

Le problème et les deux exercices sont indépendants. Dans le problème, les deux dernières parties sont indépendantes, mais utilisent la première.

Problème

Soit G un groupe. On appelle sous-groupe dérivé de G le sous-groupe $D(G)$ engendré par les commutateurs de G , i.e. par les éléments $[a, b] := aba^{-1}b^{-1}$ avec a, b dans G .

On définit par récurrence une suite décroissante $(D^k(G))_{k \in \mathbb{N}}$ de sous-groupes en posant $D^0(G) := G$ et $D^{k+1}(G) := D(D^k(G))$ pour tout $k \in \mathbb{N}$. On dit que G est résoluble si et seulement si il existe $k \in \mathbb{N}$ tel que $D^k(G) = \{1_G\}$.

On appelle centre de G , l'ensemble $Z(G) := \{z \in G : \forall g \in G, zg = gz\}$. On rappelle que $Z(G)$ est un sous-groupe distingué de G .

I. Généralités

1. Montrer que $D(G)$ est réduit à $\{1_G\}$ si et seulement si G est abélien.
2. Montrer que l'inverse d'un commutateur est encore un commutateur. En déduire que $D(G)$ est l'ensemble des produits finis de commutateurs de G .
3. On note $D(G)Z(G) := \{dz : (d, z) \in D(G) \times Z(G)\}$. Montrer que $D(G)Z(G)$ est un sous-groupe de G contenant à la fois $D(G)$ et $Z(G)$.
4. Montrer que $D(G/Z(G)) = (D(G)Z(G))/Z(G)$
5. Montrer que $D(G) \triangleleft G$ et que le quotient $G/D(G)$ est abélien.
6. Soit H un sous-groupe distingué de G . Montrer que si G/H est abélien, alors $D(G) \subset H$.

II. Cas d'un p -groupe

Dans cette partie, on fixe un nombre premier p et on suppose que G est un p -groupe, autrement dit que G est fini et que son ordre est de la forme p^α avec $\alpha \in \mathbb{N}^*$. Le but de cette partie est de montrer que G est résoluble, en admettant le résultat suivant : le centre d'un p -groupe n'est jamais réduit à l'élément neutre. Pour cela on démontre par récurrence sur l'exposant α l'implication : si $|G| = p^\alpha$, alors $|D(G)|$ divise $p^{\alpha-1}$.

1. Montrer cette implication lorsque $\alpha = 1$.
2. Soit G un groupe d'ordre p^α avec $\alpha \geq 2$. On suppose l'implication ci-dessus vraie pour tous les entiers de 1 à $\alpha - 1$.
 - (a) Montrer que $|Z(G)| = p^\beta$ avec $\beta \in \llbracket 1, \alpha \rrbracket$. Quel est l'ordre de $G/Z(G)$?
 - (b) À l'aide des questions I.3 et I.4, montrer que $|D(G)|$ divise $p^{\alpha-1}$.
3. En déduire que tout p -groupe est résoluble.

III. Cas du groupe symétrique \mathfrak{S}_n avec $n \geq 3$

1. Montrer que $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$.
2. Montrer l'inclusion réciproque. Indication : calculer le commutateur de deux transpositions $(a\ b)$ et $(a\ c)$ de supports distincts mais non disjoints.
3. Que vaut $D(\mathfrak{A}_3)$?
4. Soit K le sous-groupe de \mathfrak{S}_4 formé de id_E et des doubles transpositions $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$, $(1\ 4)(2\ 3)$. Que vaut $D(K)$?
5. Montrer que $D(\mathfrak{A}_4) \subset K$. Indication : utiliser la question 6 de la première partie.
6. Montrer l'inclusion réciproque. Indication : calculer le commutateur de deux 3-cycles distincts de la forme $(a\ b\ c)$ et $(a\ b\ d)$.
7. Montrer que si $n \geq 5$, $D(\mathfrak{A}_n) = \mathfrak{A}_n$.
8. Dédire des questions précédentes que \mathfrak{S}_n est résoluble si et seulement si $n \leq 4$.

Exercice 1

Soient G un groupe, g un élément de G et $m > 1$ un entier tel que $g^m = 1_G$. On note $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ la décomposition en facteurs premiers distincts de m .

1. Montrer que si l'ordre de g est différent de m , alors il existe un indice $i \in \llbracket 1, s \rrbracket$ tel que $g^{m/p_i} = 1_G$. La réciproque est-elle vraie ?
2. Montrer que $\bar{2}$ est un générateur du groupe $(\mathbb{Z}/37\mathbb{Z})^\times$. Indication : $\bar{2}^6 = -\bar{10}$.

Exercice 2

Soit G un groupe fini d'ordre $2m$ avec $m \geq 3$ impair. Le but de l'exercice est de montrer que G possède un sous-groupe d'ordre m . On rappelle que dans un groupe fini, si chaque élément est son propre inverse, l'ordre de ce groupe est une puissance de 2.

1. Soit $s : G \rightarrow G$ l'application définie par $s(x) = x^{-1}$.
 - (a) Montrer que $s \in \mathfrak{S}(G)$. Quel est l'ordre de s ?
 - (b) À l'aide de la décomposition de s en cycles disjoints, montrer que G a au moins un élément d'ordre 2.
2. Pour tout $g \in G$, on note $\lambda_g : G \rightarrow G$ l'application définie par $\lambda_g(x) = gx$. On rappelle que $\lambda_g \in \mathfrak{S}(G)$ et que l'application $\Lambda : G \rightarrow \mathfrak{S}(G)$ définie par $\Lambda(g) = \lambda_g$ est un morphisme de groupes. On fixe $a \in G$, d'ordre 2.
 - (a) Montrer que λ_a n'a pas de point fixe. Quel est l'ordre de λ_a dans $\mathfrak{S}(G)$?
 - (b) En déduire le type et la signature de la permutation λ_a .
 - (c) Conclure en considérant $H = \text{Ker}(\varepsilon \circ \Lambda)$, où $\varepsilon : \mathfrak{S}(G) \rightarrow \{-1, 1\}$ est le morphisme signature.

Un corrigé

Problème

I. Généralités

1. Comme $D(G)$ est engendré par les $aba^{-1}b^{-1}$ pour $a, b \in G$,

$$\begin{aligned} D(G) = \{1_G\} &\iff (\forall a, b \in G, aba^{-1}b^{-1} = 1_G), \\ &\iff (\forall a, b \in G, ab = ba), \\ &\iff G \text{ abélien.} \end{aligned}$$

2. Quels que soient a, b dans G , $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$. Comme tout élément de $D(G)$ est un produit fini de commutateurs et d'inverses de commutateurs, on peut l'écrire comme un produit fini de commutateurs.
3. Pour tout $d \in D(G)$, $d = d1_G \in D(G)Z(G)$. Donc $D(G) \subset D(G)Z(G)$. Pour tout $z \in Z(G)$, $z = 1_Gz \in D(G)Z(G)$. Donc $Z(G) \subset D(G)Z(G)$. En particulier $1_G \in D(G)Z(G)$.

Pour tous $d_1, d_2 \in D(G)$ et $z_1, z_2 \in Z(G)$,

$$d_1z_1(d_2z_2)^{-1} = d_1z_1z_2^{-1}d_2^{-1} = d_1d_2^{-1}z_1z_2^{-1} \in D(G)Z(G).$$

Ainsi, $D(G)Z(G)$ est bien un sous-groupe de G contenant $D(G)$ et $Z(G)$.

Remarque : dans le cours, le deuxième théorème d'isomorphisme assure que $D(G)Z(G)$ est un sous-groupe de G car $D(G)$ est un sous-groupe de G et $Z(G)$ un sous-groupe distingué de G .

4. Pour $x \in G$, notons \bar{x} la classe de x dans $G/Z(G)$. Alors pour tous a, b dans G ,

$$\overline{\bar{a}\bar{b}^{-1}\bar{b}^{-1}} = \overline{aba^{-1}b^{-1}} \in (D(G)Z(G))/Z(G) \text{ car } aba^{-1}b^{-1} \in D(G) \subset D(G)Z(G).$$

Comme $(D(G)Z(G))/Z(G)$ est un sous-groupe de $G/Z(G)$ contenant tous les commutateurs des éléments de $G/Z(G)$, on a $D(G/Z(G)) \subset (D(G)Z(G))/Z(G)$. Montrons l'inclusion réciproque. Soit $(d, z) \in D(G) \times Z(G)$. D'après la question 2, on peut écrire d comme un produit de commutateurs d'éléments de G :

$$d = [a_1, b_1] \cdots [a_\ell, b_\ell].$$

Dans $G/Z(G)$, on a alors

$$\overline{dz} = \overline{d}\bar{z} = \bar{d} = [\bar{a}_1, \bar{b}_1] \cdots [\bar{a}_\ell, \bar{b}_\ell] \in D(G/Z(G)).$$

Donc $(D(G)Z(G))/Z(G) \subset D(G/Z(G))$ d'où l'égalité.

5. Soit $d \in D(G)$. Écrivons d comme un produit de commutateurs :

$$d = [a_1, b_1] \cdots [a_\ell, b_\ell].$$

Pour tout $g \in G$, notons ϕ_g l'automorphisme intérieur associé à g . Alors

$$\phi_g(d) = [\phi_g(a_1), \phi_g(b_1)] \cdots [\phi_g(a_\ell), \phi_g(b_\ell)] \in D(G).$$

Donc $D(G)$ est distingué dans G .

La projection canonique p de G sur $G/D(G)$ est donc un morphisme de groupes.

Pour tous a, b dans G , $[a, b] \in D(G)$, on a donc

$$[p(a), p(b)] = p(a)p(b)p(a)^{-1}p(b)^{-1} = p(aba^{-1}b^{-1}) = p([a, b]) = p(1_G),$$

d'où $p(a)p(b) = p(b)p(a)$. Donc $G/D(G)$ est abélien.

6. Soit $\pi : G \rightarrow G/H$ la projection canonique. Comme π est un morphisme de groupes et comme G/H est abélien, on a pour tous a, b dans G ,

$$\pi(aba^{-1}b^{-1}) = \pi(a)\pi(b)\pi(a)^{-1}\pi(b)^{-1} = 1_{G/H} \text{ d'où } aba^{-1}b^{-1} \in H.$$

Le sous-groupe H contient tous les commutateurs des éléments de G donc $D(G) \subset H$.

II. Cas d'un p -groupe

1. Soit G d'ordre p premier. Alors G est cyclique, donc abélien et $D(G) = \{1_G\}$.
En particulier, $|D(G)| = 1 \mid p^{1-1}$.

2. (a) Comme $Z(G)$ est un sous-groupe de G , son ordre divise $|G| = p^\alpha$ (Lagrange).
Donc $|Z(G)| = p^\beta$ avec $\beta \leq \alpha$. Mais $Z(G) \neq \{1_G\}$ d'après le résultat donné en préambule, donc $\beta \geq 1$. L'ordre de $G/Z(G)$ est donc $p^{\alpha-\beta}$.

(b) Si $1 \leq \alpha - \beta \leq \alpha - 1$, on peut appliquer l'hypothèse de récurrence à $G/Z(G)$.
Donc $|D(G/Z(G))|$ divise $p^{\alpha-\beta-1}$. Mais d'après la question I.4 et le théorème de Lagrange, $|D(G/Z(G))| = |(D(G)Z(G))/Z(G)| = |(D(G)Z(G))|/p^\beta$. Donc $|D(G)Z(G)|$ divise $p^{\alpha-1}$. Comme $D(G)$ est un sous-groupe de $D(G)Z(G)$, $|D(G)|$ divise $|D(G)Z(G)|$ et donc $p^{\alpha-1}$.

Si $\alpha - \beta = 0$, alors $Z(G) = G$ donc G est abélien et $D(G) = \{1_G\}$. L'ordre de $D(G)$ divise encore $p^{\alpha-1}$.

3. Montrons par récurrence que pour tout $k \in \llbracket 0, \alpha \rrbracket$, $|D^k(G)|$ divise $p^{\alpha-k}$.

La divisibilité est vraie si $k = 0$ puisque $D^0(G) = G$ est d'ordre p^α .

Soit $k \in \llbracket 0, \alpha - 1 \rrbracket$. Supposons que $|D^k(G)|$ divise $p^{\alpha-k}$. Si $D^k(G) = \{1_G\}$ alors $D^{k+1}(G) = \{1_G\}$. Sinon, $|D^k(G)|$ est une puissance de p autre que 1, on peut donc appliquer le résultat de la question précédente au groupe $D^k(G)$ ce qui montre que $|D^{k+1}(G)|$ divise $|D^k(G)|/p$ qui divise $p^{\alpha-k-1}$. Dans les deux cas, $|D^{k+1}(G)|$ divise $p^{\alpha-k-1}$, ce qui achève la récurrence.

Ainsi, $|D^\alpha(G)|$ divise 1, donc $D^\alpha(G) = \{1_G\}$, ce qui montre que G est résoluble.

III. Cas du groupe symétrique \mathfrak{S}_n avec $n \geq 3$

1. Soit ε le morphisme signature de \mathfrak{S}_n dans $\{-1, 1\}$. Comme $\mathfrak{A}_n = \text{Ker}(\varepsilon)$ est distingué dans \mathfrak{S}_n , et comme $\mathfrak{S}_n/\mathfrak{A}_n$ est abélien (isomorphe à $\text{Im}(\varepsilon) = \{-1, 1\}$), on a $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$ d'après la question I.6.

Autre argument. Pour tout α, β dans \mathfrak{S}_n ,

$$\varepsilon(\alpha\beta\alpha^{-1}\beta^{-1}) = \varepsilon(\alpha)\varepsilon(\beta)\varepsilon(\alpha)^{-1}\varepsilon(\beta)^{-1} = 1,$$

car le groupe $\{-1, 1\}$ est abélien. Le sous-groupe \mathfrak{A}_n contient tous les commutateurs des éléments de \mathfrak{S}_n donc $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$.

2. Soient a, b, c des entiers distincts entre 1 et n , alors

$$(a\ b)(a\ c)(a\ b)(a\ c) = (a\ b\ c).$$

Donc les 3-cycles sont des commutateurs donc sont dans $D(\mathfrak{S}_n)$. Comme \mathfrak{A}_n est engendré par les 3-cycles, on a donc $\mathfrak{A}_n \subset D(\mathfrak{S}_n)$.

3. Le groupe \mathfrak{A}_3 est d'ordre 3 donc abélien, donc $D(\mathfrak{A}_3) = \{1\}$.
4. Le groupe K est d'ordre 4 donc abélien, donc $D(K) = \{1\}$.
5. Le groupe K est un sous-groupe distingué dans \mathfrak{S}_4 et inclus dans \mathfrak{A}_4 . C'est donc un sous-groupe distingué de \mathfrak{A}_4 . Le groupe quotient K/\mathfrak{A}_4 est d'ordre 3 donc abélien. D'après la question 6, $D(\mathfrak{A}_4) \subset K$.
6. Soient $(a\ b\ c)$ et $(a\ b\ d)$ deux 3-cycles, alors

$$[(a\ b\ c), (a\ b\ d)] = (a\ b\ c)(a\ b\ d)(a\ c\ b)(a\ d\ b) = (a\ b)(c\ d).$$

Toutes les doubles transpositions sont des commutateurs d'éléments de \mathfrak{A}_4 et id appartient au sous-groupe $D(\mathfrak{A}_4)$, donc $K \subset D(\mathfrak{A}_4)$.

7. Si $n \geq 5$, $D(\mathfrak{A}_n)$ est un sous-groupe distingué de \mathfrak{A}_n , non réduit à $\{\text{id}\}$ puisque \mathfrak{A}_n n'est pas abélien. Comme \mathfrak{A}_n est simple, on a donc $D(\mathfrak{A}_n) = \mathfrak{A}_n$.
8. Pour tout $n \geq 3$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$.
Si $n = 3$, alors $D(\mathfrak{A}_3) = \{1\}$ donc \mathfrak{S}_3 est résoluble.
Si $n = 4$, $D(\mathfrak{A}_4) = K$ et $D(K) = \{1\}$ donc \mathfrak{S}_4 est résoluble.
Si $n \geq 5$, alors $D(\mathfrak{A}_n) = \mathfrak{A}_n$ donc \mathfrak{S}_n n'est pas résoluble.

Exercice 1

1. Soit d l'ordre de g . Comme $g^m = 1_G$, on a $d \mid m$, donc d est de la forme $\prod_{i=1}^s p_i^{\beta_i}$ avec $\beta_i \leq \alpha_i$ pour tout $1 \leq i \leq s$. Si $d \neq m$, alors il existe un indice i_0 tel que $\beta_{i_0} \leq \alpha_{i_0} - 1$. Par suite $d \mid (n/p_{i_0})$. Réciproquement, si $d \mid (n/p_i)$ pour un certain i , alors $d \leq (n/p_i) < n$.

2. Comme 37 est un nombre premier, $|(\mathbb{Z}/37\mathbb{Z})^\times|$ est égal à $36 = 2^2 \cdot 3^2$. D'après le théorème de Lagrange, on a $\bar{2}^{36} = 1$. Or $\bar{2}^{36/3} = \bar{2}^{12} = (-\bar{10})^2 = \bar{100} = -\bar{11} \neq \bar{1}$ et $\bar{2}^{36/2} = \bar{2}^{18} = \bar{2}^{12} \cdot \bar{2}^6 = (-\bar{11}) \cdot (-\bar{10}) = -\bar{1} \neq \bar{1}$. Ainsi, $\bar{2}$ est d'ordre 36, c'est un générateur du groupe $(\mathbb{Z}/37\mathbb{Z})^\times$.

Exercice 2

1. (a) Comme $s \circ s = id$, l'application s est bien une permutation de G et son ordre divise 2. Si s était l'application identité, tout élément de G serait son propre inverse; d'après le résultat rappelé en préambule, $|G|$ serait une puissance de 2, ce qui contredirait l'hypothèse faite sur $|G|$. Donc s est d'ordre 2.
- (b) Comme l'ordre est le PPCM des longueurs des cycles dans la décomposition en cycles disjoints, s est un produit non vide de transpositions à supports disjoints. Soit r le nombre de ces cycles. Le nombre de points fixes de s est pair puisqu'il vaut $2m - 2r$. Comme 1_G est un point fixe, s possède au moins un autre point fixe a . Comme $a \neq 1_G$ et $a^2 = 1_G$, a est d'ordre 2 dans G .
2. (a) Soit $a \in G$, d'ordre 2. S'il existait un élément g de G tel que $\lambda_a(g) = g$, alors on aurait $ag = g$ et donc $a = 1_G$, ce qui contredirait le fait que $\text{ord}(a) = 2$. En particulier $\lambda_a \neq id$. Or $\lambda_a \circ \lambda_a = \lambda_{a^2} = \lambda_{1_G} = id$, donc λ_a est d'ordre 2.
- (b) Ainsi, λ_a est donc un produit de m transpositions à supports disjoints. En particulier $\varepsilon(\lambda_a) = (-1)^m = -1$.
- (c) Comme $\varepsilon(\Lambda(a)) = -1$ et $\varepsilon(\Lambda(1_G)) = 1$, le morphisme de groupes $\varepsilon \circ \Lambda$ de G vers $\{-1; 1\}$ est surjectif. Comme $H = \text{Ker}(\varepsilon \circ \Lambda)$, le théorème d'isomorphisme montre que G/H est isomorphe à $\{-1; 1\}$. En particulier, $|G/H| = 2$ donc $|H| = |G|/2 = m$ et G possède bien un sous-groupe d'ordre m .

Barème

Problème partie I : $1+1+2+2,5+2+1 = 9,5$

Problème partie II : $1+1,5+1,5+1 = 5$

Problème partie I : $1+1+0,5+0,5+1+1+1+1,5 = 7,5$

Exercice 1 : $2+2 = 4$

Exercice 2 : $1,5+1,5+1,5+1+1,5 = 7$

Total : 33, multiplié par un facteur $21/33 = 7/11$.

Remarque sur les copies. Ce serait bien d'en tenir compte pour la suite !

La notion de sous-groupe engendré est très mal utilisée. On montre que $D(G)$ est l'ensemble des produits finis de commutateurs d'éléments de G . Ne pas faire comme si $D(G)$ était seulement l'ensemble des produits finis de commutateurs !

Si H et K sont deux sous-groupes de G , le cardinal de HK n'est pas toujours le produit des cardinaux ! La formule générale vue en TD est $|HK| \times |H \cap K| = |H| \times |K|$.

Le fait qu'un quotient G/H soit abélien n'autorise pas à commuter entre eux les éléments de $GH = \{gh : (g, h) \in G \times H\}$.

Pour montrer que (S_n) contient \mathfrak{A}_n , l'énoncé suggère de calculer un commutateur de deux transpositions qui ne commutent pas. On trouve un 3 cycle $(a b c)$. Il est indispensable d'utiliser ensuite le fait que les 3-cycles engendrent \mathfrak{A}_n pour conclure.

Beaucoup donnent des mauvaises raisons ou des raisons incomplètes pour voir que le groupe dérivé d'un groupe d'ordre p , de \mathfrak{A}_3 et du groupe de Klein est réduit au neutre, alors qu'il suffisait de montrer que ces groupes étaient abéliens au vu de leur ordre ! Si l'on entreprend de calculer tous les commutateurs des éléments de \mathfrak{A}_3 , il y en a 9 à considérer. Pour le groupe de Klein, il y en a 16 à considérer, même si beaucoup sont trivialement égaux à id.

Les récurrences sont à rédiger correctement lorsqu'elles ne sont pas triviales.

L'équivalence (valable lorsque g est élément d'un groupe multiplicatif G et $m \in \mathbb{Z}$) $g^m = 1_G \iff o(g) | m$ n'est toujours pas maîtrisée par certains. En particulier, pour dire que g est d'ordre 2, il faut dire que $g^2 = 1_G$ et que $g \neq 1_G$.

Beaucoup de preuves maladroites de la bijectivité de l'application $s : x \mapsto x^{-1}$ de G dans G . Ici, montrer l'injectivité puis la surjectivité est maladroit, surtout si la justification de la surjectivité est fautive !

Les permutations d'ordre 2 sont tous les produits non vides de transpositions à supports disjoints.

Dans l'exercice 1, très peu ont utilisé correctement la question 1 pour résoudre la question 2. Une fois qu'on a vu que $\bar{2}$ est dans $(\mathbb{Z}/37\mathbb{Z})^\times$ qui est d'ordre 36 (car 37 est premier), d'où $\bar{2}^{36} = \bar{1}$, il reste seulement à vérifier que $\bar{2}^{36/2} \neq \bar{1}$ et $\bar{2}^{36/3} \neq \bar{1}$.

Les diviseurs de $p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ sont tous les $p_1^{\beta_1} \cdots p_s^{\beta_s}$ où pour tout $i \in \llbracket 1, s \rrbracket$ on choisit β_i dans $\llbracket 0, \alpha_i \rrbracket$. Cela fait en tout $(\alpha_1 + 1) \cdots (\alpha_d + 1)$ diviseurs.

Les implications et équivalences sont utilisées souvent à mauvais escient.