THÉORIE DES GROUPES - SÉRIE 11

29 novembre 2019

p-groupes

Exercice 1 (Théorème de Cauchy)**.** Soit p un nombre premier et soit G un groupe tel que p divise $|G|$. Montrer qu'il existe un élément dans G d'ordre p.

Solution. Par le Théorème de Sylow, il existe un p-sous-groupe de Sylow P dans G. Soit $x \in P$. Alors x est d'ordre p^k pour un certain $k \in \mathbb{N}$. Ainsi $x^{p^{k-1}}$ est un élément d'ordre p dans G.

Exercice 2 (A rendre pour le 6 décembre)**.** Soit G un p-groupe d'ordre p^n, pour $n \geq 1$. Montrer que:

(a) G a un sous-groupe normal d'ordre p^k, pour tout $0 \leq k \leq n$,

(b) G est résoluble.

Solution.

(a) On procède par récurrence sur k. Pour $k = 0$, alors $\{e\}$ est un sous-groupe normal d'ordre $p^0 = 1$ de G. Si $k = n$, alors G est un sous-groupe normal d'ordre p^n. Supposons que $0 < k < n$ et qu'il existe un sous-groupe normal N de G d'ordre p^{k-1}. Alors G/N est un p-groupe non trivial. Par l'Exercice 2 (a) Série 10 et le Théorème de Lagrange, $Z(G/N)$ est aussi un p-groupe non trivial. Par le Théorème de Cauchy, il existe un élément $xN \in Z(G/N)$ d'ordre p. On considère l'homomorphisme quotient $\pi\colon G \to G/N$ et on montre que $\pi^{-1}(\langle xN\rangle)$ est un sous-groupe normal d'ordre p^k dans G. Comme $\langle xN\rangle < Z(G/N)$, alors $\langle xN\rangle$ est un sous-groupe normal de G/N et ainsi $\pi^{-1}(\langle xN\rangle)$ est un sous-groupe normal de G, car la préimage d'un sous-groupe normal est normale. De plus, par le premier Théorème d'isomorphisme,

$$|\pi^{-1}(\langle xN\rangle)| = |\langle xN\rangle| \cdot |\mathrm{Ker}(\pi)| = |\langle xN\rangle| \cdot |N| = p \cdot p^{k-1} = p^k.$$

(b) On construit une suite $G = H_0 > H_1 > \ldots > H_n = \{e\}$ par récurrence, où $H_k < H_{k-1}$ est normal pour tout $1 \leq k \leq n$ et $|H_k| = p^{n-k}$ pour tout $0 \leq k \leq n$. On pose $H_0 = G$. Soit $k > 0$. Par récurrence, on a H_{k-1} d'ordre p^{n-k+1}. Par (a), il existe un sous-groupe normal $H_k < H_{k-1}$ d'ordre p^{n-k}. On obtient donc la suite désirée. De plus, H_k/H_{k-1} est d'ordre p, donc cyclique, donc abélien, pour tout $1 \leq k \leq n$. Cela montre que G est résoluble.

p-sous-groupes de Sylow

Exercice 3. Soient $p > q$ deux nombres premiers et soit G un groupe d'ordre pq. Montrer que:

(a) le groupe G a un sous-groupe normal d'ordre p. *(Astuce: utiliser l'Exercice 4 (e) Série 5.)*

(b) si q ne divise pas $p-1$, alors G est cyclique. *(Astuce: se rappeler l'Exercice 8 (c) Série 4 et l'Exercice 6 Série 10.)*

(c) si q divise $p-1$, alors soit G est cyclique, soit $G = \langle a, b\rangle$ avec a un élément d'ordre p et b un élément d'ordre q tels que $bab^{-1} = a^m$ où $m^q \equiv 1 (\mathrm{mod}\ p)$ mais $m \not\equiv 1 (\mathrm{mod}\ p)$.

Solution.

(a) Soit P un p-sous-groupe de Sylow de G. Alors $[G : P] = q$, le plus petit nombre premier qui divise l'ordre de G. Par l'Exercice 4 (e) Série 5, on obtient que P est normal dans G. Ainsi P est un sous-groupe normal de G d'ordre p.

(b) Par (a), comme un p-sous-groupe de Sylow est normal dans G, on a que le nombre n_p de p-sous-groupes de Sylow vaut 1, par l'Exercice 3 (b) Série 10. Ensuite, le nombre n_q de q-sous-groupes de Sylow est tel que $n_q \equiv 1 (\mathrm{mod}\ q)$ et n_q divise $|G| = pq$. Puisque q ne divise pas $p-1$, on a forcément $n_q = 1$. Ainsi P a un unique p-sous-groupe de Sylow et un unique q-sous-groupe de Sylow. Par l'Exercice 6 Série 10, on a que $G \cong P \times Q$. Or $|P| = p$, d'où $P \cong \mathbb{Z}/p\mathbb{Z}$, et $|Q| = q$, d'où $Q \cong \mathbb{Z}/q\mathbb{Z}$. On conclut, par l'Exercice 8 (c) Série 4, que $G \cong P \times Q \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$ est cyclique.

(c) Comme en (b), on a que le nombre n_p de p-sous-groupes de Sylow de G vaut 1. Ensuite, le nombre n_q de q-sous-groupes de Sylow est tel que $n_q \equiv 1 (\mathrm{mod}\ q)$ et n_q divise $|G| = pq$. On a donc $n_q \in \{1, p\}$ puisque q divise $p-1$. Si $n_q = 1$, on procède comme en (b) pour montrer que G est cyclique. Supposons donc que $n_q = p$. Soit P l'unique p-sous-groupe de Sylow de G. Alors P est normal dans G, par l'Exercice 3 (b) Série 10, et P est cyclique d'ordre p. Soit $a \in G$ tel que $P = \langle a \rangle$. Alors a est d'ordre p. Comme q divise $|G|$, il existe un élément b d'ordre q dans G. Alors $Q = \langle b \rangle$ est un q-sous-groupe de Sylow de G et n'est donc pas normal, par l'Exercice 3 (b) Série 10. Comme P est normal dans G, $bPb^{-1} = P$ et il existe $m \in \mathbb{N}$ tel que $bab^{-1} = a^m$. Si $m \equiv 1 (\mathrm{mod}\ p)$, alors $bab^{-1} = a$ et G est abélien, ce qui est absurde vu que tout sous-groupe d'un groupe abélien est normal, mais Q n'est pas normal dans G. On a donc $m \not\equiv 1 (\mathrm{mod}\ p)$. On prouve facilement par récurrence que $b^k a b^{-k} = a^{m^k}$ pour tout $k \in \mathbb{N}$. En particulier, comme b est d'ordre q, $a = b^q a b^{-q} = a^{m^q}$. Donc $m^q \equiv 1 (\mathrm{mod}\ p)$.

Exercice 4. Montrer que tous les groupes d'ordre 15, 33, 35 et 51 sont cycliques.

Solution. On applique le résultat de l'Exercice 1 (b). Comme $15 = 3 \cdot 5$ et 3 ne divise pas $5 - 1 = 4$, tout groupe d'ordre 15 est cyclique et isomorphe à $\mathbb{Z}/15\mathbb{Z}$. Comme $33 = 3 \cdot 11$ et 3 ne divise pas $11 - 1 = 10$, tout groupe d'ordre 33 est cyclique et isomorphe à $\mathbb{Z}/33\mathbb{Z}$. Comme $35 = 5 \cdot 7$ et 5 ne divise pas $7 - 1 = 6$, tout groupe d'ordre 35 est cyclique et isomorphe à $\mathbb{Z}/35\mathbb{Z}$. Comme $51 = 3 \cdot 17$ et 3 ne divise pas $17 - 1 = 16$, tout groupe d'ordre 51 est cyclique et isomorphe à $\mathbb{Z}/51\mathbb{Z}$

Exercice 5. Déterminer (à isomorphisme près) tous les groupes d'ordre 6 et tous les groupes d'ordre 10.

Solution.

(a) Soit G un groupe d'ordre 6. On a que $6 = 2 \cdot 3$, où 2 divise $3 - 1 = 2$. Par l'Exercice 1 (c), si $n_2 = 1$, alors G est cyclique. Si $n_2 = 3$, alors $G = \langle a, b \rangle$ avec $a^3 = e$, $b^2 = e$ et $bab^{-1} = a^m$, avec $m^2 \equiv 1 (\mathrm{mod}\ 3)$ mais $m \not\equiv 1 (\mathrm{mod}\ 3)$. Comme a est d'ordre 3, il suffit de considérer les cas où $m \in \{1, 2\}$. Comme $m \not\equiv 1 (\mathrm{mod}\ 3)$, on a forcément $m = 2$. Remarquez qu'on a bien $m^2 = 4 \equiv 1 (\mathrm{mod}\ 3)$. Donc $G = \langle a, b \rangle$ avec $a^3 = e$, $b^2 = e$ et $bab^{-1} = a^2$. Pour résumé, on a donc que G est soit isomorphe à $\mathbb{Z}/6\mathbb{Z}$, soit isomorphe à S_3. On avait déjà trouvé ce résultat à l'Exercice 9 Série 5.

(b) Soit G un groupe d'ordre 10. On a que $10 = 2 \cdot 5$, où 2 divise $5-1 = 4$. Par l'Exercice 1 (c), si $n_2 = 1$, alors G est cyclique. Si $n_2 = 5$, alors $G = \langle a, b \rangle$ avec $a^5 = e$, $b^2 = e$ et $bab^{-1} = a^m$, avec $m^2 \equiv 1 (\text{mod } 5)$ mais $m \not\equiv 1 (\text{mod } 3)$. Comme a est d'ordre 5, il suffit de considérer les cas où $m \in \{1, 2, 3, 4\}$. Comme $m \not\equiv 1 (\text{mod } 5)$, on a $m \neq 1$. De plus, $2^2 = 4 \not\equiv 1 (\text{mod } 5)$ et $3^2 = 9 \not\equiv 1 (\text{mod } 5)$. Donc on a forcément $m = 4$. Remarquez qu'on a bien $m^2 = 4^2 = 16 \equiv 1 (\text{mod } 5)$. Donc $G = \langle a, b \rangle$ avec $a^3 = e$, $b^2 = e$ et $bab^{-1} = a^4 = a^{-1}$. Pour résumé, on a donc que G est soit isomorphe à $\mathbb{Z}/10\mathbb{Z}$, soit isomorphe à D_{10}, le groupe diédral d'ordre 10.

Plus généralement, on peut montrer que, si p est premier, un groupe d'ordre $2p$ est soit isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ soit isomorphe à D_{2p}, le groupe diédral d'ordre $2p$. Plus précisément, on a

$$D_{2p} = \langle a, b \mid a^p = e, b^2 = e, bab^{-1} = a^{-1} \rangle.$$

Exercice 6. On considère $SL_2(\mathbb{F}_3)$, le groupe spécial de degré 2 sur le corps $\mathbb{F}_3 (\cong \mathbb{Z}/3\mathbb{Z})$.

(a) Montrer que $|SL_2(\mathbb{F}_3)| = 24$.

(b) Calculer le nombre de 3-sous-groupes de Sylow de $SL_2(\mathbb{F}_3)$.

(c) En déduire le nombre de 2-sous-groupes de Sylow de $SL_2(\mathbb{F}_3)$.

Solution.

(a) Par l'Exercice 4 (b) Série 9, on a $|GL_2(\mathbb{F}_3)| = (3^2 - 1)(3^2 - 3) = 48$. De plus, $SL_2(\mathbb{F}_3)$ est le noyau du déterminant $\det \colon GL_2(\mathbb{F}_3) \to (\mathbb{F}_3)^*$. Par le premier théorème d'isomorphisme,

$$|SL_2(\mathbb{F}_3)| = \frac{|GL_2(\mathbb{F}_3)|}{|(\mathbb{F}_3)^*|} = \frac{48}{2} = 24.$$

(b) On calcule le nombre n_3 de 3-sous-groupes de Sylow de $SL_2(\mathbb{F}_3)$. On a que n_3 divise 24 et $n_3 \equiv 1 (\text{mod } 3)$. Donc $n_3 \in \{1, 4\}$. On trouve un 3-sous-groupe de Sylow qui n'est pas normal et on en déduit que $n_3 \neq 1$. On considère les matrices de $SL_2(\mathbb{F}_3)$:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Alors A est d'ordre 3, donc $\langle A \rangle$ est un 3-sous-groupe de Sylow. Mais

$$BAB^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \notin \langle A \rangle.$$

Donc $\langle A \rangle$ n'est pas normal. Ainsi $n_3 = 4$.

(c) On calcule le nombre n_2 de 2-sous-groupes de Sylow de $SL_2(\mathbb{F}_3)$. On a que n_2 divise $24 = 2^3 \cdot 3$ et $n_2 \equiv 1 (\text{mod } 2)$. Donc $n_2 \in \{1, 3\}$. Supposons par l'absurde que $n_2 = 3$. Alors on a 3 2-sous-groupes de Sylow d'ordre $2^3 = 8$ qui peuvent s'intersecter en au plus 4 éléments, dont l'élément neutre. Donc on a au moins $3 \cdot (8 - 4) + 3 = 15$ éléments d'ordre une puissance de 2 dans $SL_2(\mathbb{F}_3)$. Par (b), on a que $n_3 = 4$. Donc on a $4 \cdot (3 - 1) = 8$ éléments d'ordre 3 dans $SL_2(\mathbb{F}_3)$. Cela fait un total de $15 + 8 = 23$ éléments (+ l'élément neutre que l'on n'a pas compté). Donc tous les éléments dans $SL_2(\mathbb{F}_3)$ sont d'ordre une puissance de 2 ou d'ordre 3. Or la matrice

$$\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$$

est d'ordre 6 dans $SL_2(\mathbb{F}_3)$. Contradiction. Donc $n_2 = 1$. Ainsi $SL_2(\mathbb{F}_3)$ a un unique 2-sous-groupe de Sylow, qui est normal. (On peut montrer de plus que ce 2-sous-groupe de Sylow est isomorphe au groupe des quaternions $\mathbf{Q}$.)