FST Mulhouse.

Licence 1 Maths-Info

Mathématiques : ARITHMETIQUE-ALGEBRE

Elisabeth REMM

Chapitre 4

Polynômes à une indéterminée

Table des matières

1. Définitions 2
1.1. Définition d'un polynôme à une indéterminée 2
1.2. Addition de polynômes à une indéterminée 2
1.3. Multplication de polynômes à une indéterminée 3
2. La division euclidienne 4
2.1. Diviseurs et multiples d'un polynôme à une indéterminée 4
2.2. La division euclidienne 4
3. PGCD de deux polynômes 6
3.1. Définition du PGCD 6
3.2. Calul pratique du PGCD : l'algorithme d'Euclide 7
3.3. L'identité de Bézout 7
3.4. Application de l'identité de Bézout 8
3.5. Polynômes premiers entre eux 9
4. Racines d'un polynôme 9
4.1. Racines d'un polynôme 9
4.2. $\mathbb{K} = \mathbb{C}$: le théorème de d'Alembert 10
4.3. $\mathbb{K} = \mathbb{R}$ 11
4.4. Relations entre les racines et les coefficients 12
4.5. Racines multiples, polynôme dérivé 12
5. Polynômes irréductibles 13
5.1. Définition 13
5.2. Le théorème de d'Alembert 14
6. Division suivant les puissances croissantes 15

1. Définitions

1.1. **Définition d'un polynôme à une indéterminée.** Dans les classes antérieures, la notion de fonction polynômiale d'une variable réelle a été étudiée. C'est une fonction de la forme

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

où x est une variable réelle et les coefficients $a_0, a_1, \cdots, a_n$ sont des nombres réels donnés. Dans ce cours, nous ne voulons plus considérer un polynôme comme une fonction, mais comme une expression formelle. Grosso modo, ceci signifie que nous nous intéresserons uniquement à la suite des coefficients $(a_0, a_1, \cdots, a_n)$. Nous pourrions alors définir un polynôme "formel" à une indéterminée comme une suite finie $(a_0, a_1, \cdots, a_n)$ de nombres réels. Mais pour être plus conforme à l'expression polynôme à une indéterminée, nous allons donner la définition suivante

Définition 1. *On appelle polynôme réel (respectivement complexe) à une indéterminée notée X toute expression de la forme*

$$P(X) = a_0 + a_1 X + \cdots + a_n X^n$$

avec $a_0, a_1, \cdots, a_n \in \mathbb{R}$ (respectivement $a_0, a_1, \cdots, a_n \in \mathbb{C}$).

Nous voyons bien que le polynôme à une indéterminée X, $P(X) = a_0 + a_1 X + \cdots + a_n X^n$, est entièrement défini par la suite des coefficients $(a_0, a_1, \cdots, a_n)$. Ceci permet de donner une définition intrinsèque de la notion de polynôme (sans faire intervenir la notion d'indéterminée) :

Définition 2. *On appelle polynôme à coefficients dans $\mathbb{K}$ toute suite finie $P = (a_0, a_1, \cdots, a_n)$ d'éléments de $\mathbb{K}$.*

Par exemple le polynôme $P = (0, 1)$ correspond au polynôme à une indéterminée $P_1(X) = X$. Notons que l'on identifiera souvent, surtout pour raccourcir le texte, le polynôme P et le polynôme à une indéterminée $P(X)$.

Définition 3. *Etant donné un polynôme à une indéterminée $P(X) = a_0 + a_1 X = \cdots + a_n X^n$ avec $a_n \neq 0$, on dira alors que n est le degré de $P(X)$ et on écrira $n = \mathrm{d^o(P(X))}$.*

Principe d'identification. Nous dirons que deux polynômes $P(X) = a_0 + a_1 X + \cdots + a_p X^p$ et $Q(X) = b_0 + b_1 X + \cdots + b_q X^q$ à une indéterminée X sont égaux si et seulement si les coefficients sont égaux, c'est-à-dire

$$p = q, \qquad a_0 = b_0, a_1 = b_1, \cdots, a_p = b_p.$$

Si tous les coefficients sont nuls, le polynôme correspondant sera appelé le polynôme nul et noté $0(X)$ ou tout simplement 0, nous conviendrons de dire que son degré est $-\infty$:

$$\mathrm{d^o}0 = -\infty.$$

1.2. **Addition de polynômes à une indéterminée.** Nous allons noter par $\mathbb{R}[X]$ l'ensemble des polynômes à une indéterminée à coefficients réels et par $\mathbb{C}[X]$ l'ensemble des polynômes à une indéterminée à coefficients complexes. Lorsque nous ne voudrons pas différencier ces deux cas, nous noterons $\mathbb{K}[X]$ l'un ou l'autre de ces ensembles.

Soient $P(X) = a_0 + a_1 X + \cdots + a_p X^p$ et $Q(X) = b_0 + b_1 X + \cdots + b_q X^q$ deux éléments de $\mathbb{K}[X]$. Nous pouvons supposer que $q \leq p$. Alors le polynôme somme de $P(X)$ et $Q(X)$ est le polynôme $(P + Q)(X)$ défini par

$$(P + Q)(X) = (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_q + b_q)X^q + a_{q+1}X^{q+1} + \cdots + a_p X^p.$$

Nous remarquons immédiatement que si $p = \mathrm{d^o(P(X))}$ et $q = \mathrm{d^o(Q(X))}$ alors

$$\mathrm{d^o(P + Q)(X)} \leq \mathrm{Max(p, q)}.$$

On a l'égalité lorsque $p \neq q$ et lorsque $p = q$ si $a_p + b_p \neq 0$.

Cette addition vérifie les propriétés suivantes :

(1) Elle est commutative : pour tout $P(X), Q(X) \in \mathbb{K}[X]$,
$$(P + Q)(X) = (Q + P)(X).$$

(2) Elle est associative pour tout $P_1(X), P_2(X), P_3(X) \in \mathbb{K}[X]$,
$$((P_1 + P_2) + P_3)(X) = (P_1 + (P_2 + P_3))(X).$$

(3) Le polynôme nul est élément neutre : pour tout $P(X) \in \mathbb{K}[X]$,
$$P(X) + 0(X) = P(X).$$

(4) Pour tout $P(X) \in \mathbb{K}[X]$, il existe un polynôme $(-P)(X)$ tel que $(P + (-P))(X) = 0$. Si $P(X) = a_0 + a_1X + \cdots + a_nX^n$, alors $(-P)(X) = -a_0 - a_1X - \cdots - a_nX^n$. Pour abréger, on écrira $-P(X)$ pour $(-P)(X)$.

Ces propriétés se vérifient sans peine.

1.3. **Multplication de polynômes à une indéterminée.** Le produit de polynômes à une indéterminée est basé sur la loi

$$X^pX^q = X^{p+q}.$$

Par exemple

$$(a_0 + a_1X + a_2X^2)(b_0 + b_1X) = a_0b_0 + (a_1b_0 + a_0b_1)X + (a_2b_0 + a_1b_1)X^2 + (a_2b_1)X^3.$$

De manière générale le coefficient c_i du produit des polynômes $a_0 + a_1X + \cdots + a_pX^p$ et $b_0 + b_1X + \cdots + b_qX^q$ est

$$c_i = a_ib_0 + a_{i-1}b_1 + a_{i-2}b_2 + \cdots + a_jb_{i-j} + \cdots + a_1b_{i-1} + b_ia_0$$

certains de ces coefficients pouvant être nuls.

Proposition 1. *Soient $P(X)$ et $Q(X)$ dans $\mathbb{K}[X]$ de degré respectif $\mathrm{d^oP(x) = p}$ et $\mathrm{d^oQ(X) = q}$. Alors le degré du produit $P(X)Q(X)$ est égal à $p + q$.*

En effet le coefficient du plus haut degré est a_pb_q et d'après la définition du degré a_p et b_q sont non nuls.

On vérifie aisément les propriétés suivantes de la multiplication

(1) La multiplication est commutative, c'est-à-dire pour tous $P(X), Q(X) \in \mathbb{K}[X]$
$$P(X)Q(X) = Q(X)P(X)$$

(2) La multiplication est associative : pour tous $P(X), Q(X), R(X) \in \mathbb{K}[X]$:
$$P(X)(Q(X)R(X)) = (P(X)Q(X))R(X).$$

(3) La multiplication est distributive par rapport à l'addition, : $\forall P(X), Q(X), R(X) \in \mathbb{K}[X]$:
$$P(X)(Q(X) + R(X)) = P(X)Q(X) + P(X)R(X).$$

(4) La multiplication admet un élément neutre : le polynôme $1(X)$ aussi noté 1 défini par

$$1(X) = 1$$

ce polynôme vérifie

$$P(X)1(X) = P(X)$$

pour tout $P(X) \in \mathbb{K}[X]$.

Nous verrons dans le dernier chapitre ce que l'on peut dire de l'ensemble $\mathbb{K}[X]$ muni de l'addition et de la multiplication, ces deux opérations vérifiant les propriétés citées ci-dessus.

2. La division euclidienne

2.1. Diviseurs et multiples d'un polynôme à une indéterminée.

Définition 4. *On dit qu'un polynôme $A(X) \in \mathbb{K}[X]$ est divisible par un polynôme $B(X) \in \mathbb{K}[X]$ (ou que $B(X)$ divise $A(X)$) s'il existe un polynôme $Q(X) \in \mathbb{K}[X]$ tel que*

$$A(X) = B(X)Q(X).$$

On dit alors que $Q(X)$ est le quotient de $A(X)$ par $B(X)$.

Nous pouvons noter que la relation $B(X)$ divise $A(X)$ est une relation qui est reflexive ($A(X)$ divise $A(X)$ le quotient étant 1) et transitive (si $B(X)$ divise $A(X)$ et $C(X)$ divise $B(X)$ alors $C(X)$ divise $A(X)$). mais cette relation n'est pas symétrique. Ce n'est pas une relation d'équivalence. Notons également que si $B(X)$ divise $A(X)$ alors $\mathrm{d^oB(X)} \leq \mathrm{d^oA(X)}$ et que 0 est divisible par tout polynôme : $0 = B(X) \cdot 0$.

Proposition 2. *Soit $A(X)$ et $B(X)$ deux polynômes tels que*

$$A(X)B(X) = 0.$$

Alors l'un des deux polynômes est nul.

2.2. La division euclidienne.

Théorème 1. *Etant donnés un polynôme $A(X) \in \mathbb{K}[X]$ et un polynôme $B(X) \neq 0 \in \mathbb{K}[X]$, il existe un couple et un seul de polynômes $Q(X)$ et $R(X)$ vérifiant les condition*

(1)

$$A(X) = B(X)Q(X) + R(X)$$

(2)

$$\mathrm{d^oR(X)} < \mathrm{d^oB(X)}.$$

Déterminer ce couple c'est effectuer la division euclidienne de $A(X)$ par le polynôme NON NUL $B(X)$, les polynômes $Q(X)$ et $R(X)$ étant respectivement le quotient et le reste de cette division.

Démonstration. Montrons l'unicité de ce couple. Supposons qu'il y ait deux couples répondant à la proposition :

$$A(X) = B(X)Q(X) + R(X), \quad \mathrm{d^oR(X)} < \mathrm{d^oB(X)},$$
$$A(X) = B(X)Q_1(X) + R_1(X), \quad \mathrm{d^oR_1(X)} < \mathrm{d^oB(X)}.$$

On en déduit

$$0 = B(X)(Q(X) - Q_1(X)) + R(X) - R_1(X).$$

Ainsi

$$B(X)(Q(X)-Q_1(X))=-R(X)+R_1(X).$$

Ceci signifie que le polynôme $B(X)$ divise le polynôme $R_1(X)-R(X)$. Ceci implique

$$\mathrm{d^oB(X)} \leq \mathrm{d^o(R_1(X)-R(X))}.$$

Mais par hypothèse $\mathrm{d^oR(X)} < \mathrm{d^oB(X)}$ et $\mathrm{d^oR_1(X)} < \mathrm{d^oB(X)}$. Ainsi comme $B(X)$ divise un polynôme $R_1(X)-R(X)$ de degré strictement plus petit que $\mathrm{d^oB(X)}$, la seule possibilité est que $R_1(X)-R(X)=0$ soit $R_1(X)=R(X)$. On en déduit alors $B(X)(Q(X)-Q_1(X))=0$ ce qui implique $Q(X)=Q_1(X)$ et le couple $(Q(X),R(X))$ est bien unique.

Il nous reste à démontrer l'existence de cette division. Pour cela nous allons présenter un procédé pratique pour calculer le quotient et le reste. Ce procédé est proche de celui utilisé dans la division euclidienne des entiers. Soient deux polynômes $A(X)$ et $B(X)$ de $\mathbb{K}[X]$, $B(X)\neq 0$.

(1) Si $\mathrm{d^oA(X)} < \mathrm{d^oB(X)}$, alors on prend $Q(X)=0$ et $R(X)=A(X)$ et on a bien dans ce cas $\mathrm{d^oR(X)} < \mathrm{d^oB(X)}$.

(2) Supposons $\mathrm{d^oA(X)} \geq \mathrm{d^oB(X)}$. Soient a_pX^P et b_qX^q les termes de plus haut degré de $A(X)$ et $B(X)$. Par hypothèse $p \geq q$. Nous allons commencer la division en comparant ces deux termes. Comme $p \geq q$ on peut écrire

$$\frac{a_pX^p}{b_qX^q}=\frac{a_p}{b_q}X^{p-q}$$

et nous allons considérer ce terme comme terme de plus haut degré de $Q(X)$. Pour poursuivre la division, on remplace $A(X)$ par le polynôme

$$A_1(X)=A(X)-fraca_pb_qX^{p-q}B(X).$$

Il est clair que $\mathrm{d^oA_1(X)} < \mathrm{d^oA(X)}$, ce qui permet d'envisager une procédure qui s'arrêtera lorsque le nouveau polynôme aura un degré strictement inférieur à celui de $B(X)$. On voit donc l'analogie avec la division euclidienne des entiers.

Illustrons ceci par un exemple : soit à effectuer la division euclidienne des polynômes $A(X)=X^5-2X^4-X^3+22X$ par le polynôme $B(X)=X^2-4X+1$. Pratiquement nous allons poser notre division comme une division ordinaire

$$\begin{array}{lllll|ll}
X^5 & -2X^4 & -X^3 & & 22X & \multicolumn{2}{l}{X^2\quad -4X\quad +1} \\
 & & & & & \multicolumn{2}{l}{---\quad ---\quad ---\quad --} \\
X^5 & -4X^4 & +X^3 & & & \multicolumn{2}{l}{X^3\quad +6X^2\quad +22X\quad +82} \\
 & 6X^4 & -2X^3 & & +22X & & \\
 & 6X^4 & -24X^3 & +6X^2 & & & \\
 & & 22X^3 & -6X^2 & +22X & & \\
 & & 22X^3 & -88X^2 & +22X & & \\
 & & & 82X^2 & & & \\
 & & & 82X^2 & -328X & +82 & \\
 & & & & 328X & -82 &
\end{array}$$

Le dernier polynôme obtenu est $328X-82$, son degré est inférieur à celui de $B(X)$, on en déduit

$$Q(X)=X^3+6X^2+22X+82,\quad R(X)=328X-82$$

et on a bien

$$\mathrm{d^oR(X)} < \mathrm{d^oB(X)}$$

.

3. PGCD de deux polynômes

Nous avons défini au paragraphe précédent la notion de diviseur d'un polynôme de $\mathbb{K}[X]$. Il est facile d'en déduire la notion de diviseurs communs à deux (ou plusieurs) polynômes. Mais pour définir, comme pour les entiers, une notion de PGCD, soit de Plus Grand Commun Diviseur, il est nécessaire de savoir ce que l'on entend par plus grand. Ceci est naturel pour les entiers, mais pour les polynômes loin s'en faut. Nous allons contourner cette difficulté en comparant des polynômes au travers de leur degré.

3.1. **Définition du PGCD.** Soient deux polynômes $A(X)$ et $B(X)$ de $\mathbb{K}[X]$ non nuls. Regardons tous les diviseurs communs. Il y en a au moins un, le polynôme 1 qui divise tous les polynômes non nuls.

Définition 5. *Soient deux polynômes $A(X)$ et $B(X)$ de $\mathbb{K}[X]$ non nuls. On dira qu'un polynôme $D(X)$ est un PGCD de $A(X)$ et $B(X)$, si $D(X)$ divise $A(X)$ et $B(X)$ et s'il vérifie*

$$\mathrm{d^oD(X)} \geq \mathrm{d^oQ(X)}$$

pour tout diviseur commun $Q(X)$ de $A(X)$ et $B(X)$.

Il est clair que tout couple de polynômes non nuls possède un PGCD, celui-ci aura un degré inférieur ou égal au plus petit des degrés de $A(X)$ et $B(X)$. Mais contrairement au cas des entiers, il n'y a pas unicité.

Proposition 3. *Soient deux polynômes $A(X)$ et $B(X)$ de $\mathbb{K}[X]$ non nuls et soit $D(X)$ un PGCD. Alors tout autre PGCD est de la forme $\lambda D(X)$ pour tout $\lambda \neq 0$ et inversement, tout polynôme qui s'écrit $\lambda D(X)$ est un PGCD de $A(X)$ et $B(X)$.*

Démonstration. Commençons par caractériser les diviseurs communs à $A(X)$ et $B(X)$. Soit $E(X)$ un diviseur commun à ces deux polynômes. Il est alors aussi un diviseur à tout polynôme de la forme $A(X)P(X) + B(X)Q(X)$. Considérons l'ensemble $\mathcal{I}$ des polynômes de la forme $A(X)P(X) + B(X)Q(X)$ où $P(X)$ et $Q(X)$ sont dans $\mathbb{K}[X]$. Soit $D(X)$ un élément de $\mathcal{I}$ de plus bas degré. En particulier tout polynôme non nul de degré strictement inférieur à celui de $D(X)$ n'est pas dans I autrement dit 0 est le seul polynôme de $\mathcal{I}$ de degré strictement inférieur à celui de $D(X)$.

Lemme 1. *Le polynôme $D(X)$ est un diviseur commun à $A(X)$ et $B(X)$.*

Démontrons ce lemme. Si $F(X) \neq 0$ est dans $\mathcal{I}$, alors $\mathrm{d^oF(X)} \geq \mathrm{d^oD(X)}$ et la division euclidienne de $F(X)$ par $D(X)$ s'écrit

$$F(X) = D(X)Q(X) + R(X)$$

avec $\mathrm{d^oR(X)} < \mathrm{d^oD(X)}$. Mais les polynômes $F(X)$ et $D(X)$ étant dans $\mathcal{I}$, s'écrivent

$$F(X) = A(X)P_1(X) + B(X)Q_2(X), \quad D(X) = A(X)P_2(X) + B(X)Q_2(X).$$

On en déduit que $R(X) = F(X) - D(X)Q(X)$ s'écrit aussi sous la forme $R(X) = A(X)P_3(X) + B(X)Q_3(X)$ et est donc dans $\mathcal{I}$. Mais son degré est strictement plus petit que celui de $D(X)$ dont tout polynôme de $\mathcal{I}$ est de degré plus grand. On en conclut que $R(X) = 0$ et donc $D(X)$ divise tout polynôme de $\mathcal{I}$.

Revenons à la démonstration du théorème. Comme $D(X)$ est dans $\mathcal{I}$, tout diviseur de $A(X)$ et $B(X)$ divise $D(X)$. Ainsi $D(X)$ est un PGCD de $A(X)$ et $B(X)$. Inversement si $E(X)$ est

un PGCD de $A(X)$ et $B(X)$ alors en tant que diviseur commun à $A(X)$ et $B(X)$ il divise tout élément de $\mathcal{I}$, donc il divise $D(X)$. Comme c'est un PGCD, nécessairement on doit avoir

$$E(X) = \lambda D(X)$$

avec $\lambda \in \mathbb{K}$ et $\lambda \neq 0$. La proposition s'en déduit.

3.2. **Calul pratique du PGCD : l'algorithme d'Euclide.** Comme en arithmétique l'algorithme d'Euclide ;, calqué sur celui de l'arithmétique, va nous fournir un procédé pratique du calcul du PGCD. Soient deux polynômes non nuls $A(X)$ et $B(X)$ avec $\mathrm{d^oA(X)} \geq \mathrm{d^oB(X)}$. Cet algorithme se présente sous forme d'une suite de divisions euclidiennes :

$$\begin{array}{lcll} A(X) & = & B(X)Q_1(X) + R_1(X) & ; \ \mathrm{d^oR_1(X) < d^oB(X)} \\ B(X) & = & R_1(X)Q_2(X) + R_2(X) & ; \ \mathrm{d^oR_2(X) < d^oR_1(X)} \\ R_1(X) & = & R_2(X)Q_3(X) + R_3(X) & ; \ \mathrm{d^oR_3(X) < d^oR_2(X)} \\ \cdots & = & \cdots & ; \ \cdots \\ R_{k-2}(X) & = & R_{k-1}(X)Q_{k-1}(X) + R_k(X) & ; \ \mathrm{d^oR_k(X) < d^oR_{k-1}(X)} \\ R_{k-1}(X) & = & R_k(X)Q_k(X) & ; \end{array}$$

et le dernier reste non nul est un PGCD de $A'X)$ et $B(X)$

$$PGCD(A(X), B(X)) = R_k(X).$$

3.3. **L'identité de Bézout.**

Théorème 2. *Soient $A(X)$ et $B(X)$ deux polynômes de $\mathbb{K}[X]$ non nuls tous les deux nuls. Soit $D(X)$ un PGCD de $A(X)$ et $B(X)$. Il existe alors deux polynômes $U(X)$ et $V(X)$ de $\mathbb{K}[X]$ tels que :*

$$D(X) = A(X)U(X) + B(X)V(X).$$

Démonstration. Ces polynômes $U(X)$ et $V(X)$ se calculent, comme en arithmétique des entiers, en "remontant" l'algorithme d'Euclide permettant de calculer le PGCD.

Remarque. Ces polynômes $U(X)$ et $V(X)$ que nous calculons via l'algorithme d'Euclide, ne sont pas les euls à vérifier l'identité de Bézout relative aux polynômes donnés $A(X)$ et $B(X)$. En effet soit $Q(X)$ un polynômes quelconque. Considérons les polynômes $U_1(X) = U(X) + Q(X)B(X)$ et $V_1(X) = V(X) - Q(X)A(X)$. On a alors

$$\begin{array}{rl} U_1(X)A(X) + V_1(X)B(X) & = (U(X) + Q(X)B(X))A(X) + (V(X) - Q(X)A(X))B(X) \\ & = U(X)A(X) + V(X)D(X) = D(X). \end{array}$$

On peut toutefois exiger un peu plus sur ces polynômes $U(X)$ et $V(X)$ pur ne récupérer que les solutions issues de l'algorithme d'Euclide (à une constante multiplicative près) :

Soient $A(X)$ et $B(X)$ deux polynômes de $\mathbb{K}[X]$ non nuls tous les deux nuls. Soit $D(X)$ un PGCD de $A(X)$ et $B(X)$. Il existe alors deux polynômes $U(X)$ et $V(X)$ de $\mathbb{K}[X]$ tels que :

$$\mathrm{d^oU(X) < d^oB(X)}, \qquad \mathrm{d^oV(X) < d^oA(X)}$$

vérifiant l'identité

$$D(X) = A(X)U(X) + B(X)V(X)$$

3.4. **Application de l'identité de Bézout.** Etant donnés deux polynômes $A(X)$ $B(X)$ et $C(X)$, nous nous intéressons à la résolution d'équations du type

$$A(X)U(X) + B(X)V(X) = C(X).$$

Supposons de plus que si $D(X) = PGCD(A(X), B(X))$, alors

$$C(X) = C_1(X)D(X)$$

c'est-à-dire le polynôme donné $C(X)$ est divisible par le PGCD de $A(X)$ et $B(X)$. Pour résoudre cette équation, on part de l'identité de Bézout :

$$A(X)U_1(X) + B(X)U_2(X) = D(X)$$

les polynômes $U_1(X)$ et $V_1(X)$ étant calculés par exemple à partir de l'algorithme d'Euclide. Multiplions cette identité par $C_1(X)$

$$A(X)U_1(X)C_1(X) + B(X)U_2(X)C_1(X) = D(X)C_1(X) = C(X).$$

Ainsi $U(X) = U_1(X)C_1(X)$, $V(X) = V_1(X)C_1(X)$ est un couple de solution particulière. La solution générale sera donnée par les couples

$$U(X) = U_1(X)C_1(X) + Q(X)B(X),\ V(X) = V_1(X)C_1(X) - Q(X)A(A(X))$$

où $Q(X)$ est un polynôme quelconque de $\mathbb{K}[X]$.

Exemple. Soit à résoudre

$$(X^3 - 1)U(X) + (X^2 + 1)V(X) = 2X^2.$$

Déterminons le PGCD de $A(X) = X^3 - 1$ et $B(X) = X^2 + 1$). L'algorithme d'Euclide s'écrit

$$\begin{array}{ll} X^3 - 1 & = (X^2 + 1)(X) + (-X - 1) \\ X^2 + 1 & = (-X - 1)(-X + 1) + 2 \end{array}$$

On en déduit que 2 est un PGCD de $A(X)$ et $B(X)$. Retrouvons l'identité de Bézout

$$\begin{array}{ll} 2 & = X^2 + 1 - (-X - 1)(-X + 1) \\ 2 & = X^2 + 1 - (X^3 - 1)(-X + 1) - (X^2 + 1)(X)(-X + 1) \\ & = (X^3 - 1)(X - 1) + (X^2 + 1)(-X^2 + X + 1) \end{array}$$

Ainsi

$$(X - 3 - 1)(X - 1) + (X2 + 1)(-X^2 + X + 1) = 2$$

et donc

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

Le couple

$$(U(X) = X^2(X - 1), V(X) = (X^2(-X^2 + X + 1)$$

est une solution particulière de l'équation donnée.

3.5. **Polynômes premiers entre eux.**

Définition 6. *Soient $A(X)$ et $B(X)$ deux polynômes non nuls de $\mathbb{K}[X]$. On dit qu'ils sont premiers entre eux si* 1 *est un PGCD de $A(X)$ et $B(X)$*

Dans ce cas tout polynôme constant non nul est un PGCD de $A(X)$ et $B(X)$. Dans l'algorithme d'Euclide, le dernier reste non nul est constant.

Théorème 3. *Soient $A(X), B(X)$ et $C(X)$ des éléments non nuls de $\mathbb{K}[X]$. Si $A(X)$ divise le produit $B(X)C(X)$ et si $A(X)$ est premier avec $B(X)$, alors il divise $C(X)$.*

Démonstration. Le polynôme $A(X)$ divise les produits $B(X)C(X)$ (par hypothèse) et $A(X)C(X)$. Il divise donc le PGCD de $B(X)C(X)$ et $5A(X)C(X)$. Or $A(X)$ est premier avec $B(X)$. Donc l$PGCD(B(X)C(X), A(X)C(X) = C(X)$. Donc $A(X)$ divise $C(X)$.

On en déduit la caractérisation suivante des polynômes premiers entre eux.

Théorème 4. *Soient $A(X)$ et $B(X)$ des polynômes non nuls de $\mathbb{K}[X]$. Pour qu'ils soient premiers entre eux il faut et il suffit qu'il existe deux polynômes $U(X), V(X) \in \mathbb{K}[X]$ tels que*

$$A(X)U(X) + B(X)V(X) = 1.$$

Démonstration. La condition est nécessaire, ce n'est que l'identité de Bézout. Réciproquement, supposons qu'il existe deux polynômes $U(X), V(X) \in \mathbb{K}[X]$ tels que $A(X)U(X) + B(X)V(X) = 1$. Tout diviseur commun à $A(X)$ et $B(X)$ divise $A(X)U(X) + B(X)V(X)$. Il divise donc le polynôme constant 1, c'est donc une constante. Ainsi tout diviseur commun à $A(X)$ et $B(X)$ est une constante, ces polynômes sont premiers entre eux.

4. Racines d'un polynôme

A tout polynôme $P(X) = a_0 + a_1X + \cdots + a_pX^p$ de $\mathbb{K}[X]$, nous pouvons lui associé de manière biunivoque la fonction d'une variable

$$f_P : \mathbb{K} :\to \mathbb{K}$$

où $\mathbb{K}$ est soit le corps des réels soit celui des complexes, définie par

$$f_P(x) = a_0 + a_1x + \cdots + a_px^p.$$

4.1. **Racines d'un polynôme.**

Définition 7. *Soit $P(X) \in \mathbb{K}[X]$. On dit qu'un élément $\alpha \in \mathbb{K}$ est une racine de $P[X]$ si α est une racine de l'équation polynomiale $f_P(x) = 0$, c'est-à-dire si α vérifie*

$$f_P(\alpha) = a_0 + a_1\alpha + \cdots + a_p\alpha^p = 0.$$

On dit parfois aussi que α est un zéro de $P(X)$.

Théorème 5. *Soient $P(X) \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$. Pour que α soit une racine de $P(X)$ il faut et il suffit que $P(X)$ soit divisible par le polynôme $X - \alpha$.*

Démonstration. Si $P(X) = (X-\alpha)Q(X)$, avec $Q(X) \in \mathbb{K}[X]$, alors

$$f_P(\alpha) = (\alpha - \alpha) f_Q(\alpha) = 0$$

et α est une racine. Réciproquement supposons que α soit racine, c'est-à-dire $f_P(\alpha) = 0$. La division euclidienne de $P(X)$ par $X - \alpha$ (on suppose bien sur d°P(X) ≥ 1), s'écrit

$$P(X) = (X-\alpha)Q(X) + R(X)$$

avec d°R(X) < 1, c'est-à-dire d°R(X) $= 0$. Ainsi $R(X) = \beta$ est une constante. Ceci implique

$$f_P(\alpha) = 0 = (\alpha - \alpha)Q(\alpha) + \beta = \beta.$$

Ainsi $\beta = 0$ et donc $R(X) = 0$ et

$$P(X) = (X-\alpha)Q(X).$$

Le polynôme $P(X)$ est donc divisible par $(X - \alpha)$.

4.2. $\mathbb{K} = \mathbb{C}$ **: le théorème de d'Alembert.** Noua admettrons le théorème suivant, qui montre l'intérêt du corps des nombres complexes

Théorème 6. *(***Théorème de d'Alembert***). Tout polynôme $P(X)$ appartenant à $\mathbb{C}[X]$ de degré supérieur ou égal à* 1 *admet au moins une racine.*

Nous déduisons immédiatement que tout polynôme complexe se factorise en produit de facteurs du premier degré

$$P(X) = a_0 + a_1 X + \cdots + a_p X^p = a_n(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_p)$$

les racines α_i étant complexes et certaines peuvent être égales entre elles. En regroupant les racines égales, le polynôme $P(X)$ se factorise ainsi

$$P(X) = a_n(X-\beta_1)^{p_1}(X-\beta_2)^{p_2}\cdots(X-\beta_k)^{p_k}$$

avec $\beta_i \neq \beta_j$ dès que $i \neq j$ et $p_1 + p_2 + \cdots + p_k = p$.

Remarque. Comment calculer les racines ? Le théorème de d'Alembert nous assure l'existe pour un polynôme de degré p de p racines complexes simples ou confondues. Dans la décomposition précédente, la racine β est multiple de multiplicité $k_i i$. Si $k_i = 1$ la racine est dite simple. Mais comment calculer ces racines ?

(1) Si d°P(X) $= 1$, on sait faire, depuis le cours de troisième.

(2) Si d°P(X) $= 2$, là aussi on sait, depuis la classe de seconde. Rappelons toutefois les formules : Soit $P(X) = a_0 + a_1 X + a_2 X^2$ avec $a_2 \neq 0$. Alors les deux racines α_1 et α_2 sont données par

$$\alpha_1 = \frac{-a_1 + \sqrt{a_1^2 - 4a_0a_2}}{2a_2}, \quad \alpha_2 = \frac{-a_1 - \sqrt{a_1^2 - 4a_0a_2}}{2a_2},$$

Dans le cours d'analyse, on apprend à calculer la racine carrée d'un nombre complexe ici le discriminant $a_1^2 - 4a_2a_0$.

(3) Pour le degré 3 les choses se compliquent un peu. Nous verrons comment dans le cas réel calculer les racines d'un polynôme réel de degré 3. Mais au delà du degré trois, on utilise des méthodes numériques et on renvoie le lecteur au cours d'analyse numérique.

(4) Il existe toutefois des équations polynômiales pour lesquelles les solutions sont bien définies. Prenons par exemple les polynômes du type

$$P(X) = X^p - 1$$

Les racines de ce polynômes sont les racine d'ordre p de l'unité. Elles s'écriventt

$$\xi_k e^{\frac{2ik\pi}{p}}, \quad k = 1, 2, \cdots, p.$$

4.3. $\mathbb{K} = \mathbb{R}$**.** Contrairement au cas complexe, il existe des polynômes de $\mathbb{R}[X]$ qui n'ont aucune racine. Rappelons le résultat suivant, qui a été démontré dans les classes de lycées :

Proposition 4. *Soit $P(X) = a_2X^2+a_1X+a_0$, avec $a_2 \neq 0$ un polynôme de degré 2 a coefficient tels. Ce polynôme admet des racines si et seulement si le discriminant $\Delta = a_1^2-4a_2a_0$ est positif ou nul. S'il est strictement positif, il admet deux racines simples*

$$\alpha_1 = \frac{-a_1 + \sqrt{a_1^2 - 4a_0a_2}}{2a_2}, \quad \alpha_2 = \frac{-a_1 - \sqrt{a_1^2 - 4a_0a_2}}{2a_2},$$

Si $\Delta = 0$, il admet une racine double (de multiplicité 2 :

$$\alpha = \frac{-a_1}{2a_2}.$$

Pour les degrés supérieur nous n'avons pas de résultat analogue aussi précis. Mais il existe des polynômes sans racine, par exemple $X^4 + 1$. Toutefois, on a le résultat suivant

Proposition 5. *Soit $P(X) = a_{2s+1}X^{2s+1} + a_{2s}X^{2s} + \cdots + a_1X + a_0$ un polynôme réel de degré impair $p = 2s + 1$ ($a_{2s+1} \neq 0$). Alors $P(X)$ possède au moins une racine.*

Démonstration. La démonstration a été faite dans les classes terminales. On considère la fonction polynomiale $f_P(x)$ d'une variable réelle associée. Elle est continue, Elle varie suivant le signe de a_{2s+1} de $-\infty$ à $+\infty$ ou de $+\infty$ à $-\infty$. Le théorème des valeurs intermèdeiares permet de conclure.

Il n'existe pas dans le cas réel non plus, de méthode algébrique pour calculer explicitement les racines d'un polynôme réel. Plus préciséent, dès le degré 5, on sait qu'il n'existe aucune formule portant sur les coefficients qui donneraient explicitement ces racines. Ceci est un des plus grands résultats d'algèbre du à Evariste Galois. Toutefois en degré 3 il existe une méthode, due à Tartaglia et appelée méthode Cardan qui se résume ainsi : Soit $P(X) = X^3+a_2X^2+a_1X+a_0$ un polynôme de degré 3. Comme on cherche les racines de $P(X)$ on peut toujours supposer ce polynôme unitaire c'est-à-dire $a_3 = 1$, sinon on considère le polynôme $a_3^{-1}P(X)$ qui admet les mêmes racines que $P(X)$.

(1) Première étape : on réduit $P(X)$ sous la forme

$$P(X) = X^3 + 3pX + q$$

en faisant un changement de variable en posant

$$X = Y - \frac{a_2}{3}.$$

(2) Le discriminnt du polynôme $P(X) = X^3 + 3pX + q$ est

$$\Delta = p^3 + q^2.$$

(3) On a alors une racine réelle de $P(X) = X^3 + 3pX + q$
$$\alpha = \sqrt[3]{\sqrt{\Delta} - q} - \sqrt[3]{\sqrt{\Delta} + q}.$$

(4) Ce nombre α est bien réel, même si Δ est négatif. On utilise pour le calculer les nombres complexes.

4.4. **Relations entre les racines et les coefficients.** Nous venons de voir que lorsqu'on connaît des formules pouvant exprimer les valeurs des racines, ces formules s'expriment toujours à l'aide des coefficients du polynôme. Supposons donné un polynôme dans $\mathbb{K}[X]$ ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$) de degré p ayant p racines distinctes ou confondues comptées avec leur multiplicité. Autrement dit $P(X)$ de factorise
$$P(X) = a_p(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_p)$$
certaines racines pouvant être égales entre elles. Un tel polynôme est dit scindé.

Théorème 7. *On a les relations suivantes*

(1) $\alpha_1 + \alpha_2 + \cdots + \alpha_p = \dfrac{a_{p-1}}{a_p}$.

(2) $\displaystyle\sum_{1\le i<j\le p} \alpha_i\alpha_j = \frac{a_{p-2}}{a_p}$

(3) $\cdots$

(4) $\displaystyle\sum_{1\le i_1<i_2<\cdots<i_k\le p} \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k} = (-1)^{k-1}\frac{a_{p-k}}{a_p}$

(5) $\cdots$

(6) $\alpha_1\alpha_2\cdots\alpha_p = (-1)^p\dfrac{a_0}{a_p}$.

Par exemple, pour un trinôme de degré 2, $P(X) = a_2X^2 + a_1X + a_0$ avec $a_2 \neq 0$, si ce polynôme admet deux racines distinctes ou non, on a alors
$$\alpha_1 + \alpha_2 = \frac{a_1}{a_0}, \quad \alpha_1\alpha_2 = -\frac{a_0}{a_2}.$$
Ces formules sont bien utiles par exemple pour calculer une deuxième racine si on en connaît déjà une.

4.5. **Racines multiples, polynôme dérivé.**

Définition 8. *Soit $P(X) = a_0 + a_1X + \cdots + a_pX^p$ un polynôme de degré p de $\mathbb{K}[X]$. On appelle polynôme dérivé de $P(X)$ le polynôme, noté $P'(X)$ donné par*
$$P'(X) = a_1 + 2a_2X + \cdots + pa_pX^{p-1}.$$

On voit donc que tout polynôme constant a pour dérivé 0 et la dérivée du polynôme X^k et kX^{k-1} dès que $k \geq 1$.

Plus généralement on appellera dérivé k-ième du polynôme $P(X)$ le polynôme noté $P^{(k)}(X)$ défini par induction par la formule
$$P^{(k)}(X) = (P^{(k-1)})'(X).$$

Proposition 6. *Le degré du polynôme dérivé vérifie*

$$\mathrm{d^oP'(X) = d^oP(X) - 1.}$$

En particulier la dérivée k-ième d'un polynôme de degré p est nulle dès que $k \geq p+1$.

Proposition 7. *Soit α une racine du polynôme $P(X) \in \mathbb{K}[X]$. Alors α est une racine de multiplicité plus grande que 2 si et seulement si α est racine du polynôme dérivé $P'(X)$.*

Démonstration. En effet si α est racine de multiplicité k avec $k > 1$, alors on a la factorisation

$$P(X) = (X-\alpha)^k Q(X)$$

avec $Q(X) \in \mathbb{K}[X]$. On en déduit

$$P'(x) = k(X-\alpha)^{k-1}Q(X) + (X-\alpha)^k Q'(X).$$

Ainsi $P'(\alpha) = 0$.

Proposition 8. Développement de Taylor. *Soit $P(X) \in \mathbb{K}[X]$ de degré p. Pour tout $a \in \mathbb{K}$, on a*

$$P(X) = P(a) + (X-a)P'(a) + \cdots + \frac{(X-a)^k}{k!}P^{(k)}(a) + \cdots + \frac{(X-a)^p}{p!}P^{(p)}(a).$$

Ce développement s'appelle le développement de Taylor du polynôme $P(X)$ au point a. Dans cette expression $P(a)$ désigne plus précisément $f_P(a)$ la valeur de la fontion polynôme associée au point a. L'écrire du polynôme $P(X)$ correspond au développement de Taylor au point $a = 0$

Exemple. Trouver un polynôme de $\mathbb{R}[X]$ de degré 3 tel que

$$P(1) = 2,\ P'(1) = -2,\ P^{(2)}(1) = 0,\ P^{(3)}(1) = 6.$$

Le développement de Taylor de $P(X)$ pour $a = 1$ s'écrit

$$P(X) = P(1) + (X-1)P'(1) + \frac{(X-1)^2}{2!}P^{(2)}(1) + \frac{(X-1)^3}{3!}P^{(3)}(1)$$

soit en remplaçant

$$P(X) = 2 - 2(X-1) + 6\frac{(X-1)^3}{3!} = 2 + 2x - 3X^2 + X^3.$$

5. Polynômes irréductibles

5.1. Définition.

Définition 9. *Soit $P(X) \in \mathbb{K}[X]$. On dit que $P(X)$ est irréductible si*

(1) $\mathrm{d^oP(X) \geq 1}$,

(2) Tout diviseur de P est de la forme $aP(X)$ avec $a \in \mathbb{K}$ ou est un polynôme constant non nul.

Par exemple tout polynôme de degré 1 est irréductible. Un autre exemple, le polynôme X^2+1 est irréductible dans $\mathbb{R}[X]$ (sinon il aurait un racine) et n'est pas irréductible dans $\mathbb{C}[X]$ car dans ce cas il s'écrit $(X+i)(X-i)$.

Nous admettrons le résultat suivant : tout polynôme de $\mathbb{K}[X]$ peut s'écrire comme un produit de polynômes irréductibles. Ce résultat montre l'intérêt de connaître la famille des polynômes irréductibles.

5.2. **Le théorème de d'Alembert.** Nous rappelons ici, ce théorème fondamental, qui montre l'intérêt de a construction de l'ensemble des nombres complexes.

Théorème 8. *Tout polynôme non constant, à coefficients complexes, admet au moins une racine complexe.*

Ce théorème est également appelé le théorème fondamental de l'algèbre. Nous ne le démontrerons pas ici. Une des démonstrations classiques repose sur l'analyse des fonctions d'une variable complexe. Cette étude est abordée en troisième année de Licence sous l'étiquette "Etude des fonctions holomorphes."

Une des conséquences de ce théorème fondamental est la proposition suivante :

Proposition 9. Cas complexe. *Un polynôme $P(X)$ appartenant à $\mathbb{C}[X]$ est irréductible si et seulement si il est de degré* 1.

On déduit de ce résultat la description des polynômes dans le cas réel.

Proposition 10. Cas réel. *Un polynôme $P(X)$ appartenant à $\mathbb{R}[X]$ est irréductible si et seulement si*

(1) Soit il est de degré 1,

(2) Soit il est de degré 2 *avec un discriminant négatif.*

Démonstration. En effet tout polynôme $P(X)$ réel peut être considéré comme un polynôme complexe. Dans ce cas il admet p racines si $p = \mathrm{d^oP(X)}$. Mais si α est une racine complexe non réelle, alors sa conjuguée $\overline{\alpha}$ est aussi une racine complexe non réelle. Dans la décomposition en facteurs du premier degré, on regroupe alors les facteur

$$(X-\alpha)(X-\overline{\alpha}) = X^2 + (\alpha+\overline{\alpha})X + \alpha\overline{\alpha}$$

qui est à coefficient réels car $\alpha+\overline{\alpha})$ et $\alpha\overline{\alpha}$ sont des nombres réels.

Remarque. Un polynôme irréductible de degré plus grand que 1 n'a pas de racine. Mais la réciproque est fausse. Un polynôme peut n'avoir aucune racine est être réductible. Par exemple $P(X) = X^4 + 1$ n'a aucune racine réelle mais il se décompose

$$P(X) = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1).$$

6. Division suivant les puissances croissantes

Cette opération est souvent très utile pour étudier des développements limités de quotient de fonctions polynômes. Mais ce n'est pas la seule utilité.

Théorème 9. *Soit k un entier positif donné et soient $A(X)$ et $B(X)$ deux polynômes de $\mathbb{K}[X]$ avec $B(0) \neq 0$. Il existe un et un seul couple de polynômes $Q(X)$ et $R(X)$ tels que*

$$A(X) = B(X)Q(X) + X^{k+1}R(X)$$

avec $/dgQ(X) \leq k$.

Le polynôme $Q(X)$ est appelé le quotient d'ordre k et $X^{k+1}R(X)$ le reste de la division de $A(X)$ et $B(X)$ suivant les puissances croissantes de X. L'exemple suivant montre la technique de cette division.

$$\begin{array}{ccccccc|ccc}
1 & + & +X^2 & +X^3 & & & & 1 & +2X & -X^3 \\
 & & & & & & & -- & -- & -- \\
-1 & -2X & & +X^3 & & & & 1 & -2X & +5X^3 \\
-- & -- & -- & -- & & & & & & \\
 & -2X & +X^2 & +2X^3 & & & & & & \\
 & 2X & +4X^2 & & -2X^4 & & & & & \\
 & -- & -- & -- & -- & & & & & \\
 & & +5X^2 & +2X^3 & -2X^4 & & & & & \\
 & & -5X^2 & -10X^3 & & +5X^5 & & & & \\
 & & -- & -- & -- & -- & & & & \\
 & & & -8X^3 & -2X^4 & +5X^5 & & & &
\end{array}$$

Le quotient d'ordre 2 est $1 - 2X + 5X^2$ et le reste $-8X^3 - 2X^4 + 5X^5$.