Arithmétique sur K[X] et ses quotients

K est un corps commutatif, K[X] anneau des polynômes à une variable à coefficients dans K.
Un polynôme est défini par la suite (ai) de ses coefficients, avec i ≥ 0. F=(ai) = $\sum_i a_i x^i$.
Par défaut on considère que les polynômes ci –dessous appartiennent au même corps K[X]

Division euclidienne

- **Degré de F** noté deg(F). **deg(F) = –∞ si F=0** sinon **deg(F) = plus grand indice i pour lequel ai≠0**.
- deg(P+Q) ≤ Max[deg(F) ; deg(Q)] et deg(PQ) = deg(F) + deg(Q)
- **K[X] est intègre et ses éléments inversibles sont les éléments non nuls de K.**
  P.Q=0 implique deg(P)+deg(Q) = –∞ implique P ou Q = 0 donc pas de diviseurs de 0 non nuls (intégrité)
- Soient A = $a_k x^k$+…. , B=$b_q x^q$ + … avec k ≥ q. alors $Q_1 = \frac{a_k}{b_q} x^{k-q}$ est tel que deg(A – BQ_1) < deg(A)

- **Si B non nul, deg(B)≤ deg(A) → ∃ Q, R uniques avec deg(R)<deg(B) tels que A = BQ + R**
  Q est le quotient de la division euclidienne de A par B et R est le reste.

A	$3x^2$+4x+2	x+1	B
BQ1	$3x^2$+3x	3x	Q1
R1	x +2	+1	Q2
BQ2	x +1		
R2	1		

On appelle R_1 le polynôme A – BQ_1 de l'opération précédente et on recommence pour trouver $R_2 = R_1 – BQ_2$ et ainsi de suite jusqu'à $R_n = (R_{n-1} – BQ_n)$ avec deg(Rn) < deg(B).
On a A = BQ1 + BQ2 + … +BQn + Rn = BQ + R avec R =Rn et deg(R) < deg(B).
Dans l'exemple ci-contre (K=ℝ) on trouve que le division euclidienne de $(3x^2+4x+2)$ par (x+1) donne pour quotient 3x +1, et pour reste 1. On a bien $3x^2+4x+2 = (x+1)(3x+1) +1$.
On arrête la division quand le degré du reste est inférieur au degré de B.

- B divise A non nul (ou A est un multiple de B) si ∃ Q tel que A = BQ (Le reste de la division euclidienne R =0)
- A et B sont dits **associés** s'il existe λ∈K tel que B= λA.

Idéaux de K[X] , PGCD, PPCM

- L'ensemble des multiples du polynôme P est l'idéal engendré par P. On le note (P).
- Pour tout idéal J de K[X] il existe un unique polynôme unitaire P tel que J=(P).
- Soient A et B 2 polynômes non nuls de K[X] l'ensemble J= {AP+BP' |P,P'∈K[X] } est un idéal de K[X]
  En effet cet ensemble est un sous-groupe de (K[X] ,+) et si x∈J et y∈K[X] , xy ∈J.
- **PGCD de A et de B**. C'est l'unique polynôme unitaire D générateur de J ={AP+BP'}. J = (D).

  Soit A et B ont pour diviseur commun un polynôme D de dégré n ≥ 1 et le PGCD est $\frac{D}{a_n}$. Soit le PGCD est 1.

  Si le PGCD de A et B est 1, on dit qu'ils sont premiers entre eux.
  Calcul du PGCD de A et B par l'algorithme d'Euclide. On commence par la division euclidienne de A par B (A=BQ+R) puis on procède à des divisions euclidiennes successives telles que le diviseur de la division précédente devient dividende et le reste devient diviseur (B=Rq +r). On s'arrête quand le reste est nul. Le PGCD est le dernier reste non nul rendu unitaire. Cela provient du fait que les restes successifs sont divisibles par le PGCD (si mD=nDQ+R alors R =D(m–nQ)).
- **Bézout dans K[X] :** ∃ P,P', tels que D= AP + BP'. Si A et B premiers entre eux ∃ P,P' tels que AP+BP'=1.
  L'algorithme d'Euclide permet de trouver les polynômes P et P' de l'égalité de Bézout. En effet chaque reste successif peut être exprimé en fonction de A et B à partir de R = A – BQ. Quand on en arrive à Rn–2 = QRn-1 +D, il suffit d'écrire Rn-2 et Rn-1 en fonction de A et B et on a Bézout.
- **Gauss:** Si C divise AB et que C est premier avec A , alors C divise B.
- **PPCM de A et B**. (A)∩(B) est un idéal. Son générateur unitaire est le PPCM de A et B. (M)= (A)∩(B

M unitaire est le PPCM de A et B	équivalent à	M est un multiple de A et de B Tout polynôme multiple de A et de B est un multiple de M

- A,B de PGCD D et de PPCM M on a (AB) =(DM)
  A =pD , B=qD , M =pqD donc AB = pqD^2 et DM = pqD^2

Polynômes irréductibles

- A ∈K[X] de degré n ≥ 1 est irréductible s'il n'est divisible que par les éléments non nuls de K.
  A est irréductible s'il n'a pas de diviseur de degré compris entre 1 et n–1. C'est le cas si deg(P) ≤ 1.
- Si A irréductible divise un produit de polynômes $A_1A_2..A_n$ alors A divise au moins l'un des A_i.
- Tout polynôme A non nul peut s'écrire de manière unique A =λ $\prod P_i^{n_i}$ où les P_i sont les diviseurs de A
- Si A = λ $\prod P_i^{n_i}$ et B=μ$\prod P_j^{n_j}$ Le PGCD de A et B est le produit des facteurs communs à l'exposant min(n_i,n_j)

Le PPCM de A et de B est le produit de tous les facteurs à l'exposant max(n_i ,n_j) pour les facteurs communs

Racines d'un polynôme

■ Fonction polynôme qui à x ∈K associe P(x) = $\sum a_i x^i$ à valeur dans K.
■ a est une racine de P si P(a) = 0
■ Si a est une racine de P, P est divisible par (x–a)
■ a est une racine d'ordre r si r est le plus grand entier naturel pour lequel P est divisible par $(x-a)^r$
■ Un polynôme de degré n a au plus n racines distinctes dans K.
■ P' polynôme dérivé de P si P'(x)= $\sum i a_i x^{i-1}$
■ a racine d'ordre 1 de P si et seulement si P(a) = 0 et P'(a) ≠ 0.
■ **Wilson:** p est premier si et seulement si (p –1) ! + 1 est divisible par p.

Fermat dit si p est premier et a non divisible par p → $a^{p-1} \equiv 1$ mod(p). Il en résulte que pour a compris entre 1 et p-1 $\bar{a}$ est racine de $X^{p-1} - \bar{1}$ dans $\mathbb{Z}/P\mathbb{Z}[X]$. D'où $X^{p-1} - \bar{1} = \prod_{i=1}^{i=p-1}(X - \bar{i})$. En développant on trouve $\overline{-1} = (-1)^{p-1}(p-1)!$ ou $-1 \equiv (-1)^{p-1}(p-1)!$ mod(p) et p divise (p–1) ! + 1. Inversement si on suppose que p divise (p–1) ! + 1, aucun des nombres de 2 à p–1 ne divise p sinon on aurait p=ak avec a et k entre 2 et n-1 et p=ak(reste de la factorielle) +1 ce qui est impossible. p est donc premier.

Les algèbres quotients de k[X] modulo un idéal

Dans ce qui suit (λ,β)∈K^2 et (X,Y)∈E^2. On omet les symboles multiplicatifs quand la nature des éléments composés est précisée.
■ **K-espace vectoriel E** : Groupe commutatif doté d'une loi de composition externe (λ,X)∈KXE →λX ∈E telle que (λ+β)X = λX+βX (λβ)X = λ(βX) λ(X+Y) =λX + λY 1X = X
■ **K-algèbre E**: E doté de 2 lois de compositions internes + et x telles que (E, +, x) soit un anneau et une loi de composition externe telle que (E,+,.) soit un K-espace vectoriel vérifiant . λ(XY) = (λX)Y = X(λY)
■ **Homomorphismes, isomorphismes de K-algèbres** : Applications k-linéaires et morphismes d'anneaux.

Structure de K-algèbre sur le quotient de K[X] modulo un idéal

Soit (P) un idéal de K[X] , P polynôme générateur .
Dans K[X] /(P) $\bar{A}$ = {A + λP}, $\overline{A+B} = \bar{A}\bar{B}$, $\bar{A} + \bar{B} = \overline{A+B}$ et on ajoute $\lambda\bar{A} = \overline{\lambda A}$
■ Si deg(P) = n le K-espace vectoriel E=K[X] /(P) est de dimension n. { $[X+(P)]^d$ avec 0≤ d ≤ n–1} base de E

Il faut comprendre que le reste de la division d'un polynôme de K[X] par P de degré n est de degré n–1 et peut s'écrire $\sum_{d=0}^{n-1} \lambda_d X^d$
Si P=$\sum_{d=0}^{n} a_d x^d$ dans K[X] /(P) on a $\bar{P} = \bar{0}$.
Les coordonnées de A dans la base de E sont: soit ses coefficients si deg(A)≤ n–1 soit les coefficients du reste de la division A/P.

Exemple: K=ℤ/2ℤ et $P=X^3+X+1$ sans racine dans K et irréductible dans K[X].
A =K[X] /(P) est un corps a 8 éléments qui sont (0 ou 1)X^2 +(0 ou 1)X +(0 ou 1).
Si α=X mod P on a P(α)=0 d'où P =(X–α)(X^2 + αX+ 1 +α^2)

■ On a (λ+(P))(P+(P))=λP+(P)=λ(P+(P)).
f: λ∈K → f(λ)= $\bar{\lambda}$ dans K[X] /(P) ={λ+(P)| λ∈K} est un isomorphisme entre K et le sous anneau {λ+(P)| λ∈K}
■ Les éléments inversibles de E sont les classes des polynômes premiers avec P.

Si P premier avec A ∃ U, V tels que PU + AV = 1 et comme $\overline{PU}$ = 0 on a $\overline{AV} = \bar{1}$ ce qui prouve que A est inversible.

■ 3 assertions équivalentes:

K[X] /(P) est intègre	P de degré ≥ 0 est irréductible dans k[X]	K[X] /(P) est un corps

■ Soit P de degré n irréductible dans K[X] . Il existe un corps L contenant K tel que P ait une racine dans L[X], l'espace vectoriel L[X] /(P) étant de dimension n.

P= $\sum a_d x^d$ irréductible. Posons A = K[X] /(P). C'est un corps. L'application h: de K dans A est définie par h(λ)=λ+(P).
W est le complémentaire de h(K) dans A. L est la réunion de h(K) et de W.
Pour λ∈K et q ∈W, l'application f de A dans L est définie par f(h(λ))=λ et f(q)=q. C'est une bijection de A sur L.
Lois sur L: Pour X et Y ∈L si x et y sont leurs antécédents par f, on définit les lois : X+Y=f(x+y), XY=f(xy) et λX = f(λx)
Donc A et L sont isomorphes, donc k-espace vectoriel de même dimension n, L contient f(h(K))= K, c'est donc un surcorps de K.
Soit α = X mod P Puisque $\bar{P}$ = 0 on a $\overline{\sum a_d x^d}$ =$\sum a_d \bar{x}^d$ = $\sum a_d \alpha^d$=0 et f(P(α))=0 ce qui dans L donne P(f(α)) = 0. f(α) racine.

■ Soit F polynôme unitaire de degré n de ℤ[X]. Si F a une racine dans ℚ elle est dans ℤ.