Feuille 1

Exercice 1.

Calculer l'orde de tous les éléments des groupes :

a) D_6

b) D_8

Exercice 2.

Trouver tous les sous-groupes cycliques de D_8.

Trouver un sous-groupe propre de D_8 qui n'est pas cyclique.

Exercice 3.

Utiliser les générateurs et les relations de la présentation $\mathrm{D}_{2n} =< r, s \mid r^n = s^2 = 1, rs = sr^{-1} >$ pour montrer que chaque élément de D_{2n} qui n'est pas une puissance de r est d'ordre 2. En déduire que D_{2n} est engendré par les deux éléments s et sr, tous les deux d'ordre 2.

Exercice 4.

Soit n un entier ≥ 3. Montrer que :

a) le centre du groupe diédral $Z(\mathrm{D}_{2n}) = \{1\}$, si n est impair ;

b) $Z(\mathrm{D}_{2n}) = \{1,\, r^k\}$, si $n = 2k$ est pair.

Exercice 5.

a) Soit $\mathbb{F}_2$ le corps fini de deux éléments. Montrer que l'ordre de $\mathrm{GL}_2(\mathbb{F}_2)$ est égal à 6.

b) Doqnner les éléments de $\mathrm{GL}_2(\mathbb{F}_2)$ et calculer l'ordre de chaque élément.

Exercice 6.

Soient F un corps et $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$ le groupe de Heisenberg de F. Soient

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$$

des éléments de $H(F)$.

a) Calculer le produit XY et en déduire que $H(F)$ est fermé sous la multiplication de matrices. Montrer que $H(F)$ n'est pas abélien.

b) Donner une formule pour l'inverse X^{-1} et en déduire que $H(F)$ est fermé sous l'inverse.

c) Montrer que $H(F)$ est un groupe d'ordre $|F|^3$.

d) Trouver l'ordre de chaque élément du groupe $H(\mathbb{Z}/2\mathbb{Z})$.

d) Montrer que chaque élément non-trivial de $H(\mathbb{R})$ est d'ordre infini.

Exercice 7.

Soit G le groupe $\mathrm{SL}_2(\mathbb{Z})$. Montrer que

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad Y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

sont d'ordre fini mais pas XY.

Exercice 8.

Soit G un groupe abélien fini d'exposant e. Montrer que G contient un élément d'ordre e.

Exercice 9.

Soit $n \in \mathbb{N}^*$. Soient r et s les générateurs usuels de D_{2n}. Posons $\theta = 2\pi/n$. Montrer que l'application $\phi\colon \mathrm{D}_{2n} \to \mathrm{GL}_2(\mathbb{R})$ définie sur les générateurs par

$$\phi(r) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \quad \text{et} \quad \phi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

définit un morphisme injectif de D_{2n} dans $\mathrm{GL}_2(\mathbb{R})$.

Exercice 10.

Soient i et j les générateurs usuels de $Q_8 =< i, j \mid i^4 = 1, i^2 = j^2, iji = j >$. Montrer que l'application $\phi\colon Q_8 \mapsto \mathrm{GL}_2(\mathbb{C})$ définie sur les générateurs par

$$\phi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \quad \text{et} \quad \phi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

définit un morphisme injectif de Q_8 dans $\mathrm{GL}_2(\mathbb{C})$.

Exercice 11.

a) Pour tout groupe G, montrer que l'on a une bijection entre les groupes $\mathrm{Hom}_{\mathrm{gp}}(\mathbb{Z}, G)$ et G. Lorsque G est abélien, montrer qu'il s'agit d'un isomorphisme de groupes.

b) Déterminer

$$\mathrm{Hom}_{\mathrm{gp}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}), \qquad \mathrm{Hom}_{\mathrm{gp}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}), \qquad \mathrm{Hom}_{\mathrm{gp}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}).$$

Plus généralement, expliciter une bijection entre $\mathrm{Hom}_{\mathrm{gp}}(\mathbb{Z}/n, G)$ et l'ensemble des éléments de G d'ordre divisant n.

Exercice 12.

a) Soit d un diviseur de n. Montrer que le morphisme *de réduction*

$$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/d\mathbb{Z} \\ x \mod n = [x]_n & \mapsto & x \mod d = [x]_d \end{array}$$

est bien défini et surjectif. Quel est son noyau ?

b) Si m et n sont deux entiers premiers entre eux, montrer que le morphisme de réduction $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est un isomorphisme (*lemme chinois*).

c) Quel est le noyau du morphisme de réduction $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$? En déduire une condition nécessaire pour que ce morphisme soit un isomorphisme. Montrer que son image est isomorphe à $\mathbb{Z}/\mathrm{ppcm}(m,n)\mathbb{Z}$.
Montrer qu'un élément $(x \mod m, y \mod n)$ est dans son image si et seulement si on a

$$x \equiv y \mod \mathrm{pgcd}(n,m).$$

d) On considère le morphisme de réduction $\phi\colon \mathbb{Z}/35\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Déterminer la préimage de $([1]_7, [3]_5)$.

e) Résoudre dans $\mathbb{Z}$:

$$\begin{cases} x \equiv 1 \ [45] \\ x \equiv 3 \ [6] \end{cases}, \qquad \begin{cases} x \equiv 4 \ [45] \\ x \equiv 1 \ [6] \end{cases}$$

Exercice 13.

a) Soient G et H des anneaux. Montrer que $(G \times H)^* = G^* \times H^*$.

b) Soient $x \in G$ et $y \in H$ d'ordre fini. Montrer que l'ordre de $(x, y) \in G \times H$ est égal au $\mathrm{ppcm}(o(x), o(y))$.

c) Calculer l'ordre de $\overline{526}$ dans $(\mathbb{Z}/561\mathbb{Z})^*$.

Exercice 14.

a) Montrer que les sous-groupes finis de $\mathbb{C}^*$ sont cycliques.

b) Quels sont les sous-groupes finis de $\mathbb{R}^*$?

c) Montrer qu'un sous-groupe de $(\mathbb{Q}, +)$ engendré par un nombre fini d'éléments est monogène.

d) Soit p un nombre premier. Montrer que

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b},\ a \in \mathbb{Z} \text{ et } b \text{ premier à } p \right\} \quad (\text{"}\mathbb{Z} \text{ localisé en } p\text{"})$$

est un sous-groupe de $(\mathbb{Q}, +)$ qui n'est pas de type fini.

Exercice 15. [Automorphismes de $\mathbb{Z}/n\mathbb{Z}$, Perrin, Cours d'Algèbre, pages 24-26 ; Serre, Cours d'arithmétique, PUF, Paris (1970), pages 12-13]

Soient n un entier ≥ 2. Si s est un élément de $\mathbb{Z}$ notons $\overline{s}$ son image dans $\mathbb{Z}/n\mathbb{Z}$.

a) Montrer que les propriétés suivantes sont équivalentes :
   1) s est premier avec n,
   2) $\overline{s}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$,
   3) $\overline{s}$ appartient au groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles pour la multiplication de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

b) Montrer que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ et $(\mathbb{Z}/n\mathbb{Z})^*$ sont isomorphes.

c) Démontrer le

Lemme chinois. *Si p et q sont premiers entre eux, alors*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

d) Précisons maintenant la structure de $(\mathbb{Z}/n\mathbb{Z})^*$ suivant la décomposition en facteurs premiers de n. Soit n un entier, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ et les α_i dans $\mathbb{N}^*$. Montrer que $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$.

Si d divise n, désignons par C_d l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. Soit Φ_d l'ensemble des générateurs de C_d. Comme tout élément de $\mathbb{Z}/n\mathbb{Z}$ engendre l'un des C_d le groupe $\mathbb{Z}/n\mathbb{Z}$ est réunion disjointe des Φ_d et

$$n = \#(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \#\Phi_d = \sum_{d|n} \varphi(d).$$

e) Soit H un groupe d'ordre fini n. Supposons que pour tout diviseur d de n

$$\#\{g \in H \mid g^d = 1\} \leq d.$$

Montrer que H est cyclique.

f) Reste à déterminer la structure des $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ pour p premier. Soit p un nombre premier. Montrer que

$$(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

Exercice 16.

Soit E un ensemble muni d'une loi de composition associative, avec un élément neutre e, et telle que tout élément de E possède un inverse à gauche.

Montrer que tout élément de E possède un inverse à droite qui coïncide avec son inverse à gauche. En déduire que E est un groupe.

Exercice 17.

Soit G un groupe tel que $g^2 = e$ pour tout g dans G. Montrer que G est abélien.

Exercice 18.

Soit G un groupe et soit H un sous-ensemble fini non vide de G stable pour la loi de composition du groupe G.

a) Montrer que H est un sous-groupe de G.

b) Trouver un exemple de groupe G et d'un sous-ensemble non vide de G stable pour la loi de composition du groupe G qui ne soit pas un sous-groupe de G.

Exercice 19.

Soit G un groupe fini.

a) Montrer que des éléments conjugués dans G sont de même ordre.

b) Deux éléments de même ordre dans G sont-ils toujours conjugués ?

c) Trouver tous les groupes abéliens finis G pour lesquels la question précédente a une réponse positive. Un exemple non abélien ?

Exercice 20.

Soit $\varphi\colon G_1 \to G_2$ un morphisme de groupes. Soit g un élément de G_1 d'ordre fini.
Montrer que l'ordre de $\varphi(g)$ divise l'ordre de g.

Exercice 21.

Soit G un groupe de type fini.

a) Un sous-groupe H de G est-il nécessairement de type fini ?

b) Même question en supposant de plus que G/H est fini.

Exercice 22.

a) Déterminer les classes de conjugaison dans $\mathcal{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Exercice 23.

Soit n un entier. Rappelons que $\mathcal{A}_n$ est le sous-groupe de $\mathcal{S}_n$ formé par les permutations paires.

a) Montrer que le produit de deux transpositions distinctes de $\mathcal{S}_n$ est un 3-cycle ou un produit de deux 3-cycles. En déduire que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles de $\mathcal{S}_n$.

b) i) Montrer que pour $n \geq 3$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles $(1\ 2\ 3)$, $\ldots$, $(1\ 2\ n)$. En déduire que $\mathcal{A}_n$ est pour $n \geq 3$ stable par tout automorphisme ϕ de $\mathcal{S}_n$ ($\mathcal{A}_n$ est donc un sous-groupe caractéristique de $\mathcal{S}_n$).

ii) Montrer que $\mathcal{A}_n$ est engendré
— si n est impair ≥ 5 par $(1\ 2\ 3)$ et $(3\ 4\ \ldots\ n)$;
— si n est pair ≥ 4 par $(1\ 2\ 3)$ et $(1\ 2)(3\ 4\ \ldots\ n)$.

c) Montrer que pour $n \geq 5$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des permutations de $\mathcal{S}_n$ de la forme $(a\ b)(c\ d)$ avec a, b, c, d deux à deux distincts.

Exercice 24. [Étude du groupe $\mathrm{O}(p,q)$, Caldero, Germoni, Histoires hédonistes de groupes et géométries, tome 1]

Soit n un entier naturel. L'ensemble des matrices symétriques définies positives de taille $n \times n$ est

$$\begin{aligned}
\mathrm{S}^{++}(n,\mathbb{R}) &= \left\{ S \in \mathrm{GL}(n,\mathbb{R}) \mid \left\{ \begin{array}{l} {}^{\mathrm{t}}S = S \\ \forall x \in \mathbb{R}^n \smallsetminus \{0\} \quad {}^{\mathrm{t}}xSx > 0 \end{array} \right. \right\} \\
&= \left\{ P\,{}^{\mathrm{t}}P \in \mathrm{M}(n,\mathbb{R}) \mid P \in \mathrm{GL}(n,\mathbb{R}) \right\}
\end{aligned}$$

Cet ensemble forme un système homogène (*i.e.* un espace sur lequel un groupe agit de façon transitive).

Rappelons le théorème de décomposition polaire : la multiplication matricielle induit l'homéomorphisme

$$\mathrm{O}(n,\mathbb{R}) \times \mathrm{S}^{++}(n,\mathbb{R}) \xrightarrow{\sim} \mathrm{GL}(n,\mathbb{R}), \qquad\qquad (O,S) \mapsto OS$$

Soient p et q deux entiers naturels. On désigne par $\mathrm{O}(p,q)$ le sous-groupe de $\mathrm{GL}(p+q,\mathbb{R})$ formé des isométries de la forme quadratique standard sur $\mathbb{R}^{p+q}$ de signature (p,q) c'est-à-dire

$$x_1^2 + x_2^2 + \ldots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \ldots - x_{p+q}^2$$

dont la matrice dans la base canonique est

$$I_{p,q} = \left(\begin{array}{cccc|cccc}
1 & 0 & \ldots & 0 & & & & \\
0 & \ddots & \ddots & \vdots & & & 0 & \\
\vdots & \ddots & \ddots & 0 & & & & \\
0 & \ldots & 0 & 1 & & & & \\
\hline
 & & & & -1 & 0 & \ldots & 0 \\
 & & 0 & & 0 & \ddots & \ddots & \vdots \\
 & & & & \vdots & \ddots & \ddots & 0 \\
 & & & & 0 & \ldots & 0 & -1
\end{array} \right)$$

Soient p et q deux entiers naturels distincts. Montrer que le groupe $\mathrm{O}(p,q)$ est homéomorphe à $\mathrm{O}(p) \times \mathrm{O}(q) \times \mathbb{R}^{pq}$.

Exercice 25. [Sous-groupes additifs de $\mathbb{R}$, Francinou, Giunella, Nicolas, exercices de mathématiques, oraux x-ens, analyse 1, page 29]

Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$. Montrer que G est ou bien dense dans $\mathbb{R}$, ou bien monogène, *i.e.* de la forme $a\mathbb{Z}$ avec $a > 0$ (donc discret).

Exercice 26.

Quels sont les éléments d'ordre 3 du groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

Exercice 27.

Étudier le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 28.

Montrer que les groupes $\mathbb{R}/\mathbb{Z}$ et $\mathcal{U} = \big\{z \in \mathbb{C} \,|\, |z| = 1\big\}$ sont isomorphes.

Exercice 29.

Donner un exemple de groupe et de sous-groupes dont la réunion n'est pas un sous-groupe.

Exercice 30.

Soient G un groupe fini, H et K deux sous-groupes de G d'ordre h et k respectivement.

Si h et k sont premiers entre eux, que peut-on dire de $\mathrm{H} \cap \mathrm{K}$?

Exercice 31.

Quel est le cardinal de $\mathrm{Aut}\Big(\mathbb{Z}/4\mathbb{Z}\Big)$? Et le cardinal de $(\mathbb{F}_4)^\times$?

Exercice 32.

Dans les groupes suivants, donner un exemple d'élément d'ordre 4 s'il en existe, sinon donner un argument pour justifier qu'il n'y en a pas :

(a) le groupe linéaire $\mathrm{GL}_2(\mathbb{R})$;
(b) le groupe alterné $\mathcal{A}_8$;
(c) le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}_3(\mathbb{R})$ des rotations de $\mathbb{R}^3$ préservant un tétraèdre régulier T ;
(d) un groupe d'ordre 16 quelconque (attention il s'agit de déterminer si *tout* sous-groupe d'ordre 16 admet un élément d'ordre 4).

Exercice 33.

(1) Soit G un groupe abélien. Soient a et b deux éléments de G d'ordres finis premiers entre eux. Montrer que $\mathrm{ordre}(ab) = \mathrm{ordre}(a)\mathrm{ordre}(b)$.
(2) Soit G un groupe abélien fini et soit m le maximum parmi les ordres des éléments de G, m est appelé l'exposant de G. Montrer que l'ordre de tout élément de G divise m.
(3) Soit $\Bbbk$ un corps et $\mathrm{G} \subset \Bbbk^*$ un sous-groupe fini du groupe multiplicatif $\Bbbk^*$. Montrer que G est cyclique. [Indication : on peut considérer les racines du polynôme $X^m - 1 \in \Bbbk[X]$ où m est l'exposant de G.]
(4) Qu'en déduire pour le groupe $\Big(\mathbb{Z}/p\mathbb{Z}\Big)^*$ avec p premier ? Qu'en déduire pour le groupe $\mathbb{C}^*$?

Exercice 34.

(1) Soient $n \geq 1$ et k deux entiers. Montrer l'équivalence des assertions suivantes :
  (i) $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ engendre $\mathbb{Z}/n\mathbb{Z}$;
  (ii) n et k sont premiers entre eux ;
  (iii) $\overline{k}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$.
(2) Montrer que $\big(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ\big) \simeq \big((\mathbb{Z}/n\mathbb{Z})^*, \times\big)$.

Exercice 35.

Soit G un groupe abélien infini. Montrer que l'ensemble T des éléments d'ordre fini de G est un sous-groupe de G.

Si $\mathrm{T} = \{e\}$, on dit que G est sans torsion.

Montrer que G/T est sans torsion.

Exercice 36.

Soient $p < q$ deux nombres premiers tels que p divise $q - 1$. Donner un exemple de groupe non-abélien G d'ordre pq constitué de matrices triangulaires dans $\mathrm{GL}_2\big(\mathbb{Z}/q\mathbb{Z}\big)$.

Exercice 37.
Le groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^*$ est-il cyclique ? Si oui, donner un générateur, et si non, donner un court argument.

Exercice 38.
Montrer que $\mathrm{GL}_2(\mathbb{F}_2)$ est isomorphe à $\mathcal{S}_3$.

Exercice 39.
(1) Montrer que $(\mathbb{Z},+)$ n'est pas isomorphe à $(\mathbb{Z}^2,+)$ et que $(\mathbb{Q},+)$ n'est pas isomorphe à $(\mathbb{Q}^2,+)$.
(2) Montrer que le groupe abélien $(\mathbb{Q},+)$ n'est pas de type fini.
(3) Soit G un groupe de $(\mathbb{C}^*,\cdot)$ dont chaque élément est d'ordre fini. Est-il vrai que G est forcément fini ? de type fini ?
(4) Montrer que les sous-groupes de $(\mathbb{R},+)$ sont soit de la forme $a\mathbb{Z}$, soit denses.
(5) Que dire de $\mathbb{Z}[\sqrt{2}]$?

Exercice 40.
a) Soit G un sous-groupe fini de $\mathbb{C}^*$. Montrer que $\mathrm{G} = \mathbb{U}_n$ où $n = [\mathrm{G} : 1]$.
b) Soient m, $n \in \mathbb{N}^*$. Déterminer le sous-groupe de $\mathbb{C}^*$ engendré par $\mathbb{U}_m$ et $\mathbb{U}_n$.
c) Soient n, p, $q \in \mathbb{N}^*$. À quelle condition a-t-on $\mathbb{U}_n \simeq \mathbb{U}_p \times \mathbb{U}_q$?
d) Pour un tel choix montrer que $\mathrm{Aut}(\mathbb{U}_n) \simeq \mathrm{Aut}(\mathbb{U}_p) \times \mathrm{Aut}(\mathbb{U}_q)$.

Exercice 41.
(1) Montrer que $\mathrm{GL}_n(\mathbb{C})$ est connexe par arcs.
(2) Montrer que $\mathrm{GL}_n(\mathbb{R})$ n'est pas connexe par arcs.

Exercice 42.
Montrer que $\mathrm{SO}_n(\mathbb{R})$ est connexe par arcs.