.

Racines de polynômes gauches

et

transformations pseudo-linéaires

Limoges, le 18 janvier 2012

Plan :

1) Introduction.

2) Anneaux de polynômes.
   A) Définition des anneaux de polynômes gauches.
   B) Exemples
   C) Propriétés et remarques.

3) Applications polynomiales non commutatives
   A) Défintions et exemples.
   B) Polynômes à coefficients dans des algèbres à division.

4) Applications pseudo-linéaires.
   A) Définition et lien avec les applications polynomiales.
   B) Exemples.
   C) Propriétés.
   D) Formule du produit généralisée.

5) Applications.
   A) Applications aux corps finis.
   B) Polynômes unitaires et PPCM.
   C) Applications aux codes.

1 Introduction

-Anneaux de polynômes gauches introduits par Oystein Ore (1933).
-Transformations Pseudo-linéaires Jacobson (1937),
-S.A. Amitsur, Bergman, Cauchon, P.M. Cohn, K. Goodearl, T.Y.Lam,...
-Applications : Opérateurs différentiels (livre récent d'Henri Bourlès et Bogdan Marinescu, 2011), contre exemples (Bergman, Cohn, Schofield,...), théorie des codes non commutatifs.

2 Anneau de polynômes non commutatifs

A) Définition d'une extension de Ore

A un anneau, $1 \in A$.
Structure d'anneau sur le A-module $R := A^{\oplus \mathbb{N}}$?
$a = (a_0, \dots, a_n, 0, \dots,), b = (b_0, \dots, b_l, 0, \dots,) \in R$, comment définir ab ?
Posons : $e_i = (0, \dots, 1, 0 \dots, 0 \dots)$ pour $i \in \mathbb{N}$, donc $a = \sum a_i e_i$ où $a_i \in A$.

contraintes :
(C1) $e_i e_j = e_{i+j}$ (for $i, j \in \mathbb{N}$).

Donc si on pose $e_i = e_1^i$ et $t := e_1$, les éléments de R s'écrivent de manière unique

$$\sum a_i t^i, \ a_i \in A.$$

On doit définir tb pour $b \in A$.
Autres contraintes :

(C2) $\forall a \in A, \ ta \in A + At$

Il existe des applications σ, δ de A vers A telles que $ta = \delta(a) + \sigma(a)t$.
$t(a+b) = ta + tb, \implies \sigma, \delta \in End(A, +)$
$t(ab) = \sigma(ab)t + \delta(ab)$
$(ta)b = (\sigma(a)t + \delta(a))b = \sigma(a)(tb) + \delta(a)b$
$\quad = \sigma(a)\sigma(b)t + \sigma(a)\delta(b) + \delta(a)b.$
$\sigma(ab) = \sigma(a)\sigma(b)$ et $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$

Les éléments de R sont des polynômes en t i.e. des sommes finies $\sum a_i t^i$, $a_i \in A$ et $ta = \sigma(a)t + \delta(a)$, for $a \in A$.

Définitions 2.1. Soit A un anneau unitaire et σ un endomorphisme de l'anneau A.

(a) Une application additive $\delta \in End(A, +)$ est une σ-dérivation si, pour tout $a, b \in R$, on a :

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b, \text{ for } a, b \in A.$$

(b) $\sum a_i t^i \in R = A[t; \sigma, \delta]$. Addition : comme pour les polynômes usuels et la multiplication est basée sur la loi de commutation

$$tr = \sigma(r)t + \delta(r).$$

(c) Le degré d'un polynôme non nul $f = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$ est défini par $\deg(f) = max\{i | a_i \neq 0\}$ et on pose $\deg(0) = -\infty$.

B) Exemples

Exemples 2.2. (1) Si $\sigma = id.$ et $\delta = 0$ on a $A[t; \sigma, \delta] = A[t]$.
Si $\sigma = id.$ mais $\delta \neq 0$ on note $A[t; id., \delta] = A[t; \delta]$ (polynômes différentiels) ;
Si $\delta = 0$ mais $\sigma \neq id.$ on écrit $A[t; \sigma, \delta] = A[t; \sigma]$ (type endomorphisme).

(2) $\mathbb{C}[t; \sigma]$; σ conjugaison in $\mathbb{C}$; $a \in \mathbb{C}$, $ta = \sigma(a)t$
$t^2 a = \sigma^2(a)t^2 = at^2$ $\quad$ $t^2, t^2 + 1$ sont des polynômes centraux.
$\mathbb{H} \cong \mathbb{C}[t; \sigma]/(t^2 + 1)$.

(3) Soit k un corps, $R = k[x][t; id.; d/dx]$ (algèbre de Weyl) relation

$$tx - xt = 1.$$

Si char$k = 0$ l'algèbre est un anneau simple.
Par contraste si char$k = p > 0$ alors t^p et x^p sont des éléments centraux.
EX : char$k = 3$; $tx^3 = x^3 t + d/dx(x^3) = x^3 t + 3x^2 = x^3 t$.
$t^3 x = t^2(xt + 1) = t(xt + 1)t + t^2 = txt^2 + 2t^2$
$= (xt + 1)t^2 + 2t^2 = xt^3 + 3t^2 = xt^3$

(4) Soit $A := k(x)$, k un corps, σ le k-endomorphisme de A défini par $\sigma(x) = x^2$. $R := A[t;\sigma]$ est intègre.

R n'est pas un domaine de Ore à droite ($tR \cap xtR = 0$). En particulier, R n'est pas noethérien à droite.

R est un anneau intègre principal à gauche mais non noethérien à droite.

(5) Pour $a \in A$ on définit la σ-dérivation interne induite par a : $d_a(r) := ar - \sigma(r)a$. Remarquons que $A[t;\sigma,d_{a,\sigma}] = A[t-a,\sigma]$.

Pour un automorphisme interne I_a, induit par a : $A[t;I_a] = A[a^{-1}t]$.

(6) Soit $0 \neq q \in k$, k un corps, σ le k-endomorphisme de $A := k[x]$ défini par $\sigma(x) = qx$; $R_q := k[x][y;\sigma]$. C'est ce que l'on appelle le plan quantique.

$$i,j > 0\ ,\ y^j x^i = q^{ij} x^i y^j.$$

R_q est un anneau noethérien.

Quelques définitions :

1. Pour $n > 0$ on définit $(n)_q = 1 + q + \cdots + q^{n-1} = \frac{q^n-1}{q-1}$.
2. Pour $n > 0$, $(n)!_q = (1)_q(2)_q \ldots (n)_q = \frac{(q-1)(q^2-1)\ldots(q^n-1}{(q-1)^n}$ tandis que $(0)!_q = 1$ (bien sur $(n)!_q$ est appelé q-factoriel de n).
3. Pour $0 \leq k \leq n$ on pose $\binom{n}{k}_q := \frac{(n)!_q}{(k)!_q(n-k)!_q}$.

En utilisant ces définitions on a :

a) $\binom{n}{k}_q$ est un polynôme en q à coefficients entiers.
b) $\binom{n}{k}_q = \binom{n}{n-k}_q$.
c) $\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k\binom{n-1}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q$.
d) Si $yx = qxy$ alors $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}_q x^k y^{n-k}$.

Ex : $(x+y)^2 = x^2y+xy+yx+y^2 = x^2+(1+q)xy+y^2 = x^2+2_q+y^2$.

Beaucoup de groupes quantiques peuvent être construits comme des extensions de Ore itérées.

(7) Soit p un nombre premier, $n \in \mathbb{N}$ et $q = p^n$. Considérons $A = \mathbb{F}_q$ un corps fini et θ l'automorphisme de Frobenius défini par $\theta(a) = a^p$ pour $a \in A = \mathbb{F}_q$. L'extension de Ore $A[t;\theta]$ a été utilisée récemment en théorie des codes non commutatifs.

C) Propriéts et remarques

Proposition 2.3. *Soit $R = A[t;\sigma,\delta]$ un anneau de polynômes gauches sur un anneau A.*

(a) Si A est intègre et σ est injectif R est intègre.

(b) (Ore, 1933) Si $A = K$ est un corps alors R est un, anneau principal à gauche. il est noethérien à droite (et alors principal à droite) si et seulement si σ est un automorphisme.

(c) (Ore, P.M. Cohn) Si K est un corps $K[t;\sigma,\delta]$ est un domaine de Ore à gauche : son corps des fractions à gauche est noté $K(t;\sigma,\delta)$.

(d) Si $p(t) \in R$ est un polyynôme unitaire alors pour tout polynôme $f(t) \in R$ il existe $q(t), r(t) \in R$ tel que $f(t) = p(t)q(t) + r(t)$ et $deg(r(t)) < deg(p(t))$.

(e) (Ore)Si A est un corps (=algèbre à division) R est un domaine de factorisation unique i.e. tout élément $f \in R$ peut s'écrire comme un produit de polynômes irréductibles et si $f = p_1 \cdots p_n = q_1 \cdots q_m$ sont deux telles écritures alors $m = n$ et il existe une permutation $\pi \in S_n$ telle que pour tout $1 \leq i \leq n$, il existe un isomorphisme $R/Rp_i \cong R/Rq_{\pi(i)}$.

(f) (Lam,Leroy,Leung,Matczuk) Introduction des polynômes invariants et semi-invariants. Critère pour que $R = A[t; \sigma, \delta]$ (A un corps ou un anneau simple) soit simple, structure des idéaux.

(g) (Leroy, Matczuk) Comme en (f) pour A un anneau premier (utilisation des anneaux des quotients de Martindale).

3 Applications polynomiales non commutatives

A) Définition et exemples

Définition 3.1. (Lam, L.)
$f(t) \in R = A[t; \sigma, \delta]$ and $a \in A$

$$\exists Q(t) \in \ \exists r \in A \text{ such that } f(t) = q(t)(t-a) + r$$

L'application polynomiale associée à $f(t)$ est l'application $f : A \longrightarrow A$ définie par $f(a) := r$.

Pour $i \geq 0$, on note N_i l'application polynomiale déterminée par t^i.

Donnons quelques exemples.

Exemples 3.2. 1. Si $\sigma = id.$ et $\delta = 0$ on retrouve les appliactions polynomiales classiques : $\sum(c_i t^i)(a) = \sum c_i a^i$.

2. $N_0(A) = 1, N_1(a) = a,\ N_2(a) = \sigma(a)a + \delta(a)$,

$$\forall a \in A,\ N_{i+1}(a) = \sigma(N_i(a))a + \delta(N_i(a)).$$

3. Si k est un corps, le nombre de racines de $f(t) \in k[x]$ est borné par son degré $\deg(f(x))$.

   -Ceci est faux si on travaille avec un anneau (même commutatif) : $(x-2)(x-1) \in \frac{\mathbb{Z}}{4\mathbb{Z}}[x]$.

   -Ceci est faux dans un contexte non commutatif (même sur un corps) : $t^2 + 1 \in \mathbb{H}[t]$ possède une infinité de solution : ce sont exactement tous les conjugués de i.

   -Un anneau R est dit avoir la propriété FZP (finite zero property) si pour tout $f(x) \in R[x]$, le nombre des racines de $f(x)$ dans R est fini. (Fuchs et al.).

-Le nombre de racines d'un polynôme à coefficients sur un anneau de matrices à coefficients complexe a été étudié par Wilson et son étudiant(e) (Slusky).

4. Attention lorsque l'on travaille avec les racines à droite d'un polynôme. Par exemple, si $\mathbb{H}$ est le corps des quaternions sur $\mathbb{R}$, dans $\mathbb{H}[t]$ le polynôme $f(t) := (t-j)(t-i) = t^2 - (i+j)t + ji$ est tel que $f(j) = j^2 - (i+j)j + ji = 2ji \neq 0$. Ceci signifie que j n'est pas racine *à droite* de $f(t)$. En fait, i est la seule racine (à droite) de $(t-j)(t-i)$.

5. Si $\delta = 0$, il est facile de vérifier que pour $i > 0$ l'application polynomiale associée à $f(t) = t^i \in K[t;\sigma]$ est la i^{eme}-norme i.e. $N_i(a) = \sigma^{i-1}(a)\ldots\sigma(a)a$, et donc si $f(t) = \sum_{i=0}^{n} c_i t^i \in K[t;\sigma]$, et $a \in K$, on a $f(a) = \sum_{i=0}^{n} c_i \sigma^{i-1}(a)\ldots\sigma(a)a$.

6. Notons "$-$" la conjugaison sur le corps des nombres complexes $\mathbb{C}$. Le polynôme $t^2 - i \in \mathbb{C}[t;-]$ ne possède aucune racine (à droite) et donc il est irréductible. Ceci montre qu'il existe des polynômes irréductibles de degré deux dans $\mathbb{C}[t;-]$. Bien sur ceci contraste avec le cas des polynômes classiques. ring $\mathbb{C}[t]$.

7. Si $\sigma = id.$ on peut montrer $N_2(a) = t^2(a) = a^2 + \delta(a)$ et $N_3(a) = a^3 + 2\delta(a)a + a\delta(a) + \delta^2(a)$. Si $\delta(a)$ commute avec a et la caractéristique de K est 3 alors $N_3(a) = a^3 + \delta^2(a)$.

8. Soit $\mathbb{F}_q$ le corps à $q = p^n$ éléments (p est premier). Considérons θ l' automorphisme de Frobenius sur $\mathbb{F}_q$ défini par $\theta(x) = x^p$ pour $x \in \mathbb{F}_q$. Comme en théorie quantique écrivons, pour $n \geq 1$, $[n]$ pour $\frac{p^n-1}{p-1}$ et posons $[0] = 0$. Il est alors facile de montrer que, pour $f(t) := \sum_{i=0}^{m} a_i t^i \in \mathbb{F}_q[t;\theta]$ et $b \in \mathbb{F}_q$, on a $f(b) = \sum_{i=0}^{m} a_i b^{[i]}$.

B) Applications polynomiales sur des algèbres à division.

$A = K$ un corps (non nécessairement commutatif) $a \in K$, et $c \in K$, $c \neq 0$, posons :

$$a^c := \sigma(c)ac^{-1} + \delta(c)c^{-1}.$$

Soit $f, g \in R = K[t; \sigma, \delta]$.
- Si $g(a) = 0$ alors $(fg)(a) = 0$.
- Si $g(a) \neq 0$, alors $(fg)(a) = f(a^{g(a)})g(a)$ (**Formule du produit**).

Exemples 3.3. 1. Supposons $a \neq b \in K$,

Trouver c tel que $(t - c)(t - b) \in R(t - a)$?

c ? tel que $(t - c)(t - b)(a) = 0$

Ici $g(t) = t - b$, $f(t) = t - c$, $g(a) = a - b$ et $f(a^{g(a)}) = a^{a-b} - c$

donc $(t - c)(t - b)(a) = (a^{a-b} - c)(a - b) = 0 \Longrightarrow c = a^{a-b}$.

$$R(t - a^{a-b})(t - b) = R(t - b) \cap R(t - a).$$

Notons que

$$(t - b^{b-a})(t - a) = (t - a^{a-b})(t - b).$$

En égalant les coefficients :

$$b^{b-a}a - \delta(a) = a^{a-b}b - \delta(b) \quad \text{and} \quad a^{a-b} + \sigma(b) = b^{b-a} + \sigma(a).$$

PPCM $\Longrightarrow (\sigma, \delta)$ fonctions symétriques généralisées.

(σ, δ) symmetric functions (Delenclos, L.).

En utilisant les quasi-déterminants les fonctions symétriques généralisées furent introduites par Gelfand, Krob, Lascoux,Retakh, Wislon,... (dans le cas non commutatif mais avec où $(\sigma = id, \delta = 0)$). le point de vue ci-dessus évite les quasi-déterminants...)

2. Plus généralement si $a_1, \ldots, a_n \in K$ sont tels que le PPCM de $t - a_1, \ldots, t - a_n$ est de degré n, ce PPCM peut-être calculé

3. quand $deg[t - a_1, \ldots, t - a_n] = n$?

   Réponse : quand la matrice de vandermonde généralisée suivante est inversible :

   Pour $a_1, \ldots, a_n \in K$:

$$V^{\sigma,\delta}(a_1, \ldots, a_n) := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ a_1 & a_2 & \ldots & \ldots & a_n \\ N_2(a_1) & N_2(a_2) & \ldots & \ldots & N_2(a_n) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ N_{n-1}(a_1) & N_{n-1}(a_2) & \ldots & \ldots & N_{n-1}(a_n) \end{pmatrix}$$

   Rappel $N_i(a) = t^i(a)$

   Il existe aussi des matrices Wronskiennes généralisées et...elles sont étroitement liées aux matrices de Vandermonde généralisées) (Lam, L.)

Theorem 3.4. *(Lam, L.)*

a) $C^{\sigma,\delta}(a) := \{a^x \mid 0 \neq x \in K\}$ *est un sous corps de* K*.*

b) Pour $f \in R$*, l'ensemble* $E(f, a) := \{x \in K \setminus \{0\} \mid f(a^x) = 0\} \cup \{0\}$ *est un espace vectoriel à droite sur* $C^{\sigma,\delta}(a)$*. De plus*

$$Dim_{C^{\sigma,\delta}(a)} E(f, a) \leq \deg f(t).$$

Mentionnons $E(f, 0) = \ker f(\delta)$.

Les applications pseudo-linéaires éclaireront et permettront de généraliser ces résultats.

4 Transformations Pseudo-linéaires

A) Définition et lien avec les applications polynomiales.

Définition 4.1. A un anneau, $\sigma \in End(A)$, δ une σ-dérivation de A, V un A-module à gauche.

$T \in End(V,+)$ tel que, pour $\alpha \in A$ et $v \in V$,

$$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v.$$

est appelé une transformation (σ,δ) pseudo-linéaire (ou une (σ,δ)-PLT).

Les PLT (pseudo linear transformations ; TPL en français "très peu linéaire" !) introduites par Jacobson en 1937 (V un espace vectoriel finidimensionnel sur un corps et σ un automorphisme).

$R = A[t;\sigma,\delta]$ et ${}_RV$ un R-module à gauche alors la multiplication à gauche par t agit sur V comme une (σ,δ)-PLT. Réciproquement si $T : V \longrightarrow V$ est une (σ,δ)-PLT sur... Donc :

$$(\sigma,\delta) - PLT < - - - - - - - - - - > R - \text{modules à gauche.}$$

Proposition 4.2. *L'application* $\Lambda : R = A[t;\sigma,\delta] \longrightarrow End(V,+)$ *définie par* $\Lambda(f(t)) = \Lambda(\sum a_i t^i) = f(T) = \sum a_i T^i$ *est un homomorphisme d'anneaux. En particulier, si* $f,g \in R$, *on a* $fg(T) = f(T)g(T)$.

Exemple : $a \in A$, $T_a \in End(A,+)$ définie par $T_a(x) = \sigma(x)a + \delta(x)$ est une (σ,δ)PLT. Notons que $T_0 = \delta$ et $T_1 = \sigma + \delta$.

Lien avec les applications polynomiales : $f(t) \in R = A[t;\sigma,\delta]$, $a \in A$ then :

$$f(a) = f(T_a)(1)$$

B) Exemples

(1) Soit ${}_AV$ libre et $\beta = \{e_1, \ldots, e_n\}$ une base.

$T : V \longrightarrow V$ une (σ, δ)-PLT.

$C = (c_{ij}) \in M_n(A)$ définie par $T(e_i) = \sum_i^n c_{ij} e_j$.

On étend σ et δ à l'anneau A^n (composantes par composantes).

On obtient une (σ, δ)-PLT sur ${}_AA^n$: pour $\underline{v} \in A^n$.

$$T_C(\underline{v}) = \sigma(\underline{v})C + \delta(\underline{v})$$

, Attention : C inversible **n'implique pas** T est inversible.

(2) β une base de ${}_AV$; $f(t) \in R = A[t; \sigma, \delta]$, on définit $T_\beta = M_\beta(T)$ et $f(T)_\beta = M_\beta(f(T))$ comme en (1).

$$f(T)_\beta = f(T_\beta)$$

Où σ, δ étendu à $M_n(A)$ et $f(T_\beta)$ est le reste de $f(t) \in M_n(A)[t; \sigma, \delta]$ divisé par $t - T_\beta$.

(3) ${}_AV_B$ un (A, B)-bimodule,

S une σ application semi-linéaire sur ${}_AV$,

T une (σ, δ) PLT sur ${}_AV$,

$b \in B$, l'application T_b définie par $T_b(v) = S(v)b + T(v)$, pour $v \in V$, est une (σ, δ) application pseudo-linéaire sur V.

C) Quelques propriétés

Proposition 4.3. *${}_RV$ un R-module tel que ${}_AV$ est un A-module libre de base β,*
T une (σ,δ)-PLT sur V déterminée par ${}_RV$,
Si $\varphi \in End_A(V,+)$ est un morphisme de A-modules.
$C, B \in M_n(A)$ représentent T et φ dans la base β.
Alors les affirmations suivantes sont équivalentes :

(i) $\varphi \in End_R(V)$;

(ii) $\varphi T = T\varphi$;

(iii) $CB = \sigma(B)C + \delta(B)$.

Corollaire 4.4. *$p(t), q(t) \in R$ unitaire de degré n,*
(a)*C_p, C_q les matrices compagnes.*

$$R/Rp \cong R/Rq \quad \text{iff} \quad \exists B \in U(M_n(A)) : C_pB = \sigma(B)C_q + \delta(B).$$

(b) $End_R(R/Rp) \cong C_p^{\sigma,\delta} := \{B \in M_n(A) \,|\, CB = \sigma(B)C + \delta(B\}$.
A^n possède une $(R, C_p^{\sigma,\delta})$-structure de bimodule.

(c) $T :_A V \longrightarrow_A V$ *une (σ,δ)-PLT*
${}_RV_S$ *où* $S = End_R(V)$.
T correspond à la multiplication à gauche par t, $\Longrightarrow T \in End_S(V_S)$.
$f(t) \in R \Longrightarrow f(T) \in End_S(V_S)$.

(d) *En particulier, $V = R/Rp$ donne T_p sur A^n*
$Kerf(T_p)$ *est un $C_p^{\sigma,\delta}$-module à droite.*
$K = A$ *un corps (algèbre à division) $p = t - a$*
$Ker(f(T_a)) = \{0 \neq x \in K \mid f(a^x) = 0\} \cup \{0\}$ *est un $C_{(t-a)}^{\sigma,\delta}$ espace vectoriel à droite. (noté plus haut $E(f,a)$)*

Formule du produit généralisée

$f(t), g(t) \in R = A[t; \sigma, \delta]$, $a, x \in A$:

Etape 1 $(f(t)x)(a) = (fx)(T_a)(1) = f(T_a)(xT_a^0)(1) = f(T_a)(x)$.

Etape 2 $(fg)(a) = (fg)(T_a)(1) = f(T_a)g(T_a)(1) = f(T_a)(g(a))$.

Etape 3 Si $p(t) \in R$ est un polynôme unitaire de degré n ;

$f(p)$ est le reste de $f(t)$ divisé par p.

$\overline{f(p)}$ = coefficients de $f(p)$ ($\overline{f(p)} \in A^n$).

T_p PLT sur A^n induite par $C(p)$, matrice compagne de p.

Formule du produit forme générale : $\overline{fg(p)} = f(T_p)(\overline{g(p)})$.

Utilité : A n'est pas nécessairement un corps.

Fonctions polynomiales à plusieurs variables non comuutatives.

Exerçons nous : la formule du produit :

Si $x \in U(A)$, $a^x = \sigma(x)ax^{-1} + \delta(x)x^{-1}$.

$(t - a^x)x = tx - a^x x = \sigma(x)t + \delta(x) - (\sigma(x)a + \delta(x)) = \sigma(x)(t - a)$.

$f(t)x - f(a^x)x = (f(t) - f(a^x))x \in R(t - a)$.

Donc $f(a^x)x = (f(t)x)(a) = f(T_a)(x)$

$g(a) \in U(A) \Longrightarrow fg(a) = f(T_a)(g(a)) = f(a^{g(a)})g(a)$

On retrouve notre "vieille" formule du produit.

5 Applications

(A) Applications aux corps finis.

Gordon Motzkin $f(t) \in K[t]$ ont des racines dans au plus $degf(t)$ classe de conjugaison.

En présence de (σ, δ) on a $\Delta^{\sigma,\delta}(a) := \{a^x \mid 0 \neq x \in K\}$.

Theorem 5.1. *(Lam, Ozturk, L.) Soit $f(t) \in R = K[t; \sigma, \delta]$ un polynôme de degré n. Alors :*

1) $f(t)$ a des racines dans au plus n (σ, δ) classes de conjugaison, disons $\{\Delta(a_1), \ldots, \Delta(a_r)\}$, $r \leq n$;

2) $\sum_{i=1}^{r} dim_{C(a_i)} \ker(f(T_{a_i})) \leq n$; $C(a_i) := C^{\sigma,\delta}(a_i)$ for $1 \leq i \leq r$.

Egalité (2) $\Leftrightarrow$ $f(t)$ est un polynôme de Wedderburn.
Ceci généralise et précise le résultat de Gordon-Motzkin.

Theorem 5.2. *(L)*

Soient p un nombre premier, $\mathbb{F}_q$ le corps fini à $q = p^n$ éléments, θ l'automorphisme de Frobenius. Alors :

a) Il y a p θ-classes de conjugaison distinctes dans $\mathbb{F}_q$.

b) Pour $0 \neq a \in \mathbb{F}_q$ on a $C^\theta(a) = \mathbb{F}_p$ et $C^\theta(0) = \mathbb{F}_q$.

c) Dans $R = \mathbb{F}_q[t; \theta]$, le PPCM de tous les polynômes de la forme $t - a$ pour $a \in \mathbb{F}_q$ est le polynôme

$$G(t) := t^{(p-1)n+1} - t$$

.

d) Le polynôme $G(t)$ est invariant, i.e. $RG(t) = G(t)R$.

But : Factorisation in $\mathbb{F}_q[t;\theta]$ versus factorisation in $\mathbb{F}_q[x]$

Définitions 5.3. p un nombre premier,
(a)$i \geq 1$, on pose $[i] := \frac{p^i-1}{p-1} = p^{i-1} + p^{i-2} + \cdots + 1$ and put $[0] = 0$.
(b) $q = p^n$. On définit $\mathbb{F}_q[x^{[]}] \subset \mathbb{F}_q[x]$ par :

$$\mathbb{F}_q[x^{[]}] := \{\sum_{i\geq 0} \alpha_i x^{[i]} \in \mathbb{F}_q[x]\}$$

Les éléments de $\mathbb{F}_q[x^{[]}]$ sont appelés $[p]$-polynômes.

On étend θ à $F_q[x]$ via $\theta(x) = x^p$ i.e. $\theta(g) = g^p$ pour tout $g \in F_q[x]$.

Considérons $R := F_q[t;\theta] \subset S := F_q[x][t;\theta]$.

Pour $f \in R := \mathbb{F}_q[t;\theta] \subset \mathbb{F}_q[x][t;\theta]$
on peut évaluer f en x.
on note $f(t)(x) = f^{[]}(x) \in \mathbb{F}_q[x]$.

Theorem 5.4. *Soit $f(t) = \sum_{i=0}^n a_i t^i$ un polynôme de $R := \mathbb{F}_q[t;\theta] \subset S := \mathbb{F}_q[x][t;\theta]$. Avec les notations ci-dessus on a :*

1) Pour tout $b \in \mathbb{F}_q$, $f(b) = \sum_{i=0}^n a_i b^{[i]}$.

2) $f^{[]}(x) = \sum_{i=0}^n a_i x^{[i]} \in \mathbb{F}_q[x^{[]}]$.

3) $\{f^{[]} | f \in R = \mathbb{F}_q[t;\theta]\} = \mathbb{F}_q[x^{[]}]$.

4) Pour $i \geq 0$ et $h(x) \in \mathbb{F}_q[x]$ on a $T_x^i(h) = h^{p^i} x^{[i]}$.

5) Si $g(t) \in S = F_q[x][t;\theta]$ et $h(x) \in \mathbb{F}_q[x]$ $g(T_x)(h(x)) \in \mathbb{F}_q[x]h(x)$.

6) Pour tout $h(t) \in R = \mathbb{F}_q[t;\theta]$, $f(t) \in Rh(t)$ si et seulement si $f^{[]}(x) \in \mathbb{F}_q[x]h^{[]}(x)$.

Corollaire 5.5. *Un polynôme $f(t) \in \mathbb{F}_q[t;\theta]$ est irréductible si et seulement si le p-polynôme $f^{[]}$ qui lui correspond ne possède pas de facteurs non trivial dans $\mathbb{F}_q[x^{[]}]$.*

Exemple Considérons $f(t) = t^4 + (a+1)t^3 + a^2t^2 + (1+a)t + 1 \in \mathbb{F}_4[t;\theta]$. Son $[p]$-polynôme est $x^{15}+(a+1)x^7+(a+1)x^3+(1+a)x+1 \in \mathbb{F}_4[x]$. On peut le factoriser :

$$(x^{12}+ax^{10}+x^9+(a+1)x^8+(a+1)x^5+(a+1)x^4+x^3+ax^2+x+1)(x^3+ax+1)$$

Ce dernier facteur est un $[p]$-polynôme qui correspond à $t^2+at+1 \in \mathbb{F}_4[t;\theta]$. De plus puisque x^3+ax+1 est en fait irréductible dans $\mathbb{F}_4[x]$, on a t^2+at+1 est aussi irréductible dans $\mathbb{F}_4[t;\theta]$. On en conclut que $f(t) = (t^2+t+1)(t^2+at+1)$ est une décomposition de $f(t)$ en facteurs irréductibles dans $\mathbb{F}_4[t;\theta]$.

(B) Polynômes unitaires et PPCM

Proposition 5.6. *Soient A, σ, δ un anneau, un endomorphisme de A et une σ-dérivation de A. Les affirmations suivantes sont équivalentes :*

(i) For $a, b \in A$, il existe $c, d \in A$ tel que $(t-c)(t-a) = (t-d)(t-b)$ in $R = A[t;\sigma,\delta]$.

(ii) Pour $a, b \in A$, il existe $c \in A$ tels que $T_b(a) = ca = L_c(a)$

(iii) Pour tout $a, b \in A$, il existe $c \in A$ tels que $\sigma(a)b + \delta(a) = ca$.

En particulier, quand $\sigma = id.$ et $\delta = 0$, les conditions ci dessus sont aussi équivalentes au fait que l'anneau A duo à gauche.

Définition 5.7. Un anneau A est (σ,δ)-duo à gauche si pour tout $a, b \in A$, il existe $c \in A$ tels que $T_b(a) = ca$.

Theorem 5.8. *Soit $a_1, \ldots, a_n$ des éléments d'un anneau (σ,δ)-duo à gauche A. Alors pour tout polynôme unitaire $g(t) \in R = A[t;\sigma,\delta]$ il existe un ppcm unitaire de $g(t)$ et de $(t-a_n)\cdots(t-a_1)$ qui est de degré $\leq n + \deg(g)$.*

(C) Applications aux codes

Pour $f \in A[t;\sigma,\delta]$ unitaire de degré n, on note $T_f : A^n \longrightarrow A^n$ la PLT définie par $T_f(v) = \sigma(v)C_f + \delta(v)$ où σ et δ ont été étendu

composantes par composantes à A^n et C_f dénote la matrice compagnon associée à f. L'application $\varphi : R/Rf \longrightarrow A^n$ donnée par $\varphi(p + Rf) = p(T_f)(1, 0, \ldots, 0)$ est une bijection.

Définitions 5.9. Soit $f \in R = A[t; \sigma, \delta]$ un polynôme unitaire invariant ($fR = Rf$) de degré n. Un (σ, δ)-code $C(t)$ est un idéal principal à gauche I de R/Rf. L'ensemble $C \subset A^n$ des mots codes qui correspondent à $C(t)$ est l'image de $C(t)$ par l'application φ définie plus haut.

En d'autres termes $I = Rg/Rf$, il existe $h, h' \in R$ tels que $f = gh = h'g$. Le code $C \subseteq A^n$ associé à cet idéal est le sous ensemble de A^n constitués des coordonnées des éléments de Rg/Rf dans la base $\{1, t, \ldots, t^{n-1}\}$.

Theorem 5.10. *(a) Si $v := (a_0, a_1, \ldots, a_{n-1}) \in C$ alors $T_f(v) \in C$.*

(b) Les lignes définies par $(T_f)^k(g_0, g_1, \ldots, g_r)$ for $1 \leq k \leq n - r$ forment une partie génératrice du code C.

On peut retrouver les codes tordus considérés par F.Ulmer, Boucher, P. Solé,...

Matrice de contrôle ?
En écrivant $f = gh$ on a $C(t) = lann_{R/Rf}h$.

Lemme 5.11. *En utilisant les notations précédentes on a :*

(i) $(c_0, \ldots, c_{n-1}) \in C$,
(ii) $(\sum_{i=0}^{n-1} c_i t^i)h(t) \in Rf$,
(iii) $\sum_{i=0}^{n-1} c_i T_f^i(\underline{h}) = \underline{0}$,
(iv) $\sum_{j=0}^{n-1}(\sum_{i=j}^{n-1} c_i f_j^i(\underline{h}))N_j(C_f) = \underline{0}$.

Soit $g(t) \in A[t; \sigma, \delta]$ un polynôme unitaire de degré r qui est le PPCM de polynômes $t - a_1,\ dots, t - a_r$ alors la matrice de Vandermonde généralisée $r \times r\ V(a_1, \ldots, a_r)$ est inversible.

Un (σ, δ, g)-code polynomial C est l'ensemble des n-uples, $n > r$, de A^n correspondant aux coefficients des polynômes de Rg de degré $\leq n-1$. Alors :

(a) Une matrice génératrice d'un (σ, δ, g)-code polynomial C est donnée par les coefficients de $g(t), tg(t), \ldots, t^{n-r-1}g(t)$.

(b) $(c_0, c_1, \ldots, c_{n-1} \in C$ si et seulement si $(c_0, c_1, \ldots, c_{n-1})V_{n\times r}(a_1, \ldots, a_r) = (0, \ldots, 0)$, où $V_{n\times r}(a_1, \ldots, a_r)$ est la matrice de vandermonde généralisée basée sur $a_1, \ldots, a_r$