Lucas Toury - Lycée Saint Martin 28 Septembre 2022

De $\mathbb{N}$ à $\mathbb{Z}$

1 Introduction

On considère un ensemble G qui est pour le moment simplement une collection d'élèments qui ne peuvent pas interragir entre eux. Pour ce faire on munit G d'une opération interne notée $*$, c'est-à-dire :

$$\begin{array}{rccc} *: & G \times G & \to & G \\ & (a,b) & \mapsto & a*b \end{array}$$

Le mot opération signifie que l'on prend deux éléments pour n'en former qu'un.
Le mot interne signifie que l'élément associé reste dans l'ensemble G.

Donner des exemples d'opérations internes sur $\mathbb{N}$:

puis en donner une qui n'est pas interne :

2 Groupes

Définition 2.1. Soit G muni d'une loi de composition interne (notée $*$).
On dit que $(G,*)$ est un groupe lorsque l'opération $*$:
1) est associative, càd :

2) admet un élément neutre, càd :

3) et que tout élément admet un inverse, càd :

Remarque 2.1. On dit que $(G, *)$ est commutatif ou abélien si $*$ est commutative, càd :

Exemple 2.1. Est-ce que ce sont des groupes ?
$(\mathbb{N}, +)$

$(\mathbb{Z}, +)$

$(\mathbb{Q}, \times)$

$(\mathbb{Q}^*, \times)$

$(\mathbb{Q}^*_+, \times)$

$(\{-1, 1\}, \times)$

$(\{0, 1\}, +)$

Remarque 2.2. La plupart du temps, lorsqu'on nomme un groupe, on ne note que l'ensemble, l'opération interne est sous-entendue.
On note aussi de manière générale l'opération interne $\cdot$, (comme une muplitiplication) de façon à écrire "ag" au lieu de "$a \cdot g$" ou "$a * g$". Dans ce cas l'inverse de x est noté x^{-1}.
Si le groupe est abélien on aura tendance à écrire "+" pour l'opération interne. Dans ce cas l'inverse de x est noté $-x$.

Propriété 2.2. L'inverse est unique et de plus $((x^{-1})^{-1}) = x$.

Démonstration

Propriété 2.3. Si y est inverse à gauche de x alors il est aussi inverse à droite.

Démonstration

3 Construction de $\mathbb{Z}$

$(\mathbb{N}, +)$ est donc une ensemble muni d'une loi de composition interne associative avec un élément neutre. On veut lui donner une structure de groupe. On voit qu'il nous faut donc introduire les inverses pour l'addition de chaque entiers naturels car pour l'instant seul 0 a un inverse. On va donc créer $\mathbb{Z}$ en rajoutant les négatifs, mais pourquoi simplement les rajouter ne suffit pas ?

Construction de $\mathbb{Z}$ *:*

4 Sous-groupes

Comme son nom l'indique, un sous-groupe est un groupe contenu dans un groupe plus grand.

Exemple 4.1. $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{Q}, +)$ qui est un sous-groupe de $(\mathbb{R}, +)$ qui est un sous groupe de $(\mathbb{C}, +)$.

Définition 4.1. On dit que H est un sous-groupe de G et on note $H < G$ si :
1) l'élément neutre appartient à H.
2) H est stable par $\cdot$, càd :

3) si $x \in H$ alors $x^{-1} \in H$.

Exemple 4.2. Soit G un groupe, donner deux sous-groupes évidents de G.

Propriété 4.2. Un sous-groupe est un groupe.

Démonstration

Remarque 4.1. Cette proposition sert à montrer plus facilement que G est un groupe en le voyant comme sous-groupe d'un ensemble plus grand.

Propriété 4.3. Si I est un sous-groupe de H qui est lui-même un sous-groupe de G alors K est un sous-groupe de G.

Propriété 4.4. Soient H et K deux sous-groupes de G, alors $H \cap K$ est un sous-groupe de G.

Démonstration

Exemple 4.3. Donner un sous-groupe de $\mathbb{Z}$ non trivial.

5 Exercices

Exercice 1 ($\bullet\bullet\circ$). Soit $(G, *)$ un groupe vérifiant $\forall x \in G, x * x = e$. Montrer que G est abélien.

Exercice 2 ($\bullet\circ\circ$). Soit $(G, \cdot)$ un groupe non abélien. On définit $x * y = yx$. Montrer que $(G, *)$ est un groupe.

Exercice 3 ($\bullet\circ\circ$). Soit $(G,\cdot)$ un groupe non abélien. On appelle centre de G l'ensemble $Z = \{x \in G | \forall y \in G,\ xy = yx\}$. Montrer que Z est un sous-groupe commutatif de G.

Exercice 4 ($\bullet\bullet\circ$). Montrer que tout sous-groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Exercice 5 ($\bullet\bullet\circ$). Soit $(G,\cdot)$ un groupe et H_1, H_2 deux sous-groupes. Montrer que $H_1 \cup H_2$ est un sous-groupe de G ssi $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.

Exercice 6 ($\bullet\bullet\circ$). Soit $(G,\cdot)$ un groupe. On dit qu'un sous-groupe H de G est maximal si $H \neq G$ et si K est un sous-groupe de G qui vérifie $H \subseteq K$ alors $K = H$ ou $K = G$. Trouver tous les sous-groupes maximaux de $(\mathbb{Z}, +)$.

Exercice 7 ($\bullet\circ\circ$). Soit $(G,\cdot)$ un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G. Montrer que $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Exercice 8 ($\bullet\bullet\bullet$). Soit G un groupe. Montrer que G admet un nombre fini de sous-groupes si et seulement si G est fini. (exercice dur qui demande de connaître la notion de sous-groupe engendré par un élément)

6 Pour aller plus loin - Sous-groupe de Frattini

Ce qui va suivre est clairement d'un niveau supérieur (même très supérieur) et demande beaucoup de définitions qui sont difficiles à digérer lorsqu'on les découvre.

Définition 6.1. Soit G un groupe et $x \in G$. On appelle sous-groupe engendré par x le plus petit sous-groupe contenant x au sens de l'inclusion. On le note $< x >$.

Remarque 6.1. Est-ce que cela est toujours bien défini ?
Oui ! Il suffit de voir que $< x >= \bigcap_{H<G | x\in H} H$. C'est un sous-groupe d'après l'exo 7 et l'intersection est non vide car G est dedans.

Exo vérifier sa minimalité.

Définition 6.2. Soit G un groupe et $A \subseteq G$, on définit de même le sous-groupe engendré par A comme le plus petit sous-groupe contenant A au sens de l'inclusion. On le note $< A >$.

Remarque 6.2. On dit que x est générateur si $< x >= G$, dans ce cas on dit que G est monogène. On dit que A est génératrice de G si $< A >= G$.

Définition 6.3. Soit G un groupe. Les éléments de G qui appartiennent à tout sous-groupe maximal (définit comme dans l'exo 6) de G forment un sous-groupe de G, qu'on appelle le sous-groupe de *Frattini* de G et qu'on note $\Phi(G)$. Si G admet au moins un sous-groupe maximal, on peut parler de l'intersection de ses sous-groupes maximaux et $\Phi(G)$ est égal à cette intersection. Si G n'a pas de sous-groupe maximal, $\Phi(G)$ est égal à G tout entier.

Définition 6.4. On appelle élément superflu d'un groupe G tout élément x de G possédant la propriété suivante : toute partie X de G telle que $X \cup \{x\}$ soit une partie génératrice de G est elle-même une partie génératrice de G.

Théorème 6.5. *Le sous-groupe de Frattini $\Phi(G)$ de G est l'ensemble des éléments superflus de G.*

Pour démontrer ce théorème nous aurons besoin du lemme de *Zorn* que nous ne démontrerons pas. (extrêment dur)

Définition 6.6. Un ensemble ordonné tel que toute chaîne (sous-ensemble totalement ordonné) possède un majorant est appelé ensemble inductif.

Remarque 6.3. Voir ce qu'est une relation d'ordre pour la définition d'un ensemble ordonné et totalement ordonné.

Définition 6.7. Dans un ensemble ordonné, un élément maximal est un élément tel qu'il n'existe aucun autre élément de cet ensemble qui lui soit supérieur.

Lemme 6.8. *Zorn* Tout ensemble inductif, admet un élément maximal.

Démonstration du théorème de Frattini
On pourra procéder par double inclusion, c'est-à-dire :
1) Prendre $x \in \Phi(G)$ et montrer que x est superflu.
2) Prendre un élément superflu puis montrer qu'il est dans $\Phi(G)$. Pour ce faire on pourra plutôt essayer de montrer la contraposée, càd : si $x \notin \Phi(G)$ alors x n'est pas superflu. (C'est ici que le lemme de Zorn va intervenir). La preuve du 2) est extrêment dure, prévenez-moi si vous voulez le corriger.