{\sim} \mathrm{Isom}(\mathrm{Tétraèdre}) \subset \mathrm{GL}_3(\mathbb{R})$ (une isométrie du tétraèdre permute les quatre sommets dudit tétraèdre). La représentation V de dimension 2 est définie par l'action de $\mathfrak{S}_4$ sur un triangle équilatéral de $\mathbb{R}^2$ via le morphisme quotient naturel $\mathfrak{S}_4 \to \mathfrak{S}_4/K \simeq \mathfrak{S}_3$, où K désigne le sous-groupe de $\mathfrak{S}_4$ engendré par les bitranspositions.

— Le groupe $\mathfrak{A}_4$ a exactement quatre classes de conjugaison, à savoir celle de id (de cardinal 1), celle de (123) (de cardinal 4), celle de (132) (de cardinal 4), celle de (12)(34) (de cardinal 3). Le groupe dérivé de $\mathfrak{A}_4$ est le groupe de Klein engendré par les bitranspositions, et le quotient de $\mathfrak{A}_4$ par son sous-groupe dérivé est isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Donc $\mathfrak{A}_4$ admet trois représentations de dimension 1. On en déduit que la quatrième représentation irréductible est de dimension 3 et on obtient son caractère par orthogonalité. D'où la table de caractères suivante :

$\mathfrak{A}_4$	1	4	4	3
	id	(123)	(132)	(12)(34)
χ_{triv}	1	1	1	1
χ	1	j	j^2	-1
χ^2	1	j^2	j	1
$\chi_{V_0'}$	3	0	0	-1

On constate que la représentation V_0' est la restriction de la représentation standard V_0 de $\mathfrak{S}_4$ et correspond donc à un sous-groupe du groupe des isométries directes du cube en dimension 3.

c) — La table de caractères de $\mathfrak{S}_5$ est dans le cours. L'interprétation géométrique de ces représentations est difficile.

— Le groupe $\mathfrak{A}_5$ a exactement 5 classes de conjugaison, à savoir celle de id (de cardinal 1), celle de (123) (de cardinal 20, c'est la classe de tous les 3-cycles), celle de (12)(34) (de cardinal 15, c'est la classe de toutes les bitranspositions), celle de (12345) (de cardinal 12) et celle de (21345) (de cardinal 12). On considère les représentations irréductibles de $\mathfrak{S}_5$ et on regarde si leur restrictions à $\mathfrak{A}_5$ sont irréductibles ou non. Avec les notations du cours, on constate que $\chi_{\mathrm{triv}|_{\mathfrak{A}_5}} = \chi_{\mathrm{sign}|_{\mathfrak{A}_5}}$ est la représentation triviale de $\mathfrak{A}_5$. De même, les restrictions de V_0 et $V_0 \otimes \mathrm{sign}$ sont isomorphes et irréductibles. Et les restrictions de V et $V \otimes \mathrm{sign}$ sont isomorphes et irréductibles. En revanche, la restriction de $\bigwedge^2 V_0$ n'est pas irréductible. On a donc déterminé trois représentations irréductibles de $\mathfrak{A}_5$ sur cinq. La formule sur les dimensions assure que les deux représentations restantes, notées W et W', sont de dimension 3. On peut déterminer leur caractère via les relations d'orthogonalité.

D'où la table de caractères suivante :

$\mathfrak{A}_4$	1	20	15	12	12
	id	(123)	(12)(34)	(12345)	(21345)
χ_{triv}	1	1	1	1	1
χ_W	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
$\chi_{W'}$	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_{V_0}	4	1	0	-1	-1
χ_V	5	-1	1	0	0

On peut montrer que les représentations W et W' de dimension 3 s'obtiennent respectivement via l'isomorphisme $\mathfrak{A}_5 \xleftarrow{\sim} \mathrm{Isom}^+(\text{Dodécaèdre}) \simeq \mathrm{Isom}^+(\text{Icosaèdre}) \subset \mathrm{GL}_3(\mathbb{R})$, ainsi qu'en composant cette représentation avec l'automorphisme de $\mathfrak{A}_5$ défini par la conjugaison par $(12) \in \mathfrak{S}_5$ (cet automorphisme échange (12345) et (21345)).

Exercice 12 : $\star\star$

Soit p un nombre premier et soit $f \geq 1$ un entier ; on pose $q = p^f$. Soit G le groupe $\{x \mapsto ax + b \mid a \in \mathbb{F}_q^\times,\ b \in \mathbb{F}_q\}$.

a) Déterminer la table des caractères de G sur $\mathbb{C}$.

b) Déterminer les représentations irréductibles de G sur $\mathbb{C}$.

Solution de l'exercice 12.

a) Le groupe G, qui est le groupe affine de la droite affine de $\mathbb{F}_q$, s'insère dans une suite exacte scindée naturelle :

$$0 \to \mathbb{F}_q \to G \to \mathbb{F}_q^* \to 0\,,$$

où le noyau $\mathbb{F}_q$ s'identifie aux translations dans le groupe affine, et le morphisme de droite associe à une application affine sa partie linéaire. On en déduit donc au moins $q-1$ représentations de dimension 1 de G via les caractéres de $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Or on vérifie qu'il y a exactement q classes de conjugaison dans G (on a deux classes correspondant à $a = 1$, selon que $b = 0$ ou $b \neq 0$, et pour tout $a \neq 1$, et exactement une classe pour toute valeur de $a \neq 0, 1$), donc il reste une représentation irréductible V de dimension supérieure à déterminer. Son caractère vaut $q-1$ sur $\{1\}$ (donc sa dimension vaut $q-1$) et -1 sur $\{x \mapsto x + b \mid b \in \mathbb{F}_q^\times\}$. On a donc la table de caractères de G suivante, où $\zeta \in \mathbb{F}_q^*$ est un générateur de $\mathbb{F}_q^*$:

G	1	$q-1$	q	q	$\dots$	q
	id	translations	$x \mapsto \zeta x$	$x \mapsto \zeta^2 x$	$\dots$	$x \mapsto \zeta^{q-2} x$
χ_{triv}	1	1	1	1	$\dots$	1
χ_1	1	1	ζ	ζ^2	$\dots$	ζ^{q-2}
χ_2	1	1	ζ^2	ζ^4	$\dots$	$\zeta^{2(q-2)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
χ_{q-2}	1	1	ζ^{q-2}	$\zeta^{2(q-2)}$	$\dots$	$\zeta^{(q-2)(q-2)}$
χ_V	$q-1$	-1	0	0	$\dots$	0

b) On peut par exemple considérer la représentation naturelle de G sur $W := \mathbb{C}^{\mathbb{F}_q}$ définie par $g \cdot [x] := [g(x)]$, où $[x] \in W$ désigne la fonction indicatrice de $\{x\}$, pour $x \in \mathbb{F}_q$. Alors $\dim(W) = q$, et l'hyperplan $V := \{\sum_{x \in \mathbb{F}_q} \lambda_x [x] : \sum_x \lambda_x = 0 \text{ dans } \mathbb{C}\}$ est une sous-représentation de W de dimension $q-1$. On voit facilement que V n'admet pas de droite stable, donc V est la représentation irréductible de dimension $q-1$ recherchée.

On peut aussi la voir comme la représentation naturelle sur

$$V = \left\{ f : \mathbb{F}_q \to \mathbb{C} \;\middle|\; \sum\nolimits_{\mathbb{F}_q} f(x) = 0 \right\}.$$

Exercice 13 :
Soient G_1 et G_2 deux groupes finis. Déterminer l'ensemble des représentations irréductibles de $G_1 \times G_2$ en fonction des représentations irréductibles de G_1 et G_2.

Solution de l'exercice 13. Si V_1 et V_2 sont des représentations de G_1 et G_2 respectivement, le produit tensoriel $V_1 \otimes V_2$ est naturellement une représentation de $G_1 \times G_2$ pour l'action $(g_1, g_2) \cdot (v_1 \otimes v_2) := (g_1 \cdot v_1) \otimes (g_2 \otimes v_2)$.
On voit facilement que si V_1 et V_2 sont irréductibles, alors $V_1 \otimes V_2$ est une représentation irréductible de $G_1 \times G_2$: pour cela, on peut par exemple remarquer que $\chi_{V_1 \otimes V_2}(g_1, g_2) = \chi_{V_1}(g_1)\chi_{V_2}(g_2)$.
Or il est clair que le nombre de classes de conjugaison de $G_1 \times G_2$ est le produit du nombre de classes de conjugaison de G_1 par celui de G_2. Il suffit donc de montrer que pour V_i, W_i représentations irréductibles de G_i, les représentations $V_1 \otimes V_2$ et $W_1 \otimes W_2$ sont isomorphes comme représentations de $G_1 \times G_2$ si et seulement $V_i \cong W_i$ pour $i = 1$ et 2. Or un calcul simple assure que l'on a

$$\langle \chi_{V_1 \otimes V_2}, \chi_{W_1 \otimes W_2} \rangle = \langle \chi_{V_1}, \chi_{W_1} \rangle \langle \chi_{V_2}, \chi_{W_2} \rangle ,$$

ce qui implique que $V_1 \otimes V_2$ et $W_1 \otimes W_2$ ne sont pas isomorphes si V_1 et W_1 (ou V_2 et W_2) ne sont pas isomorphes.

Exercice 14 : $\star\star$
Soient p un nombre premier, G un p-groupe fini et K un corps de caractéristique p.

a) Montrer que toute représentation linéaire de G sur un K-espace vectoriel non nul admet des vecteurs fixes non nuls.

b) Montrer que toute représentation irréductible de G à coefficients dans K est isomorphe à la représentation triviale.

Solution de l'exercice 14.

a) Soit V une telle représentation. On note $k \cong \mathbb{F}_p$ le sous-corps premier de K et on fixe un vecteur non nul $v \in V$. On définit $W \subset V$ comme le sous-$\mathbb{F}_p$-espace vectoriel de V engendré par les $g \cdot v$, g décrivant G. Alors W est une sous-$\mathbb{F}_p$-représentation de dimension finie de V. Alors l'équation aux classes pour l'action de G sur W assure que

$$|W^G| \equiv |W| \ \ [p] ,$$

donc p divise $|W^G|$. Or $0 \in W^G$, donc $W^G \neq \{0\}$, donc $V^G \neq \{0\}$.

b) Soit V une représentation irréductible de G sur K. La question a) assure que V admet un vecteur fixe non nul $v \in V$. Donc $Kv \subset V$ est une sous-représentation triviale de V, donc par irréductibilité, $V = Kv$ est la représentation triviale de G.

Exercice 15 : $\star\star$
Soient G un groupe fini, χ le caractère d'une représentation et $K_\chi := \{g \in G : \chi(g) = \chi(e)\}$.

a) Montrer que K_χ est un sous-groupe distingué de G.

b) Montrer que G est simple si et seulement si $K_\chi = \{e\}$ pour tout caractère irréductible $\chi \neq 1$.

Solution de l'exercice 15.

Exercice 16 :
Soit G un groupe fini et soit X un ensemble fini sur lequel G agit transitivement. Soit ρ la représentation de permutation sur $\mathbb{C}$ définie par X et soit χ son caractère.

a) Montrer la décomposition $\rho = 1 \oplus \theta$, où θ ne contient pas la représentation triviale 1.

On fait opérer diagonalement G sur le produit $X \times X$ en posant $g(x, y) = (gx, gy)$ pour tout $g \in G$ et tous $x, y \in X$.

b) Montrer que le caractère de la représentation de permutation sur $X \times X$ est égal à χ^2.

c) Montrer que les assertions suivantes sont équivalentes

(i) l'action de G sur X est doublement transitive ;

(ii) on a l'égalité $\langle \chi^2, 1\rangle = 2$;

(iii) la représentation θ est irréductible.

Solution de l'exercice 16.

a) On a par la formule de Burnside :

$$\langle \chi, 1\rangle = \frac{1}{|G|}\sum\nolimits_G \chi(g) = \frac{1}{|G|}\sum\nolimits_G |\mathrm{Fix}\, g| = 1\,,$$

donc la représentation triviale apparaît avec multiplicité 1 dans la décomposition en irréductibles de ρ.

b) L'application bilinéaire naturelle et G-équivariante $\mathbb{C}^X \times \mathbb{C}^X \to C^{X\times X}$ définie par $(f,g) \mapsto ((x_1,x_2) \mapsto f(x_1)g(x_2))$ induit un isomorphisme de G-représentations $\mathbb{C}^X \otimes \mathbb{C}^X \simeq \mathbb{C}^{X\times X}$, ce qui assure le résultat.

c) En utilisant la question b), le même raisonnement qu'en a) donne l'équivalence entre (i) et (ii). De plus, si ψ est le caractère de θ, on a $\chi^2 = 1 + 2\psi + \psi^2$, donc

$$\langle \chi^2, 1\rangle = \langle 1, 1\rangle + 2\langle \psi, 1\rangle + \langle \psi^2, 1\rangle = 1 + 0 + \frac{1}{|G|}\sum\nolimits_{g\in G} \psi^2(g) = 1 + \langle \psi, \psi\rangle\,,$$

où la dernière égalité provient du fait que ψ est à valeurs réelles (puisque ρ est définie sur $\mathbb{R}$, χ est à valeurs réelles, donc ψ aussi).

L'équivalence entre (ii) et (iii) est alors claire.

Exercice 17 : $\star\star\star$

a) Soit G un groupe abélien (éventuellement infini) et (V,ρ) une représentation complexe irréductible de G (de dimension éventuellement infinie). Sous quelles hypothèses cette représentation est-elle de dimension 1 ? Est-ce toujours le cas ?

b) Soit K un corps de caractéristique nulle, G un groupe (éventuellement infini) et (V,ρ) une représentation de G sur K (de dimension éventuellement infinie). Sous quelles hypothèses cette représentation est-elle somme directe de sous-représentations irréductibles ? Est-ce toujours le cas ?

Solution de l'exercice 17.

a) i) Si le groupe G est fini, $\dim(V) = 1$ même si la dimension de V est infinie, car V contient une sous-représentation non nulle de dimension finie, obtenue en fixant un vecteur de v et en prenant le sous-espace vectoriel engendré par l'orbite de v sous G.

ii) Si la représentation (V,ρ) est de dimension finie n et le groupe G quelconque, alors $\dim(V) = 1$: le sous-groupe $\rho(G)$ de $\mathrm{GL}(V)$ est un sous-groupe abélien formé d'endomorphismes trigonalisables, donc les éléments de $\rho(G)$ sont cotrigonalisables, ce qui assure que G admet une droite stable dans $\mathbb{C}^n$, donc $n = 1$ par irréductibilité.

iii) Si le cardinal de G est strictement inférieur à celui de $\mathbb{C}$ (par exemple si G est un groupe abélien de type fini), alors $\dim(V) = 1$.

Pour montrer ce résultat, on étend d'abord le lemme de Schur à de tels groupes. Soit V une représentation irréductible de G et $\pi : V \to V$ un morphisme de représentations. Tout d'abord, il est clair que tout morphisme non nul de représentations $V \to V$ est un isomorphisme ($\mathrm{Ker}(\pi)$ et $\mathrm{Im}\,(\pi)$ sont des sous-représentations de V). Supposons que π ne soit pas une homothétie. Alors pour tout $\lambda \in \mathbb{C}$, on dispose de l'isomorphisme $\pi_\lambda := (\pi - \lambda)^{-1} : V \to V$. On montre alors facilement que pour tout $v \in V \setminus \{0\}$, les vecteurs $(\pi_\lambda(v))_{\lambda\in\mathbb{C}}$ forment une famille libre dans V. Donc la dimension de V est supérieure ou égale au cardinal

de $\mathbb{C}$. Or V est engendré par l'orbite $G \cdot v$ de v, qui est de cardinal strictement inférieur à celui de $\mathbb{C}$. On a donc une contradiction, ce qui assure que π est une homothétie.

On déduit alors facilement du lemme de Schur le fait que sous les hypothèses de a)ii), toute représentation irréductible de G est de dimension 1 : si (V, ρ) est une telle représentation, pour tout $g \in G$, $\rho(g) : V \to V$ est un morphisme de représentations irréductibles, donc c'est une homothétie, et on conclut facilementcomme en ii).

iv) En général, $\dim(V) \neq 1$. On peut construire un exemple de la façon suivante : considérons le $\mathbb{C}$-espace vectoriel $V = \mathbb{C}(T)$ et le groupe abélien (multiplicatif) $G = \mathbb{C}(T)^*$. Alors G agit linéairement sur V par multiplication (à gauche), et cette action est transitive sur les vecteurs non nuls de V. Cela assure que la représentation $G \to \mathrm{GL}(V)$ qui s'en déduit est irréductible et de dimension infinie.

b) i) Si G est fini, la réponse est positive. En effet, tout vecteur de la représentation V est contenu dans une sous-représentation de dimension finie, ce qui assure que V est somme (pas directe a priori) de sous-représentations irréductibles. Le lemme de Zorn assure alors que V est somme directe de sous-représentations irréductibles (considérer les sous-familles en somme directe dans la décomposition précédente : elles forment bien un ensemble inductif).

ii) Si G est infini, la réponse est négative en général. Un contre-exemple est donné par $G = \mathbb{Z}$ et sa représentation de dimension 2 sur le corps K définie par $\rho : \mathbb{Z} \to \mathrm{GL}_2(K)$ qui envoie $n \in \mathbb{Z}$ sur la matrice $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Il est clair que cette représentation n'est pas irréductible, (on a une droite stable évidente), mais que celle-ci ne se décompose pas en somme de représentations irréductibles (si c'était le cas, la matrice $\rho(1)$ serait diagonalisable, ce qui n'est pas le cas).

TD12 : Représentations des groupes finis II

Exercices ⋆ : à préparer à la maison avant le TD, seront corrigés en début de TD.
Exercices ⋆⋆ : seront traités en classe en priorité.
Exercices ⋆⋆⋆ : plus difficiles.

Exercice 1 : ⋆

Soit G un groupe fini, soit H un sous-groupe de G et soit π une représentation de G de caractère χ.

a) Montrer que la restriction de π à H a pour caractère la restriction $\chi|_H$.

b) Si π est irréductible, est-ce que $\chi|_H$ est un caractère irréductible ?

Solution de l'exercice 1.

a) C'est évident : pour tout $h \in H$, on a $\chi_{\pi|_H}(h) := \mathrm{tr}(\pi|_H(h)) = \mathrm{tr}(\pi(h)) = \chi(h) = \chi|_H(h)$.

b) Non : si G est un groupe fini non abélien, $H = \{1\}$ le sous-groupe trivial de G et π une représentation complexe irréductible de G de dimension ≥ 2 (une telle représentation existe), alors toute droite de π est un sous-espace strict non nul de π stable par H, donc $\chi|_H$ n'est pas irréductible.

Exercice 2 : ⋆

Soit G un groupe fini, soit H un sous-groupe de G et soit (π, V) une représentation de H. On pose

$$W := \mathrm{Ind}_H^G(\pi) := \{f : G \to V \mid \forall x \in G\ \forall h \in H \quad f(hx) = \pi(h)f(x)\},$$

avec action de G donnée par $g(f) : x \mapsto f(xg)$.

a) Montrer que $\mathrm{Ind}_H^G(\pi)$ est une représentation de G. Quelle est sa dimension ?

b) Si π est irréductible, est-ce que $\mathrm{Ind}_H^G(\pi)$ est une représentation irréductible de G ?

Solution de l'exercice 2.

a) On vérifie facilement les points suivants :
— l'ensemble $\mathrm{Ind}_H^G(\pi)$ est un sous-espace vectoriel de V^G.
— la formule $(g, f) \mapsto g(f)$ définit une action de groupe linéaire de G sur $\mathrm{Ind}_H^G(\pi)$.
— pour tout $g \in G$ et $f \in \mathrm{Ind}_H^G(\pi)$, $f(g) \in \mathrm{Ind}_H^G(\pi)$: en effet, pour tout $h \in H$ et $x \in G$, on a

$$f(g)(hx) = f(h(xg)) = \pi(h)f(xg) = \pi(h)f(g)(x)\,.$$

Ces trois points assurent que $\mathrm{Ind}_H^G(\pi)$ est naturellement une représentation de G.

En outre, si $R \subset G$ désigne un ensemble de représentants de G modulo H, l'application $\mathrm{Ind}_H^G(\pi) \to V^R$ définie par $f \mapsto f_{|R}$ est une application linéaire, et c'est un isomorphisme par définition de $\mathrm{Ind}_H^G(\pi)$: un élément de $\mathrm{Ind}_H^G(\pi)$ est entièrement déterminé par l'image des éléments de R. Cela assure que $\dim\left(\mathrm{Ind}_H^G(\pi)\right) = |R| \dim(V)$, i.e.

$$\dim\left(\mathrm{Ind}_H^G(\pi)\right) = [G : H] \dim V\,.$$

b) Non : pour avoir un contre-exemple, on s'inspire de l'exercice 3 suivant. On considère un groupe G non trivial et $H = \{1\}$ le sous-groupe trivial. La représentation trivial de H, notée triv, est irréductible. Alors l'exercice 3 assure que $\mathrm{Ind}_H^G(\mathrm{triv}) \simeq K[G]$, où $K[G]$ désigne la représentation régulière de G. Or on sait que cette dernière est irréductible si et seulement si $|G| = 1$, ce que l'on a exclut.

Exercice 3 :
Soit G un groupe fini ; notons triv la représentation triviale du sous-groupe $\{e_G\}$ de G. Déterminer la représentation $\mathrm{Ind}_{\{e_G\}}^G(\mathrm{triv})$.

Solution de l'exercice 3. Par définition, on a

$$\mathrm{Ind}_{\{e\}}^G(\mathrm{triv}) = \{f : V \to G\} = V^G\,,$$

avec l'action de G définie par $g(f) := f(.g)$.
On voit donc tout de suite que $\mathrm{Ind}_{\{e\}}^G(\mathrm{triv})$ est isomorphe à la représentation régulière de G.

Exercice 4 : $\star\star$
Soit G un groupe fini et soit H un sous-groupe de G. On va définir une application entre espaces de fonctions centrales

$$\begin{array}{ccc} \mathcal{C}(H) & \longrightarrow & \mathcal{C}(G) \\ f & \mapsto & f^G. \end{array}$$

D'abord on définit $f^0 : G \to \mathbb{C}$ par

$$f^0(x) = \begin{cases} f(x) & \text{si } x \in H, \\ 0 & \text{sinon.} \end{cases}$$

Ensuite on pose $f^G(g) = \frac{1}{|H|}\sum_{x\in G} f^0(xgx^{-1})$.

a) Montrer que $f^G \in \mathcal{C}(G)$.

b) Supposons que f est un caractère irréductible. Est-ce que f^G est irréductible ?

c) Soit (π, V) une représentation de H et soit χ son caractère. Montrer que χ^G est le caractère de $\mathrm{Ind}_H^G(\pi)$.

Solution de l'exercice 4.

a) Soient $gx \in G$. Alors par définition on a

$$f^G(gxg^{-1}) = \frac{1}{|H|}\sum_{y\in G} f^0(y(gxg^{-1})y^{-1}) = \frac{1}{|H|}\sum_{y\in G} f^0((yg)x(yg)^{-1})\,.$$

Or l'application $y \mapsto yg$ est une bijection de G, donc on a

$$f^G(gxg^{-1}) = \frac{1}{|H|}\sum_{y\in G} f^0(yxy^{-1}) = f^G(x)\,,$$

donc $f^G \in \mathcal{C}(G)$.

b) Non : prenons $H = \{e_G\}$, avec G un groupe non trivial, et triv la représentation triviale de H, qui est un caractère irréductible de H. Alors par définition triv^0 est la fonction indicatrice 1_{e_G} de $\{e_G\}$, et donc pour tout $x \in G$

$$\mathrm{triv}^G(x) = \sum_{g\in G} f^0(gxg^{-1}) = \sum_{g\in G : gxg^{-1}=e_G} 1 = |G|1_{e_G}(x)\,.$$

Par conséquent, on constate que triv^G est le caractère de la représentation régulière de G, qui n'est pas irréductible.

c) On a vu à l'exercice 2 que la représentation $\mathrm{Ind}_H^G(\pi)$ se décomposait en somme directe de sous-espaces vectoriels de la forme

$$\mathrm{Ind}_H^G(\pi) = \bigoplus_{g\in R} V^g\,,$$

où $R \subset G$ est un ensemble de représentants de G modulo H et $V^g = V$, avec l'inclusion $V^g \subset \mathrm{Ind}_H^G(\pi)$ définie par $v \mapsto f_g$, où $f_g : R \to V$ est la fonction indicatrice de $\{g\} \subset R$ multipliée par v. En explicitant l'action de G sur cette décomposition, on trouve facilement que, pour tout $g \in G$,

$$\begin{aligned}\chi_{\mathrm{Ind}_H^G(\pi)}(g) &= \textstyle\sum_{g' \in R\,:\, g'gg'^{-1} \in H} \chi_{V^{g'}}(g'gg'^{-1}) = \sum_{g' \in R\,:\, g'gg'^{-1} \in H} \chi_V(g'gg'^{-1}) \\ &= \tfrac{1}{|H|} \textstyle\sum_{g' \in G\,:\, g'gg'^{-1}} \chi_V(g'gg'^{-1}) = \tfrac{1}{|H|} \sum_{g' \in G} \chi_V^0(g'gg'^{-1}) = \chi^G(g)\,,\end{aligned}$$

d'où finalement $\chi_{\mathrm{Ind}_H^G(\pi)} = \chi^G$.

Exercice 5 : (Réciprocité de Frobenius, point de vue des représentations) $\star\star$
Soient G un groupe fini, H un sous-groupe de G, π une représentation de H et ρ une représentation de G.

a) Montrer :
$$\mathrm{Hom}_G(\rho, \mathrm{Ind}_H^G(\pi)) = \mathrm{Hom}_H(\rho_{|_H}, \pi)\,.$$

b) En déduire que, si ρ et π sont irréductibles, la multiplicité de ρ dans $\mathrm{Ind}_H^G(\pi)$ est égale à la multiplicité de π dans $\rho_{|_H}$.

Solution de l'exercice 5.

a) Définissons une application naturelle $\alpha : \mathrm{Hom}_G(\rho, \mathrm{Ind}_H^G(\pi)) \to \mathrm{Hom}_H(\rho_{|_H}, \pi)$. Si $\phi : \rho \to \mathrm{Ind}_H^G(\pi)$ est un morphisme de G-représentations, on définit $\psi = \alpha(\phi)$ comme l'application linéaire $\psi : \rho_{|_H} : \pi$ tel que $\psi(v) := \phi(v)(e_G)$. Un calcul simple assure qu'effectivement $\psi = \alpha(\phi)$ est H-équivariante, et que l'application $\phi \mapsto \alpha(\phi)$ est linéaire.

Réciproquement, on définit une application $\beta : \mathrm{Hom}_H(\rho_{|_H}, \pi) \to \mathrm{Hom}_G(\rho, \mathrm{Ind}_H^G(\pi))$ en introduisant pour tout $\psi : \rho_{|H} \to \pi$, l'application linéaire $\phi = \beta(\psi) : \rho \to \mathrm{Ind}_H^G(\pi)$, où $\phi(w) : G \to V$ est définie par $g \mapsto \psi(g \cdot w)$. On vérifie également que $\beta(\psi)$ est G-équivariant, et que l'application β est linéaire.

Alors en suivant les définitions, on obtient que pour tout $\psi : \rho_{|H} \to \pi$, $\alpha(\beta(\psi)) = \psi$, et pour tout $\psi : \rho \to \mathrm{Ind}_H^G(\pi)$, $\beta(\alpha(\phi)) = \phi$. Donc α et β sont inverses l'une de l'autre, donc elles définissent un isomorphisme naturel

$$\mathrm{Hom}_G(\rho, \mathrm{Ind}_H^G(\pi)) = \mathrm{Hom}_H(\rho_{|_H}, \pi)\,.$$

b) Le lemme de Schur assure que la multiplicité de ρ dans $\mathrm{Ind}_H^G(\pi)$ est égale à la dimension de l'espace vectoriel $\mathrm{Hom}_G(\rho, \mathrm{Ind}_H^G(\pi))$. De même, la multiplicité de π dans $\rho_{|_H}$ est égale à la dimension de l'espace vectoriel $\mathrm{Hom}_H(\rho_{|_H}, \pi)$. La question a) assure que ces deux entiers sont égaux.

Exercice 6 : (Réciprocité de Frobenius, point de vue des caractères)
Soient G un groupe fini, H un sous-groupe de G, ϕ une fonction centrale sur G et ψ une fonction centrale sur H. Montrer
$$\langle \phi, \psi^G \rangle = \langle \phi|_H, \psi \rangle.$$

Solution de l'exercice 6. L'exercice 4 permet le calcul suivant :

$$\begin{aligned}
\langle \phi, \psi^G \rangle &= \frac{1}{|G|} \sum_{x \in G} \phi(x^{-1}) \psi^G(x) \\
&= \frac{1}{|G|} \sum_{x \in G, y \in G/H} \phi(x^{-1}) \psi^0(yxy^{-1}) \\
&= \frac{1}{|G|} \sum_{x \in G, y \in G/H} \phi(yx^{-1}y^{-1}) \psi^0(yxy^{-1}) \\
&= \frac{1}{|H|} \sum_{h \in H} \phi(h^{-1}) \psi^0(h) \\
&= \langle \phi_{|_H}, \psi \rangle \,,
\end{aligned}$$

d'où le résultat.

Exercice 7 : (Théorème de Frobenius)
Soit $n \geq 1$ un entier et soit G un groupe fini. Soit X un ensemble à n éléments muni d'une action transitive de G, soit $x_0 \in X$ et notons H le stabilisateur de x_0. On suppose que tout élément de G autre que l'identité fixe au plus un élément de X.
On note G_1 l'ensemble des éléments de G qui agissent sur X sans point fixe ; on pose $G_0 := G_1 \cup \{1\}$.

a) Déterminer le cardinal de G_0.

b) Soit χ_σ le caractère de la $\mathbb{C}$-représentation de permutation donnée par l'action de G sur X et soit χ_1 le caractère de la représentation triviale. On pose $\chi = \chi_\sigma - \chi_1$. Montrer que χ est un caractère.

c) Soient ψ un caractère irréductible de H et ψ_G le caractère de l'induite de H à G. On pose $\phi = \psi_G - \psi(1)\chi$. Montrer que ϕ est un caractère irréductible de G. En déduire que G_0 est un sous-groupe distingué de G.

d) Montrer que G est le produit semi-direct de H par G_0.

Solution de l'exercice 7.

a) L'hypothèse nous dit que $\{1\} \cup \bigcup_{x \in X} (\mathrm{Stab}_G(x) \setminus \{1\})$ est une union disjointe. Le cardinal de $\bigcup_X \mathrm{Stab}\, x$ est alors $n(|H|-1)+1 = |G| - n + 1$. Ainsi le cardinal de G_0 est n.

b) Remarquons d'abord que $\chi_\sigma(g)$ est égal au cardinal de $\mathrm{Fix}(g)$. On veut montrer que la représentation de permutation σ contient la représentation triviale. Pour cela calculons :

$$\langle \chi_\sigma, 1 \rangle = \frac{1}{|G|} \left(n + \sum_{g \notin G_0} \chi_\sigma(g) \right) = 1 \,.$$

Cela assure que la représentation triviale est une sous-représentation de σ (avec multiplicité 1), donc χ est le caractère d'une sous-représentation de σ supplémentaire de cette sous-représentation triviale.

c) En utilisant l'exercice 2, on a $\phi(1) = n\psi(1) - (n-1)\psi(1) = \psi(1)$.
Soit $g \in G_1$. On a $\phi(g) = \psi_G(g) - \psi(1)(\chi_\sigma(g) - 1)$, or $\chi_\sigma(g) = 0$ car g ne fixe aucun point de X, donc $\phi(g) = \psi_G(g) + \psi(1)$. Or pour tout $g' \in G$, on a $g'gg'^{-1} \in H$ si et seulement si g fixe $g'x_0$, ce qui n'arrive jamais. Donc la formule permettant de calculer ψ_G (voir exercice 4) assure que $\psi_G(g) = 0$. Donc finalement, pour tout $g \in G_1$, $\phi(g) = \psi(1)$.
Soit $g \in G \setminus G_0$. Alors g fixe exactement un point de X, donc il existe $h \in H$ conjugué à g dans G et la formule de l'exercice 4 assure que l'on a $\phi(g) = \psi(h)$.

On calcule ensuite

$$\begin{aligned}\langle\phi,\phi\rangle &= \tfrac{1}{|G|}\left(\psi(1)^2+\sum_{g\in G_0\setminus\{1\}}\psi(1)^2+\sum_{g\neq 1,\, g\in\bigcup \mathrm{Stab}(x)}\phi(g)\overline{\phi(g)}\right)\\ &= \tfrac{1}{|G|}\left(\psi(1)^2+\sum_{g\in G_0\setminus\{1\}}\psi(1)^2+n\sum_{h\in H\setminus\{1\}}\psi(h)\overline{\psi(h)}\right).\end{aligned}$$

Reste à utiliser le fait que ψ est un caractère irréductible pour en déduire que $\langle\phi,\phi\rangle$ vaut 1. Dès lors, ϕ est le caractère d'une représentation irréductible ou alors son opposé. Mais on a $\phi(1)=\psi(1)>0$, d'où le résultat.

Comme on a $\phi(g)=\phi(1)$ pour tout $g\in G_0$, on sait que G_0 est dans le noyau de la représentation correspondant à ϕ.

Soit $g\in G\setminus G_0$. Alors g est conjugué à un élément $h\in H\setminus\{1\}$. Comme les caractères irréductibles forment une base des fonctions centrales sur H, il existe un caractère irréductible ψ avec $\psi(h)\neq\psi(1)$. Dès lors, g n'est pas dans le noyau de la représentation ϕ correspondant à ce ψ. Finalement, G_0 est exactement l'intersection des noyaux des représentations de caractère $\psi_G-\psi(1)\chi$, où ψ parcourt l'ensemble des caractères irréductibles de H. En tant que tel, G_0 est bien un sous-groupe distingué de G.

d) On a les propriétés suivantes :
- H est un sous-groupe de G, G_0 est un sous-groupe distingué de G.
- $H\cap G_0=\{1\}$ car tout élément de H fixe x_0 et les éléments de $G_0\setminus\{1\}$ sont sans point fixe.
- Montrons que $G=G_0\cdot H$. Pour cela, on considère l'application $\pi: G_0\to X$ définie par $\pi(g):=g\cdot x_0$. Puisque les éléments de $G_0\setminus\{1\}$ ne fixent pas x_0, on voit que π est injective. Or la question a) assure que $|G|=n=|X|$, donc π est bijective. Donc G_0 agit transitivement sur X.

  Soit alors $g\in G$. Par le raisonnement précédent, il existe $g_0\in G_0$ tel que $g\cdot x_0=g_0\cdot x_0$. Donc $h:=g_0^{-1}g\in H$ et $g=g_0h$. Cela assure que $G=G_0\cdot H$.

Les trois points précédents assurent que G est le produit semi-direct de H par G_0 (voir TD4, exercice 2).

Exercice 8 : (Critère de Mackey)
Soit G un groupe fini et soit k un corps algébriquement clos de caractéristique première à $|G|$. Soient H et K des sous-groupes de G et soit (ρ,W) une représentation de H sur k. On pose $V:=\mathrm{Ind}_H^G W$. Soit S un système de représentants de $K\backslash G/H$ contenant 1. Pour $s\in S$, on pose $H_s=sHs^{-1}\cap K$ et on note W_s la représentation de H_s correspondant au morphisme $\begin{array}{rccc}\rho^s: & H_s & \to & \mathrm{GL}(W)\\ & x & \mapsto & \rho(s^{-1}xs)\end{array}$.

a) Montrer que V est isomorphe à $\bigoplus_{s\in S}\mathrm{Ind}_{H_s}^K W_s$ en tant que représentation de K.

b) Montrer que V est irréductible si et seulement si les conditions suivantes sont satisfaites :
   (i) W est irréductible ;
   (ii) pour tout $s\in S\smallsetminus\{1\}$, $\mathrm{Hom}(W_s,W|_{H_s})=0$ (on dit alors que W_s, et $W|_{H_s}$ ne s'entrelacent pas).

Solution de l'exercice 8.

a) On a vu aux exercices 2 et 4 que l'on a une décomposition d'espaces vectoriels $V=\bigoplus_{g\in G/H}gW$. Pour $s\in S$, on définit $V_{(s)}=\bigoplus_{g\in KsH/H}gW$; c'est une sous-K-représentation de V, et on a $V=\bigoplus_{s\in S}V_{(s)}$. Le groupe K agit transitivement sur les gW pour $g\in KsH/H$ et le stabilisateur de sW est H_s. On peut donc réécrire $V_{(s)}=\bigoplus_{g\in K/H_s}g(sW)=\mathrm{Ind}_{H_s}^K(sW)$. Et sW est isomorphe à W_s en tant que H_s-représentation. D'où le résultat.

b) En appliquant la question a) à $K=H$, on sait que V est isomorphe à $\bigoplus_{s\in S}\mathrm{Ind}_{H_s}^H(W_s)$ en tant que H-représentation. Appliquons la réciprocité de Frobenius (voir exercice 5) :

$$\mathrm{Hom}_G(V,V)\simeq\bigoplus_{s\in S}\mathrm{Hom}_H(W,\mathrm{Ind}_{H_s}^H W_s).$$

En appliquant une réciprocité de Frobenius à droite cette fois-ci, on obtient

$$\mathrm{Hom}_H(W, \mathrm{Ind}_{H_s}^H W_s) \simeq \mathrm{Hom}_{H_s}(W_{|_{H_s}}, W_s)\,.$$

Les dimensions étant additives, V est irréductible si et seulement si $\dim \mathrm{Hom}_H(W,W) = 1$ et $\dim \mathrm{Hom}_{H_s}(W_{|_{H_s}}, W_s) = 0$ pour tout $s \in S \setminus \{1\}$. D'où l'équivalence demandée.

Exercice 9 : ⋆⋆
Soit G un groupe fini et (V, ρ) une représentation complexe de G, de caractère χ.
Montrer les deux équivalences suivantes :

a) le caractère χ est à valeurs dans $\mathbb{R}$ si et seulement si V admet une forme bilinéaire non dégénérée invariante par G.

b) la représentation ρ provient d'une représentation réelle par extension des scalaires si et seulement si V admet une forme bilinèaire symétrique non dégénérée invariante par G.

Solution de l'exercice 9.

a) On note V^* l'espace dual de V. On dispose de la représentation duale de ρ définie par $\rho^* : G \to \mathrm{GL}(V^*)$ telle que pour tout $g \in G$, $\rho^*(g) : f \mapsto f(g^{-1}\cdot)$. Alors un calcul simple via la base duale assure que pour tout $g \in G$,

$$\chi_{V^*}(g) = \chi(g^{-1}) = \overline{\chi(g)}\,.$$

Par conséquent, χ est à valeurs réelles si et seulement si $\chi_{V^*} = \chi$ si et seulement si V et V^* sont isomorphes comme représentations de G si et seulement s'il existe une forme bilinéaire $V \otimes V \to \mathbb{C}$ non dégénérée invariante par G (on rappelle qu'on dispose toujours de la forme bilinéaire naturelle invariante par G et non dégénérée $V \otimes V^* \to \mathbb{C}$).

b) — On suppose d'abord que $V = V_0 \otimes_{\mathbb{R}} \mathbb{C}$ et $\rho = \rho_0 \otimes_{\mathbb{R}} \mathbb{C}$, où (V_0, ρ_0) est une représentation de G sur $\mathbb{R}$. Alors on voit V_0 comme un sous-$\mathbb{R}$-espace vectoriel de V stable par G, et donc on a $V = V_0 \oplus iV_0$. On munit V_0 de la forme quadratique définie positive q_0 invariante par G définie par sa forme polaire b_0 :

$$b_0(x,y) := \sum_{g \in G} \langle g \cdot x, g \cdot y \rangle\,,$$

où $\langle .,. \rangle$ est un produit scalaire quelconque sur V_0.
Alors $q_0 \otimes_{\mathbb{R}} \mathbb{C}$ est une forme quadratique sur V, dont la forme polaire est la forme bilinéaire symétrique non dégénérée invariant par G recherchée.

— Réciproquement, supposons V muni d'une forme bilinéaire symétrique non dégénérée B, invariante par G. On sait (comme dans le point précédente) que V admet un produit scalaire hermitien (défini positif) $\langle .,. \rangle$ et invariant par G (obtenu en moyennant un produit hermitien quelconque sur V). La non-dégénérescence de $\langle .,. \rangle$ assure que pour tout $x \in V$, il existe un unique $\varphi(x) \in V$ tel que $B(x,\cdot) = \overline{\langle \varphi(x), \cdot \rangle}$. On voit facilement que $\varphi : V \to V$ est une bijection antilinéaire, donc $\varphi^2 := \varphi \circ \varphi \in \mathrm{GL}(V)$. On a alors, pour tout $x, y \in V$,

$$\langle \varphi^2(x), y \rangle = \overline{B(\varphi(x), y)} = \overline{B(y, \varphi(x))} = \langle \varphi(y), \varphi(x) \rangle$$

par symétrie de B. Or le produit $\langle .,. \rangle$ est hermitien, donc on déduit de l'égalité précédente que

$$\langle \varphi^2(x), y \rangle = \overline{\langle \varphi^2(y), x \rangle} = \langle x, \varphi^2(y) \rangle\,,$$

ce qui assure que φ^2 est unitaire. Or pour tout $x \in V$, on a $\langle \varphi^2(x), x \rangle = \langle \varphi(x), \varphi(x) \rangle$, donc φ^2 est définie positive. Donc la réduction des endomorphismes hermitiens assure qu'il existe un unique $u \in \mathrm{GL}(V)$ hermitien défini positif tel que $\varphi^2 = u^2$ (et on sait que u est un polynôme en φ). Posons alors $\sigma := \varphi \circ u^{-1}$. Alors $\sigma^2 = \mathrm{id}_V$, i.e. σ est une involution antilinéaire de V. Donc V se décompose en une somme directe de $\mathbb{R}$-sous-espaces propres $V = V_+ \oplus V_-$ avec $iV_+ = V_-$. On a donc $V = V_+ \oplus iV_+$. Enfin, B et $\langle .,. \rangle$ sont invariants par G, donc on en déduit que φ, u et σ sont G-équivariants, donc V_+ et iV_+ sont stables par G. Cela assure que V_+ est une représentation réelle de G telle que $V \simeq V_+ \otimes_{\mathbb{R}} \mathbb{C}$.

Exercice 10 : (Représentations complexes de $\mathfrak{S}_n$) ⋆⋆⋆

Soit $n \geq 1$ un entier et soit λ une partition de n, c'est-à-dire une suite $(\lambda_k)_{k\geq 1}$ d'entiers naturels vérifiant $n = \sum_k \lambda_k$ avec $\lambda_k \geq \lambda_{k+1}$ pour tout k. À cette partition λ, on associe un *tableau de Young* T_λ, qui est un tableau de n cases alignées à gauche dans lequel la i-ème ligne a λ_i colonnes.

Le groupe symétrique $\mathfrak{S}_n$ s'identifie au groupe de permutations des cases de T_λ. On définit alors le sous-groupe P_λ (resp. Q_λ) comme étant respectivement le stabilisateur des lignes (resp. des colonnes) de T_λ. On appelle *projecteurs de Young* les éléments de $\mathbb{C}[\mathfrak{S}_n]$ suivants

$$a_\lambda = \frac{1}{|P_\lambda|}\sum\nolimits_{P_\lambda} g, \quad b_\lambda = \frac{1}{|Q_\lambda|}\sum\nolimits_{Q_\lambda} \varepsilon(g)\, g,$$

où $\varepsilon(g)$ désigne la signature de la permutation g. On pose $c_\lambda = a_\lambda b_\lambda$.

a) Supposons $g \in \mathfrak{S}_n \smallsetminus P_\lambda Q_\lambda$. Montrer qu'il existe une transposition $t \in P_\lambda$ vérifiant $g^{-1}tg \in Q_\lambda$.

b) En déduire l'existence d'une application linéaire $l_\lambda : \mathbb{C}[\mathfrak{S}_n] \to \mathbb{C}$ telle que l'on ait $a_\lambda g b_\lambda = l_\lambda(g)c_\lambda$ pour tout $g \in \mathbb{C}[\mathfrak{S}_n]$.

c) Soit μ une partition de n. On introduit l'ordre lexicographique sur les partitions de n : on a $\lambda > \mu$ s'il existe $j \geq 1$ tel que $\lambda_j > \mu_j$ et $\lambda_i = \mu_i$ pour tout $i < j$. Supposons $\lambda > \mu$. Montrer que l'on a $a_\lambda \mathbb{C}[\mathfrak{S}_n] b_\mu = 0$.

d) Soit A une algèbre. Un élément $e \in A$ est dit *idempotent* s'il vérifie $e^2 = e$. Montrer que pour tout A-module à gauche M, on a $\mathrm{Hom}_A(Ae, M) \simeq eM$. Montrer que c_λ est proportionnel à un idempotent de $\mathbb{C}[\mathfrak{S}_n]$.

e) Soit V_λ la représentation de $\mathfrak{S}_n$ donnée par multiplication à gauche sur l'espace $\mathbb{C}[\mathfrak{S}_n]c_\lambda$. Montrer que l'application $\lambda \mapsto V_\lambda$ induit une bijection entre l'ensemble des partitions de n et l'ensemble des classes d'isomorphisme de représentations irréductibles de $\mathfrak{S}_n$ sur $\mathbb{C}$.

Solution de l'exercice 10.

a) Soient $g \in \mathfrak{S}_n$, $T = T_\lambda$ et $T' = gT$. On veut montrer qu'il existe i et j dans $\{1, 2, \ldots, n\}$ qui sont sur une même ligne dans T et sur une même colonne dans T'. Supposons que deux tels indices n'existent pas. Alors tous les éléments de la première ligne de T se retrouvent dans des colonnes distinctes de T'. On peut donc trouver $q_1 \in gQ_\lambda g^{-1}$ tel que $q_1 T'$ ait la même première ligne (à permutation sur la ligne près) que T. Soit alors $p_1 \in P_\lambda$ tel que $p_1 T$ et $q_1 T'$ ont même première ligne. Soit S^1_λ l'ensemble des permutations de $\mathfrak{S}_n$ fixant point par point la première ligne de $p_1 T$. On peut de même trouver $q_2 \in gQ_\lambda g^{-1} \cap S^1_\lambda$ et $p_2 \in P_\lambda \cap S^1_\lambda$ tels que $p_2 p_1 T$ et $q_2 q_1 T'$ ont leurs deux premières lignes identiques. On considère ensuite S^2_λ le sous-groupe de S^1_λ fixant les points des deux premières lignes de $p_2 p_1 T$, etc... Par récurrence, on a finalement $p \in P_\lambda$ et $q \in Q_\lambda$ tels que $pT = gqg^{-1}T'$. Autrement dit, on a $pq^{-1} = g \in P_\lambda Q_\lambda$.

b) Si g s'écrit pq avec $p \in P_\lambda$ et $q \in Q_\lambda$, on a $a_\lambda g b_\lambda = \varepsilon(q)c_\lambda$. Si g n'est pas élément de $P_\lambda Q_\lambda$, soit $t \in P_\lambda$ donné par la question a). On a alors

$$a_\lambda g b_\lambda = a_\lambda t g b_\lambda = a_\lambda g(g^{-1}tg)b_\lambda = -a_\lambda g b_\lambda \ ,$$

de sorte que cette quantité est nulle.

c) Soit $g \in \mathfrak{S}_n$. Pour répéter l'argument de la question b), il nous suffit de trouver $t \in P_\lambda$ tel que $g^{-1}tg$ soit un élément de Q_μ. On pose $T = T_\lambda$ et $T' = gT_\mu$. Si on a $\lambda_1 > \mu_1$, l'existence d'indices i et j qui sont sur la même ligne de T et la même colonne de T' est claire par le principe des tiroirs. Si on a $\lambda_1 = \mu_1$, il existe $p_1 \in P\lambda$ et $q_1 \in gQ_\lambda g^{-1}$ tels que $T_2 := p_1 T$ et $T'_2 := q_1 T'$ ont même première ligne. On travaille ensuite sur la deuxième ligne de T_2 et T'_2, etc... Comme l'hypothèse assure que $\lambda > \mu$, il existe un plus petit indice α avec $\lambda_\alpha > \mu_\alpha$. Par principe des tiroirs, la α-ième ligne de T_α va alors contenir deux indices qui sont dans la même colonne de T'_α. Cela assure le résultat.

d) Les applications $\begin{array}{ccc} eM & \to & \mathrm{Hom}_A(Ae, M) \\ em & \mapsto & (ae \mapsto aem) \end{array}$ et $\begin{array}{ccc} eM & \leftarrow & \mathrm{Hom}_A(Ae, M) \\ f(e) & \hookleftarrow & f \end{array}$ sont inverses l'une de l'autre.

Par la question b), on a $c_\lambda^2 = l_\lambda(b_\lambda a_\lambda)c_\lambda$. Aussi, comme on a $c_\lambda^2(1) = 1$, le coefficient $l_\lambda(b_\lambda a_\lambda)$ n'est pas nul. Il s'ensuit que $l_\lambda(b_\lambda a_\lambda)^{-1}c_\lambda$ est un idempotent.

5. Supposons $\lambda \geq \mu$. On a par la question d) :

$$\mathrm{Hom}_{\mathfrak{S}_n}(V_\lambda, V_\mu) = \mathrm{Hom}_{\mathfrak{S}_n}(\mathbb{C}[\mathfrak{S}_n]c_\lambda, \mathbb{C}[\mathfrak{S}_n]c_\mu) \simeq c_\lambda \mathbb{C}[\mathfrak{S}_n]c_\mu\,.$$

Si on a $\lambda > \mu$, cet espace est nul par la question c). Dans le cas $\lambda = \mu$, l'espace est de dimension 1 par la question b). De ce fait, on sait que les V_λ sont irréductibles et que V_λ et V_μ sont isomorphes si et seulement si $\lambda = \mu$. Enfin, il y a autant de classes de conjugaison dans $\mathfrak{S}_n$ que de partitions de n, ce qui permet de conclure.

Exercice 11 : $\star\star\star$

On garde les notations de l'exercice précédent. Soit U_λ la représentation $\mathrm{Ind}_{P_\lambda}^{\mathfrak{S}_n} \mathbb{C}$.

a) Montrer que la représentation obtenue par multiplication à gauche sur $\mathbb{C}[\mathfrak{S}_n]a_\lambda$ est isomorphe à U_λ.

b) Montrer la décomposition $U_\lambda = \bigoplus_{\mu \geq \lambda} K_{\mu\lambda} V_\mu$, où les $K_{\mu\lambda}$ sont des entiers naturels avec $K_{\lambda\lambda} = 1$.

Les entiers $K_{\mu\lambda}$ sont appelés *nombres de Kostka*.

On définit les ensembles suivants, qui correspondent à ajouter ou enlever une case sur le tableau de Young T_λ :

$$A(\lambda) = \{\nu \text{ partition de } n+1 \mid \exists j,\, \forall i,\, \nu_i = \lambda_i + \delta_{ij}\},$$

$$R(\lambda) = \{\nu \text{ partition de } n-1 \mid \exists j,\, \forall i,\, \nu_i = \lambda_i - \delta_{ij}\}.$$

c) Montrer que V_λ est isomorphe à $\bigoplus_{\nu \in R(\lambda)} V_\nu$ en tant que $\mathfrak{S}_{n-1}$-représentation.

d) Montrer que $\mathrm{Ind}_{\mathfrak{S}_{n-1}}^{\mathfrak{S}_n} V_\nu \simeq \bigoplus_{\lambda \in A(\nu)} V_\lambda$ est un isomorphisme de $\mathfrak{S}_n$-représentations.

Solution de l'exercice 11.

a) Soit V une représentation irréductible de $\mathfrak{S}_n$. Par réciprocité de Frobenius (voir exercice 5), on a

$$\mathrm{Hom}_{\mathfrak{S}_n}(U_\lambda, V) \simeq \mathrm{Hom}_{P_\lambda}(\mathrm{id}, V)\,.$$

De plus, $\mathbb{C}[P_\lambda]a_\lambda$ est isomorphe à la P_λ-représentation triviale puisque pour tout $p \in P_\lambda$, on a $pa_\lambda = a_\lambda$. Enfin, le dernier isomorphisme provient des propriétés du produit scalaire :

$$\mathrm{Hom}_{\mathfrak{S}_n}(U_\lambda, V) \simeq \mathrm{Hom}_{P_\lambda}(\mathbb{C}[P_\lambda]a_\lambda, V) \simeq \mathrm{Hom}_{\mathfrak{S}_n}(\mathbb{C}[\mathfrak{S}_n]a_\lambda, V)\,.$$

b) On a

$$\mathrm{Hom}_{\mathfrak{S}_n}(U_\lambda, V_\mu) = \mathrm{Hom}_{\mathfrak{S}_n}(\mathbb{C}[\mathfrak{S}_n]a_\lambda, \mathbb{C}[\mathfrak{S}_n]c_\mu) \simeq a_\lambda \mathbb{C}[\mathfrak{S}_n]c_\mu\,.$$

Ce dernier est nul dans le cas $\lambda < \mu$ et est de dimension 1 si $\lambda = \mu$.

c) Soit ν une partition de $n-1$. Toute injection $\iota : \mathfrak{S}_{n-1} \hookrightarrow \mathfrak{S}_n$ se prolonge linéairement en $\iota : \mathbb{C}[\mathfrak{S}_{n-1}] \hookrightarrow \mathbb{C}[\mathfrak{S}_n]$ et munit V_λ d'une structure de représentation de $\mathfrak{S}_{n-1}$. On a par la question d) de l'exercice 10 :

$$\mathrm{Hom}_{\mathfrak{S}_{n-1}}(V_\nu, V_\lambda) = \mathrm{Hom}_{\mathfrak{S}_{n-1}}(\mathbb{C}[\mathfrak{S}_{n-1}]c_\nu, \mathbb{C}[\mathfrak{S}_n]c_\lambda) \simeq \iota(c_\nu)\mathbb{C}[\mathfrak{S}_n]c_\lambda\,.$$

En choisissant ι correspondant à l'inclusion canonique de $\{1, 2, \ldots, n-1\}$ dans $\{1, 2, \ldots, n\}$, on obtient la condition $\nu_i \leq \lambda_i$ pour tout i pour que cet espace de morphismes soit non nul. Autrement dit, il est nécessaire d'avoir $\nu \in R(\lambda)$.

Réciproquement, soit $\nu \in R(\lambda)$. Si σ désigne le n-cycle $(1\ 2\ \cdots\ n)$, alors on a $\mathfrak{S}_n = \bigoplus_{k=0}^{n-1} \mathfrak{S}_{n-1}\sigma^k$. On a ainsi

$$\mathrm{Hom}_{\mathfrak{S}_{n-1}}(V_\nu, V_\lambda) = \bigoplus_{k=0}^{n-1} \mathrm{Hom}_{\mathfrak{S}_{n-1}}(\mathbb{C}[\mathfrak{S}_{n-1}]c_\nu, \mathbb{C}[\mathfrak{S}_{n-1}]\sigma^k c_\lambda)\,.$$

Un seul de ces termes est non nul, de dimension 1, et si n_0 est la case enlevée de λ pour obtenir ν, alors cela correspond au terme $k = n - n_0$.

d) La réciprocité de Frobenius (voir exercice 5) nous donne

$$\mathrm{Hom}_{\mathfrak{S}_n}(\mathrm{Ind}_{\mathfrak{S}_{n-1}}^{\mathfrak{S}_n} V_\nu, V_\lambda) \simeq \mathrm{Hom}_{\mathfrak{S}_{n-1}}(V_\nu, V_\lambda)$$

et le résultat résulte de la question précédente.

Exercice 12 : (Théorème de Burnside) $\star\star\star$

Soient p, q deux nombres premiers, $\alpha, \beta \in \mathbb{N}$. Soit G groupe fini tel que $|G| = p^\alpha q^\beta$. L'objectif de l'exercice est de montrer que G est résoluble.

a) Soient $\zeta_1, \ldots, \zeta_n \in \mathbb{C}$ des racines de l'unité. Montrer que $\frac{\zeta_1+\cdots+\zeta_n}{n}$ est un entier algébrique si et seulement si $\zeta_1 + \cdots + \zeta_n = 0$ ou $\zeta_i = \zeta_1$ pour tout i.

b) Soit H un groupe fini, ρ une représentation irréductible de H sur $\mathbb{C}$, de caractère χ.

i) Montrer que pour tout $h \in H$, si $c(h)$ désigne le cardinal de la classe de conjugaison de h dans H, alors $c(h)\frac{\chi(h)}{\chi(1)}$ est un entier algébrique.

ii) Montrer que pour tout $h \in H$, si $c(h)$ est premier avec $\chi(1)$, alors $\frac{\chi(h)}{\chi(1)}$ est un entier algébrique.

iii) Sous les hypothèses de la question b)ii), montrer que si $\chi(h) \neq 0$, alors $\rho(h)$ est une homothétie.

c) Soit $h \in H$ tel que $c(h)$ soit une puissance d'un nombre premier. En considérant la représentation régulière de H, montrer que G contient un sous-groupe strict distingué N tel que l'image de h dans H/N soit centrale dans H/N.

d) Montrer par récurrence que G est résoluble.

Solution de l'exercice 12.

a) Rappelons que si $\alpha \in \mathbb{C}$ est un nombre algébrique (i.e. la racine d'un polynôme de $\mathbb{Q}[X]$), on appelle conjugués de α les racines du polynôme minimal de α dans $\mathbb{Q}[X]$. On montre d'abord le résultat suivant : si α et β sont deux nombres algébriques, alors $\alpha+\beta$ est un nombre algébrique et les conjugués de $\alpha + \beta$ sont de la forme $\alpha' + \beta'$, où α' et β' sont des conjugués de α et β respectivement. Par hypothèse, α et β sont algébriques de polynômes minimaux respectifs P et Q : les racines de P (resp. Q) sont exactement les conjugués de α (resp. β). On introduit les matrices compagnons A et B associées aux polynômes P et Q : ce sont des matrices à coefficients dans $\mathbb{Q}$ dont les polynômes caractéristiques sont exactement P et Q. On considère alors la matrice $C := A \otimes I + I \otimes B$. C'est une matrice à coefficients dans $\mathbb{Q}$ dont les valeurs propres sont exactement les sommes d'un conjugué de α et d'un conjugué de β. Donc $\alpha+\beta$ est algébrique et son polynôme minimal divise le polynôme caractéristique de C, donc les conjugués de $\alpha + \beta$ sont des valeurs propres de C, donc de la forme souhaitée.

Répondons maintenant à la question a). On note $\alpha := \frac{\zeta_1+\cdots+\zeta_n}{n}$ et supposons que α est un entier algébrique. Ce qui précède assure que les conjugués de α sont également de la forme $\alpha' = \frac{\zeta_1'+\cdots+\zeta_n'}{n}$, avec ζ_i' racine de l'unité pour tout i. Par conséquent, tout conjugué de α est un nombre complexe de module ≤ 1. Si les ζ_i ne sont pas tous égaux, alors l'inégalité triangulaire assure que $|\alpha| < 1$, et par conséquent le produit des conjugués de α est de module < 1 ; or ce produit est, au signe près, le coefficient constant du polynôme minimal P de α dans $\mathbb{Q}[X]$; comme α est une entier algébrique, P est à coefficients entiers, donc son coefficient constant est un entier de valeur absolue < 1, il est donc nul ; donc $P = X$ par irréductibilité, donc $\alpha = 0$.

On a bien montré que si α était un entier algébrique, alors $\alpha = 0$ ou $\zeta_i = \zeta_1$ pour tout i.

La récipoque est évidente.

b) i) Voir cours, lemme IV.3.5.

ii) Les entiers $c(h)$ et $\chi(1)$ sont premiers entre eux, donc le théorème de Bézout assure qu'il existe des entiers $a, b \in \mathbb{Z}$ tels que $ac(h) + b\chi(1) = 1$. En multipliant par $\frac{\chi(h)}{\chi(1)}$, on obtient

$$ac(h)\frac{\chi(h)}{\chi(1)} + b\chi(h) = \frac{\chi(h)}{\chi(1)}\,.$$

Or la question b)i) assure que $c(h)\frac{\chi(h)}{\chi(1)}$ est un entier algébrique, et $\chi(h)$ est un entier algébrique (c'est une somme de racines de l'unité), donc comme l'ensemble des entiers algébriques est un sous-anneau de $\mathbb{C}$, on déduit de la formule précédente que $\frac{\chi(h)}{\chi(1)}$ est un entier algébrique.

iii) Si on note $n = \rho(1)$ la dimension de la représentation ρ, on sait que $\alpha := \frac{\chi(h)}{\chi(1)} = \frac{\zeta_1+\cdots+\zeta_n}{n}$, où les ζ_i sont des racines de l'unité qui sont les valeurs propres de $\rho(h)$. La question b)ii) assure que α est un entier algébrique, qui est non nul par hypothèse, donc la question b)i) assure que $\zeta_i = \zeta_1$ pour tout i, donc $\rho(h)$ est diagonalisable avec toutes ses valeurs propres égales à ζ_1, donc $\rho(h) = \zeta_1 \mathrm{id}$, donc $\rho(h)$ est une homothétie.

c) Si $h = 1$, le résultat est évident en prenant $N = \{1\}$. Supposons désormais $h \neq 1$. On note ρ_H la représentation régulière de H. On sait que $\chi_H(h) = 0$ car $h \neq 1$, ot $\chi_H = \sum_\chi n_\chi \chi$, où χ décrit les caractères irréductibles de H et $n_\chi = \dim(\chi) = \chi(1)$. On a donc $\sum_\chi \chi(1)\chi(h) = 0$, donc $\sum_{\chi\neq\mathrm{triv}} \chi(1)\chi(h) = -1$, donc

$$\sum_{\chi\neq\mathrm{triv}} \frac{\chi(1)\chi(h)}{p} = -\frac{1}{p}\,.$$

Comme $-\frac{1}{p}$ n'est pas un entier algébrique, il existe $\chi \neq$ triv (dont on note ρ la représentation correspondante) tel que $\frac{\chi(1)\chi(h)}{p}$ n'est pas un entier algébrique. En particulier, on a $\chi(h) \neq 0$ et p ne divise pas $\chi(1) = \dim(\chi)$. Donc les entiers $c(h)$ et $\chi(1)$ sont premiers entre eux. Alors la question b)iii) assure que $\rho(h)$ est une homothétie. On définit alors $N := \mathrm{Ker}(\rho)$ qui est un sous-groupe distingué de G, distinct de G car $\chi \neq$ triv. Or $\rho(h)$ est une homothétie, donc $\rho(h)$ est central dans le groupe linéaire de ρ, donc $\rho(h)$ est central dans l'image de G dans ce groupe, donc l'image de h est centrale dans G/N.

d) On raisonne par récurrence sur $|G|$. Un groupe dont le cardinal est un puissance d'un nombre premier est nilpotent, donc résoluble. On peut donc supposer que $\alpha, \beta \geq 1$.

Écrivons l'équation aux classes pour l'action de G sur lui-même par conjugaison : on a $|G| = 1+\sum_{\overline{h}\neq 1\in G/\mathrm{conj}} c(h)$. Réduisons cette égalité modulo q : on obtient $1+\sum_{\overline{h}\neq 1\in G/\mathrm{conj}} c(h) \equiv 0\,[q]$. Par conséquent, il existe $h \in G$ tel que q ne divise pas $c(h)$.

Or $c(h)$ divise $|G|$, donc $c(h)$ est une puissance de p.

Alors la question c) assure qu'il existe un sous-groupe distingué strict $N \subset G$ tel que l'image de h dans G/N soit centrale dans G/N. On a alors deux cas :

— si $N \neq \{1\}$, on applique l'hypothèse de récurrence aux groupes N et G/N qui sont de cardinal divisant strictement celui de G, donc ils sont résolubles, donc G est résoluble.

— si $N = \{1\}$, alors $h \in Z(G)$, donc $Z(G) \neq \{1\}$, donc on peut appliquer l'hypothèse de récurrence aux groupes $Z(G)$ et $G/Z(G)$, qui sont donc résolubles, donc G est résoluble.