THÉORIE DES GROUPES - SÉRIE 10

22 novembre 2019

p-Groupes

Exercice 1. Soit p un nombre premier. Montrer qu'un groupe fini G est un p-groupe si et seulement si $|G| = p^k$ pour un certain $k \in \mathbb{N}$.

Solution. Soit G un groupe fini. Si G est un p-groupe, supposons par l'absurde qu'il existe un nombre premier $q \neq p$ tel que q divise $|G|$. Alors, par le premier théorème de Sylow, il existe un q-sous-groupe de Sylow de G qui contient (au moins) un élément d'ordre q^n pour un certain $n \geq 1$. Cela contredit le fait que G soit un p-groupe, puisque tous les éléments d'un p-groupe sont d'ordre une puissance de p. Donc le seul premier qui divise $|G|$ est p. Inversément, supposons que $|G| = p^k$ pour un certain $k \in \mathbb{N}$. Alors, l'ordre de chaque élément de G divise p^k. En particulier, l'ordre de chaque élément de G est une puissance de p, ce qui prouve que G est un p-groupe.

Exercice 2 (A rendre pour le 29 novembre)**.** Soient p un nombre premier et G un groupe fini. Montrer que:

(a) si $G \neq \{e\}$ est un p-groupe, alors $Z(G) \neq \{e\}$.

(b) si G n'est pas abélien, alors $G/Z(G)$ n'est pas cyclique.

(c) si $|G| = p^2$, alors G est abélien.

Solution.

(a) On a l'équation des classes

$$|G| = |Z(G)| + \sum_{x \in G \setminus Z(G)} [G : C_G(x)].$$

Pour $x \notin Z(G)$, le sous-groupe $C_G(x)$ est strictement contenu dans G, i.e. $[G : C_G(x)] \neq 1$. De plus, comme $|G| = p^k$ pour $k \in \mathbb{N}$, par l'Exercice 1, et $[G : C_G(x)]$ divise $|G|$, alors $[G : C_G(x)]$ est aussi une puissance de p. Ainsi p divise $|G|$ et p divise chaque $[G : C_G(x)]$ pour $x \notin Z(G)$, ce qui implique que p divise également $|Z(G)|$. En particulier, $|Z(G)| \neq 1$.

(b) On montre que si $G/Z(G)$ est cyclique, alors G est abélien. Soit $x \in G$ tel que $G/Z(G) = \langle xZ(G) \rangle$. Pour $g \in G$, il existe $m \in \mathbb{N}$ tel que $gZ(G) = (xZ(G))^m = x^m Z(G)$. Donc il existe $z \in Z(G)$ tel que $g = x^m z$. Soient $g, h \in G$ et soient $m, n \in \mathbb{N}$ et $y, z \in Z(G)$ tels que $g = x^m y$ et $h = x^n z$. Alors

$$gh = x^m y x^n z = x^m x^n y z = x^n x^m z y = x^n z x^m y = hg.$$

Donc G est abélien.

(c) Par l'Exercice 1, si $|G| = p^2$, alors G est un p-groupe. Supposons que G ne soit pas abélien. Alors $G \neq Z(G)$ et, par (a), $Z(G) \neq \{e\}$. Donc $|Z(G)| = p$. Ainsi $|G/Z(G)| = [G : Z(G)] = p$ et $G/Z(G)$ est cyclique. Par (b), on obtient une contradiction. Donc G est abélien.

p-Sous-groupes de Sylow

Exercice 3. Soient p un nombre premier et G un groupe fini qui admet au moins un p-sous-groupe de Sylow. Montrer que:

(a) le nombre de p-sous-groupes de Sylow de G divise $|G|$.

(b) le groupe G admet un unique p-sous-groupe de Sylow P si et seulement si P est normal dans G.

Solution.

(a) Soit $\{P_1, \dots, P_{n_p}\}$ l'ensemble des p-sous-groupes de Sylow de G. Alors G agit par conjugaison sur cet ensemble puisque le conjugué d'un p-sous-groupe de Sylow est également un p-sous-groupe de Sylow. De plus, tous les p-sous-groupes de Sylow sont conjugués entre eux, donc il n'y a qu'une seule orbite pour l'action de G sur $\{P_1, \dots, P_{n_p}\}$. Ainsi $n_p = |\mathcal{O}_{P_1}| = [G : N_G(P_1)]$ et n_p divise $|G|$.

(b) Supposons que G admette un unique p-sous-groupe de Sylow P. Comme gPg^{-1} est aussi un p-sous-groupe de Sylow pour tout $g \in G$, alors $gPg^{-1} = P$ pour tout $g \in G$. Cela montre que P est normal dans G. Supposons maintenant que P soit un p-sous-groupe de Sylow normal dans G. Soit Q un autre p-sous-groupe de Sylow. Alors il existe $g \in G$ tel que $Q = gPg^{-1} = P$ puisque P est normal. Donc P est l'unique p-sous-groupe de Sylow de G.

Exercice 4. On dit qu'un groupe $G \neq \{e\}$ est **simple** s'il n'admet aucun sous-groupe normal autre que $\{e\}$ et G. Montrer que:

(a) il n'existe aucun groupe simple d'ordre 30.

(b) il n'existe aucun groupe simple d'ordre 36.

(c) tout groupe d'ordre 40 admet un sous-groupe normal.

(d) tout groupe d'ordre 42 admet un sous-groupe normal.

Solution.

(a) Supposons que G soit un groupe simple d'ordre 30. On a la décomposition $30 = 2 \cdot 3 \cdot 5$. Le nombre n_5 de 5-sous-groupes de Sylow de G est tel que $n_5 \equiv 1 (\mathrm{mod}\ 5)$ et n_5 divise 30. En regardant les différentes possibilités, on voit que $n_5 \in \{1, 6\}$. Comme G n'admet aucun sous-groupe normal autre que $\{e\}$ et G, alors $n_5 \neq 1$, car sinon le 5-sous-groupe de Sylow est normal dans G par l'Exercice 3 (b). On conclut que $n_5 = 6$. Par un même raisonnement, on trouve qu'il y a $n_3 = 10$ 3-sous-groupes de Sylow dans G. Comme chaque 5-sous-groupe de Sylow est d'ordre 5 et donc cyclique, les 5-sous-groupes de Sylow sont d'intersection triviale. Ainsi on compte $6 \cdot 4 = 24$ éléments d'ordre 5, car chaque 5-sous-groupe de Sylow contient 5 éléments dont l'élément neutre. De même, comme chaque 3-sous-groupe de Sylow est d'ordre 3 et donc cyclique, les 3-sous-groupes de Sylow sont d'intersection triviale. Et on compte $10 \cdot 2 = 20$ éléments d'ordre 3, car chaque 3-sous-groupe de Sylow contient 3 éléments dont l'élément neutre. On a compté 42 éléments dans G, ce qui est absurde.

(b) Supposons que G soit un groupe simple d'ordre 36. On a la décomposition $36 = 2^2 \cdot 3^2$. Comme G est simple, il contient au moins deux 3-sous-groupes de Sylow P et Q distincts, car sinon l'unique 3-sous-groupe de Sylow est normal par l'Exercice 3 (b). Si l'intersection $P \cap Q$ est trivial, alors $|PQ| = |P| \cdot |Q| = 9 \cdot 9 = 81 > 36$, ce qui est absurde. Donc $P \cap Q \neq \{e\}$. On considère le normalisateur $N_G(P \cap Q)$. On a que P et Q sont des sous-groupes de $N_G(P \cap Q)$, puisque P et Q sont d'ordre 3^2 donc abéliens par l'Exercice 2 (c). En particulier, l'ordre de $N_G(P \cap Q)$ est un multiple de 9. De plus, comme $P \neq Q$, alors $|N_G(P \cap Q)| > 9$ et il divise 36, par le théorème de Lagrange. Donc $|N_G(P \cap Q)| \in \{18, 36\}$. Si $|N_G(P \cap Q)| = 18$, alors $N_G(P \cap Q)$ est d'indice 2 dans G et est donc normal. Si $|N_G(P \cap Q)| = 36$, alors $N_G(P \cap Q) = G$ et $P \cap Q$ est normal dans G. On obtient une contradiction.

(c) Soit G un groupe d'ordre 40. On a la décomposition $40 = 2^3 \cdot 5$. Le nombre n_5 de 5-sous-groupes de Sylow de G est tel que $n_5 \equiv 1 (\text{mod } 5)$ et n_5 divise 40. En regardant les différentes possibilités, on voit que $n_5 = 1$. Donc l'unique 5-sous-groupe de Sylow de G est normal, par l'Exercice 3 (b).

(d) Soit G un groupe d'ordre 42. On a la décomposition $42 = 2 \cdot 3 \cdot 7$. Le nombre n_7 de 7-sous-groupes de Sylow de G est tel que $n_7 \equiv 1 (\text{mod } 7)$ et n_7 divise 42. En regardant les différentes possibilités, on voit que $n_7 = 1$. Donc l'unique 7-sous-groupe de Sylow de G est normal, par l'Exercice 3 (b).

Exercice 5. Soient G un groupe et H, K deux sous-groupes normaux de G tels que $H \cap K = \{e\}$ et $G = HK$. Montrer qu'on a un isomorphisme de groupes $H \times K \cong G$.
Astuce: se rappeler de l'Exercice 7 (e) Série 3.

Solution. On considère l'application

$$f \colon H \times K \to G, \ (h, k) \mapsto hk.$$

Alors f est surjective, puisque $G = HK$. De plus, f est injective, car si $f(h, k) = e$, alors $hk = e$ et $h = k^{-1} \in H \cap K = \{e\}$, d'où $h = k = e$. Finalement, on montre que c'est un homomorphisme de groupes. Par l'Exercice 7 (e) Série 3, comme H, K sont des sous-groupes normaux de G tels que $H \cap K = \{e\}$, alors $hk = kh$ pour tous $h \in H$ et $k \in K$. Soient $h, h' \in H$ et $k, k' \in K$. Alors

$$f((h, k)(h', k')) = f(hh', kk') = hh'kk' = hkh'k' = f(h, k)f(h', k').$$

Donc f est bien un homomorphisme. On conclut que $H \times K \cong G$.

Exercice 6. Soient $p \neq q$ deux nombres premiers et G un groupe fini d'ordre $p^n q^m$, où $n, m \in \mathbb{N}$. Supposons que G a un unique p-sous-groupe de Sylow P et un unique q-sous-groupe de Sylow Q. Montrer qu'on a un isomorphisme de groupes $G \cong P \times Q$.

(Plus généralement, on peut montrer que si G a un unique p-sous-groupe de Sylow pour chaque premier p qui divise G, alors G est isomorphe au produit de ses sous-groupes de Sylow.)

Solution. Comme P consiste seulement en des éléments d'ordre une puissance de p et Q seulement en des éléments d'ordre une puissance de q, on a que $P \cap Q = \{e\}$. De plus, P et Q sont normaux dans G par l'Exercice 3 (b). Par le deuxième théorème d'isomorphisme, on a que $PQ/Q \cong P/(P \cap Q)$ et donc $|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = |P| \cdot |Q| = p^n q^m = |G|$, puisque $P \cap Q = \{e\}$. On obtient que $PQ = G$. Par l'Exercice 5, on conclut que $G \cong P \times Q$.