Introduction à la Théorie des Groupes
Première Partie

Farouk Boucekkine (avec l'aide de Thomas Chomette)

http://dma.ens.fr/culturemath

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, sous la forme d'un cours, une base à tous les développements utilisant cette notion capitale qui ont été et seront faits dans le site Culture*MATH*. Dans la 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 la Deuxième Partie, prochainement sur votre écran, nous peaufinerons ce travail puis passerons à l'étude plus détaillée de quelques exemples bien spécifiques, et pour finir on donnera brièvement quelques pistes intéressantes pour poursuivre l'étude des groupes et de leurs applications. Nous développerons plus tard des textes sur certaines de ces pistes, n'hésitez pas à nous contacter pour nous faire part de vos préférences quant aux choix des exemples à développer.

Ce texte a été conçu pour être lisible presque entièrement sans prérequis. Le plus souvent possible, les notions et propriétés apparaissent d'abord dans des exemples avant d'être énoncées en toute généralité. De nombreux commentaires sont également là pour suggérer les idées fondamentales (souvent cachées dans des énoncés épurés par des decennies de maturation), ainsi que leur écho dans d'autres parties des mathématiques.

Pour ceux qui veulent (re)découvrir les groupes, il est donc conseillé de lire le texte dans l'ordre. En guise de référence rapide, une *version courte* est disponible sur le site, suivant le même plan, mais sans les commentaires ni la plupart des exemples.

Par ailleurs, des questions posées au lecteur émaillent le texte, la plupart sont des applications immédiates de ce qui précède, pour aider à faire une synthèse ou annoncer un résultat à venir. N'hésitez surtout pas à y réfléchir, et à nous écrire si nécessaire pour demander des éclaircissements.

culturemath@dma.ens.fr

Table des matières

Rappels et Notations :

• **Utilisation des quantificateurs $\forall$ et $\exists$:** "$\forall x \in A\ldots$" signifie "pour tout x appartenant à $A\ldots$" tandis que "$\exists x \in A\ldots$" signifie "il existe un x appartenant à $A\ldots$".
Faire bien attention à l'ordre des quantificateurs !

Dans la phrase "$\forall x, \exists y \ldots$" (*pour tout x, il existe un y tel que...*), y dépend *a priori* de x.

En revanche, dans "$\exists y, \forall x \ldots$"(*il existe un y tel que pour tout x...*), le même y marche pour tous les x !

• **Application Identité :** Soit A un ensemble, on appelle application *identité de* A, l'application notée $Id_A : x \longmapsto x$.

• **Composée de deux applications :** Soient A, B et C trois ensembles. Soient $f : A \to B$ et $g : B \to C$ deux applications. On appelle *composée de f et g* l'application $g \circ f : A \to C$ définie par $\forall a \in A, g \circ f(a) := g(f(a))$.

• **Injections, surjections, bijections :** Soient A et B deux ensembles et f une application de A vers B. On dit que f est

- *injective* (ou f est une *injection*) si tout élément de B a au plus un antécédent par f ;
- *surjective* (ou f est une *surjection*) si tout élément de B a au moins un antécédent par f ;
- *bijective* (ou f est une *bijection*) si tout élément de B a exactement un et un seul antécédent par f (f établit une correpondance parfaite entre les éléments de A et ceux de B.)
  Ceci équivaut à dire qu'il existe une application $f^{-1} : B \to A$, appelée *réciproque de f* telle que $\forall x \in A,\ f^{-1}(f(x)) = x$ et $\forall y \in B,\ f(f^{-1}(y)) = y$, ce qu'on peut aussi écrire $f^{-1} \circ f = Id_A$ et $f \circ f^{-1} = Id_B$.

• **Cardinal d'un ensemble :** Le *cardinal* d'un ensemble A, noté $|A|$, est le nombre de ses éléments. Si ce nombre est infini, on note $|A| = \infty$.

Si A et B sont deux ensembles, on dit qu'ils ont même cardinal (fini ou infini) s'il existe une bijection de A sur B (et réciproquement). Dans le cas fini, ceci est une conséquence évidente de la définition même des notions de cardinal et de bijection.

Notons que s'il existe une injection de A dans B (resp. une surjection de A sur B) alors on a forcément $|A| \leq |B|$ (resp. $|A| \geq |B|$.).

• **Racines de l'unité dans $\mathbb{C}$:** Soit $n \in \mathbb{N}$, les *racines $n^{\grave{e}mes}$ de l'unité* sont les n solutions dans $\mathbb{C}$ de l'équation $X^n = 1$. Ce sont donc les nombres complexes de la formes $e^{\frac{2ik\pi}{n}}, k \in \mathbb{Z}$.

Comme $e^{\frac{2ik\pi}{n}} = e^{\frac{2il\pi}{n}} \Longleftrightarrow k \equiv l\ [n]$, il suffit en fait de prendre $0 \leq k \leq n-1$ pour toutes les avoir.

• **L'ensemble des multiples de n :** si $n \in \mathbb{Z}$, on note $n\mathbb{Z} := \{n.k, k \in \mathbb{Z}\}$.

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* $x \bullet y = y \bullet x = e_G$.

Remarque 1.1.2 *La propriété* (i) *permet alors de définir sans ambiguïté les produits d'un nombre quelconque d'éléments* $x_1 \bullet x_2 \bullet \cdots \bullet x_n$.

Notons également qu'on ne suppose pas a priori *l'unicité de l'élément neutre ni de l'inverse d'un élément donné, qui vont en fait découler de la définition même (cf. Propriété* **1.2.1***).*

Exemples 1.1.3 *Voici des premiers exemples de groupes, assez différents pour qu'on entrevoie la portée généralisatrice de cette notion :*

(0) Le groupe trivial est un singleton $\{0\}$ muni de la seule opération possible : $0 \bullet 0 = 0$, 0 étant alors élément neutre...

(i) L'ensemble des entiers relatifs $\mathbb{Z}$ muni de l'addition usuelle forme un groupe $(\mathbb{Z}, +)$. L'élément neutre est 0 et $\forall x \in \mathbb{Z}, x + (-x) = 0$. De même, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont aussi des groupes. En revanche $(\mathbb{N}, +)$ n'en est pas un ! Pourquoi ?

(i) bis $\mathbb{Z}^n$ (resp. $\mathbb{Q}^n$, $\mathbb{R}^n$, et $\mathbb{C}^n$) muni de l'opération

$$(x_1; \ldots; x_n) + (y_1; \ldots; y_n) := (x_1 + y_1; \ldots; x_n + y_n)$$

forme un groupe dont l'élément neutre est $(0, \ldots, 0)$.

(ii) L'ensemble $\mathbb{Q}^*$ (resp. $\mathbb{Q}^*_+$) des rationnels non-nuls (resp. strictement positifs), muni de la multiplication usuelle forme un groupe $(\mathbb{Q}^*, \times)$ (resp. $(\mathbb{Q}^*_+, \times)$). 1 en est l'élément neutre, et $\forall x \in \mathbb{Q}^*, x \times \frac{1}{x} = 1$. De même, $(\mathbb{C}^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{R}^*_+, \times)$ sont des groupes. En revanche, $(\mathbb{Q}, \times)$, $(\mathbb{Z}^*, \times))$ et $(\mathbb{R}^*_-, \times)$ n'en sont pas. Pourquoi ?

(iii) L'ensemble $C_2 := \{-1, 1\}$ muni de la multiplication usuelle est un groupe de cardinal 2. Qu'en est-il du même ensemble muni de l'addition usuelle ?

(iii) bis Généralisons un peu l'exemple précédent : pour tout $n \in \mathbb{N}^*$, onsidérons l'ensemble des racines n^{iemes} de 1 dans $\mathbb{C}$: $C_n := \{e^{\frac{2ik\pi}{n}},\ k \in \mathbb{Z}\}$. Munissons C_n de la multiplication usuelle de $\mathbb{C}$, et nous obtenons un nouveau groupe, de cardinal n. Notons que si on prend $n = 2$, on retombe bien sur l'exemple *(iii)*.

(iii) ter Généralisons encore cet exemple en considérant l'ensemble C des nombres complexes de module 1, que l'on munit de la multiplication usuelle de $\mathbb{C}$. On a alors encore un groupe $(C, \times)$, de cardinal infini, cette fois. On a clairement $\forall n \in \mathbb{N}^*, C_n \subset C$

(iv) Soit E un ensemble, et notons $\mathfrak{S}(E)$ l'ensemble des bijections de E sur lui-même. Munissons $\mathfrak{S}(E)$ de l'opération de composition, $(\sigma, \tau) \longmapsto \sigma \circ \tau$.

Cette opération est associative (vérifiez !), admet l'application Identité, Id_E, comme élément neutre, et toute bijection σ admet par définition une réciproque σ^{-1} qui est son inverse pour la composition : $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = Id_E$.

On obtient donc un groupe $(\mathfrak{S}(E), \circ)$.

Le cas particulier le plus important est celui où l'on considère l'ensemble $E_n := \{1, 2, \ldots, n-1, n\}$. On notera alors $\mathfrak{S}_n := \mathfrak{S}(E_n)$ et le groupe $(\mathfrak{S}_n, \circ)$ est appelé *groupe symétrique (sur n lettres)*, que nous verrons plus en détail dans la Deuxième Partie de ce texte. Notons tout de suite que son cardinal est $|\mathfrak{S}_n| = n!$.

(v) Considérons l'ensemble $\mathcal{O}(\mathcal{P})$ des transformations affines isométriques du plan $\mathcal{P}$ (i.e. les bijections du plan dans lui-même qui conservent les barycentres et les longueurs). Munissons cet ensemble de l'opération $\circ$ de composition. Cette opération est associative, les isométries affines sont toutes inversibles, et $Id_{\mathcal{P}}$ est l'élement neutre : $(\mathcal{O}(\mathcal{P}), \circ)$ est un groupe, appelé *groupe orthogonal.*

On peut remarquer que les exemples (iv) et (v) sont différents des précédents, l'opération n'étant pas une "opération usuelle sur des nombres habituels" mais plutôt la "composition d'actions sur un ensemble". Ces exemples présentent aussi une particularité que la définition suivante va nous permettre de formaliser :

Définition 1.1.4 *Un groupe* $(G, \bullet)$ *est dit* commutatif *ou* abélien *si pour tout couple* (x, y) *d'éléments de* G*, on a*

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

On voit aisément que les exemples *(i)*, *(ii)* et *(iii)* précédents sont commutatifs. En revanche, considérons (exemple *(iv)*) le groupe $(\mathfrak{S}_3, \circ)$ des permutations de l'ensemble $\{1, 2, 3\}$. Appelons τ_3 l'élément de $\mathfrak{S}_3$ qui échange 1 et 2 et τ_1 celui qui échange 2 et 3. On a alors :

k	$\tau_3(k)$	$\tau_1(k)$	$\tau_3 \circ \tau_1(k)$	$\tau_1 \circ \tau_3(k)$
1	2	1	2	3
2	1	3	3	1
3	3	2	1	2

On a clairement

$$\tau_3 \circ \tau_1 \neq \tau_1 \circ \tau_3$$

et $\mathfrak{S}_3$ n'est donc pas commutatif. Ce raisonnement se généralise évidemment à $\mathfrak{S}_n$ pour tout $n \geq 3$. Qu'en est-il de $\mathfrak{S}_2$?

Le groupe orthogonal n'est pas commutatif non plus (on l'étudiera plus en détail dans la Deuxième Partie).

Nous verrons dans la Deuxième Partie que les groupes commutatifs sont beaucoup plus simples que les groupes généraux.

1.2 Propriétés élémentaires et notations usuelles

Voici les premières propriétés des groupes, données avec démonstration pour qu'on voie un type de manipulation caractéristique à ce type de problème.

On voit aussi un exemple élémentaire de raisonnement par "condition nécessaire" : pour prouver l'unicité d'un objet, on suppose qu'il a un "jumeau", et on applique alors les contraintes imposées par la structure ambiante jusqu'à finalement constater que les deux objets sont égaux.

Propriété 1.2.1 *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.*

<u>*Démonstration*</u> : *i)* Soient e_1 et e_2 deux candidats au poste d'élément neutre de l'opération $\bullet$, montrons qu'ils sont forcément égaux.

Comme e_1 est neutre, on a

$$e_1 \bullet e_2 = e_2$$

mais, comme e_2 est également neutre, on a aussi

$$e_1 \bullet e_2 = e_1$$

on a donc $e_1 = e_1 \bullet e_2 = e_2$.

ii) Par associativité, on a

$$z \bullet x \bullet y = (z \bullet x) \bullet y = e \bullet y = y$$

mais aussi

$$z \bullet x \bullet y = z \bullet (x \bullet y) = z \bullet e = z.$$

□

Commentaires 1.2.2 *Cette propriété nous permet de répondre aux questions posées dans les exemples* **1.1.3** (i) *et* (ii).

En effet, si $(\mathbb{N}, +)$ *était un groupe, d'après la propriété précédente, 0 serait forcément son unique élément neutre. Donc l'inverse (unique)* X *de l'élément 1 vérifierait* $1 + X = 0$*, ce qui est impossible dans* $\mathbb{N}$.

Par ailleurs, on peut aisément constater que le rouage cental de la deuxième partie de cette démonstration est l'associativité, qui permet de définir sans ambiguïté les produits à plus de deux termes.

Il faut maintenant parler des notations usuelles qui sont employées lorsque l'on parle de groupes.

Notation 1.2.3 *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'opération, 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 "$x.y$"*

Une petite propriété, pour s'habituer à cette notation "condensée" et qui donne deux règles élémentaires de calcul dans les groupes :

Propriétés 1.2.4 (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*

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

Démonstration : *(i)* Il suffit de multiplier à droite ou à gauche par z^{-1}.

(ii) Toujours par associativité $(xy)(y^{-1}x^{-1}) = e_G$... □

1.3 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 1.3.1 *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 1.3.2 *Si $g \in G$, d'inverse g^{-1}, alors $\phi(g^{-1})$ est nécessairement l'inverse de $\phi(g)$ dans H. En effet, on a :*

$$\phi(g^{-1}) \circ \phi(g) = \phi(g \bullet g^{-1}) = \phi(e_G) = e_H.$$

Par unicité de l'inverse (**Propriété 1.2.1***), on en déduit que $\phi(g^{-1})$ est bien l'inverse de $\phi(g)$ dans H.*

Commentaire 1.3.3 *La notion de morphisme est commune à toutes les parties des mathématiques : dès qu'on crée une structure on veut pouvoir faire communiquer des objets relevant de cette structure, et on définit donc aussitôt les morphismes correspondants, avec des clauses de compatibilité dépendant des données qu'on veut pouvoir "suivre".*

Ainsi, pour la structure "triviale", les Ensembles, les morphismes sont les applications, qui conservent la seule donnée : l'appartenance. Pour la structure d'Espace Vectoriel, les morphismes sont les application linéaires, qui conservent la structure vectorielle. Un exemple moins algébrique et où la compatibilité se fait "à rebours" : pour la structure d'Espace Topologique, les morphismes sont les applications continues (les images réciproques *des ouverts sont des ouverts.)*

Remarque 1.3.4 *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 1.2.3***, 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.

Parlons à présent de la composition des morphismes de groupes (démonstration laissée au lecteur) :

Propriété 1.3.5 *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.*

Exemples 1.3.6 *Voici quelques exemples de morphismes de groupes, qui nous permettent de voir au passage des raisonnements typiques.*

(i) Si G et H sont deux groupes, il y a toujours au moins un morphisme de G vers H, le morphisme trivial, qui associe à tout élément de G l'élément neutre de H.

Si G est un groupe, il a toujours au moins deux endomorphismes : l'endomorphisme trivial, et l'endomorphisme Identité ($x \longmapsto x$), noté Id_G. Il existe un cas ou ces endomorphismes sont égaux, lequel ? (cf. **Exemples 1.1.3**)

(ii) Considérons les endomorphismes du groupe C_2 (**Exemple 1.1.3** (iii)) : 1, élément neutre, est nécessairement envoyé sur 1 par définition d'un morphisme, et il y a deux choix pour l'image de -1 :

$$\begin{aligned} 1 &: \ \text{on obtient le morphisme trivial.} \\ -1 &: \ \text{on obtient le morphisme identité.} \end{aligned}$$

(iii) Soit G un groupe, on va montrer qu'un morphisme $\phi : (\mathbb{Z},+) \to G$ est entièrement déterminé par $\phi(1)$. Pour cela, nous allons raisonner *par condition nécessaire*, c'est à dire utiliser la rigidité imposée à une application par le fait d'être un morphisme.

Notons $a := \phi(1) \in G$. On a $\phi(0) = e_G$ et $\forall n \in \mathbb{N}$

$$\phi(n) = \phi(\underbrace{1+1+\cdots+1}_{n\ termes}) = \underbrace{\phi(1)+\phi(1)+\cdots+\phi(1)}_{n\ termes} = a^n$$

et

$$\phi(-n) = \phi(n)^{-1} = a^{-n}.$$

Donc $\forall n \in \mathbb{Z},\ \phi(n) = a^n$: ϕ est entièrement déterminée par $a = \phi(1)$.

Ce qui fait marcher cet exemple est la propriété qu'ont les éléments de $\mathbb{Z}$ de tous être de la forme $n.1$. On dit que 1 est un *générateur* de $(\mathbb{Z},+)$, qui est dit *monogène*. Nous reverrons ces notions au **§2.3**.

Application : Prenons par exemple $G = (Z,+)$ et déterminons tous les endomorphismes de ce groupe. Nous avons montré qu'une condition nécessaire pour ϕ est d'être de la forme $\phi_a : n \longmapsto n.a$, avec $a \in \mathbb{Z}$.[1]

Le terrain est donc bien déblayé, mais il reste à déterminer quelles sont les valeurs de a pour lesquelles on obtient effectivement un endomorphisme (*condition suffisante*).

Dans notre exemple, la condition nécessaire obtenue est également suffisante : $\forall a \in \mathbb{Z}$, notons ϕ_a l'application $\phi_a : n \longmapsto a.n$, on a alors immédiatement :

$$\begin{cases} \forall x,y \in \mathbb{Z},\ \phi_a(x+y) = (x+y).a = x.a+y.a = \phi_a(x)+\phi_a(y) \\ \phi(0) = a.0 = 0 \end{cases}$$

Ainsi, les endomorphismes de $(\mathbb{Z},+)$ sont exactement les $\phi_a,\ a \in \mathbb{Z}$.

(iv) De la même manière, on peut montrer avec à peine plus d'efforts que les endomorphismes de $(\mathbb{Q},+)$ sont de la forme $\phi_a : r \longmapsto a.r$, pour $a \in \mathbb{Q}$. La petite astuce a ajouter au raisonnement précédent est laissée au lecteur *(Indication : $p = \frac{p}{q}+\cdots+\frac{p}{q}$).*

(v) En revanche, des considérations qui ne sont pas du ressort de ce texte (utilisation d'une base de $\mathbb{R}$ vu comme $\mathbb{Q}-$espace vectoriel) permettent de construire des endomorphismes de $(\mathbb{R},+)$ différents des traditionnels $\phi_a : x \longmapsto a.x$ pour $a \in \mathbb{R}$ (bien que les ϕ_a restent bien entendu des morphismes).

(vi) grâce au (iii), on sait à présent que les morphismes de $(\mathbb{Z},+)$ vers $(\mathbb{Q},+)$ (resp. vers $(\mathbb{R},+)$) sont de la forme $\phi_a : n \longmapsto a.n$, pour $a \in \mathbb{Q}$ (resp. $\phi_a : n \longmapsto a.n$ pour $a \in \mathbb{R}$).

[1]Attention ! dans le paragraphe précédent, par pure perversité nous avions noté G multiplicativement ; ici, il faut donc revenir à la notation additive de $\mathbb{Z}$, a^n devenant $n.a$. Mais vous n'avez plus de problème de conversion maintenant, non ?

(vii) Soit $n \in \mathbb{Z}$, alors $\psi_n : r \longmapsto r^n$ est un endomorphisme de $(\mathbb{Q}^*, \times)$. On peut bien entendu construire les mêmes ψ_n sur $(\mathbb{Q}_+^*, \times)$, $(\mathbb{C}^*, \times)$, etc... Ces groupes ont-ils d'autres endomorphismes ?

Si $a \in \mathbb{R}$, $\psi_a : x \longmapsto x^a$ est un endomorphisme de $(\mathbb{R}_+^*, \times)$. Qu'en est-il de $(\mathbb{R}^*, \times)$ ou de $(\mathbb{C}^*, \times)$?

(viii) La fonction ln est un morphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$, la fonction exp est un morphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$.

(ix) Il y a deux morphismes de $(\mathbb{Z}, +)$ vers $(C_2, \times)$: le morphisme trivial et le morphisme $k \longmapsto (-1)^k$ (vérifiez !).

Dans l'autre sens, soit ϕ un morphisme de $(C_2, \times)$ dans $(\mathbb{Z}, +)$, on a alors $\phi(1) = 0$, reste à déterminer $\phi(-1)$. Or, on a dans $\mathbb{Z}$:

$$0 = \phi(1) = \phi\left((-1) \times (-1)\right) = \phi(-1) + \phi(-1) = 2\phi((-1))$$

ainsi, on a dans $\mathbb{Z}$ $2\phi(-1) = 0$, donc $\phi(-1) = 0$. ϕ est donc nécessairement le morphisme trivial.

Le morphisme $\pi_n : (\mathbb{Z}, +) \to (C_n, \times),\ k \longmapsto (e^{\frac{2i\pi}{n}})^k$ généralise l'exemple précédent. Vérifiez !

Que dire des morphismes $(C_n, \times) \to (\mathbb{Z}, +)$?

Et pour finir avec cet exemple, si $\eta \in C$ (cf. **Exemple 1.1.3 (iii) ter**), alors $\mu_\eta : k \longmapsto \eta^k$ est un morphisme de groupes de $(\mathbb{Z}, +)$ vers $(C, \times)$. Y en a-t-il d'autres ?

(x) Voyons ce qui se passe avec les **Exemples 1.1.3** (*iii*) *bis* **et** *ter*). Si $k \in \mathbb{Z}$, les applications suivantes sont des morphismes de groupes :

$$\left\{ \begin{array}{ccc} C_n & \longrightarrow & C \\ z & \longmapsto & z^k \end{array} \right. \quad et \quad \left\{ \begin{array}{ccc} C_n & \longrightarrow & C_n \\ z & \longmapsto & z^k \end{array} \right.$$

Si $k \in \mathbb{Z}$ tel que $n \mid km$, alors $\forall z \in \mathbb{C}_n$, on a $z^k \in C_m$ et l'application suivante est un morphisme de groupes :

$$\left\{ \begin{array}{ccc} C_n & \longrightarrow & \mathbb{C}_m \\ z & \longmapsto & z^k \end{array} \right.$$

Et si $n \not| \, km$?

(xi) Considérons l'élément σ_n suivant de $\mathfrak{S}_n$:

$$\begin{array}{ccc} 1 & \longmapsto & 2 \\ 2 & \longmapsto & 3 \\ \vdots & & \vdots \\ n-1 & \longmapsto & n \\ n & \longmapsto & 1 \end{array}$$

On peut remarquer que $\sigma_n^n = Id$. Ca ne vous rappelle rien ? Utilisons σ_n pour construire un morphisme de $C_n \to \mathfrak{S}_n$:

$$\forall k \in \mathbb{Z},\ e^{\frac{2ik\pi}{n}} \longmapsto \sigma_n^k$$

Vérifiez que cela marche bien...

Il existe un morphisme naturel $\iota_n : \mathfrak{S}_{n-1} \to \mathfrak{S}_n$ qui, à tout élément σ de $\mathfrak{S}_{n-1}$ associe l'élément de $\mathfrak{S}_n$ qui agit comme σ sur $\{1, \ldots, n-1\}$, et envoie n sur n.

Il existe un morphisme non trivial $\varepsilon : \mathfrak{S}_n \to C_2$, appelé la *Signature*. Nous le verrons plus en détail dans la Deuxième Partie.

(xii) Un exemple un peu plus abstrait. Soit G un groupe et $x \in G$, considérons l'application

$$c_x : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & x.g.x^{-1} \end{array} \right.$$

on a immédiatement $c_x(e_G) = e_G$ et

$$c_x(g.h) = x.g.h.x^{-1} = x.g.(x^{-1}.x).h.x = (x.g.x^{-1}).(x.h.x^{-1}) = c_x(g).c_x(h).$$

c_x est donc un endomorphisme de G.

(xiii) L'exemple maudit ou béni suivant l'orientation de la supersition choisie... Justement, c'est d'orientation qu'il s'agit : on peut établir un morphisme de $\mathcal{O}(\mathcal{P})$ dans C_2 en associant :

1 aux transformations qui conservent l'orientation (e.g. les rotations)
-1 à celles qui ne conservent pas l'orientation (e.g. les symétries axiales).

Vérifiez !

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

Dans le **§1**, nous avons défini les Objets mathématiques qu'on appelle groupes comme des ensembles munis d'une loi répondant à certains axiomes, puis nous avons défini les Morphismes permettant à ces objets de communiquer.

La donnée d'une collection d'Objets et de Morphismes correspondants définit ce qu'on appelle une *Catégorie*, en l'occurence la Catégorie des Groupes. Le formalisme des catégories s'applique à de nombreux domaines des mathématiques, permettant d'englober sous une même bannière des familles apparemment très différentes. Il a même permis la naissance de nouveaux champs dans la deuxième moitié du $XX^{\text{ème}}$ siècle, sous l'influence de mathématiciens comme Grothendieck, Verdier, MacLane... Il est plus tard sorti du monde des mathématiques pures et se retrouve maintenant en informatique théorique. Nous reparlerons de ce sujet dans un futur article sur Cutlure*MATH*.

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

Il est temps à présent d'introduire deux objets très importants, qui vont nous permettre d'étudier l'injectivité et la surjectivité des morphismes 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 $Im\ \phi = H$. Ici, la structure de groupe n'apporte aucun renseignement supplémentaire permettant de simplifier l'étude de la surjectivité (pour le moment, mais on en verra plus au **§2.3**.) En revanche, la notion de Noyau, duale de celle d'Image, va tout de suite nous simplifier la vie pour l'injectivité :

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 $Ker\ \phi = \{e_G\}$.*

Démonstration : Le principe de la démonstration est simple : soit $\phi : G \to H$ un morphisme de groupes.

Alors pour $x, y \in G$, $\phi(x) = \phi(y)$ équivaut à $x.y^{-1} \in Ker\ \phi$. En effet,

$$\phi(x) = \phi(y) \Longrightarrow \phi(x.y^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = \phi(x)\phi(x)^{-1} = e_H.$$

et réciproquement

$$\phi(x.y^{-1}) = e_H \Longrightarrow \phi(x)\phi(y)^{-1} = e_H \Longrightarrow \phi(x) = \phi(y).$$

Appliquons ça au résultat qu'on veut démontrer.

Si $Ker\ \phi \neq \{e_G\}$, comme e_G est toujours dans $Ker\ \phi$, il existe $g \in G$ tel que $g \neq e_G$ et $\phi(g) = e_H = \phi(e_G)$, donc ϕ n'est pas injective.

Réciproquement (c'est le sens intéressant), si $Ker\ \phi = \{e_G\}$, montrons que ϕ est injective. Soient $x, y \in G$ tels que $\phi(x) = \phi(y)$, montrons que $x = y$. D'après ce qui précède, on a nécessairement $x.y^{-1} \in Ker\ \phi$, donc $x.y^{-1} = e_G$, donc $x = y$. □

Commentaire 2.1.4 *On voit ici un élément qui intervient dans toutes les structures algébriques : se ramener à la préimage de 0 pour étudier l'injectivité d'un morphisme. Par exemple, c'est ce qu'on fait en algèbre linéaire, où l'étude de la surjectivité peut de plus en découler aisément en dimension finie grâce à l'égalité $dim(Ker\ f) + dim(Im\ f) = dim(E)$.*

Notons également qu'en analyse, la recherche de points d'annulation de la dérivée d'une fonction (ou, en dimension n, de ses points critiques) relève de ce procédé : à chaque point a de l'espace de départ, on associe une application linéaire, la différentielle, dont on étudie le noyau. Dans le cas d'une fonction $f : \mathbb{R} \to \mathbb{R}$, par exemple, cette application linéaire est $x \longmapsto f'(a).x$. Etudier son noyau correspond bien à chercher si f' s'annule en a.

Exemples 2.1.5 *Reprenons les exemples vus ci-dessus et calculons leur image et leur noyau.*

(i) Le morphisme trivial de G à H a pour noyau G tout entier et pour image e_H, il est donc injectif si et seulement si G est lui-même le groupe trivial, et surjectif si et seulement si H est trivial.

L'endomorphisme Identité de G a pour noyau $\{e_G\}$ et pour image G, il est donc injectif et surjectif (mais n'est-ce pas là une évidence ?).

(ii) Le morphisme non-trivial de C_2 a un noyau trivial et pour image C_2, il est donc injectif et surjectif.

(iii) $\phi_a(n) = 0$ si et seulement si $an = 0$. Donc, si $a \neq 0$, $\phi_a(n) = 0$ si et seulement si $n = 0$. Donc ϕ_a est injective si et seulement si $a \neq 0$. De plus $Im\ \phi_a = a\mathbb{Z}$, donc ϕ_a est surjective si et seulement si $a = \pm 1$.

(iv) à (vi) Pour l'injectivité des ϕ_a, même raisonnement, même résultat. Pour leur surjectivité, en revanche, c'est différent, car si $a \in \mathbb{Q}$ (ou $\mathbb{R}$ ou $\mathbb{C}$), et $a \neq 0$, alors $\forall x \in \mathbb{Q}(\mathbb{R}, \mathbb{C}), x = \phi_a(\frac{x}{a})$. Donc ϕ_a est injective ET surjective si et seulement si $a \neq 0$.

Les endomorphismes non-canoniques de $(\mathbb{R}, +)$ peuvent être injectifs, surjectifs, les deux ou aucun des deux...

(vii) Calculons le noyau de $\psi_n : (\mathbb{Q}^*, \times) \to (\mathbb{Q}^*, \times),\ r \longmapsto r^n$. On a clairement $\psi_n(r) = 1 \iff r^n = 1$. Par conséquent, on a deux cas :

Si n est impair, $Ker\ \psi_n = \{1\}$, donc ψ_n est injectif.

Si n est pair, $Ker\ \psi_n = \{-1, 1\}$, donc ψ_n n'est pas injectif.

Remarquons au passage que $\psi_n : (\mathbb{Q}^*_+, \times) \to (\mathbb{Q}^*_+, \times),\ r \longmapsto r^n$ est, lui, toujours injectif (car $-1 \notin \mathbb{Q}^*_+$).

$Im\ \psi_n = \{r^n, r \in \mathbb{Q}^*\}$, par conséquent, si $n \neq \pm 1$, on a forcément $2 \notin Im\ \psi_n$, car il faudrait pour cela que $\sqrt[n]{2}$ soit rationnel. ψ_n est donc surjective si et seulement si $n = \pm 1$.

Considérons à présent, pour $n \neq 0$, $\psi_n : (\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times),\ z \longmapsto z^n$.

$Ker\ \psi_n = C_n \neq \{1\}$ si $n \neq \pm 1$.

Par conséquent ψ_n est injective si et seulement si $n = \pm 1$. En revanche, elle est toujours surjective ! En effet, si $z = r.e^{i\theta} \in \mathbb{C}^*$, alors $z = \psi_n(\sqrt[n]{r}.e^{\frac{i\theta}{n}})$.

(viii) les morphismes ln et exp sont injectifs et surjectifs (grâce à ce qu'on sait d'eux par l'analyse).

(ix) Considérons $\pi_n : (\mathbb{Z}, +) \to (C_n, \times),\ k \longmapsto (e^{\frac{2i\pi}{n}})^k$. Comme $C_n = \{e^{\frac{2ik\pi}{n}}, k \in \mathbb{Z}\}$, il est clair que π_n est surjective.

Calculons à présent son noyau : on a $\pi_n(k) = 1$ si et seulement si $n \mid k$, donc $Ker\ \psi_n = n\mathbb{Z}$ n'est pas trivial et le morphisme n'est pas injectif.

Soit $\eta \in C$, considérons $\mu_\eta : \mathbb{Z} \to C,\ k \longmapsto \eta^k$. Alors μ_η est injective si et seulement si η n'est pas une racine de l'unité (montrez-le !). Par ailleurs, μ_η n'est jamais surjective (un argument court, utilisant la théorie des cardinaux, est de dire que C n'est pas dénombrable, contrairement à $\mathbb{Z}$, et qu'il ne peut donc y avoir de surjection de $\mathbb{Z}$ sur C.)

(x) Considérons $\Phi : C_{12} \to C,\ z \longmapsto z^5$. On a $\Phi(e^{\frac{2ik\pi}{12}}) = e^{\frac{2i\pi.5k}{12}}$ est égal à 1 si et seulement si $5k \equiv 0\ (12)$. Donc

$$Ker\ \Phi = \{e^{\frac{2ik\pi}{12}}\ tels\ que\ 5k \equiv 0\ [12]\}.$$

Or $5 \wedge 12 = 1$ donc $12 \mid 5k$ si et seulement si $12 \mid k$. Ainsi $Ker\ \Phi = \{1\}$ et Φ est donc injective. En revanche, elle n'est évidemment pas surjective, C_{12} étant un ensemble fini, contrairement à C.

Considérons à présent $\phi : C_{12} \to C_{15},\ z \longmapsto z^4$. Alors

$$Ker\ \phi = \{e^{\frac{2ik\pi}{12}}\ tels\ que\ 4k \equiv 0\ [12]\} = \{e^{\frac{2ik\pi}{12}}\ tels\ que\ k \equiv 0[3]\}.$$

Donc $Ker\ \phi = \{1, -1, i, -i\}$, et ϕ n'est pas injective.

De plus, $|C_{12}| < |C_{15}|$ donc il ne peut pas y avoir de surjection de C_{12} sur C_{15}.

Une autre preuve de la non-surjectivité de ϕ : en faisant la liste des images des éléments de C_{12} (ce qu'on peut faire car il a peu d'éléments...), on peut constater que $e^{\frac{2i\pi}{15}}$ n'y figure pas. C'est encore, en fait, un argument de cardinalité.

Une dernière preuve, fondamentalement différente des précédentes : $\forall z \in C_{12}$ on a $x^{12} = 1$, et donc

$$\phi(x)^{12} = \phi(x^{12}) = \phi(1) = 1.$$

Donc $\forall z \in Im\ \phi$, $z^{12} = 1$. Or $e^{\frac{2i\pi}{15}}$ ne vérifie pas cette égalité, donc il n'appartient pas à $Im\ \phi$ et ϕ n'est pas surjective. Ce type de raisonnement est très fréquent en théorie des groupes, et on le verra plus attentivement lorsque l'on parlera de *l'ordre d'un élément* au **§3.3**.

(xi) On peut vérifier "à la main" que $\forall k \in \{1, \ldots, n-1\}, \sigma_n^k \neq Id$, et par conséquent le morphisme est injectif. En revanche il n'est pas surjectif si $n > 2$ (par exemple parceque $|C_n| = n < n! = |\mathfrak{S}_n|$).

Et si $n = 2$?

(xii) Soit G un groupe, et $x \in G$, alors

$$g \in Ker\ c_x \Longleftrightarrow x.g.x^{-1} = e_G \Longleftrightarrow g.x = x \Longleftrightarrow g = e_G.$$

Donc c_x est injective.

Montrons qu'elle est également surjective. Soit $g \in G$, alors

$$g = (x.x^{-1}).g.(x.x^{-1}) = c_x(x^{-1}.g.x).$$

(xiii) Surjective, et non injective. Le noyau est appelé $\mathcal{SO}(\mathcal{P})$, et il est composé des rotations, des translations et de leurs composées qui sont... ?

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

Considérons l'ensemble $\mathfrak{B}$ à deux éléments formé par une Chaussure et un Radiateur, et sur cet ensemble, définissons l'opération $\bullet$ suivante :

$\bullet \quad \swarrow$	*Chaussure*	*Radiateur*
Chaussure	*Radiateur*	*Chaussure*
Radiateur	*Chaussure*	*Radiateur*

On vérifie aisément que $(\mathfrak{B}, \bullet)$ est un groupe commutatif, d'élément neutre *"Radiateur"*.

Maintenant, reprenons notre groupe C_2 de l'**Exemple 1.1.3**, et considérons les applications

$\Phi : \mathfrak{B} \to C_2$ qui à *"Radiateur"* associe 1 et à *"Chaussure"* associe -1
et $\Psi : C_2 \to \mathfrak{B}$ qui à 1 associe *"Radiateur"* et à -1 associe *"Chaussure"*.

Ces applications sont clairement à la fois des bijections réciproques et des morphismes de groupes (vérifiez !).

Elles nous permettent donc d'établir une correspondance entre C_2 et $\mathfrak{B}$ de telle sorte que, **du point de vue de la structure de groupe**, ils sont indiscernables bien que n'étant pas des ENSEMBLES égaux : *"Radiateur"* joue le rôle de 1 et *"Chaussure"* celui de -1. On dit que C_2 et $\mathfrak{B}$ sont **isomorphes**.

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.*

<u>*Démonstration*</u> :

Si ϕ est un isomorphisme : alors ϕ possède par définition une réciproque ψ, et est donc nécessairement bijective.

Si ϕ est un morphisme bijectif : soit $\psi = \phi^{-1}$ sa réciproque. Montrons que ψ est un morphisme de groupes, et on aura notre propriété.

On sait que $\phi(e_G) = e_H$, donc $\Psi(e_H) = \phi^{-1} \circ \phi(e_G) = e_G$.

Soient $y_1, y_2 \in H$. Montrons que $\psi(y_1 y_2) = \psi(y_1)\psi(y_2)$. Considérons $\psi(y_1)$ et $\psi(y_2)$, éléments de G. Comme ϕ est un morphisme, on a

$$\phi\Big(\psi(y_1)\psi(y_2)\Big) = \phi\Big(\psi(y_1)\Big)\phi\Big(\psi(y_2)\Big) = y_1 y_2.$$

Appliquons ψ à cette égalité, et on obtient :

$$\psi(y_1)\psi(y_2) = \psi(y_1 y_2)$$

$\square$

Attention ! Deux groupes peuvent avoir le même cardinal et ne pas être isomorphes (autrement dit, on peut mettre des structures de groupes *différentes* sur un ensemble donné). Cf. **§2.4**.

Commentaires 2.2.3 *La notion d'isomorphisme est très importante dans les mathématiques modernes : quand on s'intéresse à un certain type de structure sur un objet donné, on parle souvent d'*égalité à isomorphisme près. *Par exemple, en algèbre linéaire, on sait qu'un $K-$espace vectoriel de dimension finie n est isomorphe à K^n et que cela suffit à décrire toutes ses propriétés linéaires.*

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

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

Exemples 2.2.5 *Reprenons nos exemples :*

(i) Si G est un groupe, Id_G est un isomorphisme, de réciproque lui-même.

Par le seul morphisme possible, tous les groupes triviaux sont isomorphes. C'est pour cela qu'on parle généralement DU groupe trivial.

(iii) Si $a \neq 0$, pour ϕ_a soit un isomorphisme, il faut et il suffit que ϕ_a soit surjective. Or l'image de ϕ_a est exactement $a\mathbb{Z}$. Donc ϕ_a est un isomorphisme si et seulement si $a = \pm 1$.

(iv) et (v) Si $a \neq 0$, ϕ_a est un isomorphisme de réciproque $\phi_{\frac{1}{a}}$.

(vi) Qu'en pensez-vous ?

(vii) $\psi_n : (\mathbb{Q}^*, \times) \to (\mathbb{Q}^*, \times)$ est un automorphisme si et seulement si $n = \pm 1$ (pareil pour $\mathbb{Q}^*_+$ et idem pour $\mathbb{C}^*$, mais pour des raisons différentes !).

(viii) exp et ln sont des isomorphismes réciproques de $(\mathbb{R}, +)$ sur $(\mathbb{R}^*_+, \times)$. Et oui, contre toute attente, $(\mathbb{R}, +)$ sur $(\mathbb{R}^*_+, \times)$ sont identiques du point de vue de la structure de groupe !

En revanche, soit Φ un morphisme de $(\mathbb{C}^*, \times)$ vers $(\mathbb{C}, +)$. On a alors

$$4\Phi(i) = \Phi(i^4) = \Phi(1) = 0.$$

Donc $i \in Ker\ \Phi$, et Φ ne peut pas être injectif, donc ne peut pas être un isomorphisme.

Et pour $(\mathbb{Q}, +)$ et $(\mathbb{Q}^*_+, \times)$?

(ix) et (x) Pas d'isomorphismes...

(xi) pour $n = 2$, on a bien $C_2 \simeq \mathfrak{S}_2$. Pour $n > 2$, on n'a plus d'isomorphisme. Y a-t-il des groupes de cardinal 2 qui ne soient pas isomorphes à C_2 ? et des groupes de cardinal 3 non-isomorphes à C_3 ? et des groupes de cardinal 4 non isomorphes à C_4 ?

(xii) Comme on l'a vu précédemment, $\forall x \in G$, c_x est injectif et surjectif, c'est donc un un automorphisme de G. Les automorphismes de la forme c_x sont appelés *automorphismes intérieurs de* G. Nous les reverrons dans le paragraphe suivant.

Quel est la réciproque de c_x ?

Maintenant, on va découvrir une nouvelle source de groupes. On a vu dès le **§1.1** que les bijections d'un ensemble E dans lui-même, munies de l'opération de composition, forment un groupe $(\mathfrak{S}(E), \circ)$.

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 2.2.6 *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.

Commentaire 2.2.7 *Plus généralement, ce type de construction illustre bien l'universalité de la notion de groupe. Dans tous les domaines des mathématiques, lorsqu'on définit une structure et ses morphismes, on doit s'intéresser aux transformations d'un objet* O *donné qui "conservent totalement" sa structure.*

Ces transformations sont alors les automorphismes de O *pour la structures considérée, et forment à nouveau un groupe que l'on pourra attacher à* O *et qui décrira en partie ses propriétés dans la structure considérée.*

Quelques exemples pour étayer ces propos bien généraux : L'ensemble des transformations affines d'un esapce affine à n dimensions (e.g un plan) forme un groupe, l'ensemble des isométries d'un tel espace aussi.

L'ensemble des isométries qui conservent une figure du plan (e.g. un triangle, un octogone, un cercle...) ou de l'espace (e.g un cube) forme également un groupe.

Nous verrons plus précisément des exemples de tels groupes dans la Deuxième Partie.

C'est ainsi que Klein a constaté l'importance de cette notion : elle apparaît partout (en géométrie) comme "ensemble des transformations préservant une structure donnée".

Exemple 2.2.8 *Déterminons le groupe $Aut(C_3)$.*

$C_3 = \{1, j, \overline{j}\}$, on a donc deux automorphismes possibles

$$\begin{array}{rl} Id: & 1 \longmapsto 1 \quad j \longmapsto j \quad \overline{j} \longmapsto \overline{j} \\ Conj: & 1 \longmapsto 1 \quad j \longmapsto \overline{j} \quad \overline{j} \longmapsto j \end{array}$$

Par conséquent $Aut(C_3) = \{Id; Conj\}$, qui est isomorphe à C_2.

2.3 Sous-groupes d'un groupe donné

Dans les premiers exemples, on constate que certains groupes sont inclus dans d'autres, de sorte que l'opération du "petit" soit la restriction de celle du "grand" (par exemple $(\mathbb{Z}, +)$ dans $(\mathbb{Q}, +)$ ou $(C_n, \times)$ dans $(C, \times)$). Ce phénomène est capital lorsqu'on étudie une structure.

On constate aussi que l'on ne peut pas prendre une partie d'un groupe au hasard et lui restreindre l'opération. Il faut que la partie soit *stable* par l'opération (par exemple $(C_2, +)$ n'est pas un groupe) et par inversion (par exemple $(\mathbb{N}, +)$ n'est pas un groupe).

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 opératoire 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 :*

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

Démonstration : Exercice... □

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

Exemples 2.3.4 *Voici quelques exemples de sous-groupes issus de notre bestiaire habituel :*

(0) Le groupe trivial est sous-groupe de tout groupe.
Tout groupe est sous-groupe de lui-même.

(i) On a $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$. De même, $(\mathbb{Q}_+^*,\times) < (\mathbb{R}_+^*,\times) < (\mathbb{C}^*,\times)$. On a aussi $(\mathbb{Q}_+^*,\times) < (\mathbb{Q}^*,\times) < (\mathbb{R}^*,\times)$, etc... Mais, bien entendu, $(\mathbb{Q}^*,\times)$ n'est pas un sous-groupe de $(\mathbb{R}_+^*,\times)$!

(ii) D'une manière plus générale, soit G un groupe et soit $x \in G$, considérons l'ensemble $\langle x\rangle := \{x^k,\ k \in \mathbb{Z}\}$. On a

$$x^k.x^l = x^{k+l} \in \langle x\rangle$$

$$et\ \ y \in \langle x\rangle \Longrightarrow y = x^k \Longrightarrow y^{-1} = x^{-k} \in \langle x\rangle\,.$$

Ainsi, $\langle x\rangle$ est un sous-groupe de G, appelé *sous-goupe engendré par x*. Nous allons développer la notion de sous-groupe engendré un peu plus loin. Remarquons tout de suite que ceci généralise l'exemple précédent : $\mathbb{Z}$ est le sous-groupe de $(\mathbb{Q},+)$ engendré par 1.

Peut-on voir C_n comme sous-groupe de C engendré par un certain élément ?

(iii) $C_n < C < (\mathbb{C}^*,\times)$. Si $n \mid m$, alors $C_n < C_m$.

(iv) Soit $\mathcal{P}$ un plan. Considérons parmi les isométries affines de $\mathcal{P}$, celles qui conservent l'orientation (e.g. les rotations, mais pas les symétries centrales ni axiales). On voit immédiatement que ce sous ensemble de $\mathcal{O}(\mathcal{P})$ est stable par inverse et par composition, c'est donc un sous-groupe, que l'on appelle le *groupe Spécial Orthogonal* (cf. **Exemples 1.3.6 (xiii)**).

(v) Soit G un groupe, et $x, y \in G$. Considérons les automorphismes intérieurs c_x et c_y associés à x et y. On a (en se souvenant de la **Propriété 1.2.4** (ii)) :

$$\forall g \in G,\ c_x \circ c_y(g) = c_x(c_y(g)) = x.(y.g.y^{-1}).x^{-1} = (x.y).g.(x.y)^{-1} = c_{xy}(g).$$

De plus, en remarquant que $c_{e_G} = Id_G$, on voit immédiatement que

$$(c_x)^{-1} = c_{x^{-1}}.$$

Par conséquent, l'ensemble $Int(G)$ des automorphismes intérieurs de G est stable par l'opération de composition et par l'inversion, c'est donc un sous-groupe de $Aut(G)$, lui-même sous-groupe de $\mathfrak{S}(G)$.

La propriété suivante lie ce paragraphe aux précédents (et sa démonstration est laissée au lecteur).

Propriété 2.3.5 *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.*

Exemples 2.3.6 *De cette manière, on a :*

(i) Soit G un groupe et $x \in G$. En considérant le morphisme

$$\left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & x^k \end{array} \right.$$

On obtient le sous-groupe $\langle x \rangle$ déjà rencontré ci-dessus.

(ii) Considérons maintenant l'application suivante

$$\mathfrak{I}_G : \left\{ \begin{array}{ccc} G & \longrightarrow & Int(G) \\ x & \longmapsto & c_x \end{array} \right.$$

En utilisant le raisonnement vu dans l'exemple précédent, on voit immédiatement que $\mathfrak{I}_G$ est un morphisme de groupes. Il est surjectif, par construction de $Int(G)$. Calculons son noyau :

$$x \in Ker\ \mathfrak{I}_G \Longleftrightarrow c_c = Id_G \Longleftrightarrow \forall g \in G, xgx^{-1} = g \Longleftrightarrow \forall g \in G, xg = gx.$$

Donc $Ker\ \mathfrak{I}_G$ est l'ensemble des $x \in G$ qui *commutent* avec **tous** les éléments de G. Ce sous-groupe de G est très important, nous le reverrons par la suite la suite (voir en particulier le **§3.5**) :

Définition 2.3.7 *Soit G un groupe. On appelle* centre *de G le groupe*

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

Remarque 2.3.8 *On peut noter que si $\phi : G \to H$ est un morphisme de groupes injectif, G est toujours isomorphe à $Im\ \phi$, ce qui fait que dans ce cas, on dit souvent que "G est un sous-groupe de H".*

Ceci est, *stricto sensu*, un abus de langage mais est une phrase tout à fait correcte *à isomorphisme près.*

Mainenant, on va introduire une notion très importante, que nous avons annoncée plusieurs fois dans les pages qui précèdent. On a vu qu'un élément $x \in G$ "engendre" un sous-groupe $\langle x \rangle$, sans préciser ce qu'"engendrer" veut dire. L'idée est simple : 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 2.3.9 *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.*

<u>Démonstration</u> : Laissée au lecteur... Mais importante ! ce type de raisonnement se retrouve partout en algèbre.

Remarque 2.3.10 *Attention ! Ca ne marche pas avec* $\bigcup_{i \in I} H_i$*. Sauriez-vous trouver un contre-exemple ?*

Définition 2.3.11 *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 2.3.12 *$\langle A \rangle$ 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 2.3.13 *Soit G un groupe et A une partie de G. alors*

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

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

Remarque 2.3.14 *Ajouter "$\cup\{e_G\}$" ne sert que dans un cas, lequel ?*

Exemples 2.3.15

(i) Soit G un groupe et $x \in G$. Suivant la propriété précédente, l'ensemble $\{x^k, k \in \mathbb{Z}\}$ est bien le sous-groupe engendré par $\{x\}$.

(ii) $\{(1,0,0\dots,0); (0,1,0,\dots,0); \dots; (0,0,0,\dots,1)\}$ engendre $\mathbb{Z}^n$. Quel est le groupe engendré par $\{(1,2);(3,5)\}$ dans $\mathbb{Z}^2$?

(iii) Considérons les éléments τ_1 et τ_3 de $\mathfrak{S}_3$ vus après la **Définition 1.1.4**. On a alors

$$\langle\{\tau_1, \tau_3\}\rangle = \mathfrak{S}_3.$$

Nous vous laissons le soin d'écrire les 6 éléments de $\mathfrak{S}_3$, puis de vérifier qu'ils sont tous de la forme décrite dans la proposition précédente.

Nous reverrons plusieurs manières d'engendrer les groupes symétriques dans la Deuxième Partie.

Nous reviendrons sur ce sujet dans la Deuxième Partie, lorsque nous parlerons de groupes définis par générateurs et relations.

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*

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

Vérifiez que c'est bien un groupe !

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

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

Que dire de la réciproque de cette dernière assertion ?

Exemples 2.4.4

(i) montrons qu'on peut avoir deux groupes de même cardinal et non-isomorphes : C_4 et $C_2 \times C_2$. Remarquons tout de suite qu'ils sont de cardinal 4 tous les deux, il y a donc des bijections de C_4 sur $C_2 \times C_2$ (comme ENSEMBLES).

Montrons à présent qu'aucun morphisme de groupes entre eux n'est bijectif. L'obstruction est que tout élément x de $C_2 \times C_2$ vérifie $x^2 = (1,1)$, la propriété correspondante étant fausse sur C_4.

Soit alors $f : C_2 \times C_2 \to C_4$ un morphisme de groupes,

$$\forall x \in C_2 \times C_2, f(x)^2 = f(x^2) = f(1,1) = 1$$

Or $i \in C_4$ et ne vérifie pas $i^2 = 1$, donc i ne peut pas appartenir à $Im\ f$.

Donc f ne peut pas être un isomorphisme.

(ii) On va à présent déterminer deux sous-groupes H_1 et H_2 de $\mathbb{Z}^2$ tels que $H_1 \cup H_2$ n'est pas un sous-groupe. Considérons pour cela les images H_1 et H_2 des morphismes π_1 et π_2 de la **Propriété 2.4.3**. On peut constater immédiatement que

$$H_1 \cup H_2 = \{(x, y) \in \mathbb{Z}^2 \text{ tels que } x = 0 \text{ OU } y = 0\}.$$

Cet ensemble n'est certainement pas stable par l'addition de $\mathbb{Z}^2$ car

$$(0, 1) + (1, 0) = (1, 1) \notin H_1 \cup H_2.$$

(iii) On a vu que le groupe engendré par un élément $x \in G$ était l'image du morphisme $\mathbb{Z} \to G$, $k \longmapsto x^k$. Peut-on généraliser ce résultat au groupe engendré par deux éléments $x, y \in G$ grâce au morphisme $\mathbb{Z}^2 \to G$, $(k, l) \longmapsto x^k.y^l$?

Mais d'abord est-ce bien un morphisme dans ce cas ? Prenez $G = \mathfrak{S}_3$ et considérez les deux éléments τ_1 et τ_3 définis après la **Définition 1.1.4**. Que constatez-vous ?

Nous reviendrons sur cette question dans la Deuxième Partie lorsque nous parlerons de la définition de groupes par *générateurs et relations* et du groupe libre à n générateurs.

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 :*

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

qui vérifie les axiomes :

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

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

Remarque 3.1.2 *On pourrait également définir les actions* à droite*, plus pratiques dans certains contextes. Quels en seraient les axiomes ?*

Exemples 3.1.3 *Voici des premiers exemples, qui s'étofferont plus loin.*

(0) Premier exemple, pas très intéressant : l'action triviale. $\forall (g, x) \in G \times E, g.x = x$...

(i) Soit E un ensemble. L'action de groupe la plus naturelle est l'action de son groupe de permutations $\mathfrak{S}(E)$ sur E :

$$\begin{cases} \mathfrak{S}(E) \times E & \longrightarrow E \\ (\sigma, x) & \longmapsto \sigma(x) \end{cases}$$

Les cas particuliers les plus intéressants étant l'action des $\mathfrak{S}_n$ sur $E_n = \{1;2;;\ldots;n\}$.

Considérons par exemple la permutation $\tau_1 \in \mathfrak{S}_3$ qui échange 2 et 3 et l'élément $x = 3$. Ici, $\tau_1.x$ sera l'élément 2, *i.*e. l'image de l'élément 3 par la permutation.

(ii) Reprenons notre **Exemple 1.1.3 (v)**. Le groupe $\mathcal{O}(\mathcal{P})$ agit sur le plan $\mathcal{P}$ de manière naturelle :

$$\begin{cases} \mathcal{O}(\mathcal{P}) \times \mathcal{P} & \longrightarrow \mathcal{P} \\ (\sigma, x) & \longmapsto \sigma(x) \end{cases}$$

(iii) Soient G un groupe et $H < G$ alors H agit sur G par translation à gauche (resp. à droite) :

$$\begin{cases} H \times G & \longrightarrow G \\ (h, x) & \longmapsto h.x \end{cases}$$

$$\left(resp. \begin{cases} H \times G & \longrightarrow G \\ (h, x) & \longmapsto x.h^{-1} \end{cases} \right).$$

Pourquoi, dans le cas de la translation à droite, a-t-on pris $(h, x) \longmapsto x.h^{-1}$ et pas $(h, x) \longmapsto x.h$? (ce serait un bel exemple d'action à droite...)

(iv) Soit G un groupe, alors G agit sur lui-même par conjugaison :

$$\begin{cases} G \times G & \longrightarrow G \\ (g, x) & \longmapsto g.x.g^{-1} \end{cases}.$$

(v) Soit G un groupe, et $\mathcal{S}(G)$ l'ensemble de ses sous-groupes. Alors si $g \in G$ et $H < G$, l'ensemble $gHg^{-1} := \{g.h.g^{-1},\ h \in H\} = c_g(H)$ est un sous-groupe de G. On peut alors vérifier que

$$\begin{cases} G \times \mathcal{S}(G) & \longrightarrow \mathcal{S}(G) \\ (g, H) & \longmapsto gHg^{-1} \end{cases}$$

définit bien une action de G sur $\mathcal{S}(G)$.

(vi) Le groupe C_2 agit sur S^2, la sphère unité de $\mathbb{R}^3$ comme suit

$$\begin{array}{rl} 1 & \text{agit trivialement comme il se doit ;} \\ -1 & \text{agit en envoyant tout point de } S^2 \text{ sur son opposé.} \end{array}$$

(vii) Un bel exemple d'utilisation de cette théorie est donné dans le texte *Les colliers de Polya*, qu'on peut trouver dans la partie *Combinatoire* de Culture*MATH*.

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 3.1.4 *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.

Commentaire 3.1.5 *Ainsi, G agit toujours sur E comme s'il était un sous-groupe de $\mathfrak{S}(E)$. Ceci permet par exemple, grâce au théorème de Lagrange, de déterminer plus facilement quelles sont les actions possibles.*

Si $|G| = 7$ et $|E| = 5$, on peut ainsi voir que seule l'action triviale est possible, pourquoi ? (cf. §**3.3**.*)*

Exemples 3.1.6 *Reprenons certains de nos exemples précédents et appliquons cette dernière propriété.*

(0) A l'action triviale correspond évidemment le morphisme trivial.

(i) A cette action naturelle correspond le morphisme $Id_{\mathfrak{S}(E)}$.

(ii) Dans ce cas, $\mathfrak{S}(\mathcal{P})$ est trop gros pour nous être utile.

(iii) Le morphisme obtenu s'appelle *morphisme de Cayley* :

$$Cayl_G : \begin{cases} G & \longrightarrow & \mathfrak{S}(G) \\ g & \longmapsto & (h \longmapsto g.h) \end{cases}$$

Calculons son noyau : $g = Id_G$ si et seulement si $\forall h \in G, gH = h$, ce qui équivaut, par unicité de l'élément neutre, à $g = e_G$. DOnc le morphisme de Cayley est injectif.

Ceci nous permet de considérer naturellement tout groupe comme un sous-groupe de groupe de permutations. Nous verrons dans la Deuxième Partie comment ces derniers sont eux-mêmes naturellement sous-groupes de Groupes Linéaires.

(iv) Le morphisme est ici $\mathfrak{I}_G : g \longmapsto c_g$, dont l'image est $Int(G)$, le groupe des automorphismes intérieurs déjà vu au **§2.3**, **Exemples 2.3.4 (v)** et **2.3.6** (ii).

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 $\omega(x)$.

Démonstration : (i) Par définition de $\omega(x)$, tout élément z de $\omega(x)$ est de la forme $z = g_z.x$. Par conséquent, $\forall z \in \omega(x), \forall h \in G, h.z = (h.g_z).x \in \omega(x)$ et donc $\omega(z) \subset \omega(x)$.

Réciproquement, il suffit de montrer que $x \in \omega(z)$. Or, on a $z = g_z.x$ donc $x = (g_z^{-1}).z$. On a bien $x \in \omega(z)$, et donc, d'après ce qui précède, $\omega(x) \subset \omega(z)$. On a donc bien l'égalité recherchée.

(ii) Encore un type de raisonnement classique : pour montrer une *disjonction* ("A *ou* B est vraie") on suppose que l'une des deux assertions est fausse et on montre que l'autre est alors forcément vraie.

Prenons donc $\omega(x) \cap \omega(y) \neq \emptyset$, et montrons alors que nécessairement $\omega(x) = \omega(y)$. En fait ceci découle immédiatement du premier point car si $z \in \omega(x) \cap \omega(y)$, on a forcément

$$\omega(x) = \omega(z) = \omega(y).$$

(iii) D'après ce qui précède, $\forall g \in G,\ \forall y \in \omega(x), g.y \in \omega(x)$, et, de plus, les axiomes sont vérifiés (puisqu'ils le sont sur E)... □

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*

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

Commentaire 3.2.5 *On verra dans la deuxième partie comment on s'arrange parfois pour transférer l'éventuelle structure de E sur E/G. Ainsi on verra que si $N < G$, alors* sous certaines hypothèses*, on peut transférer naturellement la structure de groupe au quotient G/H de G sous l'action de H par translation.*

Autre exemple, la structure topologique de la sphère S^2 peut être transférée à son quotient sous l'action de C_2, et obtient ainsi le Plan Projectif.

Nous reverrons ces exemples, et d'autres, dans la Deuxième Partie.

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

Propriété 3.2.6 (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 3.4.4** pour obtenir des informations. Un bon exemple d'application est donné dans le **§3.5**.

Exemples 3.2.7 *Reprenons nos exemples précédents.*

(0) L'orbite de tout élément $x \in E$ sous l'action triviale est égale à {x}.

(i) Sous l'action naturelle de $\mathfrak{S}(E)$, l'orbite de tout élément $x \in E$ est égale à E tout entier car pour tout $y \in E$, il est facile de construire une bijection envoyant x sur y.

(ii) Idem.

(iii) Soit G un groupe et $H < G$, agissant sur G par translation à gauche. Si $a \in G$, notons

$$Ha := \{h.a \mid h \in H\}.$$

On a alors $G/H = \{Ha, a \in G\}$, et les Ha forment une partition de G.

Nous verrons dans la démonstration du théorème de Lagrange que dans ce cas, toutes les orbites ont même cardinal (vous pouvez d'ores et déjà le démontrer).

(iv) L'orbite de $x \in G$ est appelée sa classe de conjugaison. On peut remarquer que

$$\omega(x) = \{x\} \Longleftrightarrow x \in Z(G).$$

On peut aussi noter, en vue de futurs développements, que l'ensemble des classes de conjugaison d'un groupe est un invariant très utile en théorie des représentations linéaires.

(v) Nous nous intéresserons aux points fixes de cette action dans la Deuxième Partie : ce sont les *sous-groupes distingués.* Un tel sous-groupe N permet de munir naturellement G/N (au sens de l'exemple *(iii)*) d'une structure de groupe héritée de celle de G.

(vi) Les orbites sont simples : les paires de points opposés. Notons que S^2/C_2 est le plan projectif, topologiquement et géométriquement.

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. D'après l'**Exemple 3.2.7 (iii)**, 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 :

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

<u>*Démonstration*</u> : On peut écrire la formule des classes :

$$|G| = \sum_{\omega \in G/H} |\omega|.$$

Or, par définition, il y a exactement $(G : H)$ classes. Pour démontrer le théorème, il suffit donc juste de montrer que toutes ces classes ont même cardinal égal à $|H|$.

Pour cela, soit $a \in G$. Nous allons montrer que l'application

$$\begin{cases} H & \longrightarrow Ha \\ h & \longmapsto ha \end{cases}$$

est bijective. Elle est clairement surjective, par définition de l'ensemble aH. Elle est également injective, en effet considèrons deux éléments h et h' de H tels que $ha = h'a$. Multipliant cette égalité à droite par a^{-1} : $h = h'$. Et notre application est donc bien injective.

$\square$

Les applications de ce théorème sont nombreuses. Nous verrons souvent son utilité dans la Deusième Partie. En particulier, l'image et le noyau d'un morphisme étant des sous-groupes, on peut avoir ainsi des informations importantes les concernant grâce au corollaire suivant :

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

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

Démonstration : Même principe que la démonstration précédente : $Ker\ \phi$ agit sur G par translation, et l'on constate aisément que

$$y \in \omega(x) \iff \phi(y) = \phi(x).$$

Par conséquent, le nombre d'orbites correspond au nombre d'images atteintes, autrement dit

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

il ne reste plus qu'à appliquer le théorème de Lagrange. □

Commentaire 3.3.4 *On en déduit ainsi que $|Im\ \phi|$ divise à la fois $|G|$ (par le corollaire) et $|H|$ (directement par le théorème de Lagrange) ! Ceci nous permettra de tirer bien des inférences...*

On reverra ce corollaire dans la Deuxième Partie, comme corollaire d'un autre théorème capital, la factorisation canonique, qui permet de munir $G/Ker\ \phi$ d'une structure de groupe naturellement isomorphe à celle de $Im\ \phi$.

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 3.3.5 *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 $o(x) = \min\{k \in \mathbb{N}^* |\ x = e_G\}$

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

Propriétés 3.3.6 *(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 $o(x)$.

Démonstration : (i) Corollaire du théorème de Lagrange.

(ii) f induit un morphisme surjectif $f_x : \langle x \rangle \to \langle f(x) \rangle$ auquel on peut appliquer le **Corollaire 3.3.3**.

$\square$

Remarque 3.3.7 *si $|G|$ est fini, alors, d'après le corollaire précédent, l'ordre de tout élément de G l'est aussi.*

Exemples 3.3.8 *Quelques exemples de calculs d'ordres d'éléments...*

(0) L'ordre de e_G est 1, c'est le seul élément de G qui ait cette propriété.

(i) L'ordre de n'importe quel élément non nul dans $(\mathbb{Z}, +)$ est infini.

(ii) L'ordre de -1 dans C_2 est 2. L'ordre de $e^{\frac{2ik\pi}{n}}$ dans C_n est $\frac{n}{pgcd(n,k)}$.
Nous reverrons cela dans la Deuxième Partie, lorsque nous étudierons les *Groupes Cycliques.*

L'ordre de $\eta \in C$ est fini si et seulement si η est une racine de l'unité.

(iii) Etablissons le tableau des éléments de $\mathfrak{S}_3$, et indiquons leurs ordres respectifs. Chaque élément occupe une ligne, est décrit par l'image de 1, 2 et 3. Dans la dernière colonne on note l'ordre de l'élément considéré. Vérifiez ce tableau !

	1	2	3	*ordre*
Id	1	2	3	1
τ_1	1	3	2	2
τ_2	3	2	1	2
τ_3	2	1	3	2
σ	2	3	1	3
σ^2	3	1	2	3

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.

On peut déduire de cet exemple la réponse à une question posée dans un **Commentaire** deux paragraphes précédents...

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.

<u>*Démonstration*</u> : Nous allons bien détailler cette démonstration, pour son caractère typique.

- Soient $g, h \in S_A$, on va montrer que $gh \in S_A$.
  En premier lieu, si $a \in A$, on a $h.a = a' \in A$ (car $h.A = A$), donc

$$(gh).a = g.a' = a'' \in A$$

et ainsi $gh.A \subset A$.

Réciproquement, si $a \in A$, alors $\exists a' \in A$ tel que $a = g.a'$ (car $A = g.A$), puis $\exists a'' \in A$ tel que $a' = h.a''$. Ainsi, on a

$$a = g.a' = g.(h.a'') = (gh).a.''$$

D'où $A \subset gh.A$. Donc finalement $A = gh.A$ et on a bien $gh \in S_A$.

- Soit $g \in S_A$, on va maintenant montrer que $g^{-1} \in S_A$.
  En premier lieu, si $a \in A$, $\exists a' \in A$ tel que $a = g.a'$ (car $A = g.A$). On a alors

$$g^{-1}.a = g^{-1}.(g.a') = (g^{-1}g).a' = e_G.a' = a' \in A.$$

On a donc bien $g^{-1}.A \subset A$.

Réciproquement, soit $a \in A$, on a alors

$$a = e_G.a = (g^{-1}g).a = g^{-1}.(g.a).$$

Or $g.a \in A$ (car $g.A = A$), donc $A \subset g^{-1}.A$, et on a bien finalement $g^{-1}.A = A$, et donc $g^{-1} \in S_A$.

$\square$

Commentaire 3.4.2 Attention ! *Ceci ne marcherait absolument pas si on se contentait de poser $S_A := \{g \in G \mid g.A \subset A\}$. En effet, cet ensemble n'est, a priori, pas stable par inversion ! Cherchez donc des contre-exemples... On retrouve ici une idée présentée dans le* **Commentaire 2.2.7** *: les groupes comme transformations conservant parfaitement une structure (ici la simple appartenance).*

Ce lemme très simple va nous permettre de définir un grand nombre de nouveaux groupes comme sous-groupes d'un groupe déjà connu agissant sur un ensemble. Ainsi les groupes diédraux *(cf. Deuxième Partie) sont les sous-groupes de $\mathcal{O}(\mathcal{P})$ qui conservent un polygône régulier donné. Dans le* **§3.6**, *nous allons voir le groupe des isométries directes de l'espace qui laissent invariant un cube.*

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

Définition 3.4.3 *(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 3.4.4 *(mêmes notations) Soit $x \in E$ on a alors*

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

Démonstration : Cette propriété se démontre de façon très analogue au théorème de Lagrange, on fait agir $Stab_G(x)$ sur G... à vous!

□

Exemples 3.4.5 *Reprenons nos exemples précédents.*

(0) Dans le cas de l'action triviale, le stabilisateur de tout point est G entier.

(i) Pour le cas de l'action naturelle de $\mathfrak{S}(E)$ sur E, le stabilisateur d'un élément x de E est

$$\{\sigma \in \mathfrak{S}(E) \text{ tels que } \sigma(x) = x\} \simeq \mathfrak{S}\left(E - \{x\}\right.$$

(ii) Le stabilisateur d'un point $x \in \mathcal{P}$ est l'ensemble des symétries axiales (resp. rotations) dont l'axe passe par x (resp. le centre est x).

(iii) Le stabilisateur de tout élément de G est trivial, car $g.x = x \Longrightarrow g = e_G$.

(iv) Le stabilisateur de $x \in G$ s'appelle le Centralisateur de x, c'est l'ensemble $C_G(x)$ des $g \in G$ qui commutent avec x. On peut remarquer que $C_G(x) = G \Longleftrightarrow x \in Z(G)$.

(v) Le stabilisateur de $H < G$ s'appelle le Normalisateur de H, c'est le plus grand sous-groupe de G dans lequel H est distingué... Nous reverrons tout ça bientôt.

(vi) Le stabilisateur de tout point est trivial.

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.

Une question en passant : que peut-on dire de tout sous-groupe d'un $p-$groupe ?

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.*

<u>*Démonstration*</u> : Pour démontrer cette propriété, nous allons utiliser l'Equation aux classes vue au **3.2**. Soit G un groupe de cardinal $|G| = p^n$ avec $n \geq 1$.

Commençons par exhiber une action de groupe intéressante. Quelle fut la première occurence du centre d'un groupe dans ce cours ? C'était (juste avant la **Définition 2.3.7**) comme noyau du morphisme $\mathfrak{I}_G : G \to \mathfrak{S}(G)$... qui correspond justement à l'action de G sur lui-même par conjugaison (cf. **Exemple 3.1.3 (iv)**.

Poussés par cette remarque pour l'instant anodine, considérons cette action $g.x := g.x.g^{-1}$.

Remarquons que

$$x \in Z(G) \Longleftrightarrow \forall g \in G, gx = xg \Longleftrightarrow \forall g \in G, g.x = x.$$

Ainsi, on peut séparer les éléments de G en deux sortes : ceux qui sont laissés fixes par l'action de conjugaisons (c'est à dire exactement les éléments du centre), et ceux dont l'orbite ne se réduit pas à eux seuls. On peut donc écrire la formule des classes sous la forme

$$|G| = \underbrace{\sum_{x \in Z(G)} |\omega(x)|}_{= \sum_{x \in Z(G)} 1} + \sum_{|\omega| \neq 1} |\omega(x)| = |Z(G)| + \sum_{|\omega| \neq 1} |\omega(x)|.$$

Or, d'après la **Propriété 3.4.4**, le cardinal des orbites du deuxième paquet est un diviseur $\neq 1$ de $|G| = p^n$, donc p divise le deuxième paquet.

On a donc

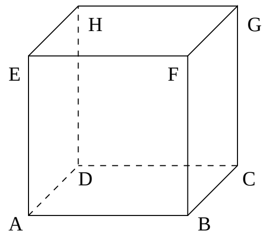
$$|Z(G)| = p^n - \sum_{|\omega| \neq 1} |\omega(x)| \text{ est divisible par } p$$

Or $e_G \in Z(G)$ donc $|Z(G)| \geq 1$, par conséquent $|Z(G)| \geq p$, et $Z(G)$ ne peut pas être trivial. $\square$

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.

Concrètement, on trouve les rotations suivantes :

- L'identité.
- Les six rotations d'angle plus ou moins $\dfrac{\pi}{2}$ 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 $\dfrac{2\pi}{3}$ autour des quatre axes joignant deux sommets opposés.