Chapitre 4

La division euclidienne dans l'algèbre $\mathbb{K}[X]$ et ses conséquences

Dans tout ce chapitre, $\mathbb{K}$ désigne un corps commutatif.

4.1 Généralités

Théorème 4.1 (Division euclidienne) *Soit A et B deux polynômes de $\mathbb{K}[X]$ tels que $B \neq 0$. Il existe un couple unique $(Q, R) \in \mathbb{K}[X]^2$ vérifiant*

$$(DE) \qquad \begin{cases} A = BQ + R \\ \deg(R) < \deg(B). \end{cases}$$

*On dit que Q est le **quotient** et R le **reste** de la division euclidienne de A par B.*

La démonstration est basée sur le lemme suivant, qui justifie la technique de la *division des polynômes suivant les puissances décroissantes*.

Lemme 4.2 *Soit U et V deux polynômes non nuls de $\mathbb{K}[X]$ tels que $\deg(U) \geq \deg(V)$. Il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $\deg(U - VQ) < \deg(U)$.*

Preuve : Soit a_k le coefficient dominant de U et b_q celui de V. Par hypothèse, on a $k \geq q$. On "tue" le monôme $a_k X^k$ en posant $\gamma = a_k (b_q)^{-1}$ et $Q = \gamma X^{k-q}$, de sorte que le coefficient dominant de VQ soit a_k et qu'ainsi $\deg(U - VQ) < k$. □

Preuve du théorème 4.1.

- *Existence.* Considérons l'ensemble $\mathcal{A} = \{A - BQ \mid Q \in \mathbb{K}[X]\} \subseteq \mathbb{K}[X]$, et soit r le plus petit des degrés des polynômes de $\mathcal{A}$. Il existe un polynôme $Q \in \mathbb{K}[X]$ tel que

$$\deg(A - BQ) = r.$$

  Supposons $r \geq \deg(B) \geq 0$. D'après le lemme 4.2, il existe $Q' \in \mathbb{K}[X]$ tel que le polynôme

$$(A - BQ) - BQ' = A - B(Q + Q')$$

  soit de degré $r' < r$, ce qui est impossible puisque $A - B(Q + Q') \in \mathcal{A}$.
  On a donc $-\infty \leq r < \deg(B)$.
- *Unicité.* Soit Q et $Q_1 \in \mathbb{K}[X]$ deux polynômes vérifiant les inégalités

$$\begin{cases} \deg(A - BQ) < \deg(B), \\ \deg(A - BQ_1) < \deg(B). \end{cases}$$

On en déduit $\deg((A - BQ) - (A - BQ_1)) = \deg(B(Q_1 - Q)) < \deg(B)$,

ce qui n'est possible que si $Q_1 - Q = 0$.
L'unicité du polynômes Q implique celle du polynôme $R = A - BQ$. □

Retenons que dans la pratique, la division euclidienne des polynômes correspond à la division suivant les puissances décroissantes.

Définition 4.1 *Soit A et B deux polynômes de $\mathbb{K}[X]$, avec $B \neq 0$.*

1. *On dit que B est un **diviseur** ou un facteur de A, ou que B divise A, ou que A est **divisible par** B, lorsque le reste de la division euclidienne de A par B est nul.*
2. *On dit que B est un **diviseur propre** de A si B divise A et si $1 \leq \deg(B) < \deg(A)$.*

Proposition 4.3 *Soit A et B deux polynômes non nuls de $\mathbb{K}[X]$. On a l'équivalence*

$$\{(A \text{ divise } B) \text{ et } (B \text{ divise } A)\} \Longleftrightarrow (\exists \lambda \in \mathbb{K}^*,\ A = \lambda B).$$

Preuve : Soit Q et Q' les deux polynômes non nuls tels que $A = QB$ et $B = Q'A$, cela donne $A = Q'QA$, l'anneau $\mathbb{K}[X]$ étant intègre, on en déduit $Q'Q = 1$, d'où $\deg(Q) = 0$. c'est-à-dire qu'il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda \in \mathbb{K}^*$. □

Définition 4.2 *Soit $P = c_0 + c_1 X + \cdots + c_k X^k$ un polynôme de $\mathbb{K}[X]$. Pour chaque $a \in \mathbb{K}$, la **valeur** de P en a est définie par*

$$P(a) = c_0 + c_1 a + \cdots + c_k a^k \in \mathbb{K}.$$

*On dit qu'un élément $a \in \mathbb{K}$ est **racine** de P si $P(a) = 0 \in \mathbb{K}$.*

Le résultat suivant est une première conséquence de la division euclidienne dans $\mathbb{K}[X]$.

Proposition 4.4 *Le polynôme $P \in \mathbb{K}[X]$ admet $a \in \mathbb{K}$ comme racine si et seulement s'il est divisible par le polynôme $(X - a)$.*

Preuve : Effectuons la division euclidienne dans $\mathbb{K}[X]$ de P par $B = X - a$. Il existe un couple unique de polynômes $(Q, R) \in \mathbb{K}[X]^2$ vérifiant $P = BQ + R$, et $\deg(R) < \deg(X - a) = 1$. Le polynôme R est donc constant. Comme $B(a) = 0$, on a $P(a) = 0$ si et seulement si $R = 0$. □
On en déduit le théorème suivant, qui joue un rôle essentiel dans la théorie des corps finis.

Théorème 4.5 *Soit $P \in \mathbb{K}[X]$ et $a_1, a_2, \ldots, a_k$ des racines **distinctes** de P dans $\mathbb{K}$, alors P est divisible par le polynôme $(X - a_1)(X - a_2)\ldots(X - a_k)$ de degré k.*
Il en résulte qu'un polynôme de degré n de $\mathbb{K}[X]$ possède au plus n racines distinctes dans $\mathbb{K}$.

Preuve : Par récurrence. La propriété est vraie pour $k = 1$ d'après la proposition 4.4 ci-dessus. Supposons-la vérifiée pour $k - 1$, alors

$$P(X) = (X - a_1)\ldots(X - a_{k-1})Q(X).$$

Comme $P(a_k) = (a_k - a_1)\ldots(a_k - a_{k-1})Q(a_k) = 0$, **l'intégrité** de $\mathbb{K}$ implique $Q(a_k) = 0$ donc $Q(X) = (X - a_k)Q_1(x)$, d'où le résultat. □
Le théorème 4.5 reste vrai si le corps $\mathbb{K}$ est remplacé par un anneau intègre.
Contrexemple Dans l'anneau $(\mathbb{Z}/6\mathbb{Z})[X]$, on a l'égalité $(X - 2)(X - 3) = X(X - 5)$.
Le polynôme $P = (X - 2)(X - 3)$ possède donc 4 racines distinctes dans l'anneau non intègre $\mathbb{Z}/6\mathbb{Z}$. Pour chacune des racines $a_i = 0$, 2, 3 ou 5, P est divisible par $(X - a_i)$. Mais P n'est pas divisible par le produit des $(X - a_i)$, qui est de degré 4.

4.2 Les idéaux de $\mathbb{K}[X]$

Soit $A \in \mathbb{K}[X]$, on voit facilement que l'ensemble $\langle A \rangle = \{AQ \mid Q \in \mathbb{K}[X]\}$ est un idéal de $\mathbb{K}[X]$.
Nous allons voir que réciproquement, comme dans le cas de $\mathbb{Z}$, la division euclidienne dans $\mathbb{K}[X]$ implique que tout idéal de $\mathbb{K}[X]$ est de cette forme.
Rappelons qu'un polynôme $A \in \mathbb{K}[X]$ est dit **unitaire** si son coefficient dominant est égal à 1.

Théorème 4.6 *Soit $\mathcal{I}$ un idéal de $\mathbb{K}[X]$ non réduit à $\{0\}$, et soit $r \geq 0$ le plus petit des degrés des polynômes non nuls appartenant à $\mathcal{I}$.*

1. *Pour tout polynôme $A \in \mathcal{I}$ de degré r, on a $\mathcal{I} = \langle A \rangle$.*
2. *Il existe un polynôme unitaire **unique** $U \in \mathcal{I}$ tel que $\mathcal{I} = \langle U \rangle$.*
3. *$\mathcal{I}$ est un idéal propre de $\mathbb{K}[X]$ si et seulement si $r \geq 1$.*

Preuve : L'entier r existe d'après la propriété fondamentale de $\mathbb{N}$ (page 6).

1. Soit $A \in \mathcal{I}$ de degré $r \geq 0$, et soit $P \in \mathcal{I}$. La division euclidienne de P par A s'écrit $P = AQ + R$, avec $\deg(R) < \deg(A) = r$.
   On voit que $R = P - AQ \in \mathcal{I}$, et comme $\deg(R) < r$, on a $R = 0$ et $P = AQ$. Cela montre que $\mathcal{I} \subseteq \langle A \rangle$. Réciproquement, il est clair que $\langle A \rangle \subseteq \mathcal{I}$.
2. Divisant A par son coefficient dominant, on obtient un polynôme unitaire $U \in \mathcal{I}$ tel que $\mathcal{I} = \langle U \rangle$. Ce polynôme est unique car si $U' \in \mathcal{I}$ est un polynôme unitaire tel que $\mathcal{I} = \langle U \rangle = \langle U' \rangle$, chacun des deux polynômes U et U' divise l'autre, il existe $\lambda \in \mathbb{K}^*$ tel que $U = \lambda U'$ (cf. proposition 4.3 page 48), les polynômes U et U' étant unitaires, on a nécessairement $\lambda = 1$ donc $U = U'$.
3. Si $\deg(U) = 0$, $U = 1 \in \mathcal{I}$, ce qui équivaut à $\mathcal{I} = \mathbb{K}[X]$. □

Remarquons que si $\mathcal{I} = \{0\}$, on peut écrire $\mathcal{I} = \langle 0 \rangle$, ce qui montre que tout idéal $\mathcal{I}$ de $\mathbb{K}[X]$ est de la forme $\mathcal{I} = \langle A \rangle$.
On pourra comparer la démonstration qui précède à celle du théorème 1.3 (page 22), et le rôle dans les deux cas de la propriété fondamentale de $\mathbb{N}$ (page 6).

4.3 Polynômes irréductibles

Définition 4.3 *Un polynôme **irréductible** est un polynôme non constant qui n'admet pas de diviseur propre. Un polynôme non irréductible est aussi dit **réductible**.*

Par exemple, tous les polynômes de degré 1 sont irréductibles. Lorsque $\mathbb{K} = \mathbb{C}$, ce sont les seuls. Lorsque $\mathbb{K} = \mathbb{R}$, il y a aussi les polynômes de degré 2 de discriminant négatif. Pour d'autres corps, nous verrons qu'il existe des polynômes irréductibles de degré arbitrairement grand.
On démontre l'exact équivalent du théorème 1.6 page 23 :

Théorème 4.7 *Soit P un polynôme de degré $n \geq 1$, et soit $\mathcal{D} \subset \mathbb{N}$ l'ensemble des degrés des diviseurs non constants de P. Alors $\mathcal{D} \neq \emptyset$ puisque $n \in \mathcal{D}$.*
Soit r le plus petit élément de $\mathcal{D}$ et soit A un diviseur de P de degré r, alors A est irréductible.
Cela signifie que tout polynôme de degré positif admet un facteur irréductible.

Attention Il est **faux de penser qu'un polynôme est irréductible si et seulement s'il n'a pas de racine.** Ainsi

1. Tout polynôme de degré 1 admet une racine, mais est irréductible.

2. Le polynôme $(X^2+1)^2$, de degré 4, n'a pas de racine dans $\mathbb{R}$ mais est réductible dans $\mathbb{R}[X]$, le polynôme $(X^2+X+1)^3$, de degré 6, n'a pas de racine dans $\mathbb{F}_2$ mais est réductible dans $\mathbb{F}_2[X]$, etc.

On a cependant l'équivalence suivante **dans les seuls cas des polynômes de degré 2 ou 3.**

Proposition 4.8 *Un polynôme de degré 2 ou 3 est irréductible dans $\mathbb{K}[X]$ si et seulement s'il n'admet pas de racine dans $\mathbb{K}$.*

Preuve : Un polynôme P est réductible si et seulement s'il possède un diviseur propre, c'est-à-dire un diviseur A vérifiant $1 \leq \deg(A) < \deg(P)$, cela implique $\deg(P) \geq 2$.
Si on écrit $P = AB$, alors on a $(1 \leq \deg(B) \leq \deg(P) - 1)$ et $(\deg(A) + \deg(B) = \deg(P))$.
Si $\deg(P) \leq 3$, on en déduit $(\deg(A) = 1)$ ou $(\deg(B) = 1)$, donc P admet une racine. □

Exercice 29 — Montrer que dans $\mathbf{F_2}[X]$, le seul polynôme irréductible de degré 2 est X^2+X+1, les seuls polynômes irréductibles de degré 3 sont X^3+X^2+1 et X^3+X+1.

Exercice 30 — Montrer que dans $\mathbb{F}_3[X]$, les seuls polynômes irréductibles unitaires de degré 2 sont X^2+1, X^2+X+2, et X^2+2X+2.

4.4 Pgcd de deux polynômes

Soit A et B deux polynômes non tous deux nuls de $\mathbb{K}[X]$, on vérifie facilement que l'ensemble

$$\mathcal{I}(A,B) = \{AU + BV \mid (U,V) \in \mathbb{K}[X]^2\}$$

est un idéal de $\mathbb{K}[X]$. Comme A et B sont éléments de $\mathcal{I}(A,B)$, cet idéal n'est pas réduit à $\{0\}$.
Il existe d'après le théorème 4.6 (page 49) un unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que

$$\mathcal{I}(A,B) = \langle D \rangle.$$

Définition 4.4 *On appelle plus grand commun diviseur de A et B, ou* pgcd *de A et B, et on désigne par* pgcd (A,B) *l'unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que $\mathcal{I}(A,B) = \langle D \rangle$.*

La démonstration des énoncés qui suivent est quasi-identique à celle des énoncés qui leur correspondent dans le cas de l'anneau $\mathbb{Z}$.

Théorème 4.9 (Propriété caractéristique du pgcd) *(Cf. théorème 1.8 page 24)*
Soit A et B deux polynômes de $\mathbb{K}[X]$ non tous deux nuls. Le pgcd *de A et B est l'unique polynôme unitaire $D \in \mathbb{K}[X]$ tel que*

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

On dira que deux polynômes A et B sont **premiers entre eux** si leur seul diviseur unitaire commun est le polynôme 1, autrement dit si leur pgcd est le polynôme 1.

Théorème 4.10 (Théorème de Bézout) *(Cf. théorème 1.9 page 25)*
Soit A et B deux polynômes de $\mathbb{K}[X]$.

1. *Soit D un **diviseur commun** unitaire de A et B. Alors D est le* pgcd *de A et B si et seulement s'il existe deux polynômes U et V dans $\mathbb{K}[X]$ tels que*

$$AU + BV = D. \tag{1}$$

2. *En particulier, les polynômes A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V dans $\mathbb{K}[X]$ tels qu'on ait*

$$AU + BV = 1. \tag{2}$$

Proposition 4.11 *(Cf. proposition 1.12 page 26) Soit A et B deux polynômes de $\mathbb{K}[X]$, avec $B \neq 0$, et soit R le reste de la division euclidienne de A par B, alors*

$$\operatorname{pgcd}(A, B) = \operatorname{pgcd}(B, R).$$

Ce résultat débouche sur **l'algorithme d'Euclide** et **l'algorithme d'Euclide étendu** pour les polynômes, respectivement identiques à leurs homonymes pour les entiers.

Comme dans le cas des entiers, le lemme de Gauss pour les polynômes et la décomposition en facteurs irréductibles résultent du théorème de Bézout.

Théorème 4.12 (Lemme de Gauss) *(Cf. théorème 1.13 page 27) Soit A, B et C trois polynômes de $\mathbb{K}[X]$. Si A divise le produit BC et est premier avec B, A divise C.*

4.5 Décomposition d'un polynôme en facteurs irréductibles

L'énoncé suivant se déduit du théorème 4.7 (page 49) d'existence d'un facteur irréductible de la même façon que le Théorème fondamental de l'arithmétique (page 29) se déduit du théorème 1.6 (page 23).

Théorème 4.13 *(Cf. Théorème fondamental de l'arithmétique 1.20 page 29)*
Tout polynôme non nul $A \in \mathbb{K}[X]$ s'écrit d'une façon unique à une permutation près

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_n^{\alpha_n},$$

où

$$\begin{cases} \lambda \in \mathbb{K}^*, \\ \text{les polynômes } P_i \text{ sont irréductibles, unitaires et tous distincts,} \\ \text{les entiers } \alpha_i \text{ sont positifs.} \end{cases}$$

Exercice 31 — Décomposer en facteurs irréductibles dans $\mathbb{F}_2[X]$ le polynôme

$$A = X^5 + X^4 + X^3 + X^2 + X + 1.$$

4.6 La $\mathbb{K}$-algèbre quotient $\mathbb{K}[X]/\langle P\rangle$

Soit $P \in \mathbb{K}[X]$ un polynôme non constant ($\deg(P) \geq 1$). Comme dans le cas de $\mathbb{Z}$, la relation d'équivalence **modulo** P est définie par

$$\forall (A, A') \in \mathbb{K}[X]^2, \quad (A \equiv A' \pmod P) \text{ si et seulement si } (A' - A \in \langle P\rangle). \tag{1}$$

Pour chaque polynôme $A \in \mathbb{K}[X]$, on désigne par $\overline{A}$ sa classe d'équivalence modulo P :

$$\overline{A} = \{A' \in \mathbb{K}[X] \mid A \equiv A' \pmod P\} = \{A + PQ \mid Q \in \mathbb{K}[X]\}.$$

On désigne par $\mathbb{K}[X]/\langle P\rangle$ l'ensemble quotient de $\mathbb{K}[X]$ par la relation d'équivalence (1), c'est-à-dire l'ensemble des classes modulo P.

Proposition 4.14 *(Cf. proposition 3.2 page 37) L'addition, la multiplication et la multiplication par un scalaire, définies sur l'ensemble quotient $\mathbb{K}[X]/\langle P\rangle$ par*

$$\forall (A, B) \in \mathbb{K}[X]^2, \quad \begin{cases} \overline{A} + \overline{B} = \overline{A+B}, \\ \overline{A}\,\overline{B} = \overline{AB}, \\ \forall a \in \mathbb{K}, \quad a\overline{A} = \overline{aA}, \end{cases}$$

font de $\mathbb{K}[X]/\langle P\rangle$ une $\mathbb{K}$-algèbre dans laquelle l'élément neutre de l'addition est $\overline{0}$, classe du polynôme $0 \in \mathbb{K}[X]$, et l'élément neutre de la multiplication est $\overline{1}$, classe du polynôme $1 \in \mathbb{K}[X]$.

Théorème 4.15 *(Cf. théorème 3.3 page 37) Soit $P \in \mathbb{K}[X]$ un polynôme non constant.*
- *La classe $\overline{A} \in \mathbb{K}[X]/\langle P\rangle$ d'un polynôme $A \in \mathbb{K}[X]$ est inversible dans $\mathbb{K}[X]/\langle P\rangle$ si et seulement si A est premier avec P.*
- *Il en résulte que l'anneau $\mathbb{K}[X]/\langle P\rangle$ est un corps si et seulement si le polynôme P est irréductible dans $\mathbb{K}[X]$.*

4.7 Représentation de la $\mathbb{K}$-algèbre $\mathbb{K}[X]/\langle P\rangle$

Soit $q \in \mathbb{Z}$ et soit n un entier positif. On a vu que la façon la plus simple de décrire la classe $\overline{q}$ dans $\mathbb{Z}/n\mathbb{Z}$ consiste à écrire $\overline{q} = \overline{r}$, où r est le reste de la division euclidienne de q par n. On peut dire dans ce sens que l'entier $r \in \{0, 1, \dots, n-1\}$ *représente* la classe $\overline{q}$ modulo n.

On procède de la même façon dans l'anneau $\mathbb{K}[X]/\langle P\rangle$, grâce à la proposition suivante.

Proposition 4.16 *Soit A et P deux éléments de $\mathbb{K}[X]$, on suppose $\deg(P) \geq 1$. Le reste R de la division euclidienne de A par P est le seul polynôme de $\mathbb{K}[X]$ tel que*

$$\begin{cases} R \equiv A \pmod P, \\ \deg(R) < \deg(P). \end{cases}$$

Preuve : Il est clair que $R \equiv A \pmod P$.
L'unicité vient de ce que si $R' \equiv R \pmod P$ avec $\deg(R') < \deg(P)$, le polynôme $R' - R$ est divisible par P et $\deg(R' - R) < \deg(P)$, ce qui implique $R' - R = 0$. □

Notation Pour chaque entier positif n, désignons par $\mathbb{K}[X]^{(n)}$ le sous-espace vectoriel de $\mathbb{K}[X]$ constitué des polynômes $Q \in \mathbb{K}[X]$ tels que $\deg(Q) < n$.

Dans ce qui suit, on pose $n = \deg(P) \geq 1$.

La proposition 4.16 énonce alors que pour tout $A \in \mathbb{K}[X]$, la classe $\overline{A} \in \mathbb{K}[X]/\langle P\rangle$ contient **un seul** polynôme appartenant à $\mathbb{K}[X]^{(n)}$, ce polynôme est le reste de la division euclidienne de A par P.

Dans la suite de ce chapitre, on désigne par α la classe du polynôme X dans la $\mathbb{K}$-algèbre quotient $\mathbb{K}[X]/\langle P\rangle$.

Pour chaque polynôme $A = a_0 + a_1 X + \dots + a_k X^k \in \mathbb{K}[X]$, posons

$$A(\alpha) = a_0 + a_1\alpha + \dots + a_k\alpha^k \in \mathbb{K}[X]/\langle P\rangle,$$

de sorte que $A(\alpha) = \overline{A} \pmod P$, et qu'en particulier on a $P(\alpha) = 0$. Cela permet d'écrire

$$\mathbb{K}[X]/\langle P\rangle = \{\overline{A} \mid A \in \mathbb{K}[X]\} = \{A(\alpha) \mid A \in \mathbb{K}[X]\}.$$

Soit $A = PQ + R$ la division euclidienne de A par P, de la relation $P(\alpha) = 0$ il résulte que

$$A(\alpha) = R(\alpha).$$

On en déduit

(1) $$\mathbb{K}[X]/\langle P\rangle = \{R(\alpha) \mid R \in \mathbb{K}[X]^{(n)}\} = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{K}\}.$$

De plus, il résulte de la proposition 4.16 que si R_1 et $R_2 \in \mathbb{K}[X]^{(n)}$, on a l'équivalence

(2) $$(R_1(\alpha) = R_2(\alpha)) \Longleftrightarrow (R_1 = R_2).$$

On déduit de (1) et (2) que la famille $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ est une base du $\mathbb{K}$-espace vectoriel $\mathbb{K}[X]/\langle P\rangle$. On a ainsi démontré l'important théorème suivant.

Théorème 4.17 *Soit $P \in \mathbb{K}[X]$ un polynôme de degré $n \geq 1$.*

1. *Tout élément $x \in \mathbb{K}[X]/\langle P\rangle$ s'écrit d'une façon et d'une seule sous la forme*
$$x = R(\alpha), \text{ où } R \in \mathbb{K}[X]^{(n)}.$$
2. *En tant que $\mathbb{K}$-algèbre, $\mathbb{K}[X]/\langle P\rangle$ est un $\mathbb{K}$-espace vectoriel de dimension n et la famille*
$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$
en constitue une base, qu'on appelle la ***base canonique*** *de $\mathbb{K}[X]/\langle P\rangle$.*

Exercice 32 — Montrer que le corps $\mathbb{C}$ des nombres complexes n'est autre que le corps quotient $\mathbb{R}[X]/\langle X^2+1\rangle$. A quoi correspond dans $\mathbb{C}$ la classe α de X dans $\mathbb{R}[X]/\langle X^2+1\rangle$? La base $\{1, \alpha\}$?

4.8 Règles de calculs dans $\mathbb{K}[X]/\langle P\rangle$

Sous les hypothèses du théorème 4.17 ci-dessus, chaque élément $x \in \mathbb{K}[X]/\langle P\rangle$ s'écrit de façon unique $x = R(\alpha)$, avec $R \in \mathbb{K}[X]^{(n)}$. L'addition ne pose pas de problème puisque la somme de deux polynômes de $\mathbb{K}[X]^{(n)}$ appartient à $\mathbb{K}[X]^{(n)}$. Pour la multiplication, on procède comme suit.

Règle de calcul pour la multiplication *Pour multiplier les deux éléments $R_1(\alpha)$ et $R_2(\alpha)$ dans $\mathbb{K}[X]/\langle P\rangle$, on calcule le reste R de la division euclidienne dans $\mathbb{K}[X]$ du polynôme produit R_1R_2 par P et on écrit*

$$R_1(\alpha)R_2(\alpha) = R(\alpha).$$

Exemple Supposons par exemple $\mathbb{K} = \mathbb{Q}$ et $P = X^3 - X + 1$.

$$\mathbb{Q}[X]/\langle P\rangle = \{a\alpha^2 + b\alpha + c \mid a, b, c \in \mathbb{Q}\}.$$

Soit à effectuer le produit de $(\alpha^2 + \alpha)$ par $(\alpha^2 + 1)$, on écrit

(1) $$(\alpha^2 + \alpha)(\alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha,$$

puis $$X^4 + X^3 + X^2 + X = (X^3 - X + 1)(X + 1) + \underbrace{2X^2 + X - 1}_{R},$$

on en déduit $$(\alpha^2 + \alpha)(\alpha^2 + 1) = R(\alpha) = 2\alpha^2 + \alpha - 1.$$

On peut aussi réduire l'expression obtenue dans (1) en utilisant la relation

$$P(\alpha) = \alpha^3 - \alpha + 1 = 0,$$

c'est-à-dire $$\alpha^3 = \alpha - 1,$$

ce qui donne, en remplaçant autant de fois qu'il le faut α^3 par $\alpha - 1$,

$$(\alpha^2 + \alpha)(\alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha(\alpha - 1) + \alpha - 1 + \alpha^2 + \alpha = 2\alpha^2 + \alpha - 1.$$