UE2 Groupes et Géométrie — Université de Nice
2019-2020

# AUTOMORPHISMES DE $\mathbb{Z}/n\mathbb{Z}$

*Références : Perrin, Cours d'Algèbre, pages* 24-26
*Serre, Cours d'arithmétique, PUF, Paris (*1970*), pages* 12-13.

*Leçons possibles :*
120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
104 : Groupes finis. Exemples et applications.

Soit $n$ un entier $\geq 2$. Si $s$ désigne un élément de $\mathbb{Z}$, nous notons $\overline{s}$ son image dans $\mathbb{Z}/n\mathbb{Z}$.

**Proposition 1.** *Soit $s \in \mathbb{Z}$. Les propriétés suivantes sont équivalentes :*
- *$s$ et $n$ sont premiers entre eux ;*
- *$\overline{s}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ ;*
- *$\overline{s}$ appartient au groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

*Démonstration.* D'après Bezout on a

$$\begin{aligned} s \text{ et } n \text{ sont premiers entre eux} &\iff \text{il existe } \lambda,\, \mu \in \mathbb{Z} \text{ tels que } \lambda s + \mu n = 1 \\ &\iff \text{il existe } \lambda \in \mathbb{Z} \text{ tel que } \overline{\lambda}\overline{s} = \overline{1} \text{ dans } \mathbb{Z}/n\mathbb{Z} \\ &\iff \overline{s} \in (\mathbb{Z}/n\mathbb{Z})^* \end{aligned}$$

D'autre part si $\lambda$ appartient à $\mathbb{Z}$, alors

$$\begin{aligned} \overline{\lambda}\overline{s} = \overline{1} &\iff \lambda\overline{s} = \overline{1} \\ &\iff \underbrace{\overline{s} + \overline{s} + \ldots + \overline{s}}_{\lambda \text{ fois}} = \overline{1} \\ &\iff \overline{1} \in \langle \overline{s} \rangle \\ &\iff \langle \overline{s} \rangle = \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

□

**Définition.** On appelle fonction d'Euler et on note $\varphi(n)$ le nombre d'entiers $m$ tels que

$$\begin{cases} 1 \leq m \leq n \\ m \text{ premier avec } n \end{cases}$$

D'après la Proposition 1 on a l'égalité

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$$

Par ailleurs si $p$ est premier il est clair que

$$\begin{cases} \varphi(p) = p-1 \\ \varphi(p^\alpha) = p^{\alpha-1}(p-1) \text{ pour un certain } \alpha \in \mathbb{N}^* \end{cases}$$

**Proposition 2.** *Les groupes* $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ *et* $(\mathbb{Z}/n\mathbb{Z})^*$ *sont isomorphes*

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

*En particulier* $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ *est un groupe abélien de cardinal* $\varphi(n)$.

*Démonstration.* Soit $\psi$ un élément de $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. Alors $\psi(1)$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ donc $\psi(1)$ appartient à $(\mathbb{Z}/n\mathbb{Z})^*$ (Proposition 1). On peut vérifier que

$$\tau \colon \psi \mapsto \psi(1)$$

est un homomorphisme.

Soit $\sigma$ défini sur $(\mathbb{Z}/n\mathbb{Z})^*$ par $\sigma(s)x = sx$. Comme $s(x+y) = sx + sy$ on a : $\sigma(s)$ est un endomorphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$. C'est un automorphisme puisque, $s$ étant inversible, $sx = 0$ entraîne $x = 0$.

On peut vérifier que $\sigma$ et $\tau$ sont réciproques l'un de l'autre. □

Précisons maintenant la structure de $(\mathbb{Z}/n\mathbb{Z})*$ suivant la décomposition en facteurs premiers de $n$. Pour ce faire rappelons le Lemme chinois :

**Proposition 3** (Lemme chinois)**.** *Si* $p$ *et* $q$ *sont premiers entre eux, alors*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

*Démonstration.* Soit $\overline{n}$, resp. $\widehat{n}$, resp. $\dot{n}$ la classe de $n$ modulo $pq$, resp. $p$, resp. $q$. Considérons l'homomorphisme

$$\mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}, \qquad \overline{n} \mapsto (\widehat{n}, \dot{n})$$

Il est injectif car $\mathrm{pgcd}(p,q) = 1$. On conclut grâce à l'égalité $|\mathbb{Z}/pq\mathbb{Z}| = |\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}|$. □

**Proposition 4.** *Soit* $n$ *un entier. Si* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ *où les* $p_i$ *désignent des entiers premiers distincts et les* $\alpha_i$ *des éléments de* $\mathbb{N}^*$*, alors on a*

- *un isomorphisme d'anneaux*

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

- *un isomorphisme de groupes*

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$$

- *et*

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

*Démonstration.* La première assertion résulte du Lemme chinois.

En passant aux éléments inversibles on obtient la seconde assertion.

Il en résulte la troisième assertion. □

Reste à déterminer la structure des $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ pour $p$ premier. Commençons par l'énoncé suivant :

**Lemme 5.** *Si $p$ est un nombre premier, alors*

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

**Remarque 6.** Si $d$ divise $n$, désignons par $C_d$ l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre $d$. Soit $\Phi_d$ l'ensemble des générateurs de $C_d$. Comme tout élément de $\mathbb{Z}/n\mathbb{Z}$ engendre l'un des $C_d$ le groupe $\mathbb{Z}/n\mathbb{Z}$ est réunion disjointe des $\Phi_d$ et

$$n = \#(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \#\Phi_d = \sum_{d|n} \varphi(d).$$

**Lemme 7.** *Soit $H$ un sous-groupe d'ordre fini $n$. Supposons que pour tout diviseur $d$ de $n$*

$$\#\big\{g \in H \,|\, g^d = 1\big\} \leq d.$$

*Alors $H$ est cyclique.*

*Démonstration.* Soit $d$ un diviseur de $n$. S'il existe $g \in H$ d'ordre $d$, alors le sous-groupe $\langle g\rangle = \{1, g, g^2, \ldots, g^{d-1}\}$ engendré par $g$ est cyclique d'ordre $d$. Étant donnée l'hypothèse tout élément $h$ de $H$ tel que $h^d = 1$ appartient à $\langle h\rangle$. En particulier les seuls éléments de $H$ d'ordre $d$ sont les générateurs de $\langle g\rangle$ et il y en a $\varphi(d)$. Si c'était 0 pour une valeur de $d$, alors $n = \sum_{d|n} \varphi(d)$ impliquerait $|H| < n$ : contradiction. En particulier il existe $g$ dans $H$ d'ordre $n$ et $H = \langle g\rangle$. □

*Démonstration du Lemme 5.* On applique le Lemme 7 à $H = (\mathbb{Z}/p\mathbb{Z})^*$ et $n = p-1$. Il est en effet clair que l'équation $x^d = 1$ qui est de degré $d$ a au plus $d$ solutions dans $\mathbb{Z}/p\mathbb{Z}$. □

Il faut ensuite distinguer les cas $p = 2$ et $p$ impair.

**Proposition 8.** *Si $p$ est un nombre premier $\geq 3$ et $\alpha$ un entier $\geq 2$, alors*

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^\alpha(p-1)\mathbb{Z}.$$

**Lemme 9.** *Si $k$ appartient à $\mathbb{N}^*$, alors $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ pour un certain $\lambda \in \mathbb{N}^*$ premier à $p$.*

*Démonstration.* Si $k = 1$, on a

$$(1+p)^p = 1 + \binom{p}{1}p + \ldots + \binom{p}{i}p^i + \ldots + p^p$$

et pour $1 \leq i < p$, $p$ divise $\binom{p}{i}$ donc pour $i \geq 2$ et $i < p$ $p^3$ divise $\binom{p}{i}p^i$ et comme $p \geq 3$ $p^3$ divise aussi $p^p$ de sorte que

$$(1+p)^p = 1 + p^2 + up^3 = 1 + p^2(1+up)$$

et $\lambda = 1 + up$ est bien premier à $p$.

Supposons que $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec $\lambda$ premier à $p$, alors

$$(1+p)^{p^{k+1}} = (1+\lambda p^{k+1})^p = 1 + \sum_{i=1}^{p-1} \binom{p}{i} \lambda^i p^{(k+1)i} + \lambda^p p^{(k+1)p}.$$

Si $i = 1$, on a $\lambda p^{k+2}$ et pour $i \geq 2$ $p^{k+3}$ est en facteur donc

$$(1+p)^{p^{k+1}} = 1 + p^{k+2}(\lambda + up).$$

□

*Démonstration de la Proposition 8.* D'après le Lemme 9 $1+p$ est un élément d'ordre $p^{\alpha-1}$ de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$. En effet

$$(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv 1 \bmod p^\alpha$$

et

$$(1+p)^{p^{\alpha-2}} = 1 + \lambda p^{\alpha-1}$$

avec $p \not| \lambda$ donc $(1+p)^{p^{\alpha-2}} \neq 1$ dans $\mathbb{Z}/p^\alpha\mathbb{Z}$.

Considérons l'homomorphisme surjectif naturel induit par l'identité de $\mathbb{Z}$ :

$$\psi \colon (\mathbb{Z}/p^\alpha\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$$

Soit $g$ un élément de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ qui engendre $\mathbb{Z}/(p-1)\mathbb{Z}$ (Lemme 5). L'ordre de $g$ est un multiple de $p-1$ et donc dans le groupe $\langle g \rangle$ il y a un élément $h$ d'ordre $p-1$. Mais comme $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est abélien, $h(1+p)$ est d'ordre $p^{\alpha-1}(p-1)$ en vertu du Lemme 9 et le groupe est cyclique. □

Il reste à traiter le cas $p = 2$ :

**Proposition 10.** *On a*

$$\begin{cases} (\mathbb{Z}/2\mathbb{Z})^* = \{1\} \\ (\mathbb{Z}/4\mathbb{Z})^* = \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z} \\ (\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \text{ pour } \alpha \geq 3 \end{cases}$$

**Remarque 11.** Le groupe $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ n'est donc pas cyclique dès que $\alpha \geq 3$.

**Lemme 12.** *Si $k$ désigne un élément de $\mathbb{N}^*$, alors $5^{2^k} = 1 + \lambda\, 2^{k+2}$ pour un certain $\lambda$ impair.*

*Démonstration.* Pour $k = 1$, on a d'une part $5^2 = 25$ et d'autre part $1 + 3 \times 2^3 = 25$.

Suppsons que $(5)^{2^k} = 1 + \lambda\, 2^{k+2}$. Alors

$$(5)^{2^{k+1}} = (1 + \lambda\, 2^{k+2})^2 = 1 + \lambda\, 2^{k+3} + \lambda^2\, 2^{2k+4} = 1 + \lambda(2 + \lambda\, 2^{k+2})\, 2^{k+2}.$$

□

*Démonstration de la Proposition 10.* Les cas 2 et 4 sont triviaux.

Traitons les autres, *i.e.* supposons que $\alpha \geq 3$. Considérons l'homomorphisme surjectif

$$\psi \colon (\mathbb{Z}/2^\alpha\mathbb{Z})^* \to (\mathbb{Z}/4\mathbb{Z})^* = \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

Posons $N = \ker \psi$. Alors $|N| = 2^{\alpha-2}$ et $5 \in N$ est d'ordre $2^{\alpha-2}$ (Lemme 12). Par suite $N$ est cyclique et on a la suite exacte

$$1 \longrightarrow \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \longrightarrow (\mathbb{Z}/2^\alpha\mathbb{Z})^* \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

D'autre part comme 1 et $-1$ ne sont pas égaux modulo 4, le sous-groupe $\{1, -1\}$ de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ fournit un relèvement de $\mathbb{Z}/2\mathbb{Z}$ de sorte que l'extension est scindée. Mais comme $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est abélien on a un produit direct :

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

□