Devoir libre $n°01$
Correction

*N'hésitez pas de me signaler les erreurs rencontrées.*

•••••••••

## Exercice

**1.** Remarquons d'abord que $a_n \neq 0$ puisque $P$ est de degré $n$. La décomposition en facteurs irréductibles de $P$ s'écrit $P(X) = a_n(X - x_1)(x - x_2)...(X - x_n)$. En développant et en identifiant les coefficients d'ordre $n-1$ et d'ordre $0$, on obtient le résultat annoncé.

**2.** (a) Si $n$ divise $k$, alors $w_n^{kp} = 1$ pour tout $p \in [\![0, n-1]\!]$ et donc $A_n(k) = \sum_{p=0}^{n-1} w_n^{kp} = n$. Si $n$ ne divise pas $k$, alors $\left\{ 1, w_n^k, w_n^{2k}, ..., w_n^{(n-1)k} \right\}$ est exactement l'ensemble de racines du polynôme $X^n - 1$, donc d'après la première question $\sum_{p=0}^{n-1} w_n^{kp} = A_n(k) = 0$ ( le coefficient de $X^{n-1}$ dans le polynôme $X^n - 1$ est nul ).

(b) Calculons $|G_n|^2$ :

$$
\begin{aligned}
|G_n|^2 &= G_n \overline{G_n} && (1)\\
&= \left( \sum_{s=0}^{n-1} w_n^{p^2} \right) \left( \sum_{r=0}^{n-1} w_n^{-q^2} \right) && (2)\\
&= \sum_{0 \leq p,q \leq n-1} w_n^{p^2-q^2} && (3)\\
&= \sum_{0 \leq p,q \leq n-1} w_n^{(p-q)(p+q)} && (4)\\
&= \sum_{p=0}^{n-1} \left( \sum_{p-n<r\leq p} w_n^{r(2p-r)} \right), \text{ avec } r = p - q && (5)
\end{aligned}
$$

Mais

$$
\begin{aligned}
\sum_{p-n<r\leq p} w_n^{r(2p-r)} &= \sum_{r=0}^{p} w_n^{r(2p-r)} + \sum_{r=p-n+1}^{-1} w_n^{r(2p-r)} && (6)\\
&= \sum_{r=0}^{p} w_n^{r(2p-r)} + \sum_{r'=p+1}^{n-1} w_n^{(r'-n)(2p-r'+n)}, \text{ avec } r' = r + n && (7)\\
&= \sum_{r=0}^{p} w_n^{r(2p-r)} + \sum_{r'=p+1}^{n-1} w_n^{r'(2p-r')}, \text{ car } w_n^n = 1 && (8)\\
&= \sum_{r=0}^{n-1} w_n^{r(2p-r)}, \text{ avec } r = r'. && (9)
\end{aligned}
$$

D'où $|G_n|^2 = \sum_{p=0}^{n-1}\left(\sum_{r=0}^{n-1} w_n^{r(2p-r)}\right)$, et c'est ainsi qu'on peut écrire

$$|G_n|^2 = \sum_{p=0}^{n-1}\left(\sum_{r=0}^{n-1} w_n^{r(2p-r)}\right) \tag{10}$$

$$= \sum_{r=0}^{n-1}\left(\sum_{p=0}^{n-1} w_n^{r(2p-r)}\right) = \sum_{r=0}^{n-1} w_n^{-r^2}\left(\sum_{p=0}^{n-1} w_n^{2pr}\right), \tag{11}$$

et enfin $|G_n|^2 = \sum_{r=0}^{n-1} w_n^{-r^2} A_n(2r)$. Mais nous savons que

$$A_n(2r) = \begin{cases} n & \text{si } n \mid 2r \\ 0 & \text{si } n \nmid 2r \end{cases}$$

On discute les deux cas suivants :
• Si $n = 2m$ alors $(n \mid 2r) \Leftrightarrow (m \mid r)$ et comme $0 \leq r < n$ nous avons conclu que cela ne se produit que dans le cas où $r \in \{0, m\}$ et donc

$$|G_n|^2 = \sum_{r=0}^{n-1} w_n^{-r^2} A_n(2r) = w_n^{-0^2} A_n(0) + w_n^{-m^2} A_n(n) = n\left(1 + (-1)^m\right).$$

• Si $n = 2m+1$ alors $(n \mid 2r) \Leftrightarrow (n \mid r)$ et comme $0 \leq r < n$ nous avons conclu que cela ne se produit que dans le cas $r = 0$ et donc

$$|G_n|^2 = \sum_{r=0}^{n-1} w_n^{-r^2} A_n(2r) = w_n^{-0^2} A_n(0) = n.$$

D'où :

$$|G_n|^2 = \begin{cases} n & \text{si } 2 \mid n-1 \\ 2n & \text{si } 4 \mid n \\ 0 & \text{si } 4 \mid n-2 \end{cases}$$

# Problème

## -I-

**1.** La propriété $\forall (a,b) \in (\mathbb{Z}/p\mathbb{Z})^2$, $T_a \circ T_b = T_{a+b}$ traduit l'égalité évidente :

$$\forall (a,b,x) \in (\mathbb{Z}/p\mathbb{Z})^3, \;\; a + (b+x) = (a+b) + x.$$

**2.** D'après ce qui précède l'ensemble $\mathscr{T} = \{ T_a \mid a \in \mathbb{Z}/p\mathbb{Z} \}$ est stable par la loi de composition des applications ( $\circ$ ), on remarque que $I$, l'application identique, est dans $\mathscr{T}$, de plus l'inverse de $T_a$ est $T_{-a}$ qui est aussi un élément de $\mathscr{T}$. D'où $(\mathscr{T}, \circ)$ est un groupe.
On peut vérifier directement que l'application $a \mapsto T_a$ est un morphisme de groupe bijectif.

## -II-

**1.** Il est clair que l'application

$$\begin{array}{rccc} 1: & (\mathbb{Z}/p\mathbb{Z},+) & \to & (G,.) \\ & a & \mapsto & e \end{array}$$

est un élément de $E_0$, donc $E_0 \neq \varnothing$.

**2.** Soit $f \in E$, donc $f(0)f(1)...f(p-1) = e$ et alors

$$\begin{aligned} f(1)...f(p-1)f(0) &= (f(0))^{-1}f(0)f(1)...f(p-1)f(0) && (12)\\ &= (f(0))^{-1}ef(0) = e && (13)\end{aligned}$$

Donc $f \circ T_1(0)f \circ T_1(1)...f \circ T_1(p-1) = e$, d'où $f \circ T_1 \in E$.
Sachant que $(f \circ T_k) \circ T_1 = f \circ T_{k+1}$, on en déduit directement et progressivement que $\forall k \in \mathbb{Z}/p\mathbb{Z}$, $f \circ T_k \in E$.

**3.** (a) Il est clair que $0 \in H_f$.
Soient $k$ et $r$ dans $H_f$, donc $f = f \circ T_k$ et $f = f \circ T_r$, d'où $f \circ T_{-r} = f \circ T_r \circ T_{-r}$ ou encore $f = f \circ T_{-r}$. De l'autre égalité, on déduit $f = f \circ T_{-r} \circ T_k = f \circ T_{k-r}$. Donc $k - r \in H_f$ et par conséquent $H_f$ est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$.
Ainsi, $H_f = \mathbb{Z}/p\mathbb{Z}$ ou $H_f = \{0\}$ puisque $p$ est un nombre premier [1]( $\mathbb{Z}/p\mathbb{Z}$ et $\{0\}$ ce sont les seuls sous-groupe de $\mathbb{Z}/p\mathbb{Z}$. )

(b)

$$\begin{aligned} (H_f = \mathbb{Z}/p\mathbb{Z}) &\Rightarrow (\forall k \in \mathbb{Z}/p\mathbb{Z},\ f = f \circ T_k) && (14)\\ &\Rightarrow (\forall k \in \mathbb{Z}/p\mathbb{Z},\ f(0) = f \circ T_k(0)) && (15)\\ &\Rightarrow (\forall k \in \mathbb{Z}/p\mathbb{Z},\ f(k) = f(0)) && (16)\\ &\Rightarrow (f \in E_0) && (17)\end{aligned}$$

L'autre sens est très clair.

(c) En fait, nous concluons de ce que nous avons démontré précédemment que $f \notin E_0 \Leftrightarrow H_f \neq \mathbb{Z}/p\mathbb{Z}$ et comme $p$ est un nombre premier, on en déduit que $H_f \neq \mathbb{Z}/p\mathbb{Z}$ est équivalent à $H_f = \{0\}$, d'où

$$f \notin E_0 \Leftrightarrow H_f = \{0\}.$$

**4.** (a) Montrons que $\mathscr{R}$ est une relation d'équivalence.
• Il est clair que $f = f \circ T_0$, donc $\forall f \in E$, $f\mathscr{R}f$.
• Si $g = f \circ T_k$, alors $f = g \circ T_{-k}$, d'où $\forall (f,g) \in E^2$, $f\mathscr{R}g \Rightarrow g\mathscr{R}f$.

1.

**Théorème de Lagrange :** Soit $(G,.)$ un groupe fini et $H$ un sous-groupe de $G$. Alors le cardinal de $H$ divise le cardinal de $G$.

**Preuve :** Notons $k$ le cardinal de $H$. Soit $x \in G$ et soit $A_x = \{\ xh \mid h \in H\ \}$. Montrons que $\text{card}(A_x) = \text{card}(H)$ : soient $h_1$ et $h_2$ deux éléments distincts de $H$. Si $xh_1 = xh_2$, alors comme on est dans un groupe on peut en déduire $h_1 = h_2$, ce qui est faux. Donc $xh_1 \neq xh_2$. Ainsi les $k$ éléments $xh$ pour $h$ variant dans $H$ sont deux à deux distincts et donc $A_x$ contient $k$ éléments : $\text{card}(A_x) = \text{card}(H)$.
Montrons maintenant que si $x$ et $y$ sont dans $G$, alors $A_x = A_y$ ou $A_x$ et $A_y$ sont disjoints. Soient donc $x$ et $y$ dans $G$. Supposons que $A_x$ et $A_y$ ne sont pas disjoints. Il existe donc un élément commun à ces deux ensembles. On a donc $h_1$ et $h_2$ dans $H$ tels que $xh_1 = yh_2$. Donc $x = yh_2h_1^{-1}$.
Considérons un élément quelconque de $A_x$. Il est de la forme $xh$ avec $h \in H$. Or $xh = yh_2h_1^{-1}h$. Comme $H$ est un sous-groupe de $G$, $h_2h_1^{-1}h \in H$ et donc $yh_2h_1^{-1}h \in A_y$. On a ainsi démontré que $xh \in A_y$ pour tout $h \in H$. Donc $A_x \subset A_y$. On montre de la même manière que $A_y \subset A_x$. Ainsi, si $A_x$ et $A_y$ ne sont pas disjoints, alors $A_x = A_y$.
Remarquons avant de conclure que puisque $e \in H$, $xe = x \in A_x$. Ainsi tout élément de $G$ est dans l'un des ensembles $A_x$.
Nous pouvons désormais conclure : tout élément de $G$ est dans une certaine partie $A_x$ de G. Chacune de ces parties est de cardinal $k$. Et ces différentes parties sont deux à deux disjointes. On en déduit que $G$ se découpe en un certain nombre de parties $A_x$ toutes de même cardinal $k$. Donc $k$ divise $n$.

• Si $g = f \circ T_k$ et $h = g \circ T_r$, alors $h = f \circ T_{r+k}$, d'où

$$\forall (f, g, h) \in E^3, \ \ (f \mathscr{R} g) \ \text{ et } \ (g \mathscr{R} h) \Rightarrow f \mathscr{R} h.$$

Et cela prouve que $\mathscr{R}$ est une relation d'équivalence sur $E$.

(b) Soit $f \in E$ et définissons l'application

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

• Soit $g \in [f]_{\mathscr{R}}$, donc $f \mathscr{R} g$ et par conséquent il existe $k \in \mathbb{Z}/p\mathbb{Z}$ tel que $g = f \circ T_k$, c'est-à-dire $\Psi_f(k) = g$. Donc $\Psi_f$ est surjective.
• Remarquons que

$$\begin{aligned} (\Psi_f(k) = \Psi_f(l)) &\Leftrightarrow (f = f \circ T_{k-l}) && (18) \\ &\Leftrightarrow k - l \in H_f && (19) \end{aligned}$$

et en conséquence, d'après le résultat de la question 3., si $f \in E \setminus E_0$, $H_f = \{0\}$ et dans ce cas $(\Psi_f(k) = \Psi_f(l)) \Rightarrow k = l$ et l'application $\Psi_f$ est injective dans ce cas.
Si $f \in E_0$, alors $f$ est constant et dans ce cas $\Psi_f$ ne peut pas être injective.

(c) Soit $f$ de $E$. Discutons les deux cas suivants :
• Si $f \in E_0$, alors $[f]_{\mathscr{R}} = \{f\}$ et donc $\text{card}\,([f]_{\mathscr{R}}) = 1$.
• Si $f \in E \setminus E_0$, alors $\Psi_f$ définie une bijection de $\mathbb{Z}/p\mathbb{Z}$ vers $[f]_{\mathscr{R}}$ et nous en concluons que $\text{card}\,([f]_{\mathscr{R}}) = \text{card}\,(\mathbb{Z}/p\mathbb{Z})) = p$.

(d) Notons $E/\mathscr{R}$ l'ensemble de classes d'équivalence pour la relation d'équivalence $\mathscr{R}$. Soit $\{A_1, A_2, ..., A_m\}$ l'ensemble des classes d'équivalence contenus dans $E \setminus E_0$, c'est-à-dire :

$$\{A_1, A_2, ..., A_m\} = \{\, A \in E/\mathscr{R} \mid A \subset E \setminus E_0 \,\}.$$

Il est clair que les ensembles $E_0, A_1, A_2, ..., A_m$ sont deux à deux disjoints et non vides.
Soit $f \in E$, si $f \notin E_0$ alors $[f]_{\mathscr{R}} \cap E_0 = \varnothing$, car la classe d'équivalence d'un élément de $E_0$ est réduit à un seul élément ( si $f \in E_0$, $[f]_{\mathscr{R}} = \{f\}$ ). D'où $[f]_{\mathscr{R}} \subset E \setminus E_0$, donc il existe $k \in [\![1, m]\!]$ vérifie $[f]_{\mathscr{R}} = A_k$ et par conséquent la famille $E_0, A_1, A_2, ..., A_m$ forme une partition de $E$. Si nous choisissons un représentant $f_k$ de chaque $A_k$, nous aurons trouvé $f_1, f_2, ..., f_m$ de $E \setminus E_0$ tels que :

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

(e) D'après la question précédente $\text{card}(E) = \text{card}(E_0) + mp$ et donc $\text{card}(E) \equiv \text{card}(E_0)\ [p]$.

**5.** Il est clair que $\Phi$ est une bijection et que sa bijection réciproque est donnée par :

$$\begin{array}{rccc} \Phi^{-1} : & G^{p-1} & \to & E \\ & a = (a_0, a_1, ..., a_{p-2}) & \mapsto & f_a \end{array}$$

où $f_a$ est définie par $f_a(k) = a_k$ si $0 \leq k \leq p-2$ et $f_a(p-1) = (a_0 a_1 ... a_{p-2})^{-1}$. Donc nécessairement $\text{card}(E) = \text{card}(G^{p-1}) = (\text{card}(G))^{p-1}$ et comme $p$ divise $\text{card}(G)$, alors $p$ divise $\text{card}(E)$.

**6.** Soit l'application :

$$\begin{array}{rccc} \Gamma : & E_0 & \to & \{\, x \in G \mid x^p = e \,\} \\ & f & \mapsto & f(0) \end{array}$$

Il est clair que $\Gamma$ est bijective, donc

$$\text{card}(E_0) = \text{card}\,(\{\, x \in G \mid x^p = e \,\})$$

et comme $\text{card}(E) \equiv \text{card}(E_0)\ [p] \equiv 0\ [p]$ alors $\text{card}\left(\{\ x \in G \mid x^p = e\ \}\right) \equiv 0\ [p]$, de plus $e \in \{\ x \in G \mid x^p = e\ \}$, donc $\text{card}\left(\{\ x \in G \mid x^p = e\ \}\right) > 1$. De ces deux propriétés en déduit que $\text{card}\left(\{\ x \in G \mid x^p = e\ \}\right) \geq p$. En conclusion, il existe nécessairement un élément $x \neq e$ et $x^p = e$, et dans ce cas le sous-groupe engendré par $x$ serait de cardinal $p$.

**7.** Puisque $G$ est finie, alors le nombre de sous-groupes de cardinal $p$ est fini. Soit $\lambda_G$ ce nombre que nous abrégerons en $\lambda$. Notons $H_1, H_2, ..., H_\lambda$ tous les sous-groupes de cardinal $p$ et posons $\overline{H}_k = H_k \setminus \{e\}$ pour $1 \leq k \leq \lambda$. On a les propriétés suivantes :
• $l \neq k \Rightarrow \overline{H}_k \cap \overline{H}_l = \varnothing$, en effet, si $x \in \overline{H}_k \cap \overline{H}_l$ et différent de $e$, alors son ordre divise $p$ puisque $(x) \subset H_l$, donc nécessairement $H_k = (x) = H_l$ et donc $k = l$.
• $\text{card}\left(\overline{H}_k\right) = p - 1$ et ceci pour tout $1 \leq k \leq \lambda$.
• Enfin $\{\ x \in G \mid x^p = e\ \} = \{e\} \cup \left(\bigcup_{k=1}^{\lambda} \overline{H_k}\right)$.
D'où :

$$\text{card}\left(\{\ x \in G \mid x^p = e\ \}\right) = 1 + \lambda(p-1) = 1 - \lambda + p\lambda$$

et comme $p$ divise $\text{card}\left(\{\ x \in G \mid x^p = e\ \}\right)$, alors $p$ divise $\lambda - 1$ ou encore $\lambda_p(G) \equiv 1\ [p]$

**8.** D'après l'étude précédente $\lambda_5(G) \equiv 1\ [5]$.
Si $\lambda_5(G) > 1$, alors $\lambda_5(G) \geq 6$ et donc $\text{card}\left(\{\ x \in G \mid x^p = e\ \}\right) = 1 + \lambda_5(G)(5-1) \geq 1 + 6 \times 4 = 25$ ce qui est absurde ( $G$ contient 15 élément ).
Donc $\lambda_5(G) = 1$, soit donc $H$ l'unique sous-groupe de $G$ de cardinal 5. D'après ce qui précède $H = \left\{\ x \in G \;\middle|\; x^5 = e\ \right\}$.
On sait que l'ordre de tout élément de $G$ divise 15, supposons que $G$ ne contient aucun élément d'ordre 15. Comme les éléments de $H$ sont d'ordre 1 ou 5, alors les éléments de $G \setminus H$ sont d'ordre 3 et donc

$$\left\{\ x \in G \;\middle|\; x^3 = e\ \right\} = \{1\} \cup (G \setminus H)$$

et par conséquent

$$\text{card}\left(\left\{\ x \in G \;\middle|\; x^3 = e\ \right\}\right) = 1 + 10 = 11$$

Ceci est absurde puisque 3 ne divise pas 11. Donc, en conclusion, il existe dans $G$ un élément $a$ d'ordre 15 et donc $G = (a)$, en particulier $G$ est cyclique.

●●●●●●●●●●