Théorème de la base de Burnside

Lemme . Soit G un p-groupe. Tout sous-groupe maximal H de G pour l'inclusion est distingué. On a alors $G/H \simeq \mathbb{Z}/p\mathbb{Z}$.

Preuve :
Soit H un sous-groupe maximal de G. On note $N := \{g \in G \; ; \; gH = Hg\}$ son normalisateur. H agit sur G/H par translation à gauche. La formule des classes donne

$$\left|G/H\right| = \left|(G/H)^H\right| + \sum_{|\mathrm{Orb}(gH)|>1} \left|\mathrm{Orb}(gH)\right|,$$

avec $(G/H)^H := \{gH \in G/H \; ; \; \forall h \in H, hgH = gH\}$ l'ensemble des points fixes de G/H sous l'action de H. Comme p divise $|G/H|$ et $|\mathrm{Orb}(gH)| > 1$, on a p divise $\left|(G/H)^H\right| \geq 1$ donc

$$\left|(G/H)^H\right| \geq p > 1.$$

On a

$$\left(G/H\right)^H = \{gH \in G/H \; ; \; \forall h \in H, hg = gH\} = \{gH \in G/H \; ; \; Hg = gH\} = N/H.$$

Donc

$$|N| = |H| \left|\left(G/H\right)^H\right| \geq p|H| > |H|.$$

Ainsi, $H \subsetneq N \subset G$. On conclut par la maximalité de H pour l'inclusion que $N = G$ et ainsi $H \lhd G$. Le théorème de correspondance entre les sous-groupes de G contenant H et ceux de G/H permet de conclure que $G/H \simeq \mathbb{Z}/p\mathbb{Z}$, car c'est un p-groupe sans sous-groupe propre, donc un p-groupe cyclique.

$\square$

Théorème . Les parties génératrices d'un p-groupe G minimales pour l'inclusion ont toutes même cardinal.

Preuve :
On note $\mathscr{M}$ l'ensemble des sous-groupes maximaux de G et on pose $\varphi(G) = \bigcap_{H \in \mathscr{M}} H$. D'après le lemme, chaque $H \in \mathscr{M}$ est distingué et contient $D(G)$, car G/H est abélien, donc $\varphi(G) \lhd G$ et $G/\varphi(G)$ est abélien. On commence par montrer le résultat sur $G/\varphi(G)$.

Pour $x, y \in G/\varphi(G)$ et $\lambda \in \mathbb{F}_p$, on pose

$$x \oplus y = xy \quad \text{et} \quad \lambda \otimes x = x^\lambda.$$

On a bien l'associativité des lois, la distributivité de $\otimes$ sur $\oplus$, et la commutativité de $\oplus$ car $G/\varphi(G)$ est abélien. Il faut vérifier que $p \otimes x = 0 \otimes x$. Soit $H \in \mathscr{M}$. On note $\sigma : G \to G/H$ la projection canonique. Alors pour tout $x \in G$ et en identifiant G/H à $\mathbb{Z}/p\mathbb{Z}$, on a $\sigma(x^p) = p\sigma(x) = 0$, ie

$x^p \in H$. Donc $p \otimes x = 0_{G/\varphi(G)}$, on a donc munit G d'une structure de $\mathbb{F}_p$-espace vectoriel. Une famille génératrice de G est alors une famille génératrice de ce $\mathbb{F}_p$-espace vectoriel, ce qui donne le résultat pour $G/\varphi(G)$.

Pour conclure dans le cas général, soit $(g_1, \ldots, g_n)$ une famille génératrice minimale de G. Alors $(\pi(g_1), \ldots, \pi(g_n))$ est une famille génératrice de $G/\varphi(G)$, avec $\pi : G \to G/\varphi(G)$. Si la famille est libre, c'est une base du $\mathbb{F}_p$-espace vectoriel $G/\varphi(G)$ et on a le résultat. Supposons par l'absurde que la famille est liée, par exemple $\pi(g_1) \in \langle \pi(g_2), \ldots, \pi(g_n) \rangle$. Alors il existe $\alpha_2, \ldots, \alpha_n$ tels que

$$\pi(g_1) = \pi(g_2)^{\alpha_2} \ldots \pi(g_n)^{\alpha_n} = \pi\left(g_2^{\alpha_2} \ldots g_n^{\alpha_n}\right).$$

En particulier, $g_1 y^{-1} \in \varphi(G)$, avec $y = g_2^{\alpha_2} \ldots g_n^{\alpha_n}$. Comme $(g_1, \ldots, g_n)$ génère G, $(g_1 y^{-1}, g_2, \ldots, g_n)$ génère G, car $g_1 = g_1 y^{-1} g_2^{\alpha_2} \ldots g_n^{\alpha_n} \in \langle g_1 y^{-1}, g_2, \ldots, g_n \rangle$. Or $(g_2, \ldots, g_n)$ ne génère pas G par hypothèse, donc

$$\text{il existe } H \in \mathscr{M} \text{ tel que } \langle g_2, \ldots, g_n \rangle \subset H.$$

Comme $g_1 y^{-1} \in \varphi(G) \subset H$, on a $\langle g_1 y^{-1}, g_2, \ldots, g_n \rangle \subset H \subsetneq G$, ce qui est absurde. Donc $n = \dim_{\mathbb{F}_p}(G/\varphi(G))$.

$\square$