Classification des groupes d'ordre pq

Combes, *Algèbre et Géométrie*, page 94

Théorème :
Soit G un groupe fini d'ordre pq où $p < q$ sont des nombres premiers.

1. Si q n'est pas congru à 1 modulo p, alors G est cyclique, isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.
2. Si q est congru à 1 modulo p, à isomorphisme près G a deux structures possibles : ou bien G est abélien, cyclique, isomorphe à $\mathbb{Z}/pq\mathbb{Z}$, ou bien G n'est pas commutatif et alors G est isomorphe à $(\mathbb{Z}/q\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/p\mathbb{Z})$ où $\theta \in Hom(\mathbb{Z}/p\mathbb{Z}, Aut(\mathbb{Z}/q\mathbb{Z}))$ est tel que $\theta(\overline{1}) = \gamma$ est d'ordre p dans $Aut(\mathbb{Z}/q\mathbb{Z})$.

D'après les théorèmes de Sylow, il existe dans G un sous-groupe H d'ordre q et un sous-groupe K d'ordre p. Le nombre n_q de q-sous-groupes de Sylow est congru à 1 modulo q et divise p. Comme on a $p < q$, cela nécessite $n_q = 1$ donc H est distingué dans G.

D'après le théorème de Lagrange, $|H \cap K|$ divise $|H| = q$ et $|K| = p$. On a donc $|H \cap K| = 1$ et $H \cap K = \{e\}$. Puisque $H \lhd K$, le théorème montre que HK est un sous-groupe de G et que $HK/H \simeq K/(H \cap K) = K$. On en déduit que $|HK| = |H||K| = pq = |G|$ et donc que $HK = G$. G est donc un produit semi-direct de H et de K, isomorphe à $(\mathbb{Z}/q\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/p\mathbb{Z})$, où θ ets un homomorphisme de $\mathbb{Z}/p\mathbb{Z}$ dans $Aut(\mathbb{Z}/q\mathbb{Z})$.

Les p-sous-groupes de Sylow, sont les conjugués de K dans G. Leur nombre n_p est congru à 1 modulo p et divise q. Donc $n_p = 1$ ou $n_p = q$. Si $n_p = q$, alors q est congru à 1 modulo p d'après le théorème de Sylow.

1. Supposons que q ne soit pas congru à 1 modulo p. D'après ce qui précède, $n_p = 1$ et donc K est distingué dans G. Le produit semi-direct précédent est alors un produit direct $H \times K$. Comme p et q sont premiers, H et K sont cycliques. Leurs ordres étant premiers entre eux, G est cyclique isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

2. Supposons q congru à 1 modulo p. L'ordre de l'image de $\theta : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z})$ divise l'ordre p de $\mathbb{Z}/p\mathbb{Z}$ et vaut p ou 1 (dans ce dernier cas, l'action est triviale.

   Si θ est l'action triviale, alors le produit semi-direct $(\mathbb{Z}/q\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/p\mathbb{Z})$ est un produit direct. Comme en 1., G est isomorphe à $\mathbb{Z}/pq\mathbb{Z}$.

   Supposons maintenant que θ ne soit pas l'action triviale. On a que $Aut(\mathbb{Z}/q\mathbb{Z})$ est cylique, d'ordre $\varphi(q) = q - 1$ (ici divisible par p). Il existe dans $Aut(\mathbb{Z}/q\mathbb{Z})$ un unique sous-groupe Γ d'ordre p. On a donc $\Gamma = Im(\theta)$. Puisque $\mathbb{Z}/p\mathbb{Z}$ et $\Gamma = Im(\theta)$ ont le même ordre, θ est un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur Γ, déterminé par le choix de $\theta(\overline{1}) = \gamma$ parmi les $p - 1$ générateurs de Γ. Vérifions que les $p - 1$ choix possibles de $\theta(\overline{1})$ conduisent à des produits semi-directs isomorphes. Soit θ' un autre isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur Γ. Alors $\alpha = \theta'^{-1} \circ \theta$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$. Il existe alors un isomorphisme f de G_θ sur $G_{\theta'}$.

Application : si $p = 2$ et si $q > 2$ est premier, un groupe G d'ordre $2q$ est soit isomorphe à $\mathbb{Z}/2q\mathbb{Z}$, soit isomorphe au groupe diédral D_p.

En effet, d'après la proposition, G n'a que deux structures possibles : l'une abélienne et $G \simeq \mathbb{Z}/2q\mathbb{Z}$, l'autre non abélienne. Comme D_q est d'ordre $2q$ et non abélien, il représente l'autre alternative.