Chapitre 25

L'anneau euclidien des polynômes

Résumé -

Bien qu'il s'agisse encore de factorisation de polynôme, ce chapitre est totalement différent du précédent.
En nous concentrant sur la division euclidienne des polynômes, nous voyons que l'ensemble $\mathbb{K}[X]$ ressemble profondément à $\mathbb{Z}$.
Ce chapitre ressemble donc profondément au chapitre d'arithmétique sur $\mathbb{Z}$. On définit le PGCD de deux polynômes avec l'algorithme d'Eucllide adapté, la relation de Bézout, le lemme de Gauss..., puis le PPCM de deux ou plusieurs polynômes.
Les polynômes irréductibles sont les polynômes premiers de $\mathbb{K}[X]$. On retrouve les équivalents aux théorème d'Euclide (décomposition unique en produit de polynômes irréductibles). Dans $\mathbb{C}[X]$, les polynômes irréductibles sont les polynômes de degré $\leqslant 1$ (Théorème de d'Alembert-Gauss). Et dans $\mathbb{R}[X]$, il s'agit des polynômes de degré $\leqslant 1$ ou de degré 2 avec un discriminant $\Delta < 0$.
Toute la théorie des congruences s'exportent de $\mathbb{Z}$ à $\mathbb{K}[X]$... Ce chapitre est aussi pour nous l'occasion de donner quelques vocabulaires sur les anneaux (idéaux...).

Sommaire

1. Problèmes

? Problème 110 - Arithmétique

L'anneau $\mathbb{Z}$ n'est pas un corps, comme $\mathbb{K}[X]$.
Néanmoins, nous avons su développer tout un chapitre intéressant sur l'étude de $\mathbb{Z}$ en développant l'arithmétique. Si l'on reprend ce chapitre, on constate qu'à la racine des résultats (PGCD, nombres premiers et congruences...) se trouve la division euclidienne.
Or nous avons également une division euclidienne dans $\mathbb{K}[X]$ (à condition que $\mathbb{K}$ soit un corps).
Quels sont alors les résultats transposables de $\mathbb{Z}$ à $\mathbb{K}[X]$? Qu'est-ce que le PGCD de deux polynômes ? Quand est-ce qu'on peut dire qu'un polynôme est un polynôme premier ?

? Problème 111 - Fonction arithmétique (multiplicative)

Le chapitre d'arithmétique sur $\mathbb{Z}$ s'est conclue avec les fonctions arithmétiques vérifiant $f(ab) = f(a)+f(b)$ ou $f(ab) = f(a)f(b)$ pour $a \wedge b = 1$.
Existe-t-il des fonctions additives sur les polynômes : $f(PQ) = f(P) + f(Q)$ si $P \wedge Q = 1$? C'est le cas de la fonction degré ou la valuation R-adique.
Existe-t-il des fonctions multiplicatives sur les polynômes : $f(PQ) = f(P)f(Q)$ si $P \wedge Q = 1$?
C'est le cas évidemment de $f_k : P \mapsto P^k$. Peut-on définir un produit de convolution pour créer un groupe de fonction arithmétique ?

$$f * g : Q \mapsto \sum_{P|Q,\, P \text{ unitaire}} f(P)g(Q/P)$$

? Problème 112 - Théorèmes de Fermat

On sait que pour p premier, $n^p \equiv n[P]$.
A-t-on pour P, irréductible : $Q^P \equiv Q[P]$? Mais que peut signifier Q^P ?
Et le grand théorème de Fermat : Existe-t-il des polynômes A, B, C et un entier n tel que $A^n + B^n = C^n$?

? Problème 113 - Corps à p^k éléments

On démontre que concernant les corps finis, ils ne peuvent avoir pour cardinal uniquement des nombres de la forme p^k, avec p premier.
Nous savons déjà fabriqué LE corps à p éléments : il s'agit de $\frac{\mathbb{Z}}{p\mathbb{Z}}$.
Est-il possible de « fabriquer » LE corps à p^k éléments ?
La stratégie consiste à se placer sur le corps $\mathbb{Z}/p\mathbb{Z}$, puis l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$, et trouver un polynôme P de degré k irréductible dans cet anneau de polynômes et enfin de considérer l'ensemble quotient $\frac{\mathbb{Z}/p\mathbb{Z}}{(P)}$ (pour la relation d'équivalence $\cdot \equiv \cdot[P]$.
Est-il toujours possible de trouver un tel polynôme P irréductible, à tout degré ?
Comment montrer qu'on obtient bien un corps à p^k éléments ?

2. Division euclidienne dans $\mathbb{K}[X]$

2.1. Multiples d'un polynômes

Définition - B divise A
Soit $(A,B) \in \mathbb{K}[X]^2$, $B \neq 0$. On dit que B divise A dans $\mathbb{K}[X]$ s'il existe $Q \in \mathbb{K}[X]$ tel que $A = BQ$.
On dit aussi que A est divisible par B, que B est un diviseur de A, ou que A est un multiple de B. On note $B|A$.

Définition - Ensemble des multiples
Soit P un polynôme.
L'ensemble des multiples de P est noté $P\mathbb{K}[X]$ ou (P).

Théorème - Polynômes associés
Soient $P, Q \in \mathbb{K}[X]$ deux polynômes non nuls. On a

$$(P|Q \text{ et } Q|P) \Leftrightarrow (\exists \lambda \in \mathbb{K} \setminus \{0\}, Q = \lambda P)$$

On dit alors que P et Q sont des polynômes associés.
On a alors $P\mathbb{K}[X] = Q\mathbb{K}[X]$

Démonstration

Exercice
Montrer qu'il s'agit d'une relation d'équivalence

Théorème - Stabilité par combinaison linéaire
Soient $P, Q \in \mathbb{K}[X]$, $A \in \mathbb{K}[X]$, $A \neq 0$. Soient $\lambda, \mu \in \mathbb{K}$, $(\mu \neq 0)$. Alors

$$(A|P \text{ et } A|Q) \Leftrightarrow (A|P \text{ et } A|\lambda P + \mu Q)$$

En terme de multiple : $P, Q \in A\mathbb{K}[X] \Longleftrightarrow P$ et $(\lambda P + \mu Q) \in A\mathbb{K}[X]$.
On a plus largement encore pour $P, Q, R \in \mathbb{K}[X]$, $A \in \mathbb{K}[X]$, $A \neq 0$ et $\mu \in \mathbb{K}^*$,

$$(A|P \text{ et } A|Q) \Leftrightarrow (A|P \text{ et } A|RP + \mu Q)$$

Démonstration

Exercice
Soient $A, B \in \mathbb{R}[X]$.
Montrer que B divise A dans $\mathbb{R}[X]$ si et seulement si B divise A dans $\mathbb{C}[X]$.

Exercice
Soit $P \in \mathbb{K}[X]$. Montrer que $P(X) - X$ divise $P(P(X)) - X$.

2.2. Existence de la division euclidienne dans $\mathbb{K}[X]$

Théorème - Existence et unicité de la division euclidienne
Soit $(A,B) \in \mathbb{K}[X]^2$, $B \neq 0$. Alors il existe un unique couple $(Q,R) \in \mathbb{K}[X]^2$ vérifiant :

$$\begin{array}{ll} A = BQ + R & \\ \deg R < \deg B & (\Leftrightarrow R = 0 \text{ ou } 0 \leqslant \deg R < \deg B) \end{array}$$

On parle alors de division euclidienne (ou de division suivant les puissances décroissantes) de A par B.

Pour aller plus loin - Division selon les puissances croissantes ?
Lorsqu'on calcule des $DL_n(0)$, on cherche à écrire des puissances croissantes en x. Par exemple lorsqu'on cherche le $DL_3(0)$ de $\frac{x^4+2x^2-x+1}{x^3+x+1}$.
Dans ce cas là, on peut poser la division exactement à l'envers et obtenir :

$$(1-x+2x^2+x^4) = (1+x+x^3)(1-2x+4x^2-5x^3) +8x^4-4x^5+5x^6$$

Et donc

$$\frac{x^4+2x^2-x+1}{x^3+x+1} = 1-2x+4x^2-5x^3+O(x^4)$$

Démonstration

Remarque - Nécessité d'un corps $\mathbb{K}$
Le rôle du corps est assuré par l'existence de b_d^{-1}. Il faut donc au moins que b_d soit inversible (et par récurrence...) pour faire une division euclidienne de A par B.
Cette démonstration nous conduit au savoir-faire :

Savoir faire - Algorithme de division euclidienne
On remarque que cette démonstration (en tout cas la partie concernant l'existence) donne un algorithme pour obtenir Q puis R.

1. On divise le terme de plus haut degré de A par celui de B
   C'est possible car $\mathbb{K}$ est un corps, cela donne un facteur du type $\dfrac{a_{\deg(A)}}{b_{\deg(B)}} X^{\deg(A)-\deg(B)}$.
   On peut, par habitude, noter ce nombre sous B (dans un tableau $A|B$)
2. Puis on soustrait à A, toute la multiplication de B par ce facteur.
   On peut, par habitude, écrire cette multiplication sous A, ce qui permet de faire la soustraction aisément
3. On obtient un nouveau terme A_1
4. et on recommence la division, jusqu'à ce que $\deg A_n < \deg B$. On a alors $R = A_n$
   Cela se termine bien car la suite $(\deg(A_k))$ est une suite entière strictement décroissante

Exercice
Effectuer la division euclidienne de $A = X^5 + 2X^4 + 3X^2 + X + 4$ par $B = X^2 + 2X + 2$.

Pour aller plus loin - Méthode de Hörner-Ruffini
Il existe un algorithme, plus ou moins efficace selon l'habitude qu'on en a, pour faire la division euclidienne de deux polynômes.
Voir wikipedia ou le DS 6 de 2016-2017

Proposition - Divisibilité et division euclidienne
On l'équivalence :
$$B|A \Longleftrightarrow R = 0$$
où R est le reste de la division euclidienne de A par B.

Démonstration

2.3. Nature de $\mathbb{K}[X]$

Finalement,

Proposition - Structure de $\mathbb{K}[X]$
On suppose que $\mathbb{K}$ est un corps.
L'ensemble des multiples de P est un idéal principal de $\mathbb{K}[X]$.
$\mathbb{K}[X]$ est un anneau principal.

Exercice
A demontrer

On notera également :

Définition - Congruence
Soit $P, Q, T \in \mathbb{K}[X]$.
On dit que P est congru à Q modulo T, noté $P \equiv Q[T]$

si $P-Q$ est un multiple de T i.e. $P-Q \in T\mathbb{K}[X]$
ou encore $P = Q + K \times T$ avec $K \in \mathbb{K}[X]$.

Exercice
Montrer que $P \equiv Q[T] \Longleftrightarrow P\%T = Q\%T$.

3. Plus Grand Commun Diviseur

3.1. Heuristique

On note momentanément $\mathcal{D}(A)$ l'ensemble des diviseurs de $A \in \mathbb{K}[X]$.

Heuristique - PGCD

Soient A et B deux éléments de $\mathbb{K}[X]$ non nuls. $\mathcal{D}(A) \cap \mathcal{D}(B)$ est une partie non vide (contient 1) de $\mathbb{K}[X]$ dont les éléments sont de degré $\leqslant \max(\deg A, \deg B)$ donc $\{\deg P ; P \in \mathcal{D}(A) \cap \mathcal{D}(B)\} (\subset \mathbb{N})$ admet un plus grand élément d.
Tout élément de $\mathcal{D}(A) \cap \mathcal{D}(B)$ de degré d est appelé un *PGCD* (Plus Grand Commun Diviseur) de A et B.
On parlera parfois de « le » PGCD de A et de B, pour désigner le polynôme unitaire de $\mathcal{D}(A) \cap \mathcal{D}(B)$ de degré d. Les autres PGCD lui sont associés.

Ce n'est pas la définition que nous choisirons. Nous reprendrons la caractéristique, plus pratique, vue en arithmétique entière.

3.2. Algorithme d'Euclide et coefficients de Bézout

Lemme - Stabilité des diviseurs et algorithme d'Euclide
Soit $(A, B) \in \mathbb{K}[X]^2$. Si $A = BQ + R$, alors $\mathcal{D}(A) \cap \mathcal{D}(B) = \mathcal{D}(B) \cap \mathcal{D}(R)$.

Pour aller plus loin - Anneau euclidien
Un autre exemple d'anneau euclidien (muni d'une division euclidienne) : $\mathbb{Z}[i]$, l'anneau des entiers de Gauss.

Démonstration

Définition - Algorithme d'Euclide
On pratique l'algorithme d'Euclide pour les polynômes A et B.
- On commence par poser $R_0 = A$ et $R_1 = B$;
- ensuite, k désignant un entier naturel non nul, tant que $R_{k+1} \neq 0$, on note R_{k+2} le reste de la division euclidienne de R_k par R_{k+1} (on a donc $\deg R_{k+2} < \deg R_{k+1}$).

Comme il n'existe qu'un nombre fini d'entiers naturels entre 0 et $\deg R_0$, il existe $N \in \mathbb{N}^*$ tel que $R_N = 0$.
$\mathcal{D}(R_{N-1}) = \mathcal{D}(A) \cap \mathcal{D}(B)$.

Démonstration

Analyse - Suites (U_n) **et** (V_n)

Théorème - Couple de Bézout
A partir de l'algorithme d'Euclide, en considérant les suites (U_n) et (V_n) définies par $U_0 = 1$, $U_1 = 0$ et $V_0 = 0$, $V_1 = 1$ et

$$\forall\ n \in \mathbb{N}, \qquad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

On a
$$\forall\ n \in \mathbb{N}, \qquad R_n = U_n A + V_n B$$

En particulier, il existe $U, V \in \mathbb{K}[X]$ tel que $R_{N-1} = UA + VB$

Truc & Astuce pour le calcul - Suites (U_n) **et** (V_n)
Avec les mêmes notations, on a finalement les deux suites de polynômes (U_n) et (V_n) définies par la même relation de récurrence :

$$\forall\ n \in \mathbb{N}, \qquad U_{n+2} = U_n - Q_{n+1}U_{n+1}, V_{n+2} = V_n - Q_{n+1}V_{n+1}$$

avec pour conditions initiales : $U_0 = 1$, $U_1 = 0$ et $V_0 = 0$, $V_1 = 1$.
Comme pour le cours d'arithmétique de $\mathbb{Z}$, on peut faire le calcul au fur et à mesure dans un tableau.
Alors, pour tout $n \in \mathbb{N}$, $R_n = U_n \times A + V_n \times B$

Exercice
Pour tout $n \in \mathbb{N}_{N-1}$ que vaut $U_n V_{n+1} - V_n U_{n+1}$?

3.3. PGCD

Définition - PGCD et couple de Bézout
Soit $(A, B) \in \mathbb{K}[X]^2$, A, B non nuls. Il existe un polynôme D dont les diviseurs sont exactement les diviseurs communs à A et B, c'est-à-dire tel que

$$\forall P \in \mathbb{K}[X], (P|A \text{ et } P|B) \Longleftrightarrow P|D.$$

D est un *PGCD* de A et B et deux polynômes D_1 et D_2 vérifiant ces

hypothèses sont associés.
L'unique polynôme D unitaire vérifiant ces hypothèses est noté $A \wedge B$ (on dit aussi que c'est **le** PGCD de A et B).

Remarque - Relation d'équivalence
$\mathscr{R}$: $A\mathscr{R}B$ ssi A et B sont PGCD de deux polynômes identiques.
En fait, il s'agit d'une relation d'équivalence, la même que : $\mathscr{R}'$: $A\mathscr{R}'B$ ssi $\exists\, \lambda \in \mathbb{K}$ tel que $A = \lambda B$.
Les classes d'équivalences ont toutes un représentant naturel : un polynôme unitaire.
Avec cette définition, il faut montrer l'existence. La proposition suivante nous donne un exemple.

Proposition - Un PGCD
Le dernier reste non nul obtenu avec l'algorithme d'Euclide est un PGCD de A et B.

Démonstration

Comme $A \wedge B = \lambda R_{N-1}$:

Corollaire - Couple de Bézout
Il existe des polynômes U et V tels que $AU + BV = A \wedge B$.
(U, V) est un couple de Bézout de A et B.

Corollaire - Autre expression du PGCD
D est un PGCD de A et B si et seulement si

$$A\mathbb{K}[X] + B\mathbb{K}[X] = D\mathbb{K}[X]$$

Démonstration

Remarque - Elargissement de la définition
On élargit :

— On pose $A \wedge 0 = A$
— Il n'y a pas unicité du couple (U,V) puisque si (U_0,V_0) est un couple de Bezout, alors pour tout $Q \in \mathbb{K}[X]$, $(U_0 + QB, V_0 - QA)$ en est aussi un.
— En pratique, comme avec les entiers, on trouve (U,V) en utilisant l'algorithme d'Euclide et en éliminant les restes successifs.

Exercice
Déterminer $PGCD(A,B)$ ainsi qu'un couple de Bezout lorsque $A = X^3 + X^2 + 2$ et $B = X^2 + 1$.

Le théorème énonce beaucoup de choses, à démontrer...

Définition - Polynômes premiers entre eux
A et B sont dits premiers entre eux si $A \wedge B = 1$.

Théorème - Théorème de Bezout
Soient A et B deux polynômes non nuls. Alors

$$A \wedge B = 1 \Longleftrightarrow \exists (U,V) \in \mathbb{K}[X]^2 \text{ tel que } AU + BV = 1.$$

Démonstration

Exercice
Sans effectuer la division euclidienne, trouver un couple de Bézout pour les polynômes $(1-X)^5$ et $(1+X)^4$.

3.4. Lemme de Gauss et facteurs relativement premiers

Théorème - Lemme de Gauss
Soient A,B,C trois polynômes de $\mathbb{K}[X]$. Alors

$$(A \wedge B = 1 \text{ et } A|BC) \Rightarrow A|C.$$

Démonstration

Proposition - Facteurs relativement premiers
Soient A,B,C trois polynômes de $\mathbb{K}[X]$. Alors

$$(A \wedge B = 1 \text{ et } A \wedge C = 1) \Rightarrow A \wedge BC = 1 \text{ (réciproque vraie)}$$

$$(A \wedge B = 1,\ A|C,\ B|C) \Rightarrow AB|C$$

Démonstration

Corollaire - Bézout avec degré minimal
Soient A, B deux polynômes non constants, premiers entre eux.
Alors il existe un unique couple (U_0, V_0) tel que $AU_0 + BV_0 = 1$ avec $\deg U_0 < \deg B$, $\deg V_0 < \deg A$.
On a alors $U = U_0 + QB$ et $V = V_0 - QA$ avec $Q \in \mathbb{K}[X]$

Démonstration

Pour aller plus loin - Résultant
Il existe un objet : le résultant de deux polynômes qui permet de calculer directement (avec un déterminant matriciel) si ces deux polynômes ont un facteur commun. Bien exploiter, on peut aussi en déduire une décomposition de Bézout.

Par récurrence de la proposition : produit des polynômes premiers entre eux :

Corollaire - Facteurs premiers
Soient $A, C, B_1, \dots, B_n$ des polynômes.

$$(\forall i \in [\![1, n]\!], A \wedge B_i = 1) \Rightarrow A \wedge \prod_{i=1}^{n} B_i = 1$$

$$(\forall (i,j) \in [\![1, n]\!]^2, i \neq j \Rightarrow B_i \wedge B_j = 1 \text{ et } \forall i \in [\![1, n]\!], B_i | C) \Rightarrow \prod_{i=1}^{n} B_i \Big| C$$

3.5. Interprétation avec racines

Proposition - Factorisation (division)
Soit $P \in \mathbb{K}[X]$. Si $x_1, \dots, x_p$ sont p racines distinctes de P de multiplicités respectives égales à $m_1, \dots, m_p$, alors $\prod_{i=1}^{p} (X - x_i)^{m_i}$ divise P.

Démonstration

Corollaire - Nombre maximal de racines
Un polynôme non nul de degré n possède au plus n racines comptées avec leur multiplicité (c'est-à-dire comptées autant de fois que leur multiplicité).

Démonstration

Exercice
Trouver les polynômes $P \in \mathbb{R}_7[X]$ tels que $(X+7)\,P(X) = (X-5) \times P(X+2)$

3.6. PGCD de plusieurs polynômes

La notion de PGCD peut être étendue à un nombre fini de polynômes :

Proposition - PGCD de plusieurs polynômes
Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(A_1, A_2, \ldots, A_k) \in \mathbb{K}[X]^k$. Il existe un unique polynôme nul ou unitaire P dont les diviseurs sont exactement les diviseurs communs à tous les A_i, c'est-à-dire tel que

$$\forall T \in \mathbb{K}[X], (\forall i \in [\![1,k]\!],\ T|A_i) \Leftrightarrow T|P$$

En fait, on a $\mathscr{D}(P) = \bigcap_{i=1}^{k} \mathscr{D}(A_i)$.
On l'appelle PGCD de $A_1, A_2, \ldots, A_k$ et on le note $A_1 \wedge A_2 \wedge \ldots \wedge A_k$ ou $\bigwedge_{i=1}^{k} A_i$.
On a de plus l'identité de Bézout :

$$\exists (U_1, \ldots, U_k) \in \mathbb{K}[X]^k \,|\, P = \sum_{i=1}^{k} U_i A_i.$$

Encore : $A_1\mathbb{K}[X] + A_2\mathbb{K}[X] + \cdots + A_k\mathbb{K}[X]$ est l'idéal engendré $P\mathbb{K}[X]$.

Démonstration

La proposition suivante permet de justifier la notation associative $\bigwedge_{i=1}^{k} A_i$

Proposition - PGCD par récurrence
Soient $k \in \mathbb{N}^*$, $k \geqslant 2$, et $(A_1, A_2, \dots, A_k) \in \mathbb{K}[X]^k$.
$\bigwedge_{i=1}^{k} A_i = \left(\bigwedge_{i=1}^{k-1} A_i\right) \wedge A_k$

Démonstration

Définition - Polynômes premiers entre eux (dans leur ensemble)
Les polynômes $A_1, \dots, A_k$ sont dits **premiers entre eux dans leur ensemble** si leur PGCD vaut 1.

Attention - Polynômes premiers entre eux
Une famille de polynômes premiers entre eux deux à deux est une famille de polynômes premiers entre eux dans leur ensemble.
La réciproque est fausse.
On peut le démontrer avec une décomposition de Bézout

Proposition - Théorème de Bézout
Soient $A_1, \dots, A_k$ des polynômes. Alors

$$\bigwedge_{i=1}^{k} A_i = 1 \Leftrightarrow \exists (U_1, \dots, U_k) \in \mathbb{K}[X]^k \mid \sum_{i=1}^{k} U_i A_i = 1$$

Démonstration

4. Plus Petit Commun Multiple

4.1. Caractérisation essentielle

Heuristique - PPCM

Soient A et B deux polynômes non nuls.
L'ensemble des multiples communs à A et B est non vide (contient AB) donc l'ensemble des degrés des multiples communs à A et B et non nul, est une partie non vide de $\mathbb{N}$ donc admet un plus petit élément.
Un multiple de A et B de plus petit degré est appelé un $PPCM$ (Plus Petit Commun Multiple) de A et B.

Pour aller plus loin - UN/LE PPCM
On devrait parler d'UN PPCM si il s'agit d'un polynôme associé à LE PPCM

Définition - Caractérisation essentielle du PPCM
Soit $(A, B) \in \mathbb{K}[X]^2$. Il existe un unique polynôme M nul ou unitaire dont les multiples sont exactement les multiples communs à A et B, c'est-à-dire tel que

$$\forall P \in \mathbb{K}[X],\ (A|P \text{ et } B|P) \Leftrightarrow M|P$$

M est appelé **le** $PPCM$ de A et B, noté $A \vee B$.

Démonstration

Une autre caractérisation essentielle

Corollaire - Autre caractérisation
M est un PPCM de A et B si et seulement si

$$A\mathbb{K}[X] \cap B\mathbb{K}[X] = M\mathbb{K}[X]$$

Démonstration

4.2. Relation PGCD/PPCM

Proposition - Relation PGCD et PPCM
Soient $A, B \in \mathbb{K}[X]$ non nuls.
- si $A \wedge B = 1$ alors $\exists \lambda \in \mathbb{K}^* \mid AB = \lambda(A \vee B)$.
- dans le cas général, $\exists \lambda \in \mathbb{K}^* \mid AB = \lambda(A \wedge B) \times (A \vee B)$.

Pour aller plus loin - Un lien avec les ensembles
Quel est le lien entre cette formule est la suivante?
$cardA + cardB = card(A \cup B) + card(A \cap B)$.

Démonstration

Heuristique - Décomposition

On peut retenir que si $A = (A \wedge B)A'$, et $B = (A \wedge B)B'$,
alors A' et B' sont premiers entre eux,
et alors $\lambda A \vee B = (A \wedge B)A'B'$.
Et donc : $A \times B = (A \wedge B)A' \times (A \wedge B)B' = (A \wedge B) \times (A \wedge B)A'B' = \lambda(A \wedge B) \times (A \vee B)$

Exercice
Déterminer le PGCD, le PPCM et un couple de Bezout lorsque $A = X^3 + 3X^2 + 3X + 2$ et $B = X^5 + 3X^4 + 2X^3 - 2X^2 - 3X + 2$.

5. Polynômes irréductibles

5.1. Décomposition unique en produit d'irréductibles

Les polynômes irréductibles jouent ici le même rôle que les nombres premiers dans $\mathbb{Z}$. Les polynômes inversibles sont les polynômes de degré 0 :

Définition - Polynômes irréductibles
$P \in \mathbb{K}[X]$ est dit irréductible si

$$(P = AB,\ A, B \in \mathbb{K}[X]) \Rightarrow \deg A = 0 \text{ ou } \deg B = 0$$

Proposition - Polynôme (de degré 1) irréductible
Quel que soit le corps $\mathbb{K}$ et $\alpha \in \mathbb{K}$, le polynôme $X - \alpha$ est irréductible sur $\mathbb{K}$.

Démonstration

Pour aller plus loin - Polynômes premiers
On dit que p est premier s'il n'est divisible que par 1 et lui-même.
Ici, cette définition ne colle pas bien.
En fait, on a p est premier si $p = ab \Rightarrow a$ ou $b \in \{-1, 1\}$.
Et plus généralement : p est premier si $p = ab \Rightarrow a$ ou b inversible

Proposition - Polynômes irréductibles et polynômes premiers entre eux
Un polynôme irréductible est premier avec tous les polynômes qu'il ne divise pas.
Un polynôme irréductible divise un produit si et seulement si il divise l'un des facteurs.

Démonstration

Théorème - Décomposition en produit de facteurs polynomiaux irréductibles
Tout polynôme non constant de $\mathbb{K}[X]$ est le produit d'un scalaire (élément de $\mathbb{K}$) par un produit de polynômes irréductibles unitaires de $\mathbb{K}[X]$.
Cette décomposition est unique à l'ordre des facteurs près.

Démonstration

Proposition - Critère de divisibilité par polynômes irréductibles
Soient $A, B \in \mathbb{K}[X]$ non nuls. Si

$$A = \lambda P_1^{\alpha_1} P_2^{\alpha_2} \dots P_k^{\alpha_k} \text{ et } B = \mu P_1^{\beta_1} P_2^{\beta_2} \dots P_k^{\beta_k}$$

où les P_i sont irréductibles unitaires distincts deux à deux, $\alpha_i, \beta_i \in \mathbb{N}$ (éventuellement nuls), alors

$$A | B \Leftrightarrow \forall i \in [\![1, k]\!], \alpha_i \leqslant \beta_i$$

$$A \wedge B = \prod_{i=1}^{k} P_i^{\min(\alpha_i, \beta_i)}$$

$$A \vee B = \prod_{i=1}^{k} P_i^{\max(\alpha_i, \beta_i)}$$

Démonstration

5.2. Décomposition dans $\mathbb{C}[X]$

Rappel :

Théorème - Théorème de d'Alembert-Gauss
Soit $P \in \mathbb{C}[X]$, $\deg P \geqslant 1$. Alors P possède au moins une racine dans $\mathbb{C}$.

Corollaire - Décomposition dans $\mathbb{C}$
Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.

Démonstration

Théorème - $\mathbb{C}$ est algébriquement clos
Tout polynôme non nul P de $\mathbb{C}[X]$ se décompose de manière unique (à une permutation près) sous la forme

$$P = \lambda \prod_{i=1}^{p} (X - x_i)^{m_i}$$

où les $x_i \in \mathbb{C}$ sont distincts et $\sum_{i=1}^{p} m_i = \deg P$.
Tout polynôme non nul de $\mathbb{C}[X]$ est donc scindé sur $\mathbb{C}$ ($\mathbb{C}$ est dit algébriquement clos).

Démonstration

Savoir faire - Décomposition en produit d'irréductibles de $\mathbb{C}[X]$
Sur $\mathbb{C}[X]$, les polynômes irréductibles sont de degré 1.
Donc décomposer un polynôme P sur $\mathbb{C}[X]$ en produit d'irréductibles est équivalent à chercher toutes les racines de P, en tenant compte de leur ordre de multiplicité.
En règle générale, on choisit, les facteurs, unitaires et on multiplie le

- produit par λ, le coefficient dominant de P.

En appliquant le critère de divisibilité par des irréductibles :

Corollaire - Critère de divisibilité dans $\mathbb{C}$
Soient $P, Q \in \mathbb{C}[X]$. Alors $P|Q$ dans $\mathbb{C}[X]$ si et seulement si les racines de P sont des racines de Q avec une multiplicité inférieure dans P.

Exercice
Démontrer à nouveau que $P(X) - X$ divise $P(P(X)) - X$.
On commencera par faire l'étude dans $\mathbb{C}$, puis dans $\mathbb{K}$.

5.3. Décomposition dans $\mathbb{R}[X]$

Comme $\mathbb{R}[X] \subset \mathbb{C}[X]$, on sait qu'un polynôme P de $\mathbb{R}[X]$ tel que $\deg P \geqslant 1$ admet dans $\mathbb{C}$ $\deg P$ racines comptées avec leur multiplicité.

Proposition - Conjugaison des racines
Si $z_0 \in \mathbb{C}$ est racine de multiplicité m de $P \in \mathbb{R}[X]$,
alors il en est de même de $\overline{z_0}$.

Démonstration

Proposition - Si $\deg P$ est impair
Soit $P \in \mathbb{R}[X]$ tel que $\deg P$ soit impair. Alors P a au moins une racine dans $\mathbb{R}$.

Démonstration

Proposition - Description des irréductibles de $\mathbb{R}[X]$
Les polynômes irréductibles dans $\mathbb{R}[X]$ sont
- les polynômes de degré 1,
- les polynômes de degré 2 à discriminant strictement négatif.

Démonstration

Théorème - Factorisation dans $\mathbb{R}[X]$
Tout polynôme non nul de $\mathbb{R}[X]$ se factorise de manière unique (à une permutation près) sous la forme

$$P = \lambda \prod_i (X-\alpha_i)^{m_i} \prod_j (X^2 + b_j X + c_j)^{p_j}$$

où les α_i, b_j, c_j sont des réels, m_i, p_j des entiers tels que

$$\sum_i m_i + 2\sum_j p_j = \deg P, \qquad \text{et} \qquad b_j^2 - 4c_j < 0.$$

Démonstration

Si la factorisation n'est pas évidente, on peut exploiter le savoir-faire suivant :

Savoir faire - Décomposition en produit d'irréductibles de $\mathbb{R}[X]$
On décompose P sur $\mathbb{C}[X]$.
Si α est racine d'ordre m, alors $\overline{\alpha}$ également.
Le polynôme $(X^2 - 2\mathrm{Re}(\alpha)X + |\alpha|^2)^m$ divise P et est irréductible sur $\mathbb{R}[X]$.

Exercice
Décomposer $2X^4+2$ dans $\mathbb{C}[X]$ et dans $\mathbb{R}[X]$.

Exercice
Décomposer dans $\mathbb{R}[X]$ le polynôme $X^{2n}-1$.
Que vaut le produit des racines $2n$-ièmes de l'unité ?

Exercice
Soit $z_0, \dots, z_{n-1}$ les racines n-ièmes de l'unité. Montrer que

$$\prod_{k=0}^{n-1} (z_k^2 - 2z_k \cos\theta + 1) = 4\sin^2(\frac{n\theta}{2}).$$

6. Bilan

Synthèse

⇝ $\mathbb{K}[X]$, comme $\mathbb{Z}$ est muni d'une division euclidienne.

$\rightsquigarrow$ On définit alors l'algorithme d'Euclide pour deux polynômes. Il conduit à la notion de PGCD de ces deux polynômes. Toute la structure est transportée de $\mathbb{Z}$ à $\mathbb{K}[X]$: PGCD, couple de Bézout, lemme de Gauss, PPCM, généralisations... Les méthodes sont identiques.
On peut exploiter en outre : les racines, la dérivations et le changement d'origine!

$\rightsquigarrow$ Les nombres premiers deviennent les polynômes irréductibles. Le théorème d'Euclide d'écriture comme produit unique d'irréductibles (unitaires) est toujours vraie.
Une description complète des irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$ est possible et assez simple.

$\rightsquigarrow$ On termine par une extension hors-programme de la notion de congruence.
Et plus largement de la notion d'anneau euclidien (factoriel...) et d'idéaux...

Savoir-faire et Truc & Astuce du chapitre

— Savoir-faire - Algorithme de la division euclidienne
— Truc & Astuce pour le calcul - Suites (U_n) et (V_n)
— Savoir-faire - Décomposition en produit d'irréductibles de $\mathbb{C}[X]$
— Savoir-faire - Décomposition en produit d'irréductibles de $\mathbb{R}[X]$

Notations

Notations	*Définitions*	*Propriétés*	*Remarques*
$\mathscr{D}(A)$	Ensemble des diviseurs de A		
$A\mathbb{K}[X]$ ou (A)	Ensemble des multiples de A		
$A \wedge B$	PGCD de A et B (généralisable)	$(A)+(B)=(A\wedge B)$	Défini à une constante multiplicative près
$A \vee B$	PPCM de A et B (généralisable)	$(A)\cap(B)=(A\vee B)$	Défini à une constante multiplicative près

Retour sur les problèmes

110. C'est le but de ce cours.
111. Considérons $f\star g : P \mapsto \displaystyle\sum_{D|P\,,\,D \text{ unitaire}} f(D)g(P/D)$.
On a toujours, pour $P\wedge Q=1$, $D|PQ \iff D=D_1D_2$ avec $D_1|P$, $D_2|P$.
Dans ce cas $\Phi : D \mapsto (D_1,D_2) := (D\wedge P, D\wedge Q)$ établit une bijection $\mathscr{D}(PQ)$ sur $\mathscr{D}(P)\times\mathscr{D}(Q)$.
Supposons que f et g soient multiplicative. Alors on a, pour $P\wedge Q=1$:
$$f\star g(PQ) = \sum_{D|PQ \text{ unitaire}} f(D)g(PQ/D) = \sum_{D_1|P,D_2|Q, \text{ unitaires}} f(D_1D_2)g(PQ/D_1D_2)$$
$$= \sum_{D_1|P,D_2|Q, \text{ unitaires}} f(D_1)f(D_2)g(P/D_1)g(Q/D_2) = f(P)\times g(Q)$$
L'élément neutre est $f:1\mapsto 1$ et $f:P\mapsto 0$ si $P\neq 1$.
Tout est pareil! avec une fonction de Möbius....
La question est : que peut nous apprendre alors un tel outil?
112. Concernant le grand théorème de Fermat, on parle ici du théorème de Liouville.
Supposons que $P^n+Q^n+R^n=0$ avec $P,Q,R\in\mathbb{C}[X]$ (avec $n\geqslant 3$).
(a) On commence par montrer qu'il suffit d'étudier le cas P,Q,R premiers entre eux deux à deux
(sinon, si $D|P$ et $D|Q$, alors $D|R$, et on peut simplifier)
(b) On dérive $\dfrac{P^n}{R^n}+\dfrac{Q^n}{R^n}=-1$(qu'on ne peut pas faire avec les entiers) :
$$P^{n-1}(PR'-RP') = -Q^{n-1}(QR'-RQ')$$

(c) Si P et R ne sont pas associés, alors $PR' - R'P \neq 0$.
Puis $Q \wedge P = 1$, donc $Q^{n-1}|PR' - R'P$ et de même $P^{n-1}|QR' - R'Q$.
On ne peut avoir $\deg R > \max(\deg P, \deg Q)$, donc au moins un des $\deg P$ ou $\deg Q$ est le maximum de $\{\deg P, \deg Q, \deg R\}$.
Supposons que $p = \deg P = \max(\deg Q, \deg R)$.
Par division $P^{n-1}|QR' - RQ'$, alors $\deg P^{n-1} = (n-1)p \leqslant \deg Q + \deg R - 1 < 2\deg P$.
Contradiction, puisque $n \geqslant 3$, donc $n-1 \geqslant 2$ (sauf si $\deg P = 0\dots$)

113. Classiquement, on noteF_p, le corps $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}, +, \times\right)$. On se place donc sur $F_p[X]$, les polynômes à coefficients dans F_p.
Si P est un polynôme irréductible de $F_p[X]$, et de degré n,
alors $\dfrac{F_p[X]}{(P)}$, l'ensemble des classes d'équivalences pour la relation $\cdot \equiv \cdot [P]$
et un corps. On exploite le théorème de Bézout.
Cet ensemble possède comme ensemble de représentant $\{Q \in F_p[X] \mid \deg Q < n\}$, de cardinal p^n.
Existe-t-il un tel polynôme irréductible ? Oui !
Comment en trouver ? On exploite le lemme suivant :
Pour tout $r \in \mathbb{N}$, sur F_p, le polynôme $R = X^{p^r} - X$ est égal au produit de tous les polynômes unitaires irréductibles de degré divisant r.
Cela donne la minoration :

$$\text{Nbre de polynôme de degré } n \text{ irréductible} \geqslant \frac{p^n - p^{\lfloor n/2 \rfloor + 1}}{n}$$

Et précisément, P de degré n est irreductible sur F_p ssi :
— $P|X^{p^n} - X$
— $\forall\ q \in \mathscr{P}$ tel que $q|n$, $P \wedge X^{p^{n/q}} - X = 1$
(... Voir Wikipedia ou le cours de Demazure p.220)