Feuille n° 3

Théorie des groupes.

Dans toute la suite, si G est un groupe, et S une partie de G, on désigne par $< S >$ le sous-groupe engendré par S, autrement dit le plus petit-sous-groupe contenant S.

Exercice 1. Montrer qu'un groupe monogène est, soit infini et isomorphe à $\mathbb{Z}$, soit fini et isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$ (on rappelle qu'un groupe G est monogène s'il est engendré par l'un de ses éléments, autrement dit s'il existe $x \in G$ tel que $G =< x >$).

Exercice 2. Soit $G =< x >$ un groupe cyclique d'ordre n. Montrer que $x^k = 1_G$ si et seulement si $k \in n\mathbb{Z}$. Montrer que l'ordre de l'élément x^k est $\frac{n}{n \wedge k}$ pour tout $k \geq 1$. En déduire le nombre de générateurs de G.
Application : Quels sont les générateurs de $\mathbb{Z}/18\mathbb{Z}$?
Combien y a-t-il d'éléments d'ordre 2 dans $\mathbb{Z}/n\mathbb{Z}$?

Exercice 3. a) Montrer que tout sous-groupe d'un groupe cyclique est cyclique.
b) Soit G un groupe cyclique d'ordre n. Montrer que pour tout diviseur d de n, il existe un et un seul sous-groupe d'ordre d. Montrer que ce sous-groupe est précisément égal à $\{g \in G, g^d = 1_G\}$. Ce résultat est-il vrai en général ?

Exercice 4. Montrer que le produit direct $G_1 \times G_2$ de deux groupes cycliques G_1 et G_2 est cyclique si et seulement si l'ordre de G_1 et celui de G_2 sont premiers entre eux.

Exercice 5. Montrer qu'un sous-groupe de $(\mathbb{R}, +)$ est, soit engendré par un élément a, soit dense dans $\mathbb{R}$.

Exercice 6. Montrer que tout groupe G est isomorphe à un sous-groupe du groupe S_g des permutations de G (on pourra considérer à $g \in G$ fixé l'application $x \mapsto gx$).

Exercice 7. Soit n un entier ≥ 1. On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles pour la multiplication.
a) Démontrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ est un groupe abélien fini. On note $\varphi(n)$ son ordre.
b) Calculer $\varphi(p^r)$ pour tout nombre premier p et tout entier $r \geq 1$.
c) Démontrer que si m et n sont premiers entre eux, alors $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ est isomorphe à $(\mathbb{Z}/mn\mathbb{Z})^\times$.
d) En déduire que $\varphi(n) = n \prod_{p|n} (1 - 1/p)$.
e) Montrer que $n = \sum_{d|n} \varphi(d)$.

Exercice 8. Soit G un groupe tel que pour tout $x \in G$ on ait $x^2 = e$, où e est l'élément neutre de G.
a) Montrer que G est commutatif.
b) Soient H un sous-groupe de G distinct de G et a un élément de G n'appartenant pas à H. Montrer que $H \cup aH$ est un sous-groupe de G contenant strictement H et que $H \cap aH = \emptyset$. Montrer que $H \cup aH \simeq H \times \mathbb{Z}/2\mathbb{Z}$.
c) Montrer que si de plus G est un groupe fini, son ordre est une puissance de 2.

Exercice 9. Soit G un groupe d'élément neutre e. On considère deux éléments a et b de G tels que $ab = ba$.
a) On suppose a et b d'ordre fini. Montrer que ab est d'ordre fini et que l'ordre de ab divise le PPCM de l'ordre de a et de l'ordre de b.
b) On suppose que $< a > \cap < b >= \{e\}$. Montrer que ab est d'ordre fini si et seulement si a et b sont d'ordre fini et que dans ce cas l'ordre de ab est égal au PPCM des ordres de a et de b.
c) Soit $a \in G$, $a \neq e$. On suppose a d'ordre fini. En considérant $b = a^{-1}$, montrer que le résultat du b) peut être faux si l'on enlève l'hypothèse $< a > \cap < b >= \{e\}$.

d) Soient a et b deux éléments de G dont les ordres sont finis et premiers entre eux. Montrer que l'ordre de ab est égal au produit des ordres de a et de b, soit en utilisant b), soit directement.

Exercice 10. Si a et b sont deux éléments d'ordre fini d'un groupe G, et si, contrairement à l'exercice précédent, *on ne suppose plus que* $ab = ba$, que peut-on dire de l'ordre de ab ? (indication : considérer les matrices $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ dans $\mathrm{SL}_2(\mathbb{Z})$).

Exercice 11. Soit $G = \{x_1, \cdots, x_n\}$ un groupe abélien d'ordre n et $a_1, a_2, \cdots, a_n$ les ordres respectifs de x_1, $x_2, \cdots, x_n$.

1. Montrer que n divise $a_1 a_2 \cdots a_n$ (indication : on pourra construire un morphisme surjectif de $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \mathbb{Z}/a_n\mathbb{Z}$ sur G).
2. En déduire que pour tout nombre premier p divisant n, il existe dans G un élément d'ordre p.
3. Soit $m = \mathrm{ppcm}\{a_1, a_2, \cdots, a_n\}$. Montrer qu'il existe $x \in G$ d'ordre m (indication : considérer la décomposition en facteurs premiers du ppcm de $a_1, a_2, \cdots, a_n$).

Exercice 12. Montrer que tout sous-groupe fini G du groupe multiplicatif $K^\times = K\backslash\{0\}$ d'un corps commutatif K est cyclique. (indication : montrer que G est contenu dans l'ensemble des racines du polynôme $X^m - 1$, où m est le ppcm des ordres des éléments de G)

Exercice 13. Soit G un groupe fini d'ordre pair (pas nécessairement abélien). On pose $A = \{x \in G \ : \ x^2 = 1_G\}$ et $B = G\backslash A$.
a) Démontrer que le cardinal de B est pair (remarquer qu'un élément de B n'est pas son propre inverse).
b) Démontrer que si B est vide alors G est abélien.
c) Montrer que G contient un élément d'ordre 2.

Exercice 14. Soit G est un groupe d'ordre pq avec $p > q$, p et q premiers. Montrer que G contient au plus un sous-groupe d'ordre p, et que celui-ci, s'il existe, est normal.

Exercice 15. Soit G un groupe, H et K deux sous groupes, avec H normal dans G.
1) Rappeler pourquoi $HK := \{hk \mid h \in H,\ k \in K\}$ est un sous-groupe.
2) Établir l'isomorphisme :

$$HK/H \simeq K/H \cap K \ .$$

***

Le but des 5 exercices qui suivent est de décrire à isomorphisme près tous les groupes d'ordre inférieur ou égal à 8.

Exercice 16. Pour commencer que peut-on dire des groupes d'ordre premier ?

Exercice 17. Montrer qu'un groupe d'ordre 4 est soit isomorphe à $\mathbb{Z}/4\mathbb{Z}$, soit isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 18. Soit G un groupe d'ordre 6. Montrer que si G n'est pas cyclique, G est non commutatif et engendré par un élément d'ordre 2 et un élément d'ordre 3. Trouver tous les sous-groupes et tous les sous-groupes normaux d'un tel groupe. En déduire qu'un groupe d'ordre 6 est soit isomorphe à $\mathbb{Z}/6\mathbb{Z}$, soit isomorphe au groupe symétrique S_3 des permutations de $\{1, 2, 3\}$.

Exercice 19. Soit G un groupe *abélien* d'ordre 8 d'élément neutre e.
a) On suppose qu'il existe dans G un élément a d'ordre 8. Montrer que G est isomorphe à $\mathbb{Z}/8\mathbb{Z}$.
b) On suppose qu'il n'y a pas d'élément d'ordre 8 dans G mais qu'il existe un élément a d'ordre 4.

- Soit b un élément de G n'appartenant pas à $< a >$. Montrer que $b^2 = e$ ou $b^2 = a^2$. En déduire l'existence d'un élément de G n'appartenant pas à $< a >$ et qui soit d'ordre 2.
- Montrer que G est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

c) On suppose enfin que tous les éléments de $G \setminus \{e\}$ sont d'ordre 2. En considérant la table de multiplication de G, montrer que G est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
d) Conclure qu'un groupe abélien d'ordre 8 est nécessairement isomorphe à $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 20. Soit maintenant G un groupe *non abélien* d'ordre 8 d'élément neutre e.
a) Montrer qu'il existe dans G un élément d'ordre 4. Soit a un tel élément.
b) Montrer que $< a >$ est un sous-groupe normal de G.
c) Soit $b \notin < a >$. Montrer que G est engendré par a et b.
d) Montrer que $b^2 = e$ ou $b^2 = a^2$.
e) En calculant l'ordre de bab^{-1} montrer que $ba = a^3b$.
f) En déduire que tout groupe non abélien d'ordre 8 est isomorphe soit à G_1 engendré par a et b tels que $a^4 = 1$, $b^2 = 1$, $ba = a^3b$, soit à G_2 engendré par a et b tels que $a^4 = 1$, $b^2 = a^2$, $ba = a^3b$, et que G_1 et G_2 ne sont pas isomorphes.

***

Exercice 21. Soit p un nombre premier et n un entier ≥ 1.
a) (Fermat) Montrer que pour tout entier m on a $m^p \equiv m \pmod{p}$.
b) (Euler) Montrer que pour tout entier m premier avec n, on a $m^{\varphi(n)} \equiv 1 \pmod{n}$.
c) (Wilson) Montrer l'equivalence entre :
(i) q est un nombre premier.
(ii) $(q-1)! \equiv -1 \pmod{q}$.

Exercice 22.

1. Démontrer que pour $n \geqslant 2$, S_n admet pour système de générateurs les permutations $(1, i)$, $i = 2, \ldots, n$.
2. Montrer que S_n est engendré par les transpositions $(k, k+1)$, $k = 1 \ldots n-1$.
3. Montrer que S_n est engendré par les deux éléments $\sigma = (1\ 2\ \ldots n)$ et $\tau = (1\ 2)$ (on pourra calculer $\sigma^i \tau \sigma^{-i}$)
4. Démontrer que pour $n \geqslant 3$, A_n admet pour système de générateurs les 3-cycles $(1, 2, i)$, $i = 3, \ldots, n$.

Exercice 23.

1. Démontrer que pour $n \geqslant 3$ les 3-cycles sont conjugués dans S_n.
2. Démontrer que pour $n \geqslant 5$ les 3-cycles sont conjugués dans A_n. Etudier les cas $n = 3, 4$.

Exercice 24. Soit n un entier supérieur ou égal à 3. Soit $\sigma \in S_n$ telque $\sigma\tau\sigma^{-1} = \tau$ pour tout τ dans S_n. En prenant $\tau = (i, j)$, démontrer que σ est la permutation identité. Que peut-on dire de $Z(S_n)$?

Exercice 25. Soit E un ensemble à n éléments, par exemple $E = \{1, \ldots, n\}$. Le groupe $G = S_n$ opère naturellement sur E, par permutation des éléments.

1. Montrer que le stabilisateur d'une partie X à k éléments est isomorphe à $S_k \times S_{n-k}$. En déduire le cardinal de l'orbite de X. Quel résultat (bien connu...) retrouve-t-on ?
2. En s'inspirant de la question précédente, calculer le nombre de partitions de E de type $(n_1, \ldots, n_s)$, c'est-à-dire le nombre de partitions de E de la forme

$$E = E_1 \cup \cdots \cup E_s, \ \text{ avec } \operatorname{Card} E_i = n_i.$$

Exercice 26. Soit G un groupe fini d'ordre n, d'élément neutre e, et p un nombre premier. On définit

$$E := \{(x_1, \cdots, x_p) \in G^p \mid x_1 \cdots x_p = e\}.$$

1. Quel est le cardinal de E ?
2. Montrer que si $(x_1, \cdots, x_p)$ appartient à E, alors $(x_2, \cdots, x_{p-1}, x_p, x_1)$ également. En déduire une action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur E.
3. On note t le nombre d'orbites ponctuelles sous l'action précédente. Montrer que $n^{p-1} \equiv t \mod p$.
   (a) Si p divise n, en déduire que G possède au moins un élément d'ordre p (c'est le théorème de Cauchy).
   (b) Si p ne divise pas n, quel résultat classique retrouve-t-on ?

Exercice 27. Soit G un groupe d'ordre p^n, avec p premier et $n \geqslant 1$, et H un sous-groupe normal non réduit à l'élément neutre. En faisant opérer G sur H par conjugaison, montrer que $H \cap Z(G) \neq \{e\}$.

Exercice 28. Soit G un groupe fini d'ordre n et H un sous-groupe normal de G ayant pour ordre le plus petit facteur premier divisant n. Montrer en faisant agir G sur H par conjugaison que H est inclus dans le centre de G.

Exercice 29. Soit G un groupe d'ordre n et H un sous-groupe de G d'indice p le plus petit facteur premier divisant n. Montrer que H est normal.
Indication : on fera agir H par translation à gauche sur l'ensemble des classes à gauche modulo H.

Exercice 30. Soit G un groupe d'ordre p^2 avec p premier.

1. Montrer que $G/Z(G)$ est cyclique et en déduire que G est abélien.
2. Conclure que G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 31. Soit $G =< a, b >$ un groupe d'ordre $2n$ avec a d'ordre n, b d'ordre 2 et ab d'ordre n. Montrer que G est isomorphe au groupe diédral d'ordre $2n$.

Exercice 32.

1. *Formule de Burnside* Soit G un groupe fini opérant sur un ensemble fini E. On note k le nombre d'orbites deux à deux disjointes de E sous cette action. Établir la formule :

$$k = \frac{1}{|G|} \sum_{g \in G} \operatorname{Card} \operatorname{Fix}_g,$$

   où pour tout $g \in G$ on a posé $\operatorname{Fix}_g = \{x \in E \mid g \cdot x = x\}$.
   Indication : considérer l'ensemble $F = \{(g, x) \in G \times E \mid g \cdot x = x\}$. En écrivant

$$F = \cup_{g \in G} \{(g, x)\ ,\ x \in E \mid g \cdot x = x\} = \cup_{x \in E} \{(g, x)\ ,\ g \in G \mid g \cdot x = x\},$$

   trouver deux expressions pour le cardinal de F et conclure.

2. Application : *le problème de la roulette.* Soit une roulette à n secteurs, $n \geqslant 2$, que l'on veut colorier à l'aide de q couleurs, chaque secteur étant peint de façon arbitraire avec l'une de ces q couleurs. Deux coloriages sont identiques si on les déduit l'un de l'autre par une rotation d'angle $\frac{2k\pi}{n}$ avec k convenable. Montrer que le nombre $\mathcal{C}(n, q)$ de coloriages possibles est :

$$\mathcal{C}(n, q) = \frac{1}{n} \sum_{d|n} \varphi(d) q^{n/d},$$

   où $\varphi(d) = |(\mathbb{Z}/d\mathbb{Z})^\times|$, fonction indicatrice d'Euler.