Introduction à la Théorie des Groupes
Version courte

Farouk Boucekkine (avec l'aide de Thomas Chomette)

http://dma.ens.fr/culturemath

Résumé

La notion de Groupe émergea progressivement au cours du $XIX^{\text{ème}}$ siècle. Evariste Galois et Niels Henrik Abel sont les premiers à l'avoir dégagée, dans leurs travaux respectifs sur la résolution des équations algébriques par radicaux. C'est le "Programme d'Erlangen" de Felix Klein (1872) qui la place au centre de la géométrie moderne, comme la charnière permettant d'unifier les différentes théories géométriques.

Les groupes sont, depuis, les premières structures algébriques modernes, et apparaissent dans presque toutes celles qui forment la base des mathématiques du $XX^{\text{ème}}$ siècle : anneaux, corps, espaces vectoriels, algèbres, modules, etc... En les étudiant, on voit apparaître des concepts et des méthodes qui sont très répandus dans toutes les parties des mathématiques : notion de structure, morphismes, isomorphismes, noyaux, quotients, extensions...

Ce texte a pour but de donner une base à tous les développements utilisant cette notion capitale qui ont été et seront faits dans le site Culture*MATH*. Dans cette Première Partie, nous définissons les concepts essentiels, et la manière dont les groupes agissent sur des ensembles, donnant un grand nombre d'exemple pour illustrer comme pour annoncer les résultats.

Dans cette version courte, destinée à être une référence rapide, les exemples et la plupart des commentaires ont été retirés. On les trouvera dans la version longue (25 pages d'exemples et de commentaires en plus), disponible sur le site.

culturemath@dma.ens.fr

Table des matières

Rappels et Notations : cf. Version Longue !

1 Dis M'sieur, c'est quoi un Groupe ?

1.1 Définition et premiers exemples

Définition 1.1.1 *Un* Groupe $(G, \bullet)$ *est un ensemble G muni d'une* opération $\bullet$*, c'est à dire une application $G \times G \to G$ telle que l'image de (x, y) est notée $x \bullet y$.*
De plus, cette opération doit posséder les propriétés suivantes :

i) associativité *:* $\forall (x, y, z),\ (x \bullet y) \bullet z = x \bullet (y \bullet z)$.

ii) existence d'un élément neutre e_G *:* $\forall x,\ x \bullet e_G = e_G \bullet x = x$

iii) existence d'inverses *:* $\forall x, \exists y$ *tel que* $x \bullet y = y \bullet x = e_G$.

Définition 1.1.2 *Un groupe $(G, \bullet)$ est dit* commutatif *ou* abélien *si pour tout couple (x, y) d'éléments de G, on a*

$$x \bullet y = y \bullet x$$

Propriété 1.1.3 *Soit $(G, \bullet)$ un groupe.*

i) Alors il n'existe qu'un seul élément neutre.

ii) Notons e l'élément neutre (unique d'après ce qui précède) de $(G, \bullet)$, et soient $x, y, z \in G$ tels que $x \bullet y = e$ ET $z \bullet x = e$. On a alors $y = z$. L'inverse d'un élément de G est donc unique.

Notation 1.1.4 *Les symboles* "+" *et* "." *sont les plus couramment utilisés pour noter l'opération sur G.*

Dans le premier cas, on parle d'un "groupe G noté additivement"*, l'élément neutre est noté* "0"*, et l'inverse de x est appelé* opposé *et noté* "$-x$". *Si $n \in \mathbb{Z}_+$ (resp. $\mathbb{Z}_-$), on écrit alors $n.x$ pour $x + \cdots + x$ (resp. $(-x) + \cdots + (-x)$). Cette terminologie spécifique généralise bien entendu les exemples (i) précédents, et ne s'emploie généralement que dans le cas de groupes commutatifs.*

Dans le second cas, on parle d'un "groupe G noté multiplicativement"*, l'élément neutre est généralement noté* "1" *(cf. exemples (ii) et (iii)),* "Id" *(cf. exemple (iv)),* "e" *ou* "e_G"*, et l'inverse de x est noté* "x^{-1}"*. Si $n \in \mathbb{Z}_+$ (resp. $\mathbb{Z}_-$), on écrit alors x^n pour $x. \cdots .x$ (resp. $(x^{-1}). \cdots .(x^{-1})$)*

En règle générale, l'expression "Soit G un groupe"*, sans spécification d'opé-ration, signifie implicitement qu'on se place dans le second cas, et il est* **très fréquent** *qu'on omette même d'écrire le symbole* "."*, écrivant* "xy" *pour* "$x.y$"

Propriétés 1.1.5 (i) *Soit G un groupe, et $x, y, z \in G$. alors*

$$xz = yz \Longrightarrow x = y \quad et \quad zx = zy \Longrightarrow x = y$$

(ii) *Soit G un groupe, et $x, y \in G$. alors*

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

1.2 Voyager d'un groupe à l'autre : les morphismes de groupes

Le **§1.1** jette les premières bases d'une structure algébrique : on donne un ensemble d'objets, G, et on précise "ce qu'on sait faire avec ces objets" grâce, en l'occurrence, à une opération $\bullet$ sur G, qui doit vérifier un certain nombre de spécifications pour pouvoir être "valable". Cela donne un groupe $(G, \bullet)$.

Dans ce paragraphe, nous allons voir comment faire "communiquer" les groupes entre eux grâce à la notion de *morphisme de groupes.* L'idée est simple : un morphisme d'un groupe G vers un groupe H est une application de G vers H qui est *compatible avec les opérations des deux groupes.*

Définition 1.2.1 *Soient $(G, \bullet)$ et $(H, \circ)$ deux groupes, d'éléments neutres respectifs e_G et e_H. On appelle* morphisme de G vers H *toute application $\phi : G \to H$ vérifiant*

$$\begin{cases} \forall x, y \in G, \ \phi(x \bullet y) = \phi(x) \circ \phi(y) \\ \qquad\qquad \phi(e_G) = e_H \end{cases}$$

*Quand $(G, \bullet) = (H, \circ)$, on parle d'*endomorphisme.

Remarque 1.2.2 *Si $g \in G$, d'inverse g^{-1}, alors $\phi(g^{-1})$ est nécessairement l'inverse de $\phi(g)$ dans H.*

Remarque 1.2.3 *Dans la définition précédente, on a noté différemment les opérations de G et de H pour bien montrer ce qui se passe. Suivant l'usage décrit à la fin de la* **Notation 1.1.4**, *cela donne :*

Soient G et H deux groupes, un morphisme *de G à H est une application ϕ telle que*

$$\forall x, y \in G, \ \phi(xy) = \phi(x)\phi(y) \quad (etc...)$$

Il suffit de bien garder en tête où "habitent" les différents éléments qui entrent en jeu, et, dans la plupart des cas, on n'a pas réellement besoin de noter l'opération.

Propriété 1.2.4 *Soient $\phi : G \to H$ et $\psi : H \to K$ deux morphismes de groupes, alors $\psi \circ \phi : G \to K$ est un morphisme de groupes.*

2 Encore un peu de structure, s'il vous plait

Maintenant que nous avons défini la structure de Groupe, nous allons voir ses particularités importantes, et des raisonnements typiques des groupes mais qui font écho à de nombreuses autres parties des mathématiques.

2.1 Noyau et Image d'un morphisme de groupes

Définition 2.1.1 *Soit $\phi : G \to H$ un morphisme de groupes. L'*Image de ϕ, *notée $Im\ \phi$ est*

$$Im\ \phi = \{\phi(x), \ x \in G\}.$$

Ainsi, ϕ est surjective si et seulement si $Im\ \phi = H$.

Définition 2.1.2 *Soit $\phi : G \to H$ un morphisme de groupes, le* Noyau *de ϕ est l'ensemble $Ker\ \phi := \{g \in G,\ \phi(g) = e_H\}$.*

Remarquons tout de suite que $Ker\ \phi$ n'est jamais vide car $e_G \in Ker\ \phi$. Le fait qu'il soit, ou pas, réduit à cet élément est l'objet de la proposition suivante :

Propriété 2.1.3 *Soit $\phi : G \to H$ un morphisme de groupes, alors ϕ est injectif si et seulement si $Ker\ \phi = \{e_G\}$.*

2.2 "Ce serait pareil... mais autrement" : les isomorphismes

Dans ce paragraphe, nous définissons comment deux groupes peuvent être IDENTIQUES du point de vue de la structure de groupe (sans pour autant être des ensembles égaux).

Définition 2.2.1 *Soit $\phi : G \to H$ un morphisme de groupes. On dit que ϕ est un* isomorphisme *s'il existe un morphisme de groupes $\psi : H \to G$ tel que :*

$$\psi \circ \phi = Id_G \quad et \quad \psi \circ \phi = Id_H$$

S'il existe un isomorphisme entre deux groupe G et H, on dit que les groupes sont isomorphes*, ce qu'on note $G \simeq H$.*

Un endomorphisme de G qui est un isomorphisme est appelé automorphisme *de G.*

On a la propriété suivante :

Propriété 2.2.2 *Un morphisme de groupes est un isomorphisme si et seulement s'il est bijectif.*

La dernière proposition n'est pas anodine même si elle paraît évidente : dans certaines structures, un morphisme bijectif n'est pas forcément un isomorphisme. Par exemple, Dans la structure d'espace topologique (par exemple $\mathbb{R}$ ou $\mathbb{C}$ munis de leur topologie usuelle, le cercle C des complexes de module 1, etc...), une application continue bijective n'a pas forcément sa réciproque continue (exemple : $[0,1[\to C,\ x \longmapsto e^{2i\pi x}$) !

Reprenant les notions introduites au paragraphe précédent, on peut à présent énoncer la proposition synthétique suivante :

Propriété 2.2.3 *Soit $\phi : G \to H$ un morphisme de groupes. Alors ϕ est un isomorphisme si et seulement si*

$$Im\ \phi = H \quad et \quad Ker\ \phi = \{e_G\}.$$

Les bijections d'un ensemble E dans lui-même, munies de l'opération de composition, forment un groupe $(\mathfrak{S}(E), \circ)$ (cf. Version Longue).

Etant donné un groupe G, parmi les bijections de G sur G, certaines sont en plus des automorphismes, on peut alors remarquer que l'ensemble des automorphismes de G forme lui-même un groupe lorsqu'on le munit de l'opération de composition ! En effet, la composée de deux automorphismes en est un, l'inverse d'un automorphisme en est un, et Id_G est un automorphisme.

Notation 2.2.4 *On note $Aut(G)$ le groupe des automorphismes de G.*

Ainsi, on a deux groupes $Aut(G) \subset \mathfrak{S}(G)$, ce qui nous donne un bon exemple de sous-groupe, notion développée dans le paragraphe suivant.

2.3 Sous-groupes d'un groupe donné

Ici, on parle de l'inclusion de groupes dans d'autres groupes, avec la même opération.

Définition 2.3.1 *Soit G un groupe, et soit $H \subset G$. On dit que H est un* sous-groupe *de G si l'opération de G restreinte à H définit une structure de groupe sur H.*

Notation 2.3.2 *Si H est un sous-groupe de G, on note $H < G$.*

Cette définition malcommode sera toujours remplacée par la propriété opéra-toire suivante :

Propriété 2.3.3 *Soit G un groupe, et soit H une partie non-vide de G. H est un* sous-groupe *de G si et seulement s'il est* stable par multiplication et par inverse*, c'est à dire :*

$$\begin{cases} \forall x, y \in H,\ xy \in H \\ \forall x \in H,\ x^{-1} \in H \end{cases}$$

On constate aisément que l'élément neutre de G appartient à tout sous-groupe de G.

Propriété 2.3.4 *Soit $\phi : G \to H$ un morphisme de groupes. Alors $Ker\ \phi$ est un sous-groupe de G et $Im\ \phi$ est un sous-groupe de H.*

Autre sous-groupe important :

Définition 2.3.5 *Soit G un groupe. On appelle* centre *de G le groupe*

$$Z(G) = \{x \in G \textit{ tels que } \forall g \in G, xg = gx\}.$$

Mainenant, on va introduire une notion très importante : si on a une partie $A \subset G$, ce n'est pas un sous-groupe a priori. Mais il existe un unique sous-groupe de G *minimal pour l'inclusion* qui contient A. Mais voyons d'abord un petit lemme technique :

Propriété 2.3.6 *Soit $(H_i)_{i \in I}$ une famille (quelconque, pas nécessairement finie) de sous-groupes de G. Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.*

Remarque 2.3.7 *Attention ! Ca ne marche pas avec $\bigcup_{i \in I} H_i$. Sauriez-vous trouver un contre-exemple ?*

Définition 2.3.8 *Soit G un groupe et A une partie de G. L'ensemble des sous-groupes de G contenant A est non-vide (car il contient au moins G).*

On définit alors le sous-groupe engendré par *A :*

$$\langle A \rangle := \bigcap_{\substack{H < G \\ A \subset H}} H.$$

Remarques 2.3.9 *$\langle A\rangle$ est le plus petit sous-groupe de G contenant A : tout autre sous-groupe de G contenant A le contient aussi.*

Par ailleurs, si $H < G$, on voit immédiatement que $\langle H\rangle = H$.

On va donner tout de suite une caractérisation plus calculatoire de cette notion :

Propriété 2.3.10 *Soit G un groupe et A une partie de G. alors*

$$\langle A\rangle = \left\{a_1 \dots a_n \mid n \in \mathbb{N} \text{ et } \forall i, (a_i \in A \text{ OU } a_i^{-1} \in A)\right\} \cup \{e_G\}$$

Si $\langle A\rangle = G$, on dit que A engendre *G ou que A* est une partie génératrice *de G.*

2.4 Un peu de collage : le produit direct de deux groupes

L'un des thèmes les plus importants en théorie des groupes est le recollement de deux groupes pour en construire un plus gros. Nous verrons dans la Deuxième Partie qu'il s'agit d'un champ extrèmement large. Pour l'heure, définissons le moyen le plus simple de faire une telle construction : le produit cartésien.

Définition 2.4.1 *Soient G et H deux groupes. On définit le* produit direct *de G et H, noté $G\times H$ en prenant l'ensemble $G\times H = \{(g,h),\ g \in G \text{ et } h \in H\}$ qu'on munit de l'opération*

$$(g,h).(g',h') := (gg',hh')$$

Remarque 2.4.2 *L'élément neutre de $G \times H$ est (e_G, e_H).*

Si G et H sont de cardinaux finis, on a alors $|G \times H| = |G| \times |H|$. En fait l'hypothèse de finitude n'est pas nécessaire si on connaît un peu la théorie des cardinaux (voir par exemple le texte sur le sujet figurant dans la partie Logique *de* Culture*MATH, p.8).*

Propriété 2.4.3 *Les applications*

$$\pi_1 : \left\{\begin{array}{ccc} G\times H & \longrightarrow & G \\ (g,h) & \longmapsto & g \end{array}\right. \quad \text{et} \quad \iota_1 : \left\{\begin{array}{ccc} G & \longrightarrow & G\times H \\ g & \longmapsto & (g,e_H) \end{array}\right.$$

$$\pi_2 : \left\{\begin{array}{ccc} G\times H & \longrightarrow & H \\ (g,h) & \longmapsto & h \end{array}\right. \quad \text{et} \quad \iota_2 : \left\{\begin{array}{ccc} H & \longrightarrow & G\times H \\ h & \longmapsto & (e_G,h) \end{array}\right.$$

sont des morphismes de groupes et

$$\left\{\begin{array}{l} \pi_1 \circ \iota_1 = Id_G \\ \pi_2 \circ \iota_2 = Id_H. \end{array}\right.$$

3 Action d'un groupe sur un ensemble

3.1 Définition et premiers exemples

Définition 3.1.1 *: Soit G un groupe, E un ensemble. Une* action *(à gauche)* du groupe G sur l'ensemble E *est une application :*

$$\left\{\begin{array}{ll} G\times E & \longrightarrow E \\ (g,x) & \longmapsto g.x \end{array}\right.$$

qui vérifie les axiomes :

i) $\forall g,g' \in G, \quad \forall x \in E, \quad g.(g'.x) = (gg').x$

ii) $\forall x \in E, \quad e_G.x = x$

On peut à présent remarquer que si G agit sur E, alors pour tout $g \in G$, l'application $\begin{cases} E & \longrightarrow E \\ x & \longmapsto g.x \end{cases}$ est une bijection, de réciproque $x \longmapsto g^{-1}.x$.

En effet,

$$\forall g \in G, \forall x \in E, g.(g^{-1}.x) = g^{-1}.(g.x) = e_G.x = x.$$

Ainsi, par l'action de G sur E, on peut associer à tout élément de G un élément de $\mathfrak{S}(E)$. On peut même être plus précis :

Propriété 3.1.2 *Soit G un groupe agissant sur un ensemble E, alors l'application*

$$\begin{cases} G & \longrightarrow & \mathfrak{S}(E) \\ g & \longmapsto & (x \longmapsto g.x) \end{cases}$$

est un morphisme de groupes.

Réciproquement, si $\phi : G \to \mathfrak{S}(E)$ est un morphisme de groupes, alors

$$\begin{cases} G \times E & \longrightarrow E \\ (g, x) & \longmapsto [\phi(g)](x) \end{cases}$$

définit une action de G sur E.

3.2 Orbite d'un élément

Si un groupe G agit sur un ensemble E, on va s'intéresser à toutes les images possibles d'un élément $x \in E$, ainsi qu'aux éléments de G qui ne bougent pas x. Nous allons voir que ces deux notions sont liées.

Définition 3.2.1 *Soit G un groupe agissant sur un ensemble E, et $x \in E$. Alors on appelle* orbite *de x l'ensemble*

$$\omega(x) := \{g.x \mid g \in G\}$$

Propriété 3.2.2 *(mêmes notations) (i) $\omega(x)$ est stable sous l'action de G, et on a même plus précisément*

$$\forall z \in \omega(x),\ \omega(z) = \omega(x).$$

(ii) Soient $x, y \in G$ alors

$$\begin{array}{ll} \textit{soit} & \omega(x) = \omega(y) \\ \textit{soit} & \omega(x) \cap \omega(y) = \emptyset. \end{array}$$

(iii) L'action de G sur E induit une action de G sur $\omega(x)$.

On a alors immédiatement :

Corollaire 3.2.3 *Les orbites de E sous l'action de G forment une partition de E (i.e. E est l'union disjointes des $\omega(x)$).*

Ainsi, l'ensemble des orbites de E sous l'action de G est important, et on est souvent amené, dans différents domaines des mathématiques, à le considérer en tant qu'objet. En quelque sorte, en le considérant, on "identifie" tous les éléments d'une même classe en un seul.

Définition 3.2.4 *On appelle* Ensemble quotient de E sous l'action de G *l'ensemble*

$$E/G := \{\omega(x), x \in E\}$$

Pour l'heure, remarquons la formule suivante, qui découle immédiatement du corollaire précédent :

Propriété 3.2.5 (Formule des classes) *Soit G agissant sur E, on a alors*

$$|E| = \sum_{\omega \in E/G} |\omega|$$

qu'on écrit traditionnellement :

$$|E| = \sum_{x} |\omega(x)|, \quad \text{“}x \text{ décrivant un ensemble de représentants de des orbites de } E\text{”}$$

On utilise souvent cette formule conjointement avec la **Propriété 3.4.3** pour obtenir des informations. Un bon exemple d'application est donné dans le §**3.5**.

3.3 Le Théorème de Lagrange

Voici à présent le théorème le plus important concernant les sous-groupes d'un groupe fini, nous le mettons ici car il illustre bien la puissance des outils développés au §**3.2**.

Soit G un groupe et $H < G$, agissant sur G par translation à gauche. On a alors $G/H = \{Ha, a \in G\}$ (et les Ha forment donc une partition de G.)

Notation 3.3.1 *Avec ces notations, on appelle* indice *du sous-groupe H, noté $(G : H)$, le cardinal (éventuellement infini) de l'ensemble G/H.*

Avec ces notations, nous pouvons énoncer le Théorème de Lagrange :

Théorème 3.3.2 *(Lagrange)*

Soit G un groupe fini, H un sous-groupe de G. Alors le cardinal de H et l'indice de H divisent le cardinal de G, et l'on a :

$$|G| = (G : H) \, . \, |H|$$

Corollaire 3.3.3 *Soit $\phi : G \to H$ un morphisme de groupes, alors*

$$|Ker\ \phi| . |Im\ \phi| = |G|$$

Un cas particulier important du théorème de Lagrange est le cas du sous-groupe engendré par un élément $x \in G$, qui nous amène à donner la définition suivante :

Définition 3.3.4 *Soit $x \in G$, on appelle* ordre *de x (noté $o(x)$) le cardinal du groupe $\langle x \rangle$.*

Comme on sait que $\langle x \rangle = \{x^k, k \in \mathbb{Z}\}$, on a donc deux possibilités :

o(x) est infini	:	alors $\forall k \in \mathbb{Z}^*$, $x^k \neq e_G$.
o(x) est fini	:	alors $o(x) = \min\{k \in \mathbb{N}^* \mid x = e_G\}$

Appliquons à présent le théorème de Lagrange à $\langle x \rangle$:

Propriétés 3.3.5 *(i) $o(x)$ divise $|G|$*

(ii) Si $f : G \to H$ est un morphisme de groupes, et si $x \in G$, alors $o(f(x))$ divie $o(x)$.

Exemple d'application : Soient G et H deux groupes tels que $|G| \wedge |H| = 1$. Alors il n'y a pas de morphisme non-trivial de G vers H. En effet, soit f un tel morphisme et soit $x \in G$, alors on a

$$\begin{array}{l} o(f(x)) \text{ divise } o(x) \text{ qui divise } |G| \quad \text{et} \\ o(f(x)) \text{ divise } |H| \end{array}$$

Donc $o(f(x))$ divise $|G| \wedge |H| = 1$, et donc $o(f(x)) = 1$, ce qui implique que $f(x) = e_H$. Par conséquent, f est le morphisme trivial.

Question : Qu'en est-il d'une réciproque au théorème de Lagrange ? Autrement dit, si n divise $|G|$, peut-on trouver un sous-groupe de $H < G$ tel que $|H| = n$?

Nous reparlerons de cette question dans la Deuxième Partie, mais d'ici-là, réfléchissez-y !

3.4 Le stabilisateur d'un élément

Intéressons-nous aux éléments du groupe G qui laissent fixent une partie donnée de E :

Lemme 3.4.1 *Soit G un groupe agissant sur un ensemble E, et soit $A \subset E$, alors l'ensemble*

$$S_A := \{g \in G \mid g.A = A\}$$

est un sous-groupe de G.

Le cas particulier le plus important de ce lemme est celui où A est réduit à un singleton $\{x\}$:

Définition 3.4.2 *(mêmes notations) Soit $x \in E$. On appelle* (sous-groupe) Stabilisateur *de x le sous-groupe suivant de G*

$$Stab_G(x) := \{g \in G \mid g.x = x\}$$

Il existe un lien très fort entre Orbite et stabilisateur d'un élément, que la propriété suivante permet d'expliciter :

Propriété 3.4.3 *(mêmes notations) Soit $x \in E$ on a alors*

$$|G| = |\omega(x)|.|Stab_G(x)|$$

3.5 Une application algébrique : le centre des $p-$groupes

Nous allons découvrir une famille très importante parmi les groupes finis : les $p-$groupes, et l'une de leurs nombreuses spécificités. Commençons donc par les définir :

Définition 3.5.1 *Soit p un* **nombre premier**. *On appelle $p-$groupe tout groupe (fini) dont le cardinal est une puissance de p.*

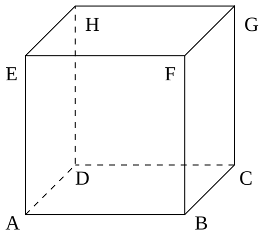
A présent venons-en à la proposition qui nous intéresse :

Propriété 3.5.2 *Le centre d'un $p-$groupe non-trivial n'est jamais trivial.*

Cette propriété est très importante dans l'étude des $p-$groupes, car elle permet l'étude de propriétés par récurrence, en quotientant par le centre. Mais ceci est une autre histoire...

3.6 Un exemple issu de la géométrie : Les isométries directes du cube

Illustrons géométriquement la notion d'action d'un groupe sur un ensemble en caractérisant le groupe des déplacements du cube. Une isométrie du cube peut être vue comme une permutation des sommets A, B, C, D, E, F, G, et H dudit cube.



C'est-à-dire que le groupe des déplacements du cube peut être vu comme un sous-groupe du groupe des permutations d'un ensemble à huit éléments, groupe de cardinal $8! = 40320$.

Mais une isométrie doit envoyer des sommets voisins sur des sommets voisins. En fait, un déplacement du cube est caractérisé par l'image de trois points : si l'on donne l'image des points A, B et D, les images de tous les autres sommets seront déterminés. Cela nous laisse donc 8 possibilités pour l'image de A, puis 3 possibilités pour l'image de B (l'un des trois voisins de l'image de A), puis encore 2 possibilités pour l'image de D. Soit, au total, 48 isométries distinctes possibles du cube. Sur ces 48 isométries possibles, la moitié sont des anti-déplacements, puisqu'elles transforment le repère direct $\left(A, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AE}\right)$ en un repère indirect.

Tout ceci nous laisse donc 24 isométries directe, ou déplacements, possibles pour le cube. Réciproquement, tout repère direct d'origine l'un des sommets du cube, et d'axes définis par trois arêtes de ce cube définissent bien un déplacement du cube : on construit aisément une rotation envoyant notre repère $\left(A, \overrightarrow{AB}, \overrightarrow{AD}, \overrightarrow{AE}\right)$ sur le repère en question. Cette rotation laisse alors nécessairement le cube globalement invariant.

Conctrètement, on trouve les rotations suivantes :

- L'identité.
- Les six rotations d'angle plus ou moins $\frac{\pi}{2}$ autour des trois axes passant par les milieu de deux faces opposées.
- Les trois rotation d'angle π autour de ces mêmes axes.
- Les six rotations d'angle π autour des six axes joignant les milieux de deux arêtes opposées.
- Les huit rotations d'angle plus ou moins $\frac{2\pi}{3}$ autour des quatre axes joignant deux sommets opposés.