A propos d'algèbres à division

Jean Creignou

25 janvier 2008

Convention : On appellera algèbre à division (anneau à division, ou encore corps gauche), un anneau unitaire ou tout élément non-nul est inversible (en particulier la loi de multiplication est associative). On notera $\mathfrak{i}$ une racine carrée de -1 (ceci pour ne pas confondre avec des indices ou des idéaux).

Quelques éléments du contexte[1]

Une modélisation des télécommunications multi-antennes amène à considérer le problème suivant. On cherche à construire un ensemble $\mathcal{C}$ de matrices $n \times n$ vérifiant les propriétés suivantes :

- $\mathcal{C}$ possède une structure linéaire, plus particulièrement $\mathcal{C}$ est un espace vectoriel de dimension n^2 sur $\mathbb{Q}[\mathfrak{i}]$.
- Il existe un sous ensemble $\mathbb{Z}[\mathfrak{i}]$ linéaire $\mathcal{C}_0 \subset \mathcal{C}$ qui possède la propriété de « Non Vanishing Determinant ». C'est à dire $\exists \delta > 0$ tel que $\forall A \neq B \in \mathcal{C}_0$, $|\det(A-B)| \geq \delta$. Ce delta est lié à la performance du code (l'évolution de la probabilité d'erreur en fonction de la puissance du signal est de l'ordre de $(\delta SNR^n)^{-1}$.

Pour des raisons de performance et de décodage les deux contraintes suivantes sont imposées.

- Les éléments de $\mathcal{C}$ possèdent une structure linéaire en couches c'est à dire qu'il existe une base $(e_1, ..., e_{n^2})$ où les e_i ont un seul coefficient non-nul par ligne et colonne (contrainte énergétique 1).
- Si on considère un sous ensemble fini de $\mathcal{C}$ (un code effectif) construit à partir d'un $A^{n^2} \subset Q[\mathfrak{i}]^{n^2}$ où A est une QAM (éléments à coordonnées entières dans un carré centré en 0). Alors « l'énergie est bien repartie sur chaque couche » (contrainte énergétique 2).

Cette dernière contrainte structurelle (shaping) sera précisée en annexes (par l'exemple).

[1] Cet exposé est destiné à des personnes n'ayant aucune connaissance sur les MIMO et les télécommunications

1 Anneaux de polynôme tordus

1.1 Définition

Définition 1 : Soit D un anneau, σ un automorphisme de D, on définit $D[t,\sigma] = \{a_0 + ... + a_i t^i + ... + a_n t^n\}$ où $ta = \sigma(a)t$: anneau de polynôme tordu.

Exemple : On pose $K = \mathbb{Q}[\mathrm{i}]$, on part du corps $K[\sqrt{5}]$ et $\sigma : \sqrt{5} \mapsto -\sqrt{5}$. On a donc un anneau non commutatif $K[t,\sigma]$. Dans cet anneau tordu on a par exemple : $t(1+\sqrt{5}) = (1-\sqrt{5})t$...

Proposition 2 : Si D est une algèbre à division alors :

- Pour un élément $f(t)$ de $D[t,\sigma]$ le degré est bien défini,
- Il existe un algorithme de division à gauche (et à droite).

Preuve : Soit $f(t),\ g(t) \in D[t,\sigma]$, $f(t) = a_0 + ... + a_n t^n$ et $g(t) = b_0 + ... + b_m t^m$, alors :

$$f(t) - a_n \left(\sigma^{(n-m)} b_m\right)^{-1} t^{(n-m)} g(t) = \text{ polynôme de degré } \leq n-1.$$

On peut donc écrire $f(t) - q(t)g(t) = r(t)$.

Corollaire 3 : $D[t,\sigma]$ est donc *principal à droite* et *principal à gauche* : c'est à dire tout idéal à droite (resp. tout idéal à gauche) est principal. Par conséquent $D[t,\sigma]$ est donc noethérien à droite et à gauche.

Un anneau principal à droite et à gauche sera appelé un PID (notation anglaise).

1.2 Idéaux et éléments bilatères dans les PID

Remarque(s) 4 : Soit R un PID, si on considère un idéal bilatère $J = Rd = \hat{d}R$. Alors :

- $d \in J$ donc $\exists u, v / d = \hat{d}u$,
- $d^* \in J$ donc $\exists u, v / \hat{d} = vd$,
- De plus $\forall a \in R$, $\exists a' / da = a'\hat{d}$ et $\exists \tilde{a} / a\hat{d} = d\tilde{a}$.

Donc on peut écrire $d = udv = uv'd$. On en déduit que u et v (v') sont des unités et $\hat{d}R = duR = dR$ en particulier $J = dR = Rd$.

Définition 5 : Un tel d est appelé élément bilatère (attention être bilatère ne signifie pas être dans le centre !). Dans la suite de tels éléments sont notés avec *.

Exemple : ... $5,\ t,\ (t^2-5)$ sont bilatères, mais pas $t+\sqrt{5}$ car $(t+\sqrt{5})t$ ne peut s'écrire $*(t+\sqrt{5})$. Entre autre t est bilatère mais n'est pas dans le centre de $R = K[t,\sigma]$...

Remarque(s) 6 : Si d est bilatère alors d^{-1} aussi. De même si 2 éléments sont bilatères dans l'expression $d_1 = d_2 d_3$, le troisième l'est aussi.

On sait caractériser les éléments bilatères (cf Thm 2.1). Cette description est un peu fastidieuse et est repoussée à une partie ultérieure.

1.3 Un peu d'arithmétique sur les PID

La plupart des résultats de cette partie sont admis ils se prouvent avec des des suites de compositions.

Définition 7 :

- $Ra \supset Rb \Leftrightarrow \exists c \ / \ b = ca$ noté $a|_r b$.
- ($a|_r b$ et $b|_r a$) $\Leftrightarrow \exists u$ unité $/ \ a = ub$ (a et b sont dit associés à gauche).

Remarque(s) 8 : On a :
$Ra + Rb = Rd \Rightarrow d|_r a, \ d|_r b$ et c'est le plus grand : $d = \gcd(a,b)_r$.
$Ra \cap Rb = Rc \Rightarrow a|_r c, \ b|_r c$ et c'est le plus petit : $c = \mathrm{lcm}[a,b]_l \quad (c = *a)$.

Définition 9 : a et b sont dit *similaires* ssi $R/Ra \cong R/Rb$ comme R-modules. ssi $R/aR \cong R/bR$ comme R-modules.

Théorème 10 : [admis] Soit R un PID alors tout $a \neq 0, \neq$ unité peu s'écrire $a = p_1 ... p_s$ où les p_i sont des irréductibles. Cette décomposition est unique à permutation et similarité près.

Notations : On note a^* un élément (idéal) bilatère et p^* un élément (idéal) bilatère maximal (i.e. maximal parmi les bilatères).

Théorème 11 : [admis] Soit R un PID alors tout $a^* \neq 0, \neq$ unité peu s'écrire $a^* = p_1^* ... p_s^*$ où les p_i^* sont des idéaux bilatères maximaux. Cette factorisation est unique à permutation et similarité près (de plus les idéaux bilatères maximaux commutent entre eux).

Théorème 12 : [important,admis] Soit R un PID alors tout idéal bilatère maximal p^* se décompose en $p^* = p_1 ... p_s$ où les p_i sont tous similaires.

Exemple : En prenant les théorèmes dans l'ordre inverse :

- $t^2 + 5$ est bilatère maximal et se factorise en $t^2 + 5 = (t - \sqrt{5})(t - \sqrt{5}) = (t + \sqrt{5})(t + \sqrt{5})$.
- $t^4 - 25$ se décompose en $(t^2 - 5)(t^2 + 5)$ (décomposition en idéaux maximaux bilatères),
- $t^3 + 5t = t(t+\sqrt{5})(t+\sqrt{5}) = (t-\sqrt{5})t(t+\sqrt{5})$ est une décomposition en irréductibles d'un élément quelconque.

2 Première application

Tout d'abord on a besoin de caractériser les éléments bilatères de $D[t, \sigma]$.

2.1 Caractérisation des éléments bilatères

Théorème 13 :

1. Les éléments bilatères de $R = D[t, \sigma]$ sont les

$$ac(t)t^n, \ a \in D, \ c(t) \in \mathrm{Cent}R$$

2. Si σ est d'ordre fini modulo les automorphismes intérieurs de D ($\sigma^r = I_u : x \mapsto uxu^{-1}$), alors
$$\mathrm{Cent}R = \gamma_0 + \gamma_1 u^{-1}t^r + ... + \gamma_s u^{-s}t^{rs}$$
où $\gamma_i u^{-i} \in \mathrm{Inv}(\langle\sigma\rangle)$ et $\gamma_i \in \mathrm{Cent}D$.
Si de plus r est l'ordre de $\sigma_{|\mathrm{Cent}D}$ on peut choisir $u \in \mathrm{Inv}(\langle\sigma\rangle)$ et $\mathrm{Cent}R = F[u^{-1}t]$ où $F = \mathrm{Cent}D \cap \mathrm{Inv}(\langle\sigma\rangle)$.

3. Sinon $\mathrm{Cent}R = F = \mathrm{Cent}D \cap \mathrm{Inv}(\langle\sigma\rangle)$.

Preuve :

1. Pour le sens non trivial, a et t^n étant bilatères on peut supposer qu'un élément bilatère s'écrit $ac(t)t^n$ où $c(t) = 1+a_1t^1+...+a_st^s$. Si $c(t)$ est bilatère en particulier il commute avec t et $a \in D$: ce qui donne la propriété.

2. On vérifie que de tels éléments sont bien dans $\mathrm{Cent}R$. Réciproquement si $c(t)$ est dans $\mathrm{Cent}R$ on décompose par degré puis on écrit $(a_it^i)a(a_it^i)^{-1} = a$ soit $t^iat^{-i} = a_i^{-1}aa_i$. D'où i est multiple de r. Le reste suit naturellement.

3. Admis (idem ci dessus).

2.2 Première construction d'algèbres à division

Une manière naturelle de construire une algèbre à division est de faire un quotient R/Rf. La dimension sur R est donnée par le degré de f (en particulier deux polynômes f et g similaires ont le même degré). Pour avoir une algèbre à division il faudrait que f engendre un idéal premier. Le but de cette partie de caractériser certains bons polynômes f.

Lemme 14 : Le reste de la division de $f(t) = a_0t^n + ... + a_n$ par $(t-b)$ est
$$\sum a_iN_{n-i}(b)$$
où $N_i(b) = (\sigma^{i-1}b)...(\sigma b)b$ et $N_0(b) = 1$.

Preuve :
$$\left(t^i - N_i(b)\right) = \left(t^{i-1} + (\sigma^{i-1}b)t^{i-2} + ... + (\sigma^{i-1}b)...(\sigma b)\right)(t-b)$$

Corollaire 15 :
$$(t-b)|_r f(t) \Leftrightarrow \sum a_iN_{n-i}(b) = 0$$

Théorème 16 : [important] Soit σ, u, r, D comme précédemment et supposons r premier alors $R/R(t^r - u\gamma)$ est une algèbre à division $\Leftrightarrow \nexists b$ / $N_r(b) = u\gamma$. On note (D, σ, t, γ) une telle construction.

Exemple : On pose $K = \mathbb{Q}[\mathrm{i}]$ (cf contexte) et $L = K[\sqrt{5}]$ une extension Galoisienne de degré 2. On a $\sigma : \sqrt{5} \mapsto -\sqrt{5}$ automorphisme d'ordre 2. On construit $D_1 = (L, \sigma, \mathrm{i})$. Il faut savoir si $\mathrm{i} = \sigma(a)a$ possède une solution. Pour cela il suffit de réduire modulo $(2+\mathrm{i})$ (~ 5) pour voir que cette équation n'a aucune solution dans L. On a donc une belle algèbre à division. Plus généralement on dispose du symbole de Hasse Minkowski $\left(\frac{a,b}{\nu}\right)$

qui dit si a est une norme pour $K(b^{\frac{1}{n}})$ relativement à la place ν.

Remarque(s) 17 : Les algèbres à division ci dessus sont appelées algèbre à division cycliques. Ces algèbres possèdent des représentations matricielles assez simple :

$$a \rightsquigarrow \begin{pmatrix} a & & & \\ & \sigma a & & \\ & & \ddots & \\ & & & \sigma^{n-1}a \end{pmatrix} \text{ et } t \rightsquigarrow \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \gamma & & & \end{pmatrix}$$

3 Avancées, contraintes et limitations

On a une algèbre à division centrale simple[2] sur K. Elle possède une base relativement naturelle : donnée par celle de L sur K et les puissances de t.

Remarque(s) 18 : On remarque que si on prend une base formée d'entiers (de L sur K) et que l'on impose aux coefficients d'être des entiers de $Q[\mathfrak{i}]$ (cf la QAM) alors on peut facilement montrer que notre déterminant non-nul est un entier. On peut montrer qu'un élément de notre algèbre à division centrale simple sur $Q[\mathfrak{i}]$ à un déterminant (et une trace) dans $\mathbb{Q}[\mathfrak{i}]$ (cf annexes). Conclusion les modules des déterminants minimaux (sauf celui de la matrice nulle) sont minorés par 1 !

Malheureusement le contexte impose des contraintes assez restrictives : Pour les raisons énergétiques citées en introduction on doit avoir γ de module 1. On est alors limité par la proposition suivante.

Proposition 19 : Toute algèbre à division cyclique D, construite à partir une extension Galoisienne cyclique L sur $K = \mathbb{Q}[\mathfrak{i}]$ (ou $\mathbb{Q}[\mathfrak{j}]$) de paramètre γ entier de module 1, vérifie $n \in [2, 3, 4, 6]$.

Or les applications aimeraient des petites puissances de 2 : 8, 16, 32, 64 (64 antennes c'est déjà pas mal).

De plus on impose d'autres contraintes liées au décodage (structure de réseau cachée) expliquées en annexe.

4 Généralisations possibles

4.1 Construction récursive

Exemple : Soit $L = K[\sqrt{a}, \sqrt{b}]$, on prend $\sigma_a : \sqrt{a} \mapsto -\sqrt{a}$, et un élément γ_a qui n'est pas une norme et on construit $D_1 = (L, \sigma_a, t_a, \gamma_a)$. Ensuite on définit $\tilde{\sigma_b}$ sur D_1 (en définissant l'image de t_a. Et l'on construit $D_2 = (D_1, \tilde{\sigma_b}, t_b, \gamma_b)$. A priori l'élément γ_b doit être dans $K = \mathrm{Cent}D_1 \cap \mathrm{Inv}\tilde{\sigma_b}$.

L'exemple ci-dessus donne l'idée générale de la construction par récurrence. Malheureusement le problème de savoir si l'élément γ_b est une norme est extrêmement compliqué,

[2]Les seuls idéaux bilatères sont triviaux.

car on n'a pas d'équivalent du symbole de Hasse Minkowsky dans le cas des algèbres à division.

Personnellement lors d'essais de construction pour $n = 4$ à partir d'une extension Galoisienne de groupe $G = (\mathbb{Z}/2\mathbb{Z})^2$, je n'ai jamais réussi à prouver de manière directe qu'un élément γ_b n'était pas une norme et pour cause de tels éléments n'existent pas si on prend γ_b dans K. La preuve est un cas particulier des résultats de la section suivante.

4.2 « General Abelian Crossed Product »

Soit E/F une extension Galoisienne de groupe G abelien $G = \langle\sigma_1\rangle \times ... \times \langle\sigma_r\rangle$ où σ_i est d'ordre n_i. On pose $F_{i_1,...,i_k} = \mathrm{Inv}(\langle\sigma_{i_1}, ..., \sigma_{i_k}\rangle)$ et $N_{i_1,...,i_k} = N_{E/F_{i_1,...,i_k}}$.

On définit $A = (E, \sigma, U, \gamma)$ où U est une matrice et γ un vecteur, par $A = \{\text{polynômes en } z_1, ..., z_r\}$ où les z_i vérifient :

- $z_i a = (\sigma_i a) z_i$,
- $z_i^{n_i} = \gamma_i$,
- $z_i z_j = u_{ij} z_j z_i$.

Cette algèbre est déterminée par la donnée du vecteur b et de la matrice U. Ces deux paramètres sont liés par les relations suivantes :

- $u_{ii} = 1$, $u_{ij} = u_{ji}^{-1}$,
- $\sigma_j \gamma_i = N_i u_{ji} \gamma_i$,
- $N_{ij}(u_{ij}) = 1$,
- $u_{jk} u_{ki} u_{ij} = (\sigma_i u_{jk})(\sigma_j u_{ki})(\sigma_k u_{ij})$.

Remarque(s) 20 : Cette construction est en fait un cas généralisant la construction récursive. Cette approche symétrise le problème et donne des critères (notement sur la matrice U) à éviter.

Il est prouvé que toute algèbre à division de degré 4 peut se redécomposer sous cette forme (décomposition effectuée avec succès sur des exemple concrets).

Définition 21 :

- Pour $\overline{m} = (m_1, ..., m_r)$ on pose $z^{\overline{m}} = z_1^{m_1} ... z_r^{m_r}$ et $u_{\overline{m},\overline{n}} = [z^{\overline{m}}, z^{\overline{n}}]$ (le commutateur).
- La matrice U est dite « dégénérante »ssi il existe $\overline{m}$ et $\overline{n}$ tels que $\langle\sigma^{\overline{m}}, \sigma^{\overline{n}}\rangle$ est non cyclique et
$$u_{\overline{m},\overline{n}} = \frac{\sigma^{\overline{m}}(c_1)}{c_1} \frac{\sigma^{\overline{n}}(c_2)}{c_2}$$
avec $c_1, c_2 \in E^*$.

On peut démontrer que si U est dégénérante alors A n'est pas une algèbre à division...
Remarque(s) 22 : Si $\sigma_i(\gamma_j) = \gamma_j$ alors la matrice U est dégénérante. En effet d'après les relations citées ci-dessus on a alors $N_i(u_{ji}) = 1$, d'après $H90$ on a $u_{ji} = \sigma_i(c)/c$. On vérifie alors trivialement les conditions de dégénérance.

Annexes

Notations : Le degré d'une algèbre A centrale simple sur K est donnée par la racine carrée de $[A : K] = n^2$.

Les théorèmes suivant sont importants :
Théorème 23 : Toute algèbre centrale simple sur K peut est isomorphe à un $M_k(D)$ où D est une algèbre à division centrale sur K (la dimension $[D : K] = d^2$ est appelé l'indice A (et de D)).

Théorème 24 : Toute algèbre centrale simple A de dimensions n^2 sur son centre, possède un corps E appelé corps de décomposition tel que $A \otimes E \cong M_n(E)$.

A Déterminant et Trace réduite

Dans cette section on prouve que le déterminant d'une algèbre centrale simple sur F (sous corps) est un élément de F, on en profite pour introduire la définition de norme et trace réduite.

Soit A une algèbre centrale simple sur un corps K de base $(u_1, ..., u_s)$, on introduit $K(\xi$ comme l'anneau de polynôme en s indéterminées $\xi_1, ..., \xi_s$ sur K et $A_{K(\xi)}. = A \otimes K(\xi)$. On appelle $x = \sum \xi u_i$ un élément générique de A, son polynôme minimal s'écrit :

$$m_x(\lambda) = \lambda^m - \tau_1(\xi)t^{m-1} + ... + (-1)^m\tau_m(\xi).$$

Lemme 25 : Les $\tau_i(\xi)$ sont des polynômes homogènes de degré i en les ξ_i dans $K(\xi)$.

Preuve : L'algèbre A possède une représentation régulière et peut être représentée comme une sous algèbre de de $M_N(K)$. Donc $A_{K(\xi)}$ est une sous algèbre de $M_N(K(\xi))$ et x est une matrice dont les coefficients sont des expressions linéaires homogènes en les ξ. Le polynôme caractéristique χ_x est donc de la forme

$$\lambda^N - t_1(\xi)t^{N-1} + ... + (-1)^N t_N,$$

où $t_i(\xi)$ est homogène de degré i. Ce polynôme est divisible par $m_x(\lambda)$. Par le lemme de Gauss $m_x(\lambda)$ $m_x(\lambda)$ est dans $K[\xi, \lambda]$ de plus χ_x étant homogène de degré N en ξ, λ, $m_x(\lambda)$ est homogène de degré m en ξ, λ.

On considère alors $m_a(\lambda)$ donné par le morphisme d'évaluation des ξ_i, $m_x \mapsto m_a$ donné par $\xi_i \mapsto \alpha_i$ avec $a = \sum \alpha_i u_i$.

Définition 26 : On appelle $t(a) = \tau_1(a)$ la trace réduite d'un élément et $n(a) = \tau_m(a)$ la norme réduite.

Remarque(s) 27 :

- Si on considère $A_E = A \otimes E$ on remarque que la base u_i de A sur K est aussi une base de A_E sur E : la norme et la trace réduite est donc invariante par extensions de corps.

- Soit A algèbre centrale simple et E corps de décomposition alors $A_E \cong M_m(E)$ et $m_a(\lambda) = \det(\lambda - a)$.

B Contrainte de réseau (shaping)

Dans cette partie on expose la contrainte de shaping sur l'exemple de l'algèbre cyclique donnée par $L = K(\sqrt{5})$, $\sigma : \sqrt{5} \mapsto -\sqrt{5}$ et $\gamma = \mathfrak{i}$. On a déjà vu que si l'on prend une base de L sur K formée d'entiers (par exemple $(1, \theta)$ où $\theta = \frac{1+\sqrt{5}}{2}$) et des coefficients entiers (dans $\mathbb{Z}[\mathfrak{i}]$) le déterminant est entier.

Ce que l'on aimerait avoir c'est une structure de réseau semblable à un $\mathbb{Z}[\mathfrak{i}]^4$ tourné... Ou (voir la suite) que les coefficients d'une couche soient donnés par multiplication à gauche par une matrice unitaire de coefficients d'une QAM.

Avant une étude de shaping les éléments de notre code décrivent

$$\begin{bmatrix} a + b\theta & c + d\theta \\ \mathfrak{i}\sigma(c + d\theta) & \sigma(a + b\theta) \end{bmatrix}$$

Si on regarde un sous réseau engendré par un idéal principal α la norme de ce sous réseau est alors :

$$\det(\Gamma) = |N_{L/K}(\alpha)|^2 |d_{L/K}| = 5|N_{L/K}(\alpha)|^2$$

On cherche à avoir une puissance égale au degré c'est à dire 2. On cherche donc α tel que $|N_{L/K}(\alpha)|^2 = 5$ par exemple $\alpha = 1 + \mathfrak{i} - \mathfrak{i}\theta$. Les coefficients d'une couche sont donc donnés par

$$M = \begin{pmatrix} \alpha & \alpha\theta \\ \sigma(\alpha) & \sigma(\alpha\theta) \end{pmatrix}$$

On vérifie que $MM^* = 5\mathrm{Id}$ et donc $\frac{1}{\sqrt{5}}M$ est une matrice unitaire. Une reconsidération du déterminant minimum des matrices obtenues sous la forme

$$X = \frac{1}{\sqrt{5}} \begin{bmatrix} \alpha(a + b\theta) & \alpha(c + d\theta) \\ \mathfrak{i}\sigma(\alpha(c + d\theta)) & \sigma(\alpha(a + b\theta)) \end{bmatrix}$$

Nous permet d'affirmer que $\min_{A \neq B} |\det(A - B)| \geq \frac{1}{5}$.
(Faire le lien entre la matrice unitaire $\frac{1}{\sqrt{5}}M$ et les conditions énergétiques)

Cas général

Soit $\omega_1, ..., \omega_n$ une base entière de L sur K on cherche un idéal $\mathcal{I} = \alpha\mathcal{O}_L$ tel que

$$M = \begin{pmatrix} \sigma_1(\alpha\omega_1) & ... & \sigma_n(\alpha\omega_1) \\ \vdots & \vdots & \vdots \\ \sigma_1(\alpha\omega_n) & ... & \sigma_n(\alpha\omega_n) \end{pmatrix}$$

Soit un multiple d'une matrice unitaire.