LE GROUPE DES ISOMÉTRIES DU CUBE

Table des matières

1. MISE EN PLACE

Soit C un cube dans l'espace affine euclidien E, de sommets a,b,c,d,e,f,g et h. On désigne précisément par C l'*enveloppe convexe* de ces huit points. Pour donner une définition encore plus précise, on peut dire que l'on considère quatre points coplanaires a,b,c,d constituant les sommets d'un carré — i.e., *abcd* est un parallélogramme, $(ab) \perp (bc)$ et $ab = bc$ — puis on définit e,f,g et h comme les images de a,b,c et d respectivement par une translation de vecteur $\mathbf{n}$, normal au plan (abc) et de norme ab. [Faire un dessin]

Les quatre droites $(ag),(bh),(ce)$ et (df) sont sécantes. Pour le justifier, il suffit de considérer le centre ω du carré *abcd* et de poser $o = \omega + \frac{1}{2}\mathbf{n}$; en vertu du théorème de Thalès appliqué dans les triangles acg, bdf, *cae* et *bdh*, le point o est le milieu de chacun des segments $[ag],[bh],[ce]$ et $[df]$.

La symétrie de centre o préserve l'ensemble $\mathscr{S}$ des sommets de C, donc préserve également leur enveloppe convexe C puisqu'il s'agit d'une application affine.

On vérifie aisément que C est l'ensemble des points de l'espace dont les coordonnées (x,y,z) dans le repère orthogonal $\mathscr{R} = \left(o; \frac{1}{2}\overrightarrow{ab}, \frac{1}{2}\overrightarrow{bc}, -\frac{1}{2}\mathbf{n}\right)$ satisfont à la condition suivante :

$$\max(|x|,|y|,|z|) = 1.$$

Les sommets sont caractérisés par la condition $|x| = |y| = |z| = 1$. Au passage, on pourra remarquer que cela fournit une autre manière de définir un cube : il suffit de choisir un repère orthogonal de E et de considérer l'enveloppe convexe des huit points de coordonnées $(\pm 1, \pm 1, \pm 1)$.

2. Isométries préservant le cube et isométries préservant les sommets

Soit f une isométrie de l'espace E. Si f préserve l'ensemble $\mathscr{S}$ des sommets de C, i.e., $f(\mathscr{S}) = \mathscr{S}$, alors f préserve nécessairement leur enveloppe convexe C puisqu'il s'agit d'une application affine ; on a donc $f(\mathrm{C}) = \mathrm{C}$.

Il est légèrement plus délicat de démontrer l'assertion réciproque : toute isométrie f de E conservant C préserve nécessairement l'ensemble $\mathscr{S}$ des sommets de C. Pour ce faire, nous devons mettre en évidence une propriété caractéristique des sommets de C qui soit invariante par isométrie. Un peu de réflexion montre que l'on peut adopter la caractérisation suivante des sommets : pour qu'un point p de C soit dans $\mathscr{S}$, il faut et il suffit qu'il existe un point $q \in \mathrm{C}$ tel que $pq = \sqrt{3}ab$. En effet :

- si p est un sommet, on peut prendre pour q le sommet opposé, symétrique de p par rapport à o ;
- si réciproquement p et q sont deux points de C tels que $pq = \sqrt{3}ab$, leurs coordonnées respectives (x,y,z) et (x',y',z') sont telles que

$$\frac{1}{4}[(x'-x)^2 + (y'-y)^2 + (z'-z)^2]ab^2 = pq^2 = 3ab^2,$$

soit encore

$$(x'-x)^2 + (y'-y)^2 + (z'-z)^2 = 12.$$

Vu les conditions $\max(|x|,|y|,|z|) = \max(|x'|,|y'|,|z'|) = 1$, on a $|x-x'|, |y-y'|, |z-z'| \leqslant 2$ et l'égalité précédente est possible si et seulement si $|x'-x| = |y'-y| = |z'-z| = 2$, ce qui implique $|x| = |y| = |z| = |x'| = |y'| = |z'| = 1$ et montre que p et q sont deux sommets opposés.

Ainsi, le groupe des isométries du cube C est le sous-groupe

$$\mathrm{G} = \{f \in \mathrm{Isom(E)} \mid f(\mathrm{C}) = \mathrm{C}\} = \{f \in \mathrm{Isom(E)} \mid f(\mathscr{S}) = \mathscr{S}\}$$

du groupe $\mathrm{Isom(E)}$ des isométries de l'espace. Tout élément f de G fixe le point o car celui-ci est l'isobarycentre des points de $\mathscr{S}$; par suite, chaque élément de G est de l'un des trois types suivants :

(i) rotation (déplacement)
(ii) réflexion (anti-déplacement)
(iii) anti-rotation (anti-déplacement)

3. Complément : les symétries affines du cube

Nous avons utilisé une caractérisation des sommets de C reposant sur un argument de distance, donc utilisant la structure euclidienne. Il est intéressant d'observer que l'on peut également donner une caractérisation purement affine. On aimerait transcrire sous une forme mathématique précise l'idée intuitive que les sommets du cube C sont des points « saillants » ; un peu de réflexion conduit à dégager la condition suivante :

pour qu'un point p de C *soit un sommet, il faut et il suffit qu'il existe un plan* H *tel que*
(a) $\mathrm{H} \cap \mathrm{C} = \{p\}$ *;*
(b) C *est entièrement contenu dans l'un des deux demi-espaces fermés de frontière* H.

Démontration. Si p est un sommet de C, le plan H passant par p et perpendiculaire à la diagonale de C issue de p satisfait aux deux conditions précédentes. En effet, si q est le symétrique de p par rapport à o, les deux demi-espaces de frontière H sont

$$\{m \in \mathrm{E} \mid \overrightarrow{pm} \cdot \overrightarrow{pq} \leqslant 0\} \text{ et } \{m \in \mathrm{E} \mid \overrightarrow{pm} \cdot \overrightarrow{pq} \geqslant 0\}.$$

Tous les points de $\mathscr{S}$ sont contenus dans le même demi-espace car $\overrightarrow{ps} \cdot \overrightarrow{pq} > 0$ pour tout sommet s de C distinct de p ; ce demi-espace étant convexe, il contient intégralement l'enveloppe convexe C de $\mathscr{S}$. Il est en outre clair que $\mathrm{H} \cap \mathrm{C}$ est réduit au point p.

Supposons réciproquement que H soit un plan contenant un unique point p de C et tel que C soit entièrement contenu dans le même demi-espace de frontière H. Considérons une forme affine $\varphi : \mathrm{E} \to \mathbb{R}$ telle que $\mathrm{H} = \{m \in \mathrm{E} \mid \varphi(m) = 0\}$; les deux demi-espaces fermés de frontière H sont

$$\{m \in \mathrm{E} \mid \varphi(m) \leqslant 0\} \text{ et } \{m \in \mathrm{E} \mid \varphi(m) \geqslant 0\}.$$

Quitte à replacer φ par $-\varphi$, on peut supposer $\mathrm{C} \subset \{m \in \mathrm{E} \mid \varphi(m) \leqslant 0\}$. Dans le repère $\mathscr{R}$ introduit plus haut, $\varphi(x,y,z) = \alpha x + \beta y + \gamma z + \delta$ avec $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ et $(\alpha, \beta, \gamma) \neq (0,0,0)$. Notant (x_0, y_0, z_0) les coordonnées du point p dans $\mathscr{R}$, on a par hypothèse $\alpha x_0 + \beta y_0 + \gamma z_0 + \delta = 0$. Si p n'est pas un sommet de C, alors l'une de ses coordonnées est de valeur absolue < 1 ; supposons pour fixer les idées que ce soit x_0. Pour tout nombre réel $\varepsilon \in]-(1-|x_0|), 1-|x_0|[$, le point de coordonnées $(x_0+\varepsilon, y_0, z_0)$ appartient à C car $|x_0+\varepsilon| \leqslant 1$; on a par conséquent $\alpha\varepsilon = \varphi(x_0+\varepsilon, y_0, z_0) \leqslant 0$ pour tout $\varepsilon \in]-(1-|x_0|), 1-|x_0|[$, ce qui implique $\alpha = 0$. Quel que soit $\varepsilon \in]-(1-|x_0|), 1-|x_0|[$, on obtient par suite $\varphi(x_0+\varepsilon, y_0, z_0) = \alpha\varepsilon = 0$, c'est-à dire $(x_0+\varepsilon, y_0, z_0) \in \mathrm{H}$; comme $(x_0+\varepsilon, y_0, z_0) \in \mathrm{C}$, ceci contredit l'hypothèse $\mathrm{H} \cap \mathrm{C} = \{p\}$. □

Nous venons de mettre en évidence une caractérisation purement *affine* des sommets. Il en découle immédiatement que toute *bijection affine* f de E (non nécessairement isométrique) préservant le cube C préserve également l'ensemble $\mathscr{S}$ de ses sommets : étant donné $p \in \mathscr{S}$, on choisit un plan H n'intersectant C qu'en p et tel que C soit entièrement contenu dans le même demi-espace fermé E^+ de frontière H ; puisque f est une bijection affine, $f(\mathrm{H})$ est un plan, $f(\mathrm{H}) \cap \mathrm{C} = f(\mathrm{H}) \cap f(\mathrm{C}) = f(\mathrm{H} \cap \mathrm{C}) = \{f(p)\}$ et $f(\mathrm{E}^+)$ est un demi-espace fermé de frontière $f(\mathrm{H})$ contenant entièrement $\mathrm{C} = f(\mathrm{C})$; ces trois conditions garantissent que le point $f(p)$ est un sommet de C.

Remarque. En s'inspirant du raisonnement précédent, il n'est pas difficile de donner une caractérisation affine des *arêtes* (resp. des faces) du cube C : ce sont précisément les parties de C de la forme $\mathrm{H} \cap \mathrm{C}$, où H est un plan contenant exactement deux (resp. quatre) sommets de C et tel que l'un des deux demi-espaces fermés de frontière H contienne entièrement C. Il en découle que toute bijection affine de l'espace préservant C transforme une arête (resp. une face) en une arête (resp. une face).

Nous pouvons en tirer une conséquence remarquable : *toute bijection affine de* E *préservant le cube* C *est une isométrie*. Considérons en effet une telle bijection affine f ; puisque f préserve les sommets et les arêtes du cube, l'image par f du repère $(a; \overrightarrow{ab}, \overrightarrow{ad}, \overrightarrow{ae})$ est de la forme $(p; \overrightarrow{pq}, \overrightarrow{pr}, \overrightarrow{ps})$, où $p, q, r, s \in \mathscr{S}$ sont des sommets tels que $[pq], [pr]$ et $[ps]$ soient des arêtes ; un tel repère est orthogonal et $pq = pr = ps = ab = ad = ae$, donc f est une isométrie.

4. Action sur les diagonales

Rappelons que l'on désigne par G le groupe des isométries de l'espace préservant le cube C. Comme chaque élément f de G tranforme un sommet en un sommet tout en préservant les distance, f transforme une diagonale en une diagonale. Soit $\Delta = \{(ag), (bh), (ce), (df)\}$ l'ensemble des quatre diagonales du cube et soit $\mathfrak{S}(\Delta)$ le groupe des permutations de cet ensemble. Chaque isométrie $f \in \mathrm{G}$ donne naissance à une permuation $\sigma_f \in \mathfrak{S}(\Delta)$ via la formule $\sigma_f(pq) = f(pq) = (f(p)f(q))$. L'application

$$\pi : \mathrm{G} \to \mathfrak{S}(\Delta), \quad f \mapsto \sigma_f$$

ainsi définie est un homomorphisme de groupes :

$$\sigma_{g\circ g}(pq) = (g(f(p))g(f(q))) = \sigma_g(f(p)f(q)) = \sigma_g(\sigma_f(pq))$$

donc

$$\sigma_{g\circ f} = \sigma_g \circ \sigma_f$$

pour tous $f, g \in \mathrm{G}$.

Remarque. Si l'on veut, on peut commencer par fixer une bijection $\nu : \{1,2,3,4\} \to \Delta$ et l'utiliser pour identifier le groupe $\mathfrak{S}(\Delta)$ avec le groupe symétrique standard $\mathfrak{S}_4$ via l'isomorphisme

$$\mathfrak{S}(\Delta) \to \mathfrak{S}_4, \quad \sigma \mapsto \nu^{-1} \circ \sigma \circ \nu.$$

L'application π est *surjective*. Pour le démontrer, on observe que son image $\pi(\mathrm{G})$ est un sous-groupe de $\mathfrak{S}(\Delta)$; par suite, il suffit de vérifier que $\pi(\mathrm{G})$ contient un ensemble de générateurs de $\mathfrak{S}(\Delta)$ pour en déduire $\pi(\mathrm{G}) = \mathfrak{S}(\Delta)$. On sait que le groupe $\mathfrak{S}(\Delta)$ est engendré par les six transpositions, permutations qui échangent deux éléments en fixant les deux autres. Pour chaque transposition τ, on trouve sans difficulté une isométrie f dans G telle que $\tau = \pi(f)$: étant données deux diagonales D et D′ de C, la réflexion par rapport au plan contenant les deux autres est une isométrie préservant C et induisant la transposition échangeant D et D′. Par exemple, pour $\mathrm{D} = (ag)$ et $\mathrm{D}' = (bh)$, la réflexion par rapport au plan (cde) convient.

Déterminons enfin le noyau H de π, c'est-à-dire le sous-groupe de G constitué des isométries f telles que $\pi(f)$ soit l'identité ; cela signifie que f préserve globalement chaque diagonale du cube. Étant donné $f \in \mathrm{H}$, on a $f(a) = a$ ou $f(a) = g$, $f(b) = b$ ou $f(b) = h$ et $f(c) = c$ ou $f(c) = e$.

Si $f(a) = a$, alors $f(b) \in \{b, d, e\}$ car f préserve les arêtes ; on en déduit $f(b) = b$. Appliquant le même raisonnement avec le sommet b, on obtient ensuite $f(c) = c$. Comme $f(o) = o$, les quatre points non coplanaires a, b, c, o sont ainsi fixés et f est donc l'identité.

Si $f(a) = g$, un raisonnement analogue au précédent montre qu'alors f est la symétrie s_o de centre o. Une variante consiste à observer que s_o préserve globalement chaque diagonale de C et appartient donc à H ; $s_o \circ f$ est alors un élément de H fixant le sommet a, d'où $s_o \circ f = \mathrm{id}$ et $f = s_o$.

Finalement, $\mathrm{H} = \{\mathrm{id}, s_o\}$ est le sous-groupe de G d'ordre 2 engendré par la symétrie de centre o. Par passage au quotient, l'homomorphisme surjectif π induit un *isomorphisme* entre le groupe quotient G/H et le groupe $\mathfrak{S}(\Delta)$. On en déduit que ces deux groupes ont le même ordre

$$|\mathrm{G}/\mathrm{H}| = |\mathfrak{S}(\Delta)| = 4! = 24,$$

ce qui montre finalement que G est un groupe fini d'ordre

$$|\mathrm{G}| = |\mathrm{H}|.|\mathrm{G}/\mathrm{H}| = 48.$$

Remarque. La section 7 est dévolue aux propriétés élémentaires de la notion de quotient.

5. Description des isométries préservant le cube

Maintenant que nous savons que le groupe G est fini et contient 48 éléments, nous pouvons essayer d'en faire la liste. L'ensemble des déplacements (isométries directes) préservant C est un sous-groupe de G, noté G^+. L'inclusion $\mathrm{G}^+ \subset \mathrm{G}$ est stricte car G contient des anti-déplacements, par exemple la réflexion σ par rapport au plan médiateur du segment $[ab]$. L'application

$$\mathrm{G}^+ \to \mathrm{G}, \quad f \mapsto \sigma \circ f$$

est injective et son image est précisément l'ensemble G^- des anti-déplacements de G ; on a donc

$$|\mathrm{G}^+| = |\mathrm{G}^-| = \frac{1}{2}|\mathrm{G}| = 24.$$

Comme tous les éléments de G fixent le point o, les déplacements constituant G^+ sont tous des rotations de centre o. Les plus évidentes sont probablement les rotations autour d'un axe passant par les milieux de deux faces opposées, l'angle d'une telle rotation r étant de mesure $\frac{\pi}{4}, \frac{\pi}{2}$ ou $\frac{3\pi}{4}$ si $r \neq \mathrm{id}$. Comme C possède trois paires de faces opposées, nous obtenons ainsi 9 rotations dans $\mathrm{G}^+ - \{\mathrm{id}\}$. Il y a ensuite les rotations autour de l'une des quatre diagonales du cube, d'angle de mesure $\frac{2\pi}{3}$ ou $\frac{4\pi}{3}$; cela donne 8 nouveaux éléments dans $\mathrm{G}^+ - \{\mathrm{id}\}$. Il y a enfin les retournements (rotations d'angle plat) autour d'un axe passant par les milieux de deux arêtes opposées de C ; comme C possède six paires d'arêtes opposées, cela fournit encore 6 éléments dans $\mathrm{G}^+ - \{\mathrm{id}\}$. Il n'y a pas de place pour autre chose : $1 + 9 + 8 + 6 = 24$.

Les éléments de G^- sont *a priori* de deux types : réflexions et anti-rotations (composé commutatif d'une rotation r et d'une réflexion s par rapport à un plan perpendiculaire à l'axe de r).

Commençons par énumérer les réflexions. Il y a de manière évidente :

(i) les réflexions par rapport à l'un des trois plans médiateurs des arêtes, ne fixant aucun sommet ;

(ii) les réflexions par rapport à l'un des six plans contenant deux arêtes opposées, qui fixent quatre des huit sommets.

On constate aisément que cette liste est complète en analysant les images possibles du sommet a par une réflexion de G^-. Il y a donc 9 réflexions dans G^-.

Passons maintenant aux anti-rotations. Étant données une rotation non triviale $r \in G^+$ et une réflexion $s \in G^-$ telles que l'axe de r soit perpendiculaire au plan de s, $r \circ s = s \circ r$ est une anti-rotation dans G^-. Remarque préliminaire : si l'angle de r est plat, alors $s \circ r$ est la symétrie de centre le point d'intersection de l'axe de r et du plan de s.

(i) Première configuration : r est un retournement dont l'axe passe par les milieux de deux faces opposées et s est la réflexion par rapport au plan médiateur des arêtes perpendiculaires à ces deux faces. Tous les cas de figure conduisent au même résultat : la symétrie de centre o.

(ii) Première configuration (bis) : r est un retournement dont l'axe passe par les milieux de deux arêtes opposées et s est la réflexion par rapport au plan passant par les quatre sommets restant. On obtient de nouveau s_o.

(iii) Deuxième configuration : r n'est pas un retournement, son axe passe par les milieux de deux faces opposées et s est la réflexion par rapport au plan médiateur des arêtes perpendiculaires à ces faces. Il y a 6 anti-rotations de ce type.

Il manque $15-7=8$ anti-rotations...

Nous n'avons pas utilisé jusqu'ici les 8 rotations r autour des diagonales car il n'existe pas de réflexion $s \in G^-$ telle que $s \circ r$ appartienne à G : il faudrait en effet que s soit une réflexion par rapport au plan médiateur d'une diagonale, or celle-ci ne préserve pas C. Pour fixer les idées, considérons la diagonale (ag) ; le plan médiateur P du segment $[ag]$ passe par o et est parallèle aux plans (bde) et (cfh). La rotation r' d'axe (ag) et d'angle de mesure $\frac{\pi}{3}$ (relativement à l'orientation faisant de (bde) un triangle direct) transforme (bde) en le triangle symétrique par rapport à (ab) ; si l'on applique alors la réflexion s' par rapport à P, on obtient le triangle (chf). Il est maintenant clair que $r' \circ s'$ est une anti-rotation préservant C et d'axe (ab). Pour s'en convaincre, il suffit d'observer la projection orthogonale de C sur le plan P...

L'inverse $(r' \circ s')^{-1} = s' \circ r'^{-1} = r'^{-1} \circ s'$ de $r' \circ s'$ est également une anti-rotation d'axe (ag) préservant C. Remplaçant (ag) par l'une des trois autres diagonales, on obtient de la sorte 8 nouvelles anti-rotations dans G^-. Cette fois, $1+6+8=15$ et le compte y est.

6. Structure du groupe des isométries du cube

Revenons à l'homomorphisme $\pi : G \to \mathfrak{S}(\Delta)$ introduit à la section 4, surjectif et de noyau $H = \{\mathrm{id}, s_o\}$. La restriction de π au sous-groupe G^+ des déplacements est un homomorphisme de groupes de noyau $H \cap G^+ = \{\mathrm{id}\}$, donc injectif ; comme par ailleurs $|G^+| = 24 = |\mathfrak{S}(\Delta)|$, il s'agit donc d'un isomorphisme.

Observons que les deux éléments id et s_o de H commutent avec *tous* les éléments de G [(1)]. Il en découle que l'application

$$H \times G^+ \to G, \quad (\varepsilon, f) \mapsto \varepsilon \circ f$$

est un homomorphisme de groupes puisque

$$(\varepsilon \circ f) \circ (\varepsilon' \circ f') = (\varepsilon \circ \varepsilon') \circ (f \circ f')$$

pour tous $\varepsilon, \varepsilon' \in H$ et $f, f' \in G^+$. C'est par ailleurs une application surjective car tout anti-déplacement g dans G s'écrit sous la forme $g = s_o \circ (s_o \circ g)$; les deux groupes étant du même ordre, il s'agit donc d'un isomorphisme.

(1) Quelle que soit l'isométrie f de E, $f \circ s_o \circ f^{-1}$ est la symétrie de centre $s_{f(o)}$. Pour le voir, il suffit d'observer que la partie linéaire de $f \circ s_o \circ f^{-1}$, étant conjuguée à la partie linéaire de s_o, a les mêmes valeurs propres, en l'occurrence -1 avec multiplicité 3 ; cette partie linéaire est donc la symétrie par rapport à l'origine et, comme $f \circ s_o \circ f^{-1}$ fixe le point $f(o)$, il s'agit finalement bien de la symétrie de centre $f(o)$.

La structure du groupe G est ainsi parfaitement comprise : G *est c'est isomorphe au produit direct du groupe* $\mathbb{Z}/2\mathbb{Z}$ *par le groupe symétrique* $\mathfrak{S}_4$. On notera au passage que le groupe G^+ des déplacements préservant le cube C fournit une réalisation géométrique simple du groupe $\mathfrak{S}_4$.

7. Quelques remarques élémentaires sur les quotients

La notion de quotient est parfois la source de difficultés qui n'ont pas lieu d'être...

a) La notion générale de quotient d'un ensemble E par une relation d'équivalence est rigoureusement équivalente à la notion de *partition* d'un ensemble en sous-ensembles deux à deux disjoints. Partant d'une relation d'équivalence $\mathscr{R}$ sur E, celui-ci est la réunion disjointe des classes modulo $\mathscr{R}$; réciproquement, la donnée d'une partition $\mathscr{F}$ de E — c'est-à-dire une famille $\mathscr{F}$ de sous-ensembles de E deux à deux disjoints dont E est la réunion — permet de définir sur cet ensemble une relation d'équivalence $\mathscr{R}_{\mathscr{F}}$: quels que soient x et y dans E, $x\mathscr{R}_{\mathscr{F}}y$ si et seulement si x et y appartiennent au même sous-ensemble dans $\mathscr{F}$.

Exemples standard :

(i) L'égalité est une relation d'équivalence ; elle correspond à la partition de E en singletons : $\mathrm{E} = \bigsqcup_{x\in\mathrm{E}}\{x\}$. À l'opposé, à la partition $\mathscr{F} = \{\mathrm{E}\}$ (un seul sous-ensemble) correspond la relation d'équivalence brutale : pour tous $x,y \in \mathrm{E}$, $x\mathscr{R}_{\mathscr{F}}y$.

(ii) La donnée d'une application $f : \mathrm{E} \to \mathrm{F}$ fournit naturellement une relation d'équivalence $\mathscr{R}_f$ sur E : pour tous $x,y \in \mathrm{E}$, $x\mathscr{R}_f y$ si et seulement si $f(x) = f(y)$. Les classes d'équivalence sont les *fibres* de l'application f ; elles constituent la partition de E correspondant à $\mathscr{R}_f$.

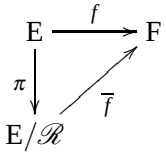
La situation (ii) se rencontre par exemple souvent dans des problèmes de dénombrement. Si E et F sont finis, on peut calculer le cardinal de |E| en comptant d'abord le nombre d'éléments de F, puis en déterminant le nombre d'antécédents de chacun d'entre eux, c'est-à-dire le cardinal de la fibre de f correspondante :

$$|\mathrm{E}| = \sum_{y\in\mathrm{F}} |f^{-1}(y)|,$$

où $|f^{-1}(y)| = |\varnothing| = 0$ si $y \notin f(\mathrm{E})$.

b) Le quotient $\mathrm{E}/\mathscr{R}$ d'un ensemble E par une relation d'équivalence $\mathscr{R}$ est simplement l'ensemble des classes d'équivalence modulo $\mathscr{R}$. On dispose d'une application naturelle $\pi : \mathrm{E} \to \mathrm{E}/\mathscr{R}$, souvent appelée *projection canonique*, associant à x sa classe d'équivalence. Le passage de E à $\mathrm{E}/\mathscr{R}$ a précisément pour effet d'*identifier* tous les éléments équivalents : pour tous $x,y \in \mathrm{E}$, $\pi(x) = \pi(y)$ si et seulement si $x\mathscr{R}y$. Ainsi, remplacer E par $\mathrm{E}/\mathscr{R}$ a pour effet de transformer la relation d'équivalence $\mathscr{R}$ en la relation d'*égalité*.

On peut aussi interpréter la construction de l'ensemble quotient comme suit : *toute relation d'équivalence* $\mathscr{R}$ *sur un ensemble* E *peut se réaliser comme la relation* $\mathscr{R}_f$ *associée à une application* $f : \mathrm{E} \to \mathrm{F}$ *convenable*. Parmi tous les choix possibles de f et F, il y en a un meilleur que les autres : $\mathrm{F} = \mathrm{E}/\mathscr{R}$ et $f = \pi$. En effet, supposons que l'on dispose d'une application $f : \mathrm{E} \to \mathrm{F}$ telle que $\mathscr{R}_f = \mathscr{R}$, c'est-à-dire dont les fibres sont exactement les classes modulo $\mathscr{R}$. Comme f est constante sur chaque classe modulo $\mathscr{R}$, on peut définir une application $\overline{f} : \mathrm{E}/\mathscr{R} \to \mathrm{F}$ en associant à chaque classe c la valeur commune de f en les éléments de f. Par construction, on a l'identité $f = \overline{f} \circ \pi$, laquelle se représente agréablement sous la forme d'un diagramme



que l'on dit *commutatif* : les deux chemins possibles pour aller de E à F, en l'occurrence f et $\overline{f} \circ \pi$, coïncident. Mieux, f prend des valeurs différentes sur des classes différentes puisque les classes sont exactement les fibres de f ; ainsi, $\overline{f}(c) \neq \overline{f}(c')$ si c et c' sont des classes distinctes et $\overline{f}$ est donc une application *injective*.

Du point de vue des valeurs prises dans F, le passage de f à $\overline{f}$ ne change rien et ces deux applications ont donc la même image. Ainsi, en remplaçant E par l'ensemble quotient $\mathrm{E}/\mathscr{R}$ et F par le *sous-ensemble*

$f(\mathrm{E})$, nous avons construit une application *bijective*

$$\overline{f} : \mathrm{E}/\mathscr{R} \to f(\mathrm{E})$$

contenant la même information que f.

c) *Exemple : les angles orientés dans un espace vectoriel euclidien* P *de dimension* 2.

On considère l'ensemble E des couples (u,v) de vecteurs unitaires de P, que l'on munit de la relation d'équivalence

$$(u,v)\mathscr{R}(u',v') \iff \left(\exists f \in \mathrm{SO}(\mathrm{P}) \mid f(u)=u', f(v)=v'\right).$$

Par ailleurs, étant donné un couple $(u,v) \in \mathrm{E}$, on démontre qu'il existe une *unique* rotation $r \in \mathrm{SO}(\mathrm{P})$ telle que $v = r(u)$. On déduit alors de la *commutativité* du groupe $\mathrm{SO}(\mathrm{P})$ que deux couples (u,v) et (u',v') dans E sont équivalents si et seulement si les rotations associées r et r' sont les mêmes. Ainsi, les classes d'équivalence pour $\mathscr{R}$ sont précisément les fibres de l'application $f : \mathrm{E} \to \mathrm{SO}(\mathrm{P})$, définie en associant à (u,v) l'unique rotation r telle que $v = r(u)$. Cette application étant manifestement surjective, elle donne ainsi naissance à une *bijection*

$$\overline{f} : \mathrm{E}/\mathscr{R} \to \mathrm{SO}(\mathrm{P}).$$

On en déduit immédiatement une structure de groupe commutatif sur l'ensemble $\mathrm{E}/\mathscr{R}$: la somme de deux classes $\widehat{(u,v)}$ et $\widehat{(u',v')}$ est définie par la condition

$$\overline{f}\left(\widehat{(u,v)} + \widehat{(u',v')}\right) = \overline{f}(\widehat{(u,v)}) \circ \overline{f}(\widehat{(u',v')}).$$

Pour calculer effectivement $\widehat{(u,v)} + \widehat{(u',v')}$, on note $r = f(u,v)$ la rotation envoyant u sur v, $r' = f(u',v')$ celle envoyant u' sur v' et on pose $w = r'(v)$. Par définition, $\widehat{(u,v)} + \widehat{(u',v')}$ est l'antécédent de $r' \circ r$ dans $\mathrm{E}/\mathscr{R}$. On a d'une part $\widehat{(v,w)} = \widehat{(u',v')}$ — car $f(v,w) = r' = f(u',v')$ — et d'autre part $w = r'(v) = (r' \circ r)(u)$, donc $f(u,w) = r' \circ r$. On obtient ainsi

$$\widehat{(u,v)} + \widehat{(u',v')} = \widehat{(u,v)} + \widehat{(v,w)} = \widehat{(u,w)},$$

ce qui démontre par la même occasion la relation de Chasles.

d) Considérons maintenant un groupe G et soit H un sous-groupe. La classe à droite d'un élément g de G modulo H est l'ensemble produits gh de g par un élément h de H ; on la note $g\mathrm{H}$. Remarquer que l'on obtient la même classe si l'on remplace g par gh avec $h \in \mathrm{H}$. Comme H contient l'élément neutre, $g\mathrm{H}$ contient g et donc G est la réunion de toutes les classes à droite modulo H. Si deux classes $g\mathrm{H}$ et $g'\mathrm{H}$ ont une intersection non vide, elles sont égales : en effet, il existe alors $h, h' \in \mathrm{H}$ tels que $gh = g'h'$ et par suite $g\mathrm{H} = (gh)\mathrm{H} = (g'h')\mathrm{H} = g'\mathrm{H}$. Les classes à droite définissent donc une partition de G ; la relation d'équivalence $\mathscr{R}_{\mathrm{H}}$ correspondante est

$$g\mathscr{R}_{\mathrm{H}}g' \iff g^{-1}g' \in \mathrm{H},$$

qui décrète que deux éléments sont équivalents si l'on peut passer de l'un à l'autre par multiplication à droite par un élément de H. L'ensemble quotient $\mathrm{G}/\mathscr{R}_{\mathrm{H}}$ est noté G/H ; ses éléments sont les classes à droite modulo H.

En privilégiant la gauche, on définit de même les classes à gauche et l'ensemble quotient$\mathrm{H}\backslash\mathrm{G}$, dont les éléments sont les classes à gauche modulo H.

Quel que soit $g \in \mathrm{G}$, la multiplication à droite par g fournit une *bijection* entre H et $g\mathrm{H}$. Lorsque G est *fini*, on en déduit que toutes les classes (à droite ou à gauche) modulo H ont le même cardinal, égal à celui de $|\mathrm{H}|$; le nombre de classes à droite étant le cardinal de l'ensemble $|\mathrm{G}/\mathrm{H}|$, on obtient la formule

$$|\mathrm{G}| = |\mathrm{H}|.|\mathrm{G}/\mathrm{H}|$$

utilisée à la fin de la section 4. On peut encore interpréter différemment cette identité : la projection canonique $\pi : \mathrm{G} \to \mathrm{G}/\mathrm{H}, \quad g \mapsto g\mathrm{H}$ est surjective et ses fibres sont (tautologiquement !) les classes à droite modulo H ; comme toutes ces classes sont de cardinal H, la formule de dénombrement mentionnée à la fin de a) fournit précisément cette identité.

e) Rappelons que les constructions exposées en b) s'adaptent au cadre des groupes. Soit $\varphi : G \to G'$ un homomorphisme de groupes. La relation d'équivalence naturellement associée à φ, soit

$$g\mathscr{R}_\varphi g' \iff \varphi(g) = \varphi(g'),$$

peut se ré-écrire sous la forme

$$g\mathscr{R}_\varphi g' \iff g^{-1}g' \in \mathrm{Ker}(\varphi) \iff g'g^{-1} \in \mathrm{Ker}(\varphi)$$

et donc

(i) les classes à droite modulo le sous-groupe $\mathrm{Ker}(\varphi)$ sont les mêmes que les classes à droite : $g\mathrm{Ker}(\varphi) = \mathrm{Ker}(\varphi)g$;

(ii) les fibres de φ sont donc précisément les classes modulo $\mathrm{Ker}(\varphi)$.

Le point (i) permet de munir l'ensemble quotient $G/\mathscr{R}_\varphi = G/\mathrm{Ker}(\varphi)$ d'une structure de groupe de telle sorte que la projection canonique $\pi : G \to G/\mathrm{Ker}(\varphi)$ devienne un homomorphisme de groupes. On n'a pas le choix : on doit définir le produit des classes $\pi(g)$ et $\pi(g')$ par $\pi(gg')$; pour que cela ait un sens, il faut que tous les $(gh)(g'h')$ soient dans la même classe lorsque h et h' parcourent $\mathrm{Ker}(\varphi)$. Tel est bien le cas : l'identité $\mathrm{Ker}(\varphi)g' = g'\mathrm{Ker}(\varphi)$ permet d'écrire hg' sous la forme $g'h''$ avec $h'' \in \mathrm{Ker}(\varphi)$, donc $(gh)(gh') = g(hg')h' = g(g'h'')h' = (gg')(h''h')$ appartient à $gg'\mathrm{H}$. L'élément neutre est la classe $\pi(e)$ de l'élément neutre et les axiomes des groupes sont automatiquement vérifiés.

Lorsqu'on munit l'ensemble $G/\mathrm{Ker}(\varphi) = G/\mathscr{R}_\varphi$ de la structure de groupe que l'on vient de définir, l'application injective $\overline{\varphi} : G/\mathrm{Ker}(\varphi) \to G'$ construite à la fin de b) devient un homomorphisme de groupes. La conclusion est la même : en remplaçant G par le groupe quotient $G/\mathrm{Ker}(\varphi)$ et G' par le sous-groupe image $\varphi(G)$, on obtient un *isomorphisme de groupes*

$$\overline{\varphi} : G/\mathrm{Ker}(\varphi) \to \varphi(G)$$

contenant la même information que φ.

On dit qu'un sous-groupe H de G est *distingué* si les classes à gauche et à droite coïcident ou, de manière équivalente, si $g\mathrm{H}g^{-1} = \mathrm{H}$ pour tout $g \in G$. Si H est distingué, on peut comme précédemment munir l'ensemble $G/\mathrm{H} = \mathrm{H}\,G$ des classes modulo H d'une structure de groupe de telle sorte que la projection π devienne un homomorphisme de groupes. L'élément neutre de G/H étant la classe H, le noyau de cet homomorphisme n'est autre que H lui-même. Au final, cela montre que *les sous-groupes distingués de* G *sont très précisément ceux que l'on peut réaliser comme le noyau d'un homomorphisme de groupes convenable*.

f) Tout ce que l'on a dit pour les groupes s'applique aux espaces vectoriels sur un corps commutatif k, la multiplication du groupe (resp. les sous-groupes ; resp. les homomorphismes de groupes) étant remplacés par l'addition des vecteurs (resp. les sous-espaces vectoriels ; resp. les applications linéaires). Tous les sous-espaces sont distingués puisque l'addition est commutative.

Étant donné un espace vectoriel V et un sous-espace W, l'espace vectoriel quotient V/W a pour éléments les classes $v + W = W + v$ modulo W et

$$\lambda(v + W) + \mu(v' + W) = (\lambda v + \mu v') + W$$

pour tous $v, v' \in V$ et $\lambda, \mu \in k$.

Il est important d'observer que ces classes ne sont pas autre chose que les *sous-espaces affines* de V de direction W, ce qui permet de visualiser très facilement l'espace vectoriel quotient V/W, au moins si $\dim(V) \leqslant 2$.

Si W' est un supplémentaire de W dans V, alors la restriction de la projection canonique $\pi : V \to V/W$ induit un *isomorphisme* entre W' et V/W' : en effet, $\pi_{|W'}$ est une application linéaire injective — car $\mathrm{Ker}(\pi) \cap W' = W \cap W' = \{0\}$ — et elle est surjective car $\pi(v) = v + W = w' + W = \pi(w')$, où w' est le projeté de v sur W' parallèlement à W.

Réciproquement, si W' est un sous-espace vectoriel de V tel que $\pi_{|W'} : W' \to V/W$ soit un isomorphisme, alors W' est un supplémentaire de W dans V (exercice !). Ainsi, on peut voir le choix d'un supplémentaire de W dans V comme une réalisation de l'espace vectoriel quotient V/W dans V. Parce qu'il n'y a pas de manière naturelle de le faire, i.e., de choix meilleur que les autres, il est souvent plus facile de travailler directement avec V/W...