Rombaldi p23

GROUPES D'ORDRE p^2

101, 103, 104

Soit p un nombre premier.

<u>Lemme</u> : Soient G un p-groupe agissant sur un ensemble fini X. Alors $\#X \equiv \#X^G \ [p]$.

<u>Lemme</u> : Le centre d'un p-groupe n'est pas trivial.

<u>Thm</u> : Un groupe d'ordre p^2 est abélien

<u>Cor</u> : $\mathbb{Z}/p^2\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^2$ représentent les 2 classes d'isomorphisme des groupes d'ordre p^2.

<u>Preuve du Lemme 1</u> : Notons $\#G = p^\alpha$, $\alpha \geq 1$. D'après l'équation aux classes, $\#X = \sum_{i=1}^r \#Orb(x_i) = \sum_{\substack{i=1 \\ \#Orb(x_i)=1}}^r 1 + \sum_{\substack{i=1 \\ \#Orb(x_i)>1}}^r \#Orb(x_i)$ $= \#X^G + \sum_{\substack{i=1 \\ \#Stab(x_i)<\#G}}^r \frac{\#G}{\#Stab(x_i)}$. Or $Stab(x_i)$ est un sous-groupe de G, donc $\#Stab(x_i) \mid \#G = p^\alpha$ d'après le théorème de LAGRANGE, donc il existe $\beta_i < \alpha$ tel que $\#Stab(x_i) = p^{\beta_i}$ car p est premier, donc $\frac{\#G}{\#Stab(x_i)} = p^{\alpha-\beta_i} \equiv 0 \ [p]$, et donc

$$\boxed{\#X \equiv \#X^G \ [p]}$$

<u>Preuve du Lemme 2</u> : Pour G agissant sur lui-même par conjugaison, $G^G = Z(G)$, d'où $\#Z(G) \equiv \#G \equiv 0 \ [p]$, donc il existe $k \in \mathbb{N}$ tel que $\#Z(G) = kp$, mais $1 \in Z(G)$ donc $\#Z(G) \neq 0$, donc $k \geq 1$, donc $\#Z(G) \geq p$, d'où $Z(G) \neq \{1\}$.

<u>Preuve du Thm</u> : Soit G d'ordre p^2, par l'absurde supposons G non abélien, i.e. $G \neq Z(G)$. Comme $Z(G)$ est un sous-groupe de G, $\#Z(G) \mid \#G$ d'après le théorème de LAGRANGE, donc $\#Z(G) \in \{1, p, p^2\}$ car p est premier. D'après Lemme 2, $\#Z(G) \neq 1$, et par hypothèse $\#Z(G) \neq p^2$, donc $\#Z(G) = p$, donc il existe $g \in Z(G)$ tel que $Z(G) = \langle g \rangle$. Soit $h \in G \setminus Z(G)$. En particulier $h \neq 1$, et $\langle h \rangle$ est abélien donc $G \neq \langle h \rangle$, donc $\#\langle h \rangle = p$. De plus, $\#Z(G) \cap \langle h \rangle \mid \#Z(G)$ donc $\#Z(G) \cap \langle h \rangle \in \{1, p\}$, i.e. $Z(G) \cap \langle h \rangle = \{1\}$ ou $Z(G) \cap \langle h \rangle = Z(G)$. Or $h \notin Z(G)$, donc le second cas est impossible, donc $Z(G) \cap \langle h \rangle = \{1\}$.

Posons $\varphi : (i,j) \in [\![0, p-1]\!]^2 \longmapsto g^i h^j$. Pour tout $(i,j), (i',j') \in [\![0,p-1]\!]^2$, si $\varphi(i,j) = \varphi(i',j')$, alors $g^i h^j g^{-i'} h^{-j'} = 1$, mais $g \in Z(G)$ donc $1 = g^i h^j g^{-i'} h^{-j'} = g^{i-i'} h^{j-j'}$, donc $Z(G) \ni g^{i-i'} = h^{j'-j} \in \langle h \rangle$, donc $g^{i-i'} = h^{j'-j} = 1$, donc $p = ord(g) \mid |i-i'|$ et $p = ord(h) \mid |j-j'|$, mais $(i,j,i',j') \in [\![0,p-1]\!]^4$ donc $|i-i'| < p$ et $|j-j'| < p$, donc $i = i'$ et $j = j'$. Ainsi, φ est injective, puis bijective par cardinalité, a fortiori donc surjective.

Soit $(a,b) \in G^2$. Il existe $(i,j,i',j') \in [\![0,p-1]\!]^4$ tel que $a = g^i h^j$ et $b = g^{i'} h^{j'}$. De là, $ab = g^i h^j g^{i'} h^{j'} = g^{i+i'} h^{j+j'} = g^{i'} h^{j'} g^i h^j = ba$ car $g \in Z(G)$. Cela montre que G est abélien, ce qui contredit l'hypothèse. Donc G est abélien.

<u>Preuve du Cor</u> : Soit G un groupe d'ordre p^2. Les éléments de G sont d'ordre divisant p^2, donc d'ordres $1, p$ ou p^2. Si G admet un élément d'ordre p^2, alors $G \simeq \mathbb{Z}/p^2\mathbb{Z}$. Sinon, tous les éléments de G distincts de 1 sont d'ordre p. Soit $h \in G \setminus \{1\}$, soit $g \in G \setminus \langle h \rangle$. Les éléments h et g sont d'ordre p, et de même que précédemment, $\langle h \rangle \cap \langle g \rangle = \{1\}$. De même que précédemment, $(i,j) \in [\![0,p-1]\!]^2 \longmapsto g^i h^j$ est une bijection (car G est abélien), et comme g et h sont d'ordre p, cette bijection induit l'isomorphisme $(\bar{i}, \bar{j}) \in (\mathbb{Z}/p\mathbb{Z})^2 \longmapsto g^i h^j$, d'où $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$.