Groupes et actions de groupes

Soyons honnêtes : l'introduction des groupes et structures algébriques dans le cours « principal » est un peu artificielle.

Ce petit document tente de revenir à des origines plus intuitives pour introduire la notion de groupe et mieux comprendre son intérêt. Cela demande un peu plus de travail et c'est la raison pour laquelle ce document est placé à part.
On y verra que les actions de groupes, loin d'être une application compliquée des groupes y jouent un rôle très naturel.

1 Manipuler un triangle

A Trouver des actions invariantes

Prenons l'exemple du polygone le plus simple : le triangle.
On peut se demander ce qui distingue *fondamentalement* un triangle quelconque, d'un triangle isocèle ou d'un triangle équilatéral.
Une façon de voir est de prendre sa règle (ou son compas) et de mesurer les longueurs des côtés :

- pour un triangle quelconque, on obtient en général trois mesures différentes,
- pour un triangle isocèle, on en obtient deux,
- pour un triangle équilatéral, on en obtient une seule : tous les côtés ont même longueur.

Mais il semble encore plus naturel pour un enfant d'essayer de replier le triangle sur lui-même de différentes façon, ou de le faire tourner, et d'observer si on trouve des superpositions.

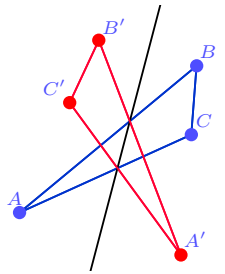
Quand on a une pièce de papier triangulaire pour faire des origamis :

- est-ce que la retourner recto/verso change quelque chose ?
- est-ce qu'il n'y a qu'une seule orientation possible, ou est-ce qu'en faisant tourner la pièce sur elle-même d'un certain angle, je retrouve la même figure ?

C'est le genre de questions que l'on retrouve aussi dans l'étude la nature en physique et en chimie : est-ce que je vois la même chose si je regarde ma modécule depuis l'autre côté ? ou ai-je l'impression que ce sont deux molécules différentes ?

Si on revient au triangle et aux différents pliages possibles, on observe que :

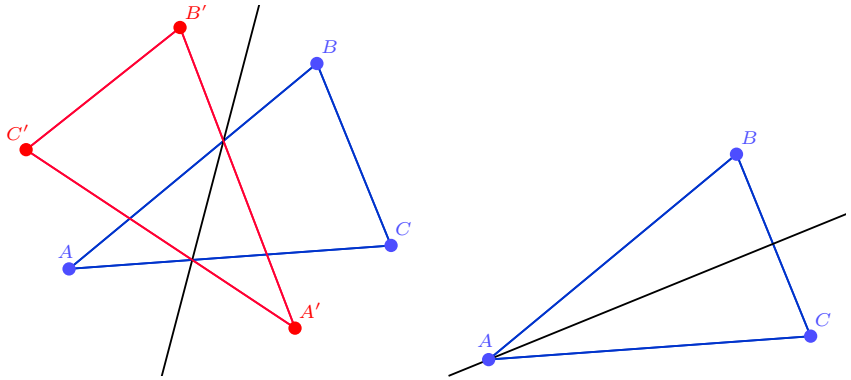
- Le triangle quelconque[1] ne possède aucun axe de symétrie. Quelle que soit la position de la pliure que je choisis, les parties du triangle ne se superposent pas.



Lorsqu'on réalise la symétrie par rapport à n'importe quel axe, on n'a JAMAIS superposition des deux triangles.

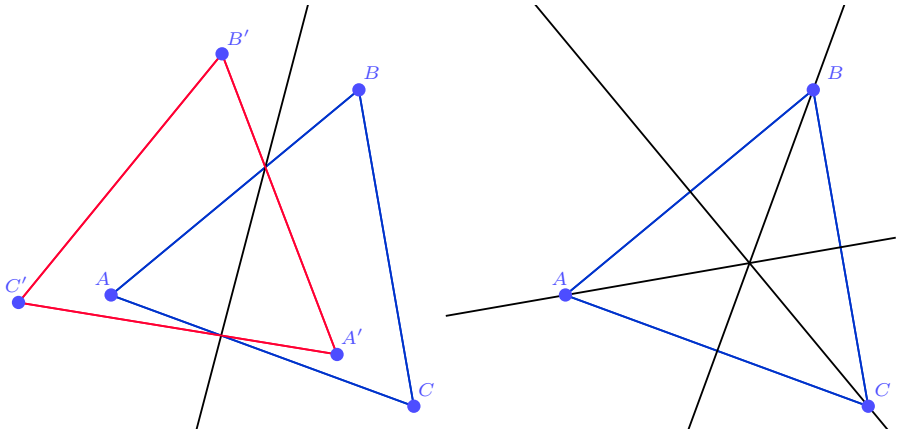
1. Ici, par abus, on désigne par triangle quelconque, un triangle qui n'est pas isocèle (ni équilatéral), donc qui n'est pas quelconque !

- Le triangle isocèle[2] possède un unique axe de symétrie : la médiatrice au troisième côté.



Parmi tous les axes, seule la médiatrice du côté $[BC]$ est un axe de symétrie. Le triangle et son symétrique se superposent parfaitement.

- Le triangle équilatéral possède trois axes de symétrie : ses trois médiatrices.



Seules les médiatrices rendent le triangle invariant par symétrie.

On voit donc que les triangles peuvent être caractérisés (classés) suivant leurs symétries. En fonction de leur nature, les triangles possèdent certaines symétries qui les rendent **invariants**[3]**.**

2. Ici, on parle de triangle isocèle dans un sens exclusif, c'est-à-dire, un triangle isocèle, mais pas équilatéral.
3. Si on applique ces symétries aux triangles, ils se superposent.

B Composer les actions

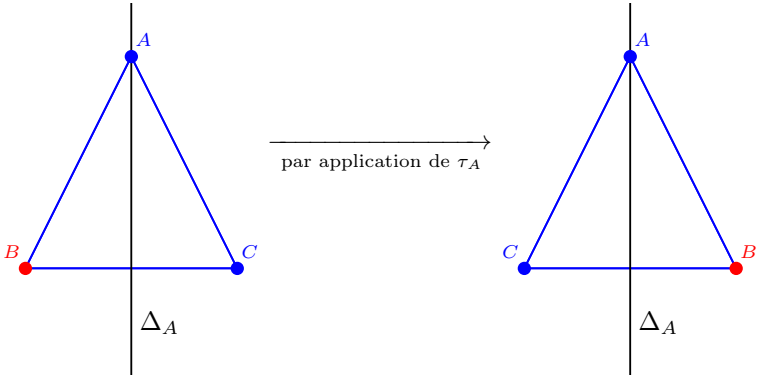
Si on considère deux actions qui rendent un triangle invariant, alors on peut les composer l'une à la suite de l'autre, et cela donne encore une action qui rend le triangle invariant.
Cependant, c'est le triangle dans son ensemble qui n'est pas modifié et les points sont individuellement déplacés comme par un jeu de chaises musicales. Ils sont mélangés, c'est-à-dire permutés.

Voyons cela sur les exemples :

Le triange isocèle : Pour le triangle ABC isocèle en A, il n'y a qu'un seul axe de symétrie qui est la médiatrice Δ_A au segment $[BC]$ et on peut noter τ_A, la symétrie correspondante.
τ_A agit sur ABC par

$$\tau_A \cdot (ABC) = (ACB).$$

Les points C et B ont été permutés.



De même

$$(\tau_A \circ \tau_A) \cdot (ABC) = \tau_A \cdot (ACB) = ABC.$$

On retrouve le triangle de départ donc :

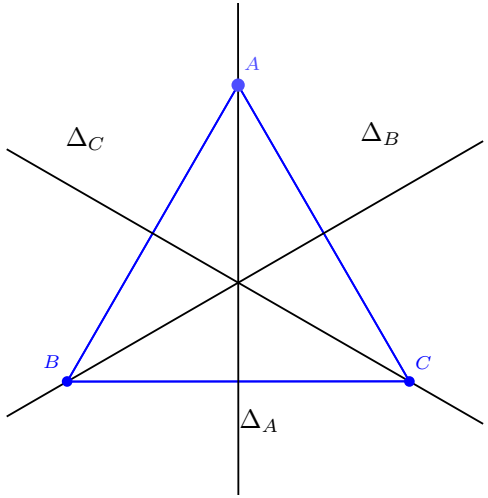
$$\tau_A \circ \tau_A = \mathrm{Id}.$$

On obtient ainsi une table de composition très simple :

$\circ$	Id	τ_A
Id	Id	τ_A
τ_A	τ_A	Id

Le triangle équilatéral : Pour le triangle ABC équilatéral, on a désormais trois axes de symétrie : Δ_A, Δ_B et Δ_C qui sont les médiatrices des trois côtés.
On peut noter τ_A, τ_B et τ_C les trois symétries correspondantes.
Voyons comment elles agissent sur le triangle.

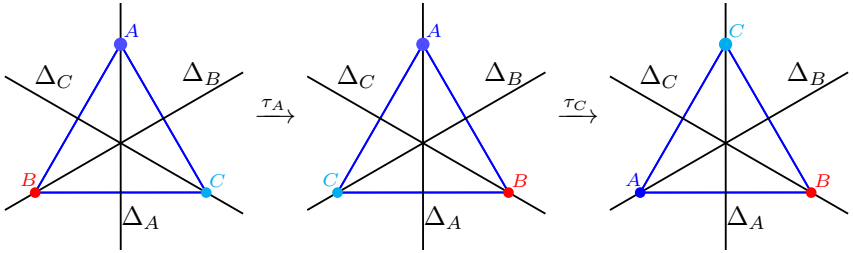
$$\tau_A \cdot (ABC) = (ACB)$$
$$\tau_B \cdot (ABC) = (CBA)$$
$$\tau_C \cdot (ABC) = (BAC)$$



À présent, on peut s'amuser à composer les symétries entre elles pour voir quelles actions on obtient :

$$(\tau_C \circ \tau_A) \cdot (ABC) = \tau_C \cdot (ACB) = (CAB).$$

⚠ ici, quand on transforme le triangle, on ne touche pas aux droites même si on renomme les sommets.
Voici graphiquement ce qu'on a fait :



Génial ! On vient de découvrir une nouvelle transformation qui rend le triangle invariant. C'est la rotation d'angle $\frac{2\pi}{3}$, que l'on peut noter R. On voit qu'elle ne correspond à aucune des symétries énoncées précédemment.

$$\tau_C \circ \tau_A = R.$$

On complète donc la liste des transformations et on continue à tester les compositions pour voir ce que ça donne.
Avec $R \circ R$, on trouve bien évidemment la rotation d'angle $\frac{4\pi}{3}$ que l'on note alors R^2.
Enfin $R^2 \circ R$ revient à faire trois fois la rotation d'angle $\frac{2\pi}{3}$, ce qui donne une rotation d'angle 2π : les points sont inchangés. On note cette dernière transformation Id.

Si on essaie toutes les autres compositions, aucune nouvelle transformation n'apparaît. Faites-le en exercice pour bien comprendre.

On peut résumer avec un tableau. Ici, on applique d'abord la transformation indiquée par la colonne, puis celle de la ligne.

$\circ$	Id	R	R^2	τ_A	τ_B	τ_C
Id	Id	R	R^2	τ_A	τ_B	τ_C
R	R	R^2	Id	τ_B	τ_C	τ_A
R^2	R^2	Id	R	τ_C	τ_A	τ_B
τ_A	τ_A	τ_C	τ_B	Id	R^2	R
τ_B	τ_B	τ_A	τ_C	R	Id	R^2
τ_C	τ_C	τ_B	τ_A	R^2	R	Id

Dans la suite, on désignera l'ensemble de ces six transformations comme **le groupe des isométries du triangle équilatéral** $\mathrm{Iso}(T)$.

C Action de groupe sur un ensemble

Lors du travail précédent, on a vu que toute la structure qui portait initialement sur le triangle, a été comme transmise à son groupe des isométries : $\mathrm{Iso}(T)$ utilisé avec la loi de composition. Connaître le groupe des isométries qui laissent invariant un triangle, c'est connaître la nature de ce triangle.
Cette idée conçue par Galois est tout à fait essentielle : connaître le groupe des invariants d'un ensemble donne beaucoup d'informations sur cet ensemble. Cette idée est largement utilisée en cristallographie.

Ici, on considère l'ensemble des 6 configurations possibles pour le triangle équilatéral :

$$\mathcal{T} = \{(ABC), (ACB), (BAC), (BCA), (CAB), (CBA)\}.$$

Les isométries de $\mathrm{Iso}(T)$ permettent alors de passer d'une configuration à une autre :

On a fait **agir** le groupe $\mathrm{Iso}(T)$ sur l'ensemble $\mathcal{T}$.

D Vers la définition du groupe

Le travail qui a été fait pour le triangle isocèle et le triangle équilatéral peut être conduit sur d'autres types de figures, quadrilatères quelconques, carrés, pentagones réguliers... Mais aussi sur d'autres structures dont on voudrait étudier les symétries.

L'idée de Galois était de faire agir des groupes sur les racines des polynômes, pour étudier les symétries et tenter de trouver des méthodes de résolution.

Cayley s'appuya sur cette idée pour donner en 1854 la première définition d'un groupe (fini) :
« A set of symbols,

$$1, \alpha, \beta, ...$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a group[4]. »
S'en suit dans son article[5] une table de composition (ou produit) exactement de la forme de celles que l'on a produites pour les isométries du triangle isocèle ou du triangle équilatéral.

Pour paraphraser Cayley, on observe que tous les groupes d'isométrie ont une structure similaire :

- Il y a toujours l'isométrie Id – que Cayley note 1 – : celle qui ne fait rien.
  En théorie des groupes, on parle d'**élément neutre.**
- Les isométries se composent entre elles et la composition de deux isométries reste évidemment une isométrie.
  On dit que le groupe est muni d'une **loi de composition interne** $\circ$.

De notre côté, on peut rajouter encore deux propriétés qui n'ont pas été explicitement données par Cayley :

- Toute transformation peut être faite dans les deux sens : à chaque isométrie correspond une isométrie réciproque, ou **inverse.**
  Cette propriété est implicite dans la définition donnée par Cayley.
- Enfin, la loi de composition est **associative.**
  Si on ne pense pas à cette condition, c'est parce qu'elle est tellement naturelle qu'on n'imagine pas travailler sans elle (l'addition, le produit, la composition... sont toutes des lois associatives).
  Par contre, on voit bien que S_3 n'est absolument pas commutatif : $R \circ \tau_A = \tau_C$ et $\tau_A \circ R = \tau_B$.

4. The idea of a group as applied to permutations or substitutions is due to Galois, and the introduction of it may be considered as marking an epoch in the progress of the theory of algebraical equations.
5. L'article de Cayley est librement consultable en ligne à l'adresse `https://archive.org/details/collectedmathema02cayluoft/page/124`.

2 Définitions liées à la notion de groupe

A Groupe

Dans la partie précédente, nous avions abouti à la définition suivante :

Définition 2.1 *(Groupe)*

Un **groupe** est un ensemble G muni d'une loi *interne* $\star$ tel que :

- la loi $\star$ est associative,
- G contient un élément neutre e pour la loi $\star$,
- tout élément x de G admet un symétrique pour $\star$.

Lorsque la loi $\star$ est commutative, on dit que le groupe est commutatif, ou *abélien.*

On pourra trouver en annexe 6, les définitions claires de tous les termes (loi interne, associativité...) pour ne laisser aucune ambigüité. Cependant, la lecture de ce qui a précédé devrait suffir à comprendre les notions essentielles.

B Sous-groupes

Dans l'exemple sur le triangle équilatéral, on se rend compte que si on ne considère qu'un seul axe de symétrie (ce qui revient à ne voir le triangle qu'isocèle), alors on obtient aussi un groupe qui agit sur le triangle.
Il est évident qu'il vérifie bien toutes les propriétés d'un groupe puisqu'il correspond aux isométries qui rendent invariant le triangle isocèle.
C'est un **sous-groupe** du groupe $\mathrm{Iso}(T)$.

Il existe d'autres sous-groupes de $\mathrm{Iso}(T)$: le plus simple est de considérer le triangle comme quelconque ce qui ne laisse plus que l'identité. C'est ce qu'on appelle le sous-groupe *trivial* : on ne prend que l'élément neutre.

On peut aussi ne considérer que les rotations : $\{\mathrm{Id}, R, R^2\}$. Si on les compose entre-elles, l'ensemble est *stable* : pas besoin d'ajouter d'autres éléments.
On obtient la table de Cayley qui est une extraction de celle qu'on avait établi pour $\mathrm{Iso}(T)$.

$\circ$	Id	R	R^2
Id	Id	R	R^2
R	R	R^2	Id
R^2	R^2	Id	R

Pour avoir un sous-groupe, il faut essentiellement que la loi reste interne. C'est-à-dire que les objets se suffisent à eux-même et si on les compose entre eux, cela ne conduit à aucun nouvel objet hors de cette liste.

Pour un groupe avec un nombre fini d'éléments (comme nous les avons vus jusqu'à

présent), cette définition est suffisante. Cependant, lorsque le sous-groupe est composé d'un nombre infini d'éléments on a besoin de vérifier en plus que l'inverse est bien dans le sous-groupe.

Définition 2.2 *(Sous-groupe)*

Soit $(G, \star)$ un groupe.
Un **sous-groupe** de $(G, \star)$ est un groupe $(G', \star)$ avec G' une partie stable de G pour la loi $\star$.

Si pour $x \in G$, on note x^{-1} l'opération inverse de x, c'est-à-dire qui vérifie $x \star x^{-1} = x^{-1} \star x = e$, alors on peut reformuler la définition d'un sous-groupe :

Théorème 2.3 *(Caractérisation des sous-groupes)*

Soit $(G, \star)$ un groupe et $G' \subset G$.
$(G', \star)$ est un sous-groupe de $(G, \star)$ si, et seulement si

1. G' est non vide.
2. $\forall (x, x') \in (G')^2,\ x \star x' \in G'$.
3. $\forall x \in G',\ x^{-1} \in G'$.

Remarques :

- Puisque $(G, \star)$ est un groupe, on sait déjà que $\star$ est associative et il ne sert à rien de refaire la vérification pour G'.
- Souvent pour montrer que G' est non vide, on montre qu'il contient l'élément neutre e de G.
- Les deux derniers points pevent être vérifiés en une seule étape :

$$\forall (x, x') \in (G')^2,\ x \star x'^{-1} \in G'.$$

Preuve

Le sens direct est trivial.
Pour le sens réciproque :

- on sait que G' non vide, donc il contient un élément x.
  alors $x^{-1} \in G'$, et par stabilité par produit, $x \star x^{-1} = e \in G'$.
  Ainsi G' contient bien l'élément neutre.
- G' contient l'inverse de tous ses éléments (en prenant $x = e$ dans le deuxième point).
- G est stable par produit par hypothèse.
- L'associativité est directement héritée de G.

Lorsque l'on « fusionne » les deux derniers points comme indiqué dans les remarques, on obtient la même preuve :

- Avec $x \in G'$, on trouve $x \star x^{-1} = e \in G'$.
- En prenant $(e, x) \in (G')^2$, on obtient la stabilité par passage à l'inverse : $x^{-1} = e \star x^{-1} \in G'$.
- Puisque pour tout $x' \in G'$, $x'^{-1} \in G'$, alors pour $x \in G'$, on a encore $x \star x' = x \star \left(x'^{-1}\right)^{-1} \in G'$.

■

Exemple

$\left(\mathbf{Q}_+^*, \times\right)$ est-il un groupe ? Même question pour $\mathbf{R}_+^*$.
Solution :
Oui, ce sont des sous-groupes de $(\mathbf{Q}^*, \times)$ et $(\mathbf{R}^*, \times)$.

Exemple

Montrer que l'ensemble des racines n-ièmes de l'unité $\mathbf{U}_n = \left\{ \mathrm{e}^{\frac{2ik\pi}{n}} \right\}_{k \in [\![0, n-1]\!]}$ muni du produit est un groupe.

Exemple

Soit $(G, \star)$ un groupe. Montrer que pour tout $x \in G$,

$$\forall (y, z) \in G^2,\ xy = yz \Rightarrow y = z.$$

On dit alors que x est *régulier à gauche.*
Solution :
Soient $(y, z) \in G^2$ tels que $xy = xz$, alors en multipliant par x^{-1} à gauche, on trouve $y = z$.
Ainsi x est régulier à gauche. On peut montrer de même qu'il est régulier à droite en multipliant à droite par x^{-1} : x est régulier.

Exemple

Montrer que si G' est un sous-groupe de G, alors son complémentaire dans G n'en est pas un.
Solution :
Il ne contient pas l'élément neutre.

On reprendra la notion de sous-groupe en fin de document sur un exemple en cardinal fini.

C Des exemples de groupes

Quelques exemples concrets de groupes, en plus des permutations du triangle.

Exemple *(Groupes additifs)*

- $(\mathbf{N}, +)$ n'est pas un groupe car ses éléments non nuls n'admettent pas d'inverse (c'est-à-dire d'opposé).
- $(\mathbf{Z}, +)$ est un groupe commutatif.
- $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ et $(\mathbf{C}, +)$ sont des groupes commutatifs.
- $(\mathscr{M}_{n,p}(\mathbf{K}), +)$ est un groupe commutatif.

Exemple *(Groupes multiplicatifs)*

Pour avoir un groupe multiplicatif sur les ensembles de nombres, il est nécessaire de retirer le 0 qui n'admet par d'inverse pour le produit.

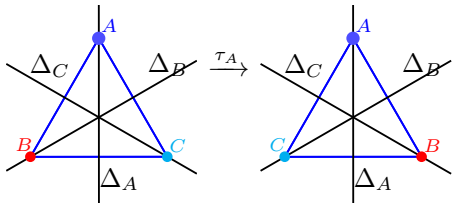
- $(\mathbf{Z}^*, \times)$ n'est pas un groupe.
- $(\mathbf{Q}^*, \times), (\mathbf{R}^*, \times)$ et $(\mathbf{C}^*, \times)$ sont des groupes commutatifs.
- $(\mathbf{U}, \times)$, l'ensemble des nombres complexes de module 1, muni du produit est un groupe commutatif.
- L'ensemble des rotations de centre O, muni de la loi de composition est un groupe.
- $(\mathrm{GL}_n(\mathbf{K}), \times)$ est un groupe non commutatif $(n \geqslant 2)$.

3 Morphismes de groupes

A Comment dupliquer un groupe ?

Dans notre cas, on peut oublier l'apparence du triangle équilatéral et considérer trois points quelconques de l'espace : au lieu de donner une signification géométrique aux isométries, on les interprète comme des permutations entre ces points.
Par exemple, τ_A est l'échange entre les deux derniers points :

$$\tau_A \cdot (ABC) = (ACB), \text{ ou encore } \tau_A \cdot (CAB) = (CBA).$$



Si on note $(S_3, \circ)$ le groupe des permutations d'un ensemble à trois éléments, et $(\mathrm{Iso}(T), \circ)$ le groupe des isométries du triangle équilatéral, alors ces deux groupes se correspondent exactement.
On retrouve par exemple qu'il existe exactement $3! = 6$ permutations différentes[6].
Formellement ces ensembles $\mathrm{Iso}(T)$ et S_3 restent différents, voyons donc comment traduire cette correspondance « parfaite » entre les deux :

- D'une part, il y a un lien bijectif entre $\mathrm{Iso}(T)$ et S_3.
- D'autre part, toute composition de deux permutations correspond exactement à la composition des deux symétries correspondantes.

6. Pour n objets distincts, il y a exactement $n!$ façons de les mélanger. Un mélange correspond à tirer les objets dans un certain ordre. Au premier tirage on a n possibilités, puis au second $n-1$,... puis au dernier tirage, on n'a plus qu'une seule possibilité. Les possibilités se multiplient entre elles pour donner $n!$ tirages possibles. Voir le chapitre de dénombrement pour plus de précisions.

Le lien entre les deux est plus fort qu'une simple bijection car il transmet les opérations. Ainsi, toute opération faite d'un côté, se retrouve également de l'autre côté.
On parle d'**isomorphisme** : les deux ensembles munis de leur loi ont la *même forme*[7], ils sont comme des copies l'un de l'autre en changeant simplement le nom donné à chaque objet.

Prenons un autre exemple :
Si on ne regarde que les rotations de $\mathrm{Iso}(T)$, alors on peut aussi lire un morphisme immédiat en associant chaque rotation au nombre de tiers de tours accomplis. Ainsi $\mathrm{Id} \mapsto 0$, $R \mapsto 1$ et $R^2 \mapsto 2$ et on voit alors que $R \circ R^2 = R^3 = \mathrm{Id} = R^0$ correspond au calcul modulo 3 : $1 + 2 = 0$ [3].
On note $(\mathbf{Z}/3\mathbf{Z}, +)$ les entiers sur lesquels on réalise des additions modulo 3, et on compare sa table de Cayley avec celle des rotations. On trouve la confirmation qu'il s'agit de la même table (en changeant simplement les noms).

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table de Cayley de $(\mathbf{Z}/3\mathbf{Z}, +)$

$\circ$	Id	R	R^2
Id	Id	R	R^2
R	R	R^2	Id
R^2	R^2	Id	R

Table de Cayley des rotations

Les deux groupes sont **isomorphes** et tout ce que l'on pourra dire de l'un sera également vrai de l'autre.
Par exemple, il est trivial que $\mathbf{Z}/3\mathbf{Z}$ est commutatif, donc le groupe des rotations qui laissent invariant le triangle équilatéral l'est aussi.

Définition 3.1 *(Isomorphisme de groupes)*

Soient $(G, \times)$ et $(G', \star)$ deux groupes (notés multiplicativement).
Soit $f : G \to G'$ une application **bijective.**
f est un **isomorphisme de groupe**, si, et seulement si

$$\forall (x, x') \in G^2,\ f(x \times x') = f(x) \star f(x').$$

Plus généralement, si l'application « transporte » la structure sans pour autant être bijective, on parle simplement de morphisme de groupe.

Définition 3.2 *(Morphisme de groupes)*

Soient $(G, \times)$ et $(G', \star)$ deux groupes (notés multiplicativement).
Soit $f : G \to G'$ une application.
f est un **morphisme de groupe**, si, et seulement si

$$\forall (x, x') \in G^2,\ f(x \times x') = f(x) \star f(x').$$

7. Le terme morphisme vient du grec et désigne la forme, comme c'est le cas lorsqu'on parle de morphologie en médecine. *iso* veut dire « même », comme dans *isométrie* : même longueur.

Ces morphismes ne font pas des copies conformes entre deux groupes, mais montrent plutôt qu'un groupe représente un aspect particulier d'un autre. On voit bien que cette notion sera aussi très utile dans l'optique de *dévisser* un groupe.
Par isométrie, on dispose donc de deux nouveaux groupes :

Exemple *(Groupe symétrique)*
Pour E un ensemble, les permutations de E munies de la composition forment un groupe, noté $S(E)$.
En particulier, si $n \geqslant 1$ et $E = \{1, \cdots, n\}$, alors le groupe symétrique (des permutation) est noté S_n.

Exemple *($\mathbf{Z}/n\mathbf{Z}$)*
Pour $n \in \mathbf{N}^*$, on désigne par $\mathbf{Z}/n\mathbf{Z}$ l'ensemble des entiers modulo n.
Muni de l'addition, $(\mathbf{Z}/n\mathbf{Z}, +)$ est un groupe (commutatif).

B Transport de la structure par morphisme

On obtient une propriété aussi pratique que naturelle : les morphismes transportent la structure de groupe.

- Si on prend l'élément neutre d'un côté, on obtient aussi l'élément neutre de l'autre : c'est-à-dire que si on ne fait rien d'un côté, alors on ne fait rien non plus de l'autre.
- Si on prend l'inverse d'un côté, on obtient aussi l'inverse de l'autre : c'est-à-dire que si on défait d'un côté, alors on défait aussi de l'autre.

Formellement, cela donne :

Propriété 3.3

Soit $f : G \to G'$ un morphisme de groupes (notés multiplicativement).
Si e est l'élément neutre de G et e' celui de G', alors

- $f(e) = e'$.
- $\forall x \in G,\ f\left(x^{-1}\right) = (f(x))^{-1}$.

Preuve

- $f(e) = f\left(e^2\right) = (f(e))^2$.
  Or $f(e) \in G'$ admet un inverse, et donc en multipliant l'égalité du dessus par cet inverse on obtient
  $$e' = f(e).$$
- Soit $x \in G$, $e' = f(xx^{-1}) = f(x)f\left(x^{-1}\right)$ et $e' = f(x)\,f(x)^{-1}$.
  Donc $f\left(x^{-1}\right) = (f(x))^{-1}$.

■

Plus généralement, si une partie forme un groupe, alors son image sera aussi un groupe (que ce soit l'image directe ou réciproque).

Théorème 3.4

Soit $f : G \to G'$ un morphisme de groupe.

- Si H est un sous groupe de G alors $f(H)$ est un sous groupe de G'.
- Si H' est un sous groupe de G' alors $f^{-1}(H')$ est un sous groupe de G.

Preuve

- On considère donc H sous groupe de G.
  Montrons que $H' = f(H)$ est un sous-groupe de G'.
  Il est tout d'abord évident que $H' \subset G'$ par définition de f.
  - $e \in H$, car c'est un sous groupe de G et $f(e) = e'$, donc $e' \in H'$.
  - Soit $(y, y') \in H'^2$, alors par définition de H', il existe $(x, x') \in H^2$ tel que $y = f(x)$ et $y' = f(x')$.
    Or $xx'^{-1} \in H$ (groupe) et $f\left(xx'^{-1}\right) = f(x)\,(f(x'))^{-1}$ (morphisme de groupes).
    Donc $yy'^{-1} = f\left(xx^{-1}\right) \in f(H) = H'$.

  H' est donc bien un sous groupe de G'.
- On considère à présent H' que l'on suppose un sous groupe de G' (sans lien avec les notations utilisées pour la preuve de l'image directe), et on note $H = f^{-1}(H')$.
  Montrons que H est un sous-groupe de G.
  Il est déjà évident, par définition, que $H \subset G$.
  - $f(e) = e' \in H'$ car H' est un sous-groupe de G' et f un morphisme de groupes.
    Donc $e \in f^{-1}(H') = H$.
  - Soit $(x, x') \in H^2$.
    Par définition $f(x) \in H'$ et $f(x') \in H'$ donc $f\left(xx'^{-1}\right) = f(x)\,(f(x'))^{-1} \in H'$
    donc $xx'^{-1} \in H$.

  Ce qui prouve donc bien que H est un sous groupe de G.

■

On voit donc que f transporte la structure de groupe « dans les deux sens ».
Donc lorsque f admet une application réciproque (c'est-à-dire qu'il est bijectif), alors cette application réciproque f^{-1} transporte aussi la structure : c'est aussi un morphisme.

Propriété 3.5

Si $f : G \to G'$ est un isomorphisme, alors sa réciproque, f^{-1} est aussi un isomorphisme.

Preuve
Ce n'est pas le caractère bijectif de f^{-1} qui nous intéresse ici (c'est une trivialité), mais le fait que f^{-1} soit lui-même un morphisme de groupes.

Soit $(y,\, y') \in (G')^2$, alors, $f\left(f^{-1}(y)f^{-1}(y')\right) = f\left(f^{-1}(y)\right) f\left(f^{-1}(y')\right) = yy'$.
En composant par f^{-1}, on trouve alors

$$f^{-1}(yy') = f^{-1}(y)f^{-1}(y').$$

■

C Image et noyau

Définition 3.6 *(Noyau et image)*

Soit $f : G \to G'$ un morphisme de groupes.
On note e' l'élément neutre de G'.

- L'**image** de f, notée $\mathrm{Im}\,(f)$ est l'image directe de G par f :

$$\mathrm{Im}\,(f) = f(G) = \{f(x),\, x \in G\} \subset G'.$$

- Le **noyau** de f, noté $\ker(f)$ est l'image réciproque de $\{e'\}$ par f :

$$\ker(f) = f^{-1}(\{e'\}) = \{x \in G,\, f(x) = e'\} \subset G.$$

Théorème 3.7

Soit $f : G \to G'$ un morphisme de groupe.
$\ker(f)$ et $\mathrm{Im}\,(f)$ sont des sous groupes respectifs de G et G'.

Preuve

Ce sont des images directes et réciproques de groupes par f. ■

Théorème 3.8

Soit $f : G \to G'$ un morphisme de groupes.

$$f \text{ est injectif si, et seulement si } \ker(f) = \{e\}.$$

Où e désigne l'élément neutre de G.

Preuve

Sens direct : Si f est injective, alors e' l'élément neutre de G' admet au plus un antécédent par f.
Or $f(e) = e'$, donc e est l'unique antécédent de e' par f.
Donc $\ker(f) = \{e\}$.
Réciproquement : si $\ker(f) = \{e\}$ alors on considère $(x,\, x') \in G^2$ tel que $f(x) = f(x')$.
Ainsi $f(x)\left(f(x')\right)^{-1} = e'$ donc $f\left(xx'^{-1}\right) = e'$.
Donc $xx^{-1} \in \ker(f) = \{e\}$ donc $x = x'$ ce qui prouve bien que le morphisme est injectif. ■

Méthode

Pour montrer qu'un endomorphisme d'un groupe *fini* est un automorphisme, il suffit de montrer qu'il est injectif : son noyau est réduit à l'élément neutre.

Preuve

Une application injective entre deux ensembles finis de même cardinal[8] est bijective. ■

Exemple *(Automorphisme intérieur)*

Soit G un groupe et $g \in G$. On définit

$$f_g : \left\{ \begin{array}{ccc} G & \to & G \\ x & \mapsto & gxg^{-1}. \end{array} \right.$$

1. Montrer que f est un automorphisme.
2. On note Z l'ensemble des $g \in G$ tel que l'automorphisme f_g correspondant soit l'application identité.
   Montrer que Z est un sous-groupe de G.
   Comment décrire simplement ses éléments ?

Solution :

1. f est un morphisme, car $\forall (x,\, y) \in G^2$, $f(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = f(x)f(y)$.
   $f_{g^{-1}}$ est clairement le morphisme réciproque de f donc f est un isomorphisme.
2. $g \in Z \iff \forall x \in G,\, gxg^{-1} = x \iff \forall x \in G,\, gx = xg$.
   Ainsi Z est l'ensemble des éléments qui commutent avec tous les autres. On dit que Z est le *centre* de G.
   On a clairement $e \in Z$, avec e l'élément neutre.
   Si $x \in Z$, alors $\forall g \in G,\, gx^{-1} = x^{-1}xgx^{-1}$.
   Or $xg = gx$, donc $gx^{-1} = x^{-1}gxx^{-1} = x^{-1}g$, donc $x^{-1} \in Z$.
   Si $(x,\, y) \in Z^2$, alors $\forall g \in G,\, gxy = xgy = xyg$, donc $xy \in Z$.
   Ce qui prouve bien que Z est un sous-groupe de G.
   On peut aussi voir Z comme le noyau de l'application

$$\varphi : \left\{ \begin{array}{ccc} G & \to & S_G \\ g & \mapsto & \left(x \mapsto gxg^{-1}\right) \end{array} \right.$$

8. Vori le cours de dénombrement.

4 Actions de groupes

A Définition

Définition 4.1 *(Action de groupe sur un ensemble)*

Soit E un ensemble et $(G, \circ)$ un groupe.
Une action de groupe de G sur E est une application

$$\left\{\begin{array}{ccc} G\times E & \to & E \\ (g,\,x) & \mapsto & g\cdot x \end{array}\right.$$

qui vérifie $\forall (g,\,g')\in G^2$, $\forall x\in E$, $(g'\circ g)\cdot x = g'\cdot(g\cdot x)$ et $\forall x\in E$, $e\cdot x = x$.

Remarque : ici, on a défini des actions à gauche et on pourrait définir de la même façon une action à droite.

Exemple

Pour le triangle équilatéral, on obtient que S_3 agit sur le triangle (formellement, il peut prendre l'ensemble des six configurations possibles du triangle en fonction de l'ordre des lettres) par l'application de la transformation au triangle :

$$(s,\,(ABC)) \mapsto s\,(ABC)\,.$$

Exemple *(Un groupe qui agit sur lui-même)*

Si on regarde les tables de Cayley, on est surpris de constater que chaque ligne (ou chaque colonne) contient exactement une et une seule fois les élements du groupe.
Ce sont des copies réordonnées du groupe et on construit donc naturellement des actions de groupe où G agit sur lui-même.
On définit les actions à gauche et à droite par

$$\left\{\begin{array}{ccc} (G,\star)\times G & \to & G \\ (g,\,x) & \mapsto & g\star x. \end{array}\right. \qquad \left\{\begin{array}{ccc} G\times (G,\star) & \to & G \\ (x,\,g) & \mapsto & x\star g. \end{array}\right.$$

Par exemple, l'action à droite de $g = R$ sur S_3 donne

x	Id	R	R^2	τ_A	τ_B	τ_C
$x\cdot R$	R	R^2	Id	τ_B	τ_C	τ_A

C'est la ligne de la table de Cayley correspondant à R.
L'action à gauche donne la colonne correspondante.

Exemple

L'automorphisme intérieur vu précédemment est aussi une action de groupe de G sur lui-même.

B Toute action de groupe est un morphisme

On remarque que lorsqu'un groupe G agit sur un ensemble E ; alors pour chaque $g\in G$, l'action peut être vue comme une application de E dans lui-même :

$$\varphi_g \;:\; \left\{\begin{array}{ccc} E & \to & E \\ x & \mapsto & g\cdot x. \end{array}\right.$$

Cette application est bijective.
Injectivité : si $g\cdot x = g\cdot x'$, alors en faisant agir g^{-1}, on obtient $g^{-1}\cdot(g\cdot x) = g^{-1}\cdot(g\cdot x')$.
Or $g^{-1}\cdot(g\cdot x) = \left(g^{-1}\star g\right)\cdot x = e\cdot x = x$, et de même pour x', donc $x = x'$.
Surjectivité : Soit $y\in E$, pour la même raison que précédemment $y = g\cdot(g^{-1}\cdot x) = \varphi_g\left(g^{-1}\dot{x}\right)$ ce qui prouve bien la surjectivité.
On voit donc que $\varphi_g\in S(E)$ l'ensemble des permutations de E.
On peut alors voir l'action de groupe comme une application

$$f \;:\; \left\{\begin{array}{ccc} G & \to & S(E) \\ g & \mapsto & \varphi_g. \end{array}\right.$$

Cette application est un morphisme de groupes entre $(G,\star)$ et $(S(E),\circ)$.
En effet les axiomes de l'action de groupe correspondent exactement à la définition du morphisme : $\forall (g,\,g')\in G^2$, $\forall x\in E$,

$$f\,(g\star g')\,(x) = (g\star g')\cdot x = g\cdot(g'\cdot x) = \varphi_g(\varphi_{g'}(x)) = (\varphi_g\circ\varphi_{g'})(x).$$

Ainsi

$$f(g\star g') = f(g)\circ f(g').$$

Réciproquement, on vérifie aussi sans peine que tout morphisme de $(g,\star)$ sur $(S(E),\,)$ définit une action de groupe.

Action et morphisme

Définir une action de groupe de G sur E, revient à définir un morphisme de groupes de G vers $S(E)$.

C Orbites

Considérons un groupe G qui agit sur un ensemble E, par exemple le groupe S_3 qui agit sur les triangles équilatéraux.
On remarque que l'action de groupe définit une relation d'équivalence :

$$\forall (x,\,y)\in E,\; x\mathscr{R}y \iff \exists g\in G,\; x = g\cdot y.$$

Preuve

La relation est bien reflexive car $e\in G$ et $e\cdot x = x$,
elle est symétrique car tout élément $g\in G$ admet un symétrique g^{-1},
et elle est transitive car G est stable par produit. ■

Les classes d'équivalence correspondent à tous les objets qui peuvent se déduire l'un de l'autre par l'action de groupe. On les appelle **orbites.**

Définition 4.2 *(Orbite)*

Soit $(G, \star)$ un groupe, et E un ensemble.
On suppose que G agit sur E par l'action de groupe $(g, x) \mapsto g \cdot x$.
Pour tout $x \in E$, on définit l'**orbite** de x par

$$\mathscr{O}_x = \{g \cdot x,\ g \in G\},$$

Exemple *(Isométries du triangle équilatéral)*

- Si E désigne les 6 triangles équilatéraux et qu'on considère le groupe comme agissant globalement sur le triangle, alors si on ne s'intéresse qu'au groupe des rotations du triangle, on obtient deux orbites : les triangles en sens direct et ceux en sens indirect. En effet, une rotation conserve l'orientation d'un triangle, et un triangle indirect ne peut donc pas être obtenu par rotation depuis un triangle direct.
  Par contre, si on prend le groupe S_3 au complet, alors, il n'y a qu'une seule orbite :tout triangle peut être obtenu à partir d'un autre par une action de S_3.
- Si E_2 désigne cette fois-ci les trois points du triangle sur lequel on fait agir G. On obtient par exemple $R.A = C$ car le point A devient C par application de la rotation d'angle $2\pi/3$.
  Dans ce cas, tous les points sont dans la même orbite (que ce soit pour le groupe S_3, ou même pour le sous-groupe des rotations).
  En effet, A peut être remplacée par B ou C suivant que l'on applique R^2 ou R, et de même pour les autres sommets.
- Enfin, on peut considérer E_3 comme étant les arêtes orientées du triangle.
  À nouveau pour S_3, il n'y a qu'une seule orbite, mais pour les rotations, il y en a deux suivant l'orientation des arêtes.

Exemple *(Rubik's cube)*

Avec le Rubik's cube, toutes les configurations ne peuvent pas être obtenues à partir du cube initial (bien coloré). Ainsi, toutes les configurations que l'on peut atteindre à partir du cube bien coloré forment son orbite.
On peut imaginer d'autres orbites, en partant d'un cube coloré différemment au départ.
Ainsi, pour faire un cube, il convient de s'assurer que la configuration de départ est bien dans la même orbite que la configuration que l'on souhaite atteindre.
Si on garde les mêmes pièces mécaniques, alors les orbites correspondent à toutes les façon de remonter le Rubik's cube que l'on aurait démantelé. Ici, l'orbite est l'objet naturel à considérer, car deux cubes qui peuvent s'obtenir l'un de l'autre par de simples rotations des couronnes, doivent être considérés comme identiques.

Dans le langage courant, lorsque l'on dit que deux objets sont égaux à une permutation près (par exemple), c'est que l'on affirme qu'ils font partie de la même orbite pour l'action de groupe des rotations.

Définition 4.3 *(Action transitive)*

Soit $(G, \star)$ un groupe qui agit sur un ensemble E.
On dit que G agit **transitivement** sur E (ou que l'action est transitive) s'il n'y a qu'une seule orbite.
C'est-à-dire si

$$\forall (x, y) \in E,\ \exists g \in G,\ y = g \cdot x.$$

Lorsqu'on s'intéresse à un objet x particulier sous l'action de G il est souvent pratique de considérer l'application orbitale associée :

Définition 4.4 *(Application orbitale)*

Soit $(G, \star)$ un groupe qui agit sur un ensemble E.
Soit $x \in E$, on définition alors l'**application orbitale** par

$$\begin{cases} G & \to & \mathscr{O}_x \\ g & \mapsto & g \cdot x. \end{cases}$$

Cette application est surjective.

D Stabilisateurs

On peut également s'intéresser à l'ensemble des éléments du groupe qui ne modifient pas un objet $x \in E$, c'est son stabilisateur.

Définition 4.5

Soit $(G, \star)$ un groupe qui agit sur un ensemble E.
Le **stabilisateur** d'un élément $x \in E$, est formé de tous les éléments $g \in G$ qui laissent x invariant.

$$\mathrm{Stab}(x) = \{g \in G,\ g \cdot x = x\}.$$

On voit que le stabilisateur d'un objet contient toujours au moins l'élément neutre du groupe.

Exemple *(Isométries du triangle équilatéral)*

Toujours avec les isométries du triangle équilatéral,

- si on considère E (les six triangles), alors chaque triangle n'a qu'un seul stabilisateur : Id.
- Si on considère E_2 (les trois points du triangle) pour le groupe S_3, alors le stabilisateur de chaque point est composé de l'identité et de la symétrique axiale qui passe par ce point.

Par exemple :

$$\mathrm{Stab}(A) = \{\mathrm{Id},\, \tau_A\}\,.$$

- Enfin, pour E_3 (les arêtes orientées), le stabilisateur est toujours réduit à Id.

Exemple *(Rubik's cube)*

Avec le Rubik's cube, une méthode classique est de réaliser d'abord une face et la couronne intermédiaire avant de réaliser la dernière face.
Lorsque l'on réalise la dernière face, on cherche des éléments du groupe qui ne modifient pas les deux faces déjà réalisées : ils sont dans leur stabilisateur.

Définition 4.6 *(Action libre)*

Soit $(G, \star)$ un groupe qui agit sur un ensemble E.
On dit que G agit **librement** sur E (ou que l'action est libre) si

$$\forall x \in E,\ \mathrm{Stab}(x) = \{e\}\,.$$

Définition 4.7 *(Action simplement transitive)*

Une action **simplement transitive** est à la fois libre et transitive.

Si on considère deux éléments d'une même orbite, par exemple x et $x' = g \cdot x$, alors on voit que le stabilisateur de x' se déduit aisément de celui de x.
En effet, si $a \cdot x = x$, alors $x' = g \cdot x = g \cdot (a \cdot x) = (gag^{-1}) \cdot (g \cdot x) = (gag^{-1}) \cdot x'$. On voit donc que les éléments gag^{-1} sont dans le stabilisateur de x'.
Par symétrie des rôles, puisque $x = g^{-1} \cdot x$, on a que si $gag^{-1} \in \mathrm{Stab}(x')$, alors $a = g^{-1}(gag^{-1})g \in \mathrm{Stab}(x)$.
On dit que les stabilisateurs sont **conjugués.**

Propriété 4.8

Deux éléments d'une même orbite ont leurs stabilisateurs conjugés.

Remarque plus subtile : On peut donc s'amuser à faire agir G par conjugaison sur les stabilisateurs des éléments de E. On obtient que pour deux deux éléments de E dans la même orbite (action initiale), les stabilisateurs sont aussi dans la même orbite pour l'action de conjugaison.

5 Étude des groupes finis

Les groupes finis, c'est-à-dire ceux qui ont un nombre fini d'éléments, sont les premiers qui ont été pensés. Cayley dans sa première définition ne considère que ceux-ci.

A Ordre d'un élément

On sait que pour toute transformation du triangle, sous réserve de la répéter suffisamment de fois, on revient au triangle initial.
Le nombre de fois qu'il faut répéter l'opération est l'**ordre** de l'élément. Il peut différer suivant les éléments.

Par exemple, la symétrie est d'ordre 2, car répétée deux fois, on revient à l'identité. Par contre, la rotation R d'angle $\frac{2\pi}{3}$ est d'ordre 3.

Le théorème important est que c'est vrai pour tout élément d'un groupe *fini*. Le **théorème de Lagrange** ira encore plus loin, puisqu'il affirme que l'ordre de l'élément divise le cardinal du groupe.

Par exemple, pour le triangle équilatéral : il existe exactement 6 transformations. L'identité est d'ordre 1, les rotations R et R^2 sont d'ordre 2 et les symétries d'ordre 3. Ce ne sont que des diviseurs de 6.

L'énoncé peut être plus impressionnant avec de grands groupes.
Par exemple, on peut considérer toutes les manipulations possibles du Rubiks'cube. Bien qu'il y ait un très grand nombre de manipulations possibles, elles restent en nombre fini (car le Rubiks'cube n'admet lui-même qu'un nombre fini de configurations) : c'est un sous-groupe[9]des permutations des petites facettes du cubes. Ainsi, on peut donc choisir arbitrairement une manipulation du cube et on sait que répétée suffisamment de fois, elle reviendra à la configuration initiale du cube (avant la première manipulation). Par contre, il n'y a aucune raison que cette manipulation permette de parcourir toutes les configurations possibles du cube.
Ce que dit Lagrange, c'est que le nombre de configurations différentes atteintes avec cette seule manipulation divise le nombre total de configurations possibles.
Lorsque la transformation en question permet d'obtenir *toutes* les configurations, alors on dit que la transformation est **primitive.**

Propriété 5.1

Soit $(G, \star)$ un groupe **fini** noté multiplicativement et e son élément neutre.

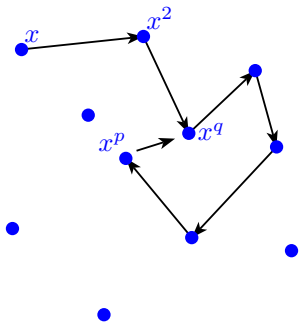
$$\forall x \in G,\ \exists k \in \mathbf{N}^*,\ x^k = e.$$

Le plus petit entier naturel non nul tel que $x^k = e$ est appelé l'**ordre** de x.

Explications

Pour comprendre pourquoi cette propriété est naturelle, considérons un groupe fini.
On imagine que l'on part d'un premier élément x et on le multiplie avec lui-même indéfiniement.
Comme le groupe ne contient qu'un nombre fini d'éléments et que la loi est interne, on ne peut pas obtenir toujours un nouvel élément et viendra nécessairement un $q \in \mathbf{N}^*$ qui retombera sur un élément déjà visité.
On trouve alors $p < q$ avec $x^p = x^q$.

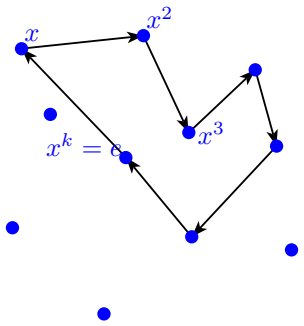
9. On voit que ce ne sont pas toutes les permutations car les contraintes physiques du cube interdisent certaines configuration (par exemple un coin ne peut pas avoir ses trois facettes de la même couleur).



On obtient ainsi une boucle sur un nombre fini d'éléments. La taille de la boule est $q-p$, en effet, pour passer de x^p à x^q, on a multiplié $q-p$ fois par x, c'est-à-dire par x^{q-p}. On trouve bien d'après les règles sur les puissances (voir annexe) :

$$x^p = x^q x^{p-q}.$$

Ainsi multiplier par $p-q$ « ne fait rien » : $x^{p-q} = e$.
Notre boucle passe donc par e et si on multiplie par x, on revient au point de départ.
La forme du schéma précédent doit donc être reprise :



Si on note k le premier entier tel que $x^k = e$, alors on voit aussi que $x^{k-1} \star x = e$, ce qui indique que x^{k-1} est l'inverse de x.
Au dela de la simple existence d'un ordre pour l'élément x, ceci indique que si on considère toute la boucle

$$\left\{x^k,\, k \in \mathbf{N}\right\}$$

alors elle forme un sous groupe de G (contient e, l'inverse de x et donc de toutes ses puissances, et la partie est stable). On l'appelle le **groupe engendré par** x.

Preuve

Soit $x \in G$, $\left\{x^k,\, k \in \mathbf{N}\right\}$ est une partie finie de G, donc il existe $p < q$ tel que $x^q = x^p$.
Or x^p admet pour symétrique x^{-p}. Si on multiplie par cette quantité on obtient $x^{q-p} = e$.
Ainsi $\left\{k \in \mathbf{N}^*,\, x^k = e\right\}$ est une partie non vide de $\mathbf{N}^*$. Elle admet donc un plus petit élément : l'ordre de x. ■

Corollaire 5.2

Soit $(G, \star)$ un groupe noté multiplicativement.
Soit $x \in G$,

$$< x >= \left\{x^k,\, k \in \mathbf{N}\right\} \text{ est un groupe.}$$

C'est le plus petit sous-groupe de G qui contient x : on l'appelle **groupe engendré par** x.
Le cardinal de $< x >$ est exactement l'ordre de $< x >$.

Preuve

On a vu que $e \in < x >$.
Si x^p et x^q sont dans $< x >$, alors $x^p \star x^q = x^{p+q} \in < x >$ par définition : la loi est interne.
Si $x^p \in < x >$, alors si on note n l'ordre de x, $\exists k \in \mathbf{N}$ tel que $kn \geqslant p$, de sorte que $kn - p \geqslant 0$ et $x^{kn-p} \in < x >$.
Ainsi $x^p x^{kn-p} = x^{kn} = (x^n)^k = e^k = e$ donc x^{kn-p} est l'inverse de x^p et il appartient à $< x >$ ce qui prouve finalement que $< x >$ est stable par passage à l'inverse.
$< x >$ est un sous-groupe de G.
Par minimalité de l'ordre, les éléments $\left\{e, x, \cdots, x^{n-1}\right\}$ sont tous distincts (où n est l'ordre de x) donc le cardinal de $< x >$ est bien n, l'ordre de x. ■

Remarque : $< x >= \left\{x^k,\, k \in \mathbf{N}\right\} = \left\{x^k,\, k \in \mathbf{Z}\right\}$.

On généralise cette définition de l'ordre à n'importe quel groupe fini :

Définition 5.3 *(Ordre d'un groupe)*

L'**ordre** d'un groupe fini est son cardinal.

Comme on l'a fait au départ avec les transformations du triangle, on peut chercher, à partir d'une ou plusieurs transformations données, toutes les transformations que l'on peut obtenir avec : il s'agit simplement du plus petit sous-groupe qui contient ces transformations.

Définition 5.4 *(Sous-groupe engendré)*

Soit $(G, \star)$ un groupe.
Pour S une partie de G, on appelle **groupe engendré** par S, le plus petit sous-groupe qui contient S.
On note $< S >$ ou $\mathrm{gr}(S)$.

Définition 5.5 *(Groupe cyclique)*

Un groupe engendré par un unique élément est dit **monogène.**
Un groupe monogène fini est **cyclique.**

Propriété 5.6

Soit $(G, \star)$ un groupe multiplicatif.
Pour $x \in G$,

$$< x >= \left\{x^k,\, k \in \mathbf{Z}\right\}.$$

L'**ordre** de x est le cardinal du sous-groupe engendré par x, c'est le plus petit entier k tel que $x^k = e$ l'élément neutre de G.

Pour obtenir le groupe engendré par x, on fait simplement agir x de nombreuses fois et tous les éléments obtenus forment le sous-groupe engendré par x.

Par définition $< x >$ est monogène.

Exemple

$(\mathbf{Z}, +)$ est un groupe monogène. Il est engendré par 1.
Pour $n \geqslant 1$, $(\mathbf{U}_n, \times)$ est un groupe cyclique qui est engendré par $\mathrm{e}^{2i\frac{\pi}{n}}$.

B Théorème de Lagrange

Théorème 5.7

Soit $(G, \star)$ un groupe fini.
L'ordre de tout élément — ou de tout sous-groupe — de G divise l'ordre de G.

Preuve

Soit H un sous-groupe de G.
L'idée est de créer des copies de H qui forment une partition de G.
Par exemple, si la partition contient 5 copies de H, on aura alors $5\#H = \#G$ ce qui prouve la divisibilité.
La méthode adaptée pour créer de telles partitions est la réalisation de classes d'équivalence.
On crée la relation d'équivalence :

$$\forall (x, y) \in G^2,\ x\mathscr{R}y \iff x^{-1}y \in H.$$

Ainsi, la classe d'équivalence de x est $\dot{x} = xH$, dont on voit qu'elle est en bijection naturelle avec H et donc de même cardinal :

$$\left\{\begin{array}{ccc} H & \to & xH \\ h & \mapsto & xh \end{array}\right. \text{ est une bijection.}$$

Toutes les classes d'équivalence ont le même cardinal : $\#H$, et comme elles forment une partition, si on note $|G : H|$ le nombre de classes d'équivalence, on a donc

$$\#G = \#\left(\bigsqcup_{xH \in (G/\mathscr{R})} xH\right) = \sum_{xH \in (G/\mathscr{R})} \#(xH) = \sum_{xH \in (G/\mathscr{R})} \#H = |G : H|\ \#H.$$

(On a noté $G/\mathscr{R}$ l'ensemble des classes d'équivalence modulo $\mathscr{R}$).
Ainsi $\#H$ divise $\#G$.

$|G : H|$ s'appelle **l'indice** de H dans G.
Je laisse en exercice la preuve formelle selon laquelle $\mathscr{R}$ est une relation d'équivalence. ■

Corollaire 5.8

L'ordre d'un élément d'un groupe fini divise le cardinal de ce groupe.

Cela vient simplement que l'ordre de x est le cardinal du groupe engendré $< x >$.

6 Annexe : définitions élémentaires liées à la notion de groupe

Cette annexe apporte des compléments formels à la sous-section A (p.4).

A Opération interne

Définition 6.1 *(Opération interne)*

Soit E un ensemble, une **opération interne** $\star$ sur E est une application de E^2 dans E, c'est-à-dire telle que

$$\forall (x,y) \in E^2,\ x \star y \in E.$$

Explications

L'opération est interne pour qu'elle ne nous fasse pas « *sortir* » de l'ensemble E. On travaille en milieu clos sans avoir à se demander à chaque fois « être ou ne pas être dans l'ensemble ? », *that is not the question*.
Pour les isométries, cela se traduit simplement par une liste *exhaustive* : la composition de deux isométries de la liste donne encore une isomérie de la liste. C'est la raison qui nous avait poussé à rajouter les rotations.

Remarque : On parle de *magma* pour un ensemble muni d'une loi interne.

B Associativité & commutativité

Définition 6.2 *(Loi associative, loi commutative)*

Une loi $\star$ sur E est dite **associative** sur E si

$$\forall (x,y,z) \in E^3,\ x \star (y \star z) = (x \star y) \star z.$$

Une loi $\star$ sur E est dite **commutative** sur E si

$$\forall (x,y) \in E^2,\ x \star y = y \star x.$$

Exemple

La composition des isométries du triangle équilatéral est associative, mais non commutative.
L'addition sur $\mathbf{Z}$ est associative et commutative.
La multiplication (sur $\mathbf{R}$ ou $\mathbf{C}$) est associative et commutative.
La division sur $\mathbf{R}^*$ n'est ni associative, ni commutative.
La soustraction sur $\mathbf{Z}$ n'est ni associative, ni commutative.
La multiplication matricielle est associative, mais pas commutative.

C Élément neutre

Définition 6.3 *(Élément neutre)*

Une loi $\star$ définie sur E admet un **élément neutre**, s'il existe $e \in E$ tel que

$$\forall x \in E, \qquad x \star e = e \star x = x.$$

e est appelé l'**élément neutre**.

Exemple

Dans le cas des isométries, c'est l'identité qui joue le rôle de l'élément neutre pour la composition.
L'élément neutre pour l'addition sur $\mathbf{Z}$ est 0.
L'élément neutre pour le produit sur $\mathbf{Z}$ est 1.

Propriété 6.4 *(Unicité de l'élément neutre)*

Si l'élément neutre existe, alors il est unique.

Preuve

Si on suppose que e et e' sont des éléments neutres pour $\star$, alors $e = e \star e' = e'$. ■

L'élément neutre n'a que peu d'intérêt en lui-même : il ne fait rien.
Par contre, il est utile pour définir le symétrique :

D Symétrique, réciproque, opposé ou inverse

Définition 6.5 *(Symétrique)*

Soit $x \in E$,
x possède un **symétrique** pour la loi $\star$ s'il existe $y \in E$ tel que

$$x \star y = y \star x = e.$$

y est alors appelé le symétrique de x pour $\star$.

⚠ Le symétrique dépend de l'opération choisie. S'il y a plusieurs opérations définies sur l'ensemble, il faut savoir de laquelle on parle.

Exemple

- Pour les isométries du triangle, le symétrique est l'application réciproque.
- Le symétrique d'un nombre entier pour l'addition est son opposé.
  -5 est le symétrique de 5 dans $\mathbf{Z}$ pour la loi $+$.
- Sur $\mathbf{N}$ muni de l'addition, seul 0 admet un symétrique.

L'absence de symétrique est un problème de $\mathbf{N}$: on n'a pas le droit de contracter des dettes. Pour palier à ce problème, on a donc inventé $\mathbf{Z}$.

- Sur $\mathbf{Q}^*$ muni de la multiplication, tous les éléments admettent un symétrique.

Propriété 6.6

L'élément neutre admet toujours un symétrique qui est lui-même.

Propriété 6.7 *(Unicité du symétrique)*

Pour une loi associative,
si un élément admet un symétrique, alors celui-ci est unique.

Preuve

Supposons que x ait deux symétriques y et z, alors $z = z\star(x\star y) = (z\star x)\star y = e\star y = y$. ■

Définition 6.8

- Lorsque la loi $\star$ est une addition, le symétrique est appelé l'**opposé**. L'opposé de x est noté $-x$.
- Lorsque la loi $\star$ est une multiplication, le symétrique est appelé l'**inverse**. L'inverse de x est noté x^{-1}.
- Lorsque la loi $\star$ est une composition, le symétrique est appelé la **réciproque**. La réciproque de f est noté f^{-1}.

Reste à savoir ce qu'est une addition, une multiplication ou une composition...
C'est une question d'usage :

- L'addition et la multiplication[10], sont souvent définies l'une par rapport à l'autre. Nous allons voir un peu plus loin la structure d'anneau qui est munie de deux opérations. Celle qui forme le groupe est l'addition et l'autre la multiplication. En général, on réserve l'addition aux opérations commutatives.
- Le terme de composition est utilisé à la place de la multiplication lorsque l'on traite d'applications.

Propriété 6.9 *(Inversibilité du produit)*

Soit E muni d'une loi de composition multiplicative interne $\star$ et associative.
Soit $(x, x') \in E$.
Si x et x' admettent tous deux des inverses (symétriques) dans E pour la loi $\star$, alors $x\star x'$ admet aussi un inverse dans E égal à $x'^{-1}\star x^{-1}$.

10. La somme est le résultat d'une addition, de même que le produit est le résultat d'une multiplication.

Preuve

On note x^{-1} et x'^{-1} les inverses respectifs de x et x'.

$$\begin{aligned}(x\star x')\star(x'^{-1}\star x^{-1}) &= x\star(x'\star x'^{-1})\star x^{-1} \qquad \text{(associativité)}\\ &= x\star(e)\star x^{-1}\\ &= x\star x^{-1} = e.\end{aligned}$$

On a de même $(x\star x')\star(x'^{-1}\star x^{-1}) = e$.
Ainsi $x\star x'$ admet un inverse qui vaut $x'^{-1}\star x^{-1}$. ■

Exemple

Écrire la même propriété en notation additive.

E Élément régulier

Définition 6.10 *(Élément régulier)*

Un élément $a \in E$ est dit **régulier à gauche** pour la loi $\star$ interne et associative si

$$\forall(x, y) \in E,\ a\star x = a\star y \Rightarrow x = y.$$

Il est dit **régulier à droite** si

$$\forall(x, y) \in E,\ x\star a = y\star a \Rightarrow x = y.$$

Il est dit **régulier** s'il est à la fois régulier à gauche et à droite.

Explications

Un élément régulier est un élément que l'on peut simplifier.
Un élément inversible (qui admet un symétrique) peut toujours être simplifié. C'est ce que l'on fait quand on résout une équation dans $\mathbf{R}$: on ajoute l'opposé, ou on mutliplie par l'inverse afin d'isoler l'inconnue.
Par contre, ce n'est pas toujours possible lorsque l'objet n'est pas inversible : c'est la difficulté avec les équations matricielles.
L'élément régulier offre un « entre-deux » : on peut simplifier même si ce n'est pas inversible. C'est le cas des polynômes non constants que l'on peut simplifier dans les équations bien qu'ils ne soient pas inversibles.

Exemple

Un élément neutre est toujours régulier.

F Partie stable

Définition 6.11 *(Partie stable)*

Soit E muni de la loi interne $\star$.
Une partie $E' \subset E$ est dite **stable** par $\star$, si

$$\forall (x,\, x') \in E',\ x \star x' \in E',$$

c'est-à-dire si la loi $\star$ est interne dans E'.

Exemple

Si E admet un élément neutre e pour la loi $\star$, alors $\{e\}$ est stable par $\star$.

G Différence entre associativité et commutativité

Le but de cet exemple est de montrer que l'associativité et la commutativité sont bien des notions distinctes. Les matrices donnent un exemple de loi qui est associative sans être commutative. L'idée ici est de trouver une loi commutative mais non associative.
Plutôt que de travailler avec les nombres, nous allons travailler avec des objets beaucoup plus simples (il n'y en aura que trois) que l'on nommera p comme « pierre », f comme « feuille » et c comme « ciseaux ».
Sur cet ensemble, nous définissons une opération $\star$ inspirée du jeu « pierre-feuille-ciseaux ». L'opération entre deux « actions » donne pour résultat le vainqueur[11].
Par exemple, pour $p \star f$, le résultat est f car c'est la feuille qui gagne contre la pierre.
Dans le cas où les deux « actions » sont identiques, alors l'opération renvoie l'action elle-même).
On note $M = \{p,\, f,\, c\}$, l'ensemble de travail. On peut alors résumer la loi avec une *table de Cayley* :

$\star$	p	f	c
p	p	f	p
f	f	f	c
c	p	c	c

Ce tableau se lit ainsi : pour calculer $p \star f$, on prend la ligne p et la colonne f et on lit le résultat : $p \star f = f$.
Cela correspond bien au jeu : entre la pierre et la feuille, c'est la feuille qui gagne.
L'opération sur M est *interne*. En effet, $\forall (x, y) \in M^2,\ x \star y \in M$ (le résultat d'une opération est toujours un des trois éléments p, f ou c).
L'opération est clairement *commutative* : $\forall (x, y) \in M^2,\ x \star y = y \star x$ (l'ordre n'a pas d'importance entre les deux joueurs).
Par contre, cette opération n'admet *pas d'élément neutre* (tout élément agit de façon non triviale sur les autres) : la structure $(M, \star)$ n'est pas un groupe. On dit que c'est un *magma* commutatif (une façon de dire que ce n'est pas très ordonné...).
Ce magma n'est pas non plus *associatif*.

11. Honte à ceux qui ne connaissent pas ce jeu !

Prenons un exemple :

$$p \star (f \star c) = p \star c = p \qquad \text{et} \qquad (p \star f) \star c = f \star c = c.$$

On voit donc que

$$p \star (f \star c) \neq (p \star f) \star c.$$

C'est simplement une façon mathématique de dire que l'on ne peut pas jouer à ce jeu à trois en même temps.
Si on voulait avoir un élément neutre, il faudrait rajouter un élément qui perd à chaque fois.
On pourrait l'appeler n de tel sorte que $\forall x \in M\ : n \star x = x$.
Grâce à cet élément neutre, on peut construire un symétrique pour chaque élément de M en imposant que $\forall x \in M,\ x \star x = n$.
Ainsi, chaque élément est son propre symétrique.
On modifie donc les règles du jeu et on obtient une nouvelle table de Cayley :

$\star$	n	p	f	c
n	n	p	f	c
p	p	n	f	p
f	f	f	n	c
c	c	p	c	n

On n'est pas très loin d'un groupe, mais il manque, encore et toujours l'associativité !

H Lois additives et multiplicatives

Propriété 6.12 *(Puissances)*

Soit $(G, \star)$ un groupe (notation multiplicative).
Soit $x \in G$.
On définit par récurrence les puissances de x avec

$$\begin{cases} x^0 = e, \\ \forall n \in \mathbf{N},\ x^{n+1} = x^n \star x = x \star x^n, \\ \forall n \in \mathbf{N},\ x^{-n} = \left(x^{-1}\right)^n = \left(x^n\right)^{-1}. \end{cases}$$

On a alors :

- $\forall x \in G,\ \forall n \in \mathbf{Z},\ x^n \in G$.
- $\forall (n,\, p) \in \mathbf{Z},\ x^{n+p} = x^n \star x^p$.

⚠ En général $(x \star y)^n \neq x^n \star y^n$ (sauf si G est un groupe commutatif).

Preuve

- G est un groupe, donc il admet bien un élément neutre que l'on peut noter e.
  La définition de x^0 est donc correcte.

- On montre par récurrence sur $n \in \mathbf{N}$ que $x^n \in G$ et $x^n \star x = x \star x^n$.
  L'initialisation est immédiate.
  Pour l'hérédité, $x^n \in G$ et $x \in G$, donc $x^{n+1} \in G$ car la loi est interne.
  De plus, $x^{n+1} \star x = (x \star x^n) \star x = x \star (x^n \star x) = x \star (x \star x^n) = x \star x^{n+1}$.
- Pour x^{-n}, on remarque déjà que si $x \in G$, alors $x^{-1} \in G$ et d'après le résultat précédent, pour tout $n \in \mathbf{N}$, $(x^{-1})^n \in G$.
  On montre ensuite l'égalité par récurrence.
  Initialisation : $x^{-0} = x^0 = e = e^{-1} = \left(x^{-1}\right)^0$.
  Hérédité : on suppose l'égalité au rang $n \in \mathbf{N}$, alors $(x^{n+1}) \star \left(x^{-1}\right)^{n+1} = x \star x^n \star \left(x^{-1}\right)^n \star x^{-1}$.
  Et par hypothèse de récurrence, $\left(x^{-1}\right)^n = (x^n)^{-1}$ donc $x^n \star \left(x^{-1}\right)^n = e$ et on obtient donc $(x^{n+1}) \star \left(x^{-1}\right)^{n+1} = x \star e \star x^{-1} = e$.
  (on fait le même raisonnement pour le calcul dans l'autre ordre).
  Ceci prouve donc l'hérédité.
- Pour montrer que $x^{n+p} = x^n \star x^p$, on procède par récurrence sur $p \in \mathbf{N}$.
  Pour $p = 0$, l'égalité et vraie pour tout $n \in \mathbf{Z}$ car $x^p = x^0 = e$.
  On suppose l'égalité pour un rang $p \in \mathbf{N}$ fixé, alors $x^{n+p+1} = x^{(n+1)+p}$ et on applique l'hypothèse de récurrence avec $n+1$ ce qui donne $x^{n+p+1} = x^{n+1} \star x^p = x^n \star x \star x^p = x^n \star x^{p+1}$ en utilisant les résultats montrés aux points précédents.
  Ceci prouve l'égalité pour tout $p \in \mathbf{N}$.
  Pour $p < 0$, on passe simplement à l'inverse en utilisant les résultats déjà démontrés.

$$x^{n+p} = \left(x^{-1}\right)^{-n-p} = \left(x^{-1}\right)^{-n} \star \left(x^{-1}\right)^{-p} = x^n \star x^p.$$

■

Propriété 6.13 *(Notation additive)*

En notation additive, pour le groupe $(G, +)$, la propriété précédente s'écrit :

$$\begin{cases} 0x = e. \\ \forall n \in \mathbf{N},\ (n+1)x = nx + x = x + nx. \\ \forall n \in \mathbf{N},\ (-n)x = -(nx) = n(-x). \end{cases}$$

On a alors :

- $\forall x \in G,\ \forall n \in \mathbf{Z},\ nx \in G$.
- $\forall (n, p) \in \mathbf{Z},\ (n+p)x = nx + px$.

Exemple

Soit $P \in \mathbf{K}[X]$, on note E l'ensemble des racines de P dans $\mathbf{K}$.
L'ensemble E, muni de la multiplication est-il un groupe ?
Exercice relativement facile sur $\mathbf{R}$*, mais difficile sur* $\mathbf{C}$.
Solution :

- *Analyse :* Si P n'admet aucune racine, ce n'est pas un groupe car E est vide.
  Donc P admet au moins une racine $\alpha \in \mathbf{K}$.
  - Si $|\alpha| > 1$, alors $\{\alpha^n,\ n \in \mathbf{Z}\}$ forme une famille de scalaires deux à deux distincts (modules distincts). Donc E qui contient cette famille (stabilité) est infini.
    Donc P possède une infinité de racines, donc P est nul.
  - Si $|\alpha| \in]0,\ 1[$, c'est la même chose avec $\frac{1}{\alpha} \in E$.
  - Si $\alpha = 0$. Cela suppose que 0 soit inversible pour le produit.
    Ce n'est évidemment pas le cas, car pour tout $x \in \mathbf{K}$, $x \times 0 = 0$.
    Mais on peut faire preuve d'audace et supposer que $0 = 1$, pour obtenir l'inversibilité. Il est alors immédiat que l'ensemble peut former un groupe à la condition d'être réduit à un seul point. Alors $\alpha = 0$ est la seule racine et P s'écrit sous la forme $X^n R$ avec $n \in \mathbf{N}^*$ et R un polynôme sans racines.

  Avant de traiter le cas $|\alpha| = 1$, on peut rédiger une synthèse partielle :
- *Synthèse « partielle »* dans le cas $|\alpha| \neq 1$.
  - Si P est nul, alors 1 est l'élément neutre, mais $0 \in E$ n'admet pas d'inverse, donc E n'est pas un groupe.
  - S'il existe $n \in \mathbf{N}^*$ et $R \in \mathbf{K}[X]$ sans racines tel que $P = X^n R$.
    Alors $E = \{0\}$ que l'on peut considérer comme un groupe d'élément neutre 0 pour la loi $\times$.
- *Conclusion pour le cas* $|\alpha| \neq 1$.
  - Pour $\mathbf{K} = \mathbf{C}$ on a nécessairement $R = \lambda \in \mathbf{K}^*$ (ce qui est aussi suffisant).
  - Pour $\mathbf{K} = \mathbf{R}$, R s'écrit sous forme de produit de polynômes de degré 2 à discriminants strictement négatifs.
- *Dernière situation :* supposons qu'il existe une racine α de module 1.
  D'après les derniers cas, on sait que toute racine est alors nécessairement de module 1.
  - Si $\mathbf{K} = \mathbf{R}$, alors $\alpha = 1$ ou $\alpha = -1$ et on peut écrire $P = (X-1)^p (X+1)^q R$ avec $(p, q) \in \mathbf{N}^2$ et R sans racines.
    - Si 1 est la seule racine, alors $E = \{1\}$ qui est bien un groupe pour $\times$.
    - Si -1 est racine, $1 = (-1)^2$ est aussi racine et $E = \{-1, 1\}$ qui est bien un groupe pour $\times$.

    On a donc $p \geqslant 1$ et $q \in \mathbf{N}$.
  - Si $\mathbf{K} = \mathbf{C}$, on note $\alpha = \mathrm{e}^{i\theta}$.
    Comme E est stable par produit et qu'on suppose P non nul on a donc $\{\alpha^n,\ n \in \mathbf{Z}\}$ qui est un ensemble fini,
    donc il existe $p > q$ tel que $\mathrm{e}^{ip\theta} = \mathrm{e}^{iq\theta}$.
    Donc $(p-q)\theta \equiv 0\ [2\pi]$.
    Ainsi θ s'écrit sous la forme $\theta = \frac{2k\pi}{n}$ (avec $n = p - q > 0$).
    Comme l'angle est égal à 2π près, on peut choisir $k \in [\![0,\ n-1]\!]$ et également supposer la fraction irréductible.
    On sait que $\mathrm{e}^{i\theta} \in E$ et pour tout $u \in \mathbf{Z}$, $\mathrm{e}^{i\theta u} \in E$ par stabilité avec la puissance.
    Or $k \wedge n = 1$ (fraction irréductible) donc on peut trouver $(u, v) \in \mathbf{Z}^2$ tel que $ku + nv = 1$, donc

$$\mathrm{e}^{i\theta u} = \mathrm{e}^{2i\pi \frac{ku}{n}} = \mathrm{e}^{2i\pi \frac{1-nv}{n}} = \mathrm{e}^{\frac{2i\pi}{n}} \in E.$$

Ainsi E contient les racines n-ièmes de l'unité.
On voit que réciproquement, $\alpha = \mathrm{e}^{i\theta} = \mathrm{e}^{\frac{2ik\pi}{n}} \in \mathbf{U}_n$.
Donc toute racine de P est nécessairement racine n-ième de l'unité et si pour $n \in \mathbf{N}^*$ fixé, une racine n-ième est dans E, alors toutes les racines n-ièmes (pour le même n) le sont aussi.
On peut donc écrire P sous la forme

$$P = \lambda \prod_{\alpha \in U} (X - \alpha)^{m_\alpha}$$

où U désigne une union finie d'ensembles $\mathbf{U}_n$ $n \in \mathbf{N}^*$ et pour tout $\alpha \in U$, $m_\alpha \geqslant 1$.
On peut noter $U = \bigcup_{n \in I} \mathbf{U}_n$ avec I un sous-ensemble fini non vide de $\mathbf{N}^*$.
Reste à s'assurer que E est stable par produit.

Cela suppose que si $p \in I$ et $q \in I$, alors pour tout $(k,\, k') \in \mathbf{Z}^2$ $\mathrm{e}^{2i\pi\left(\frac{k}{p} + \frac{k'}{q}\right)} \in E$.

En écrivant $p = dp'$ et $q = dq'$ pour $d = p \wedge q$, alors on obtient $\mathrm{e}^{2i\pi \frac{kq' + k'p'}{dpq'}} \in E$.
On a $p' \wedge q' = 1$ et d'après Bezout, on peut donc choisir $kq' + k'p' = 1$ pour les bonnes valeurs de k et k'.
On remarque alors que $dp'q' = p \vee q \in I$, ainsi I doit être stable par passage au PPCM.
Mais, toute racine p-ième de l'unité est aussi racine $(p \vee q)$-ième de l'unité, de même pour les racines q-ièmes et on a donc $\mathbf{U}_p \cup \mathbf{U}_q \subset \mathbf{U}_{p \vee q}$.
Ainsi, en prenant le PPCM de tous les éléments de I que l'on note n on obtient que $U = \mathbf{U}_n$.
Réciproquement, il est évident que cela convient et P s'écrit

$$P = \lambda \prod_{\alpha \in \mathbf{U}_n} (X - \alpha)^{m_\alpha}$$

avec $\lambda \in \mathbf{C}^*$, $n \in \mathbf{N}^*$ et pour tout $\alpha \in \mathbf{U}_n$, $m_\alpha \in \mathbf{N}^*$.