

Licence – Mathématiques
Algèbre 2

COURS À DISTANCE – SEMAINE 1 – GROUPE QUOTIENTS – CORRIGÉ TD 2

Exercice 1. On note O l'origine du plan euclidien $\mathbb{R}^2$. Montrer que $\{\text{rotations autour de } O\}$ est un sous-groupe non distingué des isométries du plan.

La multiplication est donnée ici par la composition des isométries. Notons r_α la rotation de centre O et d'angle $\alpha \in \mathbb{R}$. On a $r_\beta \circ r_\alpha = r_{\alpha+\beta}$ et $r_\alpha^{-1} = r_{-\alpha}$. Ainsi l'ensemble des rotations de centre O est non vide et stable par composition et passage à l'inverse. C'est donc un sous-groupe du groupe des isométries du plan.

Considérons maintenant la translation $\tau : \begin{cases} \mathbb{R}^2 & \rightarrow & \mathbb{R}^2 \\ (x, y) & \mapsto & (x+1, y) \end{cases}$ et l'isométrie $f = \tau \circ r_\pi \circ \tau^{-1}$ conjuguée à r_π . On a $f(O) = \tau \circ r_\pi(-1, 0) = \tau(1, 0) = (2, 0)$. Ainsi f ne fixe pas O , ce n'est donc pas une rotation de centre O . On en déduit que le sous-groupe des rotations de centre O n'est pas distingué dans le groupe des isométries du plan.

Exercice 2. On fixe $n \in \mathbb{N}$ et on considère les ensembles

$$\mathbb{U} := \{z \in \mathbb{C} \mid |z| = 1\} \quad \mathbb{U}_n := \{z \in \mathbb{C} \mid z^n = 1\} \quad \mathbb{U}_\infty := \{z \in \mathbb{C} \mid \exists k \in \mathbb{N}, z^k = 1\}.$$

1. Montrer que, pour la multiplication, $\mathbb{U}$, $\mathbb{U}_n$ et $\mathbb{U}_\infty$ sont des sous-groupes distingués de $\mathbb{C}^*$, et que $\mathbb{U}_n \subset \mathbb{U}_\infty \subset \mathbb{U}$.

L'inclusion $\mathbb{U}_n \subset \mathbb{U}_\infty$ est évidente. Si $z^k = 1$, on l'égalité $|z|^k = 1$ dans $\mathbb{R}_+$, donc $|z| = 1$. Ainsi $\mathbb{U}_\infty \subset \mathbb{U}$. Ces trois ensembles sont non vides car ils contiennent 1. On vérifie facilement qu'ils sont stables par passage à l'inverse. Il est clair que $\mathbb{U}_n$ et $\mathbb{U}$ sont stables par multiplication. Prenons $z, w \in \mathbb{U}_\infty$. Soient $k, \ell \in \mathbb{N}$ tels que $z^k = 1$ et $w^\ell = 1$. Alors $(zw)^{k\ell} = 1$. Ainsi $\mathbb{U}_\infty$ est aussi stable par multiplication. Comme $\mathbb{C}^*$ est un groupe abélien, tous ses sous-groupes sont distingués.

2. Montrer que les groupes $\mathbb{R}/\mathbb{Z}$, $\mathbb{C}^*/\mathbb{R}_+^*$, $\mathbb{C}^*/\mathbb{R}^*$ et $\mathbb{U}/\mathbb{U}_n$ sont tous isomorphes à $\mathbb{U}$.

Les applications

$$f : \begin{cases} \mathbb{R} & \rightarrow & \mathbb{U} \\ x & \mapsto & e^{2i\pi x} \end{cases}, \quad g : \begin{cases} \mathbb{C}^* & \rightarrow & \mathbb{U} \\ z & \mapsto & \frac{z}{|z|} \end{cases}, \quad h : \begin{cases} \mathbb{C}^* & \rightarrow & \mathbb{U} \\ z & \mapsto & \left(\frac{z}{|z|}\right)^2 \end{cases} \quad \text{et} \quad \varphi : \begin{cases} \mathbb{U} & \rightarrow & \mathbb{U} \\ z & \mapsto & z^n \end{cases}$$

sont des morphismes de groupes surjectifs (on peut remarquer que $h(e^{ix/2}) = e^{ix}$ et $\varphi(e^{ix/n}) = e^{ix}$). Les noyaux de ces morphismes sont

$$\ker(f) = \mathbb{Z}, \quad \ker(g) = \mathbb{R}_+^*, \quad \ker(h) = \mathbb{R}^* \quad \text{et} \quad \ker(\varphi) = \mathbb{U}_n.$$

Par le premier théorème d'isomorphisme, on en déduit que les groupes $\mathbb{R}/\mathbb{Z}$, $\mathbb{C}^*/\mathbb{R}_+^*$, $\mathbb{C}^*/\mathbb{R}^*$ et $\mathbb{U}/\mathbb{U}_n$ sont tous isomorphes à $\mathbb{U}$.

3. Montrer que $\mathbb{C}^*/\mathbb{U}_n$ est isomorphe à $\mathbb{C}^*$.

On applique à nouveau le premier théorème d'isomorphisme au morphisme de groupe surjectif

$$\psi : \begin{cases} \mathbb{C}^* & \rightarrow & \mathbb{C}^* \\ z & \mapsto & z^n \end{cases} \quad \text{de noyau } \ker(\psi) = \mathbb{U}_n.$$

4. Montrer que $\mathbb{U}_\infty$ est isomorphe à $\mathbb{Q}/\mathbb{Z}$.

L'application $\phi : \begin{cases} \mathbb{Q} & \rightarrow & \mathbb{U}_\infty \\ x & \mapsto & e^{2i\pi x} \end{cases}$ est bien définie car si $x = \frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, alors $\phi(x)^q = e^{2i\pi p} = 1$. C'est un morphisme de groupes. Soit $z \in \mathbb{U}_\infty$ et $k \in \mathbb{N}$ tel que $z^k = 1$. Alors $z = e^{2i\pi\ell/k} = \phi(\frac{\ell}{k})$ pour un $\ell \in \mathbb{Z}$. Donc ϕ est surjective. De plus, $\ker(\phi) = \mathbb{Z}$. On conclut encore avec le premier théorème d'isomorphisme.

Exercice 3.

1. Montrer que $\mathbb{Z}$ est un sous-groupe distingué de $\mathbb{Q}$.
L'ensemble $\mathbb{Z}$ est un sous-groupe de $\mathbb{Q}$ qui est abélien.
2. Montrer que, pour tout $n \in \mathbb{N}^*$, il existe un élément d'ordre n dans $\mathbb{Q}/\mathbb{Z}$.
On a $n \cdot \frac{1}{n} = 1 \in \mathbb{Z}$ et, pour tout $k \in \llbracket 1, n-1 \rrbracket$, $k \cdot \frac{1}{n} = \frac{k}{n} \notin \mathbb{Z}$. Donc la classe de $\frac{1}{n}$ est d'ordre n dans $\mathbb{Q}/\mathbb{Z}$.
3. Montrer que tout élément de $\mathbb{Q}/\mathbb{Z}$ est d'ordre fini.
Comme $q \cdot \frac{p}{q} = p \in \mathbb{Z}$ pour tout rationnel $\frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{Z}^*$, la classe de tout rationnel est d'ordre fini dans $\mathbb{Q}/\mathbb{Z}$.

Exercice 4. Soit $T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{R}^*, b \in \mathbb{R} \right\}$ et $U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}$.

1. Montrer que T est un sous-groupe de $\text{GL}_2(\mathbb{R})$. Est-il distingué ?
L'ensemble T contient la matrice identité et on vérifie par calcul direct qu'il est stable par multiplication et passage à l'inverse. C'est donc un sous-groupe de $\text{GL}_2(\mathbb{R})$.
Prenons $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \text{GL}_2(\mathbb{R})$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in T$. On a alors $ABA^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \notin T$. Donc T n'est pas distingué dans $\text{GL}_2(\mathbb{R})$.
2. Montrer que U est un sous-groupe de T . Est-il distingué ?
L'ensemble U est non vide et stable par multiplication et passage à l'inverse, donc c'est un sous-groupe de T .
Soient $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in T$ et $B = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \in U$. On a $ABA^{-1} = \begin{pmatrix} 1 & \frac{a\beta}{c} \\ 0 & 1 \end{pmatrix} \in U$. Donc U est distingué dans T . Notons que U n'est pas distingué dans $\text{GL}_2(\mathbb{R})$, comme le montre la réponse à la question précédente.

Exercice 5.

1. Montrer que la relation "être un sous-groupe" est une relation d'ordre sur les groupes.
C'est une relation réflexive : tout groupe est son propre sous-groupe. Elle est transitive : si K est un sous-groupe de H et H est un sous-groupe de G , alors K est contenu dans G , non vide, stable par multiplication et passage à l'inverse, donc K est un sous-groupe de G . Elle est également anti-symétrique : si H est un sous-groupe de G et G est un sous-groupe de H , alors, par double inclusion, on a $H = G$.
2. Montrer que la relation "être un sous-groupe distingué" n'est pas une relation d'ordre sur les groupes.
Comme précédemment, cette relation est réflexive et anti-symétrique. On va voir par un contre-exemple qu'elle n'est pas transitive. On considère le groupe diédral D_4 des isométries du plan préservant un carré. On note r la rotation de centre le centre de symétrie du carré et d'angle $\pi/2$. On note s une symétrie par rapport à l'un des axes de symétrie du carré. Le groupe D_4 contient exactement 8 éléments : $D_4 = \{1, r, r^2, r^3, s, s \circ r, s \circ r^2, s \circ r^3\}$. On a dans D_4 les relations suivantes :

$$r \circ s = s \circ r^3, \quad r^2 \circ s = s \circ r^2, \quad r^3 \circ s = s \circ r.$$

On considère maintenant le sous-groupe $\langle r^2, s \rangle$ de D_4 . Il contient exactement 4 éléments : $\langle r^2, s \rangle = \{1, r^2, s, s \circ r^2\}$. On vérifie à la main qu'il est abélien, ce qui implique en particulier que son sous-groupe $\langle s \rangle$ est distingué. On vérifie également, en utilisant les relations ci-dessus, que $\langle r^2, s \rangle$ est distingué dans D_4 . Ces relations donnent aussi

$$r \circ s \circ r^{-1} = s \circ r^2 \notin \langle s \rangle,$$

ce qui montre que $\langle s \rangle$ n'est pas distingué dans D_4 . En résumé, $\langle s \rangle$ est distingué dans $\langle r^2, s \rangle$ qui est distingué dans D_4 , mais $\langle s \rangle$ n'est pas distingué dans D_4 .

Exercice 6. Soit $n_1, \dots, n_k \in \mathbb{N}^*$ des entiers deux à deux premiers entre eux. On considère l'application

$$\varphi: \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \\ n & \longmapsto & (n \ [n_1], n \ [n_2], \dots, n \ [n_k]) \end{array}.$$

1. Montrer que φ est un morphisme de groupes.

L'addition est compatible avec les relations de congruences, donc $\varphi(n+m) = \varphi(n) + \varphi(m)$.

2. Déterminer le noyau de φ .

Un entier n est dans le noyau de φ si et seulement si il est divisible par tous les n_i . Comme les n_i sont deux à deux premiers entre eux, c'est équivalent à être divisible par le produit $n_1 n_2 \dots n_k$. Donc $\ker(\varphi) = n_1 n_2 \dots n_k \mathbb{Z}$.

3. Redémontrer le théorème des restes chinois.

Il faut montrer que φ est un morphisme surjectif. Prenons des entiers $a_1, \dots, a_k$ et cherchons $n \in \mathbb{Z}$ tel que $n = a_i \ [n_i]$ pour tout $i \in \{1, \dots, k\}$. Pour tout i , n_i est premier avec $\hat{n}_i = \prod_{j \neq i} n_j$, donc on a une relation de Bézout $u_i n_i + v_i \hat{n}_i = 1$. On pose alors $n = \sum_{i=1}^k a_i v_i \hat{n}_i$. On vérifie que $n = a_i \ [n_i]$, donc φ est surjectif. Ainsi, par le premier théorème d'isomorphisme, φ induit un isomorphisme

$$\bar{\varphi}: \begin{cases} \mathbb{Z}/n_1 n_2 \dots n_k \mathbb{Z} & \rightarrow & \mathbb{Z}/n_1 \mathbb{Z} \times \mathbb{Z}/n_2 \mathbb{Z} \times \dots \times \mathbb{Z}/n_k \mathbb{Z} \\ n & \mapsto & (n \ [n_1], n \ [n_2], \dots, n \ [n_k]) \end{cases},$$

ce qui implique le théorème des restes chinois.