Polynômes

Généralités

Autocorrection A.
Soit $P = X^3 - X^2 + 3X - 1$ et $Q = 2X^2 - X + 1$. Calculer PQ, P^2, Q^2, $P \circ Q$ et $Q \circ P$.

Autocorrection B.
Soit $n \geqslant 1$. Donner rapidement le degré, le coefficient dominant et le coefficient constant de

$$(X+1)^n + (X-1)^n \qquad \text{et} \qquad (X+1)^n - (X-1)^n.$$

Exercice 1.
Déterminer tous les polynômes $P \in K[X]$ tels que

(i) $P(2X) = P(X) - 1$;
(ii) $P(X^2) = (X^2+1)P$;
(iii) $P \circ P = P$;
(iv) $\exists Q \in K[X] : Q^2 = XP^2$.

Exercice 2.
On considère la suite de polynômes $(P_n)_{n\in\mathbb{N}}$ définie par

$$P_0 = 1, \qquad P_1 = (-2X) \qquad \text{et} \qquad \forall n \in \mathbb{N}, P_{n+2} = -2XP_{n+1} - 2(n+1)P_n.$$

1. Calculer P_2, P_3 et P_4.
2. Déterminer, pour tout $n \in \mathbb{N}$, le degré et le coefficient dominant de P_n.
3. Montrer que les polynômes constituant la suite $(P_n)_{n\in\mathbb{N}}$ sont alternativement pairs et impairs (en tant que fonctions polynomiales).
4. Déterminer, pour tout $n \in \mathbb{N}$, $P_{2n+1}(0)$.
5. Déterminer, pour tout $n \in \mathbb{N}$, $P_{2n}(0)$.

Exercice 3.

1. Soit $P \in K[X]$.
   Montrer qu'il existe un unique couple $(R_0, R_1) \in K[X]^2$ tel que $P = R_0(X^2) + X\,R_1(X^2)$.
2. Soit $P, Q \in K[X]$ tels que $P(X)^2 = Q(X^2)$.
   Montrer qu'il existe $R \in K[X]$ tel que $P = R(X^2)$ ou $P = X\,R(X^2)$.

Exercice 4$^+$.

1. Si $p \in \mathbb{N}^*$, que vaut $S_p = \sum_{z\in\mu_n(\mathbb{C})} z^p$?
2. Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{C}[X]$ de degré $d \geqslant 1$. Montrer $\exists z \in S^1 : |P(z)| \geqslant \max_{i=0}^{d} |a_i|$.

Exercice 5$^+$.
Soit $n \in \mathbb{N}$ et $P, Q \in \mathbb{R}[X]$ deux polynômes différents de degré n. Montrer que

$$\deg\left(P^3 - Q^3\right) \geqslant 2n.$$

Le résultat reste-t-il vrai si $P, Q \in \mathbb{C}[X]$?

Exercice 6$^+$.
Soit $P \in K[X]$. Montrer qu'il existe $Q \in K[X]$ tel que $P(P(X)) - X = Q(X)\big(P(X) - X\big)$.

Exercice 7.
Alice et Bob jouent ensemble : Bob pense à un polynôme P à coefficients dans $\mathbb{N}$ et Alice doit le deviner. À chaque tour, Alice choisit un entier $k \in \mathbb{Z}$ et Bob lui donne la valeur de $P(k)$. En combien de tours Alice (qui sait dès le début que les coefficients de P sont dans $\mathbb{N}$, mais n'a pas plus d'information sur ce polynôme ou son degré) peut-elle deviner P ?

Exercice 8$^+$. *X*
Montrer que tout entier relatif s'écrit de façon unique sous la forme $P(-2)$, où P est un polynôme à coefficients dans $\{0, 1\}$.

Exercice 9$^+$.
Soit K un corps et A un sous-anneau de K. On note $A[X]$ l'ensemble des éléments de $K[X]$ dont les coefficients appartiennent à A.

Montrer que $A[X]$ est un sous-anneau intègre de $K[X]$, et déterminer $A[X]^\times$.

Formule de convolution de Vandermonde

Exercice 10$^+$ (Formule de convolution de Vandermonde).
Soit $n \in \mathbb{N}$.

1. Soit $p, q \in \mathbb{N}$. En calculant de deux façons différentes le produit $(1+X)^p(1+X)^q$, montrer la *formule de convolution de Vandermonde* :
$$\sum_{k=0}^{n} \binom{p}{k}\binom{q}{n-k} = \binom{p+q}{n}.$$
2. En déduire la valeur de $\displaystyle\sum_{k=0}^{n} \binom{n}{k}^2$.

Exercice 11^{++}.
Soit $n \geqslant 1$. Montrer

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \left(\binom{n}{k} - \binom{n}{k-1}\right)^2 = \frac{1}{n+1}\binom{2n}{n}.$$

Exercice 12^{++}.
Soit $n \in \mathbb{N}^*$.

1. Montrer *l'identité de De Moivre* (1756) : $\displaystyle\sum_{k=0}^{n} k\binom{2n}{n+k} = n\binom{2n-1}{n}$.
2. En déduire les valeurs de $\displaystyle\sum_{0\leqslant k,\ell\leqslant n} \max(k,\ell)\binom{n}{k}\binom{n}{\ell}$ et $\displaystyle\sum_{0\leqslant k,\ell\leqslant n} \min(k,\ell)\binom{n}{k}\binom{n}{\ell}$.

Racines

Autocorrection C.
Déterminer tous les polynômes tels que $\forall k \in \mathbb{N}, P(k) = k^3$.

Exercice 13.
Montrer que tout polynôme de degré impair à coefficients réels possède (au moins) une racine réelle.

Exercice 14.
Soit $P \in \mathbb{Q}[X]$ tel que $P(\sqrt{2}) = 0$. Montrer que $P(-\sqrt{2}) = 0$.

Exercice 15.

1. Montrer que tout polynôme $P \in \mathbb{C}[X]$ tel que $P(X+1) = P(X)$ est constant.
2. Résoudre l'équation $P(X+1) - P(X) = X$, d'inconnue $P \in \mathbb{C}[X]$.

Exercice 16.
Soit $P \in \mathbb{C}[X]$ tel qu'il existe une infinité de réels α tels que $P(\alpha) \in \mathbb{R}$. Montrer que $P \in \mathbb{R}[X]$.

Exercice 17.
Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que $\forall x, y \in \mathbb{R}, P(xy) = P(x)\,P(y)$.

Exercice 18.
Déterminer tous les polynômes $P \in \mathbb{C}[X]$ tels que $(X+1)\,P(X) = X\,P(X+2)$.

Exercice 19$^+$.
Soit $P \in \mathbb{C}[X]$ un polynôme non nul tel que $P(X^2) = P(X)\,P(X-1)$.

1. Montrer que si $a \in \mathbb{C}$ est racine de P alors a^2 et $(a+1)^2$ sont aussi racines de P.
2. Montrer que toutes les racines de P appartiennent à $\{j, j^2\}$.

Exercice 20 (Polynômes de Čebyšëv de première espèce).

1. Soit $n \in \mathbb{N}$. Montrer qu'il existe un unique $T_n \in \mathbb{R}[X]$ tel que $\forall \theta \in \mathbb{R}, \cos(n\,\theta) = T_n(\cos\theta)$.
2. Montrer $\forall n \in \mathbb{N}, T_{n+2} = 2X\,T_{n+1} - T_n$.
3. Pour tout $n \in \mathbb{N}$, déterminer :
   - le degré et le coefficient dominant de T_n ;
   - les racines de T_n, d'abord dans $[-1, 1]$, puis dans $\mathbb{C}$.

Exercice 21$^+$.
Soit $P, Q, R \in \mathbb{R}[X]$ tels que $Q \circ P = R \circ P$.

1. Montrer que si P n'est pas constant, alors $Q = R$.
2. Montrer que l'on ne peut pas étendre la question précédente à tous les polynômes P.

Exercice 22.

1. Déterminer les polynômes $P \in \mathbb{R}[X]$ tels que $\forall x \in [0, 1], |P(x)| = 1$.
2. Même question pour les polynômes $P \in \mathbb{C}[X]$.

Exercice 23^{++}.
Déterminer les polynômes $P \in \mathbb{C}[X]$ vérifiant $\forall z \in \mathbb{U}, P(z) \in \mathbb{U}$.

Rigidité des fonctions polynomiales

Exercice 24.
Déterminer tous les polynômes $P \in \mathbb{R}[X]$ tels que $\forall n \in \mathbb{N}, P(n) = n^2 + (-1)^n$.

Exercice 25.

1. Montrer que la fonction exp : $\mathbb{R} \to \mathbb{R}$ n'est pas polynomiale.
2. Montrer que la fonction $c : \begin{cases} \mathbb{C} \to \mathbb{C} \\ z \mapsto \overline{z} \end{cases}$ n'est pas polynomiale.
3. (a) Montrer que cos : $\mathbb{R} \to \mathbb{R}$ n'est pas une fonction polynomiale.
   (b) Montrer que $\cos_{|\pi\mathbb{Z}}$ n'est pas une fonction polynomiale.
   (c) Montrer que $\cos_{|[0,2\pi]}$ n'est pas une fonction polynomiale.
   (d) Existe-t-il un ensemble infini $E \subseteq \mathbb{R}$ tel que $\cos_{|E}$ soit une fonction polynomiale ?

Exercice 26.
Montrer qu'il n'existe pas de polynôme $P \in \mathbb{R}[X]$ tel que

$$\exists A > 0 : \forall x \geqslant A, P(x) = \ln(x).$$

Exercice 27$^+$. ☑
Montrer qu'il n'existe pas de polynôme $P \in \mathbb{R}[X]$ tel que pour tout $k \in \mathbb{N}^*$,

(i) $P(k) = \dfrac{1}{k}$; (ii) $P(k) = \sqrt{k^2+1}$; (iii) $P(k) = 2^k$.

Exercice 28.
Soit $P, Q \in \mathbb{R}[X]$ deux polynômes différents. Montrer que

$$(\exists A \in \mathbb{R} : \forall t \geqslant A, P(t) < Q(t)) \quad \text{ou} \quad (\exists A \in \mathbb{R} : \forall t \geqslant A, P(t) > Q(t)).$$

Localisation des racines

Exercice 29$^+$ (Borne de Cauchy). ☑
Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme unitaire. On note $Z(P)$ l'ensemble des racines complexes de P.

1. Montrer $\forall \zeta \in Z(P), |\zeta|^n \leqslant \sum_{k=0}^{n-1} |a_k|\,|\zeta|^k$ et en déduire $\forall \zeta \in Z(P) \setminus \{0\}, |\zeta| \leqslant \sum_{\ell=0}^{n-1} \dfrac{|a_{n-1-\ell}|}{|\zeta|^\ell}$.
2. Utiliser la question précédente pour montrer

$$\forall \zeta \in Z(P), |\zeta| \leqslant \max\left(1, \sum_{k=0}^{n-1} |a_k|\right).$$

3. En réutilisant le résultat de la première question, montrer la *borne de Cauchy*

$$\forall \zeta \in Z(P), |\zeta| \leqslant 1 + \max(|a_0|, \ldots, |a_{n-1}|).$$

Exercice 30^{+} (Théorème d'Eneström-Kakeya). X

Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{R}[X]$ tel que $\forall i \in [\![0, n-1]\!]$, $a_i > 0$.

1. On suppose $a_0 \geqslant a_1 \geqslant \cdots \geqslant a_n$. Montrer que toutes les racines de P sont de module $\geqslant 1$.
2. Montrer qu'en général, les racines de P sont toutes dans la couronne

$$C(r, R) = \{z \in \mathbb{C} \,|\, r \leqslant |z| \leqslant R\},$$

où r (resp. R) est le minimum (resp. maximum) des $\left(\frac{a_k}{a_{k+1}}\right)_{k=0}^{n-1}$.

Exercice 31^{++} (Disques de Geršgorin).

Pour tous $\omega \in \mathbb{C}$ et $R > 0$, on note $D(\omega, R) = \{z \in \mathbb{C} \,|\, |z - \omega| \leqslant R\}$ le disque de centre ω et de rayon R.

1. Soit $M \in M_n(\mathbb{C})$ et $\lambda \in \mathbb{C}$. Pour tout $i \in [\![1, n]\!]$, on note $R_i = \sum_{j \in [\![1,n]\!] \setminus \{i\}} |a_{i,j}|$. Montrer

$$\lambda \notin \bigcup_{i=1}^{n} D\left([M]_{i,i}, R_i\right) \Rightarrow M - \lambda I_n \in GL_n(\mathbb{C}).$$

2. Soit $P = X^n + \sum_{k=0}^{n-1} a_k X^k \in \mathbb{C}[X]$ un polynôme unitaire. On définit la *matrice compagnon*

$$C(P) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} \in M_n(\mathbb{C})$$

Montrer que $\{\lambda \in \mathbb{C} \,|\, C(P) - \lambda I_n \notin GL_n(\mathbb{C})\}$ est l'ensemble des racines de P.

3. Déduire de ce qui précède que toute racine z de $P = X^n + \sum_{k=0}^{n-1} a_k X^k$ appartient à l'union

$$D(-a_{n-1}, 1) \cup D\left(0, \max_{0 \leqslant k \leqslant n-2} |a_k|\right).$$

Division euclidienne

Autocorrection D. ☑

Soit $P \in K[X]$ et $a, b \in K$ deux scalaires différents. Déterminer le reste dans la division euclidienne de P par $(X - a)(X - b)$ en fonction de a, b, $P(a)$ et $P(b)$.

Exercice 32. ☑

Soit $n \in \mathbb{N}$. Déterminer le reste de la division euclidienne de A par B dans les cas suivants :

(i) $A = X^n$ et $B = X^2 - 3X + 2$;

(ii) $A = X^n$ et $B = (X - 1)^2$;

(iii) $A = (X \sin t + \cos t)^n$ et $B = X^2 + 1$, où t est un réel.

Exercice 33.
Déterminer le reste de la division euclidienne de $X^{42} + X^{1729} + X^{11\,111}$ par $1 + X + X^2$.

Exercice 34. ☑
Trouver les racines complexes des polynômes suivants.

- $P_1 = X^3 + (i-3)X^2 + (7-2i)X - 5(1+i)$, en sachant qu'il a une racine imaginaire pure ;
- $P_2 = X^4 + 4iX^2 + 12(1+i)X - 45$, en sachant qu'il a une racine réelle et une imaginaire pure.

Exercice 35. ☑
Soit $A = \begin{pmatrix} 3/2 & 1/2 \\ -1/2 & 1/2 \end{pmatrix} \in M_2(\mathbb{R})$.

1. Calculer $(A - I_2)^2$.
2. Déterminer le reste dans la division euclidienne de X^{100} par $(X-1)^2$.
3. En déduire A^{100}.

Exercice 36.
Soit $f : x \mapsto \dfrac{x^3}{x^2 + 2x + 3}$. Déterminer les points entiers de son graphe, c'est-à-dire $\mathbb{Z}^2 \cap \mathrm{gr}(f)$.

Exercice 37. ☑
Soit L/K une extension de corps et $A, B \in K[X]$ deux polynômes tels que $\exists Q \in L[X] : A = QB$.

Montrer $\exists Q \in K[X] : A = QB$.

Exercice 38.
Soit A et B deux polynômes à coefficients dans $\mathbb{Z}$. On suppose B unitaire. Montrer l'existence et l'unicité d'un couple (Q, R) de polynômes à coefficients entiers tels que $A = BQ + R$ et $\deg R < \deg B$.

Dérivation

Autocorrection E. ☑
Soit $k \in \mathbb{N}$. On définit une suite de polynômes $(P_n)_{n\in\mathbb{N}}$ par

$$P_0 = X^k \qquad \text{et} \qquad \forall n \in \mathbb{N}, P_{n+1} = XP_n'.$$

Donner une expression simple pour la suite $(P_n)_{n\in\mathbb{N}}$.

Exercice 39.
Trouver une partie $H \subseteq K[X]$ telle que la dérivation $\begin{cases} H \to K[X] \\ P \mapsto P' \end{cases}$ soit une bijection.

Exercice 40.
Soit $P \in K[X]$. Donner un sens à la somme $\displaystyle\sum_{k=0}^{+\infty} \frac{(-1)^k}{(k+1)!} P^{(k)}(X)\, X^{k+1}$ et montrer qu'elle définit la « primitive » de P possédant 0 comme racine.

Exercice 41.
Déterminer tous les polynômes $P \in K[X]$ tels que

(i) $P = P'$; (ii) $(P')^2 = 4P$.

Exercice 42.
Déterminer les $P \in K[X]$ tels que $P(2X) = P'(X)P''(X)$.

Exercice 43.
Déterminer les polynômes $P \in K[X]$ tels que $X(X+1)P'' + (X+2)P' - P = 0$.

Exercice 44.
Soit $n \in \mathbb{N}^*$. Existe-t-il un polynôme $P \in \mathbb{R}[X]$ de degré n tel que $\forall k \in [\![0, n-1]\!], P^{(k)}(0) = P^{(k)}(1)$?

Exercice 45$^+$.
Trouver tous les couples $(A, B) \in K[X]^2$ tels que $AB' - BA' = 1$.

Exercice 46.
Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que $\forall k \in \mathbb{Z}, \int_k^{k+1} P(t)\,dt = k+1$.

Exercice 47.
On note $\mathcal{H} = \left\{ P \in \mathbb{R}[X] \;\middle|\; \forall x \in \mathbb{R}, P(x) = \frac{1}{2}\int_{x-1}^{x+1} P(t)\,dt \right\}$.

1. Déterminer $\mathcal{H} \cap \mathbb{R}_1[X]$, puis $\mathcal{H} \cap \mathbb{R}_2[X]$.
2. Montrer que $\mathcal{H}$ est stable par dérivation, c'est-à-dire $\forall P \in \mathcal{H}, P' \in \mathcal{H}$.
3. Que vaut $\mathcal{H}$?

Exercice 48.
Soit $(A_n)_{n\in\mathbb{N}^*}$ la suite de polynômes définie par

$$A_1 = X^2 + X \qquad \text{et} \qquad \forall n \in \mathbb{N}^*, A_{n+1} = (X^2+1)A_n + XA_n'.$$

1. Pour tout $n \in \mathbb{N}^*$, donner le degré et le terme dominant de A_n.
2. Pour tout $n \in \mathbb{N}^*$, déterminer $A_n(0)$.
3. En déduire qu'il existe une unique suite $(B_n)_{n\in\mathbb{N}^*}$ de polynômes telle que $\forall n \in \mathbb{N}^*, A_n = XB_n$.
4. Calculer B_1 et obtenir une relation de récurrence sur la suite $(B_n)_{n\in\mathbb{N}}$.
5. Pour tout $n \in \mathbb{N}^*$, calculer $B_n(0)$ et en déduire $A_n'(0)$.

Exercice 49.
Montrer que la fonction tan est lisse et qu'il existe une suite $(P_n)_{n\in\mathbb{N}}$ de polynômes à coefficients dans $\mathbb{N}$ telle que pour tout $n \in \mathbb{N}$, $\deg P_n = n+1$ et $\tan^{(n)} = P_n(\tan)$.

Exercice 50.

1. Montrer qu'il existe une unique suite de polynômes réels $(H_n)_{n\in\mathbb{N}}$ telle que, pour tout $n \in \mathbb{N}$, la fonction $g : x \mapsto e^{-x^2}$ soit n fois dérivable, de dérivée n-ième $g^{(n)} : x \mapsto H_n(x)\,e^{-x^2}$.
2. Soit $n \in \mathbb{N}$. Déterminer le degré, le terme dominant, et la parité de H_n.
3. Montrer $\forall n \in \mathbb{N}, H_{n+1}' = -2(n+1)H_n$.
4. En déduire une expression de la suite $(g^{(n)}(0))_{n\in\mathbb{N}}$.

Exercice 51.
Soit $P \in \mathbb{R}[X]$. Montrer que l'on peut trouver $A \in \mathbb{R}$ tel que la fonction polynomiale

$$\begin{cases} [A, +\infty[& \to & \mathbb{R} \\ t & \mapsto & P(t) \end{cases}$$

soit monotone.

Exercice 52.
Soit $P \in \mathbb{R}[X]$ tel que P induise une application surjective $\mathbb{N} \to \mathbb{N}$. Montrer que $P = X$.

Exercice 53.
Soit $P \in \mathbb{R}[X]$ et $a \in \mathbb{R}$ tels que $P(a) > 0$ et, pour tout $k \in \mathbb{N}^*$, $P^{(k)}(a) \geqslant 0$.

Montrer que P ne possède pas de racines dans $[a, +\infty[$.

Interpolation de Lagrange

Autocorrection F.
Soit $z_0, \dots, z_n \in K$ tous distincts.

On note, pour tout $k \in [\![0, n]\!]$, L_k l'unique polynôme de degré n tel que $\forall j \in [\![0, n]\!], L_k(x_j) = \delta_{k,j}$.

Identifier les polynômes $\displaystyle\sum_{k=0}^{n} L_k$ et $\displaystyle\sum_{k=0}^{n} x_k L_k$.

Exercice 54.
Montrer $\forall n \in \mathbb{N}, \exists \lambda_0, \dots, \lambda_n \in \mathbb{R} : \forall P \in \mathbb{R}_n[X], \displaystyle\int_0^1 P(t)\,dt = \sum_{k=0}^{n} \lambda_k P\left(\frac{k}{n}\right)$.

Exercice 55.
Soit $P \in \mathbb{R}_n[X]$ tel que $\forall k \in [\![0, n]\!], P(k) = \dfrac{k}{k+1}$.

1. Déterminer le polynôme $Q = (X+1)P - X$.
2. En déduire $P(n+1)$.

Exercice 56$^+$.
Soit $r \in \mathbb{R}$. Soit $P \in \mathbb{R}_{n-1}[X]$ tel que $\forall k \in [\![1, n]\!], P(k) = r^k$. Calculer $P(n+1)$.

Exercice 57$^+$.
Soit $P \in \mathbb{R}_n[X]$ tel que $\forall k \in [\![1, n+1]\!], P(k) = \dfrac{1}{k}$. Calculer $P(0)$.

Exercice 58.
Soit L/K une extension de corps infinis. Soit $P \in L[X]$ tel que $\forall z \in K, P(z) \in K$. Montrer $P \in K[X]$.

Exercice 59$^+$.
Soit L/K une extension de corps finis. On note $q = |K|$.

Soit $P \in L[X]$. Montrer que les deux assertions suivantes sont équivalentes.

(i) $\forall z \in K, P(z) \in K$;

(ii) $\exists (Q, R) \in L[X] \times K[X] : P = (X^q - X)Q + R$;

Exercice 60.

À quelle condition sur le corps K la fonction $\iota : \begin{cases} K \to & K \\ x \mapsto & \begin{cases} x^{-1} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases} \end{cases}$ est-elle polynomiale ?

Un peu d'algèbre et d'arithmétique

Exercice 61.

Soit $P \in \mathbb{Z}[X]$ tel que $P(0)$ et $P(1)$ soient impairs. Montrer que P ne possède pas de racine entière.

Exercice 62. ☑

Soit $P \in \mathbb{Z}[X]$ tel que, pour tout $n \in \mathbb{Z}$, le nombre entier $P(n)$ soit premier. Montrer que P est constant.

Exercice 63$^+$.

Dans tout l'exercice, on fixe un corps K et un sous-groupe fini G du groupe multiplicatif $K^\times$.

Notons $n = |G|$.

Le but de l'exercice est notamment de montrer que G est cyclique.

0. **Exemple.** Montrer que le groupe multiplicatif $\mathbb{F}_7^\times$ est cyclique et déterminer ses générateurs.
1. **Lemme.** Soit $s \in \mathbb{N}^*$. Montrer qu'il existe au plus s éléments de $K^\times$ dont l'ordre divise s.
2. On note $\mathcal{S}_G$ l'ensemble des ordres des éléments de G et $D(n)$ l'ensemble des diviseurs positifs de l'entier n. Rappeler pourquoi $\mathcal{S}_G \subseteq D(n)$.
3. Soit $s \in \mathcal{S}_G$. On fixe un élément x_s de G d'ordre s.
   (a) Montrer que le sous-groupe $\langle x_s \rangle$ possède $\varphi(s)$ générateurs.
   (b) Soit $g \in G$. Montrer que si l'ordre de g divise s, alors $g \in \langle x_s \rangle$.
   (c) Montrer que les générateurs de $\langle x_s \rangle$ sont exactement les éléments de G d'ordre s.
   (d) Déduire de ce qui précède $n = \sum_{s \in \mathcal{S}_G} \varphi(s)$.
   (e) En appliquant la formule précédente à une situation bien choisie, montrer $n = \sum_{s \in D(n)} \varphi(s)$.
4. Montrer que G est cyclique.

Exercice 64^{++}.

Soit $P \in \mathbb{Z}[X]$. Pour tout $n \in \mathbb{N}^*$, on dit que P *admet une racine modulo* n si $\exists x \in \mathbb{Z} : P(x) \equiv 0 \pmod{n}$.

Montrer qu'il existe une infinité de nombres premiers modulo lesquels P admet une racine.

Exercice 65^{++}.

Déterminer les polynômes de $\mathbb{C}[X]$ induisant une surjection $\mathbb{Q} \to \mathbb{Q}$.