Lucas Toury - Lycée Saint Martin 30 Novembre 2022

Classification des groupes d'ordre premier

1 Introduction

Le but de ce problème est de montrer qu'il n'existe qu'une seule structure de groupe lorsque que ce dernier est de cardinal p, avec p un nombre premier. Nous allons montrer que si G est un groupe de cardinal p alors $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Déjà pour pouvoir commencer il faut définir ce que veut dire "une seule structure". On sous-entend par cela : un seul groupe à isomorphisme près. Mais qu'est-ce que cela signifie ?
Essayons de comprendre : on sait bien que les groupes peuvent ne pas avoir des éléments de même nature. Par exemple, l'un peut très bien contenir des chaises, alors que l'autre contient des cartes à jouer.
Comprenons bien ce qu'est un groupe. C'est simplement une structure sur un ensemble d'éléments. Cet ensemble peut contenir des chaussettes, des tables, des arbres, des nombres, des fonctions, des vecteurs... peu importe ! Ce qui nous intéresse, ce n'est pas de savoir ce que contient le groupe, mais de savoir comment les éléments intéragissent entre eux grâce à l'opération interne qu'on a sur cet ensemble.
Dire qu'un groupe H et un groupe G ont la même structure (ou sont isomorphes), cela veut dire que leurs éléments intéragissent entre eux de la même manière. Il y a une sorte de bijection entre les deux ensembles mais encore plus forte, car cette bijection arrive à conserver l'opération des groupes. Normalement une bijection entre deux ensembles nous renseigne juste sur le fait que les deux ensembles ont "même cardinal". Ici ils ont aussi la même structure.
Imaginons que H contient des chaussettes avec l'opération interne $*$ et G des cartes à jouer avec l'opération interne $\circ$ et que ces deux groupes sont finis. Si ils ont la même structure cela veut dire que à chaque chaussette on a associé une carte à jouer mais que en plus, si on note s_1, s_2, s_3 trois chaussettes et c_1, c_2, c_3 leurs cartes associées :

$$\text{si } s_1 * s_2 = s_3 \text{ alors } c_1 \circ c_2 = c_3$$

En résumé, de manière intuitive, deux groupes ont même structure ou sont isomorphes (= même forme) si ce sont fondamentalement les mêmes. C'est-à-dire que à part la nature ou le nom de leurs éléments, ils sont identiques. Dans l'exemple précédent si dans G je remplace le mot chaussette par carte à jouer alors j'obtiens le groupe H. Essayons de formaliser tout ça.

2 Morphisme de groupes

Intuitivement, après ce qu'on vient de dire, on va définir ce qu'est un morphisme de groupe. C'est une application entre deux groupes qui se comporte bien avec les opérations de chacun.

Définition 2.1. Soit $(G, *)$ et $(H, \circ)$ deux groupes et ϕ une application de G dans H. On dit que ϕ est un morphisme de groupes entre G et H si :

$$\forall x, y \in G, \quad \phi(x * y) = \phi(x) \circ \phi(y)$$

Si de plus ϕ est une bijection (c'est-à-dire injective et surjective), on dit que ϕ est un isomorphisme et que G et H sont isomorphes.

0) Bien se convaincre que les opérations $*$ et $\circ$ sont au bon endroit.

On vient de définir proprement le fait que deux groupes aient la même strcuture. C'est le cas lorsqu'il existe un isomorphisme de entre les deux. En effet, comme on l'a dit dans l'introduction, un isomorphisme est une bijection qui se comporte en plus bien avec les opérations des groupes.

0 bis) Voir l'analogie avec l'exemple des chaussettes et cartes à jouer et la définition d'un isomorphisme.

3 Le groupe $\mathbb{Z}/_{n\mathbb{Z}}$

Maintenant que nous connaissons l'outil pour dire que deux groupes sont en réalité les "mêmes", il nous faut connaître quelques exemples classiques de groupes et bien les comprendre pour qu'on puisse dire lorsque l'on croise un nouveau groupe inconnu et que par hasard on arrive à trouver un isomorphisme avec un des groupes que l'on connaît : "Ha oui ! Je le connais ce groupe, c'est juste le groupe ... !".

L'exemple le plus classique de groupe fini est le groupe $\mathbb{Z}/_{n\mathbb{Z}}$, c'est simplement le groupe $\mathbb{Z}$ que l'on connaît avec l'addition mais dans lequel on voit tout modulo n. Par exemple si on se place dans $\mathbb{Z}/_{6\mathbb{Z}}$ on a :

$$5 + 9 = 2, \quad 12 + 5 = 5, \quad 9 + 3 = 6$$

0 ter) Vérifier que les calclus sont justes.

Par convention et soucis de clareté, on choisit de noter tous les éléments de $\mathbb{Z}/_{6\mathbb{Z}}$ avec les nombres : 0, 1, 2, 3, 4, 5

Donc on n'écrit pas $5 + 9 = 2$ mais $5 + 3 = 2$, on n'écrit pas $9 + 3 = 6$ mais $3 + 3 = 0$. De la même manière, on note les éléménts de $\mathbb{Z}/_{n\mathbb{Z}}$ avec : 0,1,2,..., $n - 1$.

On a l'impression que noter les éléments de cette manière n'est pas tellement une convention mais plutôt un choix de représentant. Par exemple dans $\mathbb{Z}/_{6\mathbb{Z}}$ on a : $-10 = -4 = 2 = 8 = 14$ mais on choisit 2. Or qui dit représentant dit classe d'équivalence ou encore relation d'équivalence. En effet on peut voir $\mathbb{Z}/_{n\mathbb{Z}}$ comme le quotient de $\mathbb{Z}$ par une certaine relation d'équivalence qui est :

$$a \sim_n b \text{ si } a \equiv b \pmod{n}$$

1) Vérifier que c'est bien une relation d'équivalence.

2) Vérifier que l'ensemble quotient est bien $\mathbb{Z}/_{n\mathbb{Z}}$.

3) Vérifier que $\mathbb{Z}/_{n\mathbb{Z}}$ a bien une strucure de groupe.

On définit donc $\mathbb{Z}/_{n\mathbb{Z}}$ de manière formelle :

Définition 3.1.

$$\mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}/_{\sim_n}$$

Il ne faut donc pas se tromper, quand on dit qu'on note les éléments de $\mathbb{Z}/_{n\mathbb{Z}}$ avec les nombres 0, 1, 2,... ,$n-1$. À ce moment là on fait la confusion entre un nombre et sa classe d'équivalence. L'ensemble $\mathbb{Z}/_{n\mathbb{Z}}$ ne contient pas réellement des nombres mais il faut se l'imaginer comme ça, car ça marche exactement de cette manière. Par la suite, quand on dit $\mathbb{Z}/_{n\mathbb{Z}}$, il faut savoir que cela provient d'un quotient, mais on se l'imagine plutôt comme les nombres de 0 à $n-1$ vus modulo n.

On remarque les deux propriétés suivantes de $\mathbb{Z}/_{n\mathbb{Z}}$:
- il est de cardinal n
- il est abélien, c'est-à-dire que son opération est commutative. C'est normal car cela vient de la commutativité de $+$ sur $\mathbb{Z}$.

Maintenant, on connaît un groupe de cardinal n (ou d'ordre n) pour tout $n \in \mathbb{N}$.

4 Sous-groupe engendré

Pour pouvoir avancer, nous avons besoin de la notion de sous-groupe engendré par un élément. Soit $x \in G$, un élément d'un groupe G, on définit $< x >$ le sous-groupe engendré par x, comme le plus petit sous-groupe (au sens de l'inclusion) de G contenant x. C'est-à-dire que si on a un sous-groupe H de G qui contient x alors $< x > \subseteq H$.
On a vu en exercice qu'une intersection quelconque de sous-groupes est un sous-groupe. On définit donc $< x >$ formellement de cette manière :

Définition 4.1. Soit $x \in G$, on définit le sous-groupe engendré par x par :

$$< x >= \bigcap_{H<G \text{ avec } x\in H} H$$

On rappelle que $H < G$ siginifie "H sous-groupe de G".
La cardinal de $< x >$ est appelé l'ordre de x.

4) Vérifier que cette définition coïncide bien avec la définition intuitive donnée avant.

On définit $P(x) = \{x^n,\ n \in \mathbb{Z}\}$

5) Montrer que $P(x) \subseteq < x >$.

6) Montrer que $P(x)$ est un sous-groupe.

7) En déduire que $< x >= P(x)$.

On a donc une forme "explicite" de $< x >$, ce qui sera parfois bien pratique. On avait déjà vu en exercice sans vraiment le dire que dans le groupe $\mathbb{Z}$: $< n >= n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$.
Remarquons d'ailleurs que cela justifie en quelque sorte la notation $\mathbb{Z}/_{n\mathbb{Z}}$. En quotientant, on a regroupé les nombres par classes d'équivalences qui sont exactement les $n\mathbb{Z}$. En réalité, on pourra voir qu'il est directement possible de quotienter un groupe par un de ses sous-groupes et que sous de bonnes hypothèses, l'ensemble quotient est lui-même muni d'une structure de groupe. C'est ce qui se passe dans le cas de $\mathbb{Z}$ et $n\mathbb{Z}$.

Définition 4.2. On dit qu'un groupe G est monogène si il existe $x \in G$ tel que :

$$G =< x >= \{x^n,\ n \in \mathbb{Z}\}$$

C'est-à-dire que G est engendré par un seul élément.

8) Montrer que si G est fini de cardinal n et monogène, alors $G \simeq \mathbb{Z}/_{n\mathbb{Z}}$, (on pourra essayer de trouver un morphisme qui va de $\mathbb{Z}/_{n\mathbb{Z}}$ dans G puis de montrer que c'est un isomorphisme). Dans ce cas on dit que G est cyclique.

9) Montrer que si G est monogène et de cardinal infini alors $G \simeq \mathbb{Z}$, (pareil, on essaiera de chercher un isomorphisme).

5 Classification des groupes d'ordre 1,2 et 3

Dans ce paragraphe, on va montrer qu'il n'existe qu'une seule structure de groupe à 1, 2 et 3 éléments. C'est-à-dire que, par exemple si $|H| = |G| = 3$ alors on aura forcément $G \simeq H$.

Lorsque le groupe a un petit cardinal il est parfois utile de dresser la table d'opération du groupe. C'est-à-dire que l'on fait un tableau à double entrées avec les éléments du groupe en entrée.

$*$	e	a	b	c
e				
a				
b				
c				

Voici un exemple d'une table d'opération (l'opération est notée $*$) pour un groupe qui a 4 éléments : le neutre noté "e" et les trois autres notés "a", "b" et "c".
Ensuite dans chaque case vide on écrit le produit de l'élément dans la ligne par celui dans la colonne. Attention c'est bien celui de la ligne par celui de la colonne dans cet ordre. Les groupes ne sont pas tous abéliens donc par exemple, le produit $a * c$ est différent de $c * a$ en général.
La donnée de ce tableau rempli détermine entièrement le groupe, en effet avec un tel tableau on connaît la manière dont les éléments interragissent entre eux. Cela détermine la loi du groupe.
Une manière de montrer qu'il n'y a qu'une seule structure de groupe à n éléments est de construire un tableau avec n lignes et n colonnes et de montrer qu'il n'existe qu'une seule manière de le remplir.

10) Soit $x \in G$, un élément d'un groupe. Montrer que l'application de G dans G, $\mu_x : a \mapsto ax$ est une bijection. Que peut-on en déduire sur la composition de chaque ligne et chaque colonne du tableau ?

11) Classifier les groupes d'ordres 1, 2 et 3. C'est-à-dire dans notre cas, montrer qu'il n'y a qu'une seule structure de groupe (donc une seule manière de remplir le tableau) et donner un groupe connu qui a cette structure.

12) Comment voit-on avec le tableau qu'un groupe est abélien ? Les groupes d'ordre 1, 2 et 3 sont-ils abéliens ?

6 Classification des groupes d'ordre premier

Le but de ce paragraphe est de montrer qu'il n'existe qu'une seule structure de groupe à p éléments si p est premier.
Pour ce faire, on va d'abord démontrer un théorème fondamental en théorie des groupes.

Théorème 6.1. Théorème de Lagrange : *Soit G un groupe de cardinal fini et H un sous-groupe de G. Alors $|H|$ divise $|G|$.*

Démonstration :
On prend les notations de l'énoncé.
13) Montrer que pour tout $a \in G$, H et $aH = \{ah,\ h \in H\}$ ont le même nombre d'éléments. C'est-à-dire trouver une bijection entre H et aH.

14) Soit $a,\ b \in G$. Montrer que forcément $aH = bH$ ou $aH \cap bH = \emptyset$.

15) Conclure (on pourra montrer que G se partionne avec des ensembles de la forme aH).

Maintenant qu'on a le théorème de Lagrange on va pouvoir conclure. Soit G un groupe d'ordre p avec p premier.

16) En prenant $x \in G$ avec $x \neq e$ et en considérant $< x >$, montrer que G est monogène.

17) En utilisant le résultat de la question 8, conclure en montrant que tout groupe d'ordre p est isomorphe à un groupe d'ordre p connu.