Classification des groupes d'ordre p^2 et $2p$:

I Le développement

Le but de ce développement est de classifier les groupes d'ordre p^2 et $2p$ (avec p un nombre premier) afin d'obtenir toutes les classes d'isomorphismes possibles dans le but de pouvoir identifier par la suite un groupe quelconque suivant certaines propriétés qu'il possède.

On s'intéresse tout d'abord aux groupes G d'ordre p^2 :
On commence tout d'abord avec un premier lemme :

Lemme 1 : [Berhuy, p.194]
Si le groupe $G/Z(G)$ est un groupe monogène, alors le groupe G est un groupe abélien.

Preuve :
On suppose que le groupe $G/Z(G)$ est un groupe monogène.
Comme $G/Z(G)$ est un groupe monogène, il existe un élément $x_0 \in G$ tel que $G/Z(G) = < \overline{x_0} >$.

On considère $x, y \in G$.
Il existe donc $k \in \mathbb{Z}$ et $\ell \in \mathbb{Z}$ tels que $\overline{x} = \overline{x_0}^k$ et $\overline{y} = \overline{x_0}^\ell$. De plus, il existe $c_x, c_y \in Z(G)$ tels que $x = c_x x_0^k$ et $y = c_0 y_0^\ell$.

On a donc :

$$xy = \left(c_x x_0^k\right)\left(c_y x_0^\ell\right) = c_x c_y x_0^k x_0^\ell = c_y c_x x_0^\ell x_0^k = \left(c_y x_0^\ell\right)\left(c_x x_0^k\right) = yx$$

Finalement, on en déduit que le groupe G est un groupe abélien.

■

On continue avec un deuxième lemme qui nous sera utile :

Lemme 2 : [Berhuy, p.194]
Le nombre premier p divise le cardinal de $Z(G)$.

Preuve :
On sait que $Z(G)$ est un sous-groupe du groupe fini G, donc par le théorème de Lagrange, $\mathrm{Card}(Z(G))$ divise $\mathrm{Card}(G) = p^2$. Autrement dit, $\mathrm{Card}(Z(G)) \in \{1; p; p^2\}$ (car $\mathrm{Card}(Z(G)) > 0$).

Or, comme G est un p-groupe, d'après l'équation aux classes pour les p-groupes (ici avec l'action de G sur lui-même par la conjugaison), on a :

$$\mathrm{Card}(G) \equiv \mathrm{Card}(Z(G)) \ [p]$$

Or, comme $\mathrm{Card}(G) = p^2$, on a alors :

$$\mathrm{Card}(Z(G)) \equiv 0 \ [p]$$

C'est-à-dire que $\mathrm{Card}(Z(G))$ est divisible par p.

Finalement, on en conclut que p divise le cardinal du centre du groupe G et on peut donc affirmer que $\mathrm{Card}(Z(G)) \in \{p; p^2\}$ (autrement dit, $Z(G) \neq \{e_G\}$).

■

On peut maintenant démontrer le résultat suivant :

Proposition 3 : [Berhuy, p.194]
Si G est d'ordre p^2, alors $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Preuve :
Montrons tout d'abord que les groupes d'ordre p^2 sont abéliens :
D'après le lemme précédent, on a $\mathrm{Card}(Z(G)) \in \{p; p^2\}$, donc :
$*$ Si $\mathrm{Card}(Z(G)) = p^2$, alors :
Comme on sait que $Z(G) \subseteq G$ (puisque $Z(G)$ est un sous-groupe de G) et que $\mathrm{Card}(Z(G)) = \mathrm{Card}(G)$, on en déduit donc que $G = Z(G)$. Or, comme $Z(G)$ est un groupe commutatif, on en déduit que le groupe G est un groupe abélien.

$*$ Si $\mathrm{Card}(Z(G)) = p$, alors :
Comme G est un ensemble fini, on a :

$$\mathrm{Card}(G/Z(G)) = \frac{\mathrm{Card}(G)}{\mathrm{Card}(Z(G))} = \frac{p^2}{p} = p$$

Donc d'après l'étude des groupes d'ordre p, le groupe $G/Z(G)$ est un groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$, il est donc monogène. Ainsi, d'après le premier lemme, on en déduit que le groupe G est un groupe abélien.

Finalement, on sait donc que tout groupe d'ordre p^2 est abélien.

On achève la démonstration par une nouvelle disjonction de cas :
$*$ S'il existe un élément x d'ordre p^2 dans G, alors on a $< x > \subseteq G$ ainsi que $\mathrm{Card}(< x >) = o(x) = \mathrm{Card}(G)$, donc $G = < x >$. Ainsi, G est abélien et cyclique (car engendré par x d'ordre p^2), donc $G \cong \mathbb{Z}/p^2\mathbb{Z}$.

$*$ S'il n'existe pas d'élément d'ordre p^2, alors il existe deux éléments $x, y \in G$ tels que $o(x) = o(y) = p$ et $y \in G \backslash < x >$. On pose alors $H =< x >\cong \mathbb{Z}/p\mathbb{Z}$ et $N =< y >\cong \mathbb{Z}/p\mathbb{Z}$.
De plus :
- H et N sont distingués dans G (car se sont deux sous-groupes de G et G est abélien).

- $\mathrm{Card}(G) = \mathrm{Card}(H)\,\mathrm{Card}(N)$.

- $H \cap N = \{e_G\}$. En effet, si ce n'est pas le cas, alors on a par cardinalité que $H \cap N = H$ et donc en particulier que $y \in H$, ce qui contredit la définition de y.

Ainsi, par la caractérisation du produit direct interne de groupes finis, on a $G \cong H \times N \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Finalement, on obtient bien que $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

■

On s'intéresse désormais aux groupes G d'ordre $2p$:
On commence une nouvelle fois avec un lemme :

Lemme 4 : [Berhuy, p.308]
Il existe deux sous-groupes de G, dont l'un est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et l'autre est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Preuve :
Puisque $\mathrm{Card}(G) = 2p$ et que p est un nombre premier différent de 2, alors par le théorème de Cauchy, il existe un élément a d'ordre p dans G et un élément b dans G d'ordre 2 et on a $< a >\cong \mathbb{Z}/p\mathbb{Z}$ et $< b >\cong \mathbb{Z}/2\mathbb{Z}$.

Finalement, il existe donc deux sous-groupes de G, dont l'un est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et l'autre est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

■

On passe maintenant au deuxième résultat important :

Proposition 5 : [Berhuy, p.308]
Si G est d'ordre $2p$, alors G est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou à D_{2p}.

Preuve :
Par les théorèmes de Sylow, on a :

$$n_p \equiv 1\ [p] \text{ et } n_p | 2, \text{ donc } n_p = 1 \text{ (car } p > 2)$$

Ainsi, G contient un unique p-Sylow noté H.

Raisonnons par l'absurde en supposant que ba est d'ordre p :
On a alors $H =< ba >=< a >$ (par unicité du p-Sylow qui est d'ordre p), donc $b = (ba)a^{-1} \in H$. Ainsi, par le théorème de Lagrange, $o(b)$ divise p. Mais puisque $o(b) = 2$ et que 2 est premier avec p (car $p \in \mathcal{P}\backslash\{2\}$), on a alors une contradiction.

Ainsi, par le théorème de Lagrange, on a trois possibilités :
- Si $o(ba) = 1$, alors $ba = e_G$ et ainsi $a = b = e_G$ mais ceci n'est pas possible car a est d'ordre p et b d'ordre 2.

- Si $o(ba) = p^2$, alors puisque l'on a $< ba >\subseteq G$ ainsi que l'égalité $\mathrm{Card}(G) = \mathrm{Card}(< ba >)$, on a finalement $G =< ba >\cong \mathbb{Z}/2p\mathbb{Z}$.

- Sinon, $o(ba) = 2$ et on a alors $baba = e_G$, c'est-à-dire $bab^{-1} = a^{-1}$ (car b est d'ordre 2). On reconnaît alors la présentation du groupe diédral et ainsi $< a, b >\cong D_{2p}$. Enfin, puisque $< a, b >\subseteq G$ et par égalité des cardinaux, on a $G \cong D_{2p}$.

Finalement, on a obtenu les deux classes d'isomorphisme voulues.

■

II Remarques sur le développement

II.1 Résultat(s) utilisé(s)

Dans ce développement, on a utilisé l'équation aux classes pour les p-groupes ainsi que les théorèmes de Sylow dont on rappelle les énoncés :

Théorème 6 : Théorèmes de Sylow [Berhuy, p.313] :
$*$ Il existe des p-sous-groupes de Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow.
$*$ Le conjugué d'un p-Sylow est un p-Sylow et tous les p-Sylow de G sont conjugués. En particulier, si S est un p-Sylow de G, alors S est distingué dans G si, et seulement si, S est l'unique p-Sylow de G.
$*$ Si n_p désigne le nombre de p-Sylow de G et $\mathrm{Card}(G) = p^m q$ (avec $p \wedge q = 1$), alors on a $n_p \equiv 1$ $[p]$ et $n_p | q$.

II.2 Pour aller plus loin...

Il est possible de montrer la première partie du développement en utilisant la structure des groupes abéliens finis (les deux seules suites de facteurs invariants de G possibles sont $\left(p^2\right)$ et (p,p)) à partir du moment où l'on a montré que les groupes d'ordre p^2 sont tous commutatifs (mais c'est utiliser un résultat très fort !). Il est également possible de montrer la deuxième partie du développement via les produits (semi-)directs en utilisant leur caractérisation sur $< a >$ et $< b >$.

II.3 Recasages

Recasages : 101 - 103 - 104 - 108 - 120 - 121.

III Bibliographie

— Grégory Berhuy, *Algèbre : le grand combat*.