GROUPES FINIS AYANT UN CARDINAL PREMIER

Soit (G,.) un groupe fini dont le cardinal est un nombre premier quelconque p > 1, et « e » son élément neutre. D'après le théorème affirmant « que l'ordre de chaque élément d'un groupe fini est un diviseur du cardinal de ce groupe », chaque élément de G a pour ordre 1 ou p. Seul l'élément e a pour ordre 1, donc tous les autres éléments ont pour ordre p.

* Soit x_i un élément quelconque de G autre que e, et le naturel non nul n < p. Posons $nx_i = x_j$ ($x_j \neq e$ puisque n < p). $(n + k)x_i = nx_ikx_i$. Si n + k < p (n et k $\in$ N*), il est impossible que $(n + k)x_i = x_j$. En effet, $(n + k)x_i = nx_ikx_i = x_jkx_i \Rightarrow kx_i = e$, ce qui est impossible puisque n + k < p $\Rightarrow$ k < p (et $x_i \neq e$). Donc nx_i engendre tous les éléments du groupe, sauf e, lorsque n varie de 1 à (p – 1), et n'oublions pas que $px_i = e$. x_i est donc un générateur du groupe ; donc ce groupe est monogène, et, comme x_i est un élément quelconque de G, hors e, ce groupe G est non seulement monogène, mais chacun de ses éléments, hors e, lui est un générateur.
Enfin ce groupe est aussi cyclique et commutatif d'après ce qui a été démontré dans le texte « Groupes monogènes »

De tout ceci il vient :

Théorème : **Tout groupe fini de cardinal premier est monogène, cyclique et commutatif. Chacun de ses éléments, hors le neutre, lui est un générateur.**

* Enfin on peut remarquer que si un groupe fini, pas nécessairement de cardinal premier, a un élément x d'ordre le cardinal de ce groupe, la démonstration précédente lui est applicable, et par conséquent :

Théorème : **Tout groupe fini dont au moins un élément a pour ordre le cardinal de ce groupe est monogène, cet élément lui étant générique.**

*

* *

J. Legout