Essentiel : groupes, sous-groupes et exemples.

Définition d'un groupe.

Un groupe $(G, \star)$ est un ensemble G muni d'une opération binaire $\star$, tel que :
- pour tout $a,b \in G$, $a \star b \in G$. On dit donc que $\star$ est une loi de composition interne.
- pour tout $x,y,z \in G$, $(x \star y) \star z = x \star (y \star z)$. On dit que la loi est associative.
- il existe un élément $e \in G$, tel que pour tout $x \in G$, $x \star e = e \star x = x$. On dit que e est l'élément neutre de G.
- pour tout $x \in G$, il existe $x' \in G$ tel que $x \star x' = x' \star x = e$. On dit que x' est l'inverse de x.

Attention ! Notation …

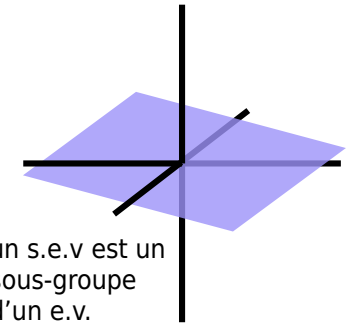
• la définition n'impose pas $a \star b = b \star a$; il n'est pas nécessaire que $\star$ soit commutative. Si c'est le cas, le groupe est dit abélien.
• la loi peut être notée par n'importe quel symbole ; par exemple +, ×, *, • …
• quand on sait de quelle opération on parle, on écrit très souvent seulement G à la place de $(G, \star)$.

Sous-groupe.

Un sous-groupe de $(G, \star)$ est un groupe $(H, \star)$ où H est un sous-ensemble de G. Pour qu'un sous-ensemble H d'un groupe G soit bien un groupe, il suffit de vérifier que $e_G \in H$, et que pour tout $a,b \in H$, $a \star b^{-1} \in H$.

Exemples de sous-groupes.

Pour n un entier, $n\mathbb{Z}$ dénote le groupe formé par l'ensemble des multiples de n. C'est bien sûr un sous-groupe de $\mathbb{Z}$. $\mathbb{R}$ a pour sous-groupes $\mathbb{Q}$, $\mathbb{Z}$, et est lui-même sous-groupe de $\mathbb{C}$. Tout sous-espace vectoriel de $\mathbb{R}^n$ est un sous-groupe de $\mathbb{R}^n$.



un s.e.v est un sous-groupe d'un e.v.

Pour tout groupe G, $\{e_G\}$ et G sont toujours des sous-groupes de G ; ils sont dits sous-groupes triviaux.

Notations courantes.

Assez couramment, la loi du groupe est écrite comme une multiplication ; donc en utilisant ×, ·, ou par rien. L'inverse est donc noté a^{-1}, $a \times \ldots \times a$ est noté a^n. Il arrive aussi que la loi soit écrite comme une addition ; donc avec +, l'inverse noté -a, a+…+a noté na.

… -1 1 … 5

Le groupe $(\mathbb{Z},+)$ et un sous-groupe, $5\mathbb{Z}$.

Ensembles classiques.

De nombreux ensembles donnent des groupes en leur ajoutant comme opération l'addition ou multiplication. Par exemple :
$(\mathbb{Q},+)$, $(\mathbb{Z}^n,+)$, $(\mathbb{R}^n,+)$, $(\mathbb{C},+)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$ …
Remarquons au passage qu'un espace vectoriel est, par définition, un groupe particulier ! Mais au contraire $(\mathbb{Q}^*,+)$, $(\mathbb{Z}^*, \times)$, $(\mathbb{R}, \times)$ ne sont pas des groupes, vu qu'il manque l'élément neutre au premier, et l'inverse d'éléments aux deux autres.

Sous-groupe engendré.

Soit A une partie d'un groupe G. Le sous-groupe engendré par A est le plus petit sous-groupe contenant A. Il est constitué de tout les produits (en notation multiplicative) des éléments de A et de leurs inverses. Si ce sous-groupe est G lui-même, on dit que A est une partie génératrice de G.

Conséquences axiomatiques.

Les 4 axiomes d'un groupe ont deux conséquences importantes : l'élément neutre est unique, et chaque élément n'a qu'un inverse.

- Soit e, f deux éléments neutres. Alors $e = e \cdot f = f$. Donc $e = f$.
- Soit b, c deux inverses de a. Alors $b = b \cdot (a \cdot c) = (b \cdot a) \cdot c = c$. Et donc $b = c$.

Morphisme de groupes

Un morphisme de groupes est une application entre deux groupes qui conserve la structure du . C'est-à-dire : pour deux groupes $(G,\star)$ et $(G',\diamond)$, un morphisme de groupes $f:G\to G'$ doit valider $f(x\star y) = f(x)\diamond f(y)$ pour tout $x,y\in G$.

De cette définition, on peut en déduire que $f(e_G) = e_{G'}$ et $f(a^{-1}) = f(a)^{-1}$.

Type de morphismes.

Comme pour les applications linéaires.
- isomorphisme : morphisme bijectif ;
- endomorphisme : morphisme d'un groupe dans lui-même ($G = G'$) ;
- automorphisme : endomorphisme bijectif.

Image et image réciproque.

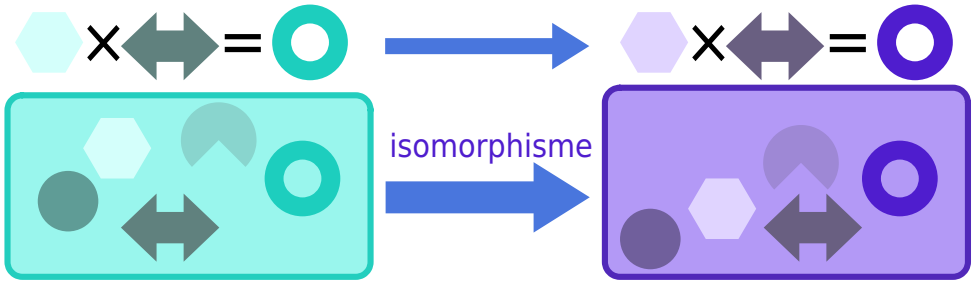
Soit $f:G\to G'$ un morphisme de groupes. L'image d'un sous-groupe de G est un sous-groupe de G', et l'image réciproque d'un sous-groupe de G' est un sous-groupe de G. En particulier, im f est l'image de G, et ker f est l'image réciproque de $\{e_{G'}\}$.

Cas particuliers.

À noter : les applications linéaires sont des exemples de morphismes de groupes (les groupes en question étant de surplus des espaces vectoriels).

Injectivité et surjectivité.

Un morphisme de groupes $f:G\to G'$ est :
- injectif ssi $\ker f = \{e_G\}$;
- surjectif ssi $\mathrm{Im}\, f = G'$.



Suppléments. Cette partie n'est pas demandée.

Sous-groupe normal/distingué.

La notion de sous-groupe normal (ou distingué) est très importante. En fait, H est dit sous-groupe normal de G (noté $H\triangleleft G$), si et seulement si pour tout $h\in H$, $g\in G$, alors $ghg^{-1}\in H$. Il existe plein d'autres définitions équivalentes !

Classe à gauche, à droite.

Si H est un sous-groupe de G, les classes à gauche de G selon H sont les parties de G de la forme $gH = \{gh|h\in H\}$, et les classes à droite de G selon H sont les parties de la forme $Hg=\{hg|h\in H\}$, où $g\in G$.

Groupe quotient.

On a $gH = Hg$ pour tout g, si H est un sous-groupe normal de G ; dans ce cas, on peut parler de classes sans préciser à gauche ou à droite. Alors, on peut définir l'ensemble des classes de G selon H. Cet ensemble est lui-même un groupe, noté G/H, dit groupe quotient.

Premier théorème d'isomorphisme.

Soit $f:G\to G'$ un morphisme de groupes. Alors $\ker f$ est un sous-groupe normal de G. Le premier théorème d'isomorphisme indique qu'il existe un isomorphisme de $G/\ker f$ vers $\mathrm{Im}\, f$ (et donc, si f est surjectif, sur G').

Exemple.

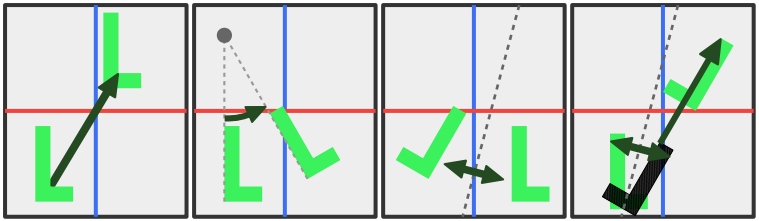
$6\mathbb{Z}$ est un sous-groupe normal de $\mathbb{Z}$. Les classes sont donc les multiples de 6 : $\{6k|k\in\mathbb{Z}\}$, les multiples de 6 plus 1 : $\{6k+1|k\in\mathbb{Z}\}$, etc. Le groupe quotient obtenu est donc noté $\mathbb{Z}/6\mathbb{Z}$, et correspond aux entiers modulo 6. Le morphisme $f:\mathbb{Z}\to(\mathbb{Z}/6\mathbb{Z})$ associe à chaque entier son reste lors d'une division par 6 ; et $\ker f = 6\mathbb{Z}$, ce qui est un cas évident du premier théorème d'isomorphisme.

Transformations géométriques.

Une transformation géométrique est une bijection d'une partie d'un ensemble géométrique dans lui-même. Donc, pas de projections ! On étudie le plan euclidien ici. Une transformation qui conserve les distances (et donc les angles) est appelée isométrie. Si elle conserve les rapports de distances, on dit que c'est une similitude. Et si elle ne conserve que la notion de parallélisme, on a une transformation affine.

Isométrie du plan euclidien.

Dans le plan euclidien, il y a 4 types d'isométries : translations, rotations, réflexions et réflexions glissées. Ces dernières consistent en une réflexion suivie d'une translation. En effet, si on applique deux isométries à la suite, la transformation résultante sera forcément une isométrie. Dans l'espace, on a de nouveaux types d'isométries; comme le vissage ou l'antirotation.



Groupe euclidien.

Le groupe des isométries d'un espace euclidien n-dimensionnel est appelé groupe euclidien; noté E(n) ou Is(n). Certains sous-groupes sont intéressants Par exemple, le sous-groupe des translations est juste $\mathbb{R}^n$; le sous-groupe des isométries qui sont des applications linéaires est noté O(n); pour n = 2, il ne contient que les rotations (par rapport à l'origine) et réflexions (par rapport à une droite passant par l'origine). Le sous-groupe des rotations est noté SO(n).

Similitudes et applications affines.

Une similitude est une transformation qui multiplie toutes les distances par un même facteur. D'ailleurs, toute similitude est simplement une homothétie suivie d'une isométrie. Deux figures sont semblables s'il existe une similitude envoyant l'une sur l'autre. Une similitude est directe si elle préserve l'orientation (translation et rotations), indirecte si elle l'inverse (réflexions et réflexions glissées). Une application affine est une transformation qui "préserve le parallélisme" (et l'alignement); si deux droites sont parallèles, leurs images seront aussi des droites parallèles. Toute application affine peut être représentée comme $x \mapsto u(x)+v$, où u est une application linéaire inversible de $\mathbb{R}^n$ dans lui-même et v un vecteur de $\mathbb{R}^n$.

Interprétation complexe.

On peut assimiler le plan complexe au plan euclidien ($\mathbb{R}^2$). Alors, toute similitude directe f peut s'écrire comme $f(z) = az+b$ avec $a \in \mathbb{C}^*$, $b \in \mathbb{C}$. Au contraire, toute similitude indirecte f peut s'écrire comme $f(z) = a\bar{z}+b$ avec $a \in \mathbb{C}^*$, $b \in \mathbb{C}$; on utilise le conjugué cette fois. Et toute application affine f peut s'écrire comme $f(z) = az+b\bar{z}+c$ ...

Théorie des groupes (avancée).

On note GL(n,$\mathbb{R}$) l'ensemble des applications linéaires inversibles de $\mathbb{R}^n$. Le groupe affine Aff($\mathbb{R}^n$) est l'ensemble des applications affines. Considérons l'ensemble des paires (u,v) d'une application linéaire u de GL(n,$\mathbb{R}$) et d'un vecteur v de $\mathbb{R}^n$. Alors, le produit défini par $(u_1,v_1)\bullet(u_2,v_2) = (u_1 \circ u_2, v_1+u_1(v_2))$ donne à GL(n,$\mathbb{R}$)$\times\mathbb{R}^n$ une structure de groupe ; celle de Aff($\mathbb{R}^n$) ! Ce moyen de construire un groupe est appelé produit semi-direct, et l'on note Aff($\mathbb{R}^n$) = $\mathbb{R}^n \rtimes$GL(n,$\mathbb{R}$) pour indiquer qu'on considère l'ensemble des paires muni d'un produit particulier.

Groupe fini.

Si un groupe G est fini (l'ensemble G est fini), son ordre, noté |G|, est son nombre d'éléments.

Groupes cycliques.

Les groupes finis les plus simples sont les groupes cycliques. On peut décrire $\mathbb{Z}_n$ (ou C_n) comme les entiers de 0 à (n-1), avec comme opération l'addition modulo n. On peut bien sûr les définir avec des classes d'équivalence. On dira que deux entiers $x,y\in\mathbb{Z}$ sont équivalents modulo n si $(x-y)\in n\mathbb{Z}$ (est un multiple de n). On peut alors partitionner $\mathbb{Z}$ en classes d'équivalence : [x] dénote l'ensemble des éléments de $\mathbb{Z}$ équivalents à x. Le groupe cyclique est alors l'ensemble des classes d'équivalence modulo n; l'opération étant [x]+[y] = [x+y]. C'est pour ça qu'on le note aussi $\mathbb{Z}/n\mathbb{Z}$.

Racines n-ièmes de l'unité.

Une racine n-ième de l'unité est, pour rappel, un nombre complexe z tel que $z^n = 1$; ζ_n défini comme $\exp(2\pi i/n)$ en est une. $\mathbb{Z}/n\mathbb{Z}$ est isomorphe ensemble des racines n-ièmes de l'unité; l'isomorphisme étant $k\in[\![0;n-1]\!]\mapsto \zeta_n^{\,k}\in\mathbb{C}$. Dans cet isomorphisme, $\mathbb{Z}/n\mathbb{Z}$ est représenté par l'ensemble $[\![0;n-1]\!]$.

Permutations.

Une permutation est simplement une bijection d'un ensemble E sur lui-même. Il existe plusieurs notations fréquentes: on prend souvent les ensembles {1, ..., n} comme ensemble E. Assez souvent, on représente une permutation σ avec deux lignes : la première étant 1 ... n, la seconde contenant l'image respective de chaque élément par la permutation. Par exemple :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 6 & 3 & 1 \end{pmatrix}$$

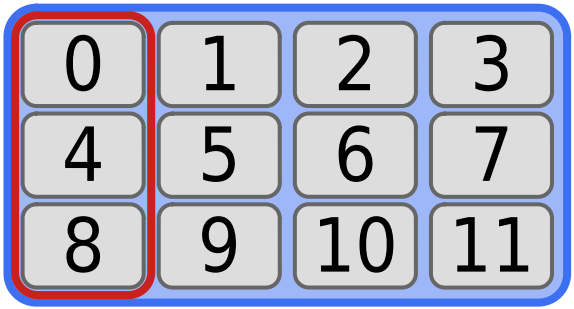
Une autre notation est en indiquant les cycles : la permutation d'avant s'écrit (1 4 6)(2)(3 5); cette notation signifie que 1 donne 4, 4 donne 6 et 6 donne 1; 2 donne 2; 3 donne 5 et 5 donne 3.

Groupe symétrique.

Si E est un ensemble, le groupe symétrique de E ou groupe des permutations de E désigne le groupe formé par l'ensemble des bijections de E sur E. On note alors S(E) ou $\mathfrak{S}(E)$. Très souvent, E = {1, ... n}, et on note alors S_n ou $\mathfrak{S}_n$. Cette structure est bien un groupe car elle valide bien les axiomes ; notamment que la composée de deux permutations est aussi une permutation. De plus, le groupe S_n est d'ordre n!.

Groupe de permutations.

Si X est un ensemble, un sous-groupe de S(X) est appelé groupe de permutations. Il a été prouvé (théorème de Cayley) que n'importe quel groupe est isomorphe à un groupe de permutations.



{0, 4, 8} sous-groupe de $\mathbb{Z}/12\mathbb{Z}$; en effet, 3|12.

Théorème de Lagrange.

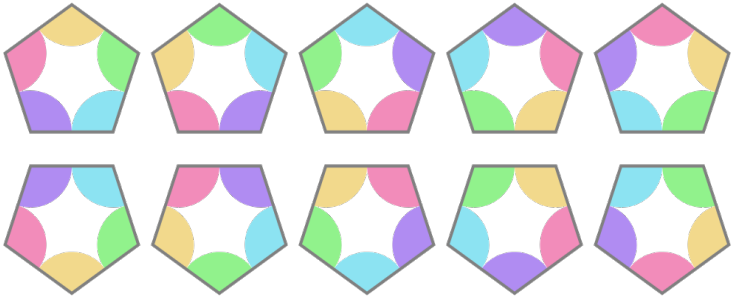
Si G est un groupe fini et H un sous-groupe de G, alors l'ordre de H divise l'ordre de G. De plus, une conséquence est que |G|/|H| est le nombre de classes de G selon H.

Groupe de symétrie.

Le groupe de symétrie d'un objet est le groupe de toutes les symétries (isométries) sous lesquelles l'objet est globalement invariant ; autrement dit, ne "change pas d'apparence".

Symétrie d'un polygone régulier.

Un polygone régulier à n côtés a pour groupe de symétrie un groupe avec 2n éléments; n rotations (incluant l'identité), et n symétries. Ces groupes sont appelés groupes diédraux, notés D_n ou D_{2n} selon l'auteur. Notamment, D_3 (groupe de symétrie d'une triangle équilatéral) est isomorphe à S_3. Pour chaque symétrie s du groupe, {Id, s} est un sous-groupe. Et le sous-groupe constitué uniquement des rotations est un groupe cyclique !

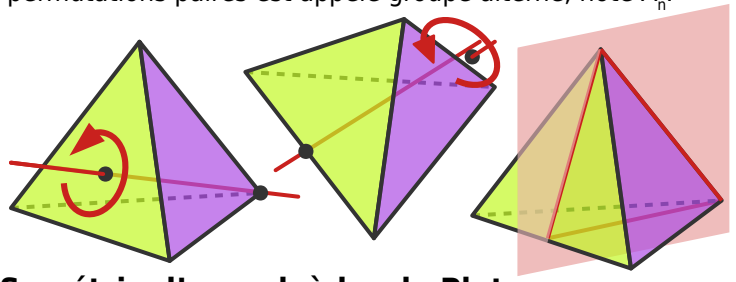


Symétrie d'un papier peint.

De même, un groupe de papier peint est un groupe des transformations (isométries) qui ne change pas l'apparence d'un papier peint; un papier peint étant défini comme un motif se répétant périodiquement dans deux directions de l'espace. Ces groupes sont composés de 4 types de transformations : translations, rotations, réflexions, et réflexions glissées : réflexions suivies d'une translation. Il y en a 17 "types"; il y en a 3 exemples à droite.

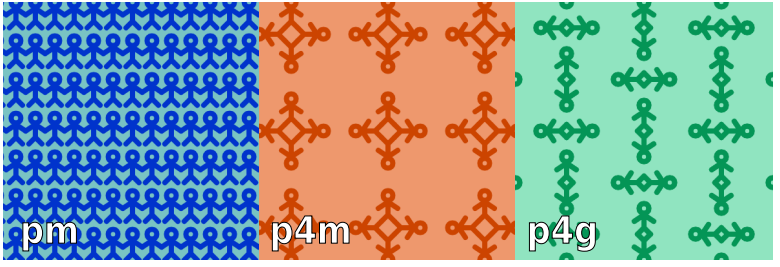
Groupe alterné.

On appelle permutation paire une permutation que l'on peut obtenir avec un nombre pair de transpositions (échange de deux éléments). Le sous-groupe de S_n ne contenant que les permutations paires est appelé groupe alterné, noté A_n.



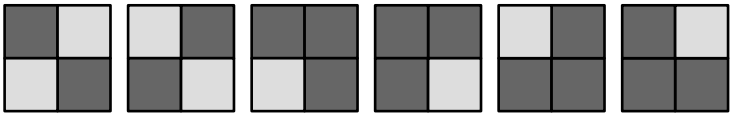
Symétrie d'un polyèdre de Platon.

C'est un fait avéré qu'il n'existe que 5 polyèdres de Platon (sous certaines conditions) : le tétraèdre régulier, le cube, l'octaèdre régulier, le dodécaèdre régulier et l'icosaèdre régulier. De même, on peut étudier leurs groupes de symétries. Celui du tétraèdre contient 24 éléments, et est isomorphe à S_4. Le sous-groupe des rotations est lui isomorphe à A_4. Celui du cube et de l'octaèdre sont les mêmes ; 48 éléments, dont 24 rotations formant un groupe isomorphe à S_4. Et celui du dodécaèdre et de l'icosaèdre sont les mêmes, avec 120 éléments, dont 60 rotations formant un sous-groupe isomorphe à A_5.



Groupe général linéaire.

Le groupe général linéaire de degré n sur un corps K est l'ensemble des matrices inversibles de n par n à coefficients dans K, où l'opération de groupe est la multiplication de matrice. On le note GL(n,K) ou $GL_n(K)$. Les axiomes de groupe sont bien vérifiés : le produit de deux matrices inversibles est inversible, l'identité est la matrice identité, l'inverse est la matrice inverse et l'associativité est une propriété de la multiplication matricielle. On s'intéresse dans ce cours à K = ℝ. Par exemple, GL(2,ℝ) est l'ensemble des matrices de 2×2 à coefficients réels, et de déterminant non-nul (donc ad-bc ≠ 0).



Le groupe général linéaire GL(2,2) (le 2 indiquant qu'on utilise le corps ℤ/2ℤ = {0,1}, modulo 2) est discret ; il contient 6 matrices, et est isomorphe au groupe symétrique S_3.

Groupe spécial linéaire.

Le groupe linéaire spécial SL(n,K) est le sous-groupe de GL(n,K) ne contenant que les matrices de déterminant 1.

Groupe spécial orthogonal.

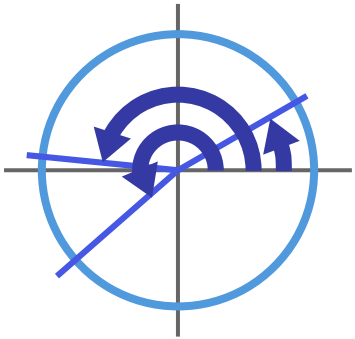
Une matrice orthogonale est une matrice Q telle que $Q^TQ = QQ^T = I$. De manière équivalente, une matrice Q telle que ses colonnes représentent une base orthonormée (vecteurs de norme 1 et orthogonaux deux à deux). Le sous-groupe de GL(n,K) ne contenant que les matrices orthogonales est dit groupe orthogonal, noté O(n,K). Et le sous-groupe de O(n,K) ne contenant que les matrices de déterminant 1 est le groupe orthogonal spécial, noté SO(n,K). O(n,K) représente les isométries fixant l'origine de K^n ; SO(n,K) les isométries directes (fixant l'origine) ; donc les rotations de K^n.

SO(2,ℝ).

On peut définir une matrice orthogonale comme une matrice Q dont l'endomorphisme associé φ laisse invariant le produit scalaire; on a ⟨φ(x), φ(y)⟩ = ⟨x,y⟩ pour tout x,y∈E. Donc le produit de deux matrices orthogonales est orthogonal. De plus, cette condition fait qu'aucun vecteur non-nul devient nul; et donc que Q est inversible ! Donc l'ensemble des matrices orthogonales de $\mathbb{R}^2$ forme un groupe. SO(2,ℝ) est d'ailleurs un groupe simple à représenter. Tout les éléments de SO(2,ℝ) sont de la forme :

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

Les éléments de SO(2,ℝ) sont les rotations autour de l'origine ; ce groupe est isomorphe au groupe cercle, l'ensemble des complexes de norme 1 muni de la multiplication complexe.



Transformations géométriques.

Les transformations géométriques vues précédemment peuvent s'exprimer sous forme matricielle. Par exemple, les rotations, réflexions, et plus généralement les similitudes qui préservent l'origine sont des applications linéaires. On a vu une matrice de rotation dans $\mathbb{R}^2$ plus haut ; une réflexion peut s'écrire avec une matrice du même genre :

$$Rf_\theta = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$

Pour $\mathbb{R}^3$, c'est plus compliqué. Les matrices orthogonales donnent des rotations, réflexions mais aussi des opérations plus complexes.