THÉORIE DES GROUPES - SÉRIE 3

4 octobre 2019

Théorème de Lagrange

Exercice 1. Soit G un groupe fini. Montrer que:

(a) l'ordre d'un élément $x \in G$ divise l'ordre de G;

(b) si $x \in G$ est d'ordre $n = mk$, où $m, k \geq 1$, alors x^k est d'ordre m;

(c) si $x \in G$ est d'ordre n, alors $\{k \in \mathbb{Z} \mid x^k = e\} = n\mathbb{Z}$;

(d) on a $x^{|G|} = e$ pour tout $x \in G$.

Solution.

(a) L'ensemble $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$ est un sous-groupe de G. Or $n = \text{ord}(x) = |\langle x \rangle|$, puisque $n = \text{ord}(x) \in \mathbb{N}$ est le plus petit entier tel que $x^n = e$. Par le théorème de Lagrange, on a que l'ordre de x divise l'ordre de G.

(b) On a que $(x^k)^m = x^{km} = x^n = e$. Donc $\text{ord}(x^k) \leq m$. Supposons que $i = \text{ord}(x^k) < m$. Alors $e = (x^k)^i = x^{ki}$, où $ki < n$. Contradiction. Donc $\text{ord}(x^k) = m$.

(c) Clairement, $x^{nk} = (x^n)^k = e^k = e$, d'où $n\mathbb{Z} \subset \{k \in \mathbb{Z} \mid x^k = e\}$. Soit $k \in \mathbb{Z}$ tel que $x^k = e$. Supposons que $k \geq 0$. Alors $n \leq k$ par définition. Donc $k = nq + r$, où $q, r \in \mathbb{N}$ et $r < n$. Ainsi
$$e = x^k = x^{nq+r} = x^{nq}x^r = (x^n)^q x^r = x^r.$$
Comme $r < n$, on a $r = 0$, et $k = nq \in n\mathbb{Z}$. Pour $k \leq 0$, faire le même raisonnement en utilisant $\text{ord}(x^{-1}) = -n$. On obtient $\{k \in \mathbb{Z} \mid x^k = e\} \subset n\mathbb{Z}$.

(d) Soit $x \in G$. Alors l'ordre de x divise $|G|$ par (a). Par (c), $x^{|G|} = e$.

Exercice 2. Soit $f\colon G \to H$ un homomorphisme de groupes. Montrer que:

(a) si $x \in G$ est d'ordre fini, alors l'ordre de $f(x)$ divise l'ordre de x;

(b) si G et H sont finis d'ordres premiers entre eux, alors $f(x) = e$ pour tout $x \in G$.

Solution.

(a) Soit $n = \text{ord}(x)$. On a que $f(x)^n = f(x^n) = f(e) = e$. Donc l'ordre de $f(x)$ divise n par l'Exercice 1 (c).

(b) Soient $x \in G$, $n = \text{ord}(x)$ et $m = \text{ord}(f(x))$. Par (a), $m|n$. Par l'Exercice 1 (a), n divise $|G|$ et m divise $|H|$. Ainsi m divise $|G|$ et $|H|$. Comme $|G|$ et $|H|$ sont premiers entre eux, on a $m = 1$. Donc $f(x) = e$.

Exercice 3 (A rendre pour le 11 octobre)**.**

(a) Soit G un groupe d'ordre 4. Montrer que G est cyclique ou que $x^2 = e$ pour tout $x \in G$. En déduire que G est abélien.

(b) Montrer que tous les groupes finis d'ordre ≤ 5 sont abéliens.

Solution.

(a) L'ordre des éléments de G divise $|G| = 4$. Supposons d'abord qu'il existe un élément $x \in G$ d'ordre 4. Alors $G = \{e, x, x^2, x^3\} = \langle x \rangle$ est cyclique. En particulier, G est abélien. Supposons qu'il n'existe aucun élément d'ordre 4. Alors tous les éléments $x \in G, x \neq e$ sont d'ordre 2. En particulier, on a que $x^2 = e$ pour tout $x \in G$, et G est abélien par l'Exercice 4 (b) de la Série 1.

(b) Soit G un groupe fini. Si $|G| = 4$, alors G est abélien par (a). Si $|G| = p \in \{2, 3, 5\}$, alors G a un élément x d'ordre p, puisque p est premier. Ainsi $G = \langle x \rangle$ est cyclique et donc abélien. Le cas $G = \{e\}$ est trivial.

Exercice 4.

(a) Soit G un groupe. Suppose que $a, b \in G$ commutent et sont d'ordres finis $\mathrm{ord}(a) = n$ et $\mathrm{ord}(b) = m$ respectivement. Montrer que $(ab)^k = e$, où k est le plus petit multiple commun de n et m. En déduire que ab est d'ordre fini.

(b) Soit $G = GL_2(\mathbb{Q})$ et soient $A, B \in G$ donnés par les matrices

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

Montrer que $A^4 = I_2 = B^3$, mais que AB est d'ordre infini. En déduire que A et B ne commutent pas.

Solution.

(a) Comme a et b commutent, on a que $(ab)^k = a^k b^k = e$ puisque $n|k$ et $m|k$. Donc l'ordre de ab divise est plus petit que k et ab est d'ordre fini.

(b) Il est facile de voir que $A^4 = I_2 = B^3$. Pour $k \geq 1$, on a

$$(AB)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$$

Donc AB est d'ordre infini, puisque $(AB)^k \neq I_2$ pour tout $k \geq 1$. Par (a), on en déduit que A et B ne commutent pas.

Sous-groupes normaux

Exercice 5. Montrer que si $H < G$ est un sous-groupe d'indice $[G : H] = 2$, alors H est un sous-groupe normal de G.

Solution. Soit $g \in G$. On montre que $gH = Hg$. Si $g \in H$, alors $gH = H = Hg$. Supposons que $g \notin H$. Alors $\{H, gH\}$ est l'ensemble des classes à gauche, puisque $[G : H] = 2$. En particulier, $G \setminus H = gH$. De même, $\{H, Hg\}$ est l'ensemble des classes à droite et on a aussi $G \setminus H = Hg$. On conclut que $gH = Hg$. Donc H est normal dans G.

Exercice 6. Montrer que $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$ est un sous-groupe normal, où $GL_n(\mathbb{R})$ est muni de la multiplication matricielle.

Solution. On a déjà vu que $SL_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$. Il reste à montrer qu'il est normal. Soient $A \in SL_n(\mathbb{R})$ et $B \in GL_n(\mathbb{R})$. On doit montrer que $BAB^{-1} \in SL_n(\mathbb{R})$. Or $\det(BAB^{-1}) = \det(B) \cdot \det(A) \cdot \det(B^{-1}) = \det(B) \cdot \det(A) \cdot \det(B)^{-1} = \det(A) = 1$. Donc $SL_n(\mathbb{R})$ est un sous-groupe normal de $GL_n(\mathbb{R})$.

Exercice 7. Soient G un groupe et $H, K < G$ deux sous-groupes de G. On définit

$$HK = \{hk \mid h \in H, k \in K\}.$$

Montrer que:

(a) si H et K sont des sous-groupes normaux de G, alors $H \cap K$ est aussi un sous-groupe normal de G;

(b) si H est un sous-groupe normal de G, alors $H \cap K$ est un sous-groupe normal de K;

(c) si H est un sous-groupe normal de G, alors $HK = KH$ et HK est un sous-groupe de G;

(d) si H et K sont des sous-groupes normaux de G, alors HK est un sous-groupe normal de G;

(e) si H et K sont des sous-groupes normaux de G et $H \cap K = \{e\}$, alors $hk = kh$ pour tous $k \in K, h \in H$.

Solution.

(a) Soient $x \in H \cap K$ et $g \in G$. Comme H et K sont normaux, $gxg^{-1} \in H$ et $gxg^{-1} \in K$. Ainsi $gxg^{-1} \in H \cap K$ et $H \cap K$ est normal.

(b) Soient $x \in H \cap K$ et $k \in K$. Comme H est normal, $kxk^{-1} \in H$. Comme K est un sous-groupe et $x, k \in K$, alors $kxk^{-1} \in K$. Ainsi $kxk^{-1} \in H \cap K$ et $H \cap K$ est un sous-groupe normal de K.

(c) Comme H est normal, alors $gH = Hg$ pour tout $g \in G$. En particulier, $kH = Hk$ pour tout $k \in K$. D'où $KH = HK$. Il reste à montrer que HK est un sous-groupe. Soient $h_1, h_2 \in H$ et $k_1, k_2 \in K$. On veut montrer que $(h_1k_1)(h_2k_2) \in HK$. Comme $h_2k_2 \in HK = KH$, donc il existe $h_3 \in H, k_3 \in K$ tels que $h_2k_2 = k_3h_3$. De plus, $k_1k_3h_3 \in KH = HK$ et il existe $h_4 \in H, k_4 \in K$ tels que $k_1k_3h_3 = h_4k_4$. Ainsi

$$h_1k_1h_2k_2 = h_1k_1k_3h_3 = h_1h_4k_4 \in HK.$$

De plus, $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Donc HK est bien un sous-groupe.

(d) Soient $h \in H$, $k \in K$ et $g \in G$. On montre que $ghkg^{-1} \in HK$. On a $ghkg^{-1} = ghg^{-1}gkg^{-1} \in HK$ puisque H et K sont normaux. Donc HK est aussi normal.

(e) Soient $h \in H$ et $k \in K$. Alors $(hkh^{-1})k^{-1} \in K$ puisque K est normal. De même, $h(kh^{-1}k^{-1}) \in H$ puisque H est normal. Ainsi $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, i.e. $hkh^{-1}k^{-1} = e$ et donc $hk = kh$.

Exercice 8 (Groupe des quaternions)**.** On définit le groupe des quaternions $\mathbf{Q}$ comme étant le sous-groupe $\langle A, B\rangle$ de $GL_2(\mathbb{C})$ engendré par les matrices

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

Donner tous les éléments de $\mathbf{Q}$ en termes de A et B et montrer que l'ordre de $\mathbf{Q}$ est 8. Déterminer tous les sous-groupes de $\mathbf{Q}$.

Solution. On calcule que

$$A^2 = -I_2, A^3 = -A, A^4 = I_2, B^2 = -I_2, B^3 = -B, B^4 = I_2, AB = -BA.$$

Ainsi on peut écrire $\mathbf{Q} = \{I_2, -I_2, A, -A, B, -B, AB, -AB\}$ et $\mathbf{Q}$ est d'ordre 8. Les éléments $A, -A, B, -B, AB, -AB$ sont d'ordre 4 et l'élément $-I_2$ est d'ordre 2. Le groupe $\mathbf{Q}$ admet les sous-groupes suivants:

- $\{I_2\}$;
- $\langle -I_2\rangle = \{I_2, -I_2\}$;
- $\langle A\rangle = \langle -A\rangle = \{I_2, -I_2, A, -A\}$;
- $\langle B\rangle = \langle -B\rangle = \{I_2, -I_2, B, -B\}$;
- $\langle AB\rangle = \langle -AB\rangle = \{I_2, -I_2, AB, -AB\}$;
- $\mathbf{Q} = \langle A, B\rangle = \langle A, AB\rangle = \langle B, AB\rangle = \ldots$.

Exercice 9. Montrer que si G est abélien, alors tous les sous-groupes de G sont normaux. Montrer que l'implication inverse est fausse (*Utiliser l'Exercice 8*).

Solution. Supposons que G soit abélien. Soit $H < G$ un sous-groupe. Alors, si $g \in G$ et $h \in H$, on a $ghg^{-1} = gg^{-1}h = h \in H$. Donc H est normal.

Pour montrer que l'implication inverse est fausse, on montre que le groupe des quaternions $\mathbf{Q}$ est tel que tous ses sous-groupes sont normaux, mais il n'est pas abélien. Les sous-groupes $\{I_2\}$ et $\mathbf{Q}$ sont trivialement normaux. Les sous-groupes d'ordre 4 sont d'indice 2 dans $\mathbf{Q}$ et sont donc normaux par l'Exercice 5. Et clairement, $\{I_2, -I_2\}$ est normal. Ainsi tous les sous-groupes de $\mathbf{Q}$ sont normaux. Par contre, $AB = -BA \neq BA$, donc $\mathbf{Q}$ n'est pas abélien.