M64 : Groupes, anneaux, corps 2

Licence de Mathématiques L3 S6 – Université de Lille – Année 2020-2021

Feuille de TD 1. Groupes

Exercice 1. On note par C_n un groupe cyclique d'ordre n et de générateur c. L'ordre d'un élément g d'un groupe est noté $\nu(g)$.
(i) Montrer que pour chaque diviseur positif d de n, C_n possède un unique sous-groupe d'ordre d que l'on peut définir par les formules

$$H_d = \langle c^{\frac{n}{d}} \rangle = \{x \in C_n \mid x^d = e\}.$$

(ii) Enumérer tous les sous-groupes de C_{15}.
(iii) Soient G, H des groupes et $\varphi : G \longrightarrow H$ un morphisme de groupes. Démontrer que $\nu(\varphi(a))$ divise $\nu(a)$ pour tout $a \in G$.
(iv) Soit $\varphi : C_{12} \longrightarrow C_{15}$ un morphisme non-trivial de groupes (c'est à dire, $\varphi(x)$ est différent de $e \in C_{15}$ pour au moins un $x \in C_{12}$). Identifier le sous-groupe $\operatorname{im} \varphi = \varphi(C_{12})$ dans C_{15}.
(v) Déterminer le nombre de morphismes distincts de groupes $\varphi : C_{12} \longrightarrow C_{15}$.
(vi) Décrire tous les morphismes de groupes $C_n \to C_m$ pour m, n quelconques. A quelle condition existe-t-il des morphismes injectifs ? surjectifs ?
(vii) Décrire tous les automorphismes de C_n.

Exercice 2. Soit G un groupe fini, K, H deux sous-groupes. On note par KH l'ensemble des produits kh, où $k \in K$, $h \in H$. Montrer :

$$|KH| = \frac{|K| \cdot |H|}{|K \cap H|}.$$

Remarque. Ici KH n'est pas forcément un sous-groupe ; en effet KH n'est un sous-groupe que si $KH = HK$.

Exercice 3. Soit G un groupe fini d'ordre > 1, et soit p le plus petit premier divisant l'ordre de G. Montrer que si G possède des sous-groupes d'indice p, alors tous tels sous-groupes sont distingués.

Exercice 4. Soit p un nombre premier. Montrer que pour tout p-groupe G non trivial, son centre $Z(G)$ est aussi un p-groupe non trivial.

Exercice 5. Montrer que si G est un groupe non abélien et H est un sous-groupe de $Z(G)$, alors H est distingué dans G et le groupe quotient G/H n'est pas cyclique.

Exercice 6. Soit p un nombre premier. Montrer que tout groupe d'ordre p^2 est abélien.

Exercice 7. Montrer que si G est un groupe d'order $p^k q$, où p, q sont des premiers, $q < p$, $k \in \mathbb{N}$, alors G est le produit semi-direct de ses sous-groupes K, H, $G = K \rtimes H$, où $|K| = p^k$, $|H| = q$.

Exercice 8. On déterminera les sous-groupes distingués de S_4 selon le plan suivant.

1. Faire une liste des classes de conjugaison de S_4, en indiquant pour chaque classe un représentant et sa cardinalité.
2. Montrer que tout sous-groupe distingué d'un groupe G est la réunion de classes de conjugaison de G.
3. Enumérer toutes les réunions de classes de conjugaison de S_4, contenant l'élément neutre, dont la cardinalité totale divise $|S_4|$, et en déduire la liste des sous-groupes distingués de S_4.

Exercice 9. Déterminer, à conjugaison près, tous les sous-groupes de S_4 avec leurs normalisateurs.

Exercice 10. Déterminer les nombres de sous-groupes de Sylow de S_4, A_4, S_5, A_5.

Exercice 11. Combien de p-sous-groupes de Sylow a le groupe S_p pour un premier p ?

Exercice 12. Donner toutes les paires K, H de groupes, à isomorphisme près, pour lesquels il existe de sous-groupes propres K', H' de G tels que $K \simeq K'$, $H \simeq H'$, et $G = K' \rtimes H'$, pour chacun des groupes G suivants : $G = S_3,\ A_4,\ S_4,\ D_8$ (le groupe du dièdre d'ordre 8), Q_8 (le groupe de quaternions). Est-ce qu'il y a des produits directs parmi ces produits semi-directs ?

Exercice 13. On rappelle qu'un groupe G est dit *simple* si ses seuls sous-groupes distingués sont G tout entier et le sous-groupe trivial réduit à l'élément neutre. Dans cet exercice on démontre que le groupe A_5 est simple.

1. Faire une liste des classes de conjugaison de S_5, en indiquant pour chaque classe un représentant et sa cardinalité.
2. Faire de même pour A_5.
3. Montrer qu'aucune réunion d'une partie de l'ensemble des classes de conjugaison de A_5 ne peut être un sous-groupe propre de A_5 et conclure.

Exercice 14. Dans cet exercice on démontre que tout groupe simple d'ordre 60 est isomorphe à A_5. On construira un plongement de G dans A_6 et on pourra se servir du fait que le groupe A_6 est simple.

1. On suppose que G est un groupe simple d'ordre 60. Montrer que G a six 5-sous-groupes de Sylow et en déduire un morphisme non trivial $\psi : G \to S_6$. Montrer que ce morphisme est injectif et que son image est contenue dans A_6.
2. Soit H un sous-groupe de A_6 d'indice 6. En considérant l'action de A_6 par translations sur les classes à gauche modulo H, montrer qu'il existe un morphisme injectif $\varphi : A_6 \to S_6$ tel que $\varphi(H)$ soit contenue dans S_5, où S_5 est plongé dans S_6 de façon naturelle comme le stabilisateur de 6.
3. Montrer que $\varphi(H) = A_5$ et conclure.

Exercice 15.

1. Soient p, q des premiers distincts, $p > q$. Montrer : a) si $q \nmid p-1$, tout groupe G d'ordre pq est isomorphe à C_{pq} ; b) si $q \mid p-1$, il existe exactement deux classes d'isomorphisme de groupes d'ordre pq, celles de C_{pq} et de $C_p \rtimes_\varphi C_q$, la classe du second groupe étant indépendante de choix d'un morphisme non trivial $\varphi : C_q \to \mathrm{Aut}(C_p)$.
2. Classifier, à isomorphisme près, tous les groupes d'ordre ≤ 15.

Exercice 16. Montrer qu'il n'existe pas de groupe simple d'ordre 750.

Exercice 17. Démontrer que tout groupe d'ordre 45 est commutatif.

Exercice 18. Montrer que les groupes d'ordres p^n ($n \geq 2$), pq, p^2q, p^2q^2, p^3q, pqr (p, q, r sont des premiers distincts) ne sont pas simples. *Indication pour le cas $|G| = p^3q$, où $p < q$:* si on note N_p, N_q les nombres de p-, q-sous-groupes de Sylow, montrer : a) si on suppose G simple, alors $N_p > 1$ et $N_q \in \{p, p^2, p^3\}$; b) éliminer les cas $N_q = p$ et $N_q = p^3$ (compter le nombre d'éléments d'ordre q pour le second cas, et en déduire que $N_p = 1$, ce qui est absurde) ; c) en supposant que $N_q = p^2$, montrer que $q|p+1$ et en déduire que $p = 2$, $q = 3$; d) montrer qu'un groupe d'ordre 24 avec $N_2 = 3$ ne peut pas être simple et conclure.

Exercice 19. Démontrer que tout groupe simple d'ordre < 60 est cyclique.

Exercice 20. Soit P le groupe des matrices $A = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}$ avec $a, b, c \in \mathbb{F}_p$. Démontrer que P est un p-groupe non-abélien d'ordre p^3 et que

$$Z(P) = \left\{ \begin{bmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; c \in \mathbb{F}_p \right\}.$$

Enumérer les classes de conjugaison de P.

Indication. $C_P(g) =< g > Z(P)$, $|C_P(g)| = p^2$ si $g \notin Z(P)$.

Exercice 21. Soit G un groupe. Un automorphisme $\varphi \in \mathrm{Aut}\, G$ est dit intérieur s'il existe un élément $g \in G$ tel que $\varphi(x) = gxg^{-1}$ pour tous $x \in G$.

1. Montrer que l'ensemble des automorphismes intérieurs $\mathrm{Int}(G)$ est un sous-groupe distingué de $\mathrm{Aut}\, G$, isomorphe à $G/Z(G)$, où $Z(G)$ est le centre de G.
2. Déterminer $\mathrm{Int}\, G$, $\mathrm{Aut}\, G$ et représenter $\mathrm{Aut}\, G$ comme produit semi-direct de $\mathrm{Int}\, G$ et de $H = \mathrm{Aut}\, G/\mathrm{Int}\, G$ pour $G = C_n$, D_{2n} (le groupe de diédre d'ordre $2n$, où $n \in \mathbb{N}^*$) et le groupe de quaternions Q_8. (*Indication :* $D_4 \simeq C_2 \times C_2$ et $\mathrm{Int}(C_2 \times C_2) = \{\mathrm{id}\}$, $\mathrm{Aut}(C_2 \times C_2) \simeq S_3$; pour $n \geq 3$, $\mathrm{Aut}(D_{2n}) \simeq \mathrm{Int}(D_{2n}) \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$, et $\mathrm{Int}(D_{2n}) \simeq D_{2n}$ lorsque n est impair, $\mathrm{Int}(D_{2n}) \simeq D_n$ lorsque n est pair ; $\mathrm{Aut}(Q_8)$ est isomorphe au groupe des isométries directes du cube "standard" $[-1, 1]^3$ de $\mathbb{R}^3$, et ce dernier groupe est isomorphe à S_4.)

3. Montrer que $\mathrm{Int}(S_n) \simeq S_n$ pour tout $n \geq 3$.
4. Montrer que $\mathrm{Aut}(S_n) = \mathrm{Int}(S_n)$ si $n \neq 6$ et que $[\mathrm{Aut}(S_6) : \mathrm{Int}(S_6)] = 2$.
   Indication. Montrer que la cardinalité de l'ensemble des transpositions dans S_n ne peut être égale à la cardinalité d'une autre classe de conjugaison de S_n que si $n = 6$. Comme tout automorphisme transforme les classes de conjugaison en les classes de conjugaison, les automorphismes de S_n pour $n \neq 6$ transforment les transpositions en les transpositions. Montrer qu'un tel automorphisme de S_n est intérieur. Pour $n = 6$, on peut construire un automorphisme φ de S_6 non intérieur en considérant l'action de S_5 sur ses six 5-sous-groupes de Sylow, par la méthode utilisée dans l'exercice 14. Montrer que φ^2 est intérieur.

Exercice 22. Pour un corps K, on introduit, hormis les groupes linéaires $GL_n(K)$, $SL_n(K)$, les groupes projectifs

$$PGL_n(K) = GL_n(K)/Z(GL_n(K)),\ PSL_n(K) = SL_n(K)/Z(SL_n(K))$$

de degré n. Si K est un corps fini $\mathbb{F}_q$ de cardinalité q, on remplace K par q dans les notations ci-dessus : $GL_n(q), SL_n(q), \ldots$ Le théorème de Jordan–Dixon affirme : Pour $n \geq 2$, les groupes $PSL_n(q)$ sont simples à l'exception de $PSL_2(2)$ et $PSL_2(3)$. Démontrer :

1. Le centre des groupes $GL_n(K)$, $SL_n(K)$ est formé des matrices scalaires $\lambda \mathbf{1}_n$, $\lambda \in K^*$ (et $\lambda^n = 1$ dans le second cas).
2. On a
$$|GL_n(q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}),$$
$$|PGL_n(q)| = |SL_n(q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-2})q^{n-1},$$
$$|PSL_n(q)| = \frac{1}{(q-1)\,\mathrm{pgcd}\,(q-1, n)} \prod_{i=0}^{n-1} (q^n - q^i).$$
3. On a les isomorphismes suivants :
$$PSL_2(2) \simeq S_3,\ PSL_2(3) \simeq A_4,\ PSL_2(4) \simeq PSL_2(5) \simeq A_5.$$