# Structure de $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$, $p$ premier impair.

Florian DUSSAP

Agrégation 2018

**Lemme 1.** *Soit $p$ premier impair, alors pour tout $k \geqslant 1$, $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec $p \nmid \lambda$.*

*Démonstration.* Par récurrence sur $k$.

— Si $k = 1$, par le binôme de Newton :

$$(1+p)^p = 1 + p^2 + \sum_{i=2}^{p-1} \binom{p}{i} p^i + p^p$$

Or pour $i \in \{2, \dots, p-1\}$, $p$ divise $\binom{p}{i}$ donc $p^3$ divise $\binom{p}{i} p^i$. De plus, comme $p \geqslant 3$, $p^3$ divise $p^p$. Ainsi, $(1+p)^p = 1 + p^2 + up^3 = 1 + (1+up)p^2$.

— Supposons que $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ avec $p$ qui ne divise pas $\lambda$. Alors :

$$\begin{aligned}
(1+p)^{p^{k+1}} &= \left((1+p)^{p^k}\right)^p \\
&= \left(1 + \lambda p^{k+1}\right)^p \\
&= 1 + \lambda p^{k+2} + \sum_{i=2}^{p} \binom{p}{i} \lambda^i p^{i(k+1)} \\
&= 1 + \lambda p^{k+2} + up^{k+3} \\
&= 1 + (\lambda + up) p^{k+2}
\end{aligned}$$

Comme $p$ ne divise pas $\lambda$, alors $p$ ne divise pas $(\lambda + up)$.

□

**Lemme 2.** *Soit $G$ un groupe et soient $x$ et $y$ dans $G$ qui commutent, d'ordres respectifs $p$ et $q$, avec $p$ et $q$ premiers entre eux. Alors $xy$ est d'ordre $pq$.*

*Démonstration.* Comme $x$ et $y$ commutent, $(xy)^{pq} = x^p y^q = 1$ donc $xy$ est d'ordre fini $n$, et $n$ divise $pq$. Montrons que $pq$ divise $n$.

Puisque $1 = (xy)^n = x^n y^n$, en élevant à la puissance $q$, on obtient $1 = x^{nq}$. Donc $p$ divise $nq$. Or $p$ et $q$ sont premiers entre eux, donc $p$ divise $n$. De même, on en déduit que $q$ divise $n$. Ainsi, $p$ et $q$ divisent $n$, et $p$ et $q$ sont premiers entre eux, donc $pq$ divise $n$. □

**Théorème.** *Soit $p$ premier impair et soit $\alpha \geqslant 1$. Alors $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ est cyclique, isomorphe à $\mathbf{Z}/\varphi(p^\alpha)\mathbf{Z}$.*

*Démonstration.* Pour démontrer le théorème, il suffit de trouver un élément de $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ qui soit d'ordre $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Dans un premier temps, montrons que $(1+p)$ est d'ordre $p^{\alpha-1}$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$. En effet, d'après le lemme 1, on écrit $(1+p)^{p^{\alpha-1}} = 1 + \lambda p^\alpha \equiv 1 \pmod{p^\alpha}$. Donc $(1+p)$ est d'ordre $p^\beta$ avec $\beta \leqslant \alpha - 1$. Supposons par l'absurde que $\beta < \alpha - 1$. Alors on écrit $1 \equiv (1+p)^{p^\beta} = 1 + \mu p^{\beta+1}$ avec $p$ qui ne divise pas $\mu$. Ainsi, $p^\alpha$ devrait diviser $\mu p^{\beta+1}$. Puisque $\beta + 1 < \alpha$ et que $p$ ne divise pas $\mu$, c'est impossible. Donc $(1+p)$ est d'ordre $p^{\alpha-1}$.

Considérons $\pi : \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ la projection canonique. C'est un morphisme d'anneaux surjectif et on a l'inclusion $p^\alpha\mathbf{Z} \subseteq p\mathbf{Z} = \ker\pi$. Par le théorème de factorisation, on en déduit un morphisme d'anneaux surjectif $\mathbf{Z}/p^\alpha\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$. Celui-ci induit un morphisme de groupes surjectif $\psi : (\mathbf{Z}/p^\alpha\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$.

Comme $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique [1] d'ordre $p-1$ et que $\psi$ est surjectif, il existe $x \in (\mathbf{Z}/p^\alpha\mathbf{Z})^*$ tel que $\psi(x)$ soit d'ordre $p-1$ dans $(\mathbf{Z}/p\mathbf{Z})^*$. Notons $n$ l'ordre de $x$; alors $p-1$ divise $n$. En effet, $1 = \psi(x^n) = \psi(x)^n$ donc $n$ est divisible par l'ordre de $\psi(x)$, c'est-à-dire par $p-1$. Puisque $\langle x \rangle$ est cyclique d'ordre $n$ et que $p-1$ divise $n$, il existe un unique sous-groupe de $\langle x \rangle$ d'ordre $p-1$.

On considère $y$ un générateur de ce sous-groupe. Alors $y$ est d'ordre $p-1$. Par ailleurs, on avait montré que $(1+p)$ était d'ordre $p^{\alpha-1}$. D'après le lemme 2, $y(1+p)$ est d'ordre $p^{\alpha-1}(p-1)$ dans $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$.

□

# Référence

— PERRIN, *Cours d'algèbre*.

1. je mets ce résultat dans le plan, je ne le démontre pas dans le développement.