Chapitre 7. Groupes

1 Magmas et monoïdes

1.1 Magmas

Définition 1.1. Une loi de composition interne sur un ensemble E est une application

$$* : \begin{cases} E \times E \to E \\ (x, y) \mapsto x * y \end{cases}$$

Un magma est un ensemble muni d'une composition interne.

Définition 1.2. Soit $(M, *)$ un magma.
Un sous-magma de M est une partie N de M telle que $\forall x, y \in N, x * y \in N$

Définition 1.3. Soit $(M, *)$ et $(N, \circ)$ deux magmas.
Un morphisme de magmas de M dans N est une application $f : M \to N$ telle que
$\forall x, y \in M, f(x * y) = f(x) \circ f(y)$

1.2 Monoïdes

Définition 1.4. Soit $(M, *)$ un magma.

* On dit que $*$ est associative si
  $\forall x, y, z \in M, x * (y * z) = (x * y) * z$
* On dit que $e \in M$ est élément neutre pour $*$ si
  $\forall x \in M, e * x = x * e = x$

Définition 1.5.

* Un monoïde est un ensemble M muni d'une loi de composition interne $*$ associative et possédant un élément neutre.
* Le monoïde $(M, *)$ est dit commutatif si
  $\forall x, y \in M, x * y = y * x$

Proposition 1.6 (Unicité de l'élément neutre). Soit $(M, *)$ un monoïde.

* L'élément neutre de M est unique.
* Plus précisément, si $e_1, e_2 \in M$ vérifient
  $\forall x \in M, e_1 * x = x$ (neutre à gauche) et $\forall x \in M, x * e_2 = x$ (neutre à droite)
  Alors $e_1 = e_2$

Définition 1.7. Soit $(M, \cdot)$ un monoïde et $x \in M$
On dit que M est inversible si $\exists y \in M, xy = yx = 1_M$

Proposition 1.8. Soit $(M, \cdot)$ un monoïde et $x \in M$

* Si x est inversible, l'inverse de x est unique.
* Mieux : si $y_1, y_2 \in M$ vérifient $y_1 x = x y_2 = 1_M$ (càd : y_1 inverse à gauche, y_2 à droite)
  Alors $y_1 = y_2$

Définition 1.9. Soit $(M,\cdot)$ un monoïde et $x \in M$

* Pour tout $n \in \mathbb{N}$, on définit $x^n = \begin{cases} 1_M \text{ si } n = 0 \\ x \cdot x \cdot x \cdot \ldots \cdot x \text{ si } n > 0 \quad (n \text{ facteurs}) \end{cases}$
* Si x est inversible, on note également, pour tout $n \in \mathbb{Z}_-$
  $x^n = (x^{-1})^{|n|} = \begin{cases} 1_M \text{ si } n = 0 \\ x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1} \text{ si } n < 0 \quad (|n| \text{ facteurs}) \end{cases}$

Proposition 1.10. Soit $(M,\cdot)$ un monoïde.

* On a $\forall \in M, \forall n, m \in \mathbb{N} \begin{cases} x^{n+m} = x^n x^m \\ (x^n)^m = x^{nm} \end{cases}$
* Ces propriétés s'étendent aux exposants négatifs si x est inversible.

Définition 1.11. Soit $(M,\cdot)$ un monoïde.
Un sous-monoïde de M est une partie N de M telle que :

* $\forall x, y \in N, xy \in N$ (N stable sous $\cdot$)
* $1_M \in \mathbb{N}$

Définition 1.12. Soit $(M,\cdot)$ et $(N,*)$ deux monoïdes.
Un morphisme de monoïdes de M dans N est une application $f : M \to N$ telle que :

* $\forall x, y \in M, f(x \cdot y) = f(x) * f(y)$
* $f(1_M) = 1_N$

2 Groupes : généralités

2.1 Définition

Définition 2.1. Un groupe est un ensemble G muni d'une loi $\cdot$ telle que :

* La loi $\cdot$ est associative.
* Il existe un élément neutre 1_G pour $\cdot$
* Tout élément de G est inversible :
  $\forall x \in G, \exists y \in G : xy = yx = 1_G$

Un groupe est dit (commutatif) ou abélien si la loi est commutative.

2.2 Sous-groupes

Définition 2.2. Soit $(G,\cdot)$ un groupe.
Un sous-groupe de G est une partie H de G telle que :

* $\forall x, y \in H, xy \in H \quad$ (H stable sous $\cdot$)
* $1_G \in H$
* $\forall x \in H, x^{-1} \in H \quad$ (H est stable par inverse)

Proposition 2.3. Soit $(G,\cdot)$ un groupe et $H \subseteq G$
Alors H est sous-groupe de G ssi H est non vide et stable sous $(x,y) \mapsto xy^{-1}$

Proposition 2.4. Soit G un groupe et $(H_i)_{i\in I}$ une famille de sous-groupes de G
Alors $\bigcap\limits_{i\in I} H_i$ est un sous-groupe de G

Théorème 2.5 (Classification des sous-groupes de $\mathbb{Z}$)**.** Soit H un sous-groupe de $(\mathbb{Z},+)$
Alors il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$

2.3 Morphismes

Définition 2.6. Soit $(G_1, \cdot)$ et $(G_2, \times)$ deux groupes.
Un morphisme (ou homomorphisme) de groupes de G_1 dans G_2 est une application $f : G_1 \to G_2$ telle que $\forall g, g' \in G_1, f(g \cdot g') = f(g) * f(g')$
Un endomorphisme de G est un morphisme $G \to G$
Un isomorphisme $G_1 \to G_2$ est un morphisme bijectif.
Un automorphisme de G est un isomorphisme $G \to G$
On note parfois $\mathrm{Hom}(G_1, G_2)$ l'ensemble des morphismes $G_1 \to G_2$

Proposition 2.7 (Stabilité par composition). Soit $(G_1, \cdot), (G_2, \cdot), (G_3, \cdot)$ trois groupes et $f \in \mathrm{Hom}(G_1, G_2)$, $g \in \mathrm{Hom}(G_2, G_3)$
Alors $g \circ f \in \mathrm{Hom}(G_1, G_3)$

Proposition 2.8. Soit $f : G_1 \to G_2$ un isomorphisme de groupes.
Alors $f^{-1} : G_2 \to G_1$ est aussi un isomorphisme.

Proposition 2.9. Soit $f : G_1 \to G_2$ un morphisme.

- Soit H_1 un sous-groupe de G_1
  Alors $f[H_1]$ est un sous-groupe de G_2
  En particulier, $\mathrm{im}(f)$ est un sous-groupe de G_2
- Soit H_2 un sous-groupe de G_2
  Alors $f^{-1}[H_2]$ est un sous-groupe de G_1
  En particulier, $\ker(f)$ est un sous-groupe de G_1

Proposition 2.10. Soit $f : G_1 \to G_2$ un morphisme de groupes.
Alors f est surjective ssi $\mathrm{im}\, f = G_2$
Et f est injective ssi $\ker f = \{1_{G_1}\}$

Définition 2.11. Soit G un groupe.
Deux éléments g_1 et g_2 sont conjugués si $\exists h \in G : g_2 = hg_1h^{-1}$

Proposition 2.12. La relation "être conjugué" est une relation d'équivalence.

2.4 Ordre d'un élément

Définition 2.13. Soit G un groupe et $g \in G$

- On dit que g est d'ordre fini si $\exists n \in \mathbb{N}^* : g^n = 1_G$
  Dans ce cas son ordre est le plus petit entier $n \in \mathbb{N}^*$ tel que $g^n = 1_G$
- On dit que g est d'ordre infini s'il n'est pas d'ordre fini.

Théorème 2.14. Soit G un groupe et $g \in G$ un élément d'ordre $n \in \mathbb{N}^*$
Alors $\forall k \in \mathbb{Z}, g^k = 1_G \iff n \mid k$

3 Parties génératrices

3.1 Sous-groupe engendré par une partie

Définition 3.1. Soit G un groupe et $A \subseteq G$
On appelle sous-groupe (de G) engendré par A l'intersection de tous les sous-groupes de G contenant A
Autrement dit

$$\langle A \rangle = \bigcap_{\substack{H \text{ sous-groupe de } G \\ A \subseteq H}} H$$

Définition 3.2. Soit G un groupe et $A \subseteq G$
On dit que A engendre G (ou est génératrice de G) si $\langle A \rangle = G$

Théorème 3.3 (Prolongement des identités, version groupes)**.**
Soit G_1, G_2 deux groupes et $\varphi, \psi : G_1 \to G_2$ deux morphismes.
Soit $A \subseteq G_1$ génératrice de G_1
Alors si φ et ψ coïncident sur A (càd si $\forall a \in A, \varphi(a) = \psi(a)$), on a $\varphi = \psi$

3.2 Groupes monogènes et cycliques

Définition 3.4.
- ∗ Un groupe G est dit monogène s'il est engendré par un de ses éléments.
- ∗ Un groupe est dit cyclique s'il est monogène et fini.

Théorème 3.5. Soit G un groupe monogène et $x \in G$ tel que $G = \langle x \rangle$ Alors :
- ∗ (Cas infini) : Si l'ordre de x est infini, on a un isomorphisme $\varphi : \begin{cases} \mathbb{Z} \to G \\ k \mapsto x^k \end{cases}$
- ∗ (Cas cyclique) : Si l'ordre de x est fini et noté $n \in \mathbb{N}^*$, on a un isomorphisme $\varphi : \begin{cases} \mathbb{Z}/n\mathbb{Z} \to G \\ [k]_n \mapsto x^k \end{cases}$

4 Théorème de Lagrange

4.1 Énoncé

Définition 4.1. Soit G un groupe fini.
L'ordre de G est son cardinal $|G|$

Théorème 4.2 (Théorème de Lagrange)**.** Soit G un groupe fini et H un sous-groupe de G
Alors $|H|$ divise $|G|$

Corollaire 4.3. Soit G un groupe fini et $x \in G$
Alors x est d'ordre fini et l'ordre de x divise $|G|$

4.2 Démonstration : Classes à gauche modulo un sous-groupe

Définition 4.4. Soit G un sous-groupe et H un sous-groupe de G
Une classe à gauche modulo H est un ensemble de la forme $gH = \{gh \mid h \in H\}$ où g est un élément de G

Proposition 4.5.
- ∗ Soit $g_1, g_2 \in G$
  Alors on a $g_1 H = g_2 H \iff g_2^{-1} g_1 \in H$
- ∗ La relation $\mathcal{R}$ définie sur G par
  $\forall g_1, g_2 \in G, g_1 \mathcal{R} g_2 \iff g_1 H = g_2 H$
  est une relation d'équivalence.

Définition 4.6. L'ensemble des classes à gauche (qui est donc l'ensemble des classe de cette relation d'équivalence) est noté G/H

Proposition 4.7. Toutes les classes à gauche modulo H sont en bijection avec H

4.3 Cas d'un morphisme de groupes

Proposition 4.8. Soit G_1, G_2 deux groupes finis et $f : G_1 \to G_2$ un morphisme de groupe.
Alors $|G_1| = |\ker f| \times |\operatorname{im} f|$