Prérequis. Sous-groupe dérivé.

Théorème 0.0.1. *Les parties génératrices minimales d'un p-groupe fini G ont toutes le même cardinal.*

Démonstration. On commence par le lemme suivant.

Lemme 0.0.2. *Tout sous-groupe maximal $H < G$ est distingué, et le quotient G/H est cyclique d'ordre p.*

Démonstration. On pose $N = \{g \in G \mid gH = Hg\}$ le normalisateur de H. C'est un sous-groupe de G, il suffit de montrer que $N = G$ pour avoir le résultat. Comme N contient H, il suffit en fait de montrer que $|N| > |H|$ puisque H est maximal.

Le sous-groupe H agit sur l'ensemble G/H par translation à gauche. La formule des classes s'écrit :

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

Comme p divise le membre de gauche et la somme à droite, on a $\left|(G/H)^H\right| \geqslant p > 1$. Or,

$$(G/H)^H = \{gH \in G/H \mid \forall h \in H,\ hgH = gH\} = \{gH \mid Hg = gH\} = N/H.$$

Donc $|N| = |H|\left|(G/H)^H\right| > |H|$, comme voulu. $\square$

Notons $\mathcal{M}$ l'ensemble des sous-groupes maximaux de G et $\Phi(G) = \bigcap_{H\in\mathcal{M}} H$. D'après le lemme, pour tout $H \in \mathcal{M}$ on a $H \lhd G$ et G/H est alors un groupe d'ordre p, c'est-à-dire C_p, donc il est abélien, d'où $H \supset DG$. Ainsi, $\Phi(G)$ est distingué dans G et contient DG donc $G/\Phi(G)$ est un groupe abélien.

On montre alors le résultat d'abord sur $G/\Phi(G)$ qui est un p-groupe élémentaire : pour $x, y \in G/\Phi(G)$ et $\lambda \in \mathbf{F}_p$, on pose :

$$x \oplus y = xy, \qquad \lambda \otimes x = x^\lambda.$$

Pour vérifier que la multiplication est bien définie, il faut vérifier que $p \otimes x = 0$. Mais si x' est un représentant de x, $H \in \mathcal{M}$ et $\pi : G \to G/H$ est la projection, on a $\pi(x'^p) = p\pi(x') = 0$ car G/H est cyclique d'ordre p. Ainsi $x'^p \in H$ pour tout H donc $x'^p \in \Phi(G)$, d'où $p \otimes x = 0$.

Ces opérations munissent $G/\Phi(G)$ d'une structure de $\mathbf{F}_p$-espace vectoriel de dimension finie, dont les bases sont exactement les parties génératrices minimales de $G/\Phi(G)$. Cela démontre le résultat.

Démonstration dans le cas général. Soit $(g_1, \ldots, g_n)$ une partie génératrice de G minimale (qui existe car G est fini). Alors en notant $\pi : G \to G/\Phi(G)$ la projection, la famille $(\pi(g_1), \ldots, \pi(g_n))$ est génératrice de $G/\Phi(G)$. Il suffit de montrer qu'elle est libre, puisqu'alors toutes les parties génératrices minimales de G auront pour cardinal la dimension de $G/\Phi(G)$.

Si cette famille était liée, disons $\pi(g_1) = \pi(g_2)^{\alpha_2} \cdot \ldots \cdot \pi(g_n)^{\alpha_n}$, alors on aurait $g_1 y^{-1} \in \Phi(G)$ après avoir posé $y = g_2^{\alpha_2} \cdot \ldots \cdot g_n^{\alpha_n}$. La famille $(g_1 y^{-1}, g_2, \ldots, g_n)$ est alors encore une partie génératrice de G (car $g_1 = g_1 y^{-1} y$ et $y \in \langle g_2, \ldots, g_n \rangle$). Or, $(g_2, \ldots, g_n)$ n'est pas une partie génératrice (par minimalité) donc il existe $H \in \mathcal{M}$ tel que $\langle g_2, \ldots, g_n \rangle \subset H$. Et puisque $g_1 y^{-1} \in \Phi(G) \subset H$, la famille $(g_1 y^{-1}, g_2, \ldots, g_n)$ ne peut pas générer un sous-groupe plus grand que H... □

Remarques.

— Le lemme utilise la même technique de réduction d'une équation aux classes modulo p que ce qu'on fait quand on montre que le centre d'un p-groupe fini n'est jamais trivial. C'est bien de savoir faire ce parallèle.

— On peut dire à l'oral que $G/\Phi(G)$ est un p-groupe élémentaire, c'est-à-dire que tous les éléments sont de puissance p triviale. On utilise le même argument de $\mathbf{F}_p$-espace vectoriel quand on dit que les groupes dans lesquels tout élément est de carré trivial sont isomorphes à un C_p^n.

— Le sous-groupe $\Phi(G)$ est assez important en théorie des groupes, on l'appelle le *sous-groupe de Frattini* de G. Il est toujours caractéristique dans G, et on peut le voir comme l'ensemble des éléments superflus de G (les éléments qui peuvent être retirés de toute partie génératrice). D'ailleurs la partie où l'on montre que $G/\Phi(G) \cong \mathbf{F}_p^n$ s'appelle le *théorème de Frattini*.

— Il est important de connaître des exemples et des contre-exemples pour accompagner ce théorème. Par exemple, le groupe quaternionique Q_8 est un 2-groupe fini, ses parties génératrices minimales sont de cardinal 2 (par exemple, (i, j)). Le groupe symétrique $\mathfrak{S}_n$ avec $n \geqslant 3$ n'est pas un p-groupe, et il a des parties génératrices minimales de cardinaux différents (par exemple, $((1\ 2), (1\ 2\ \ldots\ n))$ et $((i\ i+1))_{i<n}$). Le p-groupe de Prüfer :

$$\mathbf{Z}_{p^\infty} = \{z \in \mathbf{C} \mid \exists \alpha \in \mathbf{N},\ z^{p^\alpha} = 1\}$$

est un p-groupe mais il n'a *aucune partie génératrice minimale* (si on prend deux éléments d'une partie génératrice, l'un appartient toujours au sous-groupe engendré par l'autre. En fait, tous les sous-groupes de $\mathbf{Z}_{p^\infty}$ sont cycliques d'ordre une puissance de p, mais ce groupe n'est pas lui-même cyclique ni fini).

Recasages.

— 103 : C'est bien, on n'y parle pas beaucoup de conjugaison parce que les quotients que l'on manipule sont abéliens, mais on fait quand même intervenir de manière cruciale un normalisateur. On obtient un exemple important de sous-groupe distingué et du quotient correspondant (à rajouter au zoo du centre, sous-groupe dérivé, etc).

— 108 : C'est vraiment bien, surtout si l'on fait une partie ou une sous-partie entièrement dédiée à l'étude des parties génératrices minimales. On peut aussi y traiter le cas des groupes abéliens de type fini par exemple (dont le calcul des parties génératrices minimales est très intéressant). On peut aussi donner des bornes sur les cardinaux minimaux des parties génératrices, et tout comparer sur des cas particuliers.

— 151 : On dispose avec ce développement d'un exemple assez rare où la notion de dimension (finie) d'un espace vectoriel apparaît de manière aussi cruciale dans une démonstration. Le développement rentre très naturellement dans cette leçon, surtout si l'on y développe une sous-partie à propos des p-groupes abéliens élémentaires.