Morphismes de groupes

Définition

Soit $(G_1, \star)$ et $(G_2, \cdot)$ deux groupes et $\psi : G_1 \longrightarrow G_2$ une application.

1. On dit que ψ est un **homomorphisme** si ψ vérifie les propriétés suivantes :

$$\forall (x, y) \in G_1^2 \ , \quad \psi(x \star y) = \psi(x) \cdot \psi(y)$$

2. On dit que ψ est un **isomorphisme** si ψ est un homomorphisme bijectif. Dans ce cas, on dit que les deux groupes $(G_1, \star)$ et $(G_2, \cdot)$ sont isomorphes.
3. Un **automorphisme** de groupe est un isomorphisme d'un groupe sur lui même.

Proposition

Soit $(G_1, \star)$ et $(G_2, \cdot)$ deux groupes et $\psi : G_1 \longrightarrow G_2$ un homomorphisme. Notons e_1, e_2 les éléments neutres de G_1 et G_2 respectivement. Nous avons :

1. $\psi(e_1) = e_2$.
2. $\forall x \in G_1, \quad \psi(x^{-1}) = (\psi(x))^{-1}$.

Démonstration : On a :

$$\psi(e_1) = \psi(e_1 \star e_1) = \psi(e_1)\psi(e_1).$$

En composant avec l'inverse de $\psi(e_1)$ on obtient :

$$e_2 = (\psi(e_1))^{-1} \psi(e_1) = \psi(e_1).$$

De plus, pour tout $x \in G_1$ on a

$$\psi(x) \cdot \psi(x^{-1}) = \psi(x \star x^{-1}) = \psi(e_1) = e_2.$$

Remarque

1. La composée de deux homomorphismes de groupe est un homomorphisme de groupe.
2. Le réciproque d'un isomorphisme de groupe est un isomorphisme de groupe.

Exemple

L'application

$$\begin{array}{rcl} \exp : (\mathbb{R}, +) & \longrightarrow & (\mathbb{R}_+^*, \cdot) \\ x & \longmapsto & \exp(x) = e^x \end{array}$$

est un isomorphisme de groupe. Sa réciproque est

$$\begin{array}{rcl} \ln : (\mathbb{R}_+^*, \cdot) & \longrightarrow & (\mathbb{R}, +) \\ x & \longmapsto & \ln(x). \end{array}$$

Exemple

On rappelle que $\mathcal{G} = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \ / \ a \in \mathbb{R} \right\}$ est un groupe pour la multiplication des matrices. L'application

$$\begin{array}{rcl} \psi : (\mathbb{R}, +) & \longrightarrow & (\mathcal{G}, \cdot) \\ a & \longmapsto & \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \end{array}$$

est un isomorphisme de groupe.

Exercice

1. Montrer que l'ensemble
$$\mathcal{R} = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \ / \ \theta \in \mathbb{R} \right\}$$
est un groupe pour la multiplication des matrices. Est-il commutatif ? Montrer que l'application
$$\begin{array}{rcl} \psi : (\mathbb{R}, +) & \longrightarrow & (\mathcal{G}, \cdot) \\ \theta & \longmapsto & \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \end{array}$$
est un homomorphisme de groupe.
2. De même, montrer que l'application
$$\begin{array}{rcl} f : (\mathbb{R}, +) & \longrightarrow & (\mathbb{U}, \cdot) \\ t & \longmapsto & e^{it} \end{array}$$
est un homomorphisme de groupe.

Exemples

1. Soit $(G, \star)$ un groupe et $g \in G$. L'application
$$\begin{array}{rcl} \psi_g : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$$
est un homomorphisme de groupe.
2. Soit $(G, \star)$ un groupe **commutatif** et $n \in \mathbb{Z}$. L'application
$$\begin{array}{rcl} \psi_n : G & \longrightarrow & G \\ g & \longmapsto & g^n \end{array}$$
qui est un homomorphisme de groupe.

Exercice

Soit $(G, \star)$ un groupe tel que l'application

$$\begin{array}{rcl} \psi : G & \longrightarrow & G \\ g & \longmapsto & g^2 \end{array}$$

qui est un homomorphisme de groupe. Montrer que G est commutatif.

Définition

Soit $(G_1, \star)$ et $(G_2, \cdot)$ deux groupes et $\psi : G_1 \longrightarrow G_2$ un homomorphisme de groupe.

1. On définit le noyau de ψ par $\ker(\psi) := \psi^{-1}(\{e_2\}) = \{x \in G_1 \ / \ \psi(x) = e_2\}$.
2. On définit l'image de ψ par $\mathrm{Im}(\psi) := \psi(G_1) = \{\psi(x) \ / \ x \in G_1\}$.

L'importance de cette notion vient de la proposition suivante :

Proposition

Soit $(G_1, \star)$ et $(G_2, \cdot)$ deux groupes et $\psi : G_1 \longrightarrow G_2$ un homomorphisme de groupe.

1. $\ker(\psi)$ *est un sous groupe de G_1 et $Im(\psi)$ est un sous groupe de G_2.*
2. *ψ est surjectif si, et seulement si, $Im(\psi) = G_2$.*
3. *ψ est injectif si, et seulement si,* $\ker(\psi) = \{e_1\}$.

Démonstration (i) Par définition du noyau, $e_1 \in \ker(\psi)$. De plus, si $x, y \in \ker(\psi)$ alors

$$\begin{array}{rcl} \psi(x \star y^{-1}) & = & \psi(x) \cdot \psi(y^{-1}) \\ & = & \psi(x) \cdot (\psi(y))^{-1} \\ & = & e_2 \cdot e_2 = e_2, \end{array}$$

et $x \star y^{-1} \in \ker(\psi)$. Finalement, $\ker(\psi)$ est un sous groupe de G_1.
De même, $e_2 = \psi(e_1) \in \mathrm{Im}(\psi)$. De plus, si $y_1 = \psi(x_1), y_2 = \psi(x_2) \in \mathrm{Im}(\psi)$ alors

$$\begin{array}{rcl} y_1 \cdot {y_2}^{-1} & = & \psi(x_1) \cdot (\psi(x_2))^{-1} \\ & = & \psi(x_1) \cdot \psi(x_2^{-1}) \\ & = & \psi(x_1 \star {x_2}^{-1}) \in \mathrm{Im}(\psi). \end{array}$$

Ainsi $\mathrm{Im}(\psi)$ est un sous groupe de G_2.

(ii) Maintenant supposons que ψ est injectif. Si $x \in \ker(\psi)$ alors

$$\psi(x) = e_2 = \psi(e_1)$$

et donc $x = e_1$. Donc $\ker(\psi) \subset \{e_1\}$. Finalement, comme $e_1 \in \ker(\psi)$, on déduit que $\ker(\psi) = \{e_1\}$.
Réciproquement, supposons que $\ker(\psi) = \{e_1\}$. Soit $x, y \in G_1$ tels que $\psi(x) = \psi(y)$. Alors

$$\begin{array}{rcl} e_2 & = & \psi(x) \cdot (\psi(y))^{-1} \\ & = & \psi(x) \cdot \psi\left(y^{-1}\right) \\ & = & \psi\left(x \star y^{-1}\right) \end{array}$$

Donc $x \star y^{-1} \in \ker(\psi) = \{e_1\}$ et finalement $x = y$. La preuve est terminée.

Exercice

Soit $(G_1, \star)$ et $(G_2, \cdot)$ deux groupes et $\psi : G_1 \longrightarrow G_2$ un homomorphisme de groupe.

1. *Montrer que si H_1 est un sous de G_1 alors $\psi(H_1)$ est un sous groupe de G_2.*
2. *Montrer que si H_2 est un sous de G_2 alors $\psi^{-1}(H_2)$ est un sous groupe de G_1.*

Le groupe $\mathbb{Z}/n\mathbb{Z}$

Soit $n > 1$ un entier naturel donné. On rappelle la relation d'équivalence sur $\mathbb{Z}$ définie par

$$a \equiv b \pmod{n} \iff \exists k \in \mathbb{Z} \ / \ b - a = kn$$

On rappelle que la classe d'équivalence $\overline{a}$ d'un entier $a \in \mathbb{Z}$ est la partie de $\mathbb{Z}$ donnée par

$$\overline{a} = \{b \in \mathbb{Z} \ / \ a \equiv b \pmod{n} \}.$$

Il est clair que

$$\overline{a} = \overline{b} \iff a \equiv b \pmod{n}$$

On définit ainsi l'ensemble des classes d'équivalence

$$\mathbb{Z}/n\mathbb{Z} := \{\overline{a} \ / \ a \in \mathbb{Z}\}.$$

Montrons que

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\} \quad \text{et qu'il est de cardinal } n.$$

Pour tout $a \in \mathbb{Z}$, la division euclidienne nous assure l'existence de $(k, r) \in \mathbb{Z}^2$ tel que

$$a = kn + r \quad \text{et} \quad 0 \leq r \leq n - 1.$$

Ainsi,

$$\overline{a} = \overline{r}.$$

De plus, si $0 \leq a < b \leq n - 1$ alors $\overline{a} \neq \overline{b}$. Sinon $b - a = kn$ et $0 \leq b - a \leq n - 1$ donc $k = 0$ et $b = a$ ce qui est absurde.

Exemple

Dans $\mathbb{Z}/10\mathbb{Z}$ on a

$$\overline{10} = \overline{0} \ , \ \overline{95} = \overline{5} \ , \ \overline{-3} = \overline{7}$$

Addition sur $\mathbb{Z}/n\mathbb{Z}$

On munit $\mathbb{Z}/n\mathbb{Z}$ de l'addition suivante :

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Cette opération est bien définie. En effet, soit $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$. Alors il existe $k, k' \in \mathbb{Z}$ tels que

$$a = a' + kn \quad \text{et} \quad b = b' + k'n.$$

Donc

$$a + b = a' + b' + (k + k')n.$$

Autrement dit,

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

Théorème

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

Démonstration : L'associativité et la commutativité découle de celles de l'addition de $\mathbb{Z}$. L'élément neutre est $\overline{0}$ et l'élément opposé de $\overline{a}$ est

$$-\overline{a} = \overline{-a} = \overline{n-a}$$

En affet, $\overline{a} + \overline{n-a} = \overline{n} = \overline{0}$.

Exemple

Par exemple, posons $n = 18$. Alors

$$\mathbb{Z}/18\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{17}\};$$
$$\overline{18} = \overline{0}\ ,\ \overline{19} = \overline{1},\ ,\ \overline{183} = \overline{3};$$
$$\overline{15} + \overline{17} = \overline{14}\ ,\ \overline{150} + \overline{170} = \overline{320} = \overline{14}$$

Exemple

Expliciter les calculs dans $\mathbb{Z}/10\mathbb{Z}$ et remarquer que seul le chiffre des unités compte dans les calculs dans ce groupe.

Multiplication sur $\mathbb{Z}/n\mathbb{Z}$

On peut définir la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ par

$$\overline{a}\overline{b} = \overline{ab}.$$

Cette opération est bien définie. En effet, soit $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$. Alors il existe $k, k' \in \mathbb{Z}$ tels que $a = a' + kn$ et $b = b' + k'n$. Donc $ab = a'b' + (kb' + a'k + kk'n)n$. Autrement dit,

$$\overline{a}\overline{b} = \overline{ab} = \overline{a'b'} = \overline{a'b'}.$$

On vérifie que ce produit est associatif, commutatif et que l'élément neutre est $\overline{1}$. Cependant, les éléments non nuls de $\mathbb{Z}/n\mathbb{Z}$ n'ont pas toujours un inverse pour la multiplication, et donc $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ n'est pas toujours un groupe. Par exemple, dans $\mathbb{Z}/4\mathbb{Z}$ on a

$$\overline{2} \cdot \overline{2} = \overline{0}$$

Donc si $\overline{2}$ avait un élément inverse $\overline{a}$ alors $\overline{2} = \overline{2} \cdot (\overline{2} \cdot \overline{a}) = \overline{0}\overline{a} = \overline{0}$ ce qui est absurde.

Résoudre les équations suivantes dans $\mathbb{Z}/10\mathbb{Z}$.

1. $\overline{3} \cdot \overline{x} = \overline{2}$.
   Solution : Comme $3 \times 7 = 21$ on déduit que $\overline{3} \cdot \overline{7} = \overline{1}$ et donc $\overline{3}$ est inversible d'inverse $\overline{7}$. Ainsi notre équation admet une seule solution donnée par $\overline{x} = \overline{7} \cdot \overline{2} = \overline{14} = \overline{4}$.

2. $\overline{9} \cdot \overline{x} = \overline{4}$. Ici $\overline{9}$ est inversible d'inverse $\overline{9}$. Donc l'équation admet une seule solution $\overline{x} = \overline{9} \cdot \overline{4} = \overline{6}$.
3. $\overline{2} \cdot \overline{x} = \overline{3}$.
   Solution : Ici $\overline{2}$ n'est pas inversible. Si x est solution de l'équation alors $2x = 3 + 10k$ et donc $3 = 2(x - 5k)$ ce qui est impossible.
4. $\overline{2} \cdot \overline{x} = \overline{8}$.
   Solution : Si x solution alors $2x = 8 + 10k$, i.e. $x = 4 + 5k$. Finalement, les solutions sont $\overline{4}, \overline{9}$.

Proposition

*Un élément $\overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$ est inversible pour la multiplication si, et seulement si, x et n sont **premiers entre eux**.*

Démonstration : D'après le théorème de Bezout, x et n sont premiers entre eux si, et seulement si, il existe deux entiers u, v tels que $ux + vn = 1$, ce qui équivaut aussi à

$$\overline{u} \cdot \overline{x} = \overline{ux} = \overline{1},$$

ce qui signifie que $\overline{x}$ est inversible d'inverse $\overline{u}$. De plus, l'algorithme d'Euclide nous fournit une méthode de calcul de l'inverse.

Corollaire

*Si p est un nombre premier, alors tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible pour la multiplication. On dit que, $(\mathbb{Z}/p\mathbb{Z}), +, \cdot)$ est un **corps**. Ce corps est commutatif car le produit l'est. Cette notion est hors programme.*

Notion d'ordre d'un élément

Soit $(G, \star)$ un groupe et $g \in G$. On rappelle que l'application

$$\begin{array}{rccc} \psi_g : & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & g^n \end{array}$$

qui est un homomorphisme. En fait, nous avons

Proposition

Soit $(G, \star)$ un groupe.

1. *Si $\psi : \mathbb{Z} \longrightarrow G$ est un homomorphisme de groupe alors il existe un unique élément g de G tel que $\psi = \psi_g$.*
2. *Si $g \in G$ alors il existe un unique homomorphisme $\psi : \mathbb{Z} \longrightarrow G$ tel que $\psi(1) = g$, il s'agit de $\psi = \psi_g$.*

Démonstration : (i) Soit $\psi : \mathbb{Z} \longrightarrow G$ est un homomorphisme. Posons alors $g = \psi(1)$ qui est un élément de G. Alors

$$\psi(2) = \psi(1 + 1) = \psi(1)\psi(1) = g^2.$$

Par récurrence on montre que pour tout $n \in \mathbb{N}$ on a $\psi(n) = g^n$. Aussi,

$$\psi(0) = \psi(1 - 1) = \psi(1)\psi(-1) = e$$

et donc

$$\psi(-1) = (\psi(1))^{-1} = g^{-1}.$$

Ainsi,

$$\psi(-2) = \psi(-1-1) = \psi(-1)\psi(-1) = (g^{-1})^2 = g^{-2}.$$

Ainsi, par récurrence, pour tout $n \in \mathbb{N}$,

$$\psi(-n) = g^{-n}.$$

Finalement, nous avons montré que pour tout $n \in \mathbb{Z}$,

$$\psi(n) = g^n.$$

L'unicité de g est triviale car si un élément $x \in G$ vérifie $\psi(n) = x^n$ alors $g = \psi(1) = x$.

(ii) Soit $g \in G$. Alors on sait que le homomorphisme

$$\begin{array}{rcl} \psi_g : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$$

vérifie $\psi_g(1) = g$. Si ψ est un homomorphisme $\mathbb{Z} \longrightarrow G$ tel que $\psi(1) = g$ alors on vérifie comme plus haut que $\psi = \psi_g$.

Théorème

Soit $(G, \star)$ un groupe et $g \in G$. Alors l'ensemble

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

est un sous groupe de G. De plus, on a l'une des assertions suivantes :

1. *$\langle g \rangle$ est isomorphe à $\mathbb{Z}$ et dans ce cas on dit que g est* ***d'ordre infini****,*
2. *il existe un entier p tel que $\langle g \rangle$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Dans ce cas, on dit que g est* ***d'ordre*** *p et on a*

$$\langle g \rangle = \{e, g, \cdots, g^{p-1}\} \quad \text{et le cardinal de } \langle g \rangle \text{ est } p.$$

Démonstration : On considère le morphisme de groupe

$$\begin{array}{rcl} \psi : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & g^n \end{array}$$

Comme le noyau $\ker \psi$ est un sous groupe de $\mathbb{Z}$, il existe un entier positif p tel que

$$\ker \psi = \{k \in \mathbb{Z} \ / \ g^k = e\} = p\mathbb{Z}$$

Si $p = 0$ alors ψ est injective et le sous groupe engendré par g

$$\langle g \rangle = \{g^k \ , \ k \in \mathbb{Z}\} \quad \text{est infini}$$

et est isomorphe à $\mathbb{Z}$.

Si p est non nul alors p est le plus entier positif non nul tel que $g^p = e$, puisqu'il est le plus entier positif non nul de $\ker \psi$. En particulier, le sous groupe engendré par g est

$$\langle g \rangle = \{e, g, \cdots, g^{p-1}\} \quad \text{et il est de cardinal } p.$$

En effet, soit $k \in \mathbb{Z}$. Grâce à la division euclidienne, il existe $(q, r) \in \mathbb{Z}^2$ tel que $0 \leq r \leq p-1$ avec $k = pq + r$. Ainsi,

$$g^k = g^{pq+r} = g^{pq} \star g^r = g^r.$$

De plus, si $0 \leq m < n < p$ tel que $g^m = g^n$ alors $g^{n-m} = e$ et donc $n - m \in \ker \psi$ et $0 \leq n - m < p$; d'où $n = m$.

Maintenant, il suffit de considérer

$$\begin{array}{rcl} \Psi : \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \langle g \rangle \\ \overline{a} & \longmapsto & g^a \end{array}$$

et de montrer que Ψ est un isomorphisme de groupe.

En effet, si $\overline{a} = \overline{b}$ alors il existe un entier k tel que $b = a + kp$ et donc

$$\Psi(\overline{b}) = g^b = g^{a+kp} = g^a \star g^{kp} = g^a = \Psi(\overline{a}).$$

Autrement dit, Ψ est bien définie. De plus,

$$\Psi(\overline{a} + \overline{b}) = \Psi(\overline{a+b}) = g^{a+b} = g^a \star g^b = \Psi(\overline{a}) \star \Psi(\overline{b}).$$

Ainsi ψ est un homomorphisme. De plus, ψ est surjective puisque tout élément de G s'écrit comme une puissance de g.

Soit $\overline{a} \in \ker \Psi$. Alors

$$\Psi(\overline{a}) = g^a = e.$$

Donc $a \in \ker \psi$ et a est un multiple de p. Finalement, $\overline{a} = \overline{0}$ et Ψ est injective.

Remarque

Soit $(G, \star)$ un groupe et $g \in G$. Si $g = e$ alors $\langle g \rangle = \{e\}$. Si $g \neq e$ alors on a l'une des assertions suivantes :

1. ou bien g est d'ordre infini c'est-à-dire aucune puissance de g ne vaut e, et dans ce cas $\langle g \rangle$ est isomorphe à $\mathbb{Z}$. En particulier,
$$g^n = g^m \Longleftrightarrow n = m$$
2. ou bien g est d'ordre fini p. Dans ce cas p est le plus petit entier naturel non nul tel que $g^p = e$. De plus, $\langle g \rangle$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et
$$g^n = e \Longleftrightarrow p/n$$

Groupes cycliques

Définition

On dit que $(G, \star)$ est un groupe cyclique s'il existe un élément a de G tel que $G = \langle a \rangle = \{a^k \ , \ k \in \mathbb{Z}\}$. On dit que G est engendré par a.

1. Si $(G, \star)$ est un groupe cyclique engendré par un élément a d'ordre n alors le cardinal de G est n. On dit que G est d'ordre n.
2. Si $(G, \star)$ est un groupe cyclique alors il est commutatif.

Exemples

1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Il s'agit d'un groupe cyclique d'ordre infini. Aucun élément de $\mathbb{Z}$ autre de 1 ou -1 n'engendre $\mathbb{Z}$.
2. $(\mathbb{Z}/n\mathbb{Z}, +) = \langle \overline{1} \rangle$.
3. Dans $(\mathbb{Z}/4\mathbb{Z}, +)$, $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}\} \neq \mathbb{Z}/4\mathbb{Z}$ et $\langle \overline{1} \rangle = \langle \overline{3} \rangle = \mathbb{Z}/4\mathbb{Z}$.
4. $(\mathbb{Z}/5\mathbb{Z}, +) = \langle \overline{1} \rangle = \langle \overline{2} \rangle = \langle \overline{3} \rangle = \langle \overline{4} \rangle$.
5. Soit $n \geq 2$ un entier non nul. Posons

$$\mathbb{U}_n = \{z \in \mathbb{C} \ / \ z^n = 1\} = \{e^{\frac{2ik\pi}{n}}, k = 0, 1, \cdots, n-1\}.$$

l'ensemble des n racines $n^{\text{ème}}$ de l'unité. Il est clair que $\mathbb{U}_n$ muni de la multiplication des nombres complexes est un groupe commutatif. Ce groupe est cyclique et est engendré par $e^{\frac{2i\pi}{n}}$.

Proposition

Soit G un groupe cyclique d'ordre n engendré par a et soit $k \in \{0, 1, \cdots, n-1\}$. L'ordre de a^k vaut n si, et seulement si, k et n sont premier entre eux.

Démonstration : Notons d'abord que l'ordre de a^k est n signifie que a^k est aussi un générateur de G. Supposons que k et n ne sont pas premiers entre eux et soit d un diviseur commun de k et n autre que 1. Alors $k = dp$ et $n = dq$. Il vient que

$$(a^k)^q = a^{kq} = a^{dpq} = a^{np} = e$$

ce qui est absurde car $q < n$ et n est l'ordre de a^k.

Réciproquement supposons que k et n sont premier entre eux et que n n'est pas l'ordre de a^k. Donc il existe $0 < d < n$ tel que $a^{kd} = (a^k)^d = e$. Donc n divise kd. Comme k et n sont premier entre eux, on déduit que n divise d ce qui est impossible.

Corollaire

Si G est un groupe cyclique d'ordre premier alors G est engendré par n'importe lequel de ses éléments autre que l'élément neutre. En particulier, tous sous groupe de G contenant un élément autre que l'élément neutre est G lui même. Autrement dit, $\{e\}$ et G sont les seuls sous groupe de G.

Ceci est un cas particulier du théorème de Lagrange qui dit que le cardinal de tout sous groupe H d'un groupe fini G divise le cardinal de G : $|H|/|G|$.

Exemple

Soit $n \geq 2$ un entier non nul. Le groupe cyclique $\mathbb{U}_n$ est est engendré par $e^{\frac{2i\pi}{n}}$ ou par n'importe lequel de ses éléments $e^{\frac{2ik\pi}{n}}$ pour vu que k et n soient premiers entre eux.
Soit $z = e^{\frac{2i\pi}{n}}$ ou n'importe quel autre élément générateur de $\mathbb{U}_n$. L'application

$$\begin{array}{rcl} \psi : \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{U}_n \\ \overline{k} & \longmapsto & z^k \end{array}$$

est un isomorphisme de groupe.

En fait, nous avons le théorème suivant :

Théorème

Si $(G, \star)$ est un groupe cyclique de cardinal n alors $(G, \star)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Démonstration : Soit a un élément générateur de G, i.e.

$$G = \{e, a, \cdots, a^{n-1}\} = \langle a \rangle.$$

On sait que

$$\begin{array}{rcl} \psi : \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \langle a \rangle \\ \overline{p} & \longmapsto & a^p \end{array}$$

est un isomorphisme de groupe.