Groupes cycliques

Soit G un groupe.
Rappel $\langle g \rangle = \{ g^m \mid m \in \mathbb{Z} \}$.

Déf.
On dit qu'un groupe est <u>cyclique</u> si il existe un élément $g \in G$ t.q. $G = \langle g \rangle$.
Alors on dit que g est un <u>générateur</u> de G
On pose $\text{gen}(G) = \{ g \in G \mid \langle g \rangle = G \}$.

Remarques.
1) Un groupe cyclique est abélien ; $\{1\}$ est un groupe cyclique.
2) Si $g \in \text{gen}(G)$ alors $g^{-1} \in \text{gen}(G)$
3) Si $\varphi : G \to H$ est un morphisme de groupe et $G = \langle g \rangle$ est cyclique alors φ est complètement déterminé par $\varphi(g)$.

Exemples de groupes cycliques

1) $\mathbb{Z}$, $\text{gen}(\mathbb{Z}) = \{-1, 1\}$
2) $\mathbb{Z}/m\mathbb{Z}$, $\text{gen}(\mathbb{Z}/m\mathbb{Z}) = \{ \bar{u} \mid (u, m) = 1 \}$.

Exercice : Démontrer que les ensembles de générateurs sont bien ceux donnés dans l'exemple précédent.

Théorème (classification des groupes cycliques)

Soit G un groupe cyclique. Si $|G|$ est infini alors G est isomorphe à $\mathbb{Z}$. Si $|G| = m \in \mathbb{Z}$ alors G est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

Preuve On considère un générateur $g \in G$, et le homomorphisme de groupes $\varphi : \mathbb{Z} \longrightarrow G$.

$$1 \longmapsto g$$

En particulier $\varphi(u) = g^n$ donc φ est surjectif car $\langle g \rangle = G$.
Soit la suite exacte courte :

$$0 \to \operatorname{Ker}\varphi \longrightarrow \mathbb{Z} \xrightarrow{\varphi} G \longrightarrow 1$$

Alors $\operatorname{Ker}\varphi$ est un sous-groupe de $\mathbb{Z}$, donc $\operatorname{Ker}\varphi \simeq m\mathbb{Z}$ pour un $m \geq 0$.

cas 1 G est infini $\Leftrightarrow$ φ est injectif $\Leftrightarrow$ $G \simeq \mathbb{Z}$

cas 2 $|G| = m \Leftrightarrow o(g) = m \Leftrightarrow \operatorname{Ker}\varphi = m\mathbb{Z}$
donc $G \simeq \mathbb{Z}/m\mathbb{Z}$ □

Notations

a) additive	b) multiplicative	ordre
$\mathbb{Z}$	C_∞	∞
$\mathbb{Z}/m\mathbb{Z}$	C_m	m

On veut étudier maintenant les automorphisme des groupes cyclique. Par le théorème de classification, il suffit de considérer les cas $\mathbb{Z}/m\mathbb{Z}$, $m > 0$ ou $\mathbb{Z}$.

Théorème :

a) $\mathrm{Aut}(\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z}, +)$

b) $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \simeq ((\mathbb{Z}/m\mathbb{Z})^*, \circ)$

En particulier $|\mathrm{Aut}(C_\infty)| = |\mathrm{Aut}(\mathbb{Z})| = 2$ et $|\mathrm{Aut}(C_m)| = |\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})| = \varphi(m)$.

Preuve

On va construire un isomorphisme

$$\varphi : (\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$$

pour $m \neq 0$ (le cas $m = 0$ correspond à $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}$)

Soit $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^*$. Donc $\langle \bar{a} \rangle = \mathbb{Z}/m\mathbb{Z}$

On pose

$$\varphi(\bar{a}) := \left(\alpha_{\bar{a}} : \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \\ \bar{1} & \mapsto & \bar{a} \end{array} \right)$$

φ est un morphisme de groupes car.

$$\varphi(\bar{a}\cdot\bar{b}) = \alpha_{\bar{a}\cdot\bar{b}} = \alpha_{\bar{a}} \circ \alpha_{\bar{b}} = \varphi(\bar{a}) \circ \varphi(\bar{b}).$$

$\bar{1} \longmapsto \overline{ab}$; $\bar{1} \mapsto \bar{b} \mapsto \overline{ab}$

L'inverse de ce morphisme est donné par

$$\psi : \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$$

$$\alpha \longmapsto \alpha(\bar{1})$$

De nouveau ψ est un morphisme de groupes car.

$$\psi(\alpha \circ \beta) = \alpha \circ \beta(\bar{1}) = \alpha(\psi(\beta)) = \psi(\beta) \cdot \alpha(\bar{1}) = \psi(\alpha) \cdot \psi(\beta).$$

De plus :

$$\psi \circ \varphi(\alpha) = \varphi(\alpha(\bar{1})) = \alpha_{\alpha(\bar{1})} = \alpha \quad \text{et}$$

$$\varphi \circ \psi(\bar{a}) = \varphi(\alpha_{\bar{a}}) = \alpha_{\bar{a}}(\bar{1}) = \bar{a}$$

Donc φ et ψ sont des isomorphismes et

$$\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$$

□

Notre but est de voir la structure de C_{mn} quand $(m,n)=1$. Pour ceci on a besoin du lemme technique suivant.

Lemme. Soit une suite exacte des groupes abéliens $1 \to A \xrightarrow{u} B \xrightarrow{v} C \to 1$. Alors

1) Il existe une section s de v (i.e. $v \circ s = id_C$, $s: C \to B$ un homomorphisme de groupes) si et seulement si il existe une rétraction r de u (i.e., $r \circ u = id_A$, $r: B \to A$ un homomorphisme de groupes)

2) Dans ces conditions on a $B \simeq A \times C$.

Preuve

1) Soit $s: C \to B$ une section de v. Alors on construit $r: B \to A$ par

$$r(b) = u^{-1}(b - s \circ v(b))$$

On vérifie :

a) $b - s \circ v(b) \in \text{Image}(u)$ car $v(b - s \circ v(b)) = 0$

Donc $b - s \circ v(b) \in \text{Ker}(v) = \text{Im}(u)$

b) r est un homomorphisme :

$$\begin{aligned} r(b+b') &= u^{-1}(b+b' - s \circ v(b+b')) = \\ &= u^{-1}(b - s \circ v(b) + b' - s \circ v(b')) \\ &= u^{-1}(b - s \circ v(b)) + u^{-1}(b' - s \circ v(b')) \\ &= r(b) + r(b') \end{aligned}$$

c) r est une rétraction de u :

$$r \circ u(a) = u^{-1}(u(a) - \underbrace{s \circ v \circ u(a)}_{=0}) = a$$

Soit $r : B \to A$ une rétraction de u.
Alors on construit $s : C \to B$ en posant

$$s(c) = s(v(b)) = b - u \circ r(b)$$

A vérifier :

a) s est bien définie :

Si $v(b) = c = v(b')$ alors $v(b - b') = 0$
donc $b - b' \in \mathrm{Ker}(v) = \mathrm{Image}(u)$. Ceci entraîne qu'il existe $a \in A$ tel que $b = b' + u(a)$.
On calcule :

$$\begin{aligned} b - u \circ r(b) &= b' + u(a) - u \circ r(b' + u(a)) \\ &= b' + u(a) - u \circ r(b') - \underbrace{u \circ r \circ u}_{\mathrm{id}_A}(a) \\ &= b' - u \circ r(b') \end{aligned}$$

b) s est un homomorphisme :

$$\begin{aligned} s(c + c') &= s(v(b) + v(b')) = s(v(b + b')) = \\ &= b + b' - u \circ r(b + b') \\ &= b - u \circ r(b) + b' - u \circ r(b') \\ &= s(v(b)) + s(v(b')) \\ &= s(c) + s(c'). \end{aligned}$$

c) s est une section de v :

$$\begin{aligned} v \circ s(c) &= v \circ s(v(b)) = v(b - u \circ r(b)) = \\ &= v(b) - \underbrace{v \circ u}_{=0} \circ r(b) \\ &= v(b) = c \end{aligned}$$

2) Pour voir que B est isomorphe à $A \times C$, on construit un isomorphisme de B dans $A \times C$. En fait, on construit un homomorphisme de groupes $\varphi : B \to A \times C$ qui fait

commuter le diagramme suivant

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{u} & B & \xrightarrow{v} & C & \longrightarrow & 1 \\ & & \| & & \downarrow \varphi & & \| & & \\ 1 & \longrightarrow & A & \xrightarrow{i} & A\times C & \xrightarrow{p} & C & \longrightarrow & 1 \end{array}$$

avec : $i(a) = (a, 0)$, $p(a,c) = c$

Par le petit lemme des 5 (voir la série d'exercices) on obtient que φ est un isomorphisme.

Construction de $\varphi : B \longrightarrow A \times C$

$$b \longmapsto (r(b), v(b))$$

φ est clairement un homomorphisme de groupes.
De plus, les carrés commutent :

$$\varphi \circ u(a) = (\underbrace{r(u(a))}_{id_A}; \underbrace{v(u(a))}_{0}) = (a, 0) = i(a)$$

et $p \circ \varphi(b) = p(r(b), v(b)) = v(b)$

Donc φ est un isomorphisme. □

Application pour les groupes cyliques :

<u>Proposition</u> Si les entiers positifs m et n sont premiers entre eux alors $C_{mn} \cong C_m \times C_n$.

<u>Preuve</u> :

On a une suite exacte courte

$$1 \longrightarrow C_m \xrightarrow{u} C_{mn} \xrightarrow{v} C_n \longrightarrow 1$$

$$a \longmapsto b^n$$

$$b \longmapsto c$$

où $C_m = \langle a \rangle$, $C_{mn} = \langle b \rangle$ et $C_n = \langle c \rangle$

Il est clair que u est injective et v est surjective, de plus $\ker(v) = \langle b^n \rangle = \mathrm{Im}(u)$. Donc la suite est exacte.

Par le lemme technique, il suffit de construire une section de v.

Comme $(m,n)=1$, il existe $k, \ell \in \mathbb{Z}$ tels que $km + \ell n = 1$.

Soit $s : C_n \longrightarrow C_{mn}$ défini par $s(c) = b^{km}$, qui est bien un morphisme car $s(c^n) = b^{kmn} = 1$.

De plus, s est une section car

$$v \circ s(c) = v(b^{km}) = c^{km} = c^{1-\ell n} = c .$$

Donc, par le lemme technique, on a $C_{mn} = C_m \times C_n$.

Rem : Si $(m,n) = d \neq 1$ alors C_{mn} a un élément d'ordre d^2 donc $C_{mn} \neq C_m \times C_n$

Classification des groupes finis d'ordre m pour m premier ou $m \leq 4$

1) $m = 1 \Rightarrow G = \{1\}$

2) $m = p$ (p un nombre premier)
Tous les éléments de G différents de 1 sont d'ordre p et $g \in G \setminus \{1\}$ implique $|\langle g \rangle| = p$.
Donc $G \simeq C_p$

3) $m = 4$. Soit $G = \{1, a, b, c\}$.

cas 1 Si G a un élément g d'ordre 4 ; alors $|\langle g \rangle| = 4$ et donc $G \simeq \langle g \rangle$.
Il s'en suit que $G \simeq C_4$

cas 2 Si tous les éléments de G différents de 1 sont d'ordre 2 alors on a $a^2 = b^2 = c^2 = 1$

Que peut être $b \cdot c$. On essaye :

$$\left.\begin{array}{l} b \cdot c = b \Rightarrow c = 1 \text{ impossible} \\ b \cdot c = c \Rightarrow b = 1 \text{ impossible} \\ b \cdot c = 1 = c \cdot c \Rightarrow b = c \text{ impossible} \end{array}\right\} \Rightarrow \text{seule possibilité } bc = a$$

De même on obtient $cb = bc = a$

$ab = ba = c$

$ac = ca = b$

On se rappèle des exercices que ce groupe est appelé le groupe de Klein et il est isomorphe à $C_2 \times C_2$.