Feuille d'exercices numéro 1
Permutations et groupes

Mise au point préalable sur les notations
* Dans cette fiche, on note S_n l'ensemble des permutations de l'ensemble fini $\{1, \cdots, n\}$;
* Une permutation σ de S_n pourra être notée $\begin{pmatrix} 1 & \dots & n \\ \sigma(1) & \dots & \sigma(n) \end{pmatrix}$ ou, pour prendre moins de place, simplement $\sigma(1) \quad \dots \quad \sigma(n)$ **sans** parenthèses ;
* Étant donnés k éléments distincts de S_n, la notation $(\, i_1 \quad \dots \quad i_k \,)$ **avec** parenthèses désigne le cycle qui envoie i_1 sur i_2, i_2 sur i_3, ..., i_{k-1} sur i_k et i_k sur i_1.
Le symbole $\circ$ de composition des applications pourra être omis, notamment dans l'écriture d'une permutation comme produit de cycles de supports deux à deux disjoints.

Introduction aux permutations, sans le langage des groupes

Exercice 1

1) Dans S_5, soit les permutations $\sigma_1 = (12345)$, $\sigma_2 = (12)$ et $\sigma_3 = (135)(24)$. Représenter chacune d'entre elles par un joli dessin avec une patate, cinq points et une flèche de chaque point vers son image, et réécrire chacune d'entre elles avec la première des notations rappelées en ouverture de cette fiche.

2) Dans S_9, soit les permutations $\rho_1 = 412937568$, $\rho_2 = 351487629$ et $\rho_3 = 987654321$. Les dessiner avec patates et flèches, puis les écrire comme produits de cycles de supports deux à deux disjoints.

Exercice 2

1) Dans S_3 soit $\pi = 231$ et $\sigma = 312$. Calculer $\sigma \circ \pi$, puis σ^{-1} et préciser la signature de σ.

2) Soit $n \geq 3$. Dans S_n soit $\pi = (123)$ et $\sigma = (13)$. Calculer $\sigma\pi$ et $\pi\sigma$.

3) Dans S_4 soit $\sigma = (12)(34)$ et $\pi = (1342)$. Expliciter leurs inverses et préciser leurs signatures respectives. Écrire π comme un produit de transpositions.

4) Plus généralement soit un cycle $(i_1 \dots i_k)$ dans S_n. Préciser sa signature en fonction de n et k.

Le langage des groupes, vu à travers l'exemple des permutations

Exercice 3

1) Dans S_4, on note $\sigma = 2341$. Expliciter σ^2, σ^3 et σ^4, et se forcer à en déduire que $\sigma^3 = \sigma^{-1}$. Montrer que $\{\mathrm{Id}, \sigma, \sigma^2, \sigma^3\}$ est un sous-groupe de S_4. Ce sous-groupe est-il commutatif ? Est-il monogène ? Est-il cyclique ?

2) Soit $n \geq 1$. On note $A_n = \{\sigma \in S_n \mid \mathrm{sign}(\sigma) = 1\}$ et B_n son complémentaire. L'ensemble A_n est-il un sous-groupe de S_n ? Et l'ensemble B_n ?

3) Soit $n \geq 1$ et soit M un sous-ensemble de $\{1, \dots, n\}$. On note $H = \{\sigma \in S_n \mid \sigma(M) = M\}$. Montrer que H est un sous-groupe de S_n. Expliciter l'ordre de ce sous-groupe en fonction de n et du nombre d'éléments de M.

Exercice 4
Soit $n \geq 1$ un entier. Montrer que S_n est un groupe commutatif si et seulement si $n = 1$ ou $n = 2$. (Pensez à recycler un calcul fait plus haut !)

Exercice 5

1) Quel est l'ordre de la permutation σ de la question 1 de l'exercice 3 ?

2) Plus généralement, soit un cycle $(i_1 ... i_k)$ dans S_n. Quel est son ordre ?

3) Dans S_6, quels sont les ordres respectifs de $(123) \circ (45)$ et de $(14) \circ (2356)$?

4) Plus généralement, si $(i_1 ... i_k)$ et $(j_1 ... j_l)$ sont deux cycles dans S_n, dont les supports sont disjoints, quel est l'ordre de leur produit ?

Exercice 6

1) Combien S_3 admet-il de sous-groupes à 1 élément ? à 6 éléments ? à 4 éléments ? à 5 éléments ?

2) a) Combien y a-t-il de transpositions dans S_3 ?

b) Soit H un sous-groupe de S_3 possédant 2 éléments. Montrer que $H = \{\mathrm{Id}, t\}$ où t est une transposition. En déduire le nombre de sous-groupes de S_3 possédant 2 éléments.

3) Soit H un sous-groupe de S_3 possédant 3 éléments. Montrer que H ne contient pas de transposition. En déduire le nombre de sous-groupes de S_3 possédant 3 éléments.

Exercice 7

1) Montrer que $U_3 = \{1, j, j^2\}$ est un sous-groupe du groupe multiplicatif $\mathbf{C}^*$.

2) On note $\sigma = (123)$ dans S_3 puis on définit une application $\varphi\colon U_3 \to S_3$ en posant $\varphi(1) = \mathrm{Id}$, $\varphi(j) = \sigma$ et $\varphi(j^2) = \sigma^2$. Montrer que φ est un morphisme.

3) Soit $n \leq m$ deux entiers strictement positifs, et soit $\Phi\colon S_n \to S_m$ défini par :

$$\Phi(\sigma) = \begin{pmatrix} 1 & \dots & n & n+1 & \dots & m \\ \sigma(1) & \dots & \sigma(n) & n+1 & \dots & m \end{pmatrix}.$$

L'application Φ est-elle un morphisme de groupes ?

4) Soit X et Y deux ensembles finis non vides. Montrer que les groupes $S(X)$ et $S(Y)$ des permutations de ces ensembles sont isomorphes si et seulement si X et Y ont le même nombre d'éléments.

Exercice 8

1) a) Dans S_5, soit $\sigma_1 = (145)$ et $\rho = 25143$. Expliciter l'écriture en produit de cycles de supports disjoints de $\rho \circ \sigma_1 \circ \rho^{-1}$.

b) Généraliser ce résultat : étant donné $n \geq 1$, $\sigma_1 = (i_1 \dots i_k)$ un cycle de S_n et ρ un élément de S_n, décrire la permutation $\rho \circ \sigma_1 \circ \rho^{-1}$.

2) On rappelle que dans un groupe G, deux éléments g_1 et g_2 sont dits conjugués quand il existe un $h \in G$ tel que $g_2 = hg_1h^{-1}$. Soit $n \geq 1$ et soit σ_1 un cycle de S_n. Montrer que les conjugués de σ_1 sont exactement les cycles de même longueur que σ_1.

Exercice 9

1) Dans S_5, on pose $\sigma = (123)$ et $\tau = (34)$, puis on note $H = \langle \sigma, \tau \rangle$ le sous-groupe de S_5 engendré par σ et τ. Montrer que H est un sous-ensemble strict de S_5. (Suggestion : on pourra utiliser l'ensemble $H_1 = \{\rho \in S_5 \mid \rho(5) = 5\}$).

2) Dans S_4, on pose $\sigma = (123)$ et $\tau = (34)$, puis on note $H = \langle \sigma, \tau \rangle$ le sous-groupe de S_4 engendré par σ et τ.

a) Montrer que $(14) \in H$ et $(23) \in H$ (on peut y arriver en tâtonnant un bon moment, mais on gagnera du temps en essayant de se servir de l'exercice précédent...)

b) Montrer ensuite que $(12) \in H$, $(13) \in H$ et $(23) \in H$.

c) Conclure que $H = S_4$.

Quelques exemples de groupes commutatifs, avec des nombres dedans

On rappelle par mesure de sécurité que $(\mathbf{Z}, +)$, $(\mathbf{R}, +)$ et $(\mathbf{C}, +)$ sont des groupes, ainsi que $(\mathbf{R}^*, \times)$ et $(\mathbf{C}^*, \times)$.

Exercice 10

Parmi $(\mathbf{N}, +)$, $(\mathbf{Z}, \times)$, $(\mathbf{Z}^*, \times)$, $(\mathbf{Q}, +)$ et $(\mathbf{Q}^*, \times)$, lesquels sont des groupes ?

Exercice 11

(C'est traité en cours, mais ça ne peut pas faire de mal de le refaire...)

Montrer que les sous-groupes additifs de $\mathbf{Z}$ sont exactement les $k\mathbf{Z}$, où k est un entier positif ou nul.

Exercice 12

1) Montrer que $(\mathbf{R}, +)$ et $(\mathbf{R}^{+*}, \times)$ sont isomorphes.

2) Montrer que $(\mathbf{R}, +)$ et $(\mathbf{R}^*, \times)$ ne sont pas isomorphes.

3) Montrer que $(\mathbf{R}^*, \times)$ est isomorphe à $(\mathbf{R}, +) \times (\{-1, 1\}, \times)$.

Exercice 13
Quels sont les éléments d'ordre fini dans $\mathbf{C}^*$? Quels sont les sous-groupes d'ordre fini de $\mathbf{C}^*$? Sont-ils tous cycliques ? Pour $n \geq 1$ fixé, combien y en a-t-il qui sont d'ordre n exactement ?

Exercice 14
Déterminer tous les morphismes de groupes de $(\mathbf{Q}, +)$ vers $(\mathbf{R}, +)$.

Quelques exemples avec des matrices
On rappelle par mesure de sécurité que tout espace vectoriel est un groupe pour l'addition (et en particulier l'espace vectoriel des matrices rectangulaires d'une forme fixée), et que pour tout $n \geq 1$ l'ensemble des matrices inversibles (n, n) (réelles ou complexes) est un groupe multiplicatif, appelé groupe linéaire.

Exercice 15
Leurs ensembles respectifs constituent-ils des groupes ? (Il est vivement suggéré, quand la réponse est "oui" de le montrer en découvrant que c'est un sous-groupe d'un groupe déjà connu).

1) Les matrices (5,5) à coefficients entiers, pour l'addition.

2) Les matrices (5,5) à coefficients entiers et à déterminant non nul, pour la multiplication.

3) Les matrices (5,5) à coefficients entiers et à déterminant valant 1, pour la multiplication.

4) Les matrices (5,5) à coefficients réels A qui vérifient ${}^tA = -A$, pour l'addition.

5) Les matrices (5,5) à coefficients réels A qui vérifient ${}^tA = -A$, pour la multiplication.

6) Les matrices (5,5) à coefficients réels P qui vérifient ${}^tPP = I_5$, pour la multiplication.

Quelques exercices sur des groupes "abstraits"

Exercice 16
Soit $(G, .)$ un groupe et soit A une partie de G qui vérifie les trois propriétés suivantes :
(i) A n'est pas vide ;
(ii) Le produit de deux éléments de A est dans A ;
(iii) A est un ensemble fini.
Montrer que A est un sous-groupe de G.

Exercice 17

1) Soit $(G, .)$ un groupe ayant 120 éléments, et soit a un élément de G. Montrer que $a^{120} = e$.

2) Existe-t-il un groupe à 120 éléments dont tous les éléments soient d'ordre 120 ?

3) Existe-t-il un groupe à 120 éléments dont tous les éléments sauf l'élément neutre soient d'ordre 120 ?

4) Existe-t-il un groupe à 120 éléments qui ne contienne aucun élément d'ordre 120 ?

Exercice 18
Soit p un nombre premier.

1) Montrer que dans tout groupe G, si un élément b différent du neutre e vérifie $b^p = e$, alors l'ordre de b est p.

2) Soit $n \geq 1$ un entier, et G un groupe d'ordre p^n. Soit a un élément de G différent du neutre. En considérant les éléments a, a^p, a^{p^2},...,$a^{p^{n-1}}$, montrer que G contient un élément d'ordre p.

Exercice 19
Soit $(G, .)$ un groupe **commutatif** dont l'opération est notée multiplicativement, et soit a et b deux éléments de G d'ordres respectifs p et q. On note d le PGCD de p et q et m leur PPCM, et on rappelle que $dm = pq$.

1) Montrer que l'ordre l de ab^{-1} divise le PPCM de p et q, et donner un exemple dans lequel il n'est pas égal à ce PPCM.

2) Dans cette question, on suppose p et q premiers entre eux. Montrer que $a^l = b^l$. En réfléchissant sur ce que peut valoir l'ordre de cet élément, montrer qu'il est égal à l'élément neutre du groupe puis en déduire que $l = pq$.

3) En utilisant la question précédente, montrer que ab^{-d} est d'ordre m.

Exercice 20
Soit $(G, .)$ un groupe (dont l'opération est notée multiplicativement), et soit a un élément fixé de G.
On définit sur G une nouvelle opération $\star$ en posant, pour tous éléments x et y de G :

$$x \star y = xay.$$

Montrer que pour cette nouvelle opération, $(G, \star)$ est lui aussi un groupe.

Exercice 21
Soit $(G, .)$ un groupe fini. On suppose que tous ses éléments (sauf e) sont d'ordre 2.
Pour $A \subset G$ et $a \in G$, on note $aA = \{ax \mid x \in A\}$.

1) Montrer que G est abélien.

2) Soit H un sous-groupe de G et soit a un élément de G qui n'appartient pas à H. Montrer que $H \cup aH$ est encore un sous-groupe de G, qui a deux fois plus d'éléments que H.

3) Montrer que le nombre d'éléments de G est une puissance de 2.