Chapitre 11

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.

- $\bigcap_{i\in I} H_i \subset G$
- $\forall i,\ e\in H_i$ donc $e\in \bigcap_{i\in I} H_i$ donc $\bigcap_{i\in I} H_i \neq \emptyset$
- Soit $x,y\in \bigcap_{i\in I} H_i$

  on a $\forall i$ $x*y\in H_i$ car H_i stable par $*$

  donc $x*y\in \bigcap_{i\in I} H_i$
- Soit $x\in \bigcap_{i\in I} H_i$

  on a $\forall i$, $x\in H_i$ donc $x^{-1}\in H_i$

  donc $x^{-1}\in \bigcap_{i\in I} H_i$

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 $n \in \mathbb{N}$, $a_1, \ldots, a_n \in A$, $\varepsilon_1, \ldots, \varepsilon_n = \pm 1$.
Lorsque G est commutatif et noté additivement, le sous-groupe engendré par A est l'ensemble des éléments qui s'écrivent sous la forme :

$$k_1 a_1 + \cdots + k_p a_p$$

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

$\langle A\rangle = \bigcap_{H \supset A} H$ où H sous-groupe de G — c'est un sous-groupe de G qui contient A

Exemple : $A = \{a_1, a_2, a_3\}$ $\quad a_1, a_2, a_3 \in G$

$\langle A\rangle$ est un sous-groupe de G qui contient :

e, a_1, a_2, a_3

a_1^{-1}, a_2^{-1}, a_3^{-1}

$a_1 a_2$, a_1^2, $a_1 a_3$

$a_1 a_2^{-1}$, $a_1 a_2^{-1} a_3 a_2^{-1} a_1$ ...

$$\langle A\rangle = \underbrace{\left\{ a_{i_1}^{\pm 1} a_{i_2}^{\pm 1} a_{i_3}^{\pm 1} \cdots a_{i_n}^{\pm 1} \quad i_k \in \{1,2,3\},\ n \in \mathbb{N} \right\}}_{H}$$

Preuve : H est un sous-groupe de G.
contenant A et $\langle A\rangle \subset H$ nécessairement.

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.

- $a \equiv b\ [n] \iff \exists k \in \mathbb{Z}$ t.q. $a = b + nk$

  $\iff a$ et b ont le même reste dans la division euclidienne par n

- est réflexive
  - symétrique
  - transitive

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* $\text{Card}\,(\mathbb{Z}/n\mathbb{Z}) = n$.

Si $x \in \mathbb{Z}/n\mathbb{Z}$, il y a un représentant de x, qui est $k \in \mathbb{Z}$ t.q. $x = \overline{k}$

Par exemple : $\mathbb{Z}/3\mathbb{Z} = \{\alpha, \beta, \gamma\} = \{\overline{0}, \overline{1}, \overline{2}\}$

la classe d'équivalence de tous les entiers $k \in \mathbb{Z}$ t.q. $k \equiv 0\ [3]$ $\quad \overline{0} = \overline{3} = \overline{6} \dots$

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, $(\mathbb{Z}/n\mathbb{Z}, +)$ est donc bien un groupe commutatif.*

On définit sur $\mathbb{Z}/n\mathbb{Z}$ une loi $+$ en posant :

$\overline{a} + \overline{b} \underset{\text{déf}}{=} \overline{(a+b)}$

↑ c'est le $+$ de $\mathbb{Z}$

Exemple : Dans $\mathbb{Z}/3\mathbb{Z} = \{\alpha, \beta, \gamma\}$

$\alpha = \overline{0}$, $\beta = \overline{1}$, $\gamma = \overline{2}$, $\overline{3}$, $\overline{7}$, $\overline{11}$

$\beta + \gamma = \overline{1} + \overline{2} \overset{\text{def}}{=} \overline{(1+2)} = \overline{3} = \overline{0} = \alpha$

$= \overline{7} + \overline{11} \overset{\text{def}}{=} \overline{(7+11)} = \overline{18} = \overline{0} = \alpha$

Preuve : Soit a, b, a', b' tq $\overline{a} = \overline{a'}$, $\overline{b} = \overline{b'}$

ie $a \equiv a' \ [n]$ et $b \equiv b' \ [n]$

$k_1, k_2 \in \mathbb{Z}$ $\quad a = a' + k_1 n \quad b = b' + k_2 n$

$a + b = a' + b' + (k_1 + k_2) n$

donc $a + b \equiv a' + b' \ [n]$

Ainsi : $\overline{a+b} = \overline{a'+b'}$

Bref la déf de $\overline{a} + \overline{b}$ par $\overline{a+b}$ est indép du choix des représentants des classes d'équivalences.

$\overline{1}$ $\overline{1}$

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 $(\mathbb{Z}/12\mathbb{Z}, +)$.

$\mathbb{Z}/12\mathbb{Z} = \{\alpha, \beta, \gamma \dots \}$

$= \{\overline{0}, \overline{1}, \dots, \overline{11}\} = \{\overline{12}, \overline{25}, \dots\}$

$\langle \overline{2} \rangle = \{\overline{2}, -\overline{2}, \overline{2}+\overline{2}, -\overline{2}-\overline{2}, \overline{2}+\overline{2}+\overline{2} \dots$

$= \{n\overline{2}, n \in \mathbb{Z}\}$

$= \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$

$\overline{12}$ $\quad -\overline{2}$

donc $\overline{2}$ n'engendre pas $\mathbb{Z}/12\mathbb{Z}$

mais un sous-groupe de $\mathbb{Z}/12\mathbb{Z}$

$\langle \overline{7} \rangle = \{\overline{0}, \overline{7}, \overline{14}, \overline{21}, \overline{28}, \overline{11}$

$\overline{2}$ $\quad \overline{9}$ $\quad \overline{4}$

$\overline{18}, \overline{13}, \overline{26}, \overline{15}, \overline{10}, \overline{5}\}$

$\overline{6}$ $\quad \overline{1}$ $\quad \overline{8}$ $\quad \overline{3}$

$= \mathbb{Z}/12\mathbb{Z}$

donc $\overline{7}$ engendre $\mathbb{Z}/12\mathbb{Z}$

Th : k engendre $\mathbb{Z}/n\mathbb{Z} \iff k \wedge n = 1$

Preuve : $\Rightarrow$ On suppose $\langle \overline{k} \rangle = \mathbb{Z}/n\mathbb{Z}$

donc $\exists u \in \mathbb{Z}$ tq

$$u\overline{k} = \overline{1}$$

donc $uk \equiv 1 \quad [n]$

ie $\exists v \in \mathbb{Z}$ tq $uk = 1 + nv$

donc $uk - nv = 1$

donc (Bézout) $k \wedge n = 1$

$\Leftarrow$ On suppose k et n premiers entre eux.

$\exists u, v \in \mathbb{Z}$ tq $ku + nv = 1$

donc $\overline{ku} = \overline{1}$

donc $u\overline{k} = \overline{1}$

donc $\overline{1} \in \langle \overline{k} \rangle$

donc $\forall p \in \mathbb{Z} \quad p\overline{1} \in \langle \overline{k} \rangle$

donc $\mathbb{Z}/n\mathbb{Z} \subset \langle \overline{k} \rangle$

4 Groupes monogène et groupes cycliques

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

↑ équivalence

⇐ $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

- $n\mathbb{Z} \subset \mathbb{Z}$
- $0 \in n\mathbb{Z}$
- Si $a, b \in n\mathbb{Z}$ alors $a+b$ est un multiple de n donc $a+b \in n\mathbb{Z}$
- Si $a \in n\mathbb{Z}$, alors $-a \in n\mathbb{Z}$

⇒ Soit H sous-groupe de $\mathbb{Z}$.

Mque $\exists n \in \mathbb{Z}$ t.q. $H = n\mathbb{Z}$

1er cas : Si $H = \{0\}$, $n = 0$ convient.

2e cas : Sinon, $H \neq \{0\}$

donc H contient un entier non nul et son opposé donc $H \cap \mathbb{Z}_+^* \neq \emptyset$

$H \cap \mathbb{Z}_+^*$ est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément, noté n

Thm $H = n\mathbb{Z}$

⊇ $n \in H$ et H stable par + et opposé

donc $n\mathbb{Z} \subset H$

div eucl !

⊆ Soit $a \in H$

On effectue la div eucl. de a par n :

$a = qn + r$ où $0 \leq r < n$

on a $r = a - qn$

$a \in H$, $qn \in H$, donc $r \in H$

Si $r > 0$, $r \in H \cap \mathbb{Z}_+^*$ donc $r \geq n$

par déf de n, contradiction.

Donc $r = 0$

donc $a = qn \in n\mathbb{Z}$

Remarque : preuve à connaître.

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

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

Il est toujours commutatif.

Preuve :

On note $H = \{a^n,\ n \in \mathbb{Z}\}$

On veut montrer que $\langle a \rangle = H$

⊂ $H \ni a$

H est un sous-groupe de G

car $\langle a \rangle$ est le plus petit sous-groupe

contenant a, donc $\langle a \rangle \subset H$

⊃ $a \in \langle a \rangle$

et $\langle a \rangle$ est stable par $*$ et

passage au symétrique, donc

$\forall n \in \mathbb{N}$ $a^n \in \langle a \rangle$ par récurrence

et $\forall n \in \mathbb{Z}$ $a^n \in \langle a \rangle$ par symétrique

donc $H \subset \langle a \rangle$.

Remarque :

En notation additive, dans $(G, +)$,

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

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**.

$(3\mathbb{Z}, +) = \langle 3 \rangle$ sous-groupe de $\mathbb{Z}$ non fini

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.

Preuve : Soit G un groupe monogène, noté multiplicativement

ie $\exists a \in G$ t.q. $G = \langle a \rangle$

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

Notons $\phi_a : \mathbb{Z} \longrightarrow G$

$n \longmapsto a^n$

- ϕ_a est bien à valeur dans G, surjective

(car $\langle a \rangle = a$)

- ϕ_a est un morphisme de groupes

entre $(\mathbb{Z}, +)$ et $(G, \cdot)$

$\phi_a(n+p) = a^{n+p}$

$= a^n \cdot a^p$

$= \phi_a(n) \cdot \phi_a(p)$

On a donc 2 cas :

1er cas ϕ_a est injective, $\ker \phi_a = \{0\}$

alors ϕ_a est bijective, donc G isomorphe

à $\mathbb{Z}$ via ϕ_a et G infini

(le groupe G "se comporte" comme $\mathbb{Z}$)

2e cas ϕ_a n'est pas injective, $\ker \phi_a \neq \{0\}$

car $\ker \phi_a$ est un sous-groupe de $(\mathbb{Z}, +)$

donc $\exists n \in \mathbb{N}^* \setminus \{0\}$ tq $\ker \phi_a = n\mathbb{Z}$.

On définit

$$\varphi_a : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$$
$$\overline{k} \longmapsto a^k$$

Bien définie ?

$\varphi_a(\overline{k}) = \varphi_a(\overline{l})$ lorsque $\overline{k} = \overline{l}$?

Soit $k, l \in \mathbb{Z}$ tq $\overline{k} = \overline{l}$ ie $k \equiv l \ [n]$

$k = l + un$, $u \in \mathbb{Z}$

$$a^k = a^{l+un}$$
$$= a^l \, a^{un}$$
$$= a^l \, \phi_a(un)$$

($\phi_a(un) \in \ker \phi_a = n\mathbb{Z}$)

$$= a^l \, e$$
$$= a^l$$

Donc $\varphi_a(\overline{k})$ ne dépend pas du choix du représentant de $\overline{k}$.

- φ_a morphisme de groupes.

$$\varphi_a(\bar{k}+\bar{l}) = a^{k+l}$$
$$= a^k a^l$$
$$= \varphi_a(\bar{k})\varphi_a(\bar{l})$$

- $\bar{k} \in \operatorname{Ker}\varphi_a \iff \varphi_a(\bar{k}) = e$
$$\iff a^k = e$$
$$\iff k \in \operatorname{Ker}\varphi_a = n\mathbb{Z}$$
$$\iff k \equiv 0 \ [n]$$
$$\iff \bar{k} = \bar{0}$$

donc $\operatorname{Ker}\varphi_a = \{\bar{0}\}$, φ_a injective

- Mq φ_a est surjective

Soit $b \in G = \langle a \rangle$

donc $\exists k \in \mathbb{Z}$ t.q. $b = a^k$

$\varphi_a(\bar{k}) = a^k = b$

donc $b \in \operatorname{Im}\varphi_a$: φ_a surjective

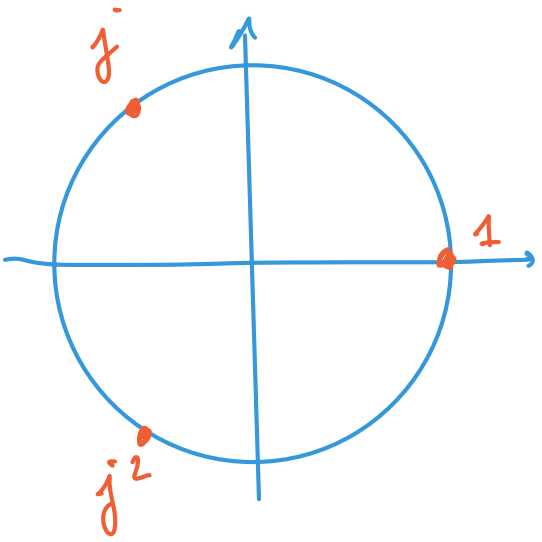
Cl: φ_a réalise un isomorphisme de groupes entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\langle a \rangle, \cdot)$

Bref : G monogène, ie $G = \langle a \rangle$

- infini → isomorphe à $\mathbb{Z}$
- fini de cardinal n → isomorphe à $\mathbb{Z}/n\mathbb{Z}$ (cyclique)

Exemple :

$$U_3 = \{1, j, j^2\}$$



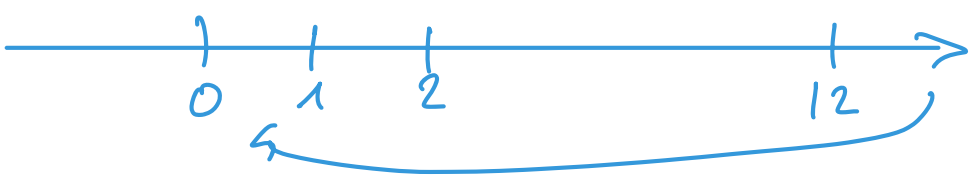
$(U_3, \times)$ groupe

$= \langle j \rangle$

$j^0 = 1 \quad j^1 = j \quad j^2 = j^2 \quad j^3 = 1 \ \ldots$

U_3 isomorphe à $\mathbb{Z}/3\mathbb{Z}$

U_{12}



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 :

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

et :

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

Exemple :

Dans le groupe $(\mathbb{U}, \times)$

on considère l'élément $j \in \mathbb{U}$.

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

$$= \{ 1, j, j^2 \}$$

donc j est d'ordre 3

$$3 = \mathrm{Min}\{ k \geq 1 \cdot \text{ tq } j^k = 1 \}$$

$$\mathrm{ordre}(a) = \mathrm{Card}\,\langle a \rangle$$

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

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

Preuve :

$\Leftarrow$ si $n = kd$

$$a^n = (a^d)^k$$
$$= e^k$$
$$= e$$

$\Rightarrow$ On effectue la div euclidienne de n par d :

$$n = dq + r \quad \text{où} \quad 0 \leq r < d$$

on a $e = a^n$

$$= a^{dq+r}$$
$$= (a^d)^q a^r$$
$$= e^q a^r$$
$$= a^r$$

or $d = \min \{k \geq 1 \text{ tq } a^k = e\}$

donc $r = 0$ ou $r \geq d$

donc $r = 0$, ie $d \mid n$

Théorème.

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

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

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

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