Algèbre II : Notes de cours - Partie 2

Hamza El Mahjour

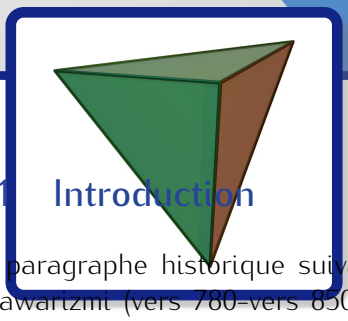
Licence 1 : SMI/SMA/SMPC

Table des matières

Rien n'est beau que le vrai.

— Hermann Minkowski

2. Polynômes



2.1 Introduction

Le paragraphe historique suivant est issu du Chapitre 13 de [1]. Mohammed Al-Khawarizmi (vers 780-vers 850), dans son traité d'algèbre écrit vers 825, classifie les équations du second degré en différents types pour ne considérer que des coefficients positifs. Par exemple : un carré et 21 dirhams sont égaux à dix racines qui correspond à l'équation $x^2 + 21 = 10x$, est une équation du type $x^2 + c = bx$ avec $b, c > 0$ (pour Al-Khawarizmi qui traite de problèmes d'héritage, les nombres sont exprimés en dirhams, l'unité monétaire arabe). " Dans ce cas, précise Al-Khawarizmi, saches que si tu divises en 2 la racine (il faut comprendre : le coefficient b de x), que tu la multiplies par elle-même, et que le produit soit plus petit que les dirhams (il faut comprendre : $\frac{b^2}{4} < c$) alors le problème est impossible". On comprend ce que l'auteur veut dire, mais l'usage de lettres rend les choses plus simples. Le calcul littéral, introduit par François Viète (1540-1603), permet à Descartes, en 1637, dans sa Géométrie, de dégager la esnotion de polynôme et de montrer comment faire la division par $X - a$. Un polynôme à une variable sur un corps $\mathbb{K}$ (où $\mathbb{K} = \mathbb{R}, \mathbb{C}$) est une expression

$$P(X) = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n,$$

où les $a_i \in \mathbb{K}$ nommés les **coefficients** du polynôme. On peut noter $P(X) = \sum_{i=0}^{n} a_i X^i$ et par convention on considère que $X^0 = 1$. Une définition plus formelle existe mais qui ne sera pas introduite ici est celle d'une suite infini composée de ces coefficients et nul à partir d'un certain rang : $(a_0, a_1, \ldots, a_n, 0, 0, 0, \ldots)$. Vu qu'on ne s'intéresse pas à la construction rigoureuse des polynômes mais plutôt leur utilisation, on présentera certaines propriétés et utilisera certains objets sans justifier leurs caractéristiques. Par exemple, l'objet X sera traité comme une variable usuelle qui peut être multiplié par un élément de $\mathbb{K}$ et qui vérifie

$$\underbrace{X \cdot X \cdot \ldots \cdot X}_{n \text{ fois}} = X^n,$$

et aussi

$$X^m \cdot X^n = X^{m+n}.$$

On notera $\mathbb{K}[X]$ l'**ensemble des polynômes à coefficients dans** $\mathbb{K}$.

Deux polynômes $P(X) = \sum_i a_i x^i$ et $P(X) = \sum_i b_i X^i$ sont égaux si et seulement si $a_i = b_i$ pour tout i.

2.2 Structures algébriques des polynômes

Définition 2.1.

1. *Le* ***degré*** *d'un polynôme est le plus grand entier n tel que a_n est non nul. On écrit* $\deg P = n$.
2. *Si* $\deg P = 1$, *on appelle P un polynôme* ***unitaire***.
3. *Par convention, le degré du polynôme nul est* $-\infty$.
4. *Si* $\deg P = 0$ *alors P est un polynôme* ***constant***.

Exemple 2.1.

— *Le polynôme* $1 - 5X^3 + 10X$ *est de degré* 3.
— *Le polynôme* $3X + 1 - 12X^2 + X^4$ *est un polynôme unitaire de degré 4.*
— *Le polynôme* $P(X) = 11$ *est un polynôme constant de degré 0.*

Remarque

Si $\deg P = n$ et a_n est le coefficient multiplié par X^n, alors on appelle a_n **coefficient dominant** du polynôme P.

Définition 2.2.
Soient P et Q deux polynômes de $\mathbb{K}[X]$ avec $P(x) = \sum_{i=0}^{m} X^i$ et $Q(X) = \sum_{i=0}^{n} b_i X^i$. On appelle ***somme*** *des polynômes P et Q (ou addition de P et Q) le polynôme de $\mathbb{K}[X]$, noté $P + Q$ et défini par*

$$(P + Q)(X) = \sum_{i=0}^{\max(m,n)} (a_i + b_i)X^i$$

Exemple 2.2.
$P(X) = 1 + 2X - X^2$ *et* $Q(X) = -2X + X^3$ *alors*

$$(P + Q)(X) = (1 + 0) + (2 - 2)X + (-1 + 0)X^2 + (0 + 1)X^3 = 1 - X^2 + X^3.$$

$\mathbb{K}[X]$ muni de cette loi forme un groupe commutatif. On peut munir aussi les polynômes d'une multiplication entre polynômes pour obtenir finalement une structure d'anneau commutatif ! Mais avant de donner la définition précise d'une multiplication de deux polynômes on travaillera sur un exemple. Soient $A(X) = 1 + 3X - X^2$ et $B(X) = 3 - 2X^2 + 5X^3$. La façon la plus naturelle d'effectuer cette multiplication est d'utiliser la distributivité de la multiplication usuelle par rapport à l'addition. On traitera A et B comme des termes deux expressions algébriques avec l'application de la règle $X^i X^j = X^{i+j}$. Ce qui peut être résumé comme suit

$$(A \cdot B)(X) = (1 + 3X - X^2) \cdot (3 - 2X^2 + 5X^3)$$

$$\begin{aligned}
(AB)(X) &= \underbrace{1 \cdot 3}_{c_0} + \underbrace{(1 \cdot 0 + 3 \cdot 3)}_{c_1} X + \underbrace{(3 \cdot 0 - 1 \cdot 3 + 1 \cdot (-2))}_{c_2} X^2 \\
&\quad + \underbrace{(1 \cdot 5 + 3 \cdot (-2) + (-1) \cdot 0 + 0 \cdot 3)}_{c_3} X^3 + \underbrace{(3 \cdot 5 + (-1) \cdot (-2) + 0 \cdot 5)}_{c_4} X^4 \\
&\quad + \underbrace{((-1) \cdot 5 + 0 \cdot (-2))}_{c_5} X^5, \\
&= 3 + 9X - 5X^2 - X^3 + 17X^4 - 5X^5.
\end{aligned}$$

Nous avons alors la définition suivante

Définition 2.3.
Soit $A(X) = \sum_{i=0}^{m} a_i X^i$ *et* $B(X) = \sum_{i=0}^{n} b_i X^i$ *avec*[1] $m \leq n$. *C'est à dire* $a_{m+1} = a_{m+2} = \ldots = a_(m + (n - m)) = 0$. *On appelle* ***produit*** *de* P *et* Q *le polynôme de* $\mathbb{K}[X]$ *noté* PQ, $P \times Q$ *ou* $P \cdot Q$ *défini par* $PQ(X) = \sum_{k=0}^{m+n} c_k X^k$ *où*

$$c_k = a_0 \cdot b_k + a_1 b_{k-1} + \ldots + a_{n-1} b_1 + a_n b_0$$

Propriétés 2.1

Soit P et Q deux polynômes non nuls de degrés m et n consécutivement.

1. $\deg(P + Q) \leq \max(m, n)$,
2. $\deg(P \cdot Q) = m \cdot n$.

Voici certains exemples qui illustrent pourquoi on a une inégalité dans la première ligne des Propriétés 2.2 et une égalité dans la deuxième.

Exemple 2.3.

1. *Soit* $P(X) = X + 1$, $Q(X) = -3X^2 - X + 5$. *On a* $(P + Q(X) = X^2 + 2$. *Donc* $\deg(P + Q) = 2 = \max(2, 1)$.
2. *Soit* $P(X) = X^4 - 3X^2 + 11$, $Q(X) = -X^4 + 13X^3 + 5$. *On a* $(P + Q(X) = 13X^3 - 3X^2 + 16$. *Donc* $\deg(P + Q) = 3 < \max(4, 4)$.
3. *Soit* $P(X) = 3X^2 - 11X$, $Q(X) = -\frac{1}{3}X^5 + 5$. *Alors* $(P \cdot Q)(X) = -X^7 + 15X^2 + \frac{11}{3}X^6 - 55X$. *Donc* $\deg(P \cdot Q) = \deg P + \deg Q = 4 + 3 = 7$.

2.3 Fonctions polynomiales

Quand on traite X comme une variable réelle, on peut percevoir le polynôme P comme une fonction $P : \mathbb{R} \longrightarrow \mathbb{R}$ où $x \mapsto P(x)$. Cette fonction est continue sur $\mathbb{R}$ c'est à dire que $\lim_{x \to x_0} P(x) = P(x_0)$. Pour obtenir l'image d'un élément a par cette fonction il suffit de remplacer x par la valeur de a. On peut évaluer les éléments d'un polynôme P en un point $X = z$. Cette vision est liée au fait que $x \mapsto P(x)$ définit bien une fonction de $\mathbb{R}$ vers $\mathbb{R}$ (ou de $\mathbb{C}$ dans $\mathbb{C}$). Si z est un scalaire du corps $\mathbb{K}$ alors la valeur de P au point z est

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \dots a_1 z + a_0.$$

Par exemple si $P(X) = 3X^2 + 5X + 1$ alors $P(1) = 3 \cdot 1 + 5 \cdot 1 + 1 = 9$.

Définition 2.4. *On dit que* z_0 *est une racine d'un polynôme* $P \in \mathbb{K}[X]$ *ssi*

$$P(z_0) = 0.$$

De plus $\exists Q \in \mathbb{K}[X]$, $P(X) = (X - z_0) \cdot Q(X)$.

Dans la définition précédente, il se peut que z_0 soit aussi racine du polynôme Q donc il existerait R dans $\mathbb{K}[X]$ tel que $Q(X) = (x - z_0) \cdot R(X)$ ce qui aboutit à $P(X) = (x - z_0)^2 \cdot R(X)$. Si on répète ce processus jusqu'à ce qu'on atteigne m fois avec un polynôme dont z_0 n'est pas une racine alors on dit que z_0 est de multiplicité m. Voici la définition plus formelle.

Définition 2.5.
Soit $z_0 \in \mathbb{K}$ *une racine de d'un polynôme* P *de degré* $n \geq 1$ *et soit* $Q \in \mathbb{K}[X]$ *tel que*

$$P(X) = (X - z_0)^m \cdot Q(X), \qquad (m \leq n)$$

avec $Q(z_0) \neq 0_{\mathbb{K}}$. *On dit que la racine* z_0 *est de* ***multiplicité*** m.

Exemple 2.4.
Les racines du polynôme $P(X) = (X-3)^4 \cdot (X+2i)^8$ *sont* 3 *est* $-2i$. *La racine* 3 *est de multiplicité* 4 *et la racine* $-2i$ *est de multiplicité* 8.

L'écriture d'un polynôme sous la forme $a(X-r_1)^{\alpha_1}(X-r_2)^{\alpha_2}\dots(X-r_k)^{\alpha_k}$ est très utile. C'est ce qu'on appelle un polynôme scindé. Cette écriture est toujours possible dans $\mathbb{C}[X]$ mais pas dans $\mathbb{R}[X]$ grâce au théorème suivant.

Théorème 2.1: Théorème fondamental de l'algèbre

Tout polynôme de $\mathbb{C}[X]$ admet exactement n racines complexes.

Les démonstrations du Théorème 2.3 ne sont pas compliquées, sauf qu'elles reposent sur des notions de topologie ou des notions d'analyse complexe qui dépassent le niveau de ce cours. Un projet précis et concis qui offre quatre démonstrations différentes du théorème peut être consulté sur [2].

Proposition 2.1: Racines *n-ème* de l'unité

Les solutions de l'équation $z^n = 1$ dans $\mathbb{C}$ sont $z_k = e^{i\frac{k}{n}\pi}$ pour $k = 0 \dots n-1$.

Démonstration. Soit $z \in \mathbb{C}$ alors l'écriture exponentielle de z est $re^{i\theta}$. Donc $z^n = 1$ est équivalent à $re^{in\theta} = 1 = 1 \cdot e^{i\cdot 0}$. C'est à dire $r = 1$ et $n\theta \equiv 0[2\pi]$. Ça veut dire $\theta = \frac{2k\pi}{n}$ pour $k \in \{0, 1, \dots, n-1\}$. □

Exemple 2.1

On veut résoudre $z^3 = 1$ dans $\mathbb{C}$. Les solutions sont $z_0 = 1, z_1 = e^{\frac{i\pi}{3}}$ et $z_1 = e^{i\frac{\pi}{3}}$

Dérivée d'un polynôme

Les fonctions polynomiales sont infiniment dérivables. La dérivée de X^n est le polynôme nX^{n-1} (notons que la dérivée d'une constante est 0). Plus généralement on a la définition suivante.

Définition 2.6. *Soit* $P(X) = a_nX^n + a_{n-1}X^{n-1} + \dots + a_1Xa_0$. *La dérivée de* P *est le polynôme* P' *tel que*

$$P'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \dots + 2a_2X + a_1.$$

On notera $P^{(k)}$ la dérivée k-ème de P.

Exemple 2.5.
Par exemple la dérivée du polynôme $X \mapsto -X^{13} + 3X^5 + 2X$ *est le polynôme* $-13X^{12} + 15X^4 + 2$.

Propriétés 2.2

1. La dérivée k-ème de X^n est le polynôme $n(n-1)(n-2)\dots(n-k+1)X^{n-k}$,
2. On a $(P+Q)' = P' + Q'$,
3. $(P \cdot Q)' = P'Q + PQ'$.

Proposition 2.2: Formules de Taylor

Soit P dans $\mathbb{K}[X]$.

1. Si $P(X) = \sum_{i=0}^{n} a_i X^i$ alors pour $k = 0, \dots n$ on a $a_k = \frac{P^{(k)}(0)}{k!}$, autrement dit :
$$\sum_{k \leq n} \frac{P^{(k)}(0)}{k!} X^k.$$
2. On a aussi, si a est un élément de $\mathbb{K}$ on a :
$$P(X+a) = \sum_{k \leq n} \frac{P^(k)(a)}{k!} X^k.$$
3. En général, soit $x_0 \in \mathbb{K}$ et soit P un polynôme de degré n. Alors
$$P(X) = P(x_0) + \frac{P'(x_0)}{1!}(X-x_0) + \frac{P^{(2)}(x_0)}{2!}(X-x_0)^2 + \dots + \frac{P^{(n)}(x_0)}{n!}(X-x_0)^n$$

2.4 Retour sur les nombres entiers !

On revient vers les nombres entiers, car c'est essentiel pour comprendre les mécanismes de l'arithmétique dans $\mathbb{K}[X]$. On dit que $a \in \mathbb{N}$ est divisible par $b \in \mathbb{N}$ s'il existe $q \in \mathbb{N}$ tel que $a = bq$. Par exemple 14 est divisible par 2 car $14 = 2 \times 7$. On dit aussi que 2 divise 14 et on note 2/14. On sait aussi qu'un nombre premier est celui qui n'est divisible que par lui même et par 1, par exemple $2, 3, 5, 7, 11, 13, 17$ sont des nombres premiers. Un résultat aussi connu pour les nombres entiers est

que chaque nombre entier peut être écrit comme produit de facteurs premiers. Par exemple $50 = 2 \cdot 5 \cdot 5$. Il existe aussi, dans le cadre des entiers, la notion du PGCD (Plus Grand Commun Diviseur). Nous allons par la suite présenté des notions connus en artihmétique de $\mathbb{N}$ avec des nouveaux théorèmes, propositions et exemples. Le but de cette partie est d'avoir en tête une idée claire et la transposer vers $\mathbb{K}[X]$.

Définition 2.7 (PGCD de deux entiers)**.**
Soient a et b dans $\mathbb{N}$. On dit que d est le PGCD de a et b si $d|a$, $d|b$ et si tout diviseur commun de a et b divise d.

Définition 2.8 (Algorithme d'Euclide)**.**
Soient a et b dans $\mathbb{Z}$. L'algorithme de calcul du PGCD est donné par Euclide (proposition 2 du livre 7 des Éléments. Euclide fait des soustractions successives et non des divisions). Il est basé sur la remarque suivante. Quand on écrit la division euclidienne de a par b : $a = bq + r$, un diviseur commun à a et b divise $r = a - bq$; d'autre part, un diviseur commun à a et r divise a. On a donc $PGCD(a, b) = PGCD(b, r)$. Soient donc deux entiers a et $b, a > b > 0$. On définit par récurrence une suite d'entiers en posant : $r_0 = a, r_1 = b$, et si $k \geq 1$ et si $r_k \neq 0, r_{k+1}$ est le reste de la division euclidienne de r_{k-1} par r_k : $r_{k-1} = r_k q_k + r_{k+1}$, avec $0 \leq r_{k+1} < r_k$; si $r_k = 0$, on arrête ; on note N ce dernier indice. Le PGCD est donc le dernier reste non nul : $PGCD(a, b) = r_{N-1}$.

Montrons-le sur un exemple.

$a = 2\,652$ et $b = 2\,310$. Les divisions successives donnent :

$$\begin{array}{rcrcr} 2\,652 & = & 2\,310 & + & 342 \\ 2\,310 & = & 342 \times 6 & + & 258 \\ 342 & = & 258 & + & 84 \\ 258 & = & 84 \times 3 & + & 6 \\ 84 & = & 6 \times 14 & + & 0 \end{array}$$

Donc PGCD(2652, 2310) = 6.

Exemple 2.2

On a PGCD(18, 24) = 6. En effet les diviseurs de 18 sont $D_{18} = \{1, 2, 3, 6, 9, 18\}$ et $D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$.

Proposition 2.3: Identité de Bézout

Soient a et b dans $\mathbb{Z}$ et $d = \text{PGCD}(a, b)$. Il existe u et v tels que $ua+vb = d$.

Démonstration. L'idéal (d) est l'idéal engendré par a et b donc contient nécessairement l'ensemble E des éléments de la forme $ma + nb$ avec m et n dans $\mathbb{Z}$, comme E est visiblement un idéal de $\mathbb{Z}$, on a $E = (d)$ donc il existe un entier u et v tels que $ua + vb = d$. □

Définition 2.9.
On dit que deux entiers a et b sont premiers entre eux ssi $PGCD(a, b) = 1$.

Exemple 2.3

1. Les nombres 16 et 14 ne sont pas premiers entre eux car 2/16 et 2/14 donc $\text{PGCD}(14, 16) \geq 2 > 1$.
2. Les nombres 26 et 21 sont premiers entre eux car $\text{PGCD}(26, 21) = 1$.

2.5 Arihtmétique des polynômes

Nous allons essayer de transposer ce qu'on a vu en $\mathbb{N}$ pour

Proposition 2.4

Soient A et B des polynômes de $\mathbb{K}[X]$ avec $B \neq 0$. Il existe un couple unique polynômes Q et R de $\mathbb{K}[X]$ tels que $A = BQ + R$ et $\deg(R) < \deg(B)$.

Démonstration. Pour l'existence et l'unicité d'un tel couple (Q, R), nous référons le lecteur enthousiaste vers la démonstration du Théorème 6.1 du livre [3]. C'est un processus de construction similaire à l'algorithme d'Euclide pour le PGCD de deux nombres entiers. □

Voici un exemple concret des étapes à suivre pour effectuer une division euclidienne.

Exemple 2.4

$$
\begin{array}{rrrr|l}
X^4 & +2X^3 & -X & +6 & X^3-6X^2+X+4 \\
\cline{5-5}
-X^4 & +6X^3 & -X^2-4X & & \underbrace{X+8}_{\text{Quotient}} \\
\cline{1-3}
0 & +8X^3 & -X^2-5X & +6 & \\
 & -8X^3 & +48X^2-8X & -32 & \\
\cline{2-4}
 & & 0 & \underbrace{+47X^2-13X-26}_{\text{Reste}} &
\end{array}
$$

Le processus s'arrête car $\deg(47X^2-13X-26) < \deg(X^3-6X^2+X+4)$. On appelle A le dividende et B le diviseur.

La divisibilité en $\mathbb{K}[X]$ est similaire à ce qui se passe dans $\mathbb{Z}$. En effet, nous avons la même définition

Définition 2.10.
On dit qu'un polynôme A est divisible par B (ou B divise A) s'il existe $Q \in \mathbb{K}[X]$ tel que $B = Q \cdot A$

Exemple 2.5

Le polynôme $x-1$ divise x^2-1 car $x^2-1 = (x-1)\cdot(x+1)$.

Définition 2.11.
Soit P un polynôme de $\mathbb{K}[X]$ tel que $\deg P \geq 1$.
*- Le polynôme P est **irréductible** (ou premier) dans $\mathbb{K}[X]$ s'il admet pour diviseur que les polynômes $\alpha \cdot \mathbb{1}_{\mathbb{K}[X]}$ et αP où $\alpha \in \mathbb{K}^*$. Autrement dit, le polynôme P de $\mathbb{K}[X]$ est irréductible lorsque les seuls polynômes qui le divisent sont, à un facteur multiplicatif près, $\not\vdash_{\mathbb{K}[X]}$ et lui même.*
*- Dans le cas contraire, on dit qu'il est **réductible**.*

Un polynôme peut être irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Proposition 2.5

1. Les seuls polynômes irréductibles dans $\mathbb{R}[X]$ sont de la forme $X+\alpha$ ou bien X^2+pX+q avec $p^2-4c<0$.
2. Les seuls polynômes irréductibles dans $\mathbb{C}[X]$ sont ceux de degré 1 seulement $X+\alpha$.

Définition 2.12.
P.G.C.D de deux polynômes Si A et B sont deux polynômes de $\mathbb{K}[X]$, on dit que le polynôme D est ***un plus grand commun diviseur*** *(ou P.G.C.D) 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.*

Par abus de langage, on peut dire "le" P.G.C.D de deux polynômes "à un facteur constant non-nul près". Pour obtenir le P.G.C.D de deux polynômes, nous allons appliquer l'algorithme d'Euclide qui est expliqué par cette exemple.
Soient $A(X)=X^5-2X^4+X^3-X^2+2X-1$ et $B(X)=X^3-X^2+2X-2$. Effectuons D'abord la division euclidienne de A par B, ceci donne

$$
\begin{array}{rl|l}
X^5 & -2X^4 + X^3 - X^2 + 2X - 1 & X^3 - X^2 + 2X - 2 \\
\hline
-X^5 & + X^4 - 2X^3 + 2X^2 & X^2 - X - 2 \\
\hline
 & - X^4 - X^3 + X^2 + 2X - 1 & \\
 & + X^4 - X^3 + 2X^2 - 2X & \\
\hline
 & -2X^3 + 3X^2 - 1 & \\
 & +2X^3 - 2X^2 + 4X - 4 & \\
\hline
 & X^2 + 4X - 5 &
\end{array}
$$

Maintenant on considère le dividende $A_1(X)=X^3-X^2+2X-2$ et le diviseur $B_1(X)=X^2+4X-5$ qui est le reste de la division euclidienne précédente. On effectue alors la division de A_1 par B_1. On obtient

$$
\begin{array}{rl|l}
X^3 & -X^2+2X-2 & X^2+4X-5 \\
\cline{3-3}
-X^3 & -4X^2+5X & X-5 \\
\cline{1-2}
 & -5X^2+7X-2 & \\
 & +5X^2+20X-25 & \\
\cline{2-2}
 & 27X-27 &
\end{array}
$$

On récupère les nouveaux dividendes et diviseurs qui seront $A_2(X) = X^2 + 4X - 5$ et $B_2(X) = 27X - 27$. Finalement, la division de A_2 par B_2 donne

$$
\begin{array}{rl|l}
X^2 & +4X-5 & X-1 \\
\cline{3-3}
-X^2 & +X & X+5 \\
\cline{1-2}
 & 5X-5 & \\
 & -5X-5 & \\
\cline{2-2}
 & 0 &
\end{array}
$$

Alors $P.G.C.D(A, B) = 27X - 27 = 27(X - 1)$ qui représente le dernier reste non-nul dans l'algorithme d'Euclide. On peut dire que le plus grand diviseur commun de A et B est le polynôme $D(X) = X - 1$ (à un facteur constant non-nul près).

Définition 2.13.
Deux polynômes sont premiers entre eux si leur PGCD est un polynôme constant.

Proposition 2.6

1. Le polynôme $X - \alpha$ divise P si et seulement si $P(\alpha) = 0$.
2. Si $A(\alpha) = 0$ et $B(\alpha) = 0$ alors $X - \alpha$ est un diviseur commun de A et B.

Démonstration. 1. On sait que la division euclidienne de P par $X - \alpha$ donne $P(X) = (X - \alpha)Q(X) + R(X)$ où $\deg R < \deg X - \alpha$. Si $X - \alpha$ divise P alors $R(X) = 0$. Donc $P(\alpha) = (\alpha - \alpha)Q(\alpha) = 0$. Maintenant, supposons que $P(\alpha) = 0$ donc $(X - \alpha)Q(X) + R(X)$ évalué au point $X = \alpha$ va donner

$R(\alpha) = 0$ et puisque $\deg R < \deg(X - \alpha) = 1$ donc $\deg R = 0$, c'est à dire que R est une constante avec $R(\alpha) = 0$ donc $R(X) = 0$. Donc P est divisible par $X - \alpha$.

2. C'est une conséquence immédiate du résultat précédent.

□

Bibliographie

[1] Jean-Pierre Escofier. *Toute l'algèbre de la Licence-4e éd. : Cours et exercices corrigés*. Dunod, 2016.

[2] Steed Matthew. Proofs of the fundamental theorem of algebra. http://math.uchicago.edu/~may/REU2014/REUPapers/Steed.pdf, January 10, 2015. [Online ; accessed 25-September-2021].

[3] Frédéric Sturm Stéphane Balac. *Algèbre et analyse : Cours mathématiques de première années avec exercices corrigés*. PPUR, 2e edition, 2009.

[4] M. Artin. *Algebra*. Pearson Modern Classics for Advanced Mathematics Series. Pearson, 2017.

[5] Thomas Scott Blyth, Thomas Scott Blyth, and EF Robertson. *Algebra Through Practice : Volume 5, Groups : A Collection of Problems in Algebra with Solutions*. CUP Archive, 1985.

[6] Thomas Scott Blyth, Thomas Scott Blyth, and EF Robertson. *Algebra Through Practice : Volume 6, Rings, fields and modules : A Collection of Problems in Algebra with Solutions*. CUP Archive, 1985.

[7] Shahriar Shahriar. *Algebra in Action : A Course in Groups, Rings, and Fields*, volume 27. American Mathematical Soc., 2017.

[8] John B Fraleigh. *A first course in abstract algebra*. Pearson Education India, 2003.