Groupes cycliques

2 notations : notation multiplicative (en général non commutatif)

xy $x*y$ x^{-1}

notation additive (commutatifs)

$x+y$ $-x$

1 Sous-groupe engendré par une partie

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.*

Description du sous-groupe engendré par A. Soit G un groupe noté multiplicativement. $\langle A\rangle$ est l'ensemble des éléments de G qui s'écrivent sous la forme :

$$a_1^{\varepsilon_1}\dots a_n^{\varepsilon_n}$$

où $n\in\mathbb{N}$, $a_1,\dots,a_n\in A$, $\varepsilon_1,\dots,\varepsilon_n=\pm 1$.

Proposition. Les sous-groupes de $\mathbb{Z}$ sont les $a\mathbb{Z}=\langle a\rangle$, où $a\in\mathbb{N}$.

(div euclidienne)

2 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 :

$$\begin{aligned} a \equiv b\ [n] &\iff a - b \in n\mathbb{Z} \\ &\iff n \mid a - b \end{aligned}$$

C'est une relation d'équivalence.

$\Leftrightarrow \exists k \in \mathbb{Z}$ tq $a = b + nk$

Proposition. Pour $n \geqslant 2$, il existe une unique loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$, encore notée $+$, pour laquelle l'application $\pi : k \mapsto \overline{k}$ soit un morphisme de groupes, i.e. :

$$\forall a, b \in \mathbb{Z},\ \overline{a+b} = \overline{a} + \overline{b}$$

De plus, $\operatorname{Ker} \pi = n\mathbb{Z}$.

$\pi : (\mathbb{Z}, +) \longrightarrow \mathbb{Z}/n\mathbb{Z}$ surjective

$k \longmapsto \overline{k}$

Générateurs de $\mathbb{Z}/n\mathbb{Z}$.

Soit n entier $\geqslant 2$. Sont équivalentes :

(*i*) $\mathbb{Z}/n\mathbb{Z} = \langle \overline{a} \rangle$

(*ii*) il existe $k \in \mathbb{N}$ tel que $\overline{ka} = \overline{1}$

(*iii*) $a \wedge n = 1$

Comment définir un morphisme $\mathbb{Z}/n\mathbb{Z} \to G$.

Soit n entier $\geqslant 2$, et $\begin{array}{ccc} \pi : \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ k & \mapsto & \overline{k} \end{array}$.

Si G est un groupe et $f : \mathbb{Z} \to G$ un morphisme de groupes, alors les propriétés suivantes sont équivalentes :

(*i*) il existe un morphisme $g : \mathbb{Z}/n\mathbb{Z} \to G$ tel que $f = g \circ \pi$

(*ii*) $n\mathbb{Z} \subset \operatorname{Ker} f$

Remarque. *Ainsi, pour définir un morphisme de groupe $\mathbb{Z}/n\mathbb{Z} \to G$, on définit un morphisme de groupe $\mathbb{Z} \to G$ dont le noyau contient $n\mathbb{Z}$, et on « passe au quotient ».*

$\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$k \longmapsto \overline{k}$

$f : \mathbb{Z} \longrightarrow G$ morphisme de groupe

$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \xrightarrow{g} G$

Preuve :

$\Rightarrow$ On suppose $\exists g$ morphisme de groupes $\mathbb{Z}/n\mathbb{Z} \to G$

tq $f = g \circ \pi$

Soit $k \in \mathbb{Z}$

$$f(nk) = g(\overline{nk})$$
$$= g(\overline{0})$$
$$= e_G \quad \text{car } g \text{ morphisme de groupe}$$

Donc $nk \in \ker f$

Bref $n\mathbb{Z} \subset \ker f$.

$\Leftarrow$ On suppose $n\mathbb{Z} \subset \ker f$

On définit $g : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$

$$x \longmapsto f(a) \text{ où } \bar{a} = x$$

désigne une classe d'équivalence modulo n

$\exists a \in \mathbb{Z}$ tq $x = \bar{a}$

• Ngpe la déf de $g(x)$ ne dépend pas du choix de a.

Soit $b \in \mathbb{Z}$ tq $\bar{b} = x = \bar{a}$

ie $a \equiv b \ [n]$

ie $\exists k \in \mathbb{Z}$ tq $b = a + kn$

Comme f morphisme de groupes donc

$(G, *)$ $\qquad f(b) = f(a) * f(\xi_m)$

$\xi_m \in n\mathbb{Z} \subset \ker f$ $\qquad = f(a) * e_G$

$\qquad = f(a)$

La valeur donnée à $g(\bar{a})$ est indép du choix des représentant a de $\bar{a}$.

- On a $g \circ \pi = f$ car :

  Pour $a \in \mathbb{Z}$, a est un représentant de $\bar{a}$

  donc $g(\bar{a}) = f(a)$ par déf de g

  $\| \; g(\pi(a))$

- g est morphisme de groupe.

  Soit $x, y \in \mathbb{Z}/n\mathbb{Z}$

  $a, b \in \mathbb{Z}$ tq $\bar{a} = x$ et $\bar{b} = y$

  $g(x+y) = g(\bar{a}+\bar{b})$

  $= g(\overline{a+b})$

  $= f(a+b)$

  $= f(a) * f(b)$ car f morphisme de groupes

  $= g(x) * g(y)$

3 Groupes monogènes et groupes cycliques

Définition.

- Un groupe G est **monogène** s'il existe $x \in G$ tel que $G = \langle x \rangle$. On dit que x est un **générateur** de x.
- Lorsque G est un groupe fini et monogène, on dit que c'est un **groupe cyclique**.

Exemple.

- $(\mathbb{Z}, +)$ est monogène, engendré par 1 (et par -1).
- Tous les sous-groupes de $\mathbb{Z}$ sont monogènes.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est monogène (cyclique). Ses générateurs sont les $\overline{k}$, où k est premier avec n.
- $(\mathbb{U}_n, \times)$ est monogène (cyclique). Ses générateurs sont les $e^{\frac{2ik\pi}{n}}$, où k est premier avec n.

preuve : Rque $\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle \iff k \wedge n = 1$

$\Leftarrow$ On suppose $k \wedge n = 1$

ie $\exists u, v \in \mathbb{Z}$ tq $uk + vn = 1$ (Bézout)

donc $\overline{uk + vn} = \overline{1}$

$\overline{uk} + \overline{vn}$

$\overline{u}\,\overline{k} + \overline{v}\,\overline{n}$

$u\overline{k}$

$\pi(uk + vn) = \pi(1)$

$\pi(uk) + \pi(vn)$

$u\pi(k) + v\pi(n)$

car $u, v \in \mathbb{Z}$, π morphisme

$\Rightarrow$ Soit $x \in \mathbb{Z}/n\mathbb{Z}$ et $a \in \mathbb{Z}$ tq $x = \overline{a}$

$x = \overline{a}$

$= a\,\overline{1}$

$= a\,u\,\overline{k}$

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

$\boxed{\Leftarrow}$ $\overline{1} = u\,\overline{k}$

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

$\langle \overline{1} \rangle = \mathbb{Z}/n\mathbb{Z}$

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

$\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ donc $\exists u \in \mathbb{Z}$ tq $\overline{1} = u\,\overline{k}$

$= \overline{uk}$

donc $\exists v \in \mathbb{Z}$ tq $1 = uk + vn$

Par Bézout, $k \wedge n = 1$

Proposition. Soit $(G,*)$ un groupe et $x \in G$. Alors :

$$\langle x \rangle = \{x^k,\ k \in \mathbb{Z}\}$$

Ainsi $\langle x \rangle = \operatorname{Im} \varphi_x$ où $\varphi_x : \begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & x^k \end{array}$.

Remarque: avec des notations additives $(G,+)$

$$\langle x \rangle = \{kx,\ k \in \mathbb{Z}\}$$
$$= \operatorname{Im} \varphi_x \quad \text{où} \quad \varphi_x : \begin{array}{ccc} \mathbb{Z} & \to & G \\ k & \mapsto & kx \end{array}$$

Théorème.

Tout groupe monogène $\langle x \rangle$ est isomorphe :

- soit à $(\mathbb{Z},+)$, lorsque $\operatorname{Ker} \varphi_x = \{0\}$;
- soit à $(\mathbb{Z}/n\mathbb{Z},+)$, lorsque $\operatorname{Ker} \varphi_x = n\mathbb{Z}$.

Remarque. *Dans le second cas,* $n = \operatorname{Min}\{k \in \mathbb{N}^*,\ x^k = e\}$.

Remarque:

- Tout groupe cyclique est isomorphe à un $\mathbb{Z}/n\mathbb{Z}$
- Il existe des groupes finis non cycliques.

  Par exemple: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ groupe produit fini, non cyclique.

Preuve:

Soit $(G,.)$ un groupe, $x \in G$

On note $\varphi_x : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & x^k \end{array}$

- φ_x est un morphisme de groupes
- $\operatorname{Im} \varphi_x = \langle x \rangle$

donc $\tilde{\varphi}_x : \mathbb{Z} \longrightarrow \langle x \rangle$

$k \longmapsto x^k$

est un morphisme surjectif de groupes.

1er cas : Si $\ker \tilde{\varphi}_x = \{0\}$, alors $\tilde{\varphi}_x$ injective

donc isomorphisme de groupe

Donc $\langle x \rangle$ et $\mathbb{Z}$ sont isomorphes

2e cas : Si $\ker \tilde{\varphi}_x \neq \{0\}$

$\ker \tilde{\varphi}_x$ est un sous-groupe de $\mathbb{Z}$

donc $\exists n \in \mathbb{Z}$ tq $\ker \tilde{\varphi}_x = n\mathbb{Z}$

(on a $n = \min \{k \in \mathbb{N}^* \text{ tq } x^k = e\}$)

On peut définir

$g : \mathbb{Z}/n\mathbb{Z} \longrightarrow \langle x \rangle$

$\overline{k} \longmapsto \varphi_x(k)$

C'est un morphisme de groupes,

surjectif car $\tilde{\varphi}_x$ l'est

injectif car $\varphi_x(k) = e$

$\Leftrightarrow k \in \ker \varphi_x = n\mathbb{Z}$

$\Leftrightarrow \overline{k} = \overline{0}$

Ainsi : $\langle x \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Remarque : Dans ce second cas, $\mathrm{Card}\ \langle x \rangle = n$

4 Ordre d'un élément dans un groupe

Définition. Soit $(G, *)$ un groupe dont le neutre est noté e, et $x \in G$. Lorsque $\langle x \rangle$ est fini, on dit que x **est d'ordre fini** et on note :

$$\text{ord}(x) = \text{Min}\{n \in \mathbb{N}^*,\ x^n = e\}$$

l'**ordre** de x.

Remarque.

- $\text{ord}(x) = n \iff \text{Ker}\,\varphi_x = n\mathbb{Z}$
- *Si $\langle x \rangle$ est infini, on convient parfois que x est d'ordre infini.*

Exemple. Quel est l'ordre de $\overline{1}$ (resp. de $\overline{12}$) dans $\mathbb{Z}/42\mathbb{Z}$?

muni de +, neutre est $\overline{0}$

- $\forall n \in \mathbb{N}^*$ $\quad n\overline{1} = \overline{n}$

  donc $n\overline{1} = \overline{0} \iff n \in 42\mathbb{Z}$

  donc $\text{ord}(\overline{1}) = 42$

- $42 = 2 \times 3 \times 7$ $\qquad 12 = 2 \times 2 \times 3$

  $12 \times 7 = 2 \times 42$ donc $7 \cdot \overline{12} = \overline{0}$

  et $\forall k \in [\![1, 6]\!]$, $k \times 12$ pas un multiple de 42

  $[\![\ldots)$

$$\text{ord}(\overline{12}) = 7$$

Proposition. Avec les notations précédentes, lorsque x est d'ordre fini n, on a :

$$x^k = e \iff n \mid k$$

preuve : $\text{ord}(x) = n \iff \ker \varphi_x = n\mathbb{Z}$

$x^k = e \iff k \in \ker \varphi_x$

$\iff k \in n\mathbb{Z}$

Théorème.

Avec les notations précédentes,

$$\text{ord}(x) = \text{Card}\left(\langle x \rangle\right)$$

Corollaire. Si G est un groupe fini, alors tout $x \in G$ est d'ordre fini.

preuve : On suppose x d'ordre fini

$\langle x \rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

où $n = \min\{k \in \mathbb{N}^* \mid x^k = e\}$

$= \text{ord}(x)$

Donc $\text{Card}\langle x \rangle = n$

$= \text{ord}(x)$

Théorème.

Soit G un groupe fini, et $x \in G$. Alors :

$$\mathrm{ord}(x) \mid \mathrm{Card}(G)$$

c'est-à-dire que $x^{\mathrm{Card}\, G} = e$.

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

Preuve :

1er cas : $(G, \cdot)$ est un groupe commutatif de cardinal n.

On note $G = \{g_1, \dots, g_n\}$ avec $g_n = e$

Soit $x \in G$. Mque $x^n = e$

Définissons $\sigma : G \longrightarrow G$, $t \longmapsto xt$

c'est une permutation de G ie bijection $G \to G$.

de réciproque $t \longmapsto x^{-1}t$

On écrit :

$$g_1 \cdots g_n = \prod_{i=1}^{n} g_i$$

car . commutative

$$= \prod_{g \in G} g$$

car $\sigma \in \mathfrak{S}(G)$

$$= \prod_{g \in G} \sigma(g)$$

$$= \prod_{g \in G} xg$$

$$= x^n \prod_{g \in G} g \quad \text{(commutatif)}$$

Donc, en composant à droite par $\left(\prod_{g \in G} g\right)^{-1}$

$$e = x^n$$

Cas général :

Soit $(G, \cdot)$ un groupe quelconque, de cardinal n.

$x \in G$ Rq $x^n = e$

Pour $a, b \in G$, on note

$$a \mathcal{R} b \iff a^{-1} b \in \langle x \rangle$$

- C'est une relation d'équivalence

réflexive : $a^{-1} a = e \in \langle x \rangle$

donc $a \mathcal{R} a$

symétrique : Si $a \mathcal{R} b$, $a^{-1} b \in \langle x \rangle$

donc $(a^{-1} b)^{-1} \in \langle x \rangle$ ↑ stable par inverse

$\| \quad b^{-1} a$

donc $b \mathcal{R} a$

transitive Si $a \mathcal{R} b$ et $b \mathcal{R} c$

alors $a^{-1} b \in \langle x \rangle$ et $b^{-1} c \in \langle x \rangle$

donc $a^{-1}b\ b^{-1}c \in \langle x \rangle$

$= a^{-1}c$ ↑ stable par .

ie $a \mathcal{R} c$

Pour $a \in G$,

$$\overline{a} = \{ b \in G \text{ tq } a^{-1}b \in \langle x \rangle \}$$

$$= \{ b \in G \text{ tq } \exists k \in \mathbb{Z} \quad a^{-1}b = x^k \}$$

$$= \{ ax^k, \ k \in \mathbb{Z} \}$$

avec x d'ordre fini d

$$= \{ a, ax, ax^2, \dots, ax^{d-1} \}$$

↑ c'est la classe d'équivalence de a

elle est de cardinal d.

$\mathcal{R}$ est une relation d'équivalence, donc

$$G = \bigcup_{\text{disjoints}} \text{classes d'équivalence}$$

$$= \bigcup_{\substack{i=1 \\ \text{disjoints}}}^{p} \text{classe d'équivalence d'un } a_i$$

$$= \bigcup_{\substack{i=1 \\ \text{disjoints}}}^{p} \overline{a_i}$$

donc $\text{Card } G = \sum_{i=1}^{p} \text{Card}(\overline{a_i})$

$$= \sum_{i=1}^{p} \mathrm{ord}(x)$$

$$= p \cdot \mathrm{ord}(x)$$

Donc $\mathrm{ord}(x) \mid \mathrm{Card}\, G$.

Remarque : Cette preuve s'adapte facilement pour montrer que :

Si H sous-groupe de G groupe fini, alors $\mathrm{Card}\, H \mid \mathrm{Card}\, G$.

111.1