Cours Algèbre I

S1

Chapitre V Groupes

Mr Bouhamza

Chapitre V — Groupes

I] Notions sur les groupes :

Définition :

* On appelle groupe tout ensemble G muni d'une loi de composition interne T tel que :
  - i) T associative
  - ii) T admet un élément neutre e.
  - iii) Tout élément de G est inversible pour T.

* Si de plus, T est commutative le groupe (G,T) est dit commutatif ou **abélien**. (Abel)

Exemples :

i) $(\mathbb{Z},+)$; $(\mathbb{Q},+)$; $(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes abéliens.

ii) $(\mathbb{Q}^*,\times)$; $(\mathbb{R}^*,\times)$ et $(\mathbb{C}^*,\times)$ sont des groupes abéliens.

iii) Soit $n\in\mathbb{N}$, $n\geqslant 3$, $(S_n,\circ)$ est un groupe non commutatif. (Galois) suède

Théorème 1 :

Soit (G,T) un groupe

Alors tout élément de G est régulier (ou simplifiable)

$(\forall a\in G / aTx = aTy \Rightarrow x=y)$

II] Sous-groupes :

Définition : Soit (G,T) un groupe et $H\subset G$

On dit que H est un sous-groupe de (G,T) si :

i) $H\neq\emptyset$

ii) H est stable pour T

iii) $\forall x\in H,\ x^{-1}\in H$

Exemples : xi) Soit (G,T) un groupe, alors G et $\{e\}$ sont des sous-groupes de (G,T) qu'on appelle les sous-groupes triviaux de (G,T)

iii) $(\mathbb{Z}, +)$ groupe, et soit $n \in \mathbb{N}$ et $H = n\mathbb{Z} = \{nk / k \in \mathbb{Z}\}$
H est un sous-groupe de $(\mathbb{Z}, +)$

Remarque ①: Soit H un sous groupe du groupe (G, T), alors: $e \in H$

Démonstration:

* Comme $H \neq \emptyset$, il existe $x \in H$
* On a aussi $x^{-1} \in H$
* Stabilité $\Rightarrow x T x^{-1} \in H \Rightarrow e \in H$

Remarque ②:
Soit (G, T) un groupe d'élément neutre e et soit $\mathcal{H}$ l'ensemble des groupes (G, T)
$\{e\}$ est le plus petit élément de $\mathcal{H}$ ordonné par $\subset$.

Théorème ②:

Soit (G, T) un groupe et $H \subset G$, alors H est un sous groupe de (G, T) ssi : ① $H \neq \emptyset$

② $\forall (x, y) \in H$, $x T y^{-1} \in H$

Démonstration:

Supposons H sous groupe de (G, T) et montrons qu'on a ②
Soit $(x, y) \in H$, d'après iii) on a $y^{-1} \in H$
On a alors $x, y^{-1} \in H$, d'où d'après ii) $x T y^{-1} \in H$
Réciproquement, supposons ① et ② vérifiées et montrons que H est un sous-groupe de (G, T)
Comme $H \neq \emptyset$, soit $x \in H$, on a alors d'après ②: $x T x^{-1} \in H$
c'est à dire $e \in H$
Soit $x \in H$ alors on a d'après ②: $e T x^{-1} \in H \Rightarrow x^{-1} \in H$
ce qui montre iii)

Soit $x, y \in H$

Comme $y^{-1} \in H$ on a d'après ② , $x T (y^{-1})^{-1} \in H$

$\Rightarrow x T y \in H$

Théorème ③ :

Soit (G, T) un groupe et $(H_i)_{i \in I}$ une famille de sous-groupe de (G, T) . Alors $H = \bigcap_{i \in I} H_i$ est un sous-groupe de (G, T).

Corollaire:

Soit (G, T) un sous-groupe et S une partie de G.
Alors l'intersection de tous les sous-groupes de (G, T) contenant S est un sous-groupe de (G, T) contenant S.

Définition:

Soit (G, T) un sous groupe et S une partie de G.
On appelle sous-groupe de (G, T) engendré par S, et on note : $\langle S \rangle$ ou $gr(S)$, l'intersection de tous les sous-groupes de (G, T) contenant S.

Exemples:

i) Soit (G, T) un groupe

$\langle \emptyset \rangle = \{e\}$

Soit H un sous-groupe de (G, T)

$\langle H \rangle = H$

ii) $(\mathbb{Z}, +)$ groupe , $n \in \mathbb{Z}$

$\langle \{n\} \rangle \subset n\mathbb{Z}$

Définition:

Soit (G,T) un groupe et $a \in G$

On appelle sous-groupe de (G,T) engendré par a et on note $\langle a \rangle$ ou $gr(a)$ le sous-groupe de (G,T) engendré par $\{a\}$

Exemples:

i) Dans $(\mathbb{Z}, +)$, $\langle n \rangle = n\mathbb{Z}$

ii) Soit (G,T) un groupe et $a \in G$

$$\langle a \rangle = \{ a^k / k \in \mathbb{Z} \}$$

$$\langle e \rangle = \{e\}$$

III] Groupes monogènes:

Définition:

Soit (G,T) un groupe et H un sous-groupe de (G,T)

On dit que H est monogène s'il existe un élément a de G tel que: $H = \langle a \rangle = \{ a^k / k \in \mathbb{Z} \}$

Exemple:

$(\mathbb{Z}, +)$ groupe commutatif

$\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}$ est donc monogène.

Soit H sous-groupe de $(\mathbb{Z}, +)$

* Si $H = \{0\}$ on a $H = \langle 0 \rangle$, donc H est monogène.
* Si $H \neq \{0\}$, soit x le plus petit élément strictement positif de H.

Alors on a : $\langle n \rangle \subset H$

Soit $x \in H$

En effectuant la division euclidienne de x par n on obtient.

$x = nk + r$ avec $0 \leq r < n$

comme $x \in H$ et $nk \in H$

On a : $x - nk \in H$

On en déduit que $r \in H$ et par suite $r = 0$ car n est le plus petit élément positif strictement de H

Donc : $x = nk$

et par conséquent $x \in \langle n \rangle$, ce qui montre que $H \subset \langle n \rangle$

et par suite $H = \langle n \rangle$.

Remarque :

Soit (G, T) un groupe et H un sous-groupe monogène de (G, T)

Si a est un générateur de H alors a^{-1} est aussi un générateur de H.

Théorème (4) :

Soit (G, T) un groupe monogène, alors tout sous-groupe de (G, T) est monogène.

Démonstration :

Soit a un générateur de G et soit H un sous-groupe de G.

$\forall x \in H, \exists k \in \mathbb{Z}$, $x = a^k$

tout d'abord si $H = \{e\}$, H est monogène.

si $H \neq \{e\}$, $\exists x \in H$ et $x \neq e$

$\Rightarrow \exists k \in \mathbb{N}^*$, $x = a^k$

$A = \{k \in \mathbb{N}^* / a^k \in H\}$

A est une partie non vide de $\mathbb{N}^*$

Soit n le plus petit élément de A

On a : $a^n \in H$

Montrons que : $H = \langle a^n \rangle$

Pour cela, il nous reste à montrer que $H \subset \langle a^n \rangle$

Soit $x \in H$, $x = a^k$, $k \in \mathbb{Z}$

$k = nq + r$, $0 \leq r < n$

on a : $a^r = a^{k-nq} \in H$

Donc : $x = a^k = a^{nq} = (a^n)^q$

$\Rightarrow x \in \langle a^n \rangle$

$\Rightarrow H \subset \langle a^n \rangle$

Remarque:

Soit (G,T) un groupe et $a \in G$

Alors $\langle a \rangle$ est le plus petit sous-groupe de (G,T) contenant a.

Pour tout sous-groupe H de (G,T) tel que $a \in H$, on a $\langle a \rangle \subset H$

Remarque :

Soit (G,T) un groupe monogène engendré par a

. Alors (G,T) est abélien.

Démonstration :

Soit $(x,y) \in G$

Comme G est engendré par a, il existe m et n dans $\mathbb{Z}$

tels que : $x = a^m$ et $y = a^n$

On a alors : $xTy = a^m T a^n = a^{m+n}$

$= a^{n+m}$

$= a^n T a^m$

$= yTx$

Ce qui montre que T est commutative

IV] Groupes quotients:

Soit (G,T) un groupe commutatif et H un sous-groupe de (G,T)

On définit dans G une relation binaire $\mathcal{R}$ par : $x \mathcal{R} y \Leftrightarrow xTy^{-1} \in H$

i) Soit $x \in G$

On a $xTx^{-1} = e \in H \Rightarrow x \mathcal{R} x$, $\mathcal{R}$ est donc réflexive.

ii) Soit $(x,y) \in G$ tels que : $x \mathcal{R} y$ on a : $x T y^{-1} \in H$

Comme H est un sous groupe, on a $(xTy^{-1})^{-1} \in H$

or : $(xTy^{-1})^{-1} = (y^{-1})^{-1} T x^{-1} = yTx^{-1}$

D'où $y \mathcal{R} x$ et $\mathcal{R}$ est donc symétrique

iii) Soit $x,y,z \in G$ tel que $x \mathcal{R} y$ et $y \mathcal{R} z$

on a : $xTy^{-1} \in H$ et $yTz^{-1} \in H$

$\Rightarrow (xTy^{-1}) T (yTz^{-1}) \in H$

$\Rightarrow x T (y^{-1} T y) T z^{-1} \in H$

$\Rightarrow x T e T z^{-1} \in H$

$\Rightarrow x T z^{-1} \in H$

$\Rightarrow x \mathcal{R} z$

Alors $\mathcal{R}$ est transitive

. $\mathcal{R}$ est donc une relation d'équivalence dans G.

L'ensemble quotient $G/\mathcal{R}$ de G par $\mathcal{R}$ se note G/H

Pour tout élément x de G, sa classe d'équivalence modulo $\mathcal{R}$

$\overline{x}$ s'appelle la classe d'équivalence de x modulo H.

$\overline{x} = \{ y \in G / x \mathcal{R} y \}$

$= \{ y \in G / y \mathcal{R} x \}$

$= \{ y \in G / yTx^{-1} \in H \}$

$= \{ y \in G / \exists k \in H, yTx^{-1} = k \}$

$= \{ y \in G / \exists k \in H, y = kTx \}$

$= \{ xTk / k \in H \}$

$= HTx$

On définit dans G/H une loi de composition interne $\overline{T}$ par : $\overline{x} \,\overline{T}\, \overline{y} = \overline{xTy}$

Théorème ⑤ :

$(G/H, \overline{T})$ est un groupe commutatif (qu'on appelle le groupe quotient de G par H).

Remarque :

Dans toute la suite $\overline{T}$ sera notée T

Théorème ⑥ :

Soit (G,T) un groupe commutatif et H un sous-groupe de (G,T)

Si G est monogène engendré par a alors G/H est monogène engendré par $\overline{a}$.

Remarque :

(G,T) groupe commutatif, H un sous-groupe de G.

Soit $x \in G$ et soit : $f : xTH \longrightarrow H$

$xTh \longmapsto h$

f est bijective.

Si H est fini à n éléments, alors $\forall x \in G$ xTH est fini à n éléments.

Toutes les classes d'équivalence modulo H ont le même nombre d'éléments qui est celui de H.

Démonstration :

Soit a un générateur de G.

Soit H un sous-groupe de (G,T) et soit $X \in G/H$. Il existe alors $x \in G$ tel que $X = \overline{x}$ comme $\langle a \rangle = G$ et existe alors $n \in \mathbb{Z}$ tel que $x = a^n$

d'où : $\overline{x} = \overline{a^n} = \overline{a}^n \Rightarrow X = \overline{a}^n \Rightarrow G/H = \langle \overline{a} \rangle$

V] Ordre d'un groupe :

Définition :

Soit (G,T) un groupe et H un sous-groupe de (G,T)

Si H est fini, on appelle ordre de H et on note $o(H)$ ou $|H|$ le nombre de ses éléments.

Exemples:

i) Soit $n \in \mathbb{N}^*$; $o(\mathbb{Z}/n\mathbb{Z}) = n$

ii) Soit $n \in \mathbb{N}^*$; $o(S_n) = n!$

Soit τ une transposition de S_n

$\tau^2 = e$

$\langle \tau \rangle = \{e, \tau\}$

$o(\langle \tau \rangle) = 2$.

Théorème (7):

Soit (G, T) un groupe fini d'ordre n.

Alors l'ordre de tout sous-groupe de (G, T) divise l'ordre de G: $o(H) \mid o(G)$

Démonstration:

Soit H un sous-groupe de (G, T)

G/H est une partition de G

Comme G est fini, G/H est fini

Posons: $G/H = \{X_1, X_2, \ldots, X_p\}$

$o(G/H) = p$

on a: $G = X_1 \cup X_2 \cup X_3 \cup \ldots \cup X_p$

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

$= p \, \text{card}(H)$

$o(G) = p \, o(H)$

$o(G) = o(G/H) \cdot o(H)$

$o(G/H) = \dfrac{o(G)}{o(H)}$

Exemple :

i) Soit $n \in \mathbb{N}^*$ et soit τ_{ij} une transposition de S_n

$\langle \tau_{ij} \rangle = \{e, \tau_{ij}\} \Rightarrow o(\tau_{ij}) = 2$

ii) Soit (G,T) un groupe fini tel que $o(G) = p$ où p est un nombre premier.

Soit H un sous-groupe de (G,T) alors et d'après Lagrange, on a $o(H)/p$, comme p est premier, on a : $o(H) = 1$ où $o(H) = p$

. Si : $o(H) = 1$ alors : $H = \{e\}$

et Si $o(H) = p$ alors : $H = G$

. Si $a \in G$, $a \neq e$

on a : $o(\langle a \rangle) = p$ et par suite : $\langle a \rangle = G$

$\Rightarrow$ G est monogène

Théorème ⑧ :

Soit (G,T) un groupe fini d'ordre de $\langle a \rangle$ est le plus petit entier naturel non nul k tel que : $a^k = e$

Démonstration :

On a : $\langle a \rangle = \{a^i / i \in \mathbb{Z}\}$

Comme G est fini : $\langle a \rangle$ est fini

Autrement dit les a^i ne sont pas deux à deux distincts, il existe alors $i \neq j$ tel que $a^i = a^j$

Il en résulte alors que : $a^{i-j} = a^{j-i} = e$

et par suite : $A = \{i \in \mathbb{N}^* / a^i = e\}$ est non vide.

Soit k le plus petit élément de A

Soit $H = \{a^0 = e, a, a^2, \ldots, a^{k-1}\}$

On a : $H \subset \langle a \rangle$

Soit $x \in \langle a \rangle$, il existe alors $i \in \mathbb{Z}$ tel que : $x = a^i$

* Trois cas sont possible pour i :

1er cas : $0 \leq i \leq k-1$

$\Rightarrow x = a^i \in H$

2ème cas : $i \geq k$

en divisant i par k, on a :

$i = kq + r$ avec $0 \leq r \leq k-1$

$x = a^i = a^{kq+r} = a^{kq} \top a^r$

$= (a^k)^q \top a^r$

$= a^q \top a^r$

$= e \top a^r$

$= a^r \in H$

3ème cas : $i < 0$

on pose $i = -j$ $(j > 0)$

on a : $x = a^i = a^{-j} = (a^{-1})^j$

or comme : $a^k = e$

on a : $a^{k-1} \top a = e$

on en déduit que $a^{(k-1)j} \in H$

Ainsi les trois cas, $x \in H$ ce qui montre que $\langle a \rangle \subset H$

et par suite : $\langle a \rangle = H = \{e, a, \ldots, a^{k-1}\}$

Définition :

Soit $(G, \top)$ un groupe fini et soit $a \in G$, on appelle ordre de a et on note $o\langle a \rangle$ l'ordre de $\langle a \rangle$.

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

Remarque :

Soit $(G, \top)$ un groupe fini et $a \in G$, alors $o(a) / o(G)$

Remarque :

Soit (G, T) un groupe fini d'ordre n

Alors : i) $\forall x \in G,\ x^n = e$

ii) Soit $a \in G$, $o(a) = k$

$t \in \mathbb{Z}$, $a^t = e \Leftrightarrow k/t$

Exemple :

On a $S_3 = \{e, \tau_{12}, \tau_{13}, \tau_{23}, \sigma, \varphi\}$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{et} \quad \varphi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$o(e) = 1$

$o(\tau_{12}) = o(\tau_{13}) = o(\tau_{23}) = 2$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e \Rightarrow o(\sigma) = 3$$

$\langle \sigma \rangle = \{e, \sigma, \sigma^2\}$

$$\varphi^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\varphi^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

$o(\varphi) = 3$

$\langle \varphi \rangle = \{e, \varphi, \varphi^2\}$

$\forall f \in S_3$ on a : $\langle f \rangle \neq S_3$

$\Rightarrow S_n$ n'est pas monogène.

Exercice :

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

Calculer : σ^2, σ^3, σ^4.

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

$$\sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e$$

$o(\sigma) = 4$

$\langle \sigma \rangle = \{e, \sigma, \sigma^2, \sigma^3\}$

VII] Groupes cycliques:

Définition:

On appelle groupe cyclique tout groupe monogène fini.

Exemples:

i) Soit (G,T) un groupe fini d'ordre p où q est premier.
(G,T) est cyclique.

ii) $\forall n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique d'ordre n.

Remarque:

Soit (G,T) un groupe cyclique

Alors: i) (G,T) est commutatif

ii) Tout sous-groupe de (G,T) est cyclique.

iii) Tout groupe quotient de (G,T) est cyclique.

Exercice:

Soit p un nombre premier, montrer que pour tout $x \in \mathbb{Z}$ on a : $p \mid x^p - x$

On a $(\mathbb{Z}/p\mathbb{Z}, +)$ est un groupe cyclique d'ordre p

Soit $x \in \mathbb{Z}$

- Si : $\bar{x} = \bar{0}$ on a : $p \mid x$
- Si : $\bar{x} \neq \bar{0}$ on a alors $\langle \bar{x} \rangle = \mathbb{Z}/p\mathbb{Z}$

et $o(\bar{x}) = p \Rightarrow p\bar{x}^p = \bar{0}$

$\Rightarrow p\bar{x} = \bar{0}$

$\Rightarrow p \mid x^p$

VIII Homomorphisme de groupes:

Définition:

Soit (E,T) et $(F,*)$ deux groupes

On appelle homomorphisme de groupes de (E,T) dans $(F,*)$ toute application $u : E \longrightarrow F$ telle que : $u(xTy) = u(x) * u(y)$, $\forall x,y \in E$

si de plus u est bijective

On dit que u est un isomorphisme de groupes.

Exemples:

i) Soit (G,T) un groupe et $a \in G$

$u : \mathbb{Z} \longrightarrow G$

$n \longmapsto a^n$

est un homomorphisme de groupes de $(\mathbb{Z},+)$ dans (G,T)

ii) Soit (G,T) un groupe cyclique d'ordre n engendré par a.

$G = \{e, a, a^2, \ldots, a^{n-1}\}$

$u : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$

$\bar{k} \longmapsto a^k$

u est un homomorphisme de groupes de $(\mathbb{Z}/n\mathbb{Z},+)$ dans (G,T)

De plus u est bijective

Donc u est un isomorphisme de groupes.

Définition :

Soit (E,T) et $(F,*)$ deux groupes.

On dit que ces deux groupes sont isomorphes et on écrit $(E,T) \simeq (F,*)$ s'il existe un isomorphisme de groupes de (E,T) dans $(F,*)$ ou de $(F,*)$ dans (E,T).

Exemples :

i) Soit (E,T) et $(F,*)$ deux groupes cycliques de même ordre n engendrés respectivement par a et b.

$E = \{e, a, a^2, \ldots\ldots, a^{n-1}\}$

$F = \{f, b, b^2, \ldots\ldots, b^{n-1}\}$

$$U : E \longrightarrow F$$

(E,T) est isomorphe à $(F,*)$

$(E,T) \simeq (F,*)$

ii) Soit (G,T) un groupe monogène infini engendré par a

$$U : \mathbb{Z} \longrightarrow G$$
$$i \longmapsto a^i$$

U est un homorphisme de groupes.

U est surjective ①

Soit i et j deux éléments de $\mathbb{Z}$ tels que :

$U(i) = U(j)$

$a^i = a^j \Rightarrow a^{i-j} = e$

. Si $i \neq j$ $(i - j \neq 0)$

a serait d'ordre fini ce qui n'est pas

Car : $G = \langle a \rangle$ est infini

Donc : $i = j$ et u est injective (2)

$u : E \longrightarrow F$

$a^i \longrightarrow b^i$

$(E, T) \simeq (F, *)$

$G = \langle a \rangle \simeq \mathbb{Z}$

G est fini ou infini

$\downarrow$

$n = o(G)$

Remarque :

Soit u un homomorphisme de groupe (E, T) dans $(F, *)$

e l'élément neutre de E

f l'élément neutre de F

alors on a : i) $u(e) = f$

ii) $\forall x \in E$, $U(x^{-1}) = U(x)^{-1}$

Définition :

Soit (G, T) un groupe

i) On appelle homomorphisme de (G, T) tout homomorphisme de groupes de (G, T) dans (G, T)

ii) On appelle automorphisme de (G, T) tout isomorphisme de groupes de (G, T) dans (G, T).

Théorème (9) :

Soit u un homomorphisme de groupes de (E, T) dans $(F, *)$

Alors : i) Pour tout sous-groupe de (E, T)

$u(H)$ est un sous-groupe de $(F, *)$

ii) Pour tout sous-groupe K de $(F, *)$

$U^{-1}(K)$ est un sous-groupe de (E, T)

Démonstration :

Du ii) : Soit K un sous-groupe de $(F, *)$

$H = U^{-1}(K) = \{x \in E / U(x) \in K\}$

* on a : $f \in K$ et $U(e) = f \Rightarrow e \in H \Rightarrow H \neq \emptyset$

* soit $x, y \in H$

on a : $U(x T y^{-1}) = U(x) * U(y^{-1})$

$= U(x) * U(y)^{-1}$

Comme K est un sous-groupe $U(x) \in K$ et $U(y) \in K$

On a $U(x) * U(y)^{-1} \in K$

donc $U(x T y^{-1}) \in K$

$\Rightarrow x T y^{-1} \in H$

donc $U^{-1}(K) = H$ est bien un sous-groupe de (E, T)

Définition :

Soit u un homomorphisme de groupes de (E, T) dans $(F, *)$

e = l'élément neutre de (E, T)

f = l'élément neutre de $(F, *)$

On appelle noyau de u et on note K_{er} u l'ensemble $\{x \in E / U(x) \in \{f\}\}$.

Remarque :

$K_{er}\ u = U^{-1}(\{f\})$

$\Rightarrow K_{er}$ u est un sous-groupe de (E, T)

Exemple :

Soit (G, T) un groupe cyclique d'ordre n engendré par a

$U : \mathbb{Z} \longrightarrow G$

$i \longrightarrow a^i$

$$\begin{aligned}\text{Ker } u &= \{ i \in \mathbb{Z} \ / \ u(i) = e \} \\ &= \{ i \in \mathbb{Z} \ / \ a^i = e \} \\ &= n\mathbb{Z}\end{aligned}$$

Théorème (10):

Soit u un homomorphisme de groupes de (E, T) dans $(F, *)$, alors :

u est injective $\iff$ $\text{Ker } u = \{e\}$