Algèbre 2

Alexey Muranov

17 avril 2025

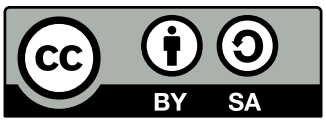

Table des matières

II. Polynômes

Ce chapitre ne traite que les polynômes à coefficients *réels*, et pour la plupart en *une* seule *indéterminée*. Ils seront appelés ici *polynômes* tout court.

II.1. Qu'est-ce que c'est, un polynôme en une indéterminée ?

Définition. Définissons les *polynômes* en une *indéterminée* X à *coefficients* réels, appelés ici *polynômes* tout court, ainsi :

(A) Tout nombre réel est un *polynôme*, dit *polynôme constant*.[1]

(B) Il y a un *polynôme* distingué X, dit l'*indéterminée*.

(C) Les opérations d'addition, de soustraction et de multiplication sont définies pour tous les *polynômes* : si A et B sont *polynômes*, alors $A+B$, $A-B$ et AB sont *polynômes* aussi. En plus, les 8 identités suivantes sont satisfaites pour tous *polynômes* A, B, C :

(1) $A+(B+C)=(A+B)+C$,

(2) $A+0=A=0+A$,

(3) $B+A=A+B$,

(4) $A+(B-A)=B$,

(5) $A(BC)=(AB)C$,

(6) $A\cdot 1=A=1\cdot A$,

(7) $BA=AB$,

(8) $A(B+C)=AB+AC$.

(D) Tout *polynôme* A s'écrit comme

$$\begin{aligned} A &= a_0+a_1X+a_2X^2+\cdots+a_nX^n \\ &= a_0X^0+a_1X^1+a_2X^2+\cdots+a_nX^n, \end{aligned}$$

où $a_0, a_1, \ldots, a_n$ sont des nombres réels, dits les *coefficients* de A.

(E) Si $a_0, a_1, \ldots, a_n$ sont des nombres réels tels que

$$a_0X^0+a_1X^1+a_2X^2+\cdots+a_nX^n=0,$$

alors $a_0=a_1=a_2=\cdots=a_n=0$.

[1] L'usage du mot « constant » ici paraît maladroit, mais telle est la tradition qui a l'origine à l'époque où on ne faisait pas de distinction entre les *polynômes* et les *fonctions polynomiales*, et où même la notion moderne de *fonction* n'existait pas. Peut-être il serait plus approprié d'appeler ces polynômes *polynômes scalaires*.

Notation. L'ensemble des polynômes en une indéterminée X à coefficients dans $\mathbf{R}$ (réels) est noté « $\mathbf{R}[X]$ ».

Remarque. Parfois on définit les polynômes comme certaines « expressions formelles ». Notons cependant que « $X^2 - 1$ », « $1X^2 + 0X + (-1)$ », et « $(X+1)(X-1)$ » sont trois expressions différentes qui représentent un même polynôme.

Définition. Soit un polynôme

$$A = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$

où X est l'*indéterminée*, et $a_0, a_1, \ldots, a_n$ sont nombres réels – les *coefficients* de A.

(1) Ceux des polynômes $a_0, a_1X, a_2X^2, \ldots, a_nX^n$ qui ne sont pas nuls sont dits *termes* de A.

(2) Si $a_0 \neq 0$, alors a_0 est dit le *terme constant*[2] de A. Si $a_0 = 0$, on peut dire que A n'a pas de *terme constant*. Cependant, souvent il peut être pratique d'appeler a_0 le *terme constant* de A même si $a_0 = 0$, et lorsque il est défini ainsi, on va le noter « $\operatorname{tc} A$ » : $\operatorname{tc} A \overset{\text{déf}}{=} a_0$.

(3) Si $a_n \neq 0$, alors a_nX^n est dit le *terme dominant* de A, qu'on va noter « $\operatorname{td} A$ », a_n est dit le *coefficient dominant* de A, qu'on va noter « $\operatorname{cd} A$ », et n est dit le *degré* de A, noté « $\deg A$ ».

(4) Si $A = 0$, alors soit on dit que le *degré* de A n'est pas défini, soit on le défini de manière qui paraît pratique dans les calculs et les raisonnements subséquents. Il est courant de définir le *degré* du polynôme zéro comme moins l'*infini*, ce qu'on peut écrire comme « $\deg 0 = -\infty$ ». Ici on va plutôt laisser « $\deg 0$ » indéfini.[3]

D'après cette définition, $\operatorname{tc} 0 = 0$, mais « $\operatorname{td} 0$ », « $\operatorname{cd} 0$ », et « $\deg 0$ » ne sont pas définis.

Définition. Un polynôme est dit *unitaire* si et seulement si son coefficient dominant est 1.

II.2. Propriétés de la multiplication

Proposition. *Pour tous* $A, B \in \mathbf{R}[X]$, $\operatorname{tc} AB = (\operatorname{tc} A)(\operatorname{tc} B)$.

Exercice. Prouver cette proposition.

Proposition. *Si* $A, B \in \mathbf{R}[X]$ *sont deux polynômes non nuls, alors le polynôme* AB *est aussi non nul, et, en plus* :

[2] Peut-être il serait plus approprié d'appeler a_0 le *terme scalaire* – voir la note 1 pour *polynôme constant*.

[3] Pour simplifier la définition de la *division euclidienne* des polynômes, il paraît pratique d'avoir $\deg 0 < 0$. Pour avoir la propriété que $\deg AB = \deg A + \deg B$, il paraît pratique d'avoir $\deg 0 = \infty$ ou $\deg 0 = -\infty$. Pour avoir la propriété que si A divise B, alors $\deg A \leqslant \deg B$, il paraît pratique d'avoir $\deg 0 = \infty$. En somme, peut-être il vaut mieux laisser le degré du polynôme nul indéfini.

(1) $\operatorname{td} AB = (\operatorname{td} A)(\operatorname{td} B)$,

(2) $\operatorname{cd} AB = (\operatorname{cd} A)(\operatorname{cd} B)$,

(3) $\deg AB = \deg A + \deg B$.

En particulier, le produit de deux polynômes unitaires est unitaire.

Exercice. Prouver la dernière proposition.

Corollaire. *Si* $A, B \in \mathbf{R}[X]$, $A \neq 0$, *et* $B \neq 0$, *alors* $AB \neq 0$.

Corollaire. *Si* $A, B, C \in \mathbf{R}[X]$, $AC = BC$, *et que* $C \neq 0$, *alors* $A = B$.

II.3. Substitution et racines

Définition. Soit

$$A = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

un polynôme dans $\mathbf{R}[X]$, où $a_1, \ldots, a_n \in \mathbf{R}$. Si B est un polynôme[4] dans $\mathbf{R}[X]$, alors le résultat de *substitution* de B dans A pour X est le polynôme noté « $A(B)$ » et défini comme

$$A(B) \overset{\text{déf}}{=} a_0 + a_1 B + a_2 B^2 + \cdots + a_n B^n.$$

En particulier, si $A = a_0 + a_1 X + \cdots + a_n X^n \in \mathbf{R}[X]$ avec $a_1, \ldots, a_n \in \mathbf{R}$, et que $x \in \mathbf{R}$, alors

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

Donc, $A(0) = a_0$, d'où on a :

$$\operatorname{tc} A = A(0).$$

Exemple. Si $A = X^2 + 4X + 4$, alors $A(0) = 4$, $A(1) = 9$, $A(-2) = 0$.

L'opération de substitution peut être complètement caractérisée par les 4 propriétés suivantes :

(1) si A est constant, alors $A(B) = A$,

(2) si $A = X$, alors $A(B) = B$,

(3) $(A + B)(C) = A(C) + B(C)$,

(4) $(AB)(C) = A(C)B(C)$.

[4] Il y a d'autres objets mathématiques qu'on peut substituer pour une indéterminée dans un polynôme, comme, par exemple, des *matrices carrées*, des *opérateurs linéaires*, ou des polynômes en une indéterminée différente, comme $B \in \mathbf{R}[Y]$.

Remarque. Malheureusement, la notation pour la substitution n'est pas vraiment différente de celle pour la multiplication. Par exemple, si $A = X + 1$, alors est-ce que $A(X-1) = (X+1)(X-1) = X^2 - 1$, ou que $A(X-1) = (X-1) + 1 = X$? Est-ce que « $X(X)$ » peut signifier le résultat de substitution de X dans X pour X, donc X ? Ainsi, on est obligé de deviner la signification de telles expressions de leur contexte.

Pour résoudre cette ambiguïté, parfois on adopte la convention de noter les polynômes en X comme « $A(X)$ » plutôt que comme « A », et alors le produit de $A(X)$ et $B(X)$ sera écrit « $A(X)B(X)$ », alors que le résultat de substitution de $B(X)$ dans $A(X)$ sera écrit « $A(B(X))$ ».

Proposition. *Si $A \in \mathbf{R}[X]$ et $B \in \mathbf{R}[X]$ sont polynômes non nuls, et que $\deg B > 0$, alors le polynôme $A(B)$ est non nul, et, en plus* :

(1) $\operatorname{td} A(B) = (\operatorname{cd} A)(\operatorname{td} B)^{\deg A}$,

(2) $\operatorname{cd} A(B) = (\operatorname{cd} A)(\operatorname{cd} B)^{\deg A}$,

(3) $\deg A(B) = (\deg A)(\deg B)$.

Exercice. Prouver cette proposition.

Définition. Un nombre a est dit une *racine* de $B \in \mathbf{R}[X]$ si et seulement si $B(a) = 0$.

Proposition. *Soient $A \in \mathbf{R}[X]$ et $B \in \mathbf{R}[X]$ deux polynômes, et c un nombre. Alors c est une racine AB si et seulement si c est une racine de A ou c est une racine de B.*

Exercice. Prouver cette proposition.

II.4. Divisibilité

Définition. On dit qu'un polynôme $A \in \mathbf{R}[X]$ *divise* un polynôme $B \in \mathbf{R}[X]$ si et seulement si il existe un polynôme $C \in \mathbf{R}[X]$ tel que $B = AC$.

Exemples. Les polynômes $X-1$, $X+1$ et $2-2X^2$ divisent X^2-1, mais X ne le divise pas. Tout polynôme divise 0. Le polynôme 0 ne divise que lui-même. Les polynômes constants non nuls divisent tous les polynômes.

Notation. On utilise la notation « $A \mid B$ » pour dire « A divise B ».

Ainsi on a défini la *relation de divisibilité* ($|$) entre polynômes.

Au lieu de dire que A divise B, on peut dire que B *se factorise* par A, ou encore que A est un *diviseur* de B, ou que B est un *multiple* de A. Voici donc quatre façons différentes d'exprimer une même relation entre A et B, notée « $A \mid B$ » :

(1) A divise B,

(2) B se factorise par A,

(3) A est diviseur de B,

(4) B est multiple de A.

Les deux propriétés suivantes de la relation ($|$) entre des polynômes sont les mêmes que pour la relation ($|$) entre des nombres naturels :

(1) si $A \mid B$ et $B \mid C$, alors $A \mid C$, (2) $A \mid A$.

Exercice. Démontrer les deux propriétés.

Cependant, il n'est pas vrai en général que si $A \mid B$ et $B \mid A$, alors $A = B$. Ce qui est vrai, en revanche, c'est que si $A \mid B$ et $B \mid A$, alors il existe un nombre réel $c \neq 0$ tel que $B = cA$.

Définition. Deux polynômes sont dits *associés* (entre eux) si et seulement chacun des deux divise l'autre.

Exercice. Montrer que deux polynômes A et B sont associés si et seulement si il existe un nombre réel $c \neq 0$ tel que $B = cA$.

Exercice. Montrer que tout polynôme non nul est associé à un unique polynôme unitaire.

Définition. Un *diviseur commun* d'une famille (ou d'un ensemble) de polynômes est la même chose qu'un diviseur commun des membres de cette famille (ou des éléments de cet ensemble) : c'est un polynôme qui est un diviseur de chaque membre de la famille (ou de chaque élément de l'ensemble).

Exemple. Chacun des polynômes

$$X(X-1),\ (X+1)(X-1),\ (X+1)X$$

est un diviseur commun de la famille

$$(X+1)X^2(X-1)^2,\ (X+1)^2X(X-1)^2,\ (X+1)^2X^2(X-1).$$

Définition. Deux polynômes sont dits *premiers entre eux* si et seulement si tout leur diviseur commun divise 1. Au lieu de dire que A et B sont premiers entre eux, on peut aussi dire que A est *premier avec* B.

Autrement dit, deux polynômes sont premiers entre eux si et seulement si ils n'ont pas de diviseurs communs autres que les polynômes constants non nuls.

Exemples. Les polynômes X^2-1 et X^2+2X sont premiers entre eux, mais X^2-1 et X^2+X ne le sont pas.

Définition. Un *multiple commun* d'une famille (ou d'un ensemble) de polynômes est la même chose qu'un multiple commun des membres de cette famille (ou des éléments de cet ensemble) : c'est un polynôme qui est un multiple de chaque membre de la famille (ou de chaque élément de l'ensemble).

Exemple. Chacun des polynômes

$$(X+1)X^2(X-1)^2,\ (X+1)^2X(X-1)^2,\ (X+1)^2X^2(X-1)$$

est un multiple commun de la famille

$$X(X-1),\ (X+1)(X-1),\ (X+1)X.$$

II.5. Division

Soient A et B deux polynômes. On peut tenter de chercher un polynôme C tel que $CA = B$. Si $A \nmid B$, il n'y en a pas. Si $A = B = 0$, alors tout valeur de C convient. Si $A \neq 0$ et que $A \mid B$, alors il y a un et un seul polynôme C tel que $CA = B$.

Définition. Si A est un polynôme non nul et B est un multiple de A, alors l'unique polynôme C tel que $CA = B$ est dit le *quotient* de B par A et est noté « B/A », ou « $A\backslash B$ », ou « $\dfrac{B}{A}$ ». Dans les autres cas, aucun polynôme n'est dit « quotient de B par A ».

Ainsi on a défini l'opération de *division* ($/$) qui à deux polynômes associe leur quotient, tant que leur quotient est défini comme un polynôme.

Exemples. $(X^2 - 1)/(X - 1) = X + 1$, $(X^2 - 1)/(2 - 2X^2) = -1/2$, mais on n'a pas défini la valeur de l'expression « $(X^2 - 1)/X$ » comme un polynôme.[5]

La définition de l'opération de division donnée ci-dessus peut être exprimée par l'équivalence suivante :

$$\frac{B}{A} = C \quad \Leftrightarrow \quad \begin{cases} B = CA \\ A \neq 0 \end{cases}.$$

Remarque. L'opération de division de polynômes définie ici n'est pas complètement « compatible » avec l'opération de substitution : il est une erreur d'écrire « $(A/B)(c) = A(c)/B(c)$ » si $B(c) = 0$. Par exemple, si $A = X^2 - 1$ et $B = X - 1$, alors $A(1) = 0$, $B(1) = 0$, mais $(A/B)(1) = 2$.

II.6. Division euclidienne

Proposition. *Soient $A \in \mathbf{R}[X]$ et $B \in \mathbf{R}[X]$ deux polynômes tels que $B \neq 0$. Alors il existe un unique couple de polynômes $Q \in \mathbf{R}[X]$ et $R \in \mathbf{R}[X]$ tel que :*

$$\begin{cases} A = BQ + R \quad \textit{et} \\ R = 0 \quad \textit{ou} \quad \deg R < \deg B. \end{cases}$$

Exercice. Prouver cette proposition.

Définition. Si $A, B, Q, R \in \mathbf{R}[X]$ sont quatre polynômes tels que $B \neq 0$ et que

$$\begin{cases} A = BQ + R \quad \text{et} \\ R = 0 \quad \text{ou} \quad \deg R < \deg B, \end{cases}$$

alors le polynôme Q est dit le *quotient* de la *division euclidienne* de A par B, et le polynôme R est dit le *reste* de la division euclidienne de A par B.

[5] Plus tard on pourra définir la valeur du quotient « $(X^2 - 1)/X$ » comme une *fraction rationnelle*.

Exemple. Le quotient et le reste de la division euclidienne de X^3 par X^2+X+1 sont $X-1$ et 1, car $X^3=(X^2+X+1)(X-1)+1$ et $\deg 1=0<2=\deg X^2+X+1$.

Voyons sur un exemple comment le quotient et le reste de la division euclidienne d'un polynôme par un autre peuvent être calculés.

Trouvons le quotient et le reste de la division euclidienne de $6X^4-5X^3+4X^2-3X+2$ par $2X^2+1$:

$$\begin{aligned}
&6X^4-5X^3+4X^2-3X+2\\
&=(2X^2+1)3X^2-5X^3+X^2-3X+2\\
&=(2X^2+1)3X^2+(2X^2+1)\left(-\frac{5}{2}X\right)+X^2-\frac{1}{2}X+2\\
&=(2X^2+1)\left(3X^2-\frac{5}{2}X\right)+X^2-\frac{1}{2}X+2\\
&=(2X^2+1)\left(3X^2-\frac{5}{2}X\right)+(2X^2+1)\frac{1}{2}-\frac{1}{2}X+\frac{3}{2}\\
&=(2X^2+1)\left(3X^2-\frac{5}{2}X+\frac{1}{2}\right)-\frac{1}{2}X+\frac{3}{2}.
\end{aligned}$$

Donc, le quotient de la division euclidienne de $6X^4-5X^3+4X^2-3X+2$ par $2X^2+1$ est $3X^2-\frac{5}{2}X+\frac{1}{2}$, et le reste est $-\frac{1}{2}X+\frac{3}{2}$.

Le calcul effectué dans la division euclidienne de $6X^4-5X^3+4X^2-3X+2$ par $2X^2+1$ peut être présenté schématiquement ainsi :

$$\begin{array}{rl|l}
 & 6X^4-5X^3+4X^2-3X+2 & 2X^2+1\\
\cline{3-3}
- & 6X^4\qquad\quad+3X^2 & 3X^2-\frac{5}{2}X+\frac{1}{2}\\
\cline{1-2}
 & -5X^3+X^2-3X+2 & \\
- & -5X^3\qquad\quad-\frac{5}{2}X & \\
\cline{1-2}
 & X^2-\frac{1}{2}X+2 & \\
- & X^2\qquad\quad+\frac{1}{2} & \\
\cline{1-2}
 & -\frac{1}{2}X+\frac{3}{2} &
\end{array}$$

Proposition. *Si $A\in\mathbf{R}[X]$ est un polynôme et $b\in\mathbf{R}$ est un nombre, alors le reste de la division euclidienne de A par $X-b$ est $A(b)$.*

Exercice. Prouver cette proposition.

Corollaire. *Soient $A \in \mathbf{R}[X]$ un polynôme et $b \in \mathbf{R}$ un nombre. Alors b est une racine de A si et seulement si $X - b$ divise A.*

Corollaire. *Le nombre des distinctes racines d'un polynôme non nul de degré n est inférieur ou égal à n.*

Exercice. Prouver ce corollaire.

II.7. 🚧 Division suivant les puissances croissantes

[...]

II.8. Racines multiples

Définition. Un nombre $a \in \mathbf{R}$ est dit une *racine de multiplicité m* de $B \in \mathbf{R}[X]$ si et seulement si $(X - a)^m$ divise B, alors que $(X - a)^{m+1}$ ne divise pas B. Une racine de multiplicité 1 est dite une *racine simple*, une racine de multiplicité 2 est dite une *racine double*.

Autrement dit, $a \in \mathbf{R}$ est une racine de multiplicité m de $B \in \mathbf{R}[X]$ si et seulement si il existe un polynôme $C \in \mathbf{R}[X]$ tel que

$$B = (X - a)^m C \quad \text{et} \quad C(a) \neq 0.$$

Exemple. Soit $A = X^3 - 2X^2 + X = (X - 0)(X - 1)^2$. Alors

(1) 0 est une racine de A de multiplicité 1 (racine simple),

(2) 1 est une racine de A de multiplicité 2 (racine double),

(3) 2 est une racine de A de multiplicité 0 (autrement dit, 2 n'est pas une racine).

Proposition. *Soient $A \in \mathbf{R}[X]$ et $B \in \mathbf{R}[X]$ deux polynômes, et c un nombre. Alors la multiplicité de c comme racine AB est la somme de la multiplicité de c comme racine A et de la multiplicité de c comme racine B.*

Exercice. Prouver cette proposition.

Corollaire. *La somme des multiplicités de toutes les distinctes racines d'un polynôme non nul de degré n est inférieure ou égale à n.*

Exercice. Prouver ce corollaire.

II.9. 🚧 Interpolation de Lagrange

[...]

II.10. PGCD et PPCM

Définition. Soit $\mathcal{A}$ une famille de polynômes. Un polynôme B et dit un *plus grand commun diviseur* (*PGCD*) de la famille $\mathcal{A}$ si et seulement si

(1) B est un diviseur commun de $\mathcal{A}$, et

(2) B est un multiple de tout diviseur commun de $\mathcal{A}$.

Un polynôme B et dit un *plus petit commun multiple* (*PPCM*) de la famille $\mathcal{A}$ si et seulement si

(1) B est un multiple commun de $\mathcal{A}$, et

(2) B est un diviseur de tout multiple commun de $\mathcal{A}$.

Pour une famille (A) à un seul membre A, A est à la fois PGCD et PPCM de (A). De même, pour toute famille de la forme $(A, \dots, A)$ (qui a A pour l'unique membre qui apparaît plusieurs fois), A est un PGCD et un PPCM de cette famille.

Pour la famille vide $()$, le polynôme nul 0 est l'unique PGCD de $()$ (car tout polynôme est un diviseur commun de $()$), et tout polynôme constant non nul est un PPCM de $()$ (car tout polynôme est un multiple commun de $()$).

Si un polynôme A est un membre d'une famille $\mathcal{B}$ et que A divise tout membre de $\mathcal{B}$, alors A est un PGCD de $\mathcal{B}$.

Si un polynôme A est un membre d'une famille $\mathcal{B}$ et que tout membre de $\mathcal{B}$ divise A, alors A est un PPCM de $\mathcal{B}$.

Supposons que $\mathcal{A}$ et $\mathcal{B}$ sont deux familles de polynômes telles que :

(1) chaque polynôme qui apparaît dans $\mathcal{A}$, apparaît aussi dans $\mathcal{B}$, et

(2) chaque polynôme qui apparaît dans $\mathcal{B}$, apparaît aussi dans $\mathcal{A}$.

Alors, évidemment, les deux familles ont les mêmes multiples communs et les mêmes diviseurs communs. D'où, elles ont les mêmes PGCD et les mêmes PPCM.

Par exemple, trouver un PGCD ou un PPCM de la famille

$$1 + 2X + X^2,\ 1 - X^2,\ 1 - X^2,\ 1 + 2X + X^2$$

revient à la même chose que de trouver un PGCD ou un PPCM de la famille

$$1 - X^2,\ 1 + 2X + X^2.$$

Autrement dit, les PPCM et les PGCD d'une famille sont complètement déterminés par l'*ensemble* des membres de cette famille, sans tenir compte des « places » et des nombres d'occurrences.

Exercice. (1) Montrer que si A et B sont deux PGCD d'une même famille, alors A et B sont associés.

(2) Montrer que si A et B sont deux PPCM d'une même famille, alors A et B sont associés.

Exemple. Trouvons un PGCD du couple $(2X^2-2,\ X^2+2X+1)$. Pour cela, observons les égalités suivantes :

$$\begin{aligned} 2X^2-2 &= 2(X^2-1),\\ X^2-1 &= (X^2+2X+1)+(-2X-2),\\ -2X-2 &= (-2)(X+1),\\ X^2+2X+1 &= (X+1)(X+1). \end{aligned}$$

D'après ces égalités, toutes les familles suivantes ont les mêmes diviseurs communs, et donc les mêmes PGCD :

$$\begin{gathered}(2X^2-2,\ X^2+2X+1),\quad (X^2-1,\ X^2+2X+1),\\ (-2X-2,\ X^2+2X+1),\quad (X+1,\ X^2+2X+1),\quad (X+1).\end{gathered}$$

Or, $X+1$ est un PGCD de la famille $(X+1)$. Donc, $X+1$ est un PGCD du couple $(2X^2-2,\ X^2+2X+1)$.

Voici quelques sortes de transformations qu'on peut appliquer à une famille de polynômes sans affecter ses diviseurs communs, et donc sans affecter ses PGCD :

(1) *Permuter* les membres (changer l'ordre ou les places des membres). Par exemple :

$$(A_1, A_2, A_3) \rightsquigarrow (A_3, A_1, A_2).$$

(2) Insérer un membre nul. Par exemple :

$$(A_1, A_2, A_3) \rightsquigarrow (A_1, A_2, A_3, 0).$$

(3) Supprimer un membre nul. Par exemple :

$$(A_1, A_2, A_3, 0) \rightsquigarrow (A_1, A_2, A_3).$$

(4) Insérer un membre qui est une somme de multiples de membres de la famille initiale. Par exemple :

$$(A_1, A_2, A_3) \rightsquigarrow (A_1,\ A_2,\ A_3,\ (X^2-1)A_1 - XA_2 + (A_1 - X^2 + 2)A_3).$$

Ce cas peut être vu comme une généralisation du cas (2).

(5) Supprimer un membre qui est une somme de multiples de certains autres membres. (Ici « autres » veut dire qu'ils apparaissent à d'autres places, mais ils ne sont pas forcement des polynômes différents.) Par exemple :

$$(A_1,\ A_2,\ A_3,\ (X^2-1)A_1 - XA_2 + (A_1 - X^2 + 2)A_3) \rightsquigarrow (A_1, A_2, A_3).$$

Ce cas peut être vu comme une généralisation du cas (3).

(6) Ajouter un multiple d'un membre à un autre. (Ici « autre » veut dire qu'il apparaît à une autre place, mais cela peut être le même polynôme.) Par exemple :

$$(A_1, A_2, A_3) \rightsquigarrow (A_1 - (A_2 - X^2 + 2)A_3,\ A_2,\ A_3).$$

(7) Ajouter une somme de multiples de certains membres à un autre. (Ici « autre » veut dire qu'il apparaît à une autre place que le membres dont on a pris la somme de multiples.) Par exemple :

$$(A_1, A_2, A_3) \rightsquigarrow (A_1 + XA_2 - (A_2 - X^2 + 2)A_3,\ A_2,\ A_3).$$

Ce cas peut être vu comme une généralisation du cas (6).

Ci-dessus, ainsi que dans la suite, une *somme de multiples* d'une famille veut dire une somme d'un nombre arbitraire de multiples (et pas uniquement une somme de *deux* multiples). En plus, tout multiple lui même est considéré comme une *somme de multiples* (il est l'unique terme de cette « somme »).

Lemme. *Soient $\mathcal{A}$ et $\mathcal{B}$ deux familles de polynômes telles que $\mathcal{B}$ est obtenue à partir de $\mathcal{A}$ par une opérations d'une des sept sortes décrites ci-dessus ($\mathcal{A} \rightsquigarrow \mathcal{B}$). Alors les familles $\mathcal{A}$ et $\mathcal{B}$ ont les mêmes diviseurs communs, et donc elles ont les mêmes PGCD.*

Exercice. Prouver ce lemme.

Théorème. *Toute famille de polynômes admet un PGCD.*

Démonstration. La famille vide (), la famille (0), ainsi que toute autre famille dont tous les membres sont 0 (comme $(0, 0, 0)$), a le polynôme 0 comme l'unique PGCD. Ainsi, toute famille qui n'admet pas de PGCD doit avoir au moins un membre non nul.

Supposons qu'il existe une famille de polynômes qui n'admet pas de PGCD.

Soit $\mathcal{A}$ une famille de polynômes qui n'a pas de PGCD et telle que le plus petit degré d'un membre non nul de cette famille soit le plus petit possible.

Soit B un membre non nul de $\mathcal{A}$ du plus petit degré.

D'après le choix de $\mathcal{A}$, si $\mathcal{C}$ est une famille de polynômes qui contient un membre non nul du degré strictement plus petit que $\deg B$, alors $\mathcal{C}$ admet un PGCD.

Si B divise tout membre de $\mathcal{A}$, alors B est un PGCD de $\mathcal{A}$. Or, $\mathcal{A}$ n'a pas de PGCD. Soit alors C un membre de $\mathcal{A}$ tel que B ne divise pas C.

Soient Q et R le quotient et le reste de la division euclidienne de C par B :

$$C = BQ + R, \qquad R \neq 0, \qquad \deg R < \deg B.$$

Soit $\mathcal{D}$ une famille obtenue en insérant R dans la famille $\mathcal{A}$. Alors, d'après le choix de $\mathcal{A}$, la famille $\mathcal{D}$ admet un PGCD. Or,

$$R = 1C - QB,$$

et donc, d'après le lemme précédent, $\mathcal{A}$ et $\mathcal{D}$ ont les mêmes PGCD. On a obtenu une contradiction (car $\mathcal{A}$ n'admet pas de PGCD).

Vu qu'on inévitablement obtient une contradiction après avoir supposé qu'il existe une famille de polynômes sans PGCD, cela montre que toute famille de polynômes possède un PGCD. □

On peut démontrer l'existence d'un PPCM en s'appuyant sur l'existence d'un PGCD.

Théorème. *Toute famille de polynômes admet un PPCM.*

Pour démontrer ce théorème, les deux lemmes suivants seront utiles.

Lemme. *Si* Π *est un ensemble non vide de polynômes, alors il existe un élément de* Π *qui divise tout élément de* Π *qui le divise.*

Démonstration. S'il n'y a qu'un seul polynôme dans Π, alors évidemment il divise tout élément de Π, car il divise soi-même.

S'il y a au moins deux polynôme dans Π, alors au moins un polynôme dans Π est non nul. Soit A un polynôme non nul dans Π du plus petit degré. Considérons un polynôme arbitraire B dans Π qui divise A. Alors $B \neq 0$ et $\deg B = \deg A$. Donc, A/B est un polynôme non nul du degré 0, c'est-à-dire, A/B est un réel non nul. D'où, $B = (1/(A/B))A$, où $(1/(A/B))$ est un réel non nul, et donc A divise B. Ainsi, A divise tout polynôme dans Π qui divise A. □

Lemme. *Soient* $\mathcal{A}$ *et* $\mathcal{B}$ *deux familles de polynômes telles que chaque membre de* $\mathcal{A}$ *divise chaque membre de* $\mathcal{B}$*. Alors tout membre de* $\mathcal{A}$ *divise tout PGCD de* $\mathcal{B}$*.*

Démonstration. Tout membre de $\mathcal{A}$ est un diviseur commun de $\mathcal{B}$, donc, il divise tout PGCD de $\mathcal{B}$. □

Démonstration du théorème d'existence du PPCM. Soit $\mathcal{A}$ une famille de polynômes. Évidemment, 0 est un multiple commun de $\mathcal{A}$. Soit B un multiple commun de $\mathcal{A}$ qui divise tout multiple commun de $\mathcal{A}$ qui le divise. (Un tel B existe d'après un des lemmes précédents.) Montrons que B est un PPCM de $\mathcal{A}$. Pour cela il ne reste qu'à prouver que B divise tout multiple commun de $\mathcal{A}$.

Soit C un multiple commun arbitraire de $\mathcal{A}$. Soit D un PGCD de la famille (B, C). (On sait, grâce au théorème précédent, qu'un PGCD de (B, C) existe.) D'après le dernier lemme, D est un multiple commun de $\mathcal{A}$. Cependant, D divise B. Alors, d'après le choix de B, B divise D. Comme B divise D et D divise C, B divise C. □

Exemple. Trouvons un PPCM du couple $(2X^2 - 2,\ X^2 + 2X + 1)$. Observons que

$$\begin{aligned}(2X^2 - 2)\frac{1}{2}(X + 1) &= X^3 + X^2 - X - 1,\\ (X^2 + 2X + 1)(X - 1) &= X^3 + X^2 - X - 1.\end{aligned}$$

Donc, $X^3 + X^2 - X - 1$ est un multiple commun de $(2X^2 - 2,\ X^2 + 2X + 1)$, et donc tout PPCM de $(2X^2 - 2,\ X^2 + 2X + 1)$ divise $X^3 + X^2 - X - 1$. Il est facile de montrer que tous les multiples communs de $(2X^2 - 2,\ X^2 + 2X + 1)$ sont non nuls et de degré au moins 3. Soit A un n'importe quel PPCM de $(2X^2 - 2,\ X^2 + 2X + 1)$ (il existe d'après le théorème). Alors $A \neq 0$, $\deg A \geqslant 3$, et $A \mid X^3 + X^2 - X - 1$. Cela n'est possible que si A et $X^3 + X^2 - X - 1$ sont associés. Donc, $X^3 + X^2 - X - 1$ est un PPCM de $(2X^2 - 2,\ X^2 + 2X + 1)$.

Il existe cependant une méthode plus directe pour calculer efficacement le PPCM de deux polynômes, la voici. On peut prouver, en utilisant le *lemme de Bézout*, que si $C \neq 0$ est un PGCD de (A, B), alors AB/C est un PPCM de (A, B).

Notation. Pour toute famille de polynômes $(A_1, \dots, A_n)$, on va noter « $\operatorname{pgcd}(A_1, \dots, A_n)$ » l'unique PGCD unitaire de $(A_1, \dots, A_n)$ s'il existe, et « $\operatorname{ppcm}(A_1, \dots, A_n)$ » l'unique PPCM unitaire de $(A_1, \dots, A_n)$ s'il existe. En revanche, si 0 est l'unique PGCD de $(A_1, \dots, A_n)$, alors on va poser $\operatorname{pgcd}(A_1, \dots, A_n) \overset{\text{déf}}{=} 0$, et si 0 est l'unique PPCM de $(A_1, \dots, A_n)$, alors on va poser $\operatorname{ppcm}(A_1, \dots, A_n) \overset{\text{déf}}{=} 0$.

II.11. Algorithme d'Euclide

Pour trouver un PGCD de deux polynômes, on peut utiliser l'*algorithme d'Euclide*, qui utilise la division euclidienne.

Soient A et B deux polynômes dont on cherche un PGCD. Posons

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

Si $R_1 = B = 0$, alors $R_0 = A$ est un PGCD de A et B. Sinon, posons Q_2 et R_2 le quotient et le reste de la division euclidienne de $R_0 = A$ par $R_1 = B$:

$$A = BQ_2 + R_2, \qquad R_2 = 0 \quad \text{ou} \quad \deg R_2 < \deg B.$$

Ainsi,

$$R_0 = R_1Q_2 + R_2, \qquad R_2 = 0 \quad \text{ou} \quad \deg R_2 < \deg R_1.$$

Si $R_2 \neq 0$, on calcule le quotient Q_3 et le reste R_3 de la division euclidienne de $R_1 = B$ par R_2 :

$$R_1 = B = R_2Q_3 + R_3, \qquad R_3 = 0 \quad \text{ou} \quad \deg R_3 < \deg R_2.$$

On continue ainsi et détermine les quotients Q_{k+2} et les restes R_{k+2} *par récurrence* :

$$R_k = R_{k+1}Q_{k+2} + R_{k+2}, \qquad R_{k+2} = 0 \quad \text{ou} \quad \deg R_{k+2} < \deg R_{k+1}.$$

On finira par trouver n tel que $R_{n+2} = 0$ et donc R_{n+1} divise R_n :

$$R_n = R_{n+1}Q_{n+2}, \qquad R_{n+2} = 0.$$

Alors R_{n+1} sera un PGCD de (A, B). En effet, les familles suivantes ont toutes les mêmes diviseurs communs, et donc les mêmes PGCD :

$$(R_0, R_1), \quad (R_1, R_2), \quad \dots \quad (R_n, R_{n+1}), \quad (R_{n+1}).$$

II.12. Lemme de Bézout

En développant légèrement la démonstration de l'existence de PGCD donnée dans la section II.10, on peut montrer que pour toute famille de polynômes, il y a une somme de multiples de membres de cette famille qui est un PGCD de cette famille. Ce fait est connu sous le nom de *lemme de Bézout* (parmi d'autres).

Lemme (Lemme de Bézout)**.** *Si $A_1, \dots, A_n$ sont des polynômes, $n \geqslant 1$, et que B est un PGCD de la famille $(A_1, \dots, A_n)$, alors il existe des polynômes $S_1, \dots, S_n$ tels que*

$$B = A_1S_1 + \cdots + A_nS_n.$$

Introduisons la notation suivante pour s'en servir dans la démonstration de ce lemme :

Notation. Pour toute famille de polynômes $(A_1, \dots, A_n)$ qui a au moins un membre non nul, notons « $\operatorname{mindeg}(A_1, \dots, A_n)$ » le plus petit nombre parmi les degrés des polynômes non nuls parmi $A_1, \dots, A_n$.

Par exemple :

$$\operatorname{mindeg}(X^3 + X,\ 0,\ X - X^2) = 2, \qquad \operatorname{mindeg}(X^3 + X,\ 2,\ X - X^2) = 0.$$

Démonstration du lemme de Bézout. Ici, si $(A_1, \dots, A_n)$ est une famille de polynômes, B est un PGCD de $(A_1, \dots, A_n)$, et qu'on dit que la conclusion du lemme de Bézout est satisfaite pour $(A_1, \dots, A_n)$ et B, cela veut dire qu'il existe des polynômes $S_1, \dots, S_n$ tels que $B = A_1S_1 + \cdots + A_nS_n$. Démontrer le lemme revient à démontrer que sa conclusion est satisfaite toute famille de polynômes $(A_1, \dots, A_n)$, $n \geqslant 1$, et pour tout PGCD de cette famille.

Observons que si la conclusion du lemme est satisfaite pour une famille $(A_1, \dots, A_n)$, $n \geqslant 1$, et pour un PGCD B de cette famille, et que $(C_1, \dots, C_n)$ est une famille obtenue de $(A_1, \dots, A_n)$ par une *permutation* (changement de l'ordre des membres), alors B est un PGCD de $(C_1, \dots, C_n)$, et en plus la conclusion du lemme est satisfait pour $(C_1, \dots, C_n)$ et B.

Pour toute famille dont tous les membres sont 0 (comme $(0, 0, 0)$) et pour son unique PGCD 0, la conclusion du lemme de Bézout est clairement satisfaite. Par exemple : $0 \cdot 0 + \cdots + 0 \cdot 0 = 0$.

Ainsi, si la conclusions du lemme n'est pas satisfaite pour une certaine famille de polynômes $(A_1, \dots, A_n)$, $n \geqslant 1$, et pour un certain PGCD de cette famille, alors parmi $A_1, \dots, A_n$ il y a au moins un polynôme non nul.

Afin de démontrer le lemme par un raisonnement *par l'absurde*, supposons qu'il existe une famille de polynômes $(A_1, \dots, A_n)$, $n \geqslant 1$, et un PGCD de cette famille pour lesquels la conclusion n'est pas satisfaite.

Soient $(A_1, \dots, A_n)$ une famille de polynômes, $n \geqslant 1$, et B un PGCD de cette famille pour lesquels la conclusion du lemme n'est pas satisfaite, et tels que $\operatorname{mindeg}(A_1, \dots, A_n)$ soit le plus petit possible.

Sans perte de généralité, supposons que $A_1 \neq 0$ et que le degré de A_1 est le plus petit parmi les degrés de tout les membres non nuls de $(A_1, \dots, A_n)$:

$$\deg A_1 = \operatorname{mindeg}(A_1, \dots, A_n).$$

Supposons que A_1 est un diviseur commun de $(A_1, \dots, A_n)$. Alors A_1 divise B. (En fait, A_1 dans ce cas est un PGCD de $(A_1, \dots, A_n)$, et donc A_1 et B sont associés.) Soit Q un polynôme tel que $B = A_1 Q$. (En fait, Q est un polynôme constant non nul.) Alors, comme

$$B = A_1 Q + A_2 \cdot 0 + \cdots + A_n \cdot 0,$$

la conclusion du lemme est satisfaite pour $(A_1, \dots, A_n)$ et B. Or, la conclusion du lemme n'est pas satisfaite pour $(A_1, \dots, A_n)$ et B (c'est ce qu'on suppose). Comme on est arrivé à une contradiction après avoir supposé que A_1 est un diviseur commun de $(A_1, \dots, A_n)$, on conclut que A_1 n'est pas un diviseur commun de $(A_1, \dots, A_n)$.

Donc, parmi les polynômes $A_2, \dots, A_n$ il y en a au moins un qui n'est pas multiple de A_1. Sans perte de généralité, supposons que A_2 n'est pas multiple de A_1.

Soient Q et R le quotient et le reste de la division euclidienne de A_2 par A_1 :

$$A_2 = A_1 Q + R, \qquad R \neq 0, \qquad \deg R < \deg A_1.$$

Alors

$$R = A_2 \cdot 1 - A_1 Q.$$

D'après un lemme de la section II.10, les familles $(A_1, \dots, A_n)$ et $(A_1, \dots, A_n, R)$ ont les mêmes PGCD, donc B est un PGCD de $(A_1, \dots, A_n, R)$.

Comme

$$\operatorname{mindeg}(A_1, \dots, A_n, R) = \deg R < \deg A_1 = \operatorname{mindeg}(A_1, \dots, A_n),$$

la conclusion du lemme de Bézout est satisfaite pour $(A_1, \dots, A_n, R)$ et B.

Soient des polynômes $T_1, \dots, T_{n+1}$ tels que

$$B = A_1 T_1 + \cdots + A_n T_n + R T_{n+1}.$$

Or,

$$\begin{aligned} B = A_1 T_1 + \cdots + A_n T_n + R T_{n+1} &= A_1 T_1 + \cdots + A_n T_n + (A_2 - A_1 Q) T_{n+1} \\ &= A_1 (T_1 - Q T_{n+1}) + A_2 (T_2 + 1) + A_3 T_3 + \cdots + A_n T_n. \end{aligned}$$

Donc, la conclusion du lemme est satisfait pour $(A_1, \dots, A_n)$ et B. On a obtenu une contradiction.

Vu qu'on inévitablement obtient une contradiction après avoir supposé qu'il existe une famille de polynômes $(A_1, \dots, A_n)$, $n \geqslant 1$, et un PGCD de cette famille pour lesquels la conclusion du lemme de Bézout n'est pas satisfaite, cela montre que la conclusion du lemme de Bézout est satisfaite pour toute famille de polynômes $(A_1, \dots, A_n)$, $n \geqslant 1$, et pour tout PGCD de cette famille, ce qui signifie que le lemme de Bézout est vrai. □

Utilisons le lemme de Bézout pour déduire quelques faits utiles.

Lemme. *Si A et B sont deux polynômes premiers entre eux, et que C est un multiple commun de A et B, alors AB divise C.*

Démonstration. Soient U et V deux polynômes tels que $AU = BV = C$. Soient S et T deux polynômes tels que $AS + BT = 1$ (ils existent d'après le lemme de Bézout). Alors

$$C = (AS + BT)C = ASC + BTC = ASBV + BTAU = AB(SV + TU). \qquad \square$$

Corollaire. *Si A et B sont deux polynômes premiers entre eux, alors AB est un PPCM de A et B.*

Lemme. *Si A et B sont deux polynômes, C est un PGCD de A et B, et que D est un multiple commun de A et B, alors AB divise CD.*

Démonstration. Soient U et V deux polynômes tels que $AU = BV = D$. Soient S et T deux polynômes tels que $AS + BT = C$ (ils existent d'après le lemme de Bézout). Alors

$$CD = (AS + BT)D = ASD + BTD = ASBV + BTAU = AB(SV + TU). \qquad \square$$

Corollaire. *Si A et B sont deux polynômes, et que $C \neq 0$ est un de leurs PGCD, alors AB/C est un PPCM de A et B.*

Démonstration. Soient U et V deux polynômes tels que $A = CU$, $B = CV$. Alors $AB/C = UCV = AV = UB$, donc, $AB/C = UCV$ est un multiple commun de A et B.

D'après le lemme précédent, si D est un multiple commun de A et B, alors AB divise CD, et donc, comme $C \neq 0$, AB/C divise D. Donc, AB/C est un PPCM de A et B. $\square$

II.13. Polynômes irréductibles et factorisation

Tout polynôme divise le polynôme nul, mais le polynôme nul ne divise que lui-même.

Tout polynôme constant non nul divise tous les polynômes, mais les seuls polynômes qui divisent un polynôme constant non nul sont les polynômes constants non nuls.

Ainsi, en ce qui concerne la relation de divisibilité sur $\mathbf{R}[X]$, le polynôme nul et les polynômes constants non nuls sont « les plus singuliers ».[6]

Les polynômes qui ne sont pas nul, ni constants non nuls, sont repartis en ceux qui s'appellent *réductibles* et ceux qui s'appellent *irréductibles*.

Définition. Un polynôme A est dit *réductible* si et seulement si

(1) A n'est pas nul, ni constant non nul, et

(2) il existe deux polynômes B et C tels que $A = BC$ et ni B, ni C n'est constant non nul.

[6] La relation de divisibilité ($|$) sur les polynômes est une *relation de préordre*. Par rapport à ce préordre, le polynôme 0 est l'élément *le plus grand* de $\mathbf{R}[X]$, et les polynômes constants non nuls sont les éléments *les plus petits* de $\mathbf{R}[X]$.

Définition. Un polynôme A est dit *irréductible* si et seulement si

(1) A n'est pas nul, ni constant non nul, et

(2) A n'est pas réductible.

Ainsi, un polynôme A est irréductible si et seulement si

(1) A ne divise pas 1 (autrement dit, n'est pas constant non nul), et

(2) les seuls polynômes qui divisent A sont les polynômes qui divisent 1 (les polynômes constants non nuls) et les polynômes associés à A.

Exemple. Les polynôme $X^2-1=(X-1)(X+1)$ et $X^3+1=(X+1)(X^2-X+1)$ sont réductibles, alors que les polynômes $X-1$, $X+1$ et X^2+1 sont irréductibles (dans $\mathbf{R}[X]$).

Remarque. Plutôt que dire qu'un certain polynôme est réductible ou irréductible, il est plus exact de dire qu'il est réductible ou irréductible *dans* $\mathbf{R}[X]$, car la propriété d'être réductible ou irréductible dépend de l'ensemble des polynômes qu'on considère. La définition donnée ci-dessus sous-entend qu'on parle de l'ensemble $\mathbf{R}[X]$ des polynômes à coefficients réels, mais on peut donner des définitions analogiques pour l'ensemble $\mathbf{Z}[X]$ des polynômes à coefficients entiers, pour l'ensemble $\mathbf{Q}[X]$ des polynômes à coefficients rationnels, pour l'ensemble $\mathbf{C}[X]$ des polynômes à coefficients *complexes*, et ainsi de suite. Ainsi, par exemple, le polynôme X^2-2 est réductible dans $\mathbf{R}[X]$ mais irréductible dans $\mathbf{Z}[X]$ et dans $\mathbf{Q}[X]$, alors que le polynôme X^2+1 est irréductible dans $\mathbf{R}[X]$ mais réductible dans $\mathbf{C}[X]$.

Proposition. *Tout polynôme réductible peut être écrit comme un produit de polynômes irréductibles.*

Exercice. Prouver cette proposition.

Lemme. *Si A et B sont deux polynômes (dans $\mathbf{R}[X]$) et P est un polynôme irréductible (dans $\mathbf{R}[X]$) qui divise AB, alors P divise A ou P divise B.*

Démonstration. Supposons que P ne divise pas A. Alors P est premier avec A. Soient S et T deux polynômes tels que $PS+AT=1$ (ils existent d'après le *lemme de Bézout*). Soit Q un polynôme tel que $AB=PQ$. Alors

$$B=(PS+AT)B=PSB+ABT=PSB+PQT=P(SB+QT),$$

et donc P divise B. □

Définition. Un polynôme $P\in\mathbf{R}[X]$ est dit *premier* dans $\mathbf{R}[X]$ si et seulement si quels que soient deux polynômes non nuls et non constants $A,B\in\mathbf{R}[X]$ tels que P divise le produit AB, on a que P divise A ou P divise B.

D'après le lemme précédent, un polynôme est premier dans $\mathbf{R}[X]$ si et seulement si il est irréductible dans $\mathbf{R}[X]$. Ainsi, dans le cas de $\mathbf{R}[X]$ (comme que dans le cas de $\mathbf{Z}$), dire qu'un élément est premier revient à la même chose que dire qu'il est irréductible.

Lemme. *Si $P, Q_1, \ldots, Q_n$ sont des polynômes irréductibles tels que P divise le produit $Q_1 \cdots Q_n$, alors il existe un indice i (entre 1 et n) tel que P est associé à Q_i.*

Démonstration. Posons

$$A_0 = 1, \quad A_1 = Q_1, \quad A_2 = Q_1Q_2, \quad A_3 = Q_1Q_2Q_3, \quad \ldots, \quad A_n = Q_1 \cdots Q_n.$$

Comme P ne divise pas A_0 mais divise A_n, il existe k entre 1 et n tel que P ne divise pas A_{k-1} mais divise A_k.

Soit k un indice entre 1 et n tel que P ne divise pas A_{k-1} mais divise $A_k = A_{k-1}Q_k$. Alors, d'après le lemme précédent, P divise Q_k, et donc P est associé à Q_k. □

Notation. Si P est un polynôme irréductible et que A est un polynôme non nul, on va noter[7] « $\nu_P A$ » le plus grand nombre naturel n tel que P^n divise A.

Observons que si P et Q sont deux polynômes irréductibles, alors

$$\nu_P Q = \begin{cases} 1 & \text{si } P \text{ et } Q \text{ sont associés,} \\ 0 & \text{sinon.} \end{cases}$$

Proposition. *Si P est un polynôme irréductible et A et B sont deux polynômes non nuls, alors*

$$\nu_P(AB) = \nu_P A + \nu_P B.$$

Démonstration. Posons $m = \nu_P A$ et $n = \nu_P B$. Soient C et D les polynômes tels que $A = P^m C$ et $B = P^n D$. Alors P ne divise ni C, ni D. Donc, d'après un lemme précédent, P ne divise pas CD. Or, $AB = P^{m+n}CD$. D'où, $\nu_P(AB) = m + n = \nu_P A + \nu_P B$. □

Ainsi, si $A_1, \ldots, A_m$ et $B_1, \ldots, B_n$ sont des polynômes non nuls tels que

$$A_1 \cdots A_m = B_1 \cdots B_n,$$

alors, pour tout polynôme irréductible P,

$$\nu_P A_1 + \cdots + \nu_P A_m = \nu_P B_1 + \cdots + \nu_P B_n.$$

Corollaire. *Si P et $Q_1, \ldots, Q_n$ sont des polynômes irréductibles et que $A = Q_1 \cdots Q_n$, alors $\nu_P A$ est le nombre d'occurrences de polynômes associés à P dans la suite $Q_1, \ldots, Q_n$.*

Exercice. Prouver ce corollaire.

[7] Par ailleurs, on peut définir une *fonction* ν_P de manière que $\nu_P A$ soit le résultat de l'application de ν_P à A et que cette fonction ν_P soit un exemple de ce qui en algèbre est dit une *valuation*.

Corollaire. *Si $P_1, \dots, P_m$ et $Q_1, \dots, Q_n$ sont des polynômes irréductibles unitaires tels que*

$$P_1 \cdots P_m = Q_1 \cdots Q_n,$$

alors $m = n$, et l'expression « $P_1 \cdots P_m$ » ne diffère de l'expression « $Q_1 \cdots Q_n$ » que par l'ordre des facteurs.

Exercice. Prouver ce corollaire.

II.14. Congruences

Définition. Soient A, B, C trois polynômes. On dit que A est *congru* à B suivant le *module* C, ou *modulo* C, si et seulement si il existe un polynôme D tel que

$$A = B + CD.$$

Autrement dit, deux polynômes A et B sont congrus modulo un polynôme C si et seulement si C divise $A - B$.

Notation. On va écrire « $A \underset{C}{\equiv} B$ » pour dire « A est congru à B modulo C ».

Ainsi, pour tout polynôme M, on a défini la relation $(\underset{M}{\equiv})$ entre polynômes, qui est dite la *relation de congruence modulo* M.

Lorsque le polynôme module M sera précisé dans le contexte, on pourra écrire « $A \equiv B$ » tout court au lieu de « $A \underset{M}{\equiv} B$ », par exemple :

$$X^2 \equiv -1 \pmod{1 + X^2}.$$

En écriture mathématique contemporaine, il est courant d'abréger « modulo » comme « mod », sans point. Par exemple :

$$X^2 \equiv -1 \pmod{1 + X^2}.$$

Note étymologique. Le mot « module » vient du latin « *modulus* », qui est la forme diminutive de « *modus* » (qui peut se traduire comme « mesure », « rythme », « borne », « limite », « mode »). Voici le tableau de déclinaison de « *modulus* » en latin :

	Singulier	Pluriel
Nominatif	modulus	modulī
Vocatif	module	modulī
Accusatif	modulum	modulōs
Génitif	modulī	modulōrum
Datif	modulō	modulīs
Ablatif	modulō	modulīs

Proposition. *Les propriétés suivantes sont satisfaites pour tous polynômes M, A, B, C :*

(1) *si* $A \underset{M}{\equiv} B \underset{M}{\equiv} C$, *alors* $A \underset{M}{\equiv} C$,

(2) $A \underset{M}{\equiv} A$,

(3) *si* $A \underset{M}{\equiv} B$, *alors* $B \underset{M}{\equiv} A$.

Exercice. Prouver cette proposition.

Proposition. *Soient* M, A_1, A_2, B_1, B_2 *des polynômes tels que* $A_1 \underset{M}{\equiv} A_2$ *et* $B_1 \underset{M}{\equiv} B_2$. *Alors* :

(1) $A_1 + B_1 \underset{M}{\equiv} A_2 + B_2$, (2) $A_1 - B_1 \underset{M}{\equiv} A_2 - B_2$, (3) $A_1 B_1 \underset{M}{\equiv} A_2 B_2$.

Exercice. Prouver cette proposition.

Lemme. *Si* A *et* B *sont deux polynômes et que* R *est le reste d'une division euclidienne de* A *par* B, *alors* $A \underset{B}{\equiv} R$.

Exercice. Prouver ce lemme.

Exercice. Soit (Δ) une relation entre des polynômes telle que :

(1) si $A \mathrel{\Delta} B \mathrel{\Delta} C$, alors $A \mathrel{\Delta} C$,

(2) $A \mathrel{\Delta} A$,

(3) si $A \mathrel{\Delta} B$, alors $B \mathrel{\Delta} A$,

(4) si $A_1 \mathrel{\Delta} A_2$ et $B_1 \mathrel{\Delta} B_2$, alors $A_1 + B_1 \mathrel{\Delta} A_2 + B_2$, $A_1 - B_1 \mathrel{\Delta} A_2 - B_2$, et $A_1 B_1 \mathrel{\Delta} A_2 B_2$.

Montrer qu'il existe un polynôme M tel que la relation (Δ) est la congruence modulo M. (Autrement dit : montrer qu'il existe $M \in \mathbf{R}[X]$ tel que $(\underset{M}{\equiv}) = (\Delta)$.)

Définition. Une *congruence* sur les polynômes[8] est une relation (Δ) entre des polynômes telle que :

(1) si $A \mathrel{\Delta} B \mathrel{\Delta} C$, alors $A \mathrel{\Delta} C$,

(2) $A \mathrel{\Delta} A$,

(3) si $A \mathrel{\Delta} B$, alors $B \mathrel{\Delta} A$,

(4) si $A_1 \mathrel{\Delta} A_2$ et $B_1 \mathrel{\Delta} B_2$, alors $A_1 + B_1 \mathrel{\Delta} A_2 + B_2$, $A_1 - B_1 \mathrel{\Delta} A_2 - B_2$, et $A_1 B_1 \mathrel{\Delta} A_2 B_2$.

[8] La notion de *congruence* sur les polynômes est un cas spécial d'une notion générale de *congruence* sur une *structure algébrique*.

II.15. Classes de congruence

Définition. Soit M un polynôme. Définissons les *classes de congruence* de polynômes modulo M ainsi :

(1) à tout polynôme A, on associe sa *classe de congruence* modulo M, notée « $[A]_M$ »[9] ;

(2) si A et B sont deux polynômes, on admet que les *classes de congruence* de A et de B modulo M coïncident si et seulement si A est congru à B modulo M :

$$[A]_M = [B]_M \quad \Leftrightarrow \quad A \underset{M}{\equiv} B\,;$$

(3) toute *classe de congruence* modulo M est la classe de congruence modulo M d'un polynôme (c'est-à-dire, elle est de la forme $[A]_M$, où A est un polynôme).

Remarque. Souvent on donne une définition différente des classes de congruence, en les *réalisant* comme des *ensembles* : on dit que la *classe de congruence* de A modulo M est l'ensemble de tous les polynômes congrus à A modulo M. En pratique, en tant que les propriétés algébriques sont concernées, cette définition équivaut la nôtre.

Notation. Lorsque le polynôme module M sera précisé dans le contexte, on pourra écrire « $[A]$ » au lieu de « $[A]_M$ ».

Définition. Soit M un polynôme. Soient α et β deux classes de congruence de polynômes modulo M. On définit la *somme* $\alpha+\beta$, la *difference* $\alpha-\beta$ et le *produit* $\alpha\beta$ ainsi : si A et B sont deux polynômes tels que $\alpha = [A]_M$ et $\beta = [B]_M$, alors

(1) $\alpha+\beta = [A]_M + [B]_M \overset{\text{déf}}{=} [A+B]_M$,

(2) $\alpha-\beta = [A]_M - [B]_M \overset{\text{déf}}{=} [A-B]_M$,

(3) $\alpha\beta = [A]_M[B]_M \overset{\text{déf}}{=} [AB]_M$.

Exercice. Montrer que pour tout polynôme M, les définitions données de l'*addition*, de la *soustraction* et de la *multiplication* des classes de congruence de polynômes modulo M sont correctes et complètes.

Remarque. Il existe une pratique d'écrire « A » tout court à la place de « $[A]_M$ » ou « $[A]$ » lorsque le contexte permet de comprendre qu'il s'agit d'une classe de congruence de polynômes modulo M. Ainsi, on peut rencontrer des formules comme celle-là :

$$\text{« } (1+X)(1-X) = 2 \mod 1+X^2 \text{ ».}$$

Cette formule doit alors être lue comme

$$\text{« } [1+X]_{1+X^2} \cdot [1-X]_{1+X^2} = [2]_{1+X^2} \text{ ».}$$

Proposition. *Soit M un polynôme et soient α, β, γ des classes de congruence de polynômes modulo M. Alors les identités suivantes sont satisfaites* :

[9] La notation « $\bar{A}_M$ » au lieu de « $[A]_M$ » peut aussi être rencontrée.

(1) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$,

(2) $\alpha + [0]_M = \alpha = [0]_M + \alpha$,

(3) $\beta + \alpha = \alpha + \beta$,

(4) $(\alpha - \beta) + \beta = \alpha$,

(5) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$,

(6) $\alpha[1]_M = \alpha = [1]_M\alpha$,

(7) $\beta\alpha = \alpha\beta$,

(8) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

Exercice. Prouver cette proposition.

Exercice. Est-il vrai que si α et β sont deux classes de congruence de polynômes modulo un polynôme M telles que $\alpha \neq [0]_M$ et $\beta \neq [0]_M$, alors $\alpha\beta \neq [0]_M$?

II.16. 🚧 Nombres complexes comme classes de congruence

[...]

II.17. Polynômes en plusieurs indéterminées

Définition. Définissons les *monômes unitaires* en *indéterminées* $X_1, \ldots, X_n$ ainsi :

(A) Le nombre 1 est un *monôme unitaire*.

(B) Il y a n *monômes unitaires* distingués $X_1, \ldots, X_n$, dit les *indéterminées*.

(C) L'opération de multiplication est définie pour tous les *monômes unitaires* : si A et B sont deux *monômes unitaires*, alors AB est un *monôme unitaire* aussi. En plus, les 3 identités suivantes sont satisfaites pour tous *monômes unitaires* A, B, C :

(1) $A(BC) = (AB)C$, (2) $A \cdot 1 = A = 1 \cdot A$, (3) $BA = AB$.

(D) Tout *monôme unitaire* A en *indéterminées* $X_1, \ldots, X_n$ s'écrit comme

$$A = X_1^{e_1} X_2^{e_2} \cdots X_n^{e_n},$$

où les exposantes $e_1, e_2, \ldots, e_n$ sont des nombres naturels.

(E) Si $d_1, d_2, \ldots, d_n$ et $e_1, e_2, \ldots, e_n$ sont des nombres naturels tels que

$$X_1^{d_1} X_2^{d_2} \cdots X_n^{d_n} = X_1^{e_1} X_2^{e_2} \cdots X_n^{e_n},$$

alors $d_1 = e_1,\ d_2 = e_2,\ \ldots,\ d_n = e_n$.

Définition. Définissons les *polynômes* en *indéterminées* $X_1, \ldots, X_n$ à *coefficients* réels, parfois appelés *polynômes* tout court, ainsi :

(A) Tout nombre réel est un *polynôme*, dit *polynôme constant*.[10]

(B) Tout monôme unitaire en indéterminées $X_1, \dots, X_n$ est un *polynôme* en *indéterminées* $X_1, \dots, X_n$.

(C) Les opérations d'addition, de soustraction et de multiplication sont définies pour tous les *polynômes* : si A et B sont *polynômes*, alors $A+B$, $A-B$ et AB sont *polynômes* aussi. En plus, les 8 identités suivantes sont satisfaites pour tous *polynômes* A, B, C :

(1) $A + (B + C) = (A + B) + C$,

(2) $A + 0 = A = 0 + A$,

(3) $B + A = A + B$,

(4) $A + (B - A) = B$,

(5) $A(BC) = (AB)C$,

(6) $A \cdot 1 = A = 1 \cdot A$,

(7) $BA = AB$,

(8) $A(B + C) = AB + AC$.

(D) Tout *polynôme* A en *indéterminées* $X_1, \dots, X_n$ s'écrit comme

$$A = a_1U_1 + a_2U_2 + \cdots + a_kU_k,$$

où $U_1, U_2, \dots, U_k$ sont des monômes unitaires en indéterminées $X_1, \dots, X_n$, et $a_1, a_2, \dots, a_k$ sont des nombres réels.

(E) Si $U_1, U_2, \dots, U_k$ sont des monômes unitaires en indéterminées $X_1, \dots, X_n$ différents deux à deux, et $a_1, a_2, \dots, a_k$ sont des nombres réels tels que

$$a_1U_1 + a_2U_2 + \cdots + a_kU_k = 0,$$

alors $a_1 = a_2 = \cdots = a_k = 0$.

Notation. L'ensemble des polynômes en indéterminées $X_1, \dots, X_n$ à coefficients dans $\mathbf{R}$ (réels) est noté « $\mathbf{R}[X_1, \dots, X_n]$ ».

Définition. Un *monôme* en *indéterminées* $X_1, \dots, X_n$ à *coefficient* réel est un polynôme de la forme $aX_1^{e_1} \cdots X_n^{e_n}$, où les exposants $e_1, \dots, e_n$ sont des nombres naturels et où a est un nombre réel non nul, dit le *coefficient* de ce monôme.

Ainsi, d'après les définitions précédentes, les monômes sont les multiples des monômes unitaires par des nombres réels non nuls.

Exemples. (1) Voici quelques monômes unitaires en X, Y, Z : 1, X, Y, XY, X^2YZ.

(2) Voici quelques monômes en X, Y, Z à coefficients réels qui ne sont pas unitaires : 3, $-X$, $Y/2$, $\sqrt{2}X^2Z^3$.

[10] Peut-être il serait plus approprié de l'appeler *polynôme scalaire* – voir la note 1 pour *polynôme constant* en une indéterminée.

(3) Voici quelques polynômes en X, Y, Z à coefficients réels qui ne sont pas monômes : $1 + X + Y$, $XY + YZ - 2Y^2$, 0.

Remarque. La notion des monômes unitaires semble être plus utile que la notion des monômes à coefficients réels. Certains auteurs utilisent le terme *monôme* exclusivement pour les monômes unitaires.

Définition. Soit un polynôme

$$A = a_1U_1 + a_2U_2 + \cdots + a_kU_k,$$

où $U_1, U_2, \ldots, U_k$ sont des monômes unitaires en indéterminées $X_1, \ldots, X_n$ différents deux à deux, et $a_1, a_2, \ldots, a_k$ sont des nombres réels.

(1) Le nombre a_i est dit le *coefficient* de A auprès de U_i.

(2) Ceux des monômes $a_1U_1, a_2U_2, \ldots, a_kU_k$ qui ne sont pas nuls sont dits *termes* de A.

(3) Si A a un terme de la forme $aX_1^0 \cdots X_n^0 = a$, avec a un reel non nul, alors ce terme est dit le *terme constant*[11] de A. Si aucun des termes de A n'est un nombre réel, on peut dire que A n'a pas de *terme constant*. Cependant, souvent il peut être pratique de dire exceptionnellement dans ce cas que le *terme constant* de A est 0.

Définition. Soit

$$A = X_1^{e_1} \cdots X_n^{e_n}$$

un monôme unitaire en indéterminées $X_1, \ldots, X_n$. Si $B_1, \ldots, B_n$ sont des polynômes[12] (peu importe en quels indéterminées), alors le résultat de *substitution* de $B_1, \ldots, B_n$ dans A pour $X_1, \ldots, X_n$ est le polynôme, qu'on va noter « $A|_{X_1=B_1,\ldots,X_n=B_n}$ », défini ainsi :

$$A|_{X_1=B_1,\ldots,X_n=B_n} \overset{\text{déf}}{=} B_1^{e_1} \cdots B_n^{e_n}.$$

Définition. Soit un polynôme

$$A = a_1U_1 + \cdots + a_kU_k,$$

où $U_1, \ldots, U_k$ sont des monômes unitaires en indéterminées $X_1, \ldots, X_n$, et $a_1, \ldots, a_k$ sont des nombres réels. Si $B_1, \ldots, B_n$ sont des polynômes[13] (peu importe en quels indéterminées), alors le résultat de *substitution* de $B_1, \ldots, B_n$ dans A pour $X_1, \ldots, X_n$ est le polynôme, qu'on va noter « $A|_{X_1=B_1,\ldots,X_n=B_n}$ », défini ainsi :

$$A|_{X_1=B_1,\ldots,X_n=B_n} \overset{\text{déf}}{=} a_1 \left(U_1|_{X_1=B_1,\ldots,X_n=B_n}\right) + \cdots + a_k \left(U_k|_{X_1=B_1,\ldots,X_n=B_n}\right).$$

[11] Peut-être il serait plus approprié de l'appeler le *terme scalaire* – voir la note 1 pour *polynôme constant* en une indéterminée.

[12] Il y a d'autres objets mathématiques qu'on peut substituer pour une indéterminée dans un monôme unitaire, comme, par exemple, des *matrices carrées* ou des *opérateurs linéaires*.

[13] Il y a d'autres objets mathématiques qu'on peut substituer pour une indéterminée dans un polynôme, comme, par exemple, des *matrices carrées* ou des *opérateurs linéaires*.

Exemples. Si $A = XY - 2YZ + 3ZX \in \mathbf{R}[X, Y, Z]$, alors :

$$\begin{aligned} A|_{X=4,\ Y=5,\ Z=6} &= 4 \cdot 5 - 2 \cdot 5 \cdot 6 + 3 \cdot 6 \cdot 4 \\ &= 20 - 60 + 72 \\ &= 32, \\ A|_{X=U,\ Y=V,\ Z=U-V} &= UV - 2V(U - V) + 3(U - V)U \\ &= UV - 2UV + 2V^2 + 3U^2 - 3UV \\ &= 3U^2 - 4UV + 2V^2. \end{aligned}$$

On peut aussi effectuer une *substitution partielle*, dont la signification doit être claire :

$$(XY - 2YZ + 3ZX)|_{X=4} = 4Y - 2YZ + 12Z.$$

Notation. On utilise souvent une notation « $A(B_1, \ldots, B_n)$ » pour le résultat de substitutions de $B_1, \ldots, B_n$ dans $A \in \mathbf{R}[X_1, \ldots, X_n]$ pour $X_1, \ldots, X_n$. Pour que cette notation ne soit pas ambiguë, il faut que les indéterminées soient ordonnées.

Exemples. Si $A = XY - 2YZ + 3ZX \in \mathbf{R}[Z, Y, X]$, et que les indéterminée Z, Y, X sont ordonnées dans cet ordre-ci, alors

$$\begin{aligned} A(6,\ 5,\ 4) &= A|_{Z=6,\ Y=5,\ X=4} = 32, \\ A(U - V,\ V,\ U) &= A|_{Z=U-V,\ Y=V,\ X=U} = 3U^2 - 4UV + 2V^2. \end{aligned}$$

II.18. 🛍 Polynôme dérivé

Définition. Soit $A \in \mathbf{R}[X]$ un polynôme en une indéterminée X. Le polynôme *dérivé* de A, noté d'habitude « A' », est le polynôme en la même indéterminée X défini ainsi :

$$A' = A'(X) \overset{\text{déf}}{=} \left.\frac{A(X + Y) - A(X)}{Y}\right|_{Y=0},$$

où Y est une nouvelle indéterminée différente de X.

Remarque. Le choix de la formule dans la définition de la *dérivation* de polynômes donnée ci-dessus est un peu arbitraire. Par exemple, quel que soit $A \in \mathbf{R}[X]$, on peut démontrer les identités suivantes, et donc on pourrait aussi bien prendre une des ces formules pour la définition de A' :

$$\begin{aligned} \left.\frac{A(X + Y) - A(X)}{Y}\right|_{Y=0} &= \left.\frac{A(X) - A(X - Y)}{Y}\right|_{Y=0} \\ &= \left.\frac{A(X + Y/2) - A(X - Y/2)}{Y}\right|_{Y=0}. \end{aligned}$$

Exemple. Si $A = X^2$, alors

$$A' = \left.\frac{(X+Y)^2 - X^2}{Y}\right|_{Y=0} = \left.\frac{2XY + Y^2}{Y}\right|_{Y=0} = (2X+Y)|_{Y=0} = 2X.$$

Pour comparaison,

$$\left.\frac{X^2 - (X-Y)^2}{Y}\right|_{Y=0} = \left.\frac{2XY - Y^2}{Y}\right|_{Y=0} = (2X-Y)|_{Y=0} = 2X$$

et

$$\left.\frac{(X+Y/2)^2 - (X-Y/2)^2}{Y}\right|_{Y=0} = \left.\frac{2XY}{Y}\right|_{Y=0} = (2X)|_{Y=0} = 2X.$$

Trouvons les polynômes dérivés des polynômes 1, X, X^2 et X^3, où X est une indéterminée :

$$1' = \left.\frac{1-1}{Y}\right|_{Y=0} = 0|_{Y=0} = 0,$$

$$X' = \left.\frac{(X+Y) - X}{Y}\right|_{Y=0} = 1|_{Y=0} = 1,$$

$$(X^2)' = \left.\frac{(X+Y)^2 - X^2}{Y}\right|_{Y=0} = (2X+Y)|_{Y=0} = 2X,$$

$$(X^3)' = \left.\frac{(X+Y)^3 - X^3}{Y}\right|_{Y=0} = (3X^2 + 3XY + Y^2)\big|_{Y=0} = 3X^2.$$

On peut montrer (et on va le faire) que pour tout $n \in \mathbf{N}$ strictement positif ($n > 0$), on a :

$$(X^n)' = nX^{n-1}.$$

[...]

Si $A, B \in \mathbf{R}[X]$ et $c \in \mathbf{R}$, alors

(1) $(A+B)' = A' + B'$, (2) $(AB)' = A'B + AB'$, (3) $(cA)' = cA'$.

Si $A, B \in \mathbf{R}[X]$ et $A(B)$ est le résultat de substitution de B dans A pour X, alors

$$(A(B))' = A'(B)B'.$$

[...]

Notation. On va utiliser la notation suivante pour la dérivation d'ordre supérieur (dérivation itérée) d'un polynôme A en une indéterminée :

$$A^{(0)} \overset{\text{déf}}{=} A, \quad A^{(1)} \overset{\text{déf}}{=} A', \quad A^{(2)} \overset{\text{déf}}{=} A'', \quad A^{(3)} \overset{\text{déf}}{=} A''', \quad \dots .$$

Autrement dit, $A^{(0)} = A$ et $A^{(n+1)} = (A^{(n)})'$ pour tout $n \in \mathbf{N}$.

[...]

II.19. 🚧 Formule de Taylor

[...]

Si A est un polynôme de degré n en une indéterminée, alors

$$\begin{aligned} A(X+Y) &= A(X) + A'(X)Y + \frac{A''(X)Y^2}{2} + \cdots + \frac{A^{(n)}(X)Y^n}{n!} \\ &= \sum_{k=0}^{n} \frac{A^{(k)}(X)Y^k}{k!}, \end{aligned}$$

où X et Y sont deux indéterminées différentes. Si on substitue 0 pour X et X pour Y, on trouve la formule suivante :

$$\begin{aligned} A(X) &= A(0) + A'(0)X + \frac{A''(0)}{2}X^2 + \cdots + \frac{A^{(n)}(0)}{n!}X^n \\ &= \sum_{k=0}^{n} \frac{A^{(k)}(0)}{k!}X^k. \end{aligned}$$

[...]