ÉNS de Lyon
M2 FEADEP

Cours d'algèbre
2018-2019

Feuille d'exercices n°5 : Groupes finis usuels

Dans toute la feuille G est un groupe et e est son élément neutre.
On rappelle que l'*exposant* d'un groupe G est $\exp(G) = \inf\{n \in \mathbb{N},\ \forall gh \in G\ h^n = e\}$.

À faire

Groupe cyclique

Un groupe est dit *monogène* s'il est engendré par un seul élément. On appelle *groupe cyclique* d'ordre n le groupe monogène C_n à n éléments.

Exercice 1. Soit $g \in G$ un élément d'ordre fini $d \in \mathbb{N}^*$. Soit $k \in \mathbb{Z}$.

1. Montrer que si G est fini, alors d divise $|G|$.
2. Montrer que $g^k = e$ si, et seulement si, d divise k.
3. Montrer que g^k est d'ordre $\frac{d}{\mathrm{pgcd}(d,k)}$.
4. Soit h un élément d'ordre δ. On suppose que g et h commutent.
   (a) Montrer que si d et δ sont premier entre eux, alors gh est d'ordre $d\delta$.
   (b) Montrer qu'il existe des entiers a, b tels que $g^a h^b$ est d'ordre $\mathrm{ppcm}(d, \delta)$.

Exercice 2.

1. Montrer que tout groupe monogène est isomorphe à $\mathbb{Z}$ ou à $C_n \simeq \mathbb{Z}/n\mathbb{Z}$.
2. Quels sont les groupes qui n'admettent pas de sous-groupes stricts non triviaux ?
3. Montrer que les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ sont les inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$ de l'anneau $\mathbb{Z}/n\mathbb{Z}$ et les décrire.
4. Montrer que C_n admet un sous-groupe (resp. quotient) d'ordre d si, et seulement si, d divise n et que ce sous-groupe (resp. quotient) est alors unique.
5. Montrer que $\mathrm{Aut}(C_n) \simeq \mathbb{Z}/n\mathbb{Z}^\times$.

Groupe symétrique et groupe alterné

Soit $n \geq 2$. On note $\mathfrak{S}_n$ le groupe des permutations de $[\![1, n]\!]$, appelé *groupe symétrique*. On note $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ la signature et $\mathfrak{A}_n$ son noyau, appelé *groupe alterné*.

Exercice 3.

1. Rappeler pourquoi toute permutation se décompose en produit de cycles à supports disjoints.
2. Montrer que les transpositions engendrent $\mathfrak{S}_n$. Montrer qu'on peut se limiter aux transpositions de la forme $(1\ i)$ (resp. de la forme $(i\ i+1)$).
3. Montrer que la transposition $(i\ j)$ et le n-cycle $(1\ 2 \dots n)$ engendrent $\mathfrak{S}_n$ si, et seulement si, $i - j$ et n sont premiers entre eux.
4. Montrer que l'ordre d'un élément de $\mathfrak{S}_n$ est le ppcm des longueurs des cycles dans une décomposition en produit de cycles à support disjoint.
5. Quel est l'exposant de $\mathfrak{S}_n$?
6. (a) Soit $(i_1 \dots i_k)$ un k-cycle et $\sigma \in \mathfrak{S}_n$. Montrer que $\sigma(i_1 \dots i_k)\sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$.
   (b) Décrire les classes de conjugaison dans $\mathfrak{S}_n$.
   (c) En déduire que le nombre de classes de conjugaison dans $\mathfrak{S}_n$ est égal au nombre de partitions de n (c'est-à-dire le nombre de manières d'écrire n comme une addition d'entiers croissants).
7. Décrire le centre de $\mathfrak{S}_n$.
8. Quels sont les morphismes de groupes de $\mathfrak{S}_n$ dans $\mathbb{C}^\times$?

Exercice 4.

1. (a) Montrer que les 3-cycles $(1\ 2\ i)$ pour $i \in [\![3, n]\!]$ engendrent $\mathfrak{A}_n$.
   (b) Montrer que les 3-cycles $(i-1\ i\ i+1)$ pour $i \in [\![2, n-1]\!]$ engendrent $\mathfrak{A}_n$.
   (c) Montrer que $\mathfrak{A}_n$ est engendré par les carrés de $\mathfrak{S}_n$.
   (d) Les éléments de $\mathfrak{A}_n$ sont-ils tous des carrés ?
   (e) Montrer que les cycles $(2\ 3\ 4)$ et $(2\ 4\ 3)$ sont conjugués dans $\mathfrak{S}_4$ mais pas dans $\mathfrak{A}_4$.
2. Décrire le centre de $\mathfrak{A}_n$.
3. Montrer que $\mathfrak{A}_n$ est le groupe dérivé de $\mathfrak{S}_n$.
4. On suppose que $n \geq 5$. Montrer que les 3-cycles sont conjugués dans $\mathfrak{A}_n$.
5. En déduire que $\mathfrak{A}_n$ est parfait, c'est-à-dire que $\mathcal{D}(\mathfrak{A}_n) = \mathfrak{A}_n$.
6. Calculer le groupe dérivé de $\mathfrak{A}_2$, $\mathfrak{A}_3$, $\mathfrak{A}_4$.

Groupe diédral

Pour $n \geq 3$, on note D_n le groupe d'isométries du polygone régulier à n sommets. On l'appelle le *groupe diédral* d'ordre $2n$ [*].

Exercice 5.

1. Montrer que l'ordre de D_n est $2n$.
2. Montrer qu'il existe deux éléments $r, s \in D_n$ qui engendrent D_n d'ordre n et 2 respectivement, tels que $rsr = s$.
3. Montrer que D_n est engendré par deux éléments d'ordre 2.
4. Montrer que les classes de conjugaison dans D_n sont :
   (a) $\{1\}$, $\{r^{\pm k}\}$ pour $k \in [\![1, \frac{n-1}{2}]\!]$ et $\{r^k s,\ k \in [\![0, n-1]\!]\}$ si n est impair ;
   (b) $\{1\}$, $\{r^{\pm k}\}$ pour $k \in [\![1, \frac{n}{2}-1]\!]$, $\{r^{n/2}\}$, $\{r^{2k}s,\ k \in [\![0, \frac{n}{2}-1]\!]\}$ et $\{r^{2k+1}s,\ k \in [\![0, \frac{n}{2}-1]\!]\}$ si n est pair.

Exercice 6.

1. Décrire le centre et le groupe dérivé de D_n.
2. Montrer que D_n est le seul groupe, à isomorphisme près, engendré par deux éléments a, b tels que $a^n = b^2 = (ab)^n = 1$.
3. Montrer qu'un groupe fini non abélien engendré par deux éléments d'ordre deux est isomorphe à D_n pour un certain $n \in \mathbb{N}^*$.
4. Montrer qu'un sous-groupe de D_n est :
   (a) soit cyclique et engendré par un r^d pour d divisant n ;
   (b) soit diédral et engendré par r^d et $r^i s$ pour d divisant n et $i \in [\![0, d-1]\!]$

   Préciser alors l'indice d'un tel sous-groupe.
5. Montrer que les sous-groupes propres distingués de D_n sont :
   (a) les sous-groupes cycliques de D_n si n est impair ;
   (b) les sous-groupes cycliques de D_n et les sous-groupes d'indice 2 – à savoir $\langle r^2, s\rangle$ et $\langle r^2, rs\rangle$ – si n est pair.

∗. On note aussi parfois D_{2n} au lieu de D_n, alors attention aux conventions de l'auteur !

Problèmes

Exercice 7. ***(Structure du groupe*** $\mathrm{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ ***)***
On note $\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$. Soit $n \in \mathbb{N}^*$ qu'on décompose en son produit de puissances de ses facteurs premiers $n = \prod_i p_i^{\alpha_i}$.

1. Montrer qu'on a un isomorphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \simeq \prod_i \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$.
2. Montrer qu'on a un isomorphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_i (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$.
3. Montrer les égalités $\varphi(n) = \prod_i \varphi(p_i^{\alpha_i}) = n\prod_i \left(1 - \frac{1}{p_i}\right)$.
4. Soit $p \geq 3$ un nombre premier et $\alpha \in \mathbb{N}^*$.
   (a) Montrer que $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.
   (b) Montrer qu'il existe un entier $m \in \mathbb{N}^*$ premier à p tel que $(1+p)^{p^\alpha} = 1 + mp^{\alpha+1}$.
   (c) En déduire un isomorphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)p^{\alpha-1}\mathbb{Z}$.
   Indication : on pourra considérer l'homomorphisme surjectif $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$.
5. Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \{1\}$ et que $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$.
6. Soit $\alpha \in \mathbb{N}^*$.
   (a) Montrer qu'il existe un nombre impair m tel que $5^{2^\alpha} = 1 + m2^{\alpha+2}$.
   (b) En déduire que, pour $\alpha \geq 3$, on a l'isomorphisme de groupes $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \left(\mathbb{Z}/2^{\alpha-2}\mathbb{Z}\right)^\times$.
   Indication : on pourra considérer l'homomorphisme surjectif $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$.

Exercice 8. ***(Classes de conjugaison dans*** $\mathfrak{A}_n$***)***
Soit $n \geq 2$. Dans cet exercice, pour toute permutation $\sigma \in \mathfrak{S}_n$ (resp. $\sigma \in \mathfrak{A}_n$), on note $\mathcal{CS}(\sigma)$ (resp. $\mathcal{CA}(\sigma)$) la classe de conjugaison de σ dans $\mathfrak{S}_n$ (resp. $\mathfrak{A}_n$). Soit $\sigma \in \mathfrak{A}_n$ et $\tau \in \mathfrak{S}_n \setminus \mathfrak{A}_n$.

1. Montrer que $\mathcal{CS}(\sigma) = \mathcal{CA}(\sigma) \cup \mathcal{CA}(\tau\sigma\tau^{-1})$.
2. Montrer que les classes de conjugaison $\mathcal{CA}(\sigma)$ et $\mathcal{CA}(\tau\sigma\tau^{-1})$ ont même cardinal et sont égales ou disjointes.
3. Montrer que $\mathcal{CS}(\sigma) = \mathcal{CA}(\sigma)$ si, et seulement si, il existe une permutation $\rho \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ telle que $\sigma = \rho\sigma\rho^{-1}$.
4. Montrer que si la décomposition de σ en produit de cycles à supports disjoints contient un cycle de longueur paire, alors $\mathcal{CS}(\sigma) = \mathcal{CA}(\sigma)$.
5. Montrer que si la décomposition de σ en produit de cycles à supports disjoints contient deux cycles de même longueur (les points fixes étant des cycles de longueur 1), alors $\mathcal{CS}(\sigma) = \mathcal{CA}(\sigma)$.
6. Montrer que dans tous les autres cas, on a $\mathcal{CS}(\sigma) \neq \mathcal{CA}(\sigma)$.
   Indication : On pourra commencer par déterminer l'ensemble des permutations qui commutent avec un cycle donné.

Exercice 9. ***(Simplicité de*** $\mathcal{A}_n$ ***pour*** $n \geq 5$***)***
Soit $n \geq 5$ et H un sous-groupe distingué non trivial de $\mathfrak{A}_n$. Soit $\sigma \in H$ un élément non trivial et $a \in [\![1, n]\!]$ un élément dans le support de σ. Soit $b = \sigma(a)$ et $c \notin \{a, \sigma(a), \sigma^{-1}(a)\}$.

1. Montrer que les 3-cycles sont conjugués dans $\mathfrak{A}_n$ pour $n \geq 5$.
2. Montrer que $(a\ b\ c)^{-1}\sigma(a\ b\ c)\sigma^{-1}$ est soit un 3-cycle, soit un 5-cycle, soit un produit de deux transpositions à supports disjoints.
3. Supposons que H contient le 5-cycle $\tau = (a\ b\ c\ d\ e)$. Calculer $(a\ b\ c)^{-1}\tau(a\ b\ c)\tau^{-1}$ et en déduire que $H = \mathfrak{A}_n$.
4. Supposons que H contient le produit de deux transpositions à supports disjoints $\tau = (a\ b)(c\ d)$. Soit $e \notin \{a, b, c, d\}$. Calculer $(a\ b\ e)^{-1}\tau(a\ b\ e)\tau^{-1}$ et en déduire que $H = \mathfrak{A}_n$.
5. Montrer que $\mathfrak{A}_n$ est simple.
6. Montrer que $\mathfrak{A}_4$ n'est pas simple.
7. Quels sont les sous-groupes distingués de $\mathfrak{S}_n$?
8. Existe-t-il un morphisme surjectif $\mathfrak{S}_n \to \mathfrak{S}_{n-1}$?
9. Montrer que tout sous-groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.

Pour aller plus loin

Exercice 10. Soit G un groupe fini d'ordre n.

1. Montrer que G a une partie génératrice avec au plus $\log_2 n$ éléments.
   Indication : on pourra définir une suite d'éléments $(g_k)_k$ tels que $g_{k+1} \notin \langle g_0, \dots, g_k \rangle$.
2. En déduire que G admet au plus $n^{\log_2 n}$ automorphismes.
3. Combien $G = (\mathbb{Z}/2\mathbb{Z})^d$ a-t-il d'automorphismes ? Comparer ce nombre avec le résultat de la question précédente.
4. Montrer qu'il y a, au plus [†], $n^{n \log_2 n}$ classes d'isomorphismes de groupes de cardinal n.
   Indication : On pourra plonger un groupe fini dans $\mathfrak{S}_n$.

†. C'est une très mauvaise approximation en général. Actuellement, on conjecture que presque tout groupe fini est un 2-groupe. Par exemple, parmi les classes d'isomorphismes de groupes d'ordre inférieur à $2000 < 2048 = 2^{11}$, il y a plus de 99% d'entre eux qui sont d'ordre exactement $1024 = 2^{10}$ mais $n^{\log_2 n}$ semble une borne plus raisonnable.