GROUPES ET GROUPES SYMÉTRIQUES

1. INTRODUCTION

1.1. Groupe abstrait

Définition 1.1.0.1. —
Un groupe est la donnée d'un couple $(G, \cdot)$ où G est un ensemble et $\cdot : G \times G \to G$ une loi de composition interne, telle que :

1. associativité :
$$\forall a, b, c \in G,\ (a \cdot b) \cdot c = a \cdot (b \cdot c);$$
2. existence de l'élément neutre $e \in G$:
$$\forall g \in G,\ g \cdot e = e \cdot g = g;$$
3. existence de l'inverse :
$$\forall x \in G, \exists y \in G,\ x \cdot y = y \cdot x = e.$$

Notations. — Pour un groupe multiplicatif on note ab l'élément $a \cdot b$, l'élément neutre est noté 1 et l'inverse de a est noté de a^{-1}.

Démonstration 1.1.0.1 (Unicité de l'élément neutre et de l'inverse)
Soient e, e' deux éléments neutres. Alors
$$e' = e \cdot e' = e.$$
Soient b, c inverses de a. Alors :
$$b = b \cdot a \cdot c = c.$$

1.2. Groupe commutatif

Définition 1.2.0.2 (Groupe commutatif (ou Abélien)). —
Un groupe G est commutatif si la loi de composition l'est :

$$\forall x, y \in G,\ xy = yx.$$

Notations. — En général la loi de composition d'un tel groupe est notée comme un groupe additif $(G, +)$. Le neutre est alors 0 et l'inverse de x est $-x$.

1.3. Exemples

- Le couple $(\mathbf{Z}, +)$ est un groupe abélien où $+$ est l'addition usuelle des entiers.
- $(\mathbf{R}, +)$ et $(\mathbf{Q}, +)$ sont également des groupes abéliens.
- $(\mathbf{R} \setminus \{0\}, \times)$ et $(\mathbf{Q} \setminus \{0\}, \times)$ sont des groupes abéliens.
- $\mathrm{GL}(n, \mathbf{R})$ est un groupe pour la composition de matrices en tant que loi de composition. Ce n'est pas un groupe commutatif.

2. SOUS-GROUPE

2.1. Sous-groupe

Définition 2.1.0.3 (Sous-groupe). —
Soit G un groupe (multiplicatif) et $H \subset G$ un sous-ensemble de G. H est un sous-groupe de G si c'est un groupe avec la loi de composition et d'inverse astreintes à H [1§].

Proposition 2.1.0.1. —
Soit G un groupe.
Si $(H_i)_{i \in I}$ est une famille de sous-groupes de G alors $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

Définition 2.1.0.4. —
Pour tout $i \in I$, H_i vérifie la propriété de sous-groupe et donc l'intersection aussi.

Remarque. — Généralement la réunion de sous-groupes n'est pas un sous-groupe. En effet si $x \in H_1$ et $y \in H_2$ alors il n'y a aucune raison que $xy \in \bigcup H_i$.

Pour une équivalence il faut rajouter une hypothèse. Si H, K sont deux sous-groupes de G alors $H \cup K$ est un sous-groupe si, et seulement si, $H \subset K$ ou $K \subset H$.

En effet supposons $H \not\subset K$ et que $H \cup K$ est un sous-groupe. Si $K \not\subset H$ alors on peut choisir $x \in K - K \cap H$ et $y \in H - K \cap H$. On a $x, y \in K \cup H$ et donc par hypothèse

1§. C'est-à-dire si H est stable par l'application $(x, y) \mapsto xy^{-1}$.

$xy \in H \cup K$ et donc il existe des inverses respectifs x^{-1}, y^{-1}. Supposons $xy \in H$: $H \ni (xy)y^{-1} = xe = x \in H$ absurde.

Définition 2.1.0.5 (Groupe engendré). —
Si G est un groupe et X une partie de G alors on appelle sous-groupe de G engendré par X le plus petit sous-groupe de G contenant X. On le notera ici $\langle X \rangle$.
On a de plus si on note $\mathbb{G}$ l'ensemble des sous-groupes de G :

$$\langle X \rangle = \bigcap_{H \in \mathbb{G} \text{ et } H \supset X} H.$$

Exemple. — Soit G un groupe et $x \in G$. Alors :

$$\langle x \rangle = \left\{ x^k \,\middle|\, k \in \mathbf{Z} \right\}.$$

En effet c'est un sous-groupe de $\langle x \rangle$ et le plus petit.

2.2. Ordre d'un groupe et d'un élément

Définition 2.2.0.6 (Ordre d'un groupe). —
Si G est un groupe fini, on appelle *ordre de* G son cardinal, on le note généralement $|G|$ ou $\sharp G$.
Si G est un groupe et $x \in G$ alors on appelle *ordre de* x le cardinal de son sous-groupe engendré (s'il est fini).
Dans le cas où le groupe en question ne serait pas fini, on dit que l'ordre est infini.

Exemples. —

- Dans $\mathbf{Z}$, tous les éléments non nuls sont d'ordre infini.
- Dans $\mathbf{Z}/n\mathbf{Z}$ pour $n \in \mathbf{N}^*$, $\mathbf{Z}/n\mathbf{Z}$ est d'ordre n puisque toute classe admet un représentant dans $\{0, \ldots, n-1\}$.
- Ordre des éléments de $\mathbf{Z}/4\mathbf{Z}$:

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\lvert x \rvert$	1	4	2	4

Théorème 2.2.0.1 (Théorème de Lagrange). —
Pour tout groupe G et tout sous-groupe H de G, l'ordre (i.e. le cardinal) de H divise l'ordre de G :

$$\sharp H \mid \sharp G.$$

Démonstration 2.2.0.2 (Théorème de Lagrange). —
Le cardinal de l'ensemble G/H est appelé *indice* de H dans G et est noté $[G : H]$. De plus, ses classes forment une partition de G et chacune d'entre elles a le même cardinal que H. On a alors :

$$\sharp G = \sharp H \times [G : H].$$

3. MORPHISME DE GROUPES

3.1. Morphisme de groupes

Définition 3.1.0.7. —
Soient G, H deux groupes. Une application $f : G \to H$ est un morphisme de groupes si :

$$\forall x, y \in G,\ f(x \cdot y) = f(x) \cdot f(y).$$

Proposition 3.1.0.2. —
Soient $f : G \to H$ un morphisme de groupes. Alors :

1. $f(e_G) = e_H$;
2. $\forall x \in G,\ f(x^{-1}) = f(x)^{-1}$

3.2. Image et noyau

Définition 3.2.0.8. —
Soit $f : G \to H$ un morphisme de groupes. On définit :

1. $\mathrm{Ker}(f) = \{x \in G \,|\, f(x) = e\}$;
2. $\mathrm{Im}(f) = \{f(x) \,|\, x \in G\}$.

Proposition 3.2.0.3. —
Soit $f : G \to H$ un morphisme de groupes.

1. $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$ sont des sous-groupes de G et H respectivement ;
2. f est injective si, et seulement si, $\mathrm{Ker}(f) = \{e\}$;
3. f est surjective si, et seulement si, $\mathrm{Im}(f) = H$.

Démonstration 3.2.0.3. —
Point par point :

1. On a bien entendu $f(e) = e$ et $f(x)^{-1} = f(x^{-1})$ pour tout $x \in G$. Ainsi $\mathrm{Im}(f) = f(G)$ est un sous-groupe de H.

   Soient $x, y \in G$, alors $f(xy^{-1}) = f(x)f(y^{-1}) = ee^{-1} = e$ donc $xy^{-1} \in G$. De plus $f(e) = e$ donc $\mathrm{Ker}(f)$ est un sous-groupe de G.

2. Soient $x, y \in G$:

$$(f(x) = f(y) \iff x = y) \iff \Big(f(xy^{-1}) = e \iff xy^{-1} = e\Big).$$

3. Par définition, si $\mathrm{Im}(f) = H$ alors f est surjective et réciproquement.