Automorphisme de $\mathbb{Z}/n\mathbb{Z}$.

Référence : *Francinou-Gianella, Exercices de mathématiques pour l'agrégation, p7 (modification de la fin pour éviter les suites exactes)*

On a l'isomorphisme

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z}) \\ s & \longmapsto & x \mapsto sx \end{array}.$$

En notant $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, par le théorème chinois, on a

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times.$$

Théorème. *p premier impair, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} = \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.*
$(\mathbb{Z}/2\mathbb{Z})^\times \cong \{1\}$; $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$; $\alpha \geq 3, (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.

Démonstration.
- p impair.

Lemme. *$\forall k \in \mathbb{N}, \exists \lambda \in \mathbb{N}^*$, pgcd$(\lambda, p) = 1$, $(1+p)^{p^k} = 1 + \lambda p^{k+1}$.*

Démonstration. Par récurrence sur k.
$k = 0$, ok avec $\lambda = 1$.
$k \geq 1$. Par hypothèse de récurrence, il existe $\lambda \in \mathbb{N}^*$, pgcd$(\lambda, p) = 1$, $(1+p)^{p^{k-1}} = 1 + \lambda p^k$.

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

Or $\forall\ 1 \leq i \leq p-1,\ p \mid \binom{p}{i}$. Donc $\forall\ 2 \leq i \leq p-1,\ p^{k+2} \mid \binom{p}{i}\lambda^i p^{ki}$ et $p^{k+2} \mid p^{kp}$ car $p \geq 3$.

Ainsi

$$\begin{aligned} (1+p)^{p^k} &= 1 + \lambda p^{k+1} + hp^{k+2} \\ &= 1 + (\lambda + ph)p^{k+1} \end{aligned}$$

et on a bien pgcd$(\lambda + ph, p)$=pgcd(λ, p)=1.

□

Ainsi $\forall k \in \{1, \dots, \alpha-2\}, (1+p)^{p^k} = 1 + \lambda_k p^{k+1} \neq 1[p^\alpha]$ et $(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1}p^\alpha = 1[p^\alpha]$. $1+p$ est donc un élément d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique de cardinal $p-1$.
$id : \mathbb{Z} \longrightarrow \mathbb{Z}$ induit

$$\psi : \begin{array}{ccc} (\mathbb{Z}/p^\alpha\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ \bar{x} & \longmapsto & x \bmod p \end{array}.$$

ψ est clairement surjectif. Soit $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $\psi(y)$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Soit r l'ordre de y. On a $1 = \psi(1) = \psi(y^r) = \psi(y)^r$. Donc $p-1 \mid r$.

Comme pour tout $d \mid n$, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$, $\exists x \in < y >$ d'ordre $p-1$.

Enfin, comme $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est abélien, $x(1+p)$ est d'ordre $p^{\alpha-1}(p-1) = \left|(\mathbb{Z}/p^\alpha\mathbb{Z})^\times\right|$ car les ordres sont premiers entre eux. $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est donc cyclique et est isomorphe à $\mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} = \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

• $p = 2$.
$(\mathbb{Z}/2\mathbb{Z})^{\times} \cong \{1\}$ et $(\mathbb{Z}/4\mathbb{Z})^{\times} \cong \mathbb{Z}/2\mathbb{Z}$ sont clairs.
Désormais $\alpha \geq 3$.

Lemme. *$\forall\ k \in \mathbb{N}, \exists \lambda$ impair tel que $5^{2^k} = 1 + \lambda 2^{k+2}$.*

Démonstration. Par récurrence sur k.
$k = 0$ est clair : $5 = 1 + 2^2$.
$k \geq 1$. Par hypothèse de récurrence, il existe λ impair tel que $5^{2^{k-1}} = 1 + \lambda 2^{k+1}$. D'où

$$\begin{array}{rcl} 5 = \left(1 + \lambda 2^{k+1}\right)^2 & = & 1 + 2\lambda 2^{k+1} + \lambda^2 2^{2k+2} \\ & = & 1 + 2^{k+2}\underbrace{(\lambda + \lambda^2 2^k)}_{\text{impair}} \end{array} .$$

□

Ainsi, comme dans le premier cas, 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times}$.
Le groupe $< 5 >$ est d'indice 2 dans $(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times}$, il est donc distingué.
$-1 \notin < 5 >$. En effet, si $-1 \in < 5 >$, il existe $r \in \mathbb{N}$ tel que $-1 = 5^r\ [2^{\alpha}]$, i.e. $-1 = 5^r + \lambda 2^{\alpha}$, $\alpha \in \mathbb{Z}$. Cette égalité modulo 4 donne $1 = 3$ ce qui est manifestement faux.
Ainsi $< -1 > \cap < 5 >= \{1\}$ et $| < -1 > |.| < 5 > | = 2^{\alpha-1} = \left|(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times}\right|$.
On a donc

$$(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times} \cong \underbrace{< 5 >}_{\cong \mathbb{Z}/2^{\alpha-2}\mathbb{Z}} \rtimes \underbrace{< -1 >}_{\cong \mathbb{Z}/2\mathbb{Z}}.$$

Or $(\mathbb{Z}/2^{\alpha}\mathbb{Z})^{\times}$ est abélien donc le produit semi-direct est en fait direct.

□