Théorie des graphes et algèbre computationnelle
Algèbre

Brandon LIN

November 10, 2023

Contents

Chapter 1

Théorie des groupes

1.1 Définitions et premières propriétés

1.1.1 Groupe

Definition 1.1.1: Groupe

On dit que $(G, \times)$ est un **groupe** lorsque G est un ensemble non vide et $\times$ une *loi de composition interne* sur G vérifiant :

- $\times$ *associative* :
$$\forall (x, y, z) \in G^3,\ (x \times y) \times z = x \times (y \times z) \tag{1.1}$$
- Existance d'un **élément neutre** $e \in G$ pour $\times$:
$$\forall x \in G,\ e \times x = x \times e = x \tag{1.2}$$
- Tout élément de G possède un inverse pour $\times$:
$$\forall x \in G, \exists y \in G,\ x \times y = y \times x = e \tag{1.3}$$
on note $x^{-1} \overset{Not}{=} y$ l'inverse de $x \in G$.

Definition 1.1.2: Abélien ou commutatif

$(G, \times)$ un groupe est **commutatif** ou **abélien** si x est commutative :
$$\forall (x, y) \in G^2,\ x \times y = y \times x \tag{1.4}$$

1.1.2 Groupe symétrique

Definition 1.1.3

- Soit E un ensemble. On note $\mathcal{S}(E)$ l'ensemble des bijections de E dans E qu'on appelle l'ensemble des **permutations** de E.
- $(\mathcal{S}(E), \circ)$ est appelé le **groupe symétrique** de E.
- Si $E = [\![1, n]\!]$ où $n \in \mathbb{N}^*$ alors on note simplement $\mathcal{S}_n$ le groupe symétrique de $[\![1, n]\!]$. Son **ordre** est égal à $\text{card}(\mathcal{S}_n) = n!$.
- Pour tout $\psi \in \mathcal{S}_n$, on note

$$\psi = \begin{pmatrix} 1 & 2 & \dots & n \\ \psi(1) & \psi(2) & \dots & \psi(n) \end{pmatrix} \tag{1.5}$$

Example 1.1.1

Pour $n = 3$, il y a 6 permutations de $[\![1, 3]\!]$:

$$\text{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \tau_{1,2} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau_{1,3} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \tag{1.6}$$

$$\tau_{2,3} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_+ = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_- = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \tag{1.7}$$

Example 1.1.2

On peut calculer :

$$\tau_{1,2} \circ \tau_{2,3} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_+ \tag{1.8}$$

Proposition 1.1.1

Si $n \geq 3$, $(\mathcal{S}_n, \circ)$ n'est pas abélien.

Proof: Soient $(a, b, c) \in [\![1, n]\!]^3$ trois éléments distincts.
On considère des permutations φ et ψ de $[\![1, n]\!]$, telles que :

$$\begin{cases} \varphi(a) = b \\ \varphi(b) = a \\ \varphi(c) = c \end{cases}, \quad \begin{cases} \psi(a) = c \\ \psi(b) = b \\ \psi(c) = a \end{cases} \tag{1.9}$$

Alors, $(\varphi \circ \psi)(a) = \varphi(\psi(a)) = \varphi(c) = c$ et $(\psi \circ \varphi)(a) = \psi(\varphi(a)) = \psi(b) = b \neq c$
Donc $\varphi \circ \psi \neq \psi \circ \varphi$, donc $\mathcal{S}_n$ n'est pas abélien. 😄

Example 1.1.3

Dans $(\mathcal{S}_3, \circ)$, on remarque que

$$\sigma_+ \circ \tau_{1,2} = \tau_{1,3}, \quad \tau_{1,2} \circ \sigma_+ = \tau_{2,3} \neq \tau_{1,3} \tag{1.10}$$

Remarque :

- De même $\mathcal{S}(E)$ n'est pas abélien lorsque E est un ensemble infini.

- Le sous-ensemble $\{\mathrm{id}, \sigma_+, \sigma_-\}$ a aussi une structure de groupe pour la composition $\circ$ ($\{\mathrm{id}, \sigma_+, \sigma_-$ est un groupe abélien fini d'ordre 3). Par contre $\{\mathrm{id}, \tau_{1,2}, \tau_{2,3}, \tau_{1,3}\}$ n'a pas de structure de groupe.

  Par exemple, $\tau_{1,2} \circ \tau_{2,3} = \sigma_+$ donc $\circ$ n'est pas un loi de composition interne.

1.1.3 Sous-groupes

Definition 1.1.4: Sous-groupe

Soit $(G, *)$ un groupe et $H \subset G$, alors on dit que H est un **sous-groupe** de $(G, *)$ lorsque

- $e \in H$
- *Stabilité par la loi de composition interne* :

$$\forall (x, y) \in H, \quad x * y \in H \tag{1.11}$$

- *Stabilité par passage au symétrie* :

$$\forall x \in H, \ \bar{x} \in H \tag{1.12}$$

Proposition 1.1.2

H est un sous-groupe de $(G, *)$ si et seulement si

- $e \in H$
- $\forall (x, y) \in H, \ x * \bar{y} \in H$

Proof:

- ($\Longrightarrow$) Simple.
- ($\Longleftarrow$) Soit $x \in H$, alors $\bar{x} = e * \bar{x} \in H$ car $(e, x) \in H^2$, donc 1.12 est vérifié. Soit $(x, y) \in H^2$, alors $x * y = x * \bar{\bar{y}} \in H$ car $(x, \bar{y}) \in H^2$, donc 1.11 est vérifié.

Example 1.1.4

- $\mathbb{Z}$ est un sous-groupe de $(\mathbb{Q}, +)$, de $(\mathbb{R}, +)$ et aussi de $(\mathbb{C}, +)$. C'est parce que $\mathbb{Q}$ est un sous-groupe de $(\mathbb{R}, +)$ et $\mathbb{R}$ est un sous-groupe de $(\mathbb{C}, +)$.
- Pour tout $n \in \mathbb{N}$, $n\mathbb{Z} = \{nk, \ k \in \mathbb{Z}\}$ est un sous-groupe de $(\mathbb{Z}, +)$

  En particulier, l'ensemble $2\mathbb{Z}$ des entiers pairs est un sous-groupe de $(\mathbb{Z}, +)$.

  Mais, l'ensemble $\{2k + 1, \ k \in \mathbb{Z}\}$ des entiers impairs n'est pas un sous-groupe de $(\mathbb{Z}, +)$ (car il ne contient pas 0 et il n'est pas stable par addition)
- L'ensemble des fonctions réelles continues sur $I \subset \mathbb{R}$ est un sous-groupe additif de l'ensemble ds fonctions réelle définies sur I (car une somme de fonctions continues est continue)

  De même l'ensemble des fonctions dérivables sur I est bien un sous-groupe additif.

  Mais, l'ensemble des fonctions positives sur I n'est pas un sous-groupe additif car il n'est pas stable par passage à l'opposé.
- Le sous-ensemble des suites réelles croissantes n'est pas un sous-groupe additif de l'ensemble des suites réelles.

  Mais, le sous-ensemble des suites réelles nulles à partir d'un certain rang est bien un sous-groupe additif.

Example 1.1.5

- Pour tout $n \in \mathbb{N}^*$, $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\}$ est un sous-groupe de $(\mathbb{U} = \{z \in \mathbb{C}, |z| = 1\}, \times)$. Ces deux groupes sont des sous-groupes de $(\mathbb{C}^*, \times)$.

  De même $\mathbb{R}^*$ et $]0, +\infty[$ sont des **sous-groupes multiplicatifs** de $\mathbb{C}^*$.

  Mais, $i\mathbb{R} = \{iy,\ y \in \mathbb{R}\}$ n'est pas un sous-groupe multiplicatif de $\mathbb{C}^*$ (car $1 \notin i\mathbb{R}$)

- $\{\mathrm{id}, \sigma_+, \sigma_-\}$ est un sous-groupe de $(\mathcal{S}_3, \circ)$

- Soit E un ensemble et $A \subset E$. On note $H = \{\varphi \in \mathcal{S}(E),\ \varphi(A) \subset A\}$ l'ensemble des permutations de E qui laissent A stable, alors H est un sous-groupe de groupe symétrique $\mathcal{S}(E)$, en effet :
  - $\mathrm{id} \in H$ car $\mathrm{id}(A) = A$
  - Si $\varphi \in H$ alros φ est une bijection qui envoie $\varphi(A)$ dans A
  - Or $A \subset E$ est un ensemble fini donc $\mathrm{card}(\varphi(A)) = \mathrm{card}(A)$.
  - Donc, $\varphi(A) = A$, $\varphi^{0-1}(A) = A$, donc H est stable par passage à symétrique. (la bijection réciproque de φ = le symétrique de φ par 0)
  - La stabilité de H par composition est immédiate.

Remarque : Soit $(G, *)$ un groupe. Alors le plus petit sous-groupe est $\{e\}$ et le plus grand sous-groupe est G. Ces deux sous-groupes sont appelés les sous-groupes **triviaux** de G.

Proposition 1.1.3

Toute intersection de sous-groupes de $(G, *)$ est un sous-groupe de $(G, *)$.
C'est en général faux pour l'union.

Proof: Intersection Soit $(H_i)_{i\in I}$ des sous-groupes de $(G, *)$, on pose $H = \bigcap_{i\in I} H_i$, alors $\forall i \in I$, $e \in H_i$ car H_i est un sous-groupe donc $e \in H$.
Si $(x, y) \in H^2$, alors $\forall i \in I$, $(x, y) \in H_i^2$ donc $x * \bar{y} \in H_i$ car H_i est un sous-groupe donc $x * \bar{y} \in H$.
Par conséquent, H est bien un sous-groupe. ☺

Example 1.1.6

Dans $(\mathbb{Z}, +)$, $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ sont les sous-groupes.
Par exemple $2\mathbb{Z} \cup 3\mathbb{Z}$ n'est pas un sous-groupe de $(\mathbb{Z}, +)$ car $5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$

Definition 1.1.5

Soit $(G, *)$ un groupe et $A \subset G$ alors l'intersection de tous les sous-groupes de $(G, *)$ qui contiennant A est appelées le **sous-groupe engendrée** par A, on le note :

$$\langle A \rangle = \bigcap_{H \text{ sous-groupe de } (G,*),\ A \subset H} H \tag{1.13}$$

Proposition 1.1.4

$\langle A \rangle$ est le plus petit sous-groupe qui contient A.

Proof:

- $\langle A \rangle$ est bien un sous-groupe comme intersection de sous-groupes.
- Il est immédiat que $A \subset \langle A \rangle$

- Si B est un sous-groupe qui contient A, alors $\langle A \rangle \subset H$ par définition.

😄