Classification des groupes d'ordre p^2

- Isenmann, Pecatte, *L'oral à l'agrégation de mathématiques.*

Lemme 1 : Soit G un groupe. Si $G/Z(G)$ est monogène, alors G est abélien.

Démonstration. Comme $G/Z(G)$ est monogène alors il existe $a \in G$ tel que $G/Z(G) = \langle \bar{a} \rangle$ où $\bar{a} = aZ(G)$. Soient $g, g' \in G$. Alors, il existe $k, k' \in \mathbb{N}$ tels que $\bar{g} = \bar{a}^k$ et $\bar{g'} = \bar{a}^{k'}$.
Comme les éléments de $Z(G)$ commutent alors $\bar{a}^k = a^k Z(G)$ et $\bar{a}^{k'} = a^{k'} Z(G)$.
Ainsi, il existe $h, h' \in Z(G)$ tels que $g = a^k h$ et $g' = a^{k'} h'$. Donc

$$gg' = a^k h a^{k'} h' = a^{k+k'} hh' = a^{k'+k} h'h = a^{k'} h' a^k h = g'g$$

Donc G est abélien. □

Lemme 2 : Soit p premier. Si G est un p-groupe alors $|Z(G)| \geqslant p$.

Démonstration.
On a $Z(G) = \{g \in G,\ \forall h \in G,\ gh = hg\} = \{g \in G,\ \forall h \in G,\ g = hgh^{-1}\}$.
Donc, $Z(G)$ est l'ensemble des points fixes de l'action $G \curvearrowright G$ par conjugaison.
L'orbite de $x \in Z(G)$ par cette action est $\{x\}$. D'autre part, si $x \notin Z(G)$ alors $|G \cdot x| > 1$ et donc $|G \cdot x| = \dfrac{|G|}{|G_x|} = 0\ [p]$ (car $G_x \leqslant G$ donc par Lagrange, on a $|G_x| \,|\, p^\alpha$ avec p premier). D'après l'équation des classes, on a

$$|G| = \sum_{x \in \mathcal{O}} |G \cdot x| = \sum_{\substack{x \in \mathcal{O} \\ x \in Z(G)}} |G \cdot x| + \sum_{\substack{x \in \mathcal{O} \\ x \notin Z(G)}} |G \cdot x| = |Z(G)|\ [p]$$

où $\mathcal{O}$ est un système de représentants.
Par conséquent, $|Z(G)| \equiv 0\ [p]$. Comme $|Z(G)| \geqslant 1$ (car $e \in Z(G)$) alors $|Z(G)| \geqslant p$.
Donc, $Z(G)$ admet un élément non trivial. □

Soit p premier. Si G est d'ordre p^2 alors G est abélien. De plus,

$$G \simeq \mathbb{Z}/p^2\mathbb{Z} \quad \text{ou} \quad G \simeq (\mathbb{Z}/p\mathbb{Z})^2$$

Démonstration. Par le théorème de Lagrange, $Z(G)$ est d'ordre un diviseur de p^2 ie 1, p ou p^2. D'après le lemme 2, $|Z(G)| \neq 1$.
- Si $|Z(G)| = p$ alors $G/Z(G)$ est d'ordre p. Tout élément différent du neutre est alors d'ordre p. Donc $G/Z(G)$ est monogène et d'après le lemme 1, G est abélien.
- Si $|Z(G)| = p^2$ alors $Z(G) = G$. Donc, G est abélien.

Finalement, G est abélien dans tous les cas. Montrons les équivalents.

- S'il existe $x \in G$ tel que l'ordre de x soit p^2.

Alors $G = \langle x \rangle$ est cyclique à p^2 éléments donc $G \simeq \mathbb{Z}/p^2\mathbb{Z}$.
- Sinon, tous les éléments de G sont d'ordre 1 ou p. Soit $x \in G$ d'ordre p. Posons $H = \langle x \rangle$.

Alors, $H \simeq \mathbb{Z}/p\mathbb{Z}$. Et comme $|H| < |G|$ alors il existe $y \in G \backslash \langle x \rangle$ également d'ordre p.
Posons alors $N = \langle y \rangle \simeq \mathbb{Z}/p\mathbb{Z}$. On a $N \lhd G$ et $H \lhd G$ (car G est abélien).
Et $N \cap H \leqslant H$ donc $|N \cap H| \in \{1, p\}$. L'inclusion est stricte car $x \in H$ et $x \notin N \cap H$.
D'où $|N \cap H| = 1$. Par conséquent, $N \cap H = \{e\}$.
L'ensemble NH est un groupe car G est abélien et $N \subset NH$ et $x = ex \in NH$.
Par conséquent, $|NH| \geqslant p + 1$. Or $|NH| \,|\, |G|$. D'où $|NH| = p^2$.
Ainsi, $G = NH$. Donc, par les propriétés du produit direct, $G \simeq N \times H \simeq (\mathbb{Z}/p\mathbb{Z})^2$. □