FEUILLE 1

Groupes, sous-groupes.

Exercice 1. Montrer que l'ensemble de matrices carrées à n lignes et n colonnes de déterminant non nul est un groupe pour la multiplication.

Exercice 2. On considère l'ensemble E des matrices carrées à coefficients réels de la forme

$$\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}, \quad a \in \mathbb{R}^{\times}, \quad b \in \mathbb{R}$$

muni du produit des matrices.

a) Montrer que E est ainsi muni d'une loi de composition interne associative.

b) Déterminer tous les éléments neutres à droite de E.

c) Montrer que E n'admet pas d'élément neutre à gauche.

d) Soit e un élément neutre à droite. Montrer que tout élément de E possède un inverse à gauche pour cet élément neutre, i.e.

$$\forall g \in E \quad \exists h \in E : hg = e.$$

> **Rappel : Sous-groupe**
> Un sous-ensemble non vide H d'un groupe G est un sous-groupe ssi H est stable par composition et passage au symétrique.

Exercice 3. Décrire tous les sous-groupes de $\mathbb{Z}$..

Exercice 4. Décrire tous les sous-groupes du groupe symétrique S_3.

Exercice 5. Montrer que les rationnels non nuls forment un sous-groupe multiplicatif de $\mathbb{R}^{\times}$.

Exercice 6. Soit H une partie non vide d'un groupe G. On pose $H^{-1} = \{x^{-1} \mid x \in H\}$. Montrer les équivalences suivantes :

a) $H < G \Leftrightarrow HH^{-1} \subset H$

b) $H < G \Leftrightarrow \forall a \in H \quad Ha = H$.

Intersection de sous-groupes.

Exercice 7. Soit A et B deux parties d'un groupe fini G vérifiant :

$$\text{Card } A + \text{Card } B > \text{Card } G.$$

Montrer que pour tout élément x de G, il existe $a \in A$ et $b \in B$ tels que $x = ab$.

Exercice 8. Soient G un groupe et H, K deux sous-groupes de G.

a) Donner une condition nécessaire et suffisante pour que $H \cup K$ soit un sous groupe de G.

b) Montrer qu'un groupe ne peut pas être la réunion de deux sous-groupes propres.

Groupes monogènes, cycliques, abéliens.

Exercice 9.

a) Donner un exemple d'un groupe monogène.

b) Montrer que tout groupe monogène est abélien.

c) Montrer que le groupe produit de deux groupes abéliens est abélien.

d) Est-ce que $\mathbb{Z} \times \mathbb{Z}$ est monogène ? Justifier votre réponse.

Exercice 10.

a) Soit G un groupe dans lequel tous les éléments g vérifient $g^2 = e$. Montrer que G est commutatif.

b) Soit G un groupe tel que, pour tous g et h dans G, on ait $(gh)^{-1} = g^{-1}h^{-1}$. Montrer que G est commutatif.

c) Soit G un groupe tel que, pour tous g et h dans G, on ait $(gh)^2 = g^2h^2$. Peut-on conclure que G est commutatif.

d) Donner un exemple de groupe non commutatif G tel que, pour tous g et h dans G, on ait $(gh)^3 = g^3h^3$.
Indication : Considérer les matrices (a_{ij}) dans $\mathrm{GL}(3, \mathbb{Z}/3\mathbb{Z})$ telles que $a_{ii} = 1$ pour $1 \leq i \leq 3$ et $a_{ij} = 0$ pour $1 \leq j < i \leq 3$.

Exercice 11. Soit n un entier strictement positif.

a) Déterminer tous les sous-groupes additifs de $\mathbb{Z}$.

b) Montrer que tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique. En déduire que tout sous-groupe d'un groupe cyclique est cyclique.

c) Montrer que pour tout d divisant n, $\mathbb{Z}/n\mathbb{Z}$ possède un unique sous-groupe d'ordre d.
Indication : considérer l'ensemble

$$H := \{\bar{k} \in \mathbb{Z}/n\mathbb{Z} : \overline{dk} = \bar{0}\}.$$

d) Montrer que le nombre d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ est égal à $\varphi(d)$.

e) En déduire une démonstration de la relation

$$n = \sum_{d|n} \varphi(d).$$

Morphisme et isomorphisme.

> **Rappel : Morphisme de groupes**
> On dit qu'une application $f : G_1 \to G_2$ entre deux groupes est un morphisme si pour tous $x, y \in G_1$ on a $f(x.y) = f(x).f(y)$.

Exercice 12.

a) Donner un exemple de morphisme de groupe de $(\mathbb{R}, +)$ vers $(\mathbb{R}^*, .)$. Est-ce un isomorphisme ?

b) L'ensemble des bijections croissantes de $\mathbb{R}$ dans $\mathbb{R}$ est-il un groupe ? Et pour les décroissantes ?

c) Est-il possible de définir une loi $*$ sur l'ensemble des entiers positifs $\mathbb{N}$ de façon à ce que $\mathbb{N}, *$ devienne un groupe ?

Exercice 13.

a) Donner deux exemples de groupes d'ordre 4 non isomorphes entre eux.

b) Donner deux exemples de groupes d'ordre 6 non isomorphes entre eux.

c) Donner cinq exemples de groupes d'ordre 8 non isomorphes entre eux.

Sous-groupes engendrés par une partie.

> **Rappel : Groupe engendré**
> Soit G un groupe et S une partie de G. On note $\langle S\rangle$ le plus petit sous-groupe de G contenant S. On dit que $\langle S\rangle$ est le sous-groupe engendré par S. Si $\langle S\rangle = G$, on dit que S est une partie génératrice de G.

Exercice 14. Donner une partie génératrice la plus petite possible du groupe $\mathbb{Z}/6\mathbb{Z}$. Y a-t-il plusieurs choix possibles ? Mêmes questions pour les groupes S_3, $\mathbb{H}_8$ et $\mathbb{Z}^n$.

Exercice 15.

a) Donner un exemple de sous-groupe additif de $\mathbb{R}$ dense de type fini (c'est-à-dire engendré par un nombre fini d'éléments).

b) Tous les sous-groupes de $\mathbb{R}$ sont-ils de type fini ?

c) Montrer que les sous-groupes additifs de $\mathbb{R}$ sont soit monogènes soit denses.

Ordre d'un élément, d'un sous-groupe. Théorème de Lagrange.

> **Rappel : Ordre d'un groupe, ordre d'un élément**
> On dit qu'un groupe G est d'ordre n s'il contient n éléments.
> L'ordre d'un élément $x \in G$ est le plus petit entier strictement positif m tel que $x^m = 1$ (en notation multiplicative).

Exercice 16. On pose $\mathrm{SL}_2(\mathbb{Z}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1\}$.

a) Montrer que $\mathrm{SL}_2(\mathbb{Z})$ est un sous-groupe du groupe des matrices inversibles.

b) On considère les deux matrices

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Montrer que A et B sont d'ordres finis mais que AB est d'ordre infini.

Exercice 17. Soit G un groupe commutatif et $a, b \in G$ tel que a soit d'ordre fini p et b d'ordre fini q avec $\mathrm{pgcd}(p, q) = 1$.

a) Montrer que $\langle a\rangle \cap \langle b\rangle = \{e\}$.

b) Montrer que ab est d'ordre pq.

Exercice 18. Soit $\mathbb{H}_8$ le sous-groupe de $GL_2(\mathbb{C})$ engendré par les matrices

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

Calculer l'ordre de $\mathbb{H}_8$ et expliciter tous ses sous-groupes. Quel est son centre ?

Exercice 19. On note D_4 le groupe des isométries du carré pour la composition des applications (on l'appelle le quatrième groupe diédral, d'où la notation). Quel est l'ordre de ce groupe ? Quel est l'ordre de chacun de ses éléments ? Est-ce un groupe cyclique ? Est-ce un groupe commutatif ?

Exercice 20.

a) Soit G un groupe d'ordre pair. Montrer qu'il existe un élément $x \in G$ tel que $x^2 = e$.

b) Soit G un groupe d'ordre impair. Montrer que l'application $f : G \to G$ définie par $f(x) = x^2$ est une bijection. En déduire que l'équation $x^2 = e$ admet une unique solution que l'on précisera.

Exercice 21. Soit G un groupe fini et m un entier premier avec l'ordre de G. Montrer que pour tout $a \in G$, l'équation $x^m = a$ admet une unique solution.

Exercice 22.

a) Donner un exemple de groupe commutatif G et de deux éléments $a, b \in G$ tous deux d'ordre 4 tels que le produit ab soit d'ordre 1 ? d'ordre 2 ? d'ordre 4 ?

b) En général, montrer que dans un groupe commutatif G, si ordre$(a) = n$ et ordre$(b) = m$ alors ordre(ab) divise PPCM(ordre(a),ordre(b)).

c) Est-il possible d'avoir un groupe G et deux éléments d'ordre 2 $x, y \in G$ tel que $x.y$ soit d'ordre infini (si oui, donner un exemple ; si non, donner un court argument) ?

d) Est-il possible d'avoir un groupe infini dont tous les éléments sont d'ordre fini ?

Exercice 23.

a) Soient x et y deux éléments d'ordres finis, premiers entre eux, d'un groupe commutatif G. Montrer que l'ordre de xy est égal au produit des ordres de x et y.

b) Soit y un élément de G d'ordre $p^\alpha m$ où m est un entier et p est premier. Montrer que y^m est d'ordre p^α.

c) Soit G un groupe commutatif de cardinal fini n. Montrer qu'il existe un élément de G dont l'ordre est le ppcm des ordres des éléments de G.

d) Calculer l'ordre de chaque élément du groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Le résultat de la question c. est-il vérifié ?

e) Calculer l'ordre de chaque élément du groupe S_3. Le résultat de la question c. est-il vérifié ?

Exercice 24.

a) Soit G un groupe fini d'ordre n tel que pour tout diviseur d de n, il y ait au plus d éléments g de G vérifiant $g^d = 1$. Montrer que G est cyclique.

b) Montrer que pour tout p premier, le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.