GROUPES D'ORDRE 75

OLIVIER SERMAN

On s'intéresse aux groupes d'ordre 75. On montre qu'à isomorphisme près il y a exactement trois groupes de cardinal 75 :

Théorème. *Un groupe d'ordre* 75 *est isomorphe à* $\mathbf{Z}/75\mathbf{Z}$*, à* $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/15\mathbf{Z}$*, ou à l'unique produit semi-direct non trivial de* $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ *et* $\mathbf{Z}/3\mathbf{Z}$*.*

Soit G un groupe d'ordre 75. Un tel groupe possède un unique 5-Sylow H. Si K désigne un 3-Sylow de G, alors G est un produit semi-direct $H \rtimes K$ de H et K. Le produit semi-direct est donné par un morphisme $\varphi\colon K \to \mathrm{Aut}(H)$ (telle que le produit est défini par $(h,k)(h',k') = (h\varphi(k)h', kk')$), et il s'agit de comprendre l'ensemble des morphismes de K vers $\mathrm{Aut}(H)$.

Le sous-groupe K est isomorphe à $\mathbf{Z}/3\mathbf{Z}$: se donner un morphisme $\varphi\colon K \to \mathrm{Aut}(H)$ revient donc à se donner un élément d'ordre divisant 3 dans $\mathrm{Aut}(H)$ (il est utile de se rappeler comment : un élément $g \in \mathrm{Aut}(H)$ d'ordre 3 définit le morphisme $\varphi\colon i \in \mathbf{Z}/3\mathbf{Z} \mapsto g^i$, et $g = \varphi(1)$).

Enfin, le sous-groupe H est d'ordre 25, et est donc isomorphe à $\mathbf{Z}/25\mathbf{Z}$ ou à $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$. On va distinguer suivant ces deux cas.

Premier cas : $H \simeq \mathbf{Z}/25\mathbf{Z}$

Le groupe des automorphismes du groupe cyclique d'ordre 25 est le groupe cyclique $\mathbf{Z}/20\mathbf{Z}$ d'ordre 20. Comme il ne contient pas d'élément d'ordre 3, le seul morphisme $K \to \mathrm{Aut}(H)$ est le morphisme trivial. Dans ce cas le groupe G est isomorphe au produit direct

$$G \simeq \mathbf{Z}/25\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \simeq \mathbf{Z}/75\mathbf{Z}.$$

Second cas : $H \simeq \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$

Le groupe des automorphismes $\mathrm{Aut}(H)$ est alors isomorphe au groupe linéaire $\mathbf{GL}_2(\mathbf{F}_5)$. C'est un groupe d'ordre $(25-1)(25-5) = 480$, dont on veut comprendre les éléments d'ordre 3.

Pour ce faire, on peut remarquer qu'un élément g d'ordre 3 de $\mathbf{GL}_2(\mathbf{F}_5)$ est un automorphisme du plan vectoriel $\mathbf{F}_5^2$ dont le polynôme minimal divise $X^3 - 1 = (X-1)(X^2+X+1)$. Comme $X^2 + X + 1$ est irréductible sur $\mathbf{F}_5$ (en tant que polynôme de degré 2 n'admettant aucune racine dans $\mathbf{F}_5$), le polynôme minimal de g est donc $X^2 + X + 1$. C'est donc aussi son polynôme caractéristique. Il en résulte que deux éléments d'ordre 3 dans $\mathbf{GL}_2(\mathbf{F}_5)$ sont nécessairement conjugués[1] : si g_1 et g_2 sont deux éléments d'ordre 3 dans $\mathbf{GL}_2(\mathbf{F}_5)$, alors il existe $h \in \mathbf{GL}_2(\mathbf{F}_5)$ tel que $g_2 = hg_1h^{-1}$.

Autrement dit, si φ_1 et φ_2 sont deux morphismes $\mathbf{Z}/3\mathbf{Z} \to \mathrm{Aut}(\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z})$ non triviaux, alors il existe $h \in \mathrm{Aut}(\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z})$ tel que pour tout $k \in \mathbf{Z}/3\mathbf{Z}$, $\varphi_2(k) = h\varphi_1(k)h^{-1}$.

Date: 27 décembre 2010.

[1] Ce résultat s'obtient également de la manière suivante : on note qu'un élément d'ordre 3 dans $\mathbf{GL}_2(\mathbf{F}_5)$ appartient à $\mathbf{SL}_2(\mathbf{F}_5)$. Mais $\mathbf{PSL}_2(\mathbf{F}_5)$ est un sous-groupe d'indice 2 dans $\mathbf{PGL}_2(\mathbf{F}_5)$, dont on sait qu'il est isomorphe à $\mathfrak{S}_5$ (cf. Perrin IV, Proposition 5.3.4) : $\mathbf{PSL}_2(\mathbf{F}_5)$ est donc isomorphe au groupe alterné A_5. Dans A_5 les 3-cycles sont deux à deux conjugués. Si g_1 et g_2 sont deux éléments d'ordre 3 dans $\mathbf{SL}_2(\mathbf{F}_5)$, leurs images dans $\mathbf{PSL}_2(\mathbf{F}_5)$ sont conjuguées par l'image d'un élément $h \in \mathbf{SL}_2(\mathbf{F}_5)$. On a donc $hg_2h^{-1} = \pm g_1$ (car $\ker(\mathbf{SL}_2(\mathbf{F}_5) \twoheadrightarrow \mathbf{PSL}_2(\mathbf{F}_5)) = Z(\mathbf{SL}_2(\mathbf{F}_5)) = \{\pm \mathrm{id}\}$) et, puisque $-g_1$ est d'ordre 6, on a bien $hg_2h^{-1} = g_1$.

Les produits semi-directs définis par ces morphismes sont alors isomorphes (cf. Perrin, exercice I.D.4)[2]). Il y a donc exactement deux classes d'isomorphismes de produits semi-directs $(\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}) \rtimes \mathbf{Z}/3\mathbf{Z}$: l'une correspond au produit direct (isomorphe à $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/15\mathbf{Z}$), et l'autre correspond à l'unique groupe non abélien d'ordre 75.

Pour finir, on peut remarquer qu'on peut « expliciter » le produit semi-direct $G \simeq (\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}) \rtimes \mathbf{Z}/3\mathbf{Z}$ non trivial en produisant un élément d'ordre 3 dans $\mathbf{GL}_2(\mathbf{F}_5)$, par exemple $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$.

On peut aussi noter que G contient 25 3-Sylow. Il contient donc 50 éléments d'ordre 3 (car deux 3-Sylow distincts sont d'intersection triviale), et 24 éléments d'ordre 5.

[2]Rappelons l'énoncé précis et sa démonstration. Si φ_1 et φ_2 sont deux morphismes $K \to \mathrm{Aut}(H)$ et s'il existe $u \in \mathrm{Aut}(H)$ tel que $\varphi_2(k) = u\varphi_1(k)u^{-1}$ pour tout $k \in K$, alors les produits semi-directs $H \rtimes_1 K$ et $H \rtimes_2 K$ qu'ils définissent sont isomorphes. Il suffit de remarquer que l'application

$$H \rtimes_1 K \to H \rtimes_2 K, (h, k) \mapsto (u(h), k),$$

qui est évidemment bijective, est un morphisme de groupes (exercice !).