

correction du partiel

1. 1. Montrons que (\mathbf{R}, \star) est un groupe.

- Pour tout $x \in \mathbf{R}$, on a $x \star 0 = (x^5 + 0^5)^{\frac{1}{5}} = x$ et $0 \star x = (0^5 + x^5)^{\frac{1}{5}} = x$. Donc 0 est l'élément neutre pour la loi \star .
- Pour tout $x, y \in \mathbf{R}$, on a $(x^5 + y^5)^{\frac{1}{5}} \in \mathbf{R}$. La loi \star est donc une loi interne.
- Pour tout $x \in \mathbf{R}$, on a $(x^5 + (-x)^5)^{\frac{1}{5}} = 0$ et $((-x)^5 + x^5)^{\frac{1}{5}} = 0$. Donc tout $x \in \mathbf{R}$ est inversible pour la loi \star , d'inverse $-x$.
- Pour tout x, y et $z \in \mathbf{R}$, on a :

$$(x \star y) \star z = (((x^5 + y^5)^{\frac{1}{5}})^5 + z^5)^{\frac{1}{5}} = (x^5 + y^5 + z^5)^{\frac{1}{5}} = (x^5 + ((y^5 + z^5)^{\frac{1}{5}})^5)^{\frac{1}{5}} = x \star (y \star z)$$

Ainsi la loi \star est associative.

(\mathbf{R}, \star) est donc un groupe.

2. On considère l'application suivante :

$$f: (\mathbf{R}, \star) \rightarrow (\mathbf{R}, +)$$

$$x \mapsto x^5$$

Soient $x, y \in \mathbf{R}$.

On a $f(x \star y) = ((x^5 + y^5)^{\frac{1}{5}})^5 = x^5 + y^5 = f(x) + f(y)$, donc f est un morphisme de groupe.

De plus f est clairement une application bijective.

(En effet pour tout $y \in \mathbf{R}$, on a $y = f(y^{\frac{1}{5}})$, donc f est surjective. Et $\text{Ker}(f) = \{x \in \mathbf{R} \mid x^5 = 0\} = \{0\}$).

Donc f est un isomorphisme et (\mathbf{R}, \star) et $(\mathbf{R}, +)$ sont alors isomorphes.

2. 1. Puisque $a^3 = b^2 = e$, tout élément de G admet un représentant de la forme $b^\epsilon a^{k_1} b a^{k_2} b \dots a^{k_n} b^\delta$ avec $k_i \in \{1, 2\}$ et $\epsilon, \delta \in \{0, 1\}$. Mais on sait que $ab = b^{-1}a^{-1} = ba^2$ donc on peut toujours trouver un représentant de la forme $b^\epsilon a^k$ avec $k \in \{1, 2\}$, et $\epsilon \in \{0, 1\}$.

On peut alors conjecturer que G est le groupe diédral D_3 .

2. On considère donc le morphisme $f: F_2 \rightarrow D_3$ surjectif défini par $f(a) = r$ et $f(b) = s$ où a et b sont les générateurs de F_2 , et r et s une rotation et une symétrie qui engendrent D_3 . On remarque que $f(a^3) = r^3 = id$, $f(b^2) = s^2$ et $f(abab) = rsrs = id$ (car rs est une symétrie). Donc $\langle a^3, b^2, abab \rangle$ est inclus dans le noyau de f . On peut donc factoriser le morphisme f par ce sous-groupe, ce qui nous donne un morphisme surjectif $\bar{f}: G \rightarrow D_3$. De plus $|G| = 6 = |D_3|$.

Donc \bar{f} est un isomorphisme, soit $G \cong D_3$.

3. 1. Pour $n = 2$, S_n contient deux éléments et est donc commutatif. Donc $Z(S_2) = S_2$.

On considère maintenant le cas $n \geq 3$.

Soit σ dans le centre de S_n . On notera $\sigma = c_1 c_2 \dots c_k$ sa décomposition en cycles disjoints.

Supposons que $k \geq 2$. On va noter $c_1 = (a_1 a_2 \dots a_u)$ et $c_2 = (b_1 b_2 \dots b_v)$. On considère maintenant la transposition $\tau = (a_1 b_1)$.

$$\tau \sigma \tau^{-1} = (b_1 a_2 \dots a_u)(a_1 b_2 \dots b_v) c_3 \dots c_k$$

Ainsi $\tau \sigma \tau^{-1} \neq \sigma$ et $\sigma \notin S_n$. Ceci est une contradiction. Donc $k \in \{0, 1\}$.

Supposons maintenant que $k = 1$, soit $\sigma = c_1 = (a_1 a_2 \dots a_u)$.

Si $u \geq 3$ alors $(a_1 a_2)(a_1 a_2 \dots a_u)(a_1 a_2)^{-1} = (a_2 a_1 \dots a_u) \neq \sigma$. Contradiction.

Si $u = 2$, $\sigma = (a_1 a_2)$ et pour $d \neq a_1, a_2$ (d existe car $n \geq 3$) on a $(a_1 d)(a_1 a_2)(a_1 d)^{-1} = (d a_2)$. Contradiction.

On en déduit donc que $k = 0$ soit $\sigma = id$. Donc pour $n \geq 3$, $Z(S_n) = id$.

2. Pour la seconde partie de l'exercice 3, il est possible de procéder de la même manière en conjuguant par des trois cycles et non plus par des transpositions. Il existe une autre manière de répondre à la question posée.

Il suffit de remarquer que le centre de A_n est un sous-groupe distingué de A_n . Donc pour $n \geq 5$, $Z(A_n) = A_n$ où $Z(A_n) = \{id\}$. Mais il est clair que pour $n \geq 5$, A_n n'est pas commutatif. Donc $Z(A_n) = \{id\}$.

Pour $n = 1, 2$, $A_n = \{id\}$, donc $Z(A_1) = Z(A_2) = \{id\}$.

Pour $n = 3$, A_3 est de cardinal 3 et est donc commutatif (parce qu'il est cyclique). Donc $Z(A_3) = A_3$.

Pour $n = 4$, les seuls sous-groupes distingués sont A_4 , $\{id\}$ et $V = \{id, (12)(34), (13)(24), (14)(23)\}$. Or $(12)(34)$ n'est pas dans le centre de A_4 puisque $(123)(12)(34)(132) = (14)(23)$. Donc $Z(A_4) = \{id\}$.

4. 1. Soit $h \in H$ on a clairement $hHh^{-1} = H$ donc $H \subset N(H)$ et en particulier $N(H)$ est non vide.
 Soient $g, g' \in N(H)$. Puisque $gHg^{-1} = H$, on a $g^{-1}Hg = H$ et donc $g^{-1} \in N(H)$. De plus $(gg')H(gg')^{-1} = g(g'Hg'^{-1})g^{-1} = gHg^{-1} = H$
 Ainsi $N(H)$ est un groupe contenant H .
 Soient $h \in H$ et $g \in N(H)$. On a $ghg^{-1} \in gHg^{-1}$ mais $gHg^{-1} = H$ donc $ghg^{-1} \in H$. H est donc distingué dans $N(H)$.
 2. H est distingué dans K donc pour $k \in K$ on a $kHk^{-1} = H$ et alors $k \in N(H)$. Ainsi $K \subset N(H)$.
 De plus K et $N(H)$ sont des sous-groupes de G donc K est un sous-groupe de $N(H)$.
 Et puisque tout sous-groupe de G contenant H dans lequel H est distingué est inclus dans $N(H)$ et que $N(H)$ est un tel sous-groupe, $N(H)$ est le plus grand de ces sous-groupes.
 3. Soient $h, h' \in H$ et $k, k' \in K$. $(hk)(h'k')^{-1} = hkk'^{-1}h'^{-1}$. Comme $K \subset N(H)$, on a $kk'^{-1} \in N(H)$ soit $kk'^{-1}Hk'k^{-1} = H$. Ainsi il existe $h'' \in H$ tel que $kk'^{-1}h'^{-1}k'k^{-1} = h''$. Donc $(hk)(h'k')^{-1} = hh''kk'^{-1} \in HK$.
 De plus HK est non vide donc HK un sous-groupe de G .
 On sait que $H \in N(H)$ et $K \in N(H)$ donc $HK \in N(H)$ et H est distingué dans HK .
 4. Question du TD.

5. 1. Soit $a \in \mathbf{Z}$.

$$\begin{aligned}
 \bar{a} \text{ inversible dans } \mathbf{Z}/n\mathbf{Z} &\Leftrightarrow \text{il existe } \bar{b} \in \mathbf{Z}/n\mathbf{Z} \text{ tel que } \bar{a}\bar{b} = \bar{1} \\
 &\Leftrightarrow \text{il existe } k \in \mathbf{Z} \text{ tel que } ab + kn = 1 \\
 &\Leftrightarrow \text{pgcd}(a, n) = 1 \\
 &\Leftrightarrow \bar{a} \text{ est un generateur de } \mathbf{Z}/n\mathbf{Z}
 \end{aligned}$$

2. Soit $\Phi \in \text{Aut}(\mathbf{Z}/n\mathbf{Z})$. On sait que Φ est totalement défini par l'image d'un générateur de l'ensemble de départ $\mathbf{Z}/n\mathbf{Z}$. Ici on regardera l'image de 1. De plus pour que Φ soit surjectif (et donc bijectif) il faut que $\Phi(1)$ soit un générateur de $\mathbf{Z}/n\mathbf{Z}$. Cela provient de $\Phi(\mathbf{Z}/n\mathbf{Z}) = \Phi(\langle 1 \rangle) = \langle \Phi(1) \rangle$. De plus, d'après la question précédente, on sait que les générateurs de $\mathbf{Z}/n\mathbf{Z}$ sont les éléments de $(\mathbf{Z}/n\mathbf{Z})^\times$. Ainsi l'application

$$\begin{aligned}
 \Psi : \text{Aut}(\mathbf{Z}/n\mathbf{Z}) &\rightarrow (\mathbf{Z}/n\mathbf{Z})^\times \\
 \Phi &\mapsto \Phi(1)
 \end{aligned}$$

est bien définie. Il nous suffit donc de montrer que cette application est bien un isomorphisme. Tout d'abord, pour $\Phi_1, \Phi_2 \in \text{Aut}(\mathbf{Z}/n\mathbf{Z})$, on a $\Psi(\Phi_1 \circ \Phi_2) = \Phi_1 \circ \Phi_2(1) = \Phi_1(\Phi_2(1)) = \Phi_2(1)\Phi_1(1) = \Psi(\Phi_1\Psi(\Phi_2))$. Ψ est donc un morphisme. De plus $\text{Kerf} = \{\Phi \in \text{Aut}(\mathbf{Z}/n\mathbf{Z}) \mid \Phi(1) = 1\} = \{Id\}$, ce qui nous donne l'injectivité de Ψ . Et pour tout $a \in \mathbf{Z}/n\mathbf{Z}$, il existe bien un automorphisme de $\mathbf{Z}/n\mathbf{Z}$ qui envoie 1 sur a , ce qui nous donne la surjectivité de Ψ .

Ψ est donc un automorphisme.