Devoir libre $n^{\circ}1$

à rendre le 19/09/2022

Exercice

1. Soit $P(X) = a_n X^n + a_{n-1}X^{n-1} + ... + a_0$ un polynôme scindé de degré n, et $x_1, x_2, ..., x_n$ ses racines distincts ou non.
Montrer que $\displaystyle\sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n}$ et $\displaystyle\prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}$.

2. Pour tout $n \in \mathbb{N}^*$, on pose $w_n = e^{\frac{2i\pi}{n}}$.

2*a*. Pour $k \in \mathbb{Z}$, calculer $A_n(k) = \displaystyle\sum_{p=0}^{n-1} w_n^{kp}$.

2*b*. Calculer $|G_n|^2$ où $G_n = \displaystyle\sum_{p=0}^{n-1} w_n^{p^2}$.

Problème

-I-

Soit p un nombre premier et $a \in \mathbb{Z}/_{p\mathbb{Z}}$. On désigne par T_a l'application de $\mathbb{Z}/_{p\mathbb{Z}}$ dans $\mathbb{Z}/_{p\mathbb{Z}}$ définie par $\forall x \in \mathbb{Z}/_{p\mathbb{Z}}, T_a(x) = x + a$.
On pose $\mathscr{T} = \{ \ T_a \mid a \in \mathbb{Z}/_{p\mathbb{Z}} \ \}$.

1. Vérifier que $\forall (a,b) \in (\mathbb{Z}/_{p\mathbb{Z}})^2, T_a \circ T_b = T_{a+b}$.

2. En déduire que $(\mathscr{T}, \circ)$ est un groupe et que l'application $\varphi : a \mapsto T_a$ est un isomorphisme de groupes.

-II-

Soit $(G, .)$ un groupe fini de cardinal n et p un nombre premier qui divise n. En considère l'ensemble E des applications $f : \mathbb{Z}/_{p\mathbb{Z}} \to G$ telles que :

$$f(0)f(1)...f(p-1) = e$$

où e l'élément neutre de G (G n'est pas nécessairement commutatif). On considère aussi le sous-ensemble E_0 de E constitué des applications constantes de E.

1. Montrer que $E_0 \neq \varnothing$.

2. Soit $f \in E$. Vérifier que $f \circ T_1 \in E$, en déduire que $\forall k \in \mathbb{Z}/_{p\mathbb{Z}}$, $f \circ T_k \in E$.

3. Pour $f \in E$, on définit $H_f = \{ k \in \mathbb{Z}/_{p\mathbb{Z}} \mid f = f \circ T_k \}$.

3*a*. Montrer que H_f est un sous-groupe de $\mathbb{Z}/_{p\mathbb{Z}}$.

3*b*. Montrer que $f \in E_0 \Leftrightarrow H_f = \mathbb{Z}/_{p\mathbb{Z}}$.

3*c*. En déduire que $f \notin E_0 \Leftrightarrow H_f = \{ 0 \}$.

4. On définit sur E la relation binaire $\mathscr{R}$ par :

$$f \mathscr{R} g \Leftrightarrow \exists k \in \mathbb{Z}/_{p\mathbb{Z}} : g = f \circ T_k.$$

4*a*. Vérifier que $\mathscr{R}$ est une relation d'équivalence.

4*b*. Soit $f \in E$, on définit l'application :

$$\begin{array}{rccc} \Psi_f : & \mathbb{Z}/_{p\mathbb{Z}} & \to & [f]_{\mathscr{R}} \\ & k & \mapsto & f \circ T_k \end{array}$$

où $[f]_{\mathscr{R}}$ désigne la classe d'équivalence de f pour la relation $\mathscr{R}$.
Montrer que Ψ_f est surjective et qu'elle est injective si, et seulement si, $f \in E \setminus E_0$.

4*c*. En déduire $\operatorname{card}([f]_{\mathscr{R}}) = \left\{ \begin{array}{ll} 1 & \text{si } f \in E_0 \\ p & \text{si } f \in E \setminus E_0 \end{array} \right.$.

4*d*. En déduire qu'il existe une partition de E de la forme

$$E = E_0 \cup \left(\bigcup_{k=1}^{m} [f_k]_{\mathscr{R}} \right)$$

avec $f_1, f_2, ..., f_m \in E \setminus E_0$.

4*e*. En déduire que $\operatorname{card}(E) = \operatorname{card}(E_0) \bmod p$.

5. Considérons l'application :

$$\begin{array}{rccc} \Phi : & E & \to & G^{p-1} \\ & f & \mapsto & (f(0), f(1), ..., f(p-2)) \end{array}$$

Montrer que Φ est bijective, en déduire que p divise $\operatorname{card}(E)$.

6. D'après ce qui précède, déduire que p divise le nombre d'éléments de l'ensemble $\{ x \in G \mid x^p = e \}$.
En déduire que G contient un sous-groupe de cardinal p.

7. Montrer que si H_1 et H_2 sont deux sous-groupes de G de même cardinal p, alors $H_1 = H_2$ ou $H_1 \cap H_2 = \{e\}$.
En déduire $\lambda_p(G)$, nombre de sous-groupes de G de cardinal p, vérifie $\lambda_p(G) = 1 \bmod p$.

8. Montrer que tout groupe de cardinal 15 est cyclique.

FIN DE L'ÉPREUVE