DÉVELOPPEMENT 20

GROUPES D'ORDRE pq

On rappelle que si H et K sont deux sous-groupes d'un groupe G vérifiant $H \lhd G$, $K \lhd G$, $HK = G$ et $H \cap K = \{e\}$ alors G est isomorphe au produit direct $H \times K$.

Lemme. — *Si H et K sont deux sous-groupes d'un groupe G vérifiant $H \lhd G$, $H \cap K = \{e\}$ et $HK = G$ alors G est isomorphe au produit semi-direct $H \rtimes_\alpha K$ où $\alpha : k \mapsto \alpha_k$ est donnée par $\alpha_k(h) = khk^{-1}$.*

Démonstration. — Tout d'abord α est bien une action par automorphismes de K sur H. Puisque $HK = G$, l'application $f : H \times K \to G, (h, k) \mapsto hk$ est surjective. Si $hk = h'k'$ alors $h'^{-1}h = k'k^{-1} \in H \cap K$ et l'hypothèse $H \cap K = \{e\}$ donne donc l'injectivité de f. Enfin, on a

$$f(h,k)f(h',k') = hkh'k' = hkh'k^{-1}kk' = h\alpha_k(h')kk' = f(h\alpha_k(h'), kk') = f((h,k)(h',k'))$$

i.e. f est bien un morphisme. □

Corollaire. — *Si H et K sont deux sous-groupes d'un groupe G vérifiant $H \lhd G$, $H \cap K = \{e\}$ et $HK = G$ alors on a équivalence entre*

(i) $G = HK$ *est le produit direct* $H \times K$

(ii) $K \lhd G$

(iii) $hk = kh$ *pour tous* $h \in H$ *et* $k \in K$

(iv) l'action α est triviale

Proposition. — *Soit G un groupe d'ordre pq où $p < q$ sont premiers.*

(i) Si $q \not\equiv 1 \pmod p$ *alors* $G \simeq \mathbb{Z}/pq\mathbb{Z}$.

(ii) Si $q \equiv 1 \pmod p$ *alors G a deux structures possibles (à isomorphismes près) :*
- *soit G est abélien et $G \simeq \mathbb{Z}/pq\mathbb{Z}$,*
- *soit G n'est pas abélien et est isomorphe au produit semi-direct $\mathbb{Z}/q\mathbb{Z} \rtimes_\theta \mathbb{Z}/p\mathbb{Z}$ où $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est tel que $\theta(\overline{1})$ soit d'ordre p dans $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.*

Démonstration. — Notons respectivement n_p et n_q les nombres de p-Sylow et de q-Sylow de G ; en particulier, on considère un p-Sylow K et un q-Sylow H. D'après le théorème de Sylow, $n_q \equiv 1 \pmod q$ et n_q divise p or $p < q$ donc $n_q = 1$ et on a donc $H \lhd G$.

D'après le théorème de Lagrange, l'ordre de $H \cap K$ divise celui de H et celui de K or ceux-ci sont premiers ente-eux donc $H \cap K = \{e\}$. Donc HK est un sous-groupe de G dans lequel H est distingué et on a $HK/H \simeq K/(H \cap K)$ *i.e.* $HK/H \simeq K$ d'où il vient $|HK| = |H|\,|K| = pq$; on a donc $HK = G$. Il s'ensuit que $G \simeq H \rtimes_\theta K$ où $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

Puisque $n_p \equiv 1 \pmod p$ et n_p divise q, on a $n_p = 1$ ou q. On distingue ces deux cas.
– Si $n_p = 1$ alors $K \lhd G$ et il s'ensuit que le produit semi-direct $H \rtimes_\theta K$ est en fait un produit direct *i.e.* $G \simeq H \times K$ or $H \simeq \mathbb{Z}/q\mathbb{Z}$ et $K \simeq \mathbb{Z}/p\mathbb{Z}$ avec p et q premiers entre eux donc $G \simeq \mathbb{Z}/pq\mathbb{Z}$.

– Si $n_p = q$ alors $q \equiv 1 \pmod{p}$ *i.e.* p divise $q-1$. L'image du morphisme $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est soit triviale, soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$ (puisque p est premier). On distingue ces deux sous-cas.
  – Si θ est trivial alors le produit semi-direct $H \rtimes_\theta K$ est un produit direct et on a comme plus haut $G \simeq \mathbb{Z}/pq\mathbb{Z}$.
  – Sinon, notons que le groupe $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ est cyclique d'ordre $\varphi(q) = q-1$ donc, pour tout diviseur d de $q-1$, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ admet un unique sous-groupe d'ordre d ; en particulier, $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ admet un unique sous-groupe Γ d'ordre p, d'où $\mathrm{Im}\ \theta = \Gamma$. En particulier θ est déterminé par le choix de $\theta(\overline{1})$. Considérons un autre morphisme $\theta' : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ alors $\alpha = \theta'^{-1} \circ \theta$ est un automorphisme de $\mathbb{Z}/p\mathbb{Z}$ donc l'application
$$f : H \rtimes_\theta K \to H \rtimes_{\theta'} K, (\widetilde{h}, \overline{k}) \mapsto (\widetilde{h}, \alpha(\overline{k}))$$
est bijective. De plus, on a
$$f\left((\widetilde{h}, \overline{k})(\widetilde{h'}, \overline{k'})\right) = f(\widetilde{h}\theta(\overline{k})(\widetilde{h'}), \overline{kk'}) = f(\widetilde{h}\theta(\overline{k})(\widetilde{h'}), \overline{kk'}) = (\widetilde{h}\theta(\overline{k})(\widetilde{h'}), \alpha(\overline{kk'}))$$
et
$$f(\widetilde{h}, \overline{k})f(\widetilde{h'}, \overline{k'}) = (\widetilde{h}, \alpha(\overline{k}))(\widetilde{h'}, \alpha(\overline{k'})) = (\widetilde{h}\theta'(\alpha(\overline{k}))(\widetilde{h'}), \alpha(\overline{k})\alpha(\overline{k'})) = (\widetilde{h}\theta(\overline{k})(\widetilde{h'}), \alpha(\overline{kk'}))$$
i.e. f est un morphisme. Les deux produits semi-directs sont donc isomorphes.

□

Exemple. — À isomorphisme près, il n'y a que deux groupes d'ordre $2p$ (où $p > 2$ est premier) : $\mathbb{Z}/2p\mathbb{Z}$ et le groupe diédral D_p. En particulier, à isomorphisme près, il n'y a que deux groupes d'ordre 6 : $\mathbb{Z}/6\mathbb{Z}$ et $D_6 \simeq S_3$.

Application. — S_5 n'a pas de sous-groupe d'ordre 15.

Démonstration. — Supposons que S_5 admette un sous-groupe d'ordre 15, comme $15 = 3 \times 5$ mais $5 \not\equiv 1 \pmod{3}$, H est nécessairement abélien, cyclique d'ordre 15. Considérons un générateur s de H que l'on décompose en un produit $s = c_1 \cdots c_k$ de cycles disjoints. Comme l'ordre de s est le ppcm des ordres des c_i, les c_i sont d'ordre 3, 5 ou 15 mais S_5 ne contient pas d'éléments d'ordre 15 donc les c_i sont d'ordre 3 ou 5 et les deux cas doivent se produire pour que le ppcm soit 15. C'est absurde puisqu'il est impossible de trouver un 3-cycle et un 5-cycle de S_5 qui soient à supports disjoints. □

Leçons concernées

04 Sous-groupes distingués, groupes quotients. Exemples et applications

05 Groupes finis. Exemples et applications

09 Congruences dans $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications

10 Nombres premiers. Applications

Référence

F. Combes, *Algèbre et géométrie*, Bréal, 1998.

Sébastien Pellerin