Chapitre 2

Polynômes

Pour le contenu du chapitre "Polynômes", on peut de reporter au chapitre 10 du Cours de mathématiques – Algèbre 1re année de F. Liret et D. Martinais (éditions Dunod). Il y a ausi une liste de résultats dans l'Appendice II du livre Algèbre Linéaire de J. Grifone (éditions Cepadues).

2.1 Généralités

Un polynôme à une variable sur un corps $\mathbb{K}$ (nous serons essentiellement intéressés par les cas où $\mathbb{K}$ est $\mathbb{R}$ ou $\mathbb{C}$) est une expression

$$a_0 + a_1X + \cdots + a_nX^n \ ,$$

où les a_i sont des éléments de $\mathbb{K}$ (les *coefficients* du polynôme). Formellement, on peut définir un polynôme comme la suite infinie $(a_0, a_1, \ldots, a_n, \ldots)$ de ses coefficients, tous nuls à partir d'un certain rang. Par exemple, le polynôme $1 + 2X^2 - X^3$ est codé par la suite $(1, 0, 2, -1, 0, 0, \ldots)$.

On note $\mathbb{K}[X]$ l'ensemble des polynômes sur $\mathbb{K}$. Il est muni des deux opérations de l'addition et de la multiplication, qui en font un anneau commutatif, comme $\mathbb{Z}$.

On identifie un élément a de $\mathbb{K}$ au polynôme constant (codé $(a, 0, 0, \ldots)$). La multiplication par les éléments de $\mathbb{K}$ munit alors $\mathbb{K}[X]$ d'une structure d'espace vectoriel sur $\mathbb{K}$.

Soit P un polynôme non nul. Le *degré* de P est le plus grand entier n tel que le coefficient a_n de X^n dans P soit non nul. Ce coefficient a_n s'appelle alors le *coefficent dominant* de P, et on dit que P est *unitaire* si son coefficient dominant est 1. Par convention on peut décréter que le degré du polynôme nul est $-\infty$. On a

$$\deg(P+Q) \le \max(\deg(P), \deg(Q)) \quad (\text{égalité si } \deg(P) \neq \deg(Q)) \qquad \deg(PQ) = \deg(P) + \deg(Q) \ .$$

Soit $c \in \mathbb{K}$ et $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme sur $\mathbb{K}$. On pose $P(c) = a_0 + a_1c + \cdots + a_nc^n$. On dit que c est *racine* de P quand $P(c) = 0$. L'application $c \mapsto P(c)$ de $\mathbb{K}$ dans lui-même est la *fonction polynôme* associée au polynôme P.

On peut *substituer* un polynôme Q à la variable X dans un autre polynôme P pour obtenir un nouveau polynôme $P(Q)$ (noté aussi $P \circ Q$ chez Liret-Martinais) : si $P = a_0 + a_1X + \cdots + a_nX^n$, alors $P(Q) = a_0 + a_1Q + \cdots + a_nQ^n$. On a $P_1(Q) + P_2(Q) = (P_1 + P_2)(Q)$ et $P_1(Q) \times P_2(Q) = (P_1P_2)(Q)$.

On dit qu'un polynôme B *divise* un polynôme A s'il existe un polynôme Q tel que $A = BQ$. Noter que le fait qu'à la fois B divise A et A divise B équivaut au fait qu'il existe une constante $c \neq 0$ telle que $A = cB$. Noter aussi que si B divise A et $\deg(A) < \deg(B)$, alors $A = 0$.

Exercice 2.1

Montrer que, si les trois polynômes P, Q, R de $\mathbb{R}[X]$ vérifient la relation

$$P^2(X) - XQ^2(X) = XR^2(X) \ ,$$

ils sont nuls. Est-ce encore vrai dans $\mathbb{C}[X]$?

Exercice 2.2

Montrer que, pour tout polynôme de $\mathbb{K}[X]$, $P(X) - X$ divise $P\big(P(X)\big) - X$.

Exercice 2.3

Soit $a \in \mathbb{K}$. Montrer que $P(X) = X(X+a)(X+2a)(X+3a) + a^4$ est un carré dans $\mathbb{K}[X]$. En déduire une décomposition de $Q(X) = X(X+1)(X+2)(X+3) - 8$ en produit dans $\mathbb{R}[X]$.

2.2 Division euclidienne, pgcd de deux polynômes

Un point important qui fait que l'anneau des polynômes à une variable sur un corps $\mathbb{K}$ est très semblable à $\mathbb{Z}$ est l'existence d'une division euclidienne.

Théorème 2.1 *Soient A et B deux polynômes de $\mathbb{K}[X]$, avec B différent du polynôme nul. Alors il existe des polynômes Q (quotient) et R (reste) tels que*

$$A = BQ + R \quad \text{avec } \deg R < \deg B \text{ ou } R = 0\ .$$

De plus, le couple (Q, R) vérifiant ces propriétés est unique.

Proposition 2.2 *Le reste de la division euclidienne de P par $X - c$ est $P(c)$. En conséquence, un élément $c \in \mathbb{K}$ est racine de P si et seulement si P est divisible par $X - c$.*

Définition 2.3 *Si A et B sont deux polynômes de $\mathbb{K}[X]$, on dit que* le polynôme D est un plus grand commun diviseur (en abrégé, pgcd) de A et B *quand*

1. *D est un diviseur commun de A et B,*
2. *tout diviseur commun de A et B divise D.*

Autrement dit, l'ensemble des diviseurs de D est égal à celui des diviseurs communs de A et B.

Ceci ne définit pas le pgcd de manière unique, mais à un facteur constant non nul près. L'existence du pgcd est établie, comme pour les entiers, par l'algorithme d'Euclide. Soient A et B deux polynômes. On pose

$$R_0 = A \qquad R_1 = B$$

et, pour $n \geq 1$, tant que R_n est non nul, on définit R_{n+1} comme le reste de la division euclidienne de R_{n-1} par R_n :

$$R_{n-1} = R_n Q_n + R_{n+1} \quad \text{avec } \deg(R_{n+1}) < \deg(R_n) \text{ ou } R_{n+1} = 0\ .$$

Comme la suite $\deg R_1,\ \deg R_2, \ldots$ est strictement décroissante, l'algorithme s'arrête au bout d'un nombre fini N d'étapes avec $R_{N+1} = 0$.

Théorème 2.4 *Le polynôme R_N obtenu à la fin de l'algorithme (c'est le dernier reste non nul, si A et B sont différents de 0) est un pgcd de A et B.*

Si A et B sont tous les deux nuls, $\mathrm{pgcd}(A, B) = 0$. Sinon, un pgcd est un polynôme de degré maximal parmi ceux qui divisent à la fois A et B ; on peut rendre le pgcd unique en demandant qu'il soit unitaire (c'est souvent comme cela que le pgcd est défini, par exemple chez Liret-Martinais).

Comme pour les entiers, on a :

Théorème 2.5 *Soient A et B deux polynômes, D un pgcd de A et B. Il existe des polynômes U et V tels que $D = UA + VB$.*

Définition 2.6 *Deux polynômes A et B sont dits* premiers entre eux *quand 1 est pgcd de A et B, autrement dit si et seulement si les seuls diviseurs communs de A et B sont les constantes non nulles.*

Théorème 2.7 (Identité de Bezout) *Deux polynômes A et B sont premiers entre eux si et seulement s'il existe des polynômes U et V tels que $UA + VB = 1$.*

Corollaire 2.8 *Soit A un polynôme premier avec chacun des polynômes $B_1, \ldots, B_r$. Alors A est premier avec le produit $B_1 \cdots B_r$.*

Théorème 2.9 (Lemme de Gauss) *Soient A, B et C des polynômes tels que A et B soient premiers entre eux et que A divise le produit BC. Alors A divise C.*

Définition 2.10 *Un polynôme M est un* plus petit commun multiple *(ppcm) de deux polynômes A et B si et seulement si*

1. *M est un multiple commun de A et B,*

2. tout multiple commun de A et B est multiple de M.

Si A ou B est nul, le ppcm de A et B est 0. Si A et B sont tous les deux non nuls, et si D est un pgcd de A et B, alors AB/D est un ppcm de A et B.

Théorème 2.11 *Soient $A_1, \ldots, A_r$ des polynômes premiers entre eux deux à deux (A_i premier avec A_j si $i \neq j$). Si chaque A_i divise B, alors la produit $A_1 \cdots A_r$ divise B.*

Dans les exercices on dira “le pgcd” ou “le ppcm”, et on notera $\mathrm{pgcd}(A, B)$ ou $\mathrm{ppcm}(A, B)$ pour le pgcd ou le ppcm unitaire.

Exercice 2.4

Effectuer les divisions euclidiennes de

$$\begin{aligned} 2X^5 - 5X^3 - 8X \quad & \text{par} \quad X + 3 \,, \\ 4X^3 + X^2 \quad & \text{par} \quad X + 1 + i \,, \\ X^5 - 2X^4 + 3X^3 - 4X^2 + 5X - 5 \quad & \text{par} \quad X^2 + X + 1 \,. \end{aligned}$$

En déduire $\mathrm{pgcd}(X^5 - 2X^4 + 3X^3 - 4X^2 + 5X - 5, X^2 + X + 1)$.

Exercice 2.5

Calculer le reste de la division dans $\mathbb{R}[X]$ de

1. $(\cos a + X \sin a)^n$ par $X^2 + 1$,
2. $(X - 1)^m + X^m - 1$ par $X^2 - X + 1$ selon la valeur de m modulo 6.

Exercice 2.6

Soit $P(X) \in \mathbb{R}[X]$ et a et b deux nombres réels distincts. Calculer le reste $R(X)$ de la division de $P(X)$ par $(X - a)(X - b)$ en fonction de $P(a)$ et $P(b)$.

Exercice 2.7

Soit $P(X) = 3X^3 + 2X^2 + 2$ et $Q(X) = X^2 - 2$.

1. Utiliser l’algorithme d’Euclide pour déterminer le pgcd D de P et Q.
2. En déduire deux polynômes U et V tels que $UP + VQ = D$.

Exercice 2.8

Examen de janvier 1997

On note $\mathbb{R}[X]$ l’ensemble des polynômes à coefficients réels et $\deg P$ le degré d’un polynôme P de $\mathbb{R}[X]$. Soit $A(X) = X^3 + 2X^2 - X - 2$ et $B(X) = X^3 - 3X - 2$.

1. Calculer D le pgcd unitaire de A et B.
2. Trouver deux polynômes U_0 et V_0 de $\mathbb{R}[X]$ vérifiant $AU_0 + BV_0 = D$ avec $\deg U_0 < \deg B$ et $\deg V_0 < \deg A$.
3. Trouver le ppcm unitaire de A et B.

Exercice 2.9

On considère les polynômes $A(X) = X^5 - X^4 + 2X^3 + 1$ et $B(X) = X^5 + X^4 + 2X^2 - 1$. Déterminer leur pgcd D et écrire D sous la forme $AU + BV$.

Exercice 2.10

Soient a et b deux entiers strictement positifs. Quel est le pgcd de $X^a - 1$ et $X^b - 1$?

Exercice 2.11

Soit $D = \mathrm{pgcd}(A, B)$ (où A et B ne sont pas nuls tous les deux), et soit (U, V) tels que $AU + BV = D$. Quel est le pgcd de U et V ?

Exercice 2.12

Soient $A(X) = (X-1)^2$ et $B(X) = (X+1)^2$.

1. Calculer le pgcd unitaire D de A et B.
2. Trouver deux polynômes U et V de $\mathbb{R}[X]$ tels que $UA + VB = D$.
3. Déduire une décomposition en éléments simples de $\dfrac{1}{(X^2-1)^2}$.

Exercice 2.13

Soit P et Q dans $\mathbb{K}[X]$ deux polynômes premiers entre eux. Montrer que, si m et n sont des entiers strictement positifs, P^m est premier avec Q^n.

Exercice 2.14

Trouver un polynôme P unitaire de degré ≤ 3, divisible par $X-1$ et tel que les restes dans la division de P par $X-2, X-3$ et $X-4$ soient égaux.

2.3 Décomposition en facteurs irréductibles

Définition 2.12 *Un polynôme $P \in \mathbb{K}[X]$ est dit* irréductible *si ce n'est pas une constante et si ses seuls diviseurs sont les constantes non nulles et les polynômes de la forme cP où c est une constante non nulle (autrement dit, $\deg(P) > 0$ et il n'y a pas de factorisation $P = Q_1Q_2$ avec $\deg(Q_1) < \deg(P)$ et $\deg(Q_2) < \deg(P)$).*

Un polynôme du premier degré est toujours irréductible. Soit P un polynôme irréductible. Si P ne divise pas le polynôme A, alors P est premier avec A. Si Q est un autre polynôme irréductible, alors ou bien il existe une constante non nulle c telle que $Q = cP$, ou bien P et Q sont premiers entre eux.

Les polynômes irréductibles jouent le rôle des nombres premiers.

Théorème 2.13 *Soit A un polynôme non constant de $\mathbb{K}[X]$. Alors il existe une décomposition*

$$A = cP_1^{\alpha_1} \cdots P_k^{\alpha_k}$$

où c est une constante non nulle, $P_1, \ldots, P_k$ sont des polynômes irréductibles unitaires distincts de $\mathbb{K}[X]$, et $\alpha_1, \ldots, \alpha_k$ des entiers strictement positifs. De plus, une telle décomposition est unique, à l'ordre des facteurs irréductibles près.

L'identification des polynômes irréductibles sur $\mathbb{C}$ et $\mathbb{R}$ repose sur le fameux

Théorème 2.14 (D'Alembert - Gauss) *Tout polynôme non constant de $\mathbb{C}[X]$ a une racine dans $\mathbb{C}$.*

La démonstration de ce théorème sort du cadre du cours. On en déduit :

Théorème 2.15 *Sur $\mathbb{C}$, les polynômes irréductibles unitaires sont les $X - c$ avec $c \in \mathbb{C}$. Sur $\mathbb{R}$, les polynômes irréductibles unitaires sont les $X - c$ avec $c \in \mathbb{R}$ et les $X^2 + bX + c$ sans racine réelle (c.-à-d. avec $b^2 - 4c < 0$).*

Rappelons que, si c est un nombre complexe, $(X-c)(X-\overline{c}) = X^2 - 2\,\mathrm{Re}(c)X + |c|^2 \in \mathbb{R}[X]$.

Exercice 2.15

Soit $P(X) = 3X^3 - 2X^2 - 7X - 2$ et $Q(X) = 2X^2 + 3X + 1$.

1. Utiliser l'algorithme d'Euclide pour déterminer le pgcd de P et Q.
2. Donner la décomposition de P en facteurs irréductibles dans $\mathbb{R}[X]$.
3. Quel est le ppcm de P et Q ?

Exercice 2.16

Décomposer dans $\mathbb{R}[X]$ puis dans $\mathbb{C}[X]$ les polynômes suivants en facteurs irréductibles

$$\begin{array}{ccc} X^3+1 & X^3-1 & X^3+2X^2+2X+1 \\ X^4+1 & X^4+X^2+1 & 1+X+X^2+X^3+X^4+X^5 \end{array}$$

Exercice 2.17

Décomposer dans $\mathbb{R}[X]$, puis dans $\mathbb{Q}[X]$ le polynôme $P(X) = X^4 + 1$.

Exercice 2.18

Montrer qu'un polynôme de degré 2 ou 3 est irréductible sur un corps $\mathbb{K}$ si et seulement s'il n'a pas de racine dans $\mathbb{K}$. En est-il de même pour un polynôme de degré 4 ?

Exercice * 2.19

Examen de janvier 1998

Soient m et n deux entiers naturels non nuls.

1. Déterminer le reste de la division euclidienne de $P(X) = X^{2m} + (X+1)^n - 1$ par $X(X+1)$.

Dans toute la suite, on désigne par $A(X)$ un polynôme de degré supérieur ou égal à 1 de $\mathbb{C}[X]$ et on pose $B(X) = [A(X)]^{2m} + (A(X)+1)^n - 1$.

2. Montrer que $[A(X)]^2 + A(X)$ divise $B(X)$.
3. Montrer que, si x_0 est racine de multiplicité 1 de $A(X)$, alors x_0 est racine de multiplicité 1 de $B(X)$.
4. On suppose que $A(X) = X^2 + 1$, $m = 1$, et $n = 3$. Donner la décomposition en produit de facteurs irréductibles du polynôme $B(X)$ dans $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$.
5. On suppose que $A(X) = 1 - X + X^2$, $m = 1$ et $n = 2$.

   Donner la décomposition en produit de facteurs irréductibles du polynôme $B(X)$ dans $\mathbb{R}[X]$, puis dans $\mathbb{C}[X]$.

Exercice 2.20

Montrer que, si $P(x) \geq 0, \forall x \in \mathbb{R}$, alors il existe A et B dans $\mathbb{R}[X]$ tels que $P = A^2 + B^2$.

On pourra montrer que, si $A, B, C, D \in \mathbb{R}[X]$, alors $(A^2 + B^2)(C^2 + D^2)$ est encore une somme de deux carrés dans $\mathbb{R}[X]$.

Décomposer $X^4 + X^2 + 1$ en une somme de deux carrés dans $\mathbb{R}[X]$.

2.4 Racines : multiplicité, relations coefficients-racines

Définition 2.16 *Soit $c \in \mathbb{K}$, P un polynôme non nul de $\mathbb{K}[X]$. On dit que c est* racine de multiplicité k *de P si $(X-c)^k$ divise P et $(X-c)^{k+1}$ ne le divise pas. Autrement dit, $P = (X-c)^k Q$ avec $Q(c) \neq 0$.*

Une racine de multiplicité 1 est dite *simple*, et une racine de multiplicité > 1 *multiple*.

Soit $P = a_0 + a_1 X + \cdots + a_n X^n$. Son *polynôme dérivé* est par définition $P' = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}$. On note $P'', \ldots, P^{(k)}, \ldots$ les polynômes dérivés successifs. Les règles usuelles de dérivation de somme ou de produit s'appliquent.

Pour le résultat suivant, il faut supposer que $\mathbb{K}$ contient $\mathbb{Q}$ (par exemple $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$)

Théorème 2.17 *Soit P un polynôme de $\mathbb{K}[X]$, et c un élément de $\mathbb{K}$. Alors les propriétés suivantes sont équivalentes.*

1. *c est racine de multiplicité k de P.*
2. *$P(c) = P'(c) = \ldots = P^{(k-1)}(c) = 0$ et $P^{(k)}(c) \neq 0$.*

En conséquence, c est racine de multiplicité $\geq k$ de P si et seulement si $P(c) = P'(c) = \ldots = P^{(k-1)}(c) = 0$.

Soient $c_1, \ldots, c_p$ des éléments distincts de $\mathbb{K}$. Si c_i est racine de multiplicité k_i de P, pour $i = 0, \ldots, p$, alors $(X-c_1)^{k_1} \cdots (X-c_p)^{k_p}$ divise P. En conséquence, un polynôme de degré n de $\mathbb{K}[X]$ ne peut pas avoir plus de n racines comptées avec multiplicité dans $\mathbb{K}$.

Un polynôme de degré $n > 0$ est dit *scindé* sur $\mathbb{K}$ s'il a exactement n racines comptées avec multiplicité dans $\mathbb{K}$. Par exemple, le théorème de d'Alembert-Gauss entraîne que tout polynôme non constant est scindé sur $\mathbb{C}$.

Théorème 2.18 *Soit $P = a_0 + \cdots + a_{n-1}X^{n-1} + X^n$ un polynôme unitaire de degré $n > 0$, scindé sur $\mathbb{K}$. Soit $c_1, \ldots, c_n$ ses racines comptées avec multiplicité (une racine de multiplicité k figure k fois). Alors :*

$$\begin{aligned}
-a_{n-1} &= \sum_{1 \le i \le n} c_i \\
a_{n-2} &= \sum_{1 \le i_1 < i_2 \le n} c_{i_1} c_{i_2} \\
&\vdots \\
(-1)^k a_{n-k} &= \sum_{1 \le i_1 < \ldots < i_k \le n} c_{i_1} c_{i_2} \cdots c i_k \\
&\vdots \\
(-1)^n a_0 &= c_1 c_2 \cdots c_n \, .
\end{aligned}$$

Autrement dit, $(-1)^k a_{n-k}$ est la somme des produits k à k des racines. En particulier, a_{n-1} est l'opposé de la somme des racines et $(-1)^n a_0$ est le produit des racines.

Exercice 2.21

Soit P le polynôme de $\mathbb{C}[X]$ donné par $P(X) = 2X^3 + X^2 + X - 1$.

1. Montrer que, si P admet une racine rationnelle écrite sous forme irréductible p/q, alors p divise 1 et q divise 2.
2. En déduire toutes les racines rationnelles de P.
3. Trouver toutes les racines de P.

Exercice 2.22

Soit m, n et p trois entiers naturels. Montrer que $X^2 + X + 1$ divise $X^{3m} + X^{3n+1} + X^{3p+2}$. Factoriser $X^8 + X^4 + X^3$. (On ne demande pas une décomposition en facteurs irréductibles).

Exercice 2.23

On considère le polynôme $P(X) = X^5 - 5X^4 + 7X^3 - 2X^2 + 4X - 8$. Quelle est la multiplicité de 2 en tant que racine de P ?

Exercice 2.24

Trouver (a, b) pour que $(X - 1)^2$ divise $aX^4 + bX^3 + 1$. Généraliser à $aX^{n+1} + bX^n + 1$.

Exercice 2.25

Trouver $P(X)$ dans $\mathbb{K}[X]$ tel que $(X - 1)^3$ divise $P(X) + 1$ et $(X + 1)^3$ divise $P(X) - 1$

1. en utilisant le polynôme dérivé P'.
2. en utilisant l'identité de Bezout.

Exercice 2.26

Trouver un polynôme P de $\mathbb{R}[X]$ de degré inférieur ou égal à 4 tel que

$$\begin{aligned}
X^3 &\quad \text{divise} \quad P(X) + 1 \, , \\
(X - 1)^2 &\quad \text{divise} \quad P(X) \, .
\end{aligned}$$

Donner la décomposition en produits de facteurs irréductibles du polynôme P dans $\mathbb{C}[X]$.

Exercice 2.27

Examen de septembre 1997

On considère le polynôme $P(X) = X^6 - 6X^5 + 15X^4 - 20X^3 + 12X^2 - 4$ et on note P' son polynôme dérivé.

1. Déterminer le pgcd unitaire de P et P'.
2. Donner la décomposition en facteurs irréductibles de P dans $\mathbb{R}[X]$ et dans $\mathbb{C}[X]$.

Exercice 2.28

On considère le polynôme $P(X) = X^4 - 2X^3 + 3X^2 - 2X + 1$ et on note P' son polynôme dérivé.

1. Calculer $D = \text{pgcd}(P, P')$.
   Trouver deux polynômes U et V tels que $D = UP + VP'$.
2. En déduire les racines doubles de P dans $\mathbb{C}[X]$ et ses décompositions en produits de facteurs irréductibles dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Exercice * 2.29

Examen de janvier 1997

Soit $A(X) = X^6 + aX^4 + bX^3 + c$ un polynôme de $\mathbb{C}[X]$.

1. Déterminer a, b et c pour que 1 soit racine double de A et que j soit racine de A.
2. Montrer alors que $A \in \mathbb{R}[X]$ et que j est racine double.
3. Décomposer A en produits de facteurs irréductibles dans $\mathbb{C}[X]$ et $\mathbb{R}[X]$.

Exercice 2.30

Soit $P(X) = 2X^3 - X^2 - 7X + a$.

Déterminer a pour que P ait deux racines de somme 1.

Exercice 2.31

Soit $P(X) = X^5 + 5X^4 + 9X^3 + 11X^2 + 7X + 3$.

1. Calculer $P(j)$ et $P'(j)$. En déduire que P admet une unique racine réelle négative. Calculer cette racine en utilisant un coefficient du polynôme. Vérifier le résultat à l'aide d'un autre coefficient.
2. Donner la décomposition de P en facteurs irréductibles sur $\mathbb{R}[X]$.
3. Quel est le pgcd de P et P' ?

Exercice 2.32

Résoudre, dans $\mathbb{C}^3$, les systèmes symétriques suivants

$$1) \left\{ \begin{array}{rl} x+y+z & = 0 \\ xy+xz+yz & = -13 \\ xyz & = -12 \end{array} \right. , \qquad 2) \left\{ \begin{array}{rl} x+y+z & = -2 \\ x^2+y^2+z^2 & = 0 \\ x^3+y^3+z^3 & = 1 \end{array} \right. .$$

Exercice 2.33

Trouver un polynôme de degré trois dont les racines sont les carrés des racines du polynôme $X^3 + X^2 - 2X - 1$.