THÉORIE DES GROUPES - SÉRIE 4

11 octobre 2019

Groupes quotients

Exercice 1. Soient G et N les ensembles

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{R},\ ac \neq 0 \right\} \text{ et } N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{R} \right\}$$

muni de la multiplication matricielle. Montrer que:

(a) G, avec la multiplication matricielle, forme bien un groupe,

(b) N est un sous-groupe normal de G,

(c) G/N est abélien.

Solution.

(a) On remarque d'abord que $G \subset GL_2(\mathbb{R})$. De plus, la multiplication de deux éléments de G reste dans G et l'inverse d'un élément de G appartient à G. Ainsi G est un sous-groupe de $GL_2(\mathbb{R})$, et donc G est un groupe.

(b) Soient

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \quad \text{et} \quad B = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \in N.$$

On montre que $ABA^{-1} \in N$. En effet,

$$ABA^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix} = \begin{pmatrix} 1 & \frac{ad}{c} \\ 0 & 1 \end{pmatrix} \in N.$$

Donc N est normal dans G.

On aurait aussi pu utiliser l'application f du point (c) et voir que, comme N est le noyau de f, alors c'est un sous-groupe normal de G.

(c) L'application

$$f\colon G \to \mathbb{R}^* \times \mathbb{R}^*, \ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$$

est un homomorphisme de groupes. Son noyau est N et f est surjectif. Donc $G/N \cong \mathbb{R}^* \times \mathbb{R}^*$ par le premier théorème d'isomorphisme et G/N est abélien.

Exercice 2. A l'Exercice 6 de la Série 3, on a montré que $SL_n(\mathbb{R})$ est un sous-groupe normal de $GL_n(\mathbb{R})$. Calculer le quotient $GL_n(\mathbb{R})/SL_n(\mathbb{R})$.

Solution. On considère l'homomorphisme surjectif

$$\det\colon GL_n(\mathbb{R}) \to \mathbb{R}^*,\ A \mapsto \det(A).$$

Son noyau est $SL_n(\mathbb{R})$ et, par le premier théorème d'isomorphisme, on a $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$.

Exercice 3. Montrer que $\mathbb{C}^*$ muni de la multiplication est isomorphe en tant que groupe au quotient $\mathbb{C}/\mathbb{Z}$, où $\mathbb{C}$ est muni de l'addition.

Solution. On considère l'homomorphisme surjectif

$$f\colon \mathbb{C} \to \mathbb{C}^*,\ z \mapsto \exp(2\pi i \cdot z).$$

Son noyau est $\mathbb{Z}$ et, par le premier théorème d'isomorphisme, on a $\mathbb{C}/\mathbb{Z} \cong \mathbb{C}^*$.

Exercice 4. Soit p un nombre premier. Montrer que

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \ncong \mathbb{Z}/p^2\mathbb{Z}.$$

Solution. Supposons par l'absurde qu'on ait un isomorphisme de groupes

$$f\colon \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Soit $x \in \mathbb{Z}/p^2\mathbb{Z}$ d'ordre p^2 et soit $(a,b) = f(x) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Alors

$$f(p \cdot x) = p \cdot f(x) = p \cdot (a,b) = (p \cdot a, p \cdot b) = (0,0),$$

mais $p \cdot x \neq 0$. Donc f n'est pas injective. Contradiction.

Exercice 5. (A rendre pour le 18 octobre) Soient G un groupe fini et H un sous-groupe normal de G tel que $(|H|, [G:H]) = 1$. Montrer que H est l'unique sous-groupe de G d'ordre $|H|$.
Astuce: Si K est un autre sous-groupe d'ordre $|H|$, que se passe-t-il pour K dans G/H?

Solution. On propose deux solutions.

1. Soient $K < G$ un sous-groupe d'ordre $|H|$, $\pi : G \to G/H$ l'application quotient et π_K la restriction de π à K. Alors l'image de π_K est un sous-groupe de G/H dont son ordre divise $[G:H]$. De plus, par le premier théorème d'isomorphisme, l'image de π_K est isomorphe à un quotient de K, donc son ordre divise également $|K| = |H|$. Or $(|H|, [G:H]) = 1$, donc l'ordre de l'image de π_K vaut 1, i.e. elle est triviale. Ainsi $K < H = \mathrm{Ker}(\pi)$ et donc $K = H$ comme ils ont le même ordre.

2. Soit $K < G$ un sous-groupe d'ordre $|H|$. Par l'Exercice 7 (c) de la Série 3, comme H est normal, on a que KH est un sous-groupe de G, donc $|KH|$ divise $|G|$ par le théorème de Lagrange. Par le deuxième théorème d'isomorphisme, on a un isomorphisme de groupes

$$KH/H \cong K/K \cap H.$$

Ainsi $|KH| = \frac{|H|^2}{|K \cap H|}$, car $|H| = |K|$. Supposons par l'absurde que $K \neq H$, alors $K \cap H \subsetneq H$ et $\frac{|H|}{|K \cap H|} > 1$. Soit p un nombre premier qui divise $\frac{|KH|}{|H|} = \frac{|H|}{|H \cap K|} > 1$, alors p divise $|H|$. Comme $(|H|, [G:H]) = 1$, p ne divise pas $[G:H]$ et donc $p \cdot |H|$ ne divise pas $|G| = |H| \cdot [G:H]$. Cela contredit le fait que $p \cdot |H|$ divise $|KH|$ qui divise $|G|$.

Exercice 6. Soit G un groupe. On dit que H un **sous-groupe maximal** de G si, lorsque K est un sous-groupe tel que $H < K < G$, alors $K = H$ ou $K = G$, et on dit que H un **sous-groupe normal maximal** de G si, lorsque N est un sous-groupe normal tel que $H < N < G$, alors $N = H$ ou $N = G$. Montrer que:

(a) H est un sous-groupe normal maximal de G si et seulement si G/H n'a pas de sous-groupe normal (à part lui-même et $\{H\}$),

(b) si H est un sous-groupe maximal et H est normal dans G, alors $[G:H]$ est fini et égal à un nombre premier.

Solution.

(a) Pour commencer, on montre que l'application

$$\begin{aligned}\alpha\colon \{\text{sous-groupes normaux } N < G \text{ tels que } H < N\} &\to \{\text{sous-groupes normaux de } G/H\} \\ N &\mapsto N/H.\end{aligned}$$

est une bijection. Elle est bien définie, car, si N est normal dans G, alors N/H est normal dans G/H. On construit l'application inverse

$$\beta\colon \{\text{sous-groupes normaux de } G/H\} \to \{\text{sous-groupes normaux } N < G \text{ tels que } H < N\}.$$

Soit $N^* < G/H$ un sous-groupe normal. On pose $\beta(N^*) = \{g \in G \mid gH \in N^*\}$. On montre que $\beta(N^*)$ est un sous-groupe normal de G qui contient H. On a que

- $H \subset \beta(N^*)$, car $H \in N^*$,
- si $g, g' \in \beta(N^*)$, alors $gH, g'H \in N^*$ et donc $(gH)(g'H) = gg'H \in N^*$, d'où $gg' \in \beta(N^*)$,
- si $g \in \beta(N^*)$, alors $gH \in N^*$ et donc $(gH)^{-1} = g^{-1}H \in N^*$, d'où $g^{-1} \in \beta(N^*)$,
- si $g \in \beta(N^*)$ et $x \in G$, alors $gH \in N^*$ et, par normalité de N^*, $(xH)(gH)(xH)^{-1} = xgx^{-1}H \in N^*$, d'où $xgx^{-1} \in \beta(N^*)$.

Finalement, on a que $\beta(N^*)/H = \{gH \mid g \in \beta(N^*)\} = N^*$, par définition, et on a aussi $\beta(N/H) = \{g \in G \mid gH \in N/H\} = N$. En effet, on a bien $N \subset \beta(N/H)$. Inversément, si $g \in \beta(N/H)$, alors il existe $n \in N$ tel que $gH = nH$, i.e. $gn^{-1} \in H \subset N$. Comme N est un sous-groupe et $gn^{-1}, n \in N$, alors $g \in N$. Cela prouve que α est bijective.

Par la bijection α, les seuls sous-groupes normaux N tels que $H < N < G$ sont H et G si et seulement si les seuls sous-groupes normaux de G/H sont $H/H = \{H\}$ et G/H. Cela prouve (a).

(b) Par de mêmes arguements qu'en (a), puisque H est normal, on a une bijection

$$\begin{aligned}\overline{\alpha}\colon \{\text{sous-groupes } N < G \text{ tels que } H < N\} &\to \{\text{sous-groupes de } G/H\} \\ N &\mapsto N/H.\end{aligned}$$

Comme H est maximal, les seuls sous-groupes de G tels que $H < N$ sont H et G. Par la bijection $\overline{\alpha}$, les seuls sous-groupes de G/H sont $H/H = \{H\}$ et G/H. Soit $gH \in G/H$ tel que $gH \neq H$. Alors le sous-groupe $\langle gH \rangle < G/H$ engendré par gH n'est pas trivial, d'où $\langle gH \rangle = G/H$. Ainsi G/H est cyclique. Si G/H est infini, alors $G/H \cong \mathbb{Z}$, ce qui est absurde puisque $\mathbb{Z}$ a des sous-groupes non triviaux. Donc $[G:H] = |G/H|$ est fini. Posons $n = [G:H]$. Alors $G/H \cong \mathbb{Z}/n\mathbb{Z}$. Par la bijection $\overline{\alpha}$ appliquée à $\mathbb{Z}$ et $n\mathbb{Z}$, les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ son, ce qui signifie que $m|n$. Si G/H a exactement deux sous-groupes, alors n a exactement deux diviseurs, 1 et lui-même. Ainsi n est premier.

Exercice 7. Prouver le troisième théorème d'isomorphisme.

Soit G un groupe et soient K et H des sous-groupes normaux de G tels que $K < H < G$. Alors H/K est un sous-groupe normal de G/K et

$$(G/K)/(H/K) \cong G/H.$$

Solution. Il est facile de vérifier que H/K est un sous-groupe normal de G/K, puisque

$$(gK)(hK)(gK)^{-1} = ghg^{-1}K$$

pour tous $g \in G, h \in H$. On pose

$$f\colon G/K \to G/H,\ gK \mapsto gH.$$

Alors f est bien définie, car $K < H$, et f est clairement un homomorphisme de groupes surjectif. De plus, son noyau est H/K. En effet, $f(gK) = H$ si et seulement si $g \in H$ si et seulement si $gK \in H/K$. On peut conclure par le premier théorème d'isomorphisme.

Exercice 8. Montrer que:

(a) si H et K sont des sous-groupes normaux d'un groupe G tels que $HK = G$, alors

$$G/(H \cap K) \cong (G/H) \times (G/K).$$

(b) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est cyclique,

(c) plus généralement, si $(a, b) = 1$, $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est cyclique.

Solution.

(a) On pose

$$f\colon G \to (G/H) \times (G/K),\ g \mapsto (gH, gK).$$

Alors f est un homomorphisme de groupes. Soit $(xH, yK) \in (G/H)\times(G/K)$. Comme $G = HK$, alors il existe $h \in H, k \in K$ tels que $x^{-1}y = hk^{-1}$. Alors $xh = yk$ et $(xhH, ykK) = (xH, yK)$ et f est surjective. De plus, $f(g) = (H, K)$ si et seulement si $g \in H \cap K$. Donc $\mathrm{Ker}(f) = H \cap K$. On conclut par le premier théorème d'isomorphisme.

(b) On a que $1 \in 2\mathbb{Z} + 3\mathbb{Z}$, car $1 = (-1) \cdot 2 + 3$, donc $\mathbb{Z} = 2\mathbb{Z} + 3\mathbb{Z}$. Par (a), on obtient que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/(2\mathbb{Z} \cap 3\mathbb{Z}) = \mathbb{Z}/6\mathbb{Z}$. Donc $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est cyclique d'ordre 6.

(c) Par l'identité de Bézout, il existe $r, s \in \mathbb{Z}$ tels que $1 = (a, b) = ra + sb$. Ainsi $\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. Par a), on obtient que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/(a\mathbb{Z} \cap b\mathbb{Z}) = \mathbb{Z}/(ab)\mathbb{Z}$. Donc $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est cyclique d'ordre ab.