10.8 Groupes cycliques, Groupes monogène

10.8.1 Ordre d'un groupe, Ordre d'un élément

Soit G un groupe d'élément neutre e

1. L'ordre du groupe G est le nombre d'éléments de ce groupe (cf 10.8.1)
2. L'ordre d'un élément $x \in G$, est le plus petit entier $n \in \mathbb{N}^*$ tel que $x^n = e$

10.8.2 Définition

Soit G un groupe

1. G est dit monogène s'il existe $a \in G$ tel que, pour tout $x \in G$, il existe $n \in \mathbb{Z}$ tel que $x = a^n$
2. G est dit cyclique s'il est monogène et d'ordre fini

Remarque 28 :

Un groupe monogène G est un groupe engendré par un seul élément $a \in G$. Nous avons : $G = \{x \text{ tel que } x = a^n \text{ avec } n \in \mathbb{Z}\}$

10.8.3 Proposition

Tout groupe monogène est abélien

Démonstration

Soit $G = \{x \text{ tel que} x = a^n \text{ avec } n \in \mathbb{Z}\}$ un groupe monogène, $x \in G$ et $y \in G$.
Alors, $xy = a^n \times a^p = a^{n+p} = a^{p+n} = a^p \times a^n = yx$
G est bien abélien

Remarque 29 :

Tout groupe cyclique est aussi abélien ; la réciproque est évidemment fausse

Exemple 14 :

1. $\mathbb{Z}$ muni de l'addition est un groupe monogène de générateur 1 ou -1
2. Pour $n \in \mathbb{N}$ et $n \geqslant 2$, $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition est un groupe cyclique d'ordre n et de générateur 1
3. Toujours pour $n \in \mathbb{N}$ et $n \geqslant 2$, $\mathbb{U}_n$, l'ensemble des racines n-ièmes de 1 muni de la multiplication est un groupe cyclique d'ordre n ; rappel : $\mathbb{U}_n = \left\{e^{\frac{2ik\pi}{n}} \text{ avec } k \in \mathbb{Z}\right\}$ et le générateur est donc $\omega_n = e^{\frac{2i\pi}{n}}$

10.8.4 Théorème

Soit G un groupe et $a \in G$ un élément de G d'ordre m.
On appelle $\langle a \rangle = \{a^n \text{ où } n \in \mathbb{Z}\}$ l'ensemble des puissances de a

1. $\langle a \rangle$ est un sous-groupe de G
2. Nous avons $\langle a \rangle = \left\{e, a, a^2, \cdots, a^{m-1}\right\}$
3. Nous avons Card $\langle a \rangle = m$, c'est à dire que pour $0 \leqslant i < m$ et $0 \leqslant j < m$, $i \neq j \Longrightarrow a^i \neq a^j$
4. m, l'ordre de a divise l'ordre de G

Démonstration

1. On montre que $\langle a\rangle$ est un sous-groupe de G
   — Tout d'abord $\langle a\rangle \neq \emptyset$ car $a \in \langle a\rangle$ ou $e = a^0 \in \langle a\rangle$
   — D'autre part, soient $x \in \langle a\rangle$ et $y \in \langle a\rangle$.
   Il existe $p \in \mathbb{Z}$ et $q \in \mathbb{Z}$ tels que $x = a^p$ et $y = a^q$, et nous avons $y^{-1} = a^{-q}$.
   Donc, $xy^{-1} = a^p \times a^{-q} = a^{p-q}$ et donc, $xy^{-1} \in \langle a\rangle$
   Donc $\langle a\rangle$ est un sous-groupe de G
2. On démontre que $\langle a\rangle = \left\{e, a, a^2, \cdots, a^{m-1}\right\}$
   On appelle $A = \left\{e, a, a^2, \cdots, a^{m-1}\right\}$, et nous allons donc montrer que $\langle a\rangle = A$
   — Il est évident que, par construction, $A \subset \langle a\rangle$
   — Démontrons maintenant que $\langle a\rangle \subset A$
   Soit $x \in \langle a\rangle$. Il existe alors $p \in \mathbb{Z}$ tel que $x = a^p$.
   Effectuons la division euclidenne de p par m :
   $$p = km + r \text{ avec } 0 \leqslant r < m$$
   Et donc, $a^p = a^{km+r} = a^r \times a^{km} = a^r \times (a^m)^k = a^r \times e = a^r$
   Et donc, $x \in A$
   En conclusion, $\langle a\rangle = \left\{e, a, a^2, \cdots, a^{m-1}\right\}$
3. On montre que Card $\langle a\rangle = m$
   En fait, il faut montrer que pour tout $0 \leqslant i < m$ et tout $0 \leqslant j < m$, $i \neq j \Longrightarrow a^i \neq a^j$
   Supposons le contraire, c'est à dire qu'il existe $0 \leqslant i < m$ et $0 \leqslant j < m$ avec $i \neq j$ (supposons $i < j$) tels que $a^i = a^j$.
   Alors, $a^{j-i} = e$ de $0 \leqslant i < m$ et $0 \leqslant j < m$ et $j > i$, nous avons $1 \leqslant j - i < m$. Ce qui contredit la définition de m comme étant le plus petit entier tel que $a^m = 1$
   Il y a donc une contradiction et on en déduit que pour tout $0 \leqslant i < m$ et tout $0 \leqslant j < m$, $i \neq j \Longrightarrow a^i \neq a^j$, c'est à dire Card $\langle a\rangle = m$
4. C'est une simple application du théorème de Lagrange *(cf 10.5.13)*

Remarque 30 :

Soit G un groupe ; le théorème 10.8.4 précise que l'ordre d'un élément $a \in G$ est l'ordre du sous-groupe $\langle a\rangle \subset G$ généré par a.

10.8.5 Corollaire

1. Soit G un groupe d'ordre n ; alors, pour tout $x \in G$, $x^n = e$
2. Tout groupe G d'ordre un nombre premier est cyclique. Il est engendré par l'un quelconque de ses éléments distincts de e
3. Soit G un groupe fini et $a \in G$. Soit m l'ordre de a. Alors, pour tout $k \in \mathbb{N}$,
   $$a^k = e \Longleftrightarrow m \text{ divise } k$$

Démonstration

1. On montre que si G est un groupe d'ordre n, alors, pour tout $x \in G$, $x^n = e$
   Soit $x \in G$, et on considère le sous-groupe $\langle x\rangle = \left\{x^k; k \in \mathbb{N}\right\}$.
   Comme $\langle x\rangle \subset G$, $\langle x\rangle$ est forcément d'ordre fini et d'ordre m, tel que $x^m = e$.
   Alors m divise n, ce qui veut dire qu'il existe $k \in \mathbb{N}$ tel que $n = km$. Alors :
   $$x^n = x^{km} = (x^m)^k = e^k = e$$
   Ce que nous voulions

2. Tout groupe G d'ordre premier est cyclique
   Soit G un groupe d'ordre p où p est un nombre premier. Soit $x \in G$ tel que $x \neq e$ et on considère $\langle x \rangle = \left\{x^k ; k \in \mathbb{N}\right\}$.
   L'une des premières choses que nous pouvons voir est que Card $\langle x \rangle \geqslant 2$. Soit m l'ordre de x, c'est à dire Card $\langle x \rangle = m$
   Alors, m divise p ; or, les seuls diviseurs entiers positifs de p sont 1 et p. Comme $m \neq 1$, $m = p$ et $G = \langle x \rangle$
   G est bien cyclique
3. Montrons que $a^k = e \Longleftrightarrow m$ divise k
   Soit $a \in G$, d'ordre m, c'est à dire tel que $a^m = e$
   — Commençons par le plus facile ! ! Supposons que m divise k, c'est à dire qu'il existe $q \in \mathbb{N}$ tel que $k = qm$. Donc
   $$a^k = a^{qm} = (a^m)^q = e^q = e$$
   — Réciproquement, soit $k \in \mathbb{N}$ tel que $a^k = e$.
   Faisons la division euclidienne de k par m : $k = qm + r$ avec $0 \leqslant r < m$.
   Et donc, $a^k = a^{qm+r} = a^{qm} \times a^r = (a^m)^q \times a^r = e \times a^r = a^r = e$; comme $0 \leqslant r < m$, $r = 0$ et donc, $k = qm$, c'est à dire que k divise m.

Exercice 29 :

1. Soit G un groupe commutatif.
   Pour $r \in \mathbb{N}$, on note :
   $$H_r = \{x \in G \text{ tels que } x^r = e\} = \{x \in G \text{ tels que ordre}\,(x) \text{ divise } r\}$$
   Il faut montrer que H_r est un sous-groupe de G
2. Soit G un groupe commutatif d'ordre n. On appelle $\mathcal{R}$ la relation :
   $$(\forall x \in G)\,(\forall y \in G)\,(x \mathcal{R} y \Longleftrightarrow x \text{ et } y \text{ ont le même ordre})$$
   (a) Montrer que $\mathcal{R}$ est une relation d'équivalence
   (b) On appelle $\psi\,(d)$ le nombre d'éléments d'ordre d de G. Montrer qu'alors on a :
   $$n = \sum_{d|n} \psi\,(d)$$

10.8.6 Définition et théorème

Soit G un groupe quelconque et $u \in G$
1. Si $(\forall h \in \mathbb{Z})\,(\forall k \in \mathbb{Z})\,\left(h \neq k \Longrightarrow u^h \neq u^k\right)$, Alors, u est dit d'ordre infini
2. Tout groupe monogène infini G est isomorphe à $(\mathbb{Z}, +)$
3. Plus généralement, si G est un groupe et $g \in G$ un élément d'ordre infini, alors le morphisme $\Psi_g : \mathbb{Z} \longrightarrow G$ tel que $\Psi_g\,(1) = g$ est un monomorphisme, dont l'image est le sous-groupe cyclique engendré par g

Démonstration

Soit G un groupe monogène infini engendré par g, et doit Ψ_g ainsi défini :
$$\left\{\begin{array}{rcl} \Psi_g : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & \Psi_g\,(n) = g^n \end{array}\right.$$

1. Alors Ψ_g est injective
   En effet, si $\Psi_g\,(m) = \Psi_g\,(n)$, nous avons $g^m = g^n$, ce qui est équivalent à $g^{m-n} = e$, c'est à dire, comme G est monogène infini, $m - n = 0 \Longleftrightarrow m = n$
   Ψ_g est donc injective

2. Ψ_g est surjective
   Soit $x \in G$; alors, il existe $k \in \mathbb{Z}$ tel que $x = g^k$ et alors $\Psi_g(k) = g^k$, et Ψ_g est donc surjective

Ψ_g est donc bijective, et dans le cas des groupes monogènes infini, Ψ_g est donc un isomorphisme

10.8.7 Définition et théorème

1. S'il existe un entier m strictement positif, $(m \in \mathbb{N}^*)$, tel que $u^m = e$, en considérant le plus petit entier positif n tel que $u^n = e$, alors, on dit que u est d'ordre n
2. Tout groupe cyclique d'ordre $n \in \mathbb{N}^*$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$
3. Plus généralement, si G est un groupe et $g \in G$ un élément d'ordre infini, alors le morphisme $\Psi_g : \mathbb{Z} \longrightarrow G$ tel que $\Psi_g(1) = g$ est un monomorphisme, dont l'image est le sous-groupe cyclique engendré par g

Démonstration

On suppose G cyclique d'ordre n de générateur g ; alors $g^n = e$. Soit Ψ_g ainsi défini :

$$\begin{cases} \Psi_g : \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & \Psi_g(n) = g^n \end{cases}$$

Nous allons démontrer que le noyau de Ψ_g est $\ker \Psi_g = n\mathbb{Z}$, et alors, d'après le théorème d'isomorphisme 10.7.5 et le paragraphe 10.7.6 nous avons alors $\mathbb{Z}/\ker\varphi = \mathbb{Z}/n\mathbb{Z}$ isomorphe à $\Psi_g(\mathbb{Z}) = G$

1. On montre que $\ker \Psi_g \subset n\mathbb{Z}$
   Soit $p \in \ker \Psi_g$; alors $\Psi_g(p) = g^p = e$; donc, d'après les résultats précédents n divise p et donc il existe $q \in \mathbb{Z}$ tel que $p = qn$; c'est à dire $p \in n\mathbb{Z}$. Nous avons donc $\ker \Psi_g \subset n\mathbb{Z}$
2. Réciproquement, soit $p \in n\mathbb{Z}$; alors, p peut s'écrire $p = kn$, et donc
   $$\Psi_g(p) = \Psi_g(kn) = g^{kn} = (g^n)^k = e^k = e$$
   et donc $p \in \ker \Psi_g$.
   Nous avons donc $n\mathbb{Z} \subset \ker \Psi_g$

Nous avons donc $\ker \Psi_g = n\mathbb{Z}$ et donc $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à G

Remarque 31 :

Ce résultats permet aussi de préciser lorsque 2 puissances d'un élément g d'ordre n sont égales :

$$g^k = g^m \Longleftrightarrow k \equiv m\,[n]$$

10.8.8 Proposition

Soit C un groupe cyclique de générateur $c \in C$. Soit G un groupe quelconque et $\Psi : C \longrightarrow G$ un homomorphisme surjectif. Alors
G est un groupe cyclique et l'ordre de G est un diviseur de l'ordre de C

Démonstration

Soit C un groupe cyclique de générateur $c \in C$, G un groupe quelconque et $\Psi : C \longrightarrow G$ un homorphisme surjectif.
Alors, soit $y \in G$; il existe $x \in C$ tel que $\Psi(x) = y$ et, il existe $k \in \mathbb{Z}$ tel que $x = c^k$, et donc :

$$y = \Psi(x) = \Psi\left(c^k\right) = (\Psi(c))^k$$

Ce qui montre que tout élément $y \in G$ peut s'écrire comme puissance d'un élément $\Psi(c)$. G est donc cyclique de générateur $\Psi(c)$
D'autre part, si n est l'ordre de C, nous avons $c^n = e$, $\Psi(c^n) = (\Psi(c))^n = (e)^n = e$, de telle sorte que l'ordre de G divise n, l'ordre de C.

10.8.9 Corollaire

L'image, par un morphisme de groupe, d'un groupe cyclique est un groupe cyclique

Démonstration

Soit G un groupe cyclique de générateur g, H un groupe quelconque et $\varphi : G \longrightarrow H$ un homomorphisme de groupe.
Soit $y \in \text{Im}\varphi = \varphi(G)$. il existe donc $x \in G$ tel que $\varphi(x) = y$ et il existe aussi $p \in \mathbb{Z}$ tel que $x = g^p$, et dès lors :

$$y = \varphi(x) = \varphi(g^p) = (\varphi(g))^p$$

Ainsi $\text{Im}\varphi = \varphi(G)$ est un sous-groupe cyclique de H de générateur $\varphi(g)$

10.8.10 Théorème

Tout sous-groupe d'un groupe cyclique est cyclique

Démonstration

Soit G un groupe cyclique.
Nous allons envisager 2 cas :

- ⋆ G est un groupe cyclique d'ordre infini
- ⋆ G est un groupe d'ordre fini n

1. **Supposons G groupe cyclique d'ordre infini**
   C'est à dire $G = \{q^n \text{ où } n \in \mathbb{Z}\}$.
   Nous allons montrer que les ensembles du type $\mathcal{C}_n = \left\{q^{nk} \text{ où } k \in \mathbb{Z}\right\}$ sont les seuls sous-groupes de G. La démonstration est tout à fait semblable à celle de 10.5.2
   ⇒ Premièrement, il est clair que les ensembles du type $\mathcal{C}_n$ sont des sous groupes
   En effet, $\mathcal{C}_n \neq \emptyset$ puisque $q^{n\times 0} = q^0 = e$ est un élément de $\mathcal{C}_n$
   Puis, si $x \in \mathcal{C}_n$, $y \in \mathcal{C}_n$, avons nous $xy^{-1} \in \mathcal{C}_n$?
   Or, $xy^{-1} = q^{nk} \times \left(q^{nk'}\right)^{-1} = q^{nk} \times q^{-nk'} = q^{n(k-k')}$ et, comme $k - k' \in \mathbb{Z}$, nous avons bien $q^{n(k-k')} \in \mathcal{C}_n$, et donc $xy^{-1} \in \mathcal{C}_n$.
   Ce qui montre que $\mathcal{C}_n$ est un sous- groupe de G
   ⇒ Réciproquement, soit S un sous-groupe de G ; montrons qu'il est du type $\mathcal{C}_n$
   Soit $x \in S$; alors, x est du type q^p avec $p \in \mathbb{Z}$
   Soit n le plus petit entier positif tel que $q^n \in S$ et effectuons la division euclidienne de p par n :

   $$p = an + b \text{ avec } 0 \leqslant b \leqslant n - 1$$

   Alors,

   $$q^p = q^{an+b} = q^{an} \times q^b \Longleftrightarrow q^b = q^{-an} \times q^p$$

   Comme $q^n \in S$, il en est de même de q^{an} et de q^{-an} qui est son inverse. Donc $q^b \in S$, ce qui est en contradiction avec le fait que n est le plus petit entier tel que $q^n \in S$, sauf si $b = 0$. On en conclue donc que $p = an$. Ainsi, $S = \{q^{na} \text{ où } a \in \mathbb{Z}\}$. S est donc du type $\mathcal{C}_n$
2. **Supposons G groupe cyclique d'ordre fini n**
   Soit c le générateur d'ordre n de G.
   Nous allons démontrer que tous les sous-groupes $S \subset G$, sont du type :

   $$S = \left\{c^{kj} \text{ où } k \text{ est un diviseur de } n \text{ tel que } n = mk \text{ et } 0 \leqslant j \leqslant m - 1\right\}$$

   ⇒ Les ensembles du type S sont des sous-groupes de G
   - ⋆ En premier lieu, $S \neq \emptyset$, car $\left(c^k\right)^0 = \left(c^k\right)^m = e$, et donc $e \in S$
   - ⋆ Ensuite, si $y \in S$ et $x \in S$, alors $x = \left(c^k\right)^j$ et $y = \left(c^k\right)^i$, donc $xy = \left(c^k\right)^j \times \left(c^k\right)^i = \left(c^k\right)^{i+j}$ et donc, $xy \in S$

⋆ Soit $y \in S$; alors $y = c^{kj}$ et l'inverse de y est donc $y^{-1} = \left(c^{kj}\right)^{-1} = c^{-kj} = \left(c^{k}\right)^{m-j}$. Donc $y^{-1} \in S$

S est donc un sous groupe de G, d'ordre m où m divise n.

$\Rightarrow$ Réciproquement, soit H un sous-groupe de G

Alors, tous les éléments de H sont du type c^p. Soit k le plus petit entier positif $0 \leqslant k \leqslant n-1$ tel que $c^k \in H$, et divisons n par k.

$$n = ak + r \text{ avec } 0 \leqslant r \leqslant k-1$$

Et donc, comme $c^n = e$, nous avons $c^{ak+r} = e$. Or, $c^{ak+r} = c^{ak} \times c^r$. Comme $c^{ak} = \left(c^k\right)^a$, nous avons $c^{ak} \in H$. et donc, par composition interne, $c^r \in H$, ce qui contredit, sauf pour $r = 0$, le fait que k soit le plus petit entier tel que $c^k \in H$. Donc, $r = 0$ et le sous groupe H est du type $S = \left\{c^{kj} \text{ où } k \text{ est un diviseur de } n \text{ tel que } n = mk \text{ et } 0 \leqslant j \leqslant m-1\right\}$

Remarque 32 :

1. On peut appliquer la démonstration du point 1 au groupe additif $(\mathbb{Z}, +)$ qui est aussi un groupe cyclique : les seuls sous-groupes de $(\mathbb{Z}, +)$ sont donc du type : $\mathcal{C}_n = \{nk \text{ où } k \in \mathbb{Z}\} = n\mathbb{Z}$.
   On retrouve donc le résultats sur les seuls sous groupes de $\mathbb{Z}$ qui sont les multiples d'un entier positif $n \geqslant 1$
2. Dans le groupe additif $\mathbb{Z}/6\mathbb{Z}$ qui est un groupe cyclique de générateur 1, les groupes sont engendrés par les diviseurs de 6. On retrouve donc comme sous-groupe :

   ⋆ $H_1 = \left\{\dot{0}, \dot{2}, \dot{4}\right\}$ ⋆ $H_2 = \left\{\dot{0}, \dot{3}\right\}$

Exercice 30 :

Soit G un groupe cyclique d'ordre n, de générateur $g \in G$ et d'élément neutre $e \in G$.

1. Montrer que, pour tout $k \in \mathbb{N}$, nous avons Card $\left\langle g^k \right\rangle = \dfrac{n}{\text{pgcd}\,(n,k)}$
2. En déduire que si k et n sont premiers entre eux, alors $\left\langle g^k \right\rangle = G$