Licence (L3) *Année 2016/2017*

ALGÈBRE

Exercices sur les groupes

A. Chambert-Loir

EXERCICE 1

Soit A un groupe fini opérant dans un ensemble fini X. Pour tout $a \in A$, on pose $X^a = \{x \in X\,;\, a \cdot x = x\}$ (ensemble des points fixes de a).

1 En comptant de deux façons l'ensemble des couples $(a,x) \in A \times X$ tels que $a \cdot x = x$, démontrer que l'on a

$$\sum_{a \in A} \operatorname{Card}(X^a) = \sum_{x \in X} \operatorname{Card}(A_x).$$

2 En déduire la « formule de Burnside » [1] :

$$\operatorname{Card}(X/A) = \frac{1}{\operatorname{Card}(A)} \sum_{a \in A} \operatorname{Card}(X^a).$$

3 Soit n et q deux entiers. On s'intéresse à des colliers de n perles pour lesquelles on dispose de q modèles. Combien y a-t-il de colliers possibles lorsqu'on identifie deux colliers qui se déduisent l'un de l'autre par une rotation ?

4 On suppose que A opère transitivement dans X. Démontrer qu'il existe un élément $a \in A$ tel que $a \cdot x \neq x$ pour tout x. [2]

EXERCICE 2

Soit p un nombre premier et soit A un groupe fini, non réduit à $\{e\}$, dont le cardinal est une puissance de p.

1 Démontrer que le centre de A n'est pas trivial.

2 Soit K un corps fini de caractéristique p, soit V un K-espace vectoriel de dimension finie et soit ρ une représentation linéaire de A dans V, c'est-à-dire un homomorphisme de groupes de A dans $\mathrm{GL}(V)$. Démontrer qu'il existe un vecteur non nul $v \in V$ tel que $\rho(a) \cdot v = v$ pour tout $a \in A$.

3 (*suite*) Démontrer qu'il existe une base de V telle que pour tout $a \in A$, la matrice de $\rho(a)$ dans cette base soit triangulaire supérieure, à diagonale formée de 1.

EXERCICE 3

On reprend les notations de l'exemple **??**. Pour chacun des trois ensembles générateurs, trouver un entier N, si possible minimal, tel que tout élément soit un produit d'au plus N éléments parmi les générateurs donnés et leurs inverses. Quels éléments de $\mathfrak{S}_n$ atteignent cette borne ?

EXERCICE 4

Soit a et b des élements de $\{1,\dots,n\}$; pour que le n-cycle $(1\ \dots\ n)$ et la transposition $(a\ b)$ engendrent $\mathfrak{S}_n$, il faut et il suffit que $\operatorname{pgcd}(n, b-a) = 1$.

1. Attribuée à Frobenius (1887) par Burnside (1897), cette formule était déjà connue de Cauchy (1845).
2. C'est un théorème de C. Jordan (1872).

EXERCICE 5

Si un ensemble S de transpositions engendre $\mathfrak{S}_n$, on a $\operatorname{Card}(S) \geqslant n-1$.

EXERCICE 6

Soit A un groupe et soit B un sous-groupe. Démontrer que B est un sous-groupe distingué de A si et seulement toute classe à droite modulo B est une classe à gauche modulo B.

EXERCICE 7 (Lemme de Zassenhaus)

Soit G un groupe, soit A, B des sous-groupes de G. Soit A' un sous-groupe distingué de A et soit B' un sous-groupe distingué de B.

1 Démontrer que $A'\cdot(A\cap B)$ est un sous-groupe de G et que $A'\cdot(A\cap B')$ en est un sous-groupe distingué.

2 Démontrer de même que $(A\cap B)\cdot B'$ est un sous-groupe de G dont $(A'\cap B)\cdot B'$ est un sous-groupe distingué.

3 Démontrer que $(A'\cap B)\cdot(A\cap B')$ est un sous-groupe distingué de $A\cap B$.

4 Démontrer que les trois groupes quotients

$$\big(A'\cdot(A\cap B)\big)/\big(A'\cdot(A\cap B')\big),$$
$$\big((A\cap B)\cdot B'\big)/\big((A'\cap B)\cdot B'\big),$$
$$(A\cap B)/\big((A'\cap B)\cdot(A\cap B')\big)$$

sont isomorphes.

EXERCICE 8 (Jordan-Hölder)

Soit A un groupe. On dit qu'une suite $(A_0,\dots,A_n)$ de sous-groupes de A est une *suite de composition* si $A_0=\{e\}$, $A_n=A$ et si A_{i-1} est un sous-groupe distingué de A_i pour tout $i\in\{1,\dots,n\}$; l'entier n est appelé sa *longueur*.

1 Soit $(A_0,\dots,A_n)$ une suite de composition de A. Démontrer que les propriétés suivantes sont équivalentes :

(i) Pour tout $i\in\{1,\dots,n\}$, le groupe quotient A_i/A_{i-1} est simple ;

(ii) Pour tout $i\in\{1,\dots,n\}$, A_{i-1} est un sous-groupe distingué maximal de A_i ;

(iii) Il n'existe pas de suite de composition $(B_0,\dots,B_m)$ de A et d'application $f\colon\{0,\dots,n\}\to\{0,\dots,m\}$ telle que $m>n$ et $A_i=B_{f(i)}$ pour tout i.

Si elles sont vérifiées, on dit que la suite $(A_0,\dots,A_n)$ est une *suite de Jordan-Hölder*.

2 On suppose que A est fini. Démontrer qu'il possède une suite de Jordan-Hölder.

3 Soit n un entier ; décrire toutes les suites de Jordan-Hölder du groupe $\mathbf{Z}/n\mathbf{Z}$.

4 Soit $(A_0,\dots,A_n)$ et $(B_0,\dots,B_m)$ des suites de Jordan-Hölder de A. On pose $f(0)=0$; pour $i\in\{1,\dots,n\}$, soit $f(i)$ le plus petit entier j tel que $A_{i-1}\cdot(A_i\cap B_j)=A_i$. Démontrer que f est une bijection de $\{0,\dots,n\}$ sur $\{0,\dots,m\}$ (en particulier, $n=m$) et que pour tout $i\in\{1,\dots,n\}$, les groupes A_i/A_{i-1} et $B_{f(i)}/B_{f(i)-1}$ sont isomorphes.

EXERCICE 9

Soit Q le groupe quaternionique d'ordre 8.

1 Démontrer que tout sous-groupe de Q est distingué, bien que ce groupe ne soit pas commutatif.

2 Quels sont les sous-groupes caractéristiques de Q ?

EXERCICE 10

Identifier les groupes engendrés par générateurs et relations suivants : $\langle x \mid x^n\rangle$ (pour $n \in \mathbf{N}$) ; $\langle x, y \mid xyx^{-1}y^{-1}\rangle$; $\langle i, j \mid jiji^{-1}, ijij^{-1}\rangle$.

EXERCICE 11

Soit G le groupe défini par l'ensemble générateur $\{x_1, \dots, x_n\}$ et les relations x_i^2 (pour $1 \leqslant i \leqslant n$), $x_i x_j x_i^{-1} x_j^{-1}$ (pour $1 \leqslant i, j \leqslant n$ et $j - i \geqslant 2$), $(x_i x_{i+1})^3$.

1 Démontrer qu'il existe un unique homomorphisme de groupes φ de G dans $\mathfrak{S}_{n+1}$ qui applique x_i sur la transposition $(i\ i+1)$, pour tout $i \in \{1, \dots, n\}$. Démontrer que φ est surjectif.

2 Démontrer que l'on a $G/H = \{H, x_n H, x_{n-1}x_n H, \dots, x_1 \dots x_n H\}$.

3 En déduire que par récurrence sur n que $\operatorname{Card}(G) \leqslant (n+1)!$, puis que φ est un isomorphisme.

EXERCICE 12

Démontrer qu'un groupe libre est sans torsion.

EXERCICE 13

Soit n un entier. Démontrer que l'ensemble des homomorphismes du groupe libre F_n dans le groupe $\mathbf{Z}/2\mathbf{Z}$ est fini et calculer son cardinal. En déduire que si m et n sont des entiers distincts, les groupes F_m et F_n ne sont pas isomorphes.

EXERCICE 14

Soit G un groupe, soit N un sous-groupe distingué de G ; on suppose que G/N est isomorphe à un groupe libre. Démontrer qu'il existe un sous-groupe F de G tel que $G = F \cdot N$ et $F \cap N = \{e\}$.

EXERCICE 15 (« Ping-pong », Felix Klein)

Soit G un groupe opérant dans un ensemble E et soit a, b des éléments de G. On suppose qu'il existe des parties A, B de E, non vides, telles que $A \not\subset B$, et telles que $a^n \cdot A \subset B$ et $b^n \cdot B \subset A$ pour tout entier $n \in \mathbf{Z}$ tel que $n \neq 0$. Soit $\varphi \colon F(a,b) \to G$ l'homomorphisme canonique du groupe libre sur $\{a, b\}$ dans G qui applique a et b sur a et b respectivement.

1 Soit $m \in M'(a,b)$ un mot réduit débutant et finissant par a ou a^{-1}. Démontrer que l'on a $\varphi(m) \cdot A \subset B$ et en déduire que $\varphi(m) \neq e$.

2 Démontrer que φ est injectif.

EXERCICE 16

On fait opérer $\mathrm{GL}(2, \mathbf{C})$ sur $\mathbf{C}^2$ de façon usuelle. Soit A (*resp.* B) l'ensemble des couples $(x, y) \in \mathbf{C}^2$ tels que $|x| < |y|$ (*resp.* $|x| > |y|$). Soit u et v des nombres complexes tels que $|u| \geqslant 2$ et $|v| \geqslant 2$; on pose $a = \left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right)$ et $b = \left(\begin{smallmatrix} 1 & 0 \\ v & 1 \end{smallmatrix}\right)$.

1 Démontrer que $a \cdot A \subset B$ et $b \cdot B \subset A$.

2 Démontrer que l'unique homomorphisme de $F(a,b)$ dans $\mathrm{GL}(2, \mathbf{C})$ qui applique a et b sur a et b respectivement est injectif.

EXERCICE 17 (Jeu de taquin [3])

Le jeu de taquin, inventé dans les années 1870 et traditionnellement attribué à Sam Loyd, consiste en 15 pièces carrées placées à l'intérieur d'une boîte 4×4 ; il reste donc une case vide et chaque étape du jeu consiste à faire coulisser une des pièces vers la case vide. Le problème initial était, partant de l'agencement

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

de retrouver l'agencement initial

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

dans lesquels les cases 14 et 15 ont retrouvées leur place.

1 On considère un état du jeu comme une permutation d'un ensemble à 16 éléments, $\{1, 2, \ldots, 15, \square\}$, où $\square$ représente la case vide. Démontrer que chaque étape du jeu consiste à multiplier la permutation précédente par une transposition. Évaluer la parité du nombre d'étapes effectuées en fonction de la position finale de la case vide. Que pensez-vous du problème posé par Sam Loyd ?

2 Pour analyser le jeu plus précisément, et notamment déterminer l'ensemble des configurations qui permettent de remettre le puzzle dans son état initial, on décide de numéroter les pièces comme suit :

4	3	2	1
5	6	7	8
12	11	10	9
13	14	15	16

Une état du puzzle est alors la suite des 15 numéros des cases, lorsqu'on les lit comme dans la configuration précédente, et en omettant la case vide.

3. Cet exercice est issu de la présentation de Michel Coste, *http://agreg-maths.univ-rennes1.fr/documentation/docs/taquin.pdf*.

Vérifier que la position de la case vide n'a pas d'importance.

3 On considère ces suites comme des permutations de l'ensemble à 15 éléments, $\{1,\dots,15\}$. Démontrer qu'une étape du jeu consiste à multiplier la permutation précédente par un cycle de longueur impaire. En déduire que seules les permutations paires permettent de ranger le puzzle dans son état initial.

4 Soit i un entier tel que $1 \leqslant i \leqslant 13$. Trouver une suite d'étapes du jeu qui revient à multiplier une permutation à droite par le 3-cycle $(i\ i+1\ i+2)$.

5 Soit n un entier; démontrer que les permutations de la forme $(i\ i+1\ i+2)$, pour $1 \leqslant i \leqslant n-2$, engendrent le groupe $\mathfrak{A}_n$.

6 Démontrer que les permutations qui permettent de ranger le puzzle dans son état initial sont exactement les permutations paires.

EXERCICE 18

Soit A un groupe et soit B un sous-groupe de A.

1 On pose $N = \bigcap_{a\in A} aBa^{-1}$; démontrer que N est un sous-groupe distingué de A.

2 On suppose que B est d'indice fini dans A. Démontrer que N est d'indice fini dans A.

3 On suppose que A est un groupe fini et que l'indice de B dans A est égal au plus petit facteur premier de $\mathrm{Card}(A)$ (par exemple, que $(A:B)=2$). Démontrer que B est un sous-groupe distingué de A.

EXERCICE 19

Déterminer « tous » les groupes abéliens de cardinal $\leqslant 100$.

EXERCICE 20

1 Déduire du théorème de structure des groupes abéliens finis qu'un sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

2 Observer que le groupe quaternionique d'ordre 8 est un sous-groupe fini du corps **H** des quaternions mais n'est pas cyclique.

EXERCICE 21

Soit n un entier.

1 Soit $\sigma \in \mathfrak{S}_n$. Déterminer l'ordre de σ et sa signature en fonction de son type.

2 Quels sont les ordres des éléments de $\mathfrak{S}_5$?

3 Quel est le plus petit entier n tel que $\mathfrak{S}_n$ contienne un élément d'ordre 12 ? deux éléments d'ordre 12 qui ne soient pas conjugués l'un de l'autre?

EXERCICE 22

Soit n un entier.

1 Soit $\pi = (m_1,\dots,m_r)$ une partition de n ; pour tout $i \geqslant 1$, soit p_i le nombre d'indices j tel que $m_j = i$. Vérifier que $\sum i p_i = n$.

2 Combien y a-t-il de permutations de type π ?

3 Soit $\sigma \in \mathfrak{S}_n$ une permutation de type π et soit Z_σ son centralisateur. Démontrer que $\mathrm{Card}(\mathrm{Z}_\sigma) = \prod_{i=1}^{n} p_i!\, i^{p_i}$.

EXERCICE 23

1 Faire la liste des différentes classes de conjugaison du groupe $\mathfrak{A}_5$ et, pour chacune d'entre elles, calculer leur cardinal.

2 Démontrer que $\{e\}$ est la seule partie de $\mathfrak{A}_5$ vérifiant les propriétés suivantes : elle contient e, elle est une réunion de classes de conjugaisons, et son cardinal divise celui de $\mathfrak{A}_5$.

3 En déduire que le groupe $\mathfrak{A}_5$ est simple.

4 Soit $n \geqslant 6$ et soit N un sous-groupe distingué de $\mathfrak{A}_n$ tel que $N \neq \{e\}$. Soit g un élément de $N \boldsymbol{-} \{1\}$; trouver un élément $h \in \mathfrak{A}_n$ tel que $[g,h] \neq e$ mais $[g,h]$ fixe un élément de $\{1,\ldots,n\}$. En déduire par récurrence que $N = \mathfrak{A}_n$.

EXERCICE 24

Soit n un entier $\geqslant 5$.

1 Soit A un sous-groupe distingué de $\mathfrak{S}_n$. Démontrer que $A = \{e\}$, $A = \mathfrak{A}_n$ ou $A = \mathfrak{S}_n$.

2 Soit A un sous-groupe de $\mathfrak{S}_n$ et soit $a = (\mathfrak{S}_n : A)$. Déduire de l'action par translations à gauche de $\mathfrak{S}_n$ sur l'ensemble $\mathfrak{S}_n/A$ des classes à droite modulo A un homomorphisme de $\mathfrak{S}_n$ dans $\mathfrak{S}(\mathfrak{S}_n/A)$. En déduire l'alternative : soit $A = \mathfrak{A}_n$, soit $A = \mathfrak{S}_n$, soit $a \geqslant n$.

3 Soit A un sous-groupe de $\mathfrak{S}_n$ tel que $(\mathfrak{S}_n : A) = n$. Démontrer que l'homomorphisme de la question précédente induit un isomorphisme de groupes de A sur le fixateur de la classe A dans $\mathfrak{S}(\mathfrak{S}_n/A)$. En particulier, A est isomorphe à $\mathfrak{S}_{n-1}$.

EXERCICE 25

Soit n un entier tel que $n \geqslant 7$.

1 Soit τ une transposition. Quel est l'ordre de $\varphi(\tau)$? Quel est le cardinal du centralisateur de $\varphi(\tau)$? En utilisant alors la formule de l'exercice , démontrer que $\varphi(\tau)$ est une transposition.

2 (*suite*) Pour $i \in \{2,\ldots,n\}$, soit τ_i la transposition $(1\ i)$. Démontrer qu'il existe une suite $(a_1,\ldots,a_n)$ d'entiers deux à deux distincts tels que $\varphi(\tau_i) = (a_1\ a_i)$. En déduire que φ est un automorphisme intérieur.

3 (*suite*) Conclure que l'homomorphisme canonique $\mathrm{Int}\colon \mathfrak{S}_n \to \mathrm{Aut}(\mathfrak{S}_n)$ est un isomorphisme.

EXERCICE 26

Soit A un groupe fini et soit p un nombre premier. Soit $\sigma\colon A^p \to A^p$ l'application donnée par $\sigma(a_1,\ldots,a_p) = (a_2,\ldots,a_p,a_1)$.

1 Quels sont les points fixes de σ ? Démontrer que les orbites de σ ont pour cardinal 1 ou p.

2 On note X l'ensemble des $(a_1,\ldots,a_p) \in A^p$ tels que $a_1 \ldots a_p = e$. Démontrer que σ induit par restriction une permutation de X.

3 Calculer $\mathrm{Card}(X)$. Si p divise $\mathrm{Card}(A)$, déduire des questions précédentes qu'il existe un élément $a \in A \boldsymbol{-} \{e\}$ tel que $a^p = e$.

4 Démontrer que pour tout élément $a \in \mathbf{N}$ qui n'est pas multiple de p, $a^{p-1} - 1$ est multiple de p.

EXERCICE 27

Soit p un nombre premier et soit n un entier naturel.

1 On suppose que que $n < 2p$; déterminer les p-sous-groupes de Sylow de $\mathfrak{S}_n$.

2 On suppose que p est impair et que $2p \leqslant n < p^2$. Décrire un p-sous-groupe de Sylow de $\mathfrak{S}_n$. Démontrer en particulier qu'ils sont commutatifs.

3 Décrire un p-sous-groupe de Sylow de $\mathfrak{S}_{p^2}$; observer qu'il n'est pas commutatif.

EXERCICE 28

Soit G un groupe fini de cardinal 60. Si p est un nombre premier, on note σ_p le nombre de p-sous-groupes de Sylow de G. On suppose dans la suite que $\sigma_5 \neq 1$; le but de l'exercice est de prouver que G est simple. On raisonne par l'absurde en considérant un sous-groupe distingué H de G, distinct de $\{e\}$ et de G.

1 Quel peut être le cardinal de H ?

2 Démontrer que $\sigma_2 \in \{1,3,5,15\}$, $\sigma_3 \in \{1,4,10\}$ et $\sigma_5 = 6$. Combien G contient-il d'éléments d'ordre 5 ?

3 On suppose que $\mathrm{Card}(H)$ est multiple de 5. Démontrer que $\mathrm{Card}(H) = 30$. Observer que H possède 20 éléments d'ordre 3 et en déduire que H possède un unique 5-sous-groupe de Sylow. Pourquoi cette assertion est-elle absurde?

4 On suppose que $\mathrm{Card}(H) \leqslant 4$. Prouver que G/H possède un unique sous-groupe d'ordre 5. En déduire que G possède un sous-groupe distingué H', distinct de G mais dont le cardinal est multiple de 5. En déduire une contradiction.

5 On suppose que $\mathrm{Card}(H) = 6$ ou 12. Si H possède un unique 3-sous-groupe de Sylow, démontrer que c'est un sous-groupe distingué de G et en déduire une contradiction. Sinon, démontrer que H possède un unique 2-sous-groupe de Sylow et en déduire encore une contradiction.

EXERCICE 29

Soit G un groupe simple de cardinal 60.

1 Soit A un sous-groupe de G. Démontrer que $(G : A) \geqslant 5$. (Faire opérer G dans G/A.) Si $(G : A) = 5$, démontrer que G est isomorphe à $\mathfrak{A}_5$.

2 Si p est un nombre premier, on note σ_p le nombre de p-sous-groupes de Sylow de G. Démontrer que $\sigma_2 \in \{5,15\}$, $\sigma_3 = 10$ et $\sigma_5 = 6$.

3 Si $\sigma_2 = 5$, démontrer que G est isomorphe à $\mathfrak{A}_5$. (Faire opérer G dans l'ensemble de ses 5-sous-groupes de Sylow.)

4 On suppose que $\sigma_2 = 15$. Démontrer que G possède 24 éléments d'ordre 5. En déduire qu'il existe deux sous-groupes de 2-Sylow de G, P et Q, tels que $\mathrm{Card}(P \cap Q) = 2$. Soit $N = \mathrm{N}_G(P \cap Q)$. Prouver que $(G : N) = 5$ puis que G est isomorphe à $\mathfrak{A}_5$, ce qui contredit l'hypothèse $\sigma_2 = 15$.

EXERCICE 30 (Argument de Frattini)

1 Soit A un groupe opérant dans un ensemble X. Soit B un sous-groupe de A tel que l'opération de B dans X déduite de celle de A soit transitive. Démontrer que pour tout $x \in X$, on a $A = B \cdot A_x$.

2 Soit A un groupe, soit G un sous-groupe fini de A et soit S un p-sous-groupe de Sylow de G. Démontrer que $A = G \cdot N_A(S)$.

3 Soit G un groupe fini, soit S un p-sous-groupe de Sylow de G et soit H un sous-groupe de G contenant $\mathrm{N}_G(S)$. Démontrer que $H = \mathrm{N}_G(H)$.

EXERCICE 31

1 Soit G un groupe fini, soit p un nombre premier; on suppose que le nombre de p-sous-groupes de Sylow de G n'est pas congru à 1 modulo p^2. Démontrer qu'il existe deux p-sous-groupes de Sylow P et Q de G tels que $(P : P \cap Q) = (Q : P \cap Q) = p$.

2 Soit G un groupe fini d'ordre 1053. Démontrer qu'il existe deux 3-sous-groupes de Sylow de G, P et Q, tels que $\mathrm{Card}(P \cap Q) = 3^3$. Soit $N = \mathrm{N}_G(P \cap Q)$. Démontrer que P et Q sont des sous-groupes de N. En déduire que $N = G$ et que G n'est pas simple.

EXERCICE 32 (Groupes nilpotents)

Soit A un groupe.

On définit par récurrence une suite (A_n) de sous-groupes distingués de A comme suit : $A_0 = \{e\}$ et, si A_n est défini, A_{n+1} est l'unique sous-groupe de A contenant A_n tel que A_{n+1}/A_n soit le centr de A/A_n.

On définit par récurrence une suite (A^n) de sous-groupes de A en posant $A^0 = A$ et, si A^n est défini, A^{n+1} est le sous-groupe de A engendré par $[A, A^n]$.

1 Démontrer que pour tout entier n, A_n et A^n sont des sous-groupes caractéristiques de A.

2 Démontrer que $A^m = \{e\}$ si et seulement si $A_m = A$. S'il existe un tel entier m, on dit que A est un groupe *nilpotent*.

3 On supose que $\{e\} = A^m \subsetneq A^{m-1}$. Démontrer que $A_{n-1} \subset A^{m-n} \subset A_n$ pour tout entier $n \in \{1, \dots, m\}$.

4 On suppose que A est un p-groupe. Démontrer que A est nilpotent.

EXERCICE 33

Soit p et q des nombres premiers tels que $p < q$, soit G un groupe fini de cardinal pq. Soit P un p-sous-groupe de Sylow de G, soit Q un q-sous-groupe de Sylow de G.

1 Démontrer que P et Q sont des groupes cycliques, de même que le groupe $\mathrm{Aut}(Q)$ des automorphismes de Q.

2 Démontrer que Q est un sous-groupe distingué de G. En déduire que G est un produit semi-direct de P et Q.

3 On suppose que p ne divise pas $q-1$. Démontrer que G est isomorphe à $\mathbf{Z}/pq\mathbf{Z}$.

4 On suppose que p divise $q-1$. Démontrer qu'il existe un groupe non commutatif de cardinal pq, et que deux tels groupes sont isomorphes.