104 — Groupes finis. Exemples et applications.

Dans cette leçon, on suppose connus les éléments de théorie des groupes, pour développer le cas particulier des groupes finis. On suppose également maîtrisées les leçons 101 et 105.

I – Généralités sur les groupes finis

A – Ordre d'un groupe, d'un élément

[U] 2 **Def 1** : Un groupe $(G,\cdot)$ est dit *fini* si G est de cardinal fini. On appelle alors *ordre* de $(G,\cdot)$ le cardinal de G.

Dans la suite, $(G,\cdot)$ désignera un groupe fini, que l'on confondra avec G.

[U] 6 **Def 2** : L'ordre d'un élément $g \in G$ est l'ordre de $\langle g \rangle$, soit encore $\min\{n \geq 1 \mid g^n = 1\}$. On note $\mathrm{ord}(g)$ l'ordre de g.

Ex 3 :
- $(\mathbb{Z}/6\mathbb{Z}, +)$ et $(\mathfrak{S}_3, \circ)$ sont des groupes d'ordre 6.
- Dans $(\mathbb{Z}/6\mathbb{Z}, +)$, $\bar{1}$ est d'ordre 6, et $\bar{2}$ est d'ordre 3.

[R] 1/2 **Prop/Def 4** : Soit $H \leq G$. L'ensemble des classes d'équivalence de la relation donnée par $g \mathcal{R} g' \iff g'g^{-1} \in H$, noté G/H, est appelé *ensemble des classes à gauche de G relativement à H*. L'ensemble $G/H = \{gH : g \in G\}$ est fini, et son cardinal est appelé *indice de H dans G*, et est noté $(G:H)$.

[R] 2 **Thm 5** (de Lagrange) : $\forall H \leq G, \quad \#G = \#H \times (G:H)$

Cor 6 : L'ordre d'un élément ou d'un sous-groupe divise $\#G$.

Rq 7 : $6 \mid \#\mathfrak{A}_4$ mais $\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6.

[R] 3 **Def 8** : Soit $H \leq G$. On dit que H est *distingué* dans G, et on note $H \trianglelefteq G$, si H est stable par conjugaison par tout élément de G.

Prop 9 : Soit $H \trianglelefteq G$. L'ensemble G/H muni de $gH \cdot g'H = gg'H$ est un groupe, appelé *groupe quotient de G par H*. [R] 9

Def 10 : On dit que G est *simple* si ses seuls sous-groupes distingués sont $\{1\}$ et G.

B – Action d'un groupe fini sur un ensemble fini

Dans ce paragraphe, X est un ensemble fini sur lequel G agit. Pour $x \in X$, on note $\mathrm{Orb}(x)$ (resp. $\mathrm{Stab}(x)$) l'orbite de x (resp. le stabilisateur de x) sous G.

Prop 11 : Pour tout $x \in X$, $G/\mathrm{Stab}(x)$ et $\mathrm{Orb}(x)$ sont équipotents. Par conséquent, $\#G = \#\mathrm{Stab}(x) \cdot \#\mathrm{Orb}(x)$ (relation orbite-stabilisateur). [R] 21

Thm 12 (équation aux classes) : $\#X = \sum_{i=1}^{r} \#\mathrm{Orb}(x_i) = \sum_{i=1}^{r} \frac{\#G}{\#\mathrm{Stab}(x_i)}$ [R] 21
où $\{x_1, \dots, x_r\}$ est un système de représentants pour les orbites.

Prop 13 : Si G est d'ordre une puissance d'un nombre premier, alors son centre $Z(G) = \{x \in G \mid \forall y \in G,\ xy = yx\}$ n'est pas réduit à $\{1\}$. [R] 22

Cor 14 : Si $\#G = p^2$, p premier, alors G est abélien (i.e. $G = Z(G)$). [R] 23

Thm 15 (de Cauchy) : Pour tout facteur premier p de G, il existe un élément de G d'ordre p. [R] 23

Thm 16 (de Cayley) : G s'identifie à un sous-groupe de $\mathfrak{S}(G)$. [R] 21 [U] 31

C – Sous-groupes de Sylow

Dans ce paragraphe, on écrit $\#G = p^\alpha m$, p premier, $m \wedge p = 1$.

Def 17 : Un *p-Sylow* de G est un sous-groupe de G d'ordre p^α. [U] 85

[U] 87 Thm 18 (de Sylow) : Notons $Syl_p(G)$ l'ensemble des p-Sylow de G, et n_p le cardinal de $Syl_p(G)$.

1▸ $Syl_p(G) \neq \emptyset$ 2▸ Les p-Sylow de G sont conjugués entre eux

3▸ $n_p \equiv 1 \ [p]$ (donc $n_p | m$).

[S] 277 $\boxed{\text{Thm 19 : Si } G \text{ est simple et d'ordre } 60, \text{ alors } G \simeq \mathcal{A}_5. \quad \text{DEV 1}}$

II - Groupes abéliens fini - classification

A - Groupes cycliques

[R] 13 Dans ce paragraphe, on suppose G cyclique, i.e. fini et engendré par un $g \in G$. On note n l'ordre de G.

[R] 14 Ex 20 : Le groupe des racines complexes de l'unité : $\mathbb{U}_n = \langle e^{\frac{2i\pi}{n}} \rangle$

[R] 14 Thm 21 : G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

[R] 14 Prop 22 : Les générateurs de G sont les g^k avec $k \wedge n = 1$.

[R] 16 Prop 23 : Pour tout $d \in \mathbb{N}$ divisant n, G admet un unique sous-groupe d'ordre d, qui est $\langle g^{\frac{n}{d}} \rangle$.

[R] 14 Prop 24 : Tout groupe d'ordre premier est cyclique.

[R] 15 Prop 25 : Si n et $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ sont premiers entre eux, alors tout groupe abélien d'ordre n est cyclique.

Ex 26 : Tout groupe abélien d'ordre 15 est cyclique

[R] 25 Thm 27 : Tout sous-groupe fini du groupe cyclique d'un corps est cyclique.

B - Le théorème de structure

Dans ce paragraphe, on suppose G abélien, fini et non trivial.

Thm 28 (des restes chinois) : Soient n et m deux entiers naturels plus grands que 2 et premiers entre eux. Les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes. [R] 285

Thm (de structure des groupes abéliens finis) Il existe d'uniques $r \geq 1$ et $a_1, \dots, a_r \geq 2$ tels que $G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_r\mathbb{Z}$ et $a_1 | a_2 | \dots | a_r$. [R] 27

Ex 29 : Tout groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $(\mathbb{Z}/p\mathbb{Z})^2$.

Ex 30 : Classification des groupes abéliens de petit ordre :

Ordre	1	2	3	4	5	6	7	8	9
Classe d'isom.	$\{1\}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^3$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/9\mathbb{Z}$ $(\mathbb{Z}/3\mathbb{Z})^2$

III - Groupes non abéliens finis

A - Groupes symétriques

Soit $n \geq 2$.

Prop 31 : Si X est un ensemble de cardinal n, alors $\mathfrak{S}(X) \simeq \mathfrak{S}_n$. [R] 39

Prop 32 : $\mathfrak{S}_n$ n'est pas abélien. [R] 39

Prop 33 : Deux permutations à supports disjoints commutent [R] 40

Thm 34 : Toute permutation se décompose de manière unique, à l'ordre des facteurs près, en produit de cycles à supports disjoints. [R] 42

Prop 35 : $(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$

[R] 44 45 Prop 36 : $\mathfrak{S}_n = \langle (i,j) : 1 \leq i,j \leq n \rangle = \langle (1,i) : 1 \leq i \leq n \rangle$
$= \langle (i,i+1) : 1 \leq i \leq n \rangle = \langle (1,2), (1,2,\dots,n) \rangle$.

[R] 47 Thm 37 : Il existe un unique morphisme $\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ qui envoie les transpositions sur -1 : on l'appelle morphisme signature.

[R] 49 Def 38 : Le n^e groupe alterné est $\mathcal{A}_n = \mathrm{Ker}(\varepsilon)$.

[R] 50 Thm 39 : Pour $n \geq 5$, $\mathcal{A}_n$ est simple.

B - Groupes d'isométries

[R] 83 Def 40 : Le n^e *groupe diédral* $(n \geq 3)$ est le groupe des isométries du plan qui conservent le polygône régulier à n côtés, de sommets $\begin{pmatrix} \cos\left(\frac{2k\pi}{n}\right) \\ \sin\left(\frac{2k\pi}{n}\right) \end{pmatrix}$.
On le note D_{2n}. FIGURE 1

[R] 83 Prop 41 : Si G contient un élément s d'ordre 2 et un élément d'ordre n tels que sr est d'ordre 2, alors $G \simeq D_{2n}$.

[R] 94 Thm 42 : L'ensemble des isométries du plan conservant un triangle équilatéral est un groupe isomorphe à $\mathfrak{S}_3$.

[R] 82 Prop 43 : Soit $\mathcal{C}$ un cube. L'ensemble des isométries de l'espace conservant $\mathcal{C}$ est un groupe, noté $Is(\mathcal{C})$. On note $Is^+(\mathcal{C})$ le sous-groupe de $\mathcal{C}$ formé de rotations. FIGURE 2

[R] 85 Thm 44 : $Is^+(\mathcal{C}) \simeq \mathfrak{S}_4$ et $Is(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ DEV 2

Thm 45 : En notant $\mathcal{T}$ le tétraèdre régulier, on a : [R] 95

$$Is(\mathcal{T}) \simeq \mathfrak{S}_4 \text{ et } Is^+(\mathcal{T}) \simeq \mathcal{A}_4$$

RÉFÉRENCES

[R] : Mathématiques pour l'agrégation - Algèbre et géométrie (Jean-Étienne Rombaldi)
[U] : Théorie des groupes (Félix Ulmer)
[S] : Algèbre pour la licence 3 (Szpirglas).

FIGURE 1 : Isométries du pentagone.

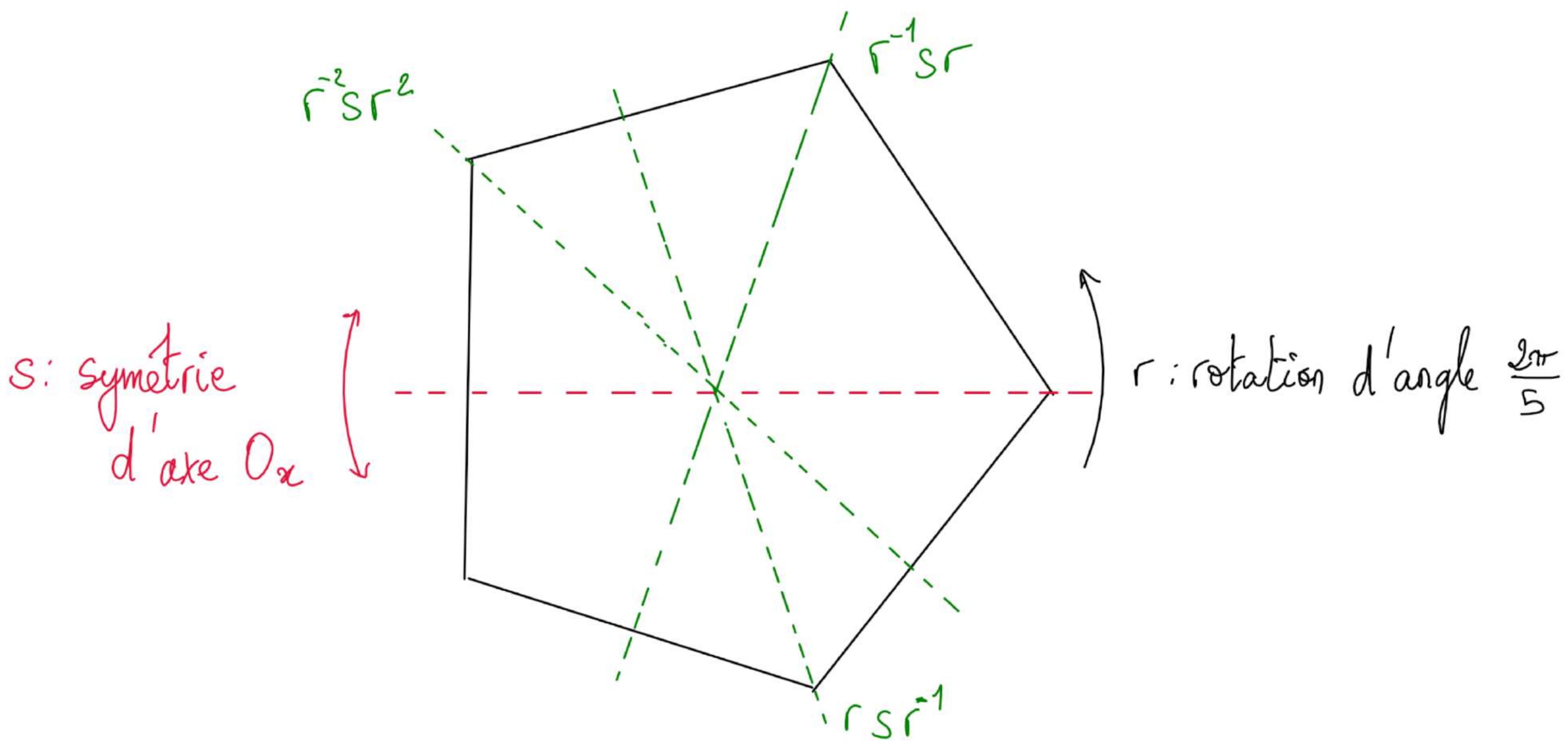
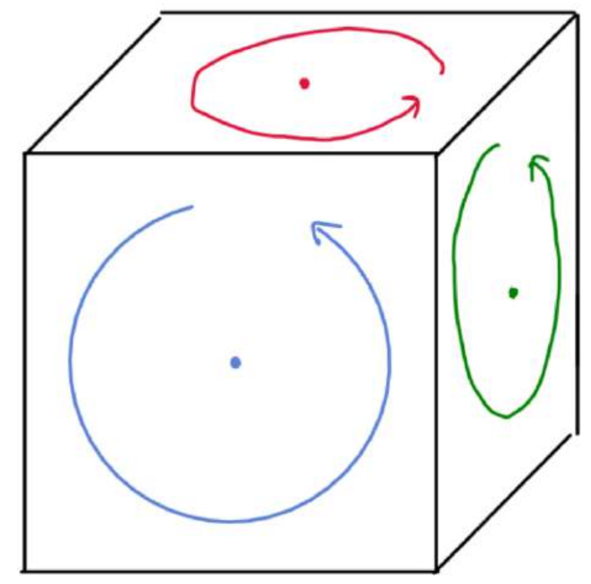
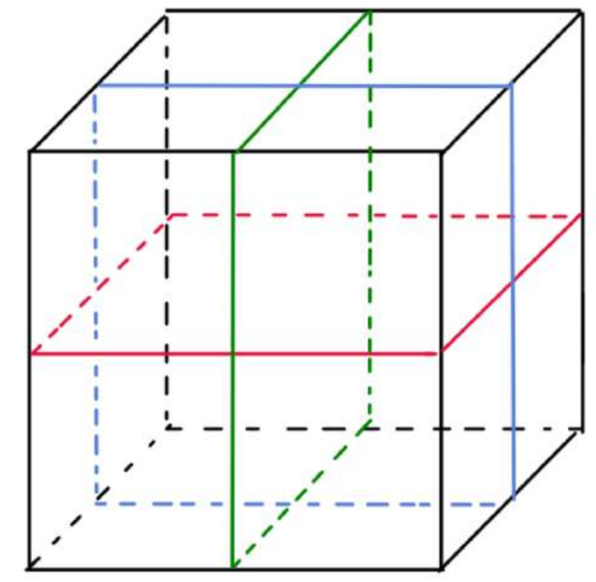


FIGURE 2 : Isométries du cube

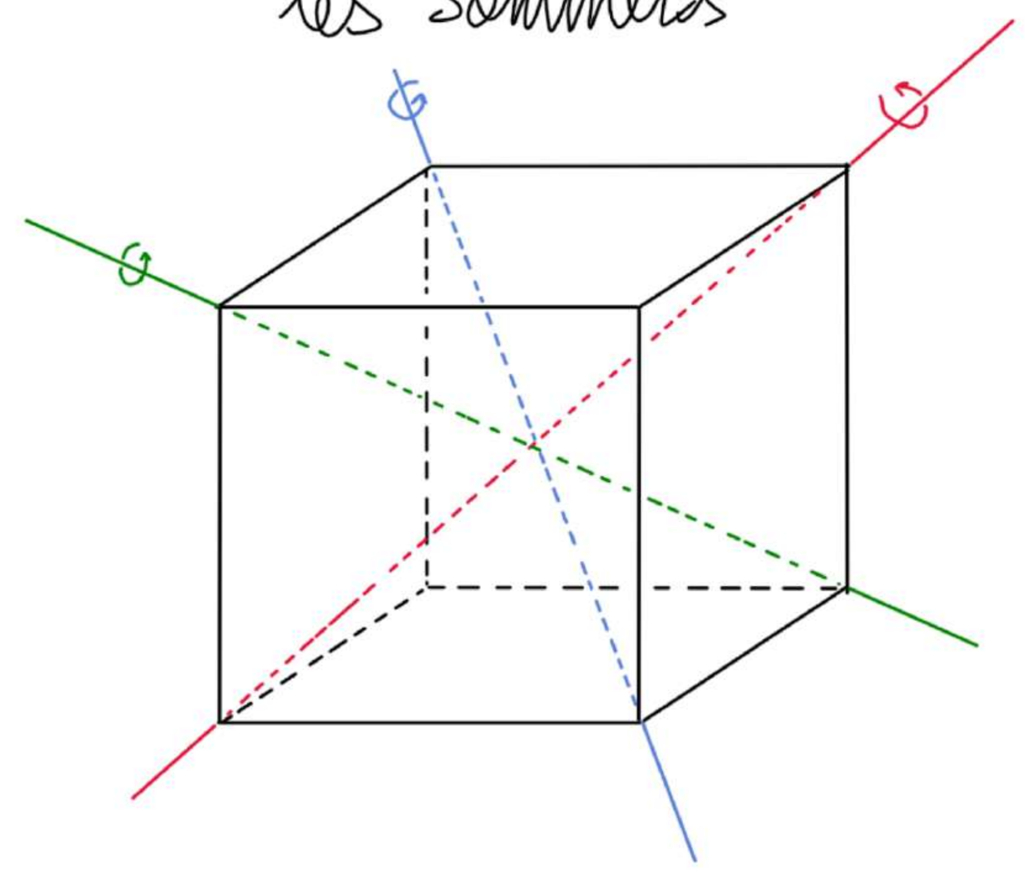
Rotations passant par les faces



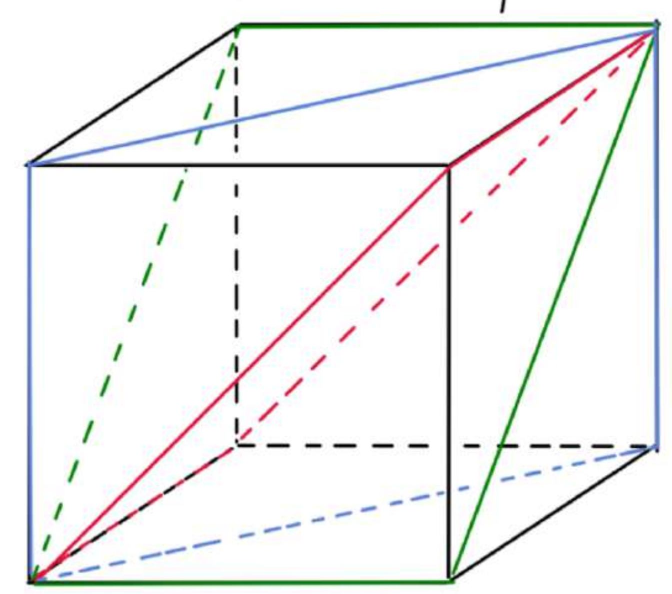
Symétries coupant les faces



Rotations passant par les sommets



Symétries passant par une arête



(pas toutes représentées)

Rotations passant par les arêtes