Groupes d'ordre pq

Arnaud Girand

17 septembre 2013

Référence :
- [Per96], p. 27–28

Prérequis :
- théorème de Sylow.

Proposition 1
Soient p, q deux nombres premiers tels que $p < q$.
Alors :

(i) si $p \nmid q-1$ tout groupe d'ordre pq est cyclique ;

(ii) si $p \mid q-1$ il existe exactement (à isomorphisme près) deux groupes d'ordre pq : le groupe cyclique et un produit semi–direct non abélien.

Démonstration : Soit G un groupe d'ordre pq. Si on note c_q le nombre de q–Sylow de G, le théorème du éponyme nous affirme que $c_q | p$ et $c_q \equiv 1[q]$. De fait $c_q = 1$ et donc l'unique q–Sylow $S_q \cong \mathbb{Z}/q\mathbb{Z}$ de G vérifie $S_q \lhd G$. De fait, si on se donne un p–Sylow $S_p \cong \mathbb{Z}/p\mathbb{Z}$ de G on a, comme $|G| = |S_p||S_q|$ et $S_p \cap S_q = \{e\}$ que $G \cong S_q \rtimes_\varphi S_p \cong \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ avec φ un morphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

Soit donc φ un morphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$. Alors si $a \in \mathbb{Z}/p\mathbb{Z}$ on a $\mathrm{id} = \varphi(pa) = \varphi(a)^p$ et donc l'ordre $\omega(a)$ de $\varphi(a)$ divise p donc $\omega(a) \in \{1, p\}$. De plus, par théorème de Lagrange, $\omega(a) \mid q-1$.

- *Cas 1 : $p \nmid q-1$.* Alors $\omega(a) = 1$ et donc φ est le morphisme trivial, ce qui implique que notre produit semi–direct est en fait direct et donc $G \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.
- *Cas 2 : $p \mid q-1$.* Alors $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous–groupe d'ordre p, soit H. Comme de plus $|\mathrm{Im}(\varphi)| \leq p$ et$p \nmid |\mathrm{Im}(\varphi)|$ (car comme φ est non trivial son image possède un élément d'ordre p), on a soit $|\mathrm{Im}(\varphi)| = 1$, auquel cas on retombe sur le produit direct, soit $|\mathrm{Im}(\varphi)| = p$ auquel cas $\mathrm{Im}(\varphi) = H$.
  Dans ce second cas, si on se donne ψ un morphisme *non trivial* de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ alors $\mathrm{Im}(\psi) = H$. Alors φ (resp. ψ) induit un morphisme surjectif $\hat{\varphi}$ (resp. $\hat{\psi}$) de $\mathbb{Z}/p\mathbb{Z}$ sur H. Par un argument de cardinaux, on a que $\hat{\varphi}$ et $\hat{\psi}$ sont des isomorphismes et donc $\alpha := \hat{\psi}^{-1} \circ \hat{\varphi}$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. On peut alors définir l'application suivante :

$$\begin{aligned} A : \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z} \\ (k, l) &\mapsto (k, \alpha(l)) \end{aligned}$$

  A définit clairement un morphisme de groupes injectif donc bijectif (cardinaux) et donc on a bien $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z} \cong ZZ/q\mathbb{Z} \rtimes_\psi \mathbb{Z}/p\mathbb{Z}$ d'où le résultat.

Détails supplémentaires :
- Cas $p = 2$. Le produit semi–direct $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ est alors le groupe diédral D_q. En effet si on pose $s := (0, 1)$ et $r := (1, 0)$ alors $\{r, s\}$ engendre le produit semi–direct et comme le seul morphisme non trivial de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/\mathrm{q}\mathbb{Z})$ est $x \mapsto (-1)^x \mathrm{id}$ (i.e $(i, j) * (k, \ell) = (i + (-1)^j k, j\ell)$ on a :

$$\begin{aligned} s^2 &= (0,1) * (0,1) = (0, 1+1) = (0,0) \\ r^q &= (1,0)^{*q} = (q, 0) = (0,0) \end{aligned}$$

$$s * r * s = (0,1) * (1,0) * (0,1) = (0,1) * (1 + (-1)^0 * 0, 1) = (0 - 1, 0) = (-1, 0) = (q-1, 0) = r^{-1}$$

  D'où le résultat.

Références

[Per96] Daniel Perrin. *Cours d'algèbre*. Ellipses, 1996.