A propos d'algèbres à division II
Corps de nombres VS Algèbres à division

Jean Creignou

7 février 2008

Cet exposé peut être vu comme un parallèle entre la théorie des extensions de corps et celle des algèbres centrales simples. En effet ces deux objets mathématiques partagent de nombreuses propriétés.

Note : Le contexte présente en début de chaque partie l'ensemble des hypothèses faites dans ces parties, celles-ci ne sont ensuite pas rappellées systématiquement à chaque énoncé.

1 Norme et Trace réduite

Contexte : On se place dans cette partie dans le cadre d'une algèbre A centrale simple de dimension finie sur un corps de nombre K. Simple signifie que les seuls idéaux bilatères sont triviaux, centrale signifie que le centre de A est précisement K. Le cadre des algèbres centrales simples est agréable car il permet d'utiliser le théorème de Wederburn.

Théorème 1 : [Wederburn] Toute algèbre centrale simple sur K peut s'écrire sous la forme $M_k(D)$ où D est une algèbre à division de centre K. De plus les dimensions $[D : K] = d^2$ et $[A : K] = k^2d^2$ sont des carrés (la dimension $[D : K] = d^2$ est appelé l'indice de A (et de D)).

Plus généralement si A est une algèbre artiniene semi-simple alors $A = B_1 \oplus .... \oplus B_r$ où les B_i sont des algèbres simples dont le théorème précédent permet une décomposition comme matrice sur une algèbre à division. Attention néanmoins aux centres des B_i qui peuvent être plus gros que celui de A.

La théorie des algèbres centrales simple fait souvent appel à la notion de corps de décomposition (dans un sens différent de celui de la théorie de Galois).

Théorème 2 : Toute algèbre à division D centrale sur K possède un corps E (contenant K) appelé corps de décomposition tel que $E \otimes_K D \cong M_n(E)$. Si D est de dimension d^2 sur son centre K alors tout sous corps maximal de D est de dimension d sur K et est un corps de décomposition.

Corollaire 3 : Toute algèbre centrale simple A de dimensions n^2 sur son centre, possède un corps E appelé corps de décomposition tel que $E \otimes_K A \cong M_n(E)$.

Définition 4 : Soit A une algèbre centrale simple sur K et $(u_1, ..., u_N)$ une base de A/K, on introduit $K(\xi)$ comme corps de fonctions rationelles en N indéterminées $\xi_1, ..., \xi_N$ sur K et $A_{K(\xi)}. = A \otimes_K K(\xi)$. On appelle $x = \sum \xi u_i$ un élément générique de A, son polynôme minimal s'écrit :

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

Ce polynôme est appelé le polynôme minimal générique de A.

Lemme 5 : 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 $M_N(K)$ (écrire la base $u_1, ..., u_N$ de A sur 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

$$\chi_x(\lambda) = \lambda^N - t_1(\xi)\lambda^{N-1} + ... + (-1)^N t_N \ \in K[\xi, \lambda],$$

où $t_i(\xi)$ est homogène de degré i. Ce polynôme est divisible par $m_x(\lambda)$. Par le lemme de Gauss, $m_x(\lambda)$ 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.

Définition 6 : Si $a=\sum a_i u_i \in A$ on définit le morphisme $\eta_a : A_{K(\xi)} \to A$, $\xi_i \mapsto a_i$. On considère alors $m_a(\lambda)$ donné par le morphisme d'évaluation $\eta : m_x \mapsto m_a$.
Le polynôme m_a est appelé polynôme caractéristique réduit de a.

Définition 7 : On appelle $tr(a)=\tau_1(a)$ la trace réduite d'un élément et $nr(a)=\tau_m(a)$ la norme réduite.

Remarque(s) 8 :

- Si on considère $A_E = E \otimes A$ 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 $A_E \cong M_m(E)$. Or si x est l'élément générique de $M_n(E)$ son polynôme minimal est $m_x = \det(\lambda - x)$ on en déduit donc que $m_a(\lambda) = \det(\lambda - (1 \otimes a))$ où $1 \otimes a$ est obtenu par plongement de A dans A_E. Si on a une représentation matricielle de bon degré, la norme et la trace réduite de a correspondent donc à la norme et la trace de la matrice associée à a par plongement.
- On a $\mu_a(\lambda)|m_a(\lambda)|\chi_a(\lambda)$ et ces trois polynômes ont les mêmes facteurs irréductibles.

Exemple : On considère par exemple les quaternions (usuels) sur $\mathbb{Q}$ alors $a+bi+cj+dk$ se représente par une matrice 2×2 à coefficients dans $\mathbb{Q}$[i] (un sous corps maximal) :

$$\begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix},$$

alors que dans la base $\{1,i,j,k\}$ la matrice de multiplication à droite s'écrit :

$$\begin{bmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{bmatrix}.$$

Prenons naïvement 1 son polynôme minimal sur $\mathbb{Q}$ est $X-1$ son polynôme réduit est X^2-1 son polynôme caractéristique est X^4-1. Moins trivialement, $i+j$ à pour polynôme minimal X^2+2 si on regarde le polynôme caractéristique réduit donné par le polynôme caractéristique de

$$\begin{bmatrix} i & 1 \\ -1 & -i \end{bmatrix},$$

on trouve le même polynôme que pour le polynôme minimal tandis que dans la base $\{1,i,j,k\}$ la matrice de $i+j$ (multiplication à droite) est

$$\begin{bmatrix} & 1 & 1 & \\ -1 & & & 1 \\ -1 & & & -1 \\ & -1 & 1 & \end{bmatrix},$$

qui donne comme polynôme caractéristique $(X^2+2)^2$.

Des exemples moins triviaux peuvent être obtenu par les « abelian crossed product » (cf notes précédentes).

Proposition 9 : a est inversible $\Leftrightarrow nr(a)\neq 0$, a est nilpotent $\Leftrightarrow m_a(\lambda)=\lambda^m$.

À retenir : On a défini une norme et une trace, qui correspondent au déterminant et à la trace pour une bonne représentation matricielle. De plus ces éléments sont dans le centre.

2 Ordres dans les algèbres à divisions

2.1 Introduction

Contexte : Dans cette partie on considère R un anneau de Dedekind de corps de fraction : K et D une algèbre à division centrale simple de dimension finie sur K.

Dans le cadre des extensions de corps de nombre on dispose de la notion d'entiers (entiers sur $\mathbb{Z}$ ect...). La stabilité de l'ensemble des éléments entiers par somme et produit nécessite la commutation ce qui pose des problèmes lorsque cette propriété n'est plus vérifiée.

Définition 10 : Un élément $a \in D$ est dit entier sur $R \Leftrightarrow$ il est racine d'un polynôme à coefficients dans R.

Remarque(s) 11 : Il y a en général un problème avec les éléments entiers dans les algèbres à division, en effet ceux ci ne forment pas forcément un anneau (problème de stabilité par addition ou multiplication).

À titre d'exemple sur les quaternions

$$x = \begin{bmatrix} \frac{3\mathrm{i}}{5} & \frac{4}{5} \\ -\frac{4}{5} & -\frac{3\mathrm{i}}{5} \end{bmatrix} \text{ et } y = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$$

sont entiers de polynômes minimaux $X^2 + 1$ et $X^2 - 2X + 2$ mais ni la somme ni le produit de ces éléments sont entiers.

Idée vague : Un ordre dans une algèbre centrale simple A est un sous anneau formé d'entiers, anneau assez gros pour remplir l'espace.

Définition 12 : Soit R un anneau de Dedekind, $K = \mathrm{Frac}(R)$ et V un K-e.v, Λ est appelé « full-$R-$lattice »de $V \Leftrightarrow K.\Lambda = V$ et Λ est finiment engendré comme R-module.

Définition 13 : Un R-ordre de A est un sous anneau $\Lambda \subset A$ qui est aussi un « full-R-lattice »de A.

2.2 Propriétés

Proposition 14 : Soit A centrale simple sur $K = \mathrm{Frac}(R)$, (R de Dedekind), et Λ un R-ordre de A alors,

$$\begin{array}{ll} \forall a \in \Lambda, & \text{pol. car.}(a) \in R[X] \\ & \text{pol. car. red.}(a) \in R[X] \\ & \text{pol. min.}(a) \in R[X]. \end{array}$$

Proposition 15 : Il existe des ordres et des ordres maximaux.

Preuve : [principe] On prend M un full-R-lattice et on considère $O_\ell(M) = \{x \in A \ / \ xM \subset M\}$...

3 Algèbres à division : le cas local

Contexte : Dans cette partie on considère R un anneau local (un seul idéal maximal : P) et complet pour la valuation ν donnée par P. Soit K le corps de fraction de R (complet aussi) et D une algèbre à division **contenant** K (pas forcément centrale simple), de dimension finie sur K.

3.1 Extensions de valuations

Rappel : Une valuation ν vérifie les propriétés suivante :

- $\nu(a) = \infty \Leftrightarrow a = 0$,
- $\nu(ab) = \nu(a) + \nu(b)$,

- $\nu(a+b) \geq \min(\nu(a), \nu(b))$,
- l'image de ν est un groupe cyclique.

Lemme 16 : Soit $f(x) \in K[X]$ irréductible, $f = a_0X^n + ... + a_n$ alors $\forall 0 \leq i \leq n, \nu(a_i) \geq \min(\nu(a_0), \nu(a_n))$.

Preuve : Soit $t = \min \nu(a_i)$ soit r le plus grand indice tel que $\nu(a_r) = t$, si $r \neq 0$ et $r \neq n$ alors $a_r^{-1}f(X) = \beta_0X^n + ... + a_rX^{n-r} + ... + \beta_n$ se factorise en $g(X)X^r$ dans $\overline{R}[X]$ où $g(X) = 1 + ...$ Les facteurs $g(X)$ et X^r étant premiers entre eux cette factorisation se remonte par Hensel en une factorisation non triviale dans $R[X]$ (R est complet).

Définition 17 : On associe au polynôme caractéristique de degré $N = [D : K]$ une forme trace et norme $\mathcal{N}_{D/K}$ et $\mathcal{T}_{D/K}$, on pose alors

- $w_1(a) = N^{-1}\nu(\mathcal{N}_{D/K}(a)) = (\deg \chi_a)^{-1}\nu(\chi_a(0))$.
- $w_2 = [K(a) : K]^{-1}\nu(\mu_a(0)) = (\deg \mu_a)^{-1}\nu(\mu_a(0))$.
- Dans le cas d'une algèbre centrale simple sur K , on peut définir : $w_3 = (\deg m_a)^{-1}\nu(m_a(0))$.

Proposition 18 : $w_1 = w_2 = w_3$.

Preuve : D étant un corps (gauche) le polynôme minimal μ_a est irréductible dans $K[X]$ donc si n est le degré du polynôme minimal, alors $\chi_a(x) = \mu_a(x)^{\frac{N}{n}}$ et $\mathcal{N}_{D/K}(a) = (-1)^*\mu_a(0)^{\frac{N}{n}}$, même raisonnement avec le polynôme réduit.

Théorème 19 : $a \in D$ est entier sur $R \Leftrightarrow \mathcal{N}_{D/K(a)} \in R \Leftrightarrow w(a) \geq 0$.

Preuve : (sens non trivial) Si $N_{D/K}(a) \in R$ alors $\mu_a(x)$ étant irréductible et $\nu(a_n) \geq 0$ on a d'après le lemme 3.1 que μ_a est dans $R[X]$.

Théorème 20 : w est une valuation.

Preuve : La seule chose non triviale à montrer est que pour tout b entier, $w(1+b) \geq 0$. Mais comme 1 et b commutent $1 + b$ est entier (la preuve usuelle marche).

Définition 21 : On pose $\Delta := \{a \in D \ / \ w(a) \geq 0\}$.

Théorème 22 : Δ est la clôture intégrale de R dans D et l'unique ordre maximal (pas de pathologie possible).

Théorème 23 : [admis] w est l'unique extension possible de ν à D !

3.2 Ramification (e) et degré d'inertie (f)

Remarque(s) 24 : L'image de w est inclue dans $\frac{1}{N}\mathbb{Z}$ donc il existe $e|N$ tel que $\mathrm{Im}(w) = \frac{1}{e}\mathbb{Z}$.

Définition 25 : On pose $e = e(D/K)$ l'indice de ramification et on pose $\nu_D = ew$. Soit $\pi \in R$, $\nu(\pi) = 1$ et $\nu_D(\pi) = e$ donc il existe une uniformisante π_D au dessus de π telle que $\nu_D(\pi_D) = 1$. On peut aussi définir le groupe des unités $\mathcal{U}(\Delta) := \{a \in \Delta \ / \ \nu_D(a) = 0\}$.

Remarque(s) 26 : Si on a une uniformisante π_D alors tout élément peu s'écrire $\pi_D^r u = u'\pi_D^r$ avec u et u' des unités de D mais u et u' n'ont aucune raison d'être égales.

Théorème 27 : [admis] Soit $\mathfrak{p} = \pi_D\Delta$ un idéal de l'ordre maximal Δ alors tout idéal de Δ est bilatère et est une puissance de $\mathfrak{p}$. De plus $\overline{\Delta} := \Delta/\mathfrak{p}$ est un corps ... sur $\overline{R}$ et $\mathfrak{p} \cap R = P$ unique idéal maximal de R.

Définition 28 : $f = f(D/K) = (\overline{\Delta} : \overline{R})$.

Théorème 29 : [admis] Si $(D : K)$ est fini alors $ef = (D : K)$.

Fait : D est complet par rapport à ν_D.

Théorème 30 : [admis] Si $K = \text{Cent}D$ et $[D : K] = n^2$ alors $ef = n^2$ et $e|n$ e $n|f$ de plus si $\overline{R}$ est fini alors $e = f = n$.

4 Quelques propriétés (étonnantes) pour faire joli (hors exposé)

4.1 Factorisation

Théorème 31 : Si $f(X)$ est irréductible sur K centre d'une algèbre à division D (centrale simble de dimension finie sur K) et $f(X)$ possède un diviseur (à droite) de degré 1 : $(X - a)$ dans $D[X]$ alors $f(X)$ se décompose totalement :

$$f(X) = \prod_i (X - a_i)$$

où les a_i sont conjugués à a dans D.

4.2 Suite exacte courte

Définition 32 : [vague] On considère l'ensemble des algèbres centrales simples sur un corps K donné. On définit une relation d'équivalence : $A \cong B$ ssi $A = M_r(D)$ et $B = M_s(D)$ avec la même algèbre à division. Et on munit l'ensemble quotient d'une loi de groupe donnée par le produit tensoriel (dont le neutre est $[K] = [M_1(K)]$ et l'inverse donné par l'algèbre opposée, les classes étant notées entre crochets). Ce groupe est appellé le groupe de Brauer de K noté $Br(K)$.

Exemple : Le groupe de Brauer de $\mathbb{R}$ est d'ordre 2 donné par $[\mathbb{R}]$ et les quaternions $[\mathbb{H}(\mathbb{R})]$, celui de $\mathbb{Q}$ est horriblement compliqué.

Proposition 33 : Si $[D : K] = d^2$ alors $[D]^{\otimes d} \cong [K]$.

Proposition 34 : On a la suite exacte courte :

$$0 \to Br(K) \to \oplus_{\mathfrak{p}} Br(K_{\mathfrak{p}}) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

La seconde flèche est donnée par la suite des invariants de Hasse, la troisième par la somme de ces invariants (vus comme des fractions).

Annexes

A L'invariant de Hasse en quelques lignes

Contexte : Soit R un anneau local de corps de fraction K, et D une algèbre à division centrale simple de dimension finie sur K.

L'algèbre à division D possède (à isomorphisme près) un unique sous corps maximal W non ramifié sur K. Ce sous corps est obtenu par l'ajout d'une racine primitive $q^n - 1$-ième de l'unité : ω. On peut alors démontrer que $\pi_D \omega \pi_D^{-1} = \omega^{q^r}$. L'exposant r est un invariant de l'algèbre à division D. Si $[D : K] = n^2$ l'invariant de Hasse est alors la fraction $\frac{r}{n}$ celui-ci caractérise l'algèbre à division à isomorphisme de K algèbre près.