Les polynômes formels à une indéterminée à coefficients dans un corps K.

Dans ce chapitre,  désigne un corps (commutatif) quelconque.

* 1. La construction
     1. Etape 1

- Soit  l’ensemble des suites d’éléments de K, indexées pas N et nulles à partir d’un certain rang.

C'est-à-dire que  est l’ensemble des  telles que 

- On peut définir deux lois + et  de la manière suivante :

Pour tous , on pose :



et  où 

Alors :

+ et  constituent des lois de composition internes sur , et  est un anneau commutatif.

* Déjà, + est bien une loi de composition interne sur .

En effet, si  et , alors il existe  tel que  et  tel que . Donc . Donc  est nulle à partir d’un certain rang, donc .

* Montrons que  est une loi de composition interne sur .

Soient ,  tel que  et  tel que . Notons enfin 

Alors , . En effet :

Soit . Alors pour tout  :

Si , alors  ou 

(car sinon  et , et alors )

Donc  ou , soit 

Donc .

Donc .

* + n’est autre que la restriction à  de la loi + sur .

Donc + est associative et commutative.

De plus, la suite  est évidemment neutre pour + et appartient à .

Et enfin, si , alors  et .

* Pour  :

 est évidemment commutative (car  est commutative sur le corps K)

Il existe un neutre pour , c’est 

En effet : notons  avec  et .

Soit alors .

Alors , où 

Donc , et par commutativité , donc *U* est bien neutre pour .

Distributivité de  sur + :

Soient . Alors :

, où, pour tout  :



Et , où, pour tout  :

.

Donc 

Et 

Associativité de  :

Soient .

Alors , où, pour tout , .

Et , où, pour tout , 

Donc 

Par ailleurs, on a de même , où, pour tout  :

.

D’où , et le résultat comme  est commutative.

Donc  est bien un anneau commutatif.

* + 1. Etape 2 : plongement de K dans .

Soit .

Alors  est un morphisme injectif d’anneaux :





Justification de la deuxième égalité :



avec .

Donc  si  et  sinon.



* Enfin, si , alors évidemment 

Par conséquent,  est un sous anneau de , isomorphe à l’anneau .

(On dit qu’« il y a une copie de K dans  ») On va identifier cette copie à K, c'est-à-dire identifier, pour chaque ,  et .

Ainsi, pour  et  (avec , ) :

 où 

Donc 









Les éléments de K seront appelés des scalaires.

* + 1. Etape 3 : introduction de l’indéterminée

Soit *X* l’élément de  défini par :



C'est-à-dire  où  et 

Alors  où  et 

Démonstration : par récurrence sur *k*.

Pour  : 

Soit , supposons que  où  et 

Alors 

Où 

Soit, pour , 

Donc 

Théorème fondamental :

Soit . Alors *P* s’écrit de manière unique sous la forme :

 où les  sont des scalaires, nuls à partir d’un certain rang.

Démonstration :

Soit .

* *P* s’écrit , suit d’éléments de K nulle à partir d’un certain rang, disons à partir du rang .

On a aussi :



D’où l’existence de *P* sous la forme  où les  sont nuls à partir d’un certain rang.

* Unicité de l’écriture :

Si , où les  et les  sont nuls à partir d’un certain rang.

Alors .

Vocabulaire :

* Les éléments de  seront toujours notés sous la forme , où les  sont des éléments de K nuls à partir d’un certain rang (on oublie la forme ).

Ils sont appelés polynômes formels à une indéterminée à coefficients dans K.

* Le polynôme *X* est appelé l’indéterminée.
* L’ensemble  des polynômes à une indéterminée à coefficients dans K est noté .
  + 1. Etape 4 : conclusion, récapitulation
* Tout  s’écrit de manière unique sous la forme  où les  sont des éléments de K nuls à partir d’un certain rang.

Ainsi, 

*  est un anneau, dont K est un sous anneau.
* Si , et  où les  sont nuls à partir du rang  et les  à partir du rang , alors :

, 

, où 



Où 

* 1. Degré
     1. Définition

Soit ,  où les  sont des éléments de K nuls à partir d’un certain rang.

* Si , c'est-à-dire  ou . Alors . On dit alors que *P* est de degré 
* Sinon,  et donc il existe  tel que . On peut alors introduire  (puisque l’ensemble est non vide, et majoré car les  sont nuls à partir d’un certain rang). *n* est appelé le degré de *P*.

Ainsi :

Pour tout , , et on a l’équivalence :



Les polynômes de degré 0 sont exactement les 

Les polynômes de degré 1 sont exactement les  avec 

Les polynômes de degré *n* sont exactement les  avec .

Les polynômes de degré  sont exactement les 

L’ensemble de ces derniers est noté  ; en particulier,  n’est autre que K, ensemble des polynômes constants.

* + 1. Propriétés

Soient  et . Alors :



Démonstration :

* Cas  évident.
* Si  et  (ou  et ), le résultat est immédiat aussi.
* Maintenant si  et  :

Notons  et .

* On pose .

On a , et 

Donc , donc 

 où  et 

Donc 

 avec 

* Résultat avec une récurrence immédiate sur *m*.

Vocabulaire :

* Si *P* est un polynôme de degré *n*, le terme  s’appelle le terme dominant de *P* et  le coefficient dominant de *P*.
* Par convention, le coefficient dominant du polynôme nul est 0.
*  s’appelle le coefficient de , et  s’appelle le monôme/terme de degré *k*.
* Un polynôme *P* non nul est dit unitaire lorsque son coefficient dominant est 1.
  1. Début d’arithmétique dans .

Théorème :

 est un anneau intègre.

Démonstration :

* Déjà,  est commutatif et non réduit à .
* Soient maintenant , supposons que 

Montrons qu’alors .

Supposons que non, c'est-à-dire que .

Soient alors . Ainsi, .

Alors  et , avec  et 

Mais alors le coefficient de  est , donc , ce qui est exclu.

Autre démonstration :

, et si , alors forcément soit , soit .

Théorème :

Les éléments inversibles de  sont exactement les éléments de .

Démonstration :

* Soit . Si *P* est inversible, alors il existe  tel que .

Alors . Or, .

Donc 

* Réciproquement, si , alors  admet un inverse .

Donc  est inverse de *P*.

Définition :

Soient . On dit que *P* est multiple de *Q* ou que *Q* est un diviseur de *P* lorsqu’il existe  tel que .

Définition :

Soient . On dit que *P* et *Q* sont associés lorsque *P* divise *Q* et *Q* divise *P* (ce qui équivaut à dire qu’il existe  tel que )

Démonstration de la parenthèse :

* Si  avec  alors *P* divise *Q* et aussi  donc *Q* divise *P*.
* Si *P* divise *Q* et *Q* divise *P* alors il existe  tels que  et . Donc . Donc , d’où, comme  est intègre, soit  soit .
* Si , alors  car *Q* divise *P* donc il existe  tel que .
* Si , alors *S* est inversible, donc , donc .
  + 1. Division euclidienne dans .

Théorème :

Soient , avec .

Alors il existe un unique couple  d’éléments de  tels que  et .

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

Démonstration :

* Unicité :

Si , avec 

Et , avec ,

Alors . Donc 

Ainsi, , donc . Donc .

Donc , soit .

D’où l’unicité.

* Existence :

Soit , de degré  et de coefficient dominant .

Montrons par récurrence que , où :



* Déjà,  est vrai, puisque si , on a :
* Soit , et alors , donc  convient.
* Soit , et donc  et donc , donc le couple  convient.
* Soit , supposons . Soit alors *A* de degré .

Alors *A* s’écrit .

Supposons  (dans le cas contraire,  et  convient)

On peut donc écrire :



Donc 

Or, . Donc  avec  et .

Donc .

Exemple :





* 1. Substitution d’un polynôme à l’indéterminée
     1. Définition, propriétés

Soit . *P* s’écrit  où les  sont nuls à partir d’un certain rang, disons . Donc 

Soit .

On note , soit 

Théorème :

Soient  et , . Alors :



Démonstration :

Soient , .

On introduit  tel que  et . On a alors :



Donc 

 où 

et 



Remarque :

Le théorème s’énonce aussi ainsi :

Pour tout , l’application  est un endomorphisme de l’anneau  (mais ni injectif ni surjectif).

Remarque :

Pour  et si K est un sous corps de C,  est injective.

* + 1. Polynômes pairs, impairs

On suppose ici que  (c'est-à-dire que  n’est pas un élément d’ordre 2 du groupe )

Définition :

Soit 

On dit que *P* est pair lorsque 

On dit que *P* est impair lorsque 

Proposition :

*P* est pair si et seulement si 

*P* est impair si et seulement si 

Démonstration :

.



Or, . On a supposé que .

Donc 

On fait de même pour impair.