VM
7/04/15

Groupes d'ordre pq

103, 104, (121)

Réf : Perrin

Théorème

Soit G un groupe d'ordre pq, $p<q$ premiers.

Si $q \not\equiv 1\ [p]$, alors $G \simeq \mathbb{Z}/(pq)\mathbb{Z}$

Si $q \equiv 1\ [p]$, alors $G \simeq \mathbb{Z}/(pq)\mathbb{Z}$ ou $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$,

où α est un morphisme de groupe^s non trivial : $\mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

→ H et J pour les notations.

Lemme : Soit G un groupe et H, K deux sous-groupes tels que $H \cap K = \{e\}$, H distingué dans G et $HK = G$.

Alors $G \simeq H \rtimes_\alpha K$, où
$$\alpha : K \to \mathrm{Aut}(H), \quad k \mapsto (h \mapsto khk^{-1}).$$

Si de plus $K \lhd G$, alors $G \simeq H \times K$.

dém (du lemme) : α est bien définie car $H \lhd G$.

On pose
$$\phi : H \rtimes_\alpha K \to G, \quad (h,k) \mapsto hk$$

ϕ est bien un morphisme de groupes :
$$\begin{aligned}\phi((h_1,k_1)\cdot(h_2,k_2)) &= \phi(h_1\alpha(k_1)(h_2), k_1k_2)\\ &= \phi(h_1k_1h_2k_1^{-1}, k_1k_2)\\ &= h_1k_1h_2k_2\\ &= \phi(h_1,k_1)\,\phi(h_2,k_2)\end{aligned}$$

ϕ est injective : si $hk=e$, alors $h = k^{-1} \in H \cap K$ donc $h=e$ et $k=e$.

ϕ est surjective car $G = HK$.

Donc $G \simeq H \rtimes_\alpha K$.

Si de plus, $K \lhd G$: soit $k \in K$.

$\forall h \in H$, $h^{-1}kh \in K$, donc $h^{-1}kh = k'$

d'où $khk^{-1} = hk'k^{-1} \in H$

et $k'k^{-1} \in H \cap K$ donc $k' = k$.

Donc $khk^{-1} = h$: α est triviale

$$G \simeq H \times K.$$

$\square$

démonstration (du théorème) :

Soit n_p le nombre de p-Sylow de G.

Soit n_q ——— q-Sylow de G.

$n_q \equiv 1 [q]$ et $n_q | p$. Or $p \not\equiv 1 [q]$ car $p < q$ et p premier,

donc $n_q = 1$. Soit H le seul q-Sylow de G.

Il est donc distingué dans G.

Soit K un p-Sylow de G. $H \cap K$ est un sous-groupe de H et de K, donc est de cardinal divisant p et q : $|H \cap K| = 1$, $H \cap K = \{e\}$.

Soit $\varphi : \begin{array}{ccc} K & \longrightarrow & HK/H \\ k & \longmapsto & kH \end{array}$.

φ est un morphisme de groupe,

injectif car si $\varphi(k) = H$, $kH = H$ et $k \in H \cap K = \{e\}$.

surjectif car $\forall (h, k) \in H \times K$

$$hkH = k\underbrace{k^{-1}hk}_{\in H}H = kH = \varphi(k)$$

Donc $|HK| = |K||H| = pq = |G|$ donc $HK = G$.

Ainsi $G \simeq H \rtimes_\alpha K \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$.

$n_p \equiv 1 [p]$ et $n_p | q$.

Si $q \not\equiv 1 [p]$, alors $n_p = 1$ et K est distingué dans G.

Donc $G \simeq H \times K \simeq \mathbb{Z}/pq\mathbb{Z}$ d'après le théorème chinois.

Si $q \equiv 1 [p]$, alors α peut être non trivial.

En effet, $\alpha : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathrm{Aut}(H) \simeq \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$

Comme p divise $q-1$, il existe un sous-groupe Γ de $\mathbb{Z}/(q-1)\mathbb{Z}$ d'ordre p. Il suffit de choisir a un générateur de Γ, et de choisir $\alpha(\bar{1}) = a$.