Théorie des graphes et algèbre computationnelle
Algèbre

Brandon LIN

November 17, 2023

Contents

Chapter 1

Définitions et premières propriétés

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 notée $(x, y) \mapsto x \times y$ vérifiant :

- $\times$ *associative* :
$$\forall (x, y, z) \in G^3, \ (x \times y) \times z = x \times (y \times z) \tag{1.1}$$
- Existence 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 $x \in G$.

1.1.1 Groupe abélien

Definition 1.1.2: Groupe 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 fini et infini

Definition 1.1.3: Groupe fini, Ordre

Si G est un ensemble fini, alors on dit $(G, \times)$ est un **groupe fini**, on note $\mathrm{card}(G)$ l'**ordre** de $(G, \times)$. Sinon on dit que $(G, \times)$ est d'**ordre infini**.

1.1.3 Groupe symétrique

Definition 1.1.4

- 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.

1.1.4 Sous-groupes

Definition 1.1.5: 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 :
  - 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 1.1.6: Sous-groupe engendrée

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.

😊

[Manque un cours ici]

Definition 1.1.7: Groupe momogène

Un groupe $(G, *)$ est dit **monogène** s'il est engendré par un élément :

$$\exists a \in G, G = \langle\{a\}\rangle = \{a^{*k,\, k\in\mathbb{Z}}\} \tag{1.14}$$

Autrement dit, G est le groupe itérés de a. Dans ce cas, on dit que a est un **générateur** de $(G, *)$.

Example 1.1.7

Pour tout $n \in \mathbb{Z}$, $n\mathbb{Z} = \{k_n,\ k \in \mathbb{Z}\}$ est un groupe additif homogène. n est $-n$ sont des générateurs de $n\mathbb{Z}$.

Theorem 1.1.1

Tout sous-groupe additif de $(\mathbb{Z}, +)$ est monogène, c'est-à-dire de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$ est unique.

Proof: Soit H un sous-groupe additif de $(\mathbb{Z}, +)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$, sinon $H \cap \mathbb{N}^* \neq \emptyset$ car H est stable par passage à l'opposé.

On pose

$$n = \min(H \cap \mathbb{N}^*)$$

.

- Montrons que $H = n\mathbb{Z}$, on a déjà que $n\mathbb{Z} \subset H$ car $n \in H$, H est stable par addition et par passage à l'opposé.

  Par l'inclusion réciproque, on fixe $h \in H$. On pose

  $$k = \max\{k \in \mathbb{Z},\ k_n \leq h\} = E\left(\frac{h}{n}\right) \quad (n \neq 0,\ n \in \mathbb{N}^*) \tag{1.15}$$

  Donc, $k \leq h/n < k+1$ donc $k_n \leq h < k_n + n$, donc $h - k_n \in [\![0, n-1]\!]$.

  Or $h - k_n \in H$ par stabilité car $h \in H$ et $n \in H$.

  On en déduit que $h - k_n = 0$ car $\min(H \cap \mathbb{N}^*) = n$ donc $h = kn \in n\mathbb{Z}$. Par conséquent $H = n\mathbb{Z}$

- L'unicité est immédiate car $\min(n\mathbb{Z} \cap \mathbb{N}^*) = n$

😊

Remarque : Les sous-groupes additifs de $\mathbb{R}$ ne sont pas tous monogènes. Par exemple $\mathbb{Q}$ n'est pas de la forme $x\mathbb{Z}$ où $x \in \mathbb{R}$

En effet, le complémentaire de $n\mathbb{Z}$ contient des intervalles (par exemple $]0, |n|[\cap n\mathbb{Z} = \emptyset$ si $n \neq 0$) alors que $\mathbb{Q}$ est dense dans $\mathbb{R}$:

$$\forall a < b,\ ]a, b[\cap\mathbb{Q} \neq \emptyset \tag{1.16}$$

Theorem 1.1.2

Tout sous-groupe additif de $(\mathbb{R}, +)$ est de l'un des deux types suivants :

- Monogène, c'est-à-dire de la forme $x\mathbb{Z}$ où $x \in \mathbb{R}_+$ est unique
- Dense dans $\mathbb{R}$, c'est-à-dire qu'il intersectetout intervalle de $\mathbb{R}$ (aussi petit qu'on veut)

Proof: Soit Hun sous-groupe de $(\mathbb{R}, +)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$. Sinon $H \cap \mathbb{R}_+^* \neq \emptyset$ (car H est stable par passage à l' opposé)

On pose

$$x = \inf(H \cap \mathbb{R}_+^*) \tag{1.17}$$

Il y a deux cas selon que l'inf est atteint ou non.

1. $x > 0$ donc $x = \min(H \cap \mathbb{R}_+^*)$. On peut montrer que $H = x\mathbb{Z}$ en raisonment comme dans la démonstration de sous-groupes de $(\mathbb{Z}, +)$ de même pour l'unicité.
2. $x = 0$ Donc il existe une suite $(h_n)_{n\in\mathbb{N}}$ telle que :
   - $\forall n \in \mathbb{N},\ h_n \in H \cap \mathbb{R}_+^*$
   - $\forall n \in \mathbb{N},\ 0 < h_{n+1} < h_n$ (strictement décroissante)
   - $h_n \underset{n\to+\infty}{\longrightarrow} 0$

   Montrons que H est dense dans $\mathbb{R}$, donc qu'il intersecte tout intervalle de $\mathbb{R}$. Soit $]a, b[\subset \mathbb{R}$, montrons $H\cap]a, b[\neq \emptyset$.

   On sait que $\exists n \in \mathbb{N},\ 0 < h_n < b - a$. On pose

   $$j = \max\{k \in \mathbb{Z},\ kh_n \leq a\} = E\left(\frac{a}{h_n}\right) \tag{1.18}$$

   Alors $a - kh_n \in [0, h_n[$.

   $$kh_n \leq a < kh_n + h_n < kh_n + b - a \leq b \tag{1.19}$$

   Donc, $(k + 1)h_n \in]a, b[$ et $(k + 1)h_n \in H$ car $h_n \in H$ et par stabilité de H.

   Par conséquent $]a, b[\cap H \neq \emptyset$, on en déduit que H est dense dans $\mathbb{R}$.

😄

Example 1.1.8

Soit $x \in \mathbb{R}$, alors il existe deux suites $(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ telles que

$$x = \lim_{n\to+\infty} a_n + b_n\sqrt{2} \tag{1.20}$$

car $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ (a, b) \in \mathbb{Z}^2\}$ l'anneaux des entiers de Gauss.
En effet, $(\mathbb{Z}[\sqrt{2}, +)$ est le sous-groupe de $(\mathbb{R}, +)$ engendré par 1 et $\sqrt{2}$, s'il $\mathbb{Z}[\sqrt{2}]$ est de la forme $y\mathbb{Z}$ où $y \in \mathbb{R}_+$ alors

$$\exists (k_1, k_2) \in \mathbb{Z}^2,\ 1 = k_1 y,\ \sqrt{2} = k_2 y \tag{1.21}$$

Donc,

$$\sqrt{2} = \frac{k_2}{k_1} \in \mathbb{Q} \tag{1.22}$$

ce qui est absurde. Donc $\mathbb{Z}[\sqrt{2}]$ est danse dans R.

Definition 1.1.8: Groupe cyclique

Soit $(G, *)$ un groupe.

- On dit que G est **cyclique** si G est monogène est fini
- Soit $a \in G$, si $\langle\{a\}\rangle$ est fini (donc cyclique) alors son ordre $|\langle\{a\}\rangle|$ est appelé l'**ordre** de a dans $(G, *)$. Sinon a est dit d'**ordre infini**.

Proposition 1.1.5

Soient $(G,*)$ un groupe et $x \in G$. Si a est d'ordre fini alors son ordre est égal à

$$\min\{n \in \mathbb{N},\ a^{*n} = e\} \tag{1.23}$$

Proof: Puisque $\langle\{a\}\rangle = \{a^{*k}, k \in \mathbb{Z}\}$ est fini, on sait que

$$\exists (k_1, k_2) \in \mathbb{Z}^2,\ a^{*k_1} = a^{*k_2},\ k_1 \neq k_2 \tag{1.24}$$

On peut supposer que $k_1 \subset k_2$, alors $a^{*(k_2-k_1)} = a^{*k_2} \times \overline{a^{*k_2}} = e$ et $k_2 - k_1 \in \mathbb{N}^*$
Donc $\{n \in \mathbb{N}^*,\ a^{*n} = e\} \neq \emptyset$, donc $n = \min\{n \in \mathbb{N}^*,\ n^{*n} = e\}$ existe.
Montrons que $\langle\{a\}\rangle = \{a^{*k},\ k \in [\![0, n-1]\!]\}$.

- L'inclusion inverse est évidente.
- Pour l'inclusion, onfixe $k \in \mathbb{Z}$, on pose $l = \max\{l \in \mathbb{Z},\ ln \leq k\} = E\left(\frac{k}{n}\right)$ donc $k = ln \in [\![0, n-1]\!]$

  Et $a^{*k} = a^{*(j-ln)} * (a^{*n})^{*l=a^{*(j-ln)}}$.

  Donc l'ordre de a est égal à

  $$|\langle\{a\}\rangle| = \text{card}\{a^{*k},\ k \in [\![0, n-1]\!]\} = n \tag{1.25}$$

  car $n = \min\{n \in \mathbb{N}^*,\ a^{*n=e}\}$ donc $\forall (k_1, k_2) \in [\![0, n-1]\!]^2,\ k_1 \neq k_2 \implies a^{*k_1} \neq a^{*k_2}$

Example 1.1.9

Soit $n \in \mathbb{N}$, alors

$$\mathbb{U}_n = \{e^{i\frac{2k\pi}{n}},\ k \in [\![0, n-1]\!]\} \tag{1.26}$$

donc $(\mathbb{U}_n, \times)$ est cyclique et $\omega = e^{\frac{2i\pi}{n}}$ est d'ordre n, qui est un générateur de $\mathbb{U}_n$

1.2 Morphismes de groupes

Definition 1.2.1: Homomorphisme

Soit $(G,*)$ et $(H,.)$ deux groupes. Un **homomorphisme** de $(G,*)$ vers $(H,.)$ est une application $f : G \longrightarrow H$ telle que

$$\forall (x,y) \in G^2,\ f(x*y) = f(x).f(y) \tag{1.27}$$

Proposition 1.2.1

Si $f : (G,*) \longrightarrow (H,.)$ est un **homomorphisme** de groupes alors :

- $f(e_G) = f(e_H)$
- $\forall x \in G,\ f(\overline{x}) = \overline{f(x)}\quad (n = -1)$
- $\forall x \in G,\ n \in \mathbb{Z},\ f(x^{*n}) = (f(x))^{.n}$

Proof:
- On a $f(e_G) = f(e_G * e_G) = f(e_G).f(e_G)$
- Soit $x \in G$, on a :

  $$f(x).f(\overline{x}) = f(x * \overline{x}) = f(e_G) = e_H \tag{1.28}$$

- De même $f(\overline{x}).f(x) = e_H$.
- Récurrence

😆

Example 1.2.1

- Soit $n \in \mathbb{R}$, alors $x \mapsto ax$ est un homomorphisme du groupe $(\mathbb{R}, +)$ vers lui-même.
- $x \mapsto \ln x$ est un homomorphisme du groupe $(\mathbb{R}_+^*, \times)$ vers $(\mathbb{R}, +)$
- $x \mapsto e^{i\theta}$ est un homomorphisme de groupe $(\mathbb{R}, +)$ vers le groupe $(\mathbb{C}^*, \times)$ au $(\mathbb{U}, \times)$

Example 1.2.2

L'application qui associe à chaque suitre convergente sa limite est un homomorphisme additif.

Example 1.2.3

a transposée des matrices de $(\mathrm{M}_n(\mathbb{K})$ est un homomorphisme additif.
Le déterminant des matrice de $\mathrm{GL}_n(\mathbb{K})$ est un homomorphisme multiplicatif.