6. Complément I : Groupes nilpotents finis

Soit G un groupe. Rappelons que pour $A, B \subset G$, on note $[A, B]$ le sous-groupe engendré par les commutateurs $aba^{-1}b^{-1}$ avec $a \in A$ et $b \in B$. On définit une suite de sous-groupes $\mathscr{C}^i(G)$ de G en posant $\mathscr{C}^0(G) = G$ puis, pour tout $i \geqslant 0$,

$$\mathscr{C}^{i+1}(G) = [G, \mathscr{C}^i(G)].$$

Définition 6.1. *Un groupe G est dit nilpotent s'il existe $i \geqslant 0$ avec $\mathscr{C}^i(G) = \{1\}$.*

Par exemple, on a $\mathscr{C}^1(G) = \mathrm{D}(G)$ (groupe dérivé de G). En revanche, le sous-groupe $\mathscr{C}^2(G) = [G, \mathrm{D}(G)]$ contient en général strictement $\mathrm{D}^2(G) = [\mathrm{D}(G), \mathrm{D}(G)]$.

Exemple 6.2. *Pour $G = \mathrm{S}_3$ on a $\mathrm{D}(G) = \mathrm{A}_3$, donc $\mathrm{D}^2(G) = \{1\}$, mais $\mathscr{C}^i(G) = \mathrm{A}_3$ pour tout $i \geqslant 1$. En particulier, le groupe résoluble S_3 n'est pas nilpotent.*

Comme pour les groupes dérivés, on constate que pour tout morphisme $f : G \to G'$ on a $f(\mathscr{C}^i(G)) \subset \mathscr{C}^i(G')$, avec égalité si f est surjectif. En particulier, on en déduit :

Proposition 6.3. *Pour tout $i \geqslant 0$, $\mathscr{C}^i(G)$ est un sous-groupe caractéristique (en particulier distingué) de G. De plus, on a $\mathscr{C}^i(G) \supset \mathscr{C}^{i+1}(G)$ et $\mathscr{C}^i(G) \supset \mathrm{D}^i(G)$ pour tout $i \geqslant 0$.*

Démonstration — Le premier point résulte de la remarque précédente appliquée aux automorphismes intérieurs de G. Pour le second, il suffit de voir que si H est distingué dans G, et $g \in G$, on a $[g, H] \subset H$. Mais cela vient de $[g, h] = (ghg^{-1})h^{-1}$. □

On en déduit que *nilpotent* implique *résoluble*, et que l'exemple de S_3 montre que la réciproque est fausse. Les groupes abéliens sont trivialement nilpotents. On vérifie immédiatement que les produits finis de groupes nilpotents sont nilpotents : on a $\mathscr{C}^i(G_1 \times G_2) = \mathscr{C}^i(G_1) \times \mathscr{C}^i(G_2)$.

Remarque 6.4. Un groupe nilpotent non trivial a un centre non trivial. En effet, soit i le plus petit entier $\geqslant 1$ tel que $\mathscr{C}^i(G) = \{1\}$. Si $i = 1$ alors G est abélien. Sinon, $\mathscr{C}^{i-1}(G) \neq \{1\}$ est inclus dans $\mathrm{Z}(G)$.

Les groupes nilpotents vérifient les propriétés de stabilité suivantes :

Proposition 6.5. *(i) Un sous-groupe d'un groupe nilpotent est nilpotent.*

(ii) Le quotient d'un groupe nilpotent par un sous-groupe distingué est nilpotent.

(iii) Si H est un sous-groupe central d'un groupe nilpotent G, et si G/H est nilpotent, alors G est nilpotent.

Démonstration — Si H est un sous-groupe de G, on constate $\mathscr{C}^i(H) \subset \mathscr{C}^i(G)$ pour tout $i \geqslant 0$. Cela montre le (i). Si $\pi : G \to G'$ est surjectif, on a déjà dit que $\pi(\mathscr{C}^i(G)) = \mathscr{C}^i(G')$. Cela montre le (ii) (prendre pour π la projection canonique). Cela montre aussi, dans le contexte du (iii), qu'il existe $i \geqslant 0$ tel que $\mathscr{C}^i(G) \subset H \subset \mathrm{Z}(G)$. On en déduit $\mathscr{C}^{i+1}(G) = \{1\}$. □

COROLLAIRE 6.6. *Les p-groupes sont nilpotents.*

DÉMONSTRATION — Soit P un p-groupe. On montre qu'il est nilpotent par récurrence sur $|P|$. On sait $\mathrm{Z}(P) \neq \{1\}$. Donc $P/\mathrm{Z}(P)$ est un p-groupe d'ordre $< |P|$. Par récurrence il est nilpotent, ainsi donc que P par la Proposition 6.5 (iii). □

En particulier, $\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$ est un groupe nilpotent. En fait, on a plus généralement (vérification laissée au lecteur) :

PROPOSITION 6.7. *Pour tout corps k, le sous-groupe $\mathrm{U}_n(k)$ de $\mathrm{GL}_n(k)$ est nilpotent.*

De manière un peu surprenante, les groupes nilpotents finis se ramènent aux p-groupes. Le théorème suivant est démontré par M. Hall dans son classique *The theory of Groups* (Chapitre 10 p.155), certaines des équivalences étant dues à Wielandt.

THÉORÈME 6.8. *Soit G un groupe fini. Il y a équivalence entre :*

(i) G est nilpotent,

(ii) pour tout sous-groupe strict H de G on a $H \subsetneq \mathrm{N}_G(H)$,

(iii) les sous-groupes maximaux de G sont distingués,

(iv) les p-Sylow de G sont distingués,

(v) G est produit direct de ses p-Sylow.

DÉMONSTRATION — On a déjà vu (iv) $\implies$ (i), car les p-groupes sont nilpotents et un produit fini de groupes nilpotents et nilpotent.

Montrons (i) $\implies$ (ii) par récurrence sur $|G|$. On peut supposer G non trivial. On sait alors que $Z := \mathrm{Z}(G)$ est non trivial. Soit H un sous-groupe strict de G. Si Z n'est pas inclus dans H, alors Z est un sous-groupe de $\mathrm{N}_G(H)$ non inclus dans H, ce qui conclut. Supposons donc Z est inclus dans H. Le sous-groupe H/Z de G/Z est strict, car H est strict dans G. Mais G/Z est nilpotent par la Proposition 6.5, donc par récurrence il existe $g \in G \smallsetminus H$ tel que gZ normalise H/Z. Mais cela signifie $gHg^{-1} \subset HZ = Z$, et donc $g \in \mathrm{N}_G(H) \smallsetminus H$.

L'implication (ii) $\implies$ (iii) est évidente. Montrons (iii) $\implies$ (iv). Soit P un p-Sylow de G. Si P n'est pas distingué dans G, alors son normalisateur $\mathrm{N}_G(P)$ est strict, et s'inclut donc dans un sous-groupe maximal M de G. Par (ii), M est distingué. De plus P est clairement un p-Sylow de M. On a donc $G = M\mathrm{N}_G(P)$ par le Lemme de Frattini, puis $G \subset M$: absurde.

Montrons enfin (iv) $\implies$ (v). Écrivons $|G| = \prod_{i=1}^n p_i^{\alpha_i}$ la décomposition en facteurs premiers de $|G|$. Soit P_i un p_i-Sylow de G. Soient i et j distincts. On a $P_i \cap P_j = \{1\}$ par Lagrange. Pour $x \in P_i$ et $y \in P_j$ on a (« deux façons de voir un commutateur ») $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} = x(yxy^{-1}) \in P_i \cap P_j = \{1\}$ et donc $xy = yx$. On en déduit que l'application

$$\varphi : \prod_{i=1}^n P_i \to G, (x_1, \ldots, x_n) \mapsto x_1 x_2 \cdots x_n,$$

est un morphisme de groupes. Son image contient P_i pour tout i. On a donc $p_i^{\alpha_i} \mid |\mathrm{Im}\,\varphi|$ pour tout i, puis $\mathrm{Im}\,\varphi = G$, et donc $\ker\varphi = \{1\}$: c'est un isomorphisme. □

COROLLAIRE 6.9. *Dans un groupe nilpotent fini, deux éléments x et y d'ordres premiers entre eux commutent.*

DÉMONSTRATION — En effet, par le théorème on peut supposer que notre groupe nilpotent fini est produit direct d'un nombre fini de p-groupes P_i, disons $i = 1, \dots, r$, avec les $|P_i|$ premiers entre eux. Soit $x = (x_1, \dots, x_r)$ dans $\prod_{i=1}^r P_i$. Si x est d'ordre a, on a $x_i^a = 1$ pour tout i, et donc $x_i = 1$ pour $(a, |P_i|) = 1$. Ainsi, si x et y sont d'ordres premiers entre eux, alors pour tout i on a soit $x_i = 1$, soit $y_i = 1$, et on a donc bien $xy = yx$. □

COROLLAIRE 6.10. *Soient G un groupe nilpotent fini, ainsi que $P_1, \dots, P_n$ ses sous-groupes de Sylow (distingués). On a un isomorphisme de groupes*

$$\mathrm{Aut}(G) \ \simeq \ \prod_{i=1}^{n} \mathrm{Aut}(P_i).$$

DÉMONSTRATION — En effet, comme chaque p-Sylow de G est distingué, il est aussi caractéristique (unique sous-groupe ayant l'ordre en question), de sorte que l'application $\mathrm{Aut}(G) \to \prod_{i=1}^n \mathrm{Aut}(P_i), \varphi \mapsto (\varphi_{|P_i})$, est bien définie. C'est clairement un morphisme de groupes. Comme G est produit direct interne des P_i par le Théorème 6.8, il est manifestement injectif et surjectif, donc bijectif. □

7. Complément II : La caractérisation de Burnside-Dickson-Pazderski

Dans ce complément, qui fait suite au précédent, on se propose de prouver le théorème suivant, démontré dans G. Pazderski, *Die Ordnungen, zu denen nur Gruppen mit gegebener Eigenschaft gehören*, Arch. Math., 10, 331–343 (1959). Un entier n sera dit *nilpotent* si sa décomposition en facteurs premiers $n = \prod_{i=1}^r {p_i}^{k_i}$, avec les p_i distincts, est telle que pour tout $i \neq j$, et tout $1 \leqslant k \leqslant k_j$, p_i ne divise pas $p_j^k - 1$.

THÉORÈME 7.1. (Pazderski) *L'entier $n \geqslant 1$ est nilpotent si, et seulement si, tout groupe d'ordre n est nilpotent.*

L'exposition qui suit est inspirée de notes d'un cours de N. Tosel (1995). Montrons d'abord que si tout groupe d'ordre n est nilpotent alors n est nilpotent.

LEMME 7.2. *Soient p et q deux nombres premier, et $k \geqslant 1$, avec $q \mid p^k - 1$. Alors il existe un groupe non nilpotent d'ordre $p^k q$.*

DÉMONSTRATION — Posons $P = (\mathbb{Z}/p\mathbb{Z})^k$. C'est un groupe abélien p-élémentaire. Son groupe d'automorphisme coïncide donc avec celui du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel associé, ce qui démontre $\mathrm{Aut}(P) = \mathrm{GL}_k(\mathbb{Z}/p\mathbb{Z})$. De la formule pour $|\mathrm{GL}_k(\mathbb{Z}/p\mathbb{Z})|$, on déduit que le cardinal de $\mathrm{Aut}(P)$ est multiple de $p^k - 1$. Par hypothèse, on en déduit que q divise $|\mathrm{Aut}(P)|$ et donc qu'il existe un morphisme injectif $\varphi : \mathbb{Z}/q\mathbb{Z} \to \mathrm{Aut}(P)$. Considérons le produit semi-direct associé $G = (\mathbb{Z}/p\mathbb{Z})^k \rtimes_\varphi \mathbb{Z}/q\mathbb{Z}$. Il est d'ordre $p^k q$. S'il était nilpotent, son unique p-Sylow serait $P' = P \times \{0\}$, et son unique q-Sylow serait $Q' = \{0\} \times \mathbb{Z}/q\mathbb{Z}$, et on aurait $ab = ba$ pour tout $a \in P'$ et $b' \in Q'$. C'est absurde car l'action de Q' par conjugaison sur P' est donnée par φ, donc non triviale. □

COROLLAIRE 7.3. *Si tout groupe d'ordre n est nilpotent, alors n est nilpotent.*

DÉMONSTRATION — En effet, si on a p_i, q_i et $1 \leqslant k \leqslant k_i$ avec $q_i \mid p_i^k - 1$, et si G est non nilpotent d'ordre $p_i^k q_i$ (par le lemme), alors $G \times \mathbb{Z}/m\mathbb{Z}$ avec $m = n/(p_i^k q_i)$ est non nilpotent d'ordre n (Proposition 6.5). □

La réciproque est plus délicate et nécessitera plusieurs étapes. On commence par montrer la proposition suivante, qui généralise au cas nilpotent (plutôt qu'abélien) le Problème 2 du partiel 2021-2022 (voir §1 App. B).

PROPOSITION 7.4. (Non simplicité d'un groupe non nilpotent minimal) *Soit G un groupe fini non nilpotent dont tous les sous-groupes stricts sont nilpotents. Alors G n'est pas simple.*

La démonstration repose sur un examen des sous-groupes maximaux de G. Pour G fini on notera $\mathscr{M}(G)$ l'ensemble des sous-groupes $\{1\} \subsetneq M \subsetneq G$ maximaux pour l'inclusion.

LEMME 7.5. *On suppose G fini simple non cyclique. Alors il existe $A, B \in \mathscr{M}(G)$ avec $A \neq B$ et $A \cap B \neq \{1\}$.*

DÉMONSTRATION — [4] Comme G n'est pas cyclique, observons que pour tout $g \in G \smallsetminus \{1\}$ on a $\{1\} \subsetneq \langle g \rangle \subsetneq G$, et donc il existe $M \in \mathscr{M}(G)$ avec $g \in M$. En particulier, l'ensemble $\mathscr{M}(G)$ est non vide.

Le groupe G agit sur $\mathscr{M}(G)$ par conjugaison. Observons que le stabilisateur dans G d'un $M \in \mathscr{M}(G)$ coïncide avec M. En effet, ce stabilisateur est $\mathrm{N}_G(M)$, contient M, et vaut donc M ou G par maximalité de M. Mais on a $M \neq \{1\}$ et $M \lhd \mathrm{N}_G(M)$, et donc $\mathrm{N}_G(M) = M$ par simplicité de G.

Supposons par l'absurde que le seul élément de G agissant sur $\mathscr{M}(G)$ avec au moins deux points fixes est l'identité. D'après l'Exercice 5.10, le groupe G agit transitivement sur $\mathscr{M}(G)$. D'après le lemme de Jordan (Exercice 5.9 (ii)), il existe alors $g \in G$ sans point fixe dans $\mathscr{M}(G)$, autrement dit n'appartenant à aucun sous-groupe maximal de G, en contradiction avec le premier paragraphe. □

DÉMONSTRATION — (de la Proposition 7.4). Supposons G simple. D'après le Lemme 7.5, il suffit de montrer que pour tout $A, B \in \mathscr{M}(G)$, on a $A \cap B = \{1\}$ ou $A = B$. Considérons $\{A, B\} \subset \mathscr{M}(G)$ avec $A \neq B$ et $|A \cap B|$ maximal, et supposons par l'absurde $A \cap B \neq \{1\}$. Posons $H = \mathrm{N}_G(A \cap B)$; on a $H \neq G$, car G est simple, et $H \neq \{1\}$ car $A \cap B \neq \{1\}$. On peut donc choisir $C \in \mathscr{M}(G)$ contenant H. Quitte à échanger les rôles de A et B on peut supposer $C \neq A$, car on a $A \neq B$. On constate

$$C \cap A \supset \mathrm{N}_G(A \cap B) \cap A = \mathrm{N}_A(A \cap B).$$

Mais $A \cap B = A$ implique $A \subset B$, une contradiction, donc $A \cap B$ est un sous-groupe strict du groupe nilpotent A. On en déduit $\mathrm{N}_A(A \cap B) \supsetneq A \cap B$ par le Théorème 6.8 (ii), puis $C \cap A \supsetneq B \cap A$ et $C \neq A$, contredisant la maximalité de $|A \cap B|$. □

4. La preuve ci-dessous est une variante de celle donnée dans le corrigé des questions (iv) à (viii) du Problème 2 du partiel 2021-2022, Sect. 6 App. B, utilisant les Exercices 5.9 et 5.10.

Démonstration — (du Théorème 7.1) D'après le Corollaire 7.3, il ne reste qu'à montrer que si n est nilpotent, alors tout groupe d'ordre n est nilpotent. On procède par récurrence sur l'entier nilpotent $n \geqslant 1$. Soit G d'ordre n. Tout diviseur de n étant encore nilpotent par définition, on en déduit par Lagrange et par récurrence que tout sous-groupe strict de G, et tout quotient strict de G, est nilpotent. Par la Proposition 7.4, on peut supposer que G n'est pas simple. On se donne H distingué dans G avec $1 < |H| < |G|$. On va utiliser ce H pour montrer $\mathrm{Z}(G) \neq \{1\}$ aux Faits 2 et 3 ci-dessous. Cela concluera car cela montre que $G/\mathrm{Z}(G)$ est nilpotent par récurrence, puis que G est nilpotent par la Proposition 6.5.

Fait 1 : *G possède un p-Sylow distingué.* Soient p premier divisant $|H|$ et P un p-Sylow de H. Comme H est nilpotent, P est l'unique p-Sylow de H. Il est donc caractéristique dans H, puis distingué dans G. Si P est un p-Sylow de G on a gagné. Sinon, on regarde G/P. Il est nilpotent et d'ordre mutiple de p, donc possède un p-Sylow distingué P' par récurrence. Mais alors on a $P' = Q/P$ avec Q un p-Sylow de G, ce qui conclut.

Fait 2 : *G possède un sous-groupe abélien p-élémentaire non trivial et distingué.* En effet, soit P un p-Sylow distingué de G (Fait 1). Alors $\mathrm{Z}(P)$ est non trivial, distingué dans P, et son sous-groupe caractéristique $\{x \in \mathrm{Z}(P) \mid x^p = 1\}$ convient.

Fait 3 : *Soit A un sous-groupe abélien p-élémentaire non trivial et distingué dans G, on a $A \subset \mathrm{Z}(G)$.* On a $A \simeq (\mathbb{Z}/p\mathbb{Z})^m$ pour un certain $m \geqslant 1$. Soient $\ell \neq p$ divisant $|G|$ et S un ℓ-Sylow de G. On regarde l'action naturelle de S par conjugaison sur A. Elle induit un morphisme $S \to \mathrm{Aut}(A)$. Mais $|S|$ est une puissance de ℓ et on a $|\mathrm{Aut}(A)| = |\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})| = p^{m(m-1)/2} \prod_{1 \leqslant i < m} (p^i - 1)$. Comme n est nilpotent (enfin !), et que p^m et ℓ sont des diviseurs de $n = |G|$, on a $(|S|, |\mathrm{Aut}(A)|) = 1$ et tout morphisme $S \to \mathrm{Aut}(A)$ est trivial. Ainsi, S agit trivialement par conjugaison sur A, et donc S est inclus dans le centralisateur $\mathrm{C}_G(A)$ de A dans G. Ainsi, $\mathrm{C}_G(A)$ contient P (car $A \subset \mathrm{Z}(P)$) et tous les ℓ-Sylow de G avec $\ell \neq p$. Il est donc d'ordre n par Lagrange, et on a $\mathrm{C}_G(A) = G$, *i.e.* $A \subset \mathrm{Z}(G)$. □

Donnons deux corollaires historiquement bien antérieurs au théorème précédent.

Corollaire 7.6. (Dickson) *Soit $n \geqslant 1$ un entier. Tout groupe d'ordre n est abélien si, et seulement si, l'entier n est nilpotent et sans facteur cube.* [5]

Démonstration — Supposons que tout groupe d'ordre n est abélien. Supposons $n = p^3 m$ avec p premier. Alors $\mathrm{U}_3(\mathbb{Z}/p\mathbb{Z}) \times \mathbb{Z}/m\mathbb{Z}$ est d'ordre n, donc abélien : absurde. Réciproquement, supposons n nilpotent sans facteur cube. Soit G d'ordre n. Alors G est nilpotent par le Théorème 7.1, et donc produit fini de p-groupes par le Théorème 6.8. Mais un p-groupe d'ordre p ou p^2 est abélien, donc G est abélien. □

Corollaire 7.7. (Burnside) *Soit $n \geqslant 1$ un entier. Il y a équivalence entre :*

(i) Tout groupe d'ordre n est cyclique,

(ii) l'entier n est nilpotent sans facteur carré,

(iii) n est premier à $\varphi(n)$.

5. Autrement dit, si p divise n alors p^3 ne divise pas n.

Démonstration — Supposons que tout groupe d'ordre n est cyclique. Supposons $n = p^2m$ avec p premier. Alors $(\mathbb{Z}/p\mathbb{Z})^2 \times \mathbb{Z}/m\mathbb{Z}$ est d'ordre n, donc cyclique : absurde car il est annulé par $pm < n$. On a montré (i) $\Longrightarrow$ (ii). Réciproquement, supposons n nilpotent sans facteur carré. On a donc $n = p_1 \dots p_r$ avec les p_i distincts. Soit G d'ordre n. Alors G est abélien par le Corollaire 7.6. Si $x_i \in G$ est d'ordre p_i, alors $x_1 \dots x_r$ est donc d'ordre $p_1 \dots p_r = n$ (Cauchy), et G est cyclique. On a montré (ii) $\Longrightarrow$ (i). L'équivalence entre (ii) et (iii) vient de la formule $\varphi(\prod_{i=1}^r p_i^{m_i}) = \prod_{i=1}^r (p_i - 1)p_i^{m_i - 1}$, où les p_i sont des premiers distincts. □

8. Complément III : Générateurs et automorphismes d'un p-groupe

Dans ce complément, on se propose détudier, suivant Burnside et P. Hall, les systèmes de générateurs et le groupe d'automorphisme d'un p-groupe. On fixe donc p premier. On a déjà dit que les systèmes de générateurs du groupe $V = (\mathbb{Z}/p\mathbb{Z})^n$ coïncident avec ceux de l'espace vectoriel $V^\sharp$ sur $\mathbb{Z}/p\mathbb{Z}$, et on a aussi déjà vu et utilisé $\mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^n) \simeq \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Commençons par étudier les systèmes minimaux de générateurs d'un p-groupe général, suivant Frattini et Burnside.

Définition 8.1. *Le sous-groupe de Frattini d'un groupe fini G est l'intersection des sous-groupes maximaux de G. C'est un sous-groupe caractéristique de G noté $\Phi(G)$, et le quotient $G/\Phi(G)$ s'appelle aussi quotient de Frattini de G.*

On a donc $\Phi(G) = \cap_M M$ où M parcourt les sous-groupes maximaux de G. Noter que si $\varphi : G \to G$ est un automorphisme, et si $M \subset G$ est maximal, alors le sous-groupe $\varphi(M)$ est encore maximal. Ainsi, φ permute l'ensemble fini des sous-groupes maximaux de G et on a bien $\varphi(\Phi(G)) = \Phi(G)$, comme affirmé ci-dessus.

Exemple 8.2.
(i) Les sous-groupes maximaux de $(\mathbb{Z}/p\mathbb{Z})^n$ sont les hyperplans vectoriels du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel associé. L'intersection de ces hyperplans est nulle : on a donc $\Phi((\mathbb{Z}/p\mathbb{Z})^n) = \{0\}$.
(ii) Les sous-groupes maximaux de H_8 sont $\langle I\rangle, \langle J\rangle$ et $\langle K\rangle$. On a donc $\Phi(\mathrm{H}_8) = \{\pm 1\}$.
(iii) Pour $G = \mathrm{S}_n$, on peut montrer que chacun des sous-groupes $\simeq \mathrm{S}_{n-1}$ obtenus en fixant l'un des points de $\{1, \dots, n\}$ est maximal (observer qu'il agit transitivement sur le complémentaire du point). On a donc encore $\Phi(\mathrm{S}_n) = \{1\}$.

En plus de fournir un sous-groupe distingué naturel, l'intérêt majeur du sous-groupe de Frattini est sa propriété suivante d'être « non-générateur » :

Proposition 8.3. (Frattini) *Soit X un sous-ensemble de G. On a $\langle X\rangle = G$ si, et seulement si, $\langle X, \Phi(G)\rangle = G$. En particulier, X engendre G si, et seulement si, son image dans $G/\Phi(G)$ engendre $G/\Phi(G)$.*

Démonstration — Il est clair que $\langle X\rangle = G$ implique $\langle X, \Phi(G)\rangle = G$. Supposons donc $\langle X, \Phi(G)\rangle = G$. Si $\langle X\rangle$ est un sous-groupe strict de G (un groupe fini), alors il s'inclut dans un sous-groupe maximal M de G. On a donc $\langle X\rangle \subset M$. Mais on a aussi $\Phi(G) \subset M$ par définition. On a donc $\langle X, \Phi(G)\rangle M$: une contradiction. Enfin, si la projection canonique $\langle X\rangle \to G/\Phi(G)$ est surjective, alors on a $\langle X, \Phi(G)\rangle = G$ (pourquoi ?), et donc $\langle X\rangle = G$. □

COROLLAIRE 8.4. *Les groupes G et $G/\Phi(G)$ on même nombre minimal de générateurs.*

Le résultat suivant est appellé *théorème de la base* de Burnside.

THÉORÈME 8.5. (Burnside) *Si P est un p-groupe et si r est le nombre minimal de générateurs de P, alors on a $P/\Phi(P) \simeq (\mathbb{Z}/p\mathbb{Z})^r$.*

DÉMONSTRATION — Le nombre minimal de générateurs de $(\mathbb{Z}/p\mathbb{Z})^r$ est r comme on l'a déjà vu (Proposition 3.7 Chap. 3). D'après le Corollaire 8.4, il suffit donc de démontrer que $P/\Phi(P)$ est abélien p-élémentaire. Mais si M est un sous-groupe maximal de P, on a vu que M est distingué dans P, et que l'on a $P/M \simeq \mathbb{Z}/p\mathbb{Z}$. On en déduit donc $\mathrm{D}(P) \subset M$ (car P/M est abélien) et aussi $g^p \subset M$ pour tout $g \in P$. Comme c'est vrai pour tout M maximal, on a donc $\mathrm{D}(P) \subset \Phi(P)$, *i.e.* $P/\Phi(P)$ est abélien, et $g^p \in \Phi(P)$ pour tout $g \in P$, et donc $P/\Phi(P)$ est p-élémentaire. □

Soit P un p-groupe. Comme $\Phi(P)$ est caractéristique dans P, le groupe P agit naturellement sur $\Phi(P)$ et $P/\Phi(P)$ par automorphismes de groupes, de sorte qu'on a une suite exacte naturelle

$$1 \to \mathrm{I}(P) \to \mathrm{Aut}(P) \to \mathrm{Aut}(P/\Phi(P)),$$

où $\mathrm{I}(P)$ est par définition le sous-groupe de $\mathrm{Aut}(P)$ agissant trivialement sur $P/\Phi(P)$. Attention, nous n'avons pas mis de 1 à droite, de sorte que nous n'affirmons pas du tout que le morphisme de droite est surjectif. Choisissons un isomorphisme $P/\Phi(P) \simeq (\mathbb{Z}/p\mathbb{Z})^r$ avec r le nombre minimal de générateurs de P, on a alors $\mathrm{Aut}(P/\Phi(P)) \simeq \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$, un groupe familier. Il ne reste qu'à étudier $\mathrm{I}(P)$.

PROPOSITION 8.6. (P. Hall) *Pour tout p-groupe P, le groupe $\mathrm{I}(P)$ est un p-groupe.*

DÉMONSTRATION — Si $\mathrm{I}(P)$ n'est pas un p-groupe, alors il possède par Cauchy un sous-groupe $H = \langle\varphi\rangle$ d'ordre premier $\ell \neq p$. Comme H est inclus $\mathrm{I}(P)$, il préserve par définition chaque partie de P de la forme $g\Phi(P)$ avec $g \in P$. Fixons $X = g\Phi(P)$ une telle partie. On a $|X| = |\Phi(P)|$, qui est une puissance de p, et donc un entier premier à ℓ. D'après la Proposition 1.3 appliquée au ℓ-groupe H agissant sur X, on en déduit que H admet un point fixe dans X. On peut donc choisir des représentants $g_1, \ldots, g_s$ des classes à gauche de $\Phi(P)$ dans P qui sont chacun point fixe de φ. Mais $g_1, \ldots, g_s$ engendrent évidemment $P/\Phi(P)$ car on a

$$P/\Phi(P) = \{g_i\Phi(P) \mid i = 1, \ldots, s\},$$

donc on a $P = \langle g_1, \ldots, g_s\rangle$ par la Proposition 8.3. On en déduit $\varphi(g) = g$ pour tout $g \in P$, et $\varphi = \mathrm{id}_P$, une contradiction. □

EXEMPLE 8.7. Si $P = (\mathbb{Z}/p^2\mathbb{Z})^n$, alors on peut montrer $\mathrm{Aut}(P) = \mathrm{GL}_n(\mathbb{Z}/p^2\mathbb{Z})$ et que $\mathrm{I}(P)$ s'identifie aux sous-groupe A de $\mathrm{GL}_n(\mathbb{Z}/p^2\mathbb{Z})$ constitué des matrices de la forme $\mathrm{I}_n + p\mathrm{M}_n(\mathbb{Z}/p^2\mathbb{Z})$. Il y en a bien une puissance de p. En fait, on a $(1+pa)(1+pb) = 1+p(a+b)$ pour $a, b \in \mathrm{M}_n(\mathbb{Z}/p^2\mathbb{Z})$, de sorte que ce groupe A est isomorphe à $(\mathrm{M}_n(\mathbb{Z}/p\mathbb{Z}), +)$.