Compléments sur les groupes

Je me souviens 2
1.1 Loi de composition interne . . . 2
1.2 Structure de groupe . . . 2
1.3 Morphisme de groupes . . . 2
1.4 Les entiers . . . 2

Cours 3
2 Sous-groupe engendré par une partie . . . 3
3 Interlude : le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ . . . 3
4 Groupes monogène et groupes cycliques . . . 4
5 Ordre d'un élément dans un groupe . . . 4

Exercices 5
Exercices et résultats classiques à connaître . . . 5
Le centre d'un groupe . . . 5
Les sous-groupes de $(\mathbb{R}, +)$ . . . 5
Exercices . . . 6
Petits problèmes d'entrainement . . . 6

Je me souviens

1.1 Loi de composition interne

1. Qu'est-ce qu'une loi de composition interne ?
2. Comment noter une loi de composition interne ?
3. Que signifient :
   - associatif ?
   - commutatif ?
   - élément neutre ? Comment le note-t-on ?
   - inversible ?
4. Soit E un ensemble, muni d'une loi de composition interne $*$. On suppose l'existe d'un élément neutre noté e. Soit a et b deux éléments de E, inversibles. Est-ce que $(a * b)$ est inversible ?
5. Pour un élément a et un entier n, qu'est-ce que a^n ?
6. Qu'est-ce qu'une **partie stable** de E pour $*$?

1.2 Structure de groupe

7. C'est quoi, un groupe ?
8. Donner des exemples de groupes.
9. Comment définir le **groupe produit** de deux groupes ?
10. C'est quoi, un sous-groupe ?
11. Quels sont les deux sous-groupes triviaux de $(G, *)$?

1.3 Morphisme de groupes

12. Qu'est-ce qu'un morphisme de groupe ?
13. Donner des exemples de morphismes de groupes.

On considère $f : (G, *) \to (H, \cdot)$ un morphisme de groupe.

14. Quelle est l'image du neutre, de l'inverse, par f ?
15. Que dire de l'image (directe) d'un sous-groupe par f ?
16. Que dire de l'image réciproque d'un sous-groupe par f ?
17. C'est quoi, le noyau de f ? Quel lien avec l'injectivité de f ?
18. C'est quoi, l'image de f ? Quel lien avec la surjectivité de f ?
19. Qu'est-ce qu'un **isomorphisme** de groupes.
20. Comment montrer qu'une application est un isomorphisme ?

1.4 Les entiers

21. Que désigne $\mathbb{Z}$? $7\mathbb{Z}$?
22. Énoncer le théorème de la division euclidienne dans $\mathbb{Z}$.

2 Sous-groupe engendré par une partie

Proposition. Une intersection de sous-groupes est un sous-groupe : si $(H_i)_{i\in I}$ une famille de sous-groupes de $(G,*)$, alors $\bigcap_{i\in I} H_i$ est un sous-groupe de G.

Définition. Soit $(G,*)$ un groupe et A une partie de G. On appelle **sous-groupe engendré par** A le plus petit sous-groupe H de $(G,*)$ qui contient A.

Remarque. *On note $\langle A\rangle$ le sous-groupe engendré par A, mais cette notation n'est pas dans le programme officiel.*

Remarque. *La définition signifie que H est le sous-groupe de $(G,*)$ engendré par A si et seulement si :*

- *H est un sous-groupe de $(G,*)$*
- *$A\subset H$*
- *Pour tout sous-groupe K de $(G,*)$, $A\subset K \implies H\subset K$*

Définition. La partie A de $(G,*)$ est dite **génératrice de** G lorsque le sous-groupe de $(G,*)$ engendré par A est G.

Remarque. *On peut décrire le sous-groupe engendré par A : C'est l'ensemble des éléments de G qui s'écrivent sous la forme :*

$$a_1^{\varepsilon_1} * \cdots * a_n^{\varepsilon_n}$$

où $n\in\mathbb{N}$, $a_1,\dots,a_n\in A$, $\varepsilon_1,\dots,\varepsilon_n=\pm1$.
Lorsque G est commutatif et noté additivement, le sous-groupe engendré par A est l'ensemble des éléments qui s'écrivent sous la forme :

$$k_1a_1+\cdots+k_pa_p$$

où $p\in\mathbb{N}$, $a_1,\dots,a_p\in A$ sont distincts, et $k_1,\dots,k_p\in\mathbb{Z}$. Ce ne sont pas tout à fait des combinaisons linéaires, puisque les « scalaires » sont ici entiers.

3 Interlude : le groupe $(\mathbb{Z}/n\mathbb{Z},+)$

Proposition. Pour $n\in\mathbb{N}$, la relation de **congruence modulo** n sur $\mathbb{Z}$ est définie par :

$$a\equiv b\ [n] \iff a-b\in n\mathbb{Z}$$

C'est une relation d'équivalence.

Remarque. *Si $n=0$, il s'agit simplement de l'égalité. Si $n=1$, tous les entiers sont en relation.*

Proposition. Pour $n\geqslant 2$, il y a exactement n classes d'équivalences :

$$\{\overline{0},\overline{1},\dots,\overline{n-1}\}$$

Définition. On note $\mathbb{Z}/n\mathbb{Z}=\{\overline{0},\overline{1},\dots,\overline{n-1}\}$, appelé « $\mathbb{Z}$ sur $n\mathbb{Z}$ ».

Remarque. *On a bien* $\mathrm{Card}\left(\mathbb{Z}/n\mathbb{Z}\right)=n$.

Proposition. Pour $n\geqslant 2$, il existe une unique loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$, encore notée $+$, pour laquelle l'application $k\mapsto\overline{k}$ soit un morphisme de groupes, i.e. :

$$\forall a,b\in\mathbb{Z},\ \overline{a+b}=\overline{a}+\overline{b}$$

Remarque. *Muni de cette loi, $\left(\mathbb{Z}/n\mathbb{Z},+\right)$ est donc bien un groupe commutatif.*

Exemple. Construire la table de la loi $+$ dans $\mathbb{Z}/4\mathbb{Z}$.

Corollaire. Pour $n\in\mathbb{N}^*$, $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$ et $k\in\mathbb{Z}$,

$$k\cdot\overline{a}=\overline{ka}$$

Théorème.

Soit n entier $\geqslant 2$. Alors $(\mathbb{Z}/n\mathbb{Z},+)$ est engendré par chaque $\overline{k}$, où $k \in \{0,\dots,n-1\}$ est premier avec n.

Exemple. Donner la liste des éléments qui engendrent $(\mathbb{Z}/12\mathbb{Z},+)$.

4 Groupes monogène et groupes cycliques

Exemple-proposition. Les sous-groupes de $(\mathbb{Z},+)$ sont les $H = n\mathbb{Z}$, où $n \in \mathbb{N}$.

Proposition. Le sous-groupe de $(G,*)$ engendré par a est

$$\langle a \rangle = \{a^n,\ n \in \mathbb{Z}\}$$

Il est toujours commutatif.

Définition. Soit $(G,*)$ un groupe. On dit que G est **monogène** s'il est engendré par un seul élément, appelé **générateur de** G :

$$\exists x \in G,\ G = \langle x \rangle$$

Lorsque G est monogène et fini, on dit que G est un **groupe cyclique**.

Exemple.

- $(\mathbb{Z},+)$ est monogène, car $\mathbb{Z} = \langle 1 \rangle$, mais n'est pas fini.
- $(\mathbb{Z}/n\mathbb{Z},+)$ est cyclique car $\mathbb{Z}/n\mathbb{Z} = \langle \overline{1} \rangle$ et de cardinal n.

Théorème.

Deux situations se présentent : un groupe monogène est isomorphe à $(\mathbb{Z},+)$ lorsqu'il est infini, et isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$ lorsqu'il est de cardinal n.

Corollaire. Pour tout $n \in \mathbb{N}^*$, $(\mathbb{U}_n,\times)$ et $(\mathbb{Z}/n\mathbb{Z},+)$ sont isomorphes.

5 Ordre d'un élément dans un groupe

Définition. Soit $(G,*)$ un groupe et $a \in G$. On dit que a **est d'ordre fini** si le sous-groupe $\langle a \rangle$ qu'il engendre est de cardinal fini, appelé **l'ordre de** a.

Remarque. *On note* ordre(a) *l'ordre de* a*, mais cette notation n'est pas dans le programme officiel.*

Rappel. Si a est un élément d'ordre d de G, l'application :

$$\begin{array}{rccc} \phi_a : & \mathbb{Z} & \to & G \\ & k & \mapsto & a^k \end{array}$$

est un morphisme de groupes, avec $\mathrm{Im}(\phi_a) = \langle a \rangle$ et $\mathrm{Ker}\,\phi_a = d\mathbb{Z}$.
De plus, l'application :

$$\begin{array}{rccc} \phi_a : & \mathbb{Z}/d\mathbb{Z} & \to & \langle a \rangle \\ & \overline{k} & \mapsto & a^k \end{array}$$

est un isomorphisme de groupes.

Théorème.

Si a est un élément d'ordre $d \in \mathbb{N}^*$ dans un groupe $(G,*)$, alors :

$$\langle a \rangle = \{e, a, a^2, \dots, a^{d-1}\}$$

et :

$$\mathrm{ordre}(a) = \mathrm{Min}\{k \in \mathbb{N}^*,\ a^k = e\}$$

Corollaire. On conserve les notations précédentes. Alors, pour tout $n \in \mathbb{Z}$:

$$a^n = e \iff d \mid n$$

Théorème.

Soit $(G, \star)$ un groupe fini. Alors tous ses éléments sont d'ordre fini.
Plus précisément, pour tout $a \in G$:

$$\mathrm{ordre}(a) \mid \mathrm{Card}(G)$$

c'est-à-dire que $a^{\mathrm{Card}(G)} = e$.

Corollaire. Tout groupe fini dont le cardinal est premier est cyclique, et engendré par chacun de ses éléments différent du neutre.

Exercices et résultats classiques à connaître

Le centre d'un groupe

11.1

Soit $(G, \star)$ un groupe. On définit son **centre** comme l'ensemble des éléments de G qui commutent avec tous les éléments de G :

$$C = \{g \in C,\ \forall h \in G,\ g \star h = h \star g\}$$

Montrer que C est un sous-groupe de $(G, \star)$.

Les sous-groupes de $(\mathbb{R}, +)$

11.2

Montrer que, si G est un sous-groupe de $(\mathbb{R}, +)$, alors il est soit de la forme $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}$, soit dense dans $\mathbb{R}$.
Dans le cas où $G \neq \{0\}$, on s'intéressera à $\alpha = \mathrm{Inf}(G \cap \mathbb{R}_+^*)$ et on discutera selon que $\alpha > 0$ ou $\alpha = 0$.

Exercices

11.3

Soit E un ensemble non vide muni d'une loi $*$ possédant un neutre e. Montrer que a admet un inverse si et seulement si l'application $f : \begin{array}{rcl} E & \to & E \\ x & \mapsto & a * x \end{array}$ est bijective.

11.4

Soit $n \in \mathbb{N}^*$. On considère $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\}$ l'ensemble des racines n-èmes de l'unité. Montrer que $(\mathbb{U}_n, \times)$ est un groupe.

11.5

Soit E un ensemble non vide, $a \in E$. On considère :

$$H = \{f \in \mathfrak{S}(E),\ f(a) = a\}$$

l'ensemble des permutations de E fixant a. Montrer que $(H, \circ)$ est un groupe.

11.6

Montrer que :

$$\mathrm{SL}_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}),\ \det(M) = 1\}$$

est un groupe pour la multiplication.

11.7

Montrer que :

$$H = \{x + y\sqrt{3},\ x, y \in \mathbb{Z},\ x^2 - 3y^2 = 1\}$$

est un sous-groupe de $(\mathbb{R}^*, \times)$.

11.8

Déterminer tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

11.9

Soit $(G, *)$ un groupe commutatif. On considère g_1, g_2 deux élements d'ordre d_1, d_2 respectivement. On suppose que $d_1 \wedge d_2 = 1$. Montrer que $g_1 * g_2$ est d'ordre fini, et calculer cet ordre.

11.10

Démontrer que la matrice :

$$\begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

est d'ordre fini dans $\mathrm{GL}_2(\mathbb{R})$.

11.11

Dans $\mathfrak{S}_{10}$, déterminer l'ordre de :

$$(14378)(257)$$

11.12

Voici la liste des éléments de $\mathfrak{S}_3$:

$$\{\mathrm{Id}, (12), (13), (23), (123), (132)\}$$

Indiquer pour chaque élément son ordre.

Petits problèmes d'entrainement

11.13 ✍

Soit $(G, \star)$ un groupe, et $\mathfrak{S}$ l'ensemble des permutations de G. On rappelle que $(\mathfrak{S}, \circ)$ est un groupe. Pour $g \in G$, on définit :

$$\phi_g : \begin{array}{rcl} G & \to & G \\ h & \mapsto & g \star h \star g^{-1} \end{array}$$

(a) Montrer que $\phi : g \mapsto \phi_g$ est un morphisme de $(G, \star)$ dans $(\mathfrak{S}, \circ)$.

(b) Caractériser les éléments du noyau de ϕ.