Historique : 1
Division euclidienne dans $\mathbb{N}$: 1
Les anneaux 2
Définition : 2
L'anneau intègre : 3
L'anneau euclidien : 3
L'anneau Z et les ensembles quotients Z/nZ : 4
Ensemble nZ des multiples d'un entier naturel n : 4
Congruences modulo n dans Z 4
Ensemble Z/nZ des classes d'équivalence de congruence 5
La division euclidienne des polynômes : 5
Les anneaux de polynômes : 5
La division euclidienne des polynômes : 6
Le PGCD : 8
Sous-groupes idéaux : 8
Une définition du PGCD dans Z : 9
PGCD : 9
Identité de Bezout : 10
Théorème de Bezout : 10
Le PGCD dans K[X] : 11
Idéaux de K[X] : 11
PGCD : 12
Identité de Bézout : 12
Théorème de Bézout : 12

Historique :

Au commencement … l'homme utilisait sans doute des traits pour dénombrer. Les peintures de doigts des magdaléniens sur les parois de leurs grottes servaient-elles à compter ?

On peut penser que l'homme a d'abord symbolisé les quantités sous forme de chiffres avant d'en explorer les propriétés. Et pourtant les premières traces de système de numérotation savante apparaissent avec les Egyptien et les Babyloniens il y a environ 4000 ans alors que l'os d'Ishango gravé il y a 20 000 ans semble représenter une table de nombres premiers. L'intérêt pour la divisibilité des nombres serait-il antérieur à leur symbolisation ?

Toujours est-il qu'au cours des siècles, l'intérêt pour cette propriété des nombres à passionné de nombreux mathématiciens. Les premières traces écrites remontent à la Grèce antique. Euclide d'Alexandrie dans ses Eléments présente la décomposition en facteurs premiers d'un entier naturel et introduit la notion de PGCD (Plus Grand Commun Diviseur).

L'étude du PGCD de nombres entiers a pris de l'ampleur au XVIème siècle grâce à Bachet qui a démontré le fameux théorème dit de Bézout pour des nombres entiers entiers. Bézout a démontré ce résultat pour des polynômes. La définition du PGCD peut donc s'étendre aux polynômes et aussi à d'autres ensembles.

Nous aborderons dans cette étude les fondements mathématiques des PGCD, leur détermination ainsi que leurs applications.

Division euclidienne dans N :

Soient a et b deux entiers naturels avec $b \neq 0$, considérons l'ensemble B des multiples de b inférieurs ou égaux à a :

$$B = \{x \in \mathbb{N} \ ; \ x = kb \text{ avec } k \in \mathbb{N} \text{ et } x \leq a\}$$

L'ensemble B est non vide puisque $0 \in B$,
B est donc un sous ensemble de $\mathbb{N}$ non vide et majoré par a .
Par suite B admet un plus grand élément et il existe donc un entier naturel q unique tel que :
$bq \leq a < b(q+1)$ en posant $r = a - bq$ on peut dire qu'il existe un couple unique (q, r) d'entiers naturels tel que :

$$\begin{cases} a = bq + r \\ r < b \end{cases}$$

On dit que q est le quotient entier et r le reste de la division euclidienne de a par b.
Si r = 0 alors a est par définition divisible par b, on dit dans ce cas que a est un multiple de b ou que b est un diviseur de a.

Nous avons ainsi défini la division euclidienne pour les entiers naturels. Une première remarque est que cette opération est différente des lois de groupes comme l'addition ou la multiplication car c'est une opération de $\mathbb{N}$x$\mathbb{N}$ dans $\mathbb{N}$x$\mathbb{N}$.

Dans quelle type d'ensemble pouvons nous utiliser cette opération ?

La division euclidienne dans R ne fait pas grand sens car pour tout a et b de R on trouve un q de R tel que r = 0. Nous allons maintenant étudier les structures qui présentent un intérêt pour la division euclidienne.

Tout d'abord, la division euclidienne requiert la préexistence d'une loi additive + et d'une loi multiplicative x. La structure qui correspond est l'anneau unitaire (le corps est exclu car il requiert la symétrie par rapport à la multiplication, ce qui est peu intéressant pour la division euclidienne, on aurait simplement $q = b^{-1} \times a$ et r = 0).

Les anneaux

Définition :

Un anneau est un ensemble A muni de deux opérations (appelées addition et multiplication) qui se comportent comme celles des entiers relatifs au sens précis suivant : A muni de l'addition est un groupe commutatif, la multiplication est associative, distributive par rapport à l'addition, et elle possède un élément neutre.

Dit de façon plus détaillée, un anneau est un ensemble dans lequel sont données deux lois de composition interne, notées + et · qui vérifient les propriétés suivantes :
Pour tous éléments a, b et c appartenant à l'ensemble A :

$(a + b) + c = a + (b + c)$
$a + b = b + a$
$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
$a \cdot (b + c) = a \cdot b + a \cdot c$
$(b + c) \cdot a = b \cdot a + c \cdot a$

Il existe un élément, noté 0 et appelé élément neutre de la loi de composition interne + tel que pour tout a appartenant à A :

$a + 0 = 0 + a = a$

Tout élément a appartenant à A possède un opposé, noté –a qui vérifie :

$a + (-a) = (-a) + a = 0$

L'anneau unitaire commutatif :

Nous avons en plus besoin d'un élément neutre pour la multiplication pour le cas où b =< a =< 2b.

Un anneau unitaire est un anneau dans lequel il existe un élément, noté 1 et appelé élément neutre de la loi de composition externe ·, ou élément unité[5], tel que pour tout a appartenant à A :

$a \cdot 1 = 1 \cdot a = a$

On appelle aussi anneau unitaire tout simplement anneau.

Nous utilisons généralement une loi multiplicative commutative (a = bq + r = qb + r). Cela n'est pas obligatoire mais dans cette étude nous utilisons des anneaux commutatifs.

Un anneau commutatif est un anneau dont la multiplication est elle aussi commutative. En explicitant comme ci-dessus, c'est un anneau où est aussi vérifiée pour tous a et b l'identité :

$a \cdot b = b \cdot a$.

L'anneau intègre :

Nous avons défini les propriétés des deux lois qui permettent de définir la division euclidienne mais il faut ajouter une propriété supplémentaire, l'absence de diviseurs de zéro. Car si pour un b donné, il existe un q tel que bq = 0 alors r peut être supérieur à b.

Un anneau commutatif $(A, +, \times)$ est dit intègre[1] s'il est

- différent de l'anneau nul, c'est-à-dire s'il possède au moins deux éléments, et
- sans diviseur de zéro, c'est-à-dire :

$$\forall (a,b) \in A^2,\ a \times b = 0 \Rightarrow (a = 0 \quad \text{ou} \quad b = 0)\ .$$

Nous pouvons maintenant définir la structure qui pourra accueillir la division euclidienne.

L'anneau euclidien :

L'anneau unitaire (commutatif) A est dit euclidien, s'il existe une application f de A dans N compatible avec l'ordre de N telle que :
i/ si b divise a, alors $f(b) \leqslant f(a)$;
ii/ Pour tout (a,b) de A^2, il existe q et r tels que a = bq + r et f(r) < f(b).
Cette application sera nommée un stathme euclidien.

On a aussi $f(0_A) = -\infty$ ou $f(0_A) = 0$ suivant le type d'anneau utilisé. On voit ici que la division euclidienne peut être étendue à d'autres ensembles que les entiers naturels et à d'autres relations d'ordres. Nous aborderons par exemple ultérieurement la division des polynômes où la relation d'ordre concerne ici leur degré avec $\deg(0) = -\infty$.

L'anneau Z et les ensembles quotients Z/nZ :

Bien entendu Z est un anneau euclidien. Les lois + et x sont conformes à la définition d'un anneau avec 0 et 1 comme éléments neutres. Il est intègre (pas de diviseur de 0). Et en plus il n'est pas inversible.

Dans Z, le stathme euclidien retenu sera la valeur absolue (application de Z dans N avec la condition |r|<|b|). Le résultat de la division euclidienne dans Z est unique si la condition $r \in N$ est respectée.

La division euclidienne dans Z est étroitement liée avec la définition d'ensembles quotients Z/nZ. Nous verrons que la généralisation des ensembles quotients à d'autres anneaux euclidiens est très utile.

Ensemble nZ des multiples d'un entier naturel n :

Définition :
Soit n un entier naturel , l'ensemble $n\mathbb{Z}$ est l'ensemble :
$n\mathbb{Z} = \{ k n ; k \in \mathbb{Z} \}$
Il est inutile de considérer l'ensemble des multiples d'un entier relatif -n, car cet ensemble est identique à l'ensemble $n\mathbb{Z}$.
Cet ensemble est infini si $n \neq 0$.

- Si n = 0 ; $n\mathbb{Z} = 0\mathbb{Z} = \{0\}$
- Si n = 1 ; $n\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$

Propriétés :

- L'ensemble $n\mathbb{Z}$ muni de la loi + est un sous-groupe de $\mathbb{Z}$
  en effet : soit x_1 et x_2 deux éléments de $n\mathbb{Z}$, alors il existe deux entiers relatifs k_1 et k_2 tels que $x_1 = k_1 n$ et $x_2 = k_2 n$
  $x_1 - x_2 = k_1 n - k_2 n = (k_1 - k_2)n$ où $k_1 - k_2 \in \mathbb{Z}$, donc $x_1 - x_2 \in n\mathbb{Z}$

Tout multiple d'un multiple d'un entier naturel n est encore un multiple de l'entier naturel n.

Congruences modulo n dans Z

Soit n un entier naturel non nul.
Considérons dans $\mathbb{Z}$ la relation notée = telle que pour tous entiers relatifs x et y :
$x = y\ (n) \Leftrightarrow$ x - y est un multiple de n dans $\mathbb{Z}$
$\Leftrightarrow \exists k \in \mathbb{Z}$ tel que x - y = kn
On démontre facilement que cette relation est une relation d'équivalence
et on appelle cette relation congruence modulo n dans $\mathbb{Z}$.

Remarque :
x = y (n) se lit : " x est congru à y modulo n ".
Donc pour que deux entiers relatifs x et y soient congrus modulo n dans $\mathbb{Z}$ il faut et il suffit qu'ils aient le même reste dans la division euclidienne par n.

Ensemble Z/nZ des classes d'équivalence de congruence

Définition : $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence pour la congruence modulo n .

Propriété :
L'ensemble $\mathbb{Z}/n\mathbb{Z}$ comporte n classes d'équivalence en effet , pour que deux entiers relatifs x et y soient congrus modulo n dans $\mathbb{Z}$, il faut et il suffit qu'ils aient le même reste dans la division euclidienne par n, or il y a n restes distincts possibles dans une division euclidienne par n, ces n restes sont : 0 ; 1 ; 2 ;....; n -1.
Un élément de $\mathbb{Z}/n\mathbb{Z}$ est noté $\dot{x}$ ou $[x]_n$, si le reste correspondant, dans la division euclidienne par n est x.
$\mathbb{Z}/n\mathbb{Z} = \{ \dot{0} ; \dot{1}; \dot{2} ; \dot{3} ; \dot{4} ; \dot{5}; \dot{6} ; \dot{7}; .....; \dot{n-1} \}$

Addition dans $\mathbb{Z}/n\mathbb{Z}$:
on sait que la somme de deux entiers relatifs congru modulo n est encore un entier congru modulo n, l'addition dans $\mathbb{Z}$ induit sur $\mathbb{Z}/n\mathbb{Z}$, une addition commutative et associative admettant pour élément neutre la classe d'équivalence $\dot{0}$:

- pour tous éléments $\dot{x}$ et $\dot{y}$ de $\mathbb{Z}/n\mathbb{Z}$: $\dot{x} + \dot{y} = \dot{x+y}$
- tout élément $\dot{x}$ de $\mathbb{Z}/n\mathbb{Z}$ admet pour la loi + un élément symétrique (opposé), $\dot{n-x}$ en effet : $\dot{x} + \dot{n-x} = \dot{0}$

on peut donc en conclure que ($\mathbb{Z}/n\mathbb{Z}$; +) est un groupe commutatif.

Multiplication dans $\mathbb{Z}/n\mathbb{Z}$:
On sait que le produit de deux entiers relatifs congru modulo n est encore un entier congru modulo n, la multiplication dans $\mathbb{Z}$ induit sur $\mathbb{Z}/n\mathbb{Z}$, une multiplication commutative et associative et distributive par rapport à l'addition (définie précédemment définie) admettant pour élément neutre la classe d'équivalence $\dot{1}$:

- pour tous éléments $\dot{x}$ et $\dot{y}$ de $\mathbb{Z}/n\mathbb{Z}$: $\dot{x} \times \dot{y} = \dot{x}\dot{y}$

La division euclidienne des polynômes :

Les anneaux de polynômes :

Intéressons nous maintenant aux anneaux polynomiaux (A[X], +, .) où A[X] est l'ensemble des polynômes à coefficients dans un anneau A. Les propriétés des lois de l'anneau A font de (A[X] , + , .) un anneau (stabilité, associativité, distribution, 0 et 1 étant les éléments neutres des deux lois).

Si le polynôme est non nul (c'est-à-dire si ses coefficients ne sont pas tous nuls), son degré est le plus grand exposant de x devant lequel le coefficient n'est pas nul (appelé aussi coefficient dominant). Par convention, le degré du polynôme nul vaut $-\infty$.

Le degré du polynôme de A[X] défini ainsi une application de A[X] \ {0} vers N compatible avec la relation d'ordre sur N. Cette application sera notre stathme

euclidien. Nous définissons ici la division euclidienne pour les polynômes de coefficient dominant inversible.

Vérifions d'abord que notre anneau A[X] est intègre.

Lemme :
Soit A un anneau intègre et P, Q deux polynômes sur A. Alors :
$deg(P.Q) = deg(P) + deg(Q)$.
Démonstration :
On suppose tout d'abord que les deux polynômes, P et Q sont non nuls. On peut écrire

$$P(X) = \sum_{i=0}^{n} a_i X^i$$

$$Q(X) = \sum_{i=0}^{m} b_i X^i.$$

où n=deg(P) et où m=deg(Q). P.Q s'écrit alors:

$$(P.Q)(X) = \sum_{i=0}^{n+m} \sum_{k=0}^{i} a_k . b_{i-k} X^i.$$

Remarquons que le monôme de degré n + m a pour coefficient $a_n . b_m$. Les deux facteurs de ce produit ne sont pas nuls (autrement P et Q ne seraient pas du degré supposé), l'anneau A étant intègre, le produit n'est donc pas nul et donc le degré de P.Q est bien n+m. Si P ou (et) Q est (sont) nul(s), la convention précédente nous permet de vérifier là encore la formule sur le degré.

Proposition :
Soit A un anneau intègre. Alors A[X] est aussi un anneau intègre.
Démonstration Soient P et Q des éléments de A[X]. On suppose que P.Q=0. La formule précédente qui est vraie dès que l'anneau est intègre nous permet d'écrire: deg(P)+deg(Q)=-∞. Ceci n'est possible que si deg(P) ou deg(Q)=-∞ et donc que si P ou Q est nul. A[X] est bien intègre.

Nous avons donc démontré que A[X] est bien intègre à condition que A soit un anneau intègre.

La division euclidienne des polynômes :

Nous allons démontrer l'existence de la division euclidienne pour les polynômes unitaires (polynômes de coefficient dominant égale à 1).

Existence :

Proposition :

Soit A un anneau intègre et soit P un élément non nul de A[X]. On suppose de plus que P est unitaire. Soit L un autre élément de A[X]. Il existe Q et R dans A[X] tels que:

- L=P.Q+R.
- deg R < deg P ou R=0.

Démonstration :
Notons:

$$P = a_0 + a_1 x + ... + a_{n-1} x^{n-1} + x^n$$

Si L est un polynôme de degré plus petit que deg P ou est le polynôme nul, alors le résultat de la division euclidienne de L par P est Q = 0 et R = L.

Si L est un polynôme de degré plus grand que deg P, il faut prouver que Q et R existent.

Cela revient à étudier l'existence d'un représentant de la classe d'équivalence de L dans l'anneau quotient A[X]/PA[X] (ensemble quotient des classes d'équivalences pour la congruence modulo P).

Si la classe d'équivalence de L dans ce quotient a pour représentant un polynôme M tel que deg M < deg P ou M =0, alors il existe Q dans A[X] tel que L-M=Q.P. La division euclidienne est alors possible. Montrons qu'un tel représentant existe toujours.

La classe d'équivalence de P dans A[X]/(P) admet le polynôme nul comme représentant. L'égalité suivante est donc vraie dans le quotient (P = 0) :

$$x^n = a_0 + a_1 x + ... + a_{n-1} x^{n-1}.$$

Cette égalité nous permet d'écrire le monôme x^n ainsi que tous les monômes de la forme x^{n+i}, i>0 en fonction des monômes 1,x,...,x^{n-1}. Dans A[X]/PA[X], le polynôme L est donc égal à un polynôme ne s'écrivant qu'avec des monômes de degré strictement plus petit que deg P. On a ainsi trouvé un représentant M de la classe de L dans A[X]/PA[X] tel que deg M < deg P.

Ainsi tout couple (A, B) de A[X] x A[X] admet une décomposition (Q, R) dans A[X] x A[X] telle que deg R < deg P. Cette décomposition est-elle unique ?

Unicité :

Démonstration :
Supposons l'existence de deux couples [redacted] et [redacted] solutions. Alors :
[redacted]
On en déduit que :
[redacted]
Si [redacted] alors :

[redacted]
ce qui est absurde donc [redacted] et ainsi [redacted] d'où l'unicité.

Donc tout élément (A,B) de A{X]x A{X] admet une image unique par la division euclidienne. Cependant, si les éléments B de A[X] admettent un inverse, la division euclidienne ne présente pas de grand intérêt. Vérifions que cela n'est pas le cas.
Division de polynômes inversibles

Proposition :
Si A est un anneau intègre et que P est un élément inversible de A[X] alors P est en fait élément de A^*.

Démonstration :
P est inversible dans A[X]. On peut donc trouver $Q \in A[x]$ tel que P.Q=1. On peut alors écrire: 0=deg(P.Q)=deg(P)+deg(Q). Ceci implique que deg(P)=deg(Q)=0. P et Q sont donc éléments de A. Comme P.Q=1, ils sont aussi éléments de A^*.

Donc les seuls éléments inversibles de A[X] sont les polynômes de degré 0. La division euclidienne n'a plus de sens car alors Q = 0.

Division euclidienne de polynômes non unitaires :

Supposons maintenant que notre polynôme ne soit pas unitaire. Il suffit alors que le coefficient dominant soit inversible. Il faut alors multiplier P par l'inverse de son coefficient dominant pour retrouver un polynôme unitaire.

Corollaire :
Si k est un corps, k[X] muni de la division définie via la fonction degré est un anneau Euclidien.

Démonstration :
Les éléments de k[X] ont leur coefficient dominant (et les autres...) qui sont éléments de k et qui sont donc inversibles. On peut alors leur appliquer la proposition précédente.

Conclusion : nous avons montré que la division euclidienne est une opération définie sur des anneaux de polynômes K[X] avec K étant un corps. Cette opération définit un quotient Q et un reste R uniques pour tout élément (P, Q) de K[X]x K[X].

Le PGCD :

Pour définir le PGCD, nous avons besoin d'approfondir les propriétés des anneaux.

Sous-groupes idéaux :

Dans un anneau commutatif A, un idéal J est un sous-groupe additif tel que pour tout a de A et tout x de J, le produit ax est élément de J.

On peut aussi dire de façon plus concise :
J est un sous-groupe additif de A stable pour la multiplication par A

On note alors aA l'idéal de A engendré par a.

Proposition :

aZ + bZ est un idéal

Soient a et b deux entiers relatifs.
On note aZ + bZ l'ensemble {a.u + b.v ; (u,v) $\in Z^2$}
aZ + bZ est un idéal, contenant a et b

Démonstration :
Soient a et b deux entiers relatifs.
aZ + bZ = {a.u + b.v ; (u,v) $\in Z^2$}

En prenant u = 1 et v = 0 (et vice-versa), on voit que a et b appartiennent à aZ + bZ
Montrons que aZ + bZ est un sous-groupe additif de Z.
Soient x et y deux éléments de aZ + bZ.
Il existe alors quatre entiers relatifs i, j, k et l tels que
x = a.i + b.j et y = a.k + b.l
On a alors x - y = a.(i-k) + b.(j-l) donc x - y $\in$ aZ + bZ
Comme l'ensemble n'est pas vide, c'est un sous-groupe de Z.

Proposition :
Tous les idéaux de Z sont de la forme nZ.

Démonstration :
Soit I un idéal de Z distinct de {0}. Notons n le plus petit entier non nul appartenant à I. Par définition de l'idéal, nZ $\subset$ I. Réciproquement, si a $\in$ I alors on peut effectuer une division euclidienne telle que a = nq + r avec 0 =< r < n. a $\in$ I donc r = 0 sinon a ne serait pas de la forme nq donc I ne serait pas idéal.

Donc tous les idéaux de Z sont engendrés par un unique élément (le n de nZ). On dit alors que Z est un anneau principal (tous ses idéaux sont engendrés par un unique élément et c'est un anneau intègre).
On peut aussi démontrer que l'anneau A[X] est un anneau principal

Une définition du PGCD dans Z :

PGCD :

$\forall$ (a, b) $\in Z^2$, on appelle PGCD de (a, b) tout entier relatif d tel que aZ + bZ = dZ

Démontrons l'existence du PGCD :

Soient a et b deux entiers relatifs.
On appelle H l'idéal engendré par a et b. Il apparaît alors que

$aZ \subset H$ et $bZ \subset H$

or H est stable pour l'addition donc :

$\forall (u, v) \in Z^2, a.u + b.v \in H$

Notons $aZ + bZ$ l'ensemble $\{a.u + b.v ; (u,v) \in Z^2\}$
On a alors :
$aZ + bZ$ est inclus dans H
$aZ + bZ$ est un idéal, contenant a et b
H étant par définition le plus petit idéal contenant a et b, il est inclus dans $aZ + bZ$.
Soit :
$(H \subset aZ + bZ)$ et $(aZ + bZ \subset H) \Rightarrow (H = aZ + bZ)$
L'idéal engendré par a et b est donc $aZ + bZ$.
Z étant principal, il existe d appartenant à Z tel que $aZ + bZ = dZ$

Remarque :

Comme $aZ \subset dZ$ et $bZ \subset dZ$ alors d|a et d|b, d est donc bien un diviseur commun de a et b.
Si c|a et c|b alors $aZ \subset cZ$ et $bZ \subset cZ$ d'où $dZ = aZ + bZ \subset cZ$ donc c|d. donc d est le plus grand diviseur de a et b.
Donc le PGCD tel que nous l'avons défini (idéal engendré par a et b) est le plus grand diviseur commun de a et b d'où son nom PGCD.

Cette définition a le mérite d'étendre la notion de PGCD à d'autres types d'anneaux que Z. Le PGCD peut être défini dans tout anneau intègre principal.

Identité de Bezout :

Soient a et b deux entiers relatifs.
Soit d = PGCD(a,b)
Il existe alors deux entiers relatifs u et v tels que d = a.u + b.v

Démonstration :
Soient a et b deux entiers relatifs.
Soit d = PGCD(a,b)
Par définition $dZ = aZ + bZ = \{ a.j + b.k ; (j,k) \in Z^2 \}$
Donc $d \in \{ a.j + b.k ; (j,k) \in Z^2 \}$ soit :
Il existe deux entiers relatifs u et v tels que d = a.u + b.v

Théorème de Bezout :

Soient a et b deux entiers relatifs.
A et b sont premiers entre eux $\Leftrightarrow$ PGCD(a,b) = 1 $\Leftrightarrow \exists (u,v) \in Z^2$ / a.u + b.v = 1
La démonstration découle de l'identité de Bezout et de la définition du PGCD

Remarques :
- Il n'y a pas unicité du couple (u, v).
Contre-exemple :
Si on considère le couple (2,4) on a PGCD(2,4) = 2 et pourtant :
2 = 2.1 + 4.0 = 2.3 - 4.1
- Il n'y a pas équivalence entre a.u + b.v = d et d = PGCD(a,b)
(Sinon on pourrait prendre n'importe quel couple (u,v))

Le PGCD dans K[X] :

On s'intéresse maintenant aux PGCD dans un anneau de polynômes K[X] où K est un corps. On a montré précédemment que K[X] est alors un anneau euclidien muni d'une division euclidienne définie précédemment. On doit donc pouvoir définir un PGCD dans K[X].

Suivre le même raisonnement que pour Z, suppose dans un premier temps de s'intéresser aux idéaux de *K*[*X*]. On recherche donc des sous ensembles non vides et stables pour l'addition et la soustraction) et aussi stables pour la multiplication par un polynôme quelconque.

Idéaux de K[X] :

Un sous-ensemble non vide *M* de *K*[*X*] est stable par addition, soustraction et multiplication par un polynôme quelconque si et seulement si il existe un polynôme *m* tel que *M* soit l'ensemble des multiples de *m*. On peut alors écrire mK[X] cet idéal.

Démonstration :
M est stable par addition, soustraction et multiplication par un polynôme quelconque si et seulement s'il existe un polynôme *m* tel que *M* soit l'ensemble des multiples de *m* :
Il est simple de remarquer que les ensembles de multiples sont stables au sens de l'énoncé.
Réciproquement on suppose que *M* est un ensemble stable au sens de l'énoncé et non réduit à 0. Soit *m* un polynôme de *M* non nul et de degré minimal ; par stabilité, *M* contient tous les multiples de *m*. Réciproquement, soit *p* un polynôme quelconque de *M* ; par stabilité, le reste de la division de *p* par *m* est un polynôme de *M* ; or le degré de ce polynôme est strictement inférieur à *m* donc par définition de *m* ce reste est nécessairement nul. Cela montre que tout élément *p* de *M* est un multiple de *m*.

Ce résultat implique en outre que *K*[*X*] est un anneau principal. Nous pouvons donc définir comme pour les entiers un PGCD et étendre la portée du théorème de Bézout.

PGCD :

On définit D$K[X]$ l'idéal engendré par deux polynômes P et Q. Alors D$K[X]$ = P$K[X]$ + Q$K[X]$ et D est le PGCD de P et Q. La démonstration est identique que dans Z.

Identité de Bézout :

Elle découle aussi de la définition du PGCD, Soit P et Q deux polynômes, soit D = PGCD(P,Q), il existe deux polynômes M et N tels que :
$PM + QN = D$

Théorème de Bézout :

Soit P et Q deux polynômes, P et Q sont premiers entre eux si et seulement s'il existe deux polynômes M et N tels que :
$PM + QN = 1$.

Il devient nécessaire de définir l'expression « polynômes premiers entre eux ». Deux polynômes à coefficients dans un corps[2] sont premiers entre eux si et seulement si les seuls polynômes qui les divisent tous les deux sont les polynômes constants non nuls. Cette définition est très proche de celle des entiers qui sont premiers entre eux lorsque les seuls diviseurs communs sont 1 et –1, c'est-à-dire les éléments inversibles de l'anneau.

Démonstration :
L'ensemble des polynômes de la forme $MP + NQ$ est stable au sens de l'énoncé précédent, c'est donc l'ensemble des multiples d'un certain polynôme m.
L'ensemble étudié contient P et Q, ce qui montre que m est un diviseur commun de P et Q. Si P et Q sont premiers entre eux, m est donc un polynôme constant non nul. L'ensemble des multiples de m contient alors $m\,m^{-1}$ égal à 1, ce qui montre que l'identité de Bézout est vérifiée pour au moins un couple de polynôme (M, N).
Réciproquement, si P et Q ne sont pas premiers entre eux, ils ont un diviseur commun C qui n'est pas de degré nul. Les $MP + NQ$ sont alors des multiples de C, donc aucun ne peut être égal à 1.