

Fiche de TD 4

Exercice 1 Parmi les exemples suivants, quels sont ceux qui sont des groupes?

- i) (S^1, \cdot) où $S^1 = \{z \in \mathbf{C}^\times, |z| = 1\}$ est le cercle unité du plan.
- ii) $(\mathcal{C}, +)$, (\mathcal{C}^*, \cdot) où $\mathcal{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, a, b \in \mathbf{R} \right\}$, $\mathcal{C}^* = \mathcal{C} \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$, $+$ est l'addition et \cdot la multiplication des matrices.
- iii) $(\mathcal{S}, +)$ et (\mathcal{S}^*, \cdot) , où $\mathcal{S} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix}, a, b \in \mathbf{R} \right\}$, $\mathcal{S}^* = \mathcal{S} \setminus \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$, $+$ est l'addition et \cdot la multiplication des matrices.
- iv) $(Sl_2(\mathbf{C}), \cdot)$ où $Sl_2(\mathbf{C}) = \{A \in Gl_2(\mathbf{C}), \det(A) = 1\}$ et \cdot est la multiplication matricielle.
- v) (GA_1, \circ) où GA_1 est l'ensemble des applications $\mathbf{R} \rightarrow \mathbf{R} : x \mapsto ax + b$, $(a, b) \in \mathbf{R}^2, a \neq 0$, et \circ est la composition des applications.
- vi) $(\mathcal{D}, +)$, $(\mathcal{D} \setminus \{0\}, \cdot)$ où $\mathcal{D} = \left\{ \frac{a}{2^l}, a \in \mathbf{Z}, l \in \mathbf{N} \right\} \subset \mathbf{Q}$. (\mathcal{D} est appelé l'ensemble des *rationnels dyadiques*.)
- vii) $(\mathbf{Q}[\sqrt{p}], +)$, $(\mathbf{Q}[\sqrt{p}] \setminus \{0\}, \cdot)$ où p est un nombre premier et $\mathbf{Q}[\sqrt{p}] = \{a + b\sqrt{p}, a, b \in \mathbf{Q}\}$.
- viii) $(S_P, \circ), (G_P, \circ)$, où pour un ensemble X et une partie $P \subset X$, S_P (resp. G_P) désigne l'ensemble des bijections $\sigma : X \rightarrow X$ telles que $\sigma(P) \subset P$ (resp. $\sigma(P) = P$) et \circ est la composition des applications.
 [Pour S_P , on pourra par exemple prendre pour X le plan réel, pour P le disque unité et pour σ l'application $(x, y) \mapsto \left(\frac{x}{2}, \frac{y}{2}\right)$]

Exercice 2

- i) Faire la liste des tables de composition possibles d'un groupe ayant deux éléments $\{e, x\}$ et ayant trois éléments $\{e, x, y\}$. (La lettre e désigne le neutre du groupe.)
- ii) Même question pour un groupe d'ordre 4.
- iii) A notations près, combien y-a-t-il de tables de groupe d'ordre 5?
 [Se servir de l'ordre d'un élément $x \neq e$.]

Exercice 3 Soit G un groupe (de neutre e) tel que $x^2 = e$ pour tout $x \in G$.

- i) Montrer que G est abélien.
- ii) Soit $n \in \mathbf{N} \setminus \{0\}$. Donner un exemple de G d'ordre 2^n .
 [Se servir de $\mathbf{Z}/2\mathbf{Z}$ et du produit direct.]
- iii) Donner un exemple de G d'ordre infini.
 [Penser aux suites.]

Exercice 4 (Rappel de cours sur l'ordre)

Soit G un groupe (de neutre noté e), $x \in G$ un élément d'ordre fini n et $m \in \mathbf{N}$ un entier.

- i) Confirmer que $x^m = e \Leftrightarrow n \mid m$.
- ii) Confirmer que l'élément x^m est d'ordre $\frac{n}{\text{pgcd}(m,n)}$.

Exercice 5 Dans cet exercice, $((\mathbf{Z}/n\mathbf{Z})^*, \cdot)$ désigne le groupe des inversibles multiplicatifs de l'anneau de congruence $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$. On rappelle que pour un entier $a \in \mathbf{Z}$,

$$\bar{a} \in (\mathbf{Z}/n\mathbf{Z})^* \Leftrightarrow \text{pgcd}(a, n) = 1 \Leftrightarrow \bar{a} \text{ est un générateur du groupe cyclique } (\mathbf{Z}/n\mathbf{Z}, +).$$

- i) Faire la liste des générateurs du groupe cyclique $(\mathbf{Z}/8\mathbf{Z}, +)$.
- ii) Montrer que le groupe $((\mathbf{Z}/8\mathbf{Z})^*, \cdot)$ n'est pas un groupe cyclique.
- iii) Montrer que $((\mathbf{Z}/9\mathbf{Z})^*, \cdot)$ est cyclique. Faire la liste de ses générateurs.
- iv) Montrer que $((\mathbf{Z}/17\mathbf{Z})^*, \cdot)$ est cyclique.

[L'ordre d'un élément divise l'ordre du groupe.]

Exercice 6

Montrer que le groupe $H \times K$, produit direct des groupes finis H et K , est un groupe cyclique ssi H et K sont cycliques d'ordres premiers entre eux (i.e. $\text{pgcd}(|H|, |K|) = 1$).

[Se servir du calcul de l'ordre d'un élément $(h, k) \in H \times K$.]

Exercice 7 (Sous-groupes d'un groupe cyclique)

Le théorème de Lagrange assure que tout sous-groupe $H \leq G$ d'un groupe fini G est d'ordre un diviseur d de $|G|$. On se propose ici de démontrer une *réciproque* de ce théorème pour les groupes cycliques.

On suppose $G = \langle x \rangle$ cyclique d'ordre n et soit d un diviseur de n .

- i) Montrer que tout sous-groupe $H \leq G$ est cyclique.
[On pourra s'inspirer de l'étude des sous-groupes de \mathbf{Z} et considérer l'entier $\min\{l \in \mathbf{N} \setminus \{0\}, x^l \in H\}$]
- ii) Montrer que le sous-groupe $\langle x^{\frac{n}{d}} \rangle$ est d'ordre d .
- iii) Montrer que $\langle x^{\frac{n}{d}} \rangle$ est l'unique sous-groupe d'ordre d de G .
- iv) Montrer que G contient exactement $\varphi(d)$ éléments d'ordre d (φ est l'indicatrice d'Euler).
- v) En déduire que $\sum_{d|n} \varphi(d) = n$.
- vi) A titre d'exemple, faire la liste des sous-groupes du groupe U_{12} des racines douzièmes de l'unité et/ou du groupe $(\mathbf{Z}/12\mathbf{Z}, +)$.

Rappel: Soit G un groupe et $P \subset G$ une partie. Le sous-groupe $\langle P \rangle \leq G$ engendré par P est l'intersection de tous les sous-groupes de G contenant P . C'est, pour l'inclusion, le plus petit sous-groupe de G contenant P .

Si $P = \{x\}$, $\langle P \rangle = \langle x \rangle$ (le sous-groupe monogène engendré par x). Dans le groupe $(\mathbf{Z}, +)$, pour tout entier a , $\langle a \rangle = \mathbf{Z}a = \{la, l \in \mathbf{Z}\}$.

Exercice 8 Soient a et b deux nombres réels.

i) Vérifier que $\mathbf{Z}a + \mathbf{Z}b = \{ka + lb, (k, l) \in \mathbf{Z}^2\}$ est un sous-groupe de $(\mathbf{R}, +)$. Montrer que $\mathbf{Z}a + \mathbf{Z}b = \langle a, b \rangle$.

ii) On suppose a et b rationnels. Existe-t-il un nombre rationnel c tel que

$$\mathbf{Z}a + \mathbf{Z}b = \mathbf{Z}c?$$

iii) On suppose a rationnel et b irrationnel. Existe-t-il un nombre réel c tel que

$$\mathbf{Z}a + \mathbf{Z}b = \mathbf{Z}c?$$

iv) Soient p et q deux nombres premiers. Existe-t-il un nombre réel c tel que

$$\mathbf{Z} \ln(p) + \mathbf{Z} \ln(q) = \mathbf{Z}c?$$

($x \mapsto \ln(x)$ est le logarithme népérien.)

Exercice 9 (Le groupe quaternionique Q_8 .)

Dans $Gl_2(\mathbf{C})$, notons

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

i) Calculer I^2, J^2, K^2 et IJ, JK, KI .

ii) En déduire les produits JI, KJ, IK .

iii) En déduire la liste des éléments du sous-groupe $\langle I, J \rangle$ de $Gl_2(\mathbf{C})$ engendré par I et J . Ce sous-groupe est noté Q_8 .

iv) Déterminer le centre de Q_8 .

v) Faire la liste des sous-groupes de Q_8 . Sont-ils tous distingués?

Exercice 10 (Le groupe diédral D_n)

On rappelle que

$$O_2(\mathbf{R}) = \left\{ A \in M_2(\mathbf{R}), {}^t AA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

est l'ensemble (des matrices dans la base canonique) des isométries linéaires du plan \mathbf{R}^2 . $O_2(\mathbf{R})$ est un sous-groupe de $Gl_2(\mathbf{R})$ appelé le *groupe orthogonal*.

Si $A \in O_2(\mathbf{R})$, $\det(A) = \pm 1$.

Si $\det(A) = 1$, $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = R(\theta)$ est la matrice d'une rotation d'angle $\theta \in \mathbf{R}$.

Si $\det(A) = -1$, $A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} = S(\theta)$ est la matrice d'une réflexion de droite fixe D_θ passant par $(0, 0)$ et $(\cos\frac{\theta}{2}, \sin\frac{\theta}{2})$.

Soit maintenant $n \geq 3$ et soit C_n le polygone régulier à n côtés de centre $(0, 0)$ et dont l'un des sommets est $(1, 0)$. (Les sommets de C_n sont les racines n -ièmes de l'unité dans $\mathbf{C} \simeq \mathbf{R}^2$.)

On se propose ici de décrire le groupe D_n des isométries du plan qui conservent l'ensemble des sommets de C_n . Ce groupe D_n est appelé le *groupe diédral*.

- i) Faire la liste (des matrices) des rotations de D_n . Montrer que celles-ci constituent un sous-groupe cyclique $\langle R \rangle \leq D_n$ dont on précisera un générateur R . (Ce générateur n'est pas unique.)
- ii) Expliciter la matrice S d'une réflexion (au choix) de D_n . En se servant du rappel, montrer que toute matrice de réflexion S' de D_n s'écrit $S' = SR'$ avec $R' \in \langle R \rangle$.
- iii) Conclure que $D_n = \langle R \rangle \cup S\langle R \rangle$ et que $|D_n| = 2n$.
- iv) Montrer que le sous-groupe $\langle R \rangle$ est distingué dans D_n .
- v) Soit $P = \{R, S\}$. Identifier le sous-groupe $\langle P \rangle \leq Gl_2(\mathbf{R})$.
- vi) A titre d'exemple, faire la liste des six matrices de D_3 et des huit matrices de D_4 .

Exercice 11 Soient H et K deux groupes finis (de neutres respectifs e_H et e_K) et $\varphi : H \rightarrow K$ un morphisme de groupes.

- i) Montrer que $\varphi(e_H) = e_K$ et pour tout entier $n \geq 0$ et $h \in H$, $\varphi(h^n) = (\varphi(h))^n$.
 - ii) Montrer que pour tout $h \in H$, $\varphi(h)^{\text{ord}(h)} = e_K$. En déduire que l'ordre de $\varphi(h)$ divise l'ordre de h .
 - iii) On suppose φ injectif. Calculer $\varphi(h^{\text{ord}(\varphi(h))})$ et en déduire que l'ordre de h divise l'ordre de $\varphi(h)$.
 - iv) Soit $d \in \mathbf{N} \setminus \{0\}$. Que peut-on conclure sur les éléments d'ordre d de deux groupes finis H et K isomorphes?
 - v) Soit p un nombre premier.
 - Que peut-on dire d'un groupe d'ordre p ?
 - Donner deux groupes abéliens d'ordre p^2 non isomorphes.
 - Donner trois groupes abéliens d'ordre p^3 non isomorphes.
- [Se servir du produit direct.]

Exercice 12 Expliquer pourquoi il y a au moins cinq groupes d'ordre 8 deux à deux non isomorphes.

[Utiliser l'exercice 11 et les groupes D_4 et Q_8 .]

Exercice 13 Soient deux anneaux $(A, +, \cdot)$ et $(B, +, \cdot)$ d'unités respectives 1_A et 1_B .

- i) Confirmer que $A \times B$ est un anneau pour les lois

$$(a, b) + (a', b') = (a + a', b + b'), \quad (a, b) \cdot (a', b') = (aa', bb').$$

- ii) Confirmer que le groupe $(A \times B)^*$ des inversibles multiplicatifs de l'anneau produit $A \times B$ est égal au produit direct $A^* \times B^*$ des groupes des inversibles multiplicatifs de A et de B .

On dit que $\psi : A \rightarrow B$ est un *morphisme d'anneaux* si 1) ψ est un morphisme de groupes de $(A, +)$ vers $(B, +)$, 2) $\psi(1_A) = 1_B$ et 3) pour tout $(a, a') \in A^2$, $\psi(aa') = \psi(a)\psi(a')$.

iii) Soit $\psi : A \rightarrow B$ un morphisme d'anneaux.

- Montrer que $\psi(A^*) \leq B^*$.

- On suppose ψ bijectif. Montrer que $\psi^{-1} : B \rightarrow A$ est aussi un morphisme d'anneaux et que $\psi(A^*) = B^*$.

Exercice 14 (Les restes chinois (bis))

Soient $m, n \in \mathbf{N} \setminus \{0\}$ premiers entre eux. On considère l'anneau produit $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ (défini dans l'exercice 13).

i) Montrer que l'application

$$\psi : \mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} : x \mapsto (\bar{x}_m, \bar{x}_n)$$

est un morphisme d'anneaux.

ii) En vous servant du théorème des restes chinois montrer que ψ est surjective.

iii) Confirmer que ψ est constante sur les classes de congruence modulo mn et en déduire que ψ induit une application

$$\bar{\psi} : \mathbf{Z}/mn\mathbf{Z} \rightarrow \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}.$$

iv) Montrer que $\bar{\psi}$ est un isomorphisme d'anneaux.

v) En prenant la restriction de $\bar{\psi}$ aux inversibles multiplicatifs, montrer que $\varphi(mn) = \varphi(m)\varphi(n)$. (φ est l'indicatrice d'Euler.)

vi) Soit p un nombre premier et $l \in \mathbf{N} \setminus \{0\}$. Calculer $\varphi(p^l)$. En se servant de la factorisation primaire, en déduire une expression de $\varphi(n)$ pour tout entier naturel $n > 0$. Que vaut $\varphi(1000)$?

[*Terminologie*: une application $\phi : \mathbf{N}^* \rightarrow \mathbf{N}^*$ telle que $\phi(ab) = \phi(a)\phi(b)$ pour tout a et b premiers entre eux est dite *arithmétiquement multiplicative*.]