THÉORIE DES GROUPES - SÉRIE 5

18 octobre 2019

Groupes résolubles

Exercice 1. Soit G un groupe. Montrer que:

(a) si $H < G$ est un sous-groupe normal de G tel que G/H est abélien, alors $[G, G] \subset H$, où

$$[G, G] = \langle [x, y] \mid x, y \in G, [x, y] = xyx^{-1}y^{-1} \rangle,$$

(b) G est résoluble si et seulement s'il existe des sous-groupes $G^{(0)}, G^{(1)}, \ldots, G^{(m)}$, où $m \geq 1$, tels que $G^{(m)} = \{e\}$ et les $G^{(i)}$ sont définis inductivement par

$$G^{(0)} = G \quad \text{et} \quad G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

Solution.

(a) On considère l'application quotient $\pi \colon G \to G/H$ et on montre que $[G, G]$ est contenu dans le noyau de π. Soit $x, y \in G$. Alors

$$\pi([x, y]) = \pi(xyx^{-1}y^{-1}) = \pi(x)\pi(y)\pi(x)^{-1}\pi(y)^{-1} = e_{G/H}$$

puisque G/H est abélien. Donc $[G, G] < H = \mathrm{Ker}(\pi)$, puisque $[G, G]$ est le sous-groupe engendré par les commutateurs et $[x, y] \in H$ pour tous $x, y \in G$. .

(b) Supposons que G soit résoluble. Alors il existe une suite de sous-groupes normaux $G = H_0 > H_1 > \ldots > H_r = \{e\}$ tels que H_i/H_{i+1} est abélien, pour tout $0 \leq i < r$. On montre que $G^{(i)} < H_i$ pour tout $0 \leq i \leq r$, ce qui implique que $G^{(r)} = \{e\}$. Clairement, $G^{(0)} = G < G = H_0$. Supposons par récurrence qu'on ait $G^{(i)} < H_i$ pour $i \geq 0$. Par a), comme H_i/H_{i+1} est abélien, on a que $[H_i, H_i] \subset H_{i+1}$. Ainsi

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subset [H_i, H_i] \subset H_{i+1}.$$

Supposons maintenant qu'on ait une suite de sous-groupes $G^{(0)}, G^{(1)}, \ldots, G^{(m)}$ de G tels que $G^{(m)} = \{e\}$, $G^{(0)} = G$ et $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ pour tout $0 \leq i < m$. Alors $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ est normal dans $G^{(i)}$ et $G^{(i)}/G^{(i+1)} = G^{(i)}/[G^{(i)}, G^{(i)}]$ est abélien, pour tout $0 \leq i < m$ (voir Exercice 1 Série 6). Donc G est résoluble.

Exercice 2. Soit $B_n \subset GL_n(\mathbb{R})$ le sous-ensemble des matrices triangulaires supérieures, i.e. $A \in B_n$ si et seulement si $A \in GL_n(\mathbb{R})$ et $A_{ij} = 0$ pour tous $i > j \in \{1, \ldots, n\}$. Montrer que B_n est un groupe résoluble.

Solution. On note que si $A \in B_n$ alors $A_{ii} \in \mathbb{R}^*$, puisque $\det(A) = \prod_{i=1}^n A_{ii} \neq 0$. On considère l'application

$$f \colon B_n \to (\mathbb{R}^*)^{\times n},\ A \mapsto (A_{ii})_{i=1}^n.$$

Il est facile de vérifier que f est un homomorphisme de groupes surjectif. Soit $U_n = \mathrm{Ker}(f)$ son noyau. Par le premier théorème d'isomorphisme, $B_n/U_n \cong (\mathbb{R}^*)^{\times n}$ et donc B_n/U_n est abélien. Remarquez que U_n est le sous-ensemble de B_n qui contient les matrices triangulaires supérieures qui n'ont que des 1 sur la diagonale.

On trouve une suite de sous-groupes $\{H_k \mid 0 \leq k \leq n-1\}$ de U_n tels que $H_0 = U_n$, $H_{n-1} = \{I_n\}$, $H_k < H_{k-1}$ est normal et H_{k-1}/H_k est abélien. Pour $0 \leq k \leq n-1$, on définit

$$H_k = \{A \in U_n \mid A_{ij} = 0 \text{ si } 1 \leq j - i \leq k\}.$$

Il est facile de vérifier que les H_k sont des sous-groupes de U_n tels que $H_k < H_{k-1}$ pour tout $1 \leq k \leq n-1$ et que $H_0 = U_n$ et $H_{n-1} = \{I_n\}$. En effet, H_k consiste en les matrices triangulaires supérieures avec que des 1 sur la diagonale et que des 0 dans les k premières diagonales supérieures. Il reste à montrer que $H_k < H_{k-1}$ est normal et H_{k-1}/H_k est abélien, pour tout $1 \leq k \leq n-1$. Pour $1 \leq k \leq n-1$, on considère l'application

$$f_k \colon H_{k-1} \to \mathbb{R}^{n-k},\ A \mapsto (A_{i,i+k})_{i=0}^{n-k},$$

qui envoie une matrice de H_{k-1} sur sa $k^{\text{ème}}$ diagonale supérieure. On vérifie par des calculs élémentaires que f_k est un homomorphisme de groupes (Attention, $\mathbb{R}^{n-k}$ est muni de l'addition!). De plus, f_k est clairement surjectif et son noyau est H_k. Ainsi H_k est normal dans H_{k-1} et $H_{k-1}/H_k \cong \mathbb{R}^{n-k}$ est abélien.

On conclut que B_n est résoluble en considérant la suite de sous-groupes

$$\{I_n\} = H_{n-1} < H_{n-2} < \ldots < H_1 < H_0 = U_n < B_n.$$

Exercice 3. On dit qu'un groupe G est **simple** s'il n'a pas d'autres sous-groupes normaux que $\{e\}$ et G. Montrer que, si un groupe non abélien G est simple, alors il n'est pas résoluble.

Solution. Soit G un groupe simple. Alors $[G,G]$ est un sous-groupe normal de G. Comme G est simple, on a soit $[G,G] = \{e\}$ soit $[G,G] = G$. On sait que $G/[G,G]$ est abélien, donc si $[G,G] = \{e\}$ on obtient que G est abélien, ce qui est absurde. Ainsi $[G,G] = G$ et, par l'Exercice 1 (b), G n'est pas résoluble.

Permutations

Exercice 4. Soit G un groupe et H un sous-groupe de G. Pour $x \in G$, on définit l'application

$$T_x \colon G/H \to G/H,\ \ yH \mapsto xyH.$$

Montrer que:

(a) T_x est une permutation de G/H,

(b) l'application

$$T \colon G \to \mathrm{Perm}(G/H),\ \ x \mapsto T_x$$

est un homomorphisme de groupes,

(c) le noyau K de T est un sous-groupe de H,

(d) si $[G:H] = n$, alors $|G/K|$ divise $n!$,

(e) si G est fini et $[G:H]$ est le plus petit nombre premier divisant $|G|$, alors H est normal dans G.

Solution.

(a) L'application T_x est bijective d'inverse $T_{x^{-1}}$.

(b) Soit $x, y \in G$. On montre que $T_{xy} = T_x \circ T_y$. Soit $zH \in G/H$, alors

$$T_{xy}(zH) = (xy)zH = x(yz)H = T_x(yzH) = T_x \circ T_y(zH).$$

(c) Comme T est un homomorphisme, K est un sous-groupe de G. Il reste à montrer que $K \subset H$. Soit $x \in K$. Alors $T_x = \mathrm{id}_{G/H}$, i.e. pour tout $yH \in G/H$, $xyH = yH$. En particulier, $xH = H$ et donc $x \in H$.

(d) Comme $|G/H| = n$, alors $|\mathrm{Perm}(G/H)| = n!$. Par le premier théorème d'isomorphisme, on a que $G/K \cong \mathrm{Im}(T)$, où $\mathrm{Im}(T)$ est un sous-groupe de $\mathrm{Perm}(G/H)$, i.e. G/K est isomorphe à un sous-groupe de $\mathrm{Perm}(G/H)$. Par le théorème de Lagrange, $|G/K|$ divise $n!$.

(e) Soit $p = [G : H]$ le plus petit nombre premier qui divise $|G|$. On montre que $K = H$ et donc H est normal dans G, puisque le noyau d'un homomorphisme est un sous-groupe normal. Soit q un nombre premier qui divise $[G : K]$. Alors q divise $|G|$ et donc $q \geq p$. Mais q divise également $p!$ par (d). Or p est le plus grand nombre premier qui divise $p! = p \cdot (p-1) \cdots 2 \cdot 1$. Donc $q \leq p$ et ainsi $q = p$, ce qui montre que p est le seul nombre premier qui divise $[G : K]$. Soit $r \geq 1$ tel que $[G : K] = p^r$. Comme p^r divise $p!$, on obtient directement que $r = 1$. Ainsi $[G : K] = p = [G : H]$ et donc K et H ont le même ordre, car G est fini. Par (c), comme $K < H$, on conclut que $K = H$.

Remarque: Ce résultat est une généralisation du fait qu'un sous-groupe d'indice 2 *est normal.*

Exercice 5. On considère le groupe symétrique S_7. Ecrire:

(a) (1 3 5)(2 3)(4 5 6) et (3 2 7)(1 4 2)(1 3) comme composition de cycles disjoints,

(b) (3 2 7 5 6) sous la forme de composition de transpositions.

Solution.

(a) (1 3 5)(2 3)(4 5 6) = (1 3 2 5 6 4) et (3 2 7)(1 4 2)(1 3) = (1 2)(3 4 7),

(b) (3 2 7 5 6) = (3 6)(3 5)(3 7)(3 2).

Exercice 6. On considère le groupe symétrique S_n, où $n \geq 1$.

(a) Soient $\sigma \in S_n$ et $\tau = (i_1\ i_2\ \cdots\ i_k)$ un k-cycle, pour $k \leq n$. Calculer $\sigma\tau\sigma^{-1}$.

(b) Calculer le centre $Z(S_n) = \{\sigma \in S_n \mid \sigma\tau = \tau\sigma \text{ pour tout } \tau \in S_n\}$ de S_n.

(c) Soient $\tau_i = (i\ \ i+1) \in S_n$ pour $i = 1, \ldots, n-1$. Montrer que $S_n = \langle \tau_1, \ldots, \tau_{n-1} \rangle$ et que $\tau_i\, \tau_{i+1}\, \tau_i = \tau_{i+1}\, \tau_i\, \tau_{i+1}$.

Solution.

(a) On montre que $\sigma\tau\sigma^{-1} = \sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$. Pour $1 \leq j < k$, on calcule que

$$\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1}\sigma(i_j) = \sigma(i_1\ i_2\ \cdots\ i_k)(i_j) = \sigma(i_{j+1})$$
$$\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1}\sigma(i_k) = \sigma(i_1\ i_2\ \cdots\ i_k)(i_k) = \sigma(i_1).$$

Soit $j \notin \{\sigma(i_1), \ldots, \sigma(i_k)\}$. Alors il existe $i \notin \{i_1, \ldots, i_k\}$ tel que $\sigma(i) = j$, car σ est une bijection. Alors

$$\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1}(j) = \sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1}\sigma(i) = \sigma(i_1\ i_2\ \cdots\ i_k)(i) = \sigma(i) = j.$$

Cela termine la preuve.

(b) Pour $n = 1, 2$, on a clairement $Z(S_n) = S_n$. Soit $n > 2$. On montre que $Z(S_n) = \{\mathrm{id}\}$. Supposons par l'absurde qu'il existe $\sigma \in Z(S_n)$ tel que $\sigma \neq \mathrm{id}$. Alors il existe $i, j \in \{1, \ldots, n\}$ tels que $i \neq j$ et $\sigma(i) = j$. Comme $n \geq 3$, il existe $k \in \{1, \ldots, n\} \setminus \{i, j\}$. On considère la transposition $\tau = (i\ k) \in S_n$. Alors

$$\sigma\tau(i) = \sigma(k) \neq j = \tau(j) = \tau\sigma(i)$$

puisque $\sigma(i) = j$ et σ est injective. Donc $\sigma\tau \neq \tau\sigma$ et on obtient une contradiction.

(c) On sait déjà que S_n est engendré par les transpositions. Il suffit donc de montrer que toute transposition s'écrit comme une composition des τ_i. Soit $i < k \in \{1, \ldots, n\}$. Alors

$$\begin{aligned}(i\ k) &= (i\ \ i+1)(i+1\ \ i+2)\cdots(k-2\ \ k-1)(k-1\ \ k)(k-2\ \ k-1)\cdots(i+1\ \ i+2)(i\ \ i+1)\\ &= \tau_i\tau_{i+1}\cdots\tau_{k-2}\tau_{k-1}\tau_{k-2}\cdots\tau_{i+1}\tau_i.\end{aligned}$$

Donc on a bien $S_n = \langle\tau_1, \ldots, \tau_{n-1}\rangle$. De plus, comme chaque transposition est son propre inverse, par (a), on obtient

$$\tau_i\,\tau_{i+1}\,\tau_i = (\tau_i(i+1)\ \ \tau_i(i+2)) = (i\ \ i+2)$$
$$\tau_{i+1}\,\tau_i\,\tau_{i+1} = (\tau_{i+1}(i)\ \ \tau_{i+1}(i+1)) = (i\ \ i+2)$$

ce qui montre l'égalité du point (c).

Exercice 7. Montrer que les groupes symétriques S_3 et S_4 sont résolubles.

Solution. On rappelle que tout groupe d'ordre ≤ 5 est abélien (Série 3, Exercice 3).

S_3: On note $\sigma = (1\ 2)$ et $\rho = (1\ 2\ 3)$. On écrit $A_3 = \langle\rho\rangle$ le groupe cyclique d'ordre 3 engendré par ρ. On montre que $\{\mathrm{id}\} < A_3 < S_3$ est une suite de sous-groupes normaux tels que chaque quotient est abélien. Comme $[S_3 : A_3] = 2$, A_3 est normal dans S_3 et S_3/A_3 est aussi abélien, car il est d'ordre 2. De plus, A_3 est abélien, vu qu'il est cyclique.

S_4: On définit les sous-groupes suivants de S_4:

$$A_4 = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2\ 3), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 3), (1\ 2\ 4), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3)\},$$
$$V_4 = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

On montre que $\{\mathrm{id}\} < V_4 < A_4 < S_4$ est une suite de sous-groupes tels que chaque sous-groupe est normal dans le suivant et chaque quotient est abélien. Comme $|A_4| = 12$, on a que $[S_4 : A_4] = 2$ et ainsi A_4 est bien un sous-groupe normal de S_4. De plus, S_4/A_4 est abélien vu qu'il est d'ordre 2. Par l'Exercice 6 (a), pour $\sigma \in S_4$ et $\{i, j, k, l\} = \{1, 2, 3, 4\}$, on a $\sigma(i\ j)(k\ l)\sigma^{-1} = (\sigma(i)\ \sigma(j))(\sigma(k)\ \sigma(l)) \in V_4$, donc V_4 est un sous-groupe normal de A_4. De plus, A_4/V_4 est abélien vu qu'il est d'ordre 3. Finalement, V_4 est abélien vu qu'il est d'ordre 4.

Exercice 8 (A rendre pour le 25 octobre)**.** Soit G un groupe abélien fini et p un nombre premier. Montrer que si p divise $|G|$, alors G a un élément d'ordre p.
Astuce: faire une récurrence sur $n = |G|$, en commençant par $n = p$.

Solution. Soit p un nombre premier qui divise $|G|$. On procède par récurrence sur $n = |G|$. Si $n = p$, alors tous les éléments de G (sauf l'élément neutre) sont d'ordre p et donc G a un élément d'ordre p. Si $n > p$, soit $x \in G$ avec $x \neq e$. Si p divise $\mathrm{ord}(x) = m$, alors $x^{m/p}$ est un élément d'ordre p dans G. Si p ne divise pas $\mathrm{ord}(x) = m$, on pose $H = \langle x \rangle$ le groupe cyclique engendré par x. Remarquez que comme G est abélien, H est normal dans G. Alors p divise $[G : H] = \frac{|G|}{|H|} = \frac{|G|}{|\langle x \rangle|} = \frac{|G|}{m}$. Comme $[G : H] < |G|$ et p divise $[G : H]$, alors G/H contient un élément d'ordre p par induction. Soit $y \in G$ tel que $yH \in G/H$ un élément d'ordre p et soit $k = \mathrm{ord}(y)$. Alors $y^k = e$, d'où $(yH)^k = H$ et donc p divise k. Ainsi $y^{k/p}$ est d'ordre p dans G.

Exercice 9. Soit G un groupe d'ordre 6. Montrer que:

(a) il existe $g, h \in G$ tels que g est d'ordre 2 et h est d'ordre 3,

(b) G est soit cyclique, soit isomorphe au groupe symétrique S_3.

Solution.

(a) Les éléments du groupe G sont d'ordre 1, 2, 3 ou 6. Si G a un élément x d'ordre 6, alors $g = x^3$ est d'ordre 2 et $h = x^2$ est d'ordre 3. Supposons maintenant que G n'ait aucun élément d'ordre 6. Par l'Exercice 4 (a) Séries 1+2, G contient au moins un élément g d'ordre 2, puisque G est d'ordre pair. Supposons par l'absurde que tous les éléments de $G \setminus \{e\}$ soient d'ordre 2. Alors G est abélien par l'Exercice 4 (b) Série 1+2. Par l'Exercice 8, comme 3 divise 6, on obtient que G a un élément h d'ordre 3. Contradiction.

(b) Si G a un élément d'ordre 6, alors G est cyclique. Supposons maintenant que G n'ait aucun élément d'ordre 6. Par (a), il existe $g, h \in G$ tels que g est d'ordre 2 et h est d'ordre 3. Le groupe cyclique $\langle h \rangle$ engendré par h est d'indice 2, donc il est normal dans G. Ainsi $ghg^{-1} \in \langle h \rangle$. On a que ghg^{-1} est d'ordre 3, car $(ghg^{-1})^m = gh^m g^{-1}$ pour tout $m \in \mathbb{Z}$. Donc on a soit $ghg^{-1} = h$ soit $ghg^{-1} = h^2$. Supposons que $ghg^{-1} = h$. Alors $gh = hg$ et donc gh est d'ordre 6. En effet, $(gh)^m = g^m h^m$ pour tout $m \in \mathbb{Z}$, car g et h commutent. On vérifie facilement que gh n'est pas d'ordre 1, 2 ou 3, puisque g est d'ordre 2 et h est d'ordre 3. Donc gh est d'ordre 6. On obtient une contradiction vu que G n'a pas d'élément d'ordre 6. Ainsi $ghg^{-1} = h^2$. Ainsi on peut écrire

$$G = \{e, g, h, h^2, gh, gh^2\}$$

et on trouve un isomorphisme de groupes $f \colon G \to S_3$ donné par $f(g) = (1\ 2)$ et $f(h) = (1\ 2\ 3)$. En effet, c'est bien un homomorphisme de groupes car

$$(1\ 2)(1\ 2\ 3)(1\ 2) = f(g)f(h)f(g) = f(ghg) = f(h^2) = (1\ 3\ 2).$$