Corps C_1

Cyrille Hériveaux et Gilles Tauzin
Encadré par David Harari

19 mai 2006

Résumé

Le but du présent exposé est de s'intéresser aux corps C_i en général et plus particulièrement aux corps C_1. Après une étude des propriétés algébriques des corps C_i, nous verrons quelques exemples de corps C_1. Nous étudions ensuite les premières propriétés des algèbres simples centrales et des corps de déploiement afin de construire le groupe de Brauer d'un corps. Le dernier résultat important sera la nullité du groupe de Brauer d'un corps C_1 et ses conséquences sur la commutativité des algèbres à division finies.

Table des matières

Les corps algébriquement clos sont caractérisés par l'existence de racines pour les polynômes sous des hypothèses très faibles. On peut alors chercher des corps vérifiant des conditions d'existence de racines pour des polynômes, sous des hypothèses de plus en plus fortes. On définit alors les corps C_i.

Il apparaît que ces conditions ont des implications algébriques intéressantes et notamment pour les corps C_1 ; en effet, si les corps algébriquement clos n'ont pas d'extensions finies différentes d'eux-mêmes, il n'existe pas d'algèbre simple centrale sur un corps C_1 qui soit non triviale (*i.e.* $M_n(k)$), nous parlerons par la suite d'extension simple centrale. Cela nous permet de revenir à leur appellation première : corps quasi-algébriquement clos. Nous définirons d'abord ces conditions d'existence de racines puis étudierons comment elles se comportent lorsque l'on effectue des extensions algébriques ou que l'on est sur un corps résiduel. Nous établirons ensuite quelques exemples de corps C_1 (corps finis, théorème de Tsen et citerons quelques autres exemples dus à S. Lang). Enfin, nous nous pencherons sur la question des algèbres simples centrales et de leurs structures — notamment les propriétés de déploiement — afin de construire le groupe de Brauer d'un corps, qui classifie les algèbres simples centrales sur un corps, pour montrer qu'il n'existe pas d'extension simple centrale d'un corps C_i.

1 Propriétés algébriques des corps C_i

Le but de cette partie est de généraliser la notion de corps algébriquement clos, comme déjà expliqué. Pour cela, donnons une définition alternative de corps algébriquement clos. Les notions de corps C_0 et de corps algébriquement clos sont équivalentes, mais on ne se place pas dans la même optique. La notion de corps C_0 met en lumière le fait que la notion de quasi-clôture algébrique (corps C_1) s'inscrit dans un cadre plus vaste : Les propriétés C_{i+1} généralisent les propriétés C_i pour tout i.

Définition 1.1. Un corps k est dit C_0 si tout polynôme homogène non constant à coefficients dans k en n variables et de degré n avec $n \geqslant 2$ a un zéro non trivial dans k.

On désigne par zéro trivial le n-uplet $(0, \ldots, 0)$.

À partir de maintenant, on notera toujours n et d le nombre de variables d'un polynôme homogène et son degré respectivement. Ceux-ci sont supposés non nuls.

Montrons qu'un corps est effectivement C_0 si et seulement s'il est algébriquement clos. En effet, si k est algébriquement clos (donc infini), il suffit de choisir une variable de degré partiel non nul, disons la première, puis de fixer les $n-1$ autres $x_2, \ldots, x_n$ telles qu'elles soient non toutes nulles, et que $P(X, x_2, \ldots, x_n)$ ne soit pas un polynôme constant. C'est possible, il suffit en effet écrire P comme un polynôme en une variable à coefficients (homogènes) dans $k[X_2, \ldots, X_n]$ et comme X est de degré partiel non nul, un des coefficients d'une puissance non nulle de X est un polynôme non nul et donc n'est pas nul pour une certaine valeur de $x_2, \ldots, x_n$ comme k est infini, de plus soit ce coefficient est une constante (pour X^d par exemple) auquel cas

on peut fixer les autres x_i à 1 et obtenir un polynôme non constant en X soit ce coefficient est un polynôme homogène en $X_2, \ldots, X_n$ de degré non nul et auquel cas il faut que les x_i soient non tous nuls pour qu'il soit non nul. On dispose donc d'un polynôme en X non constant en ayant fixé $x_2, \ldots, x_n$ non tous nuls et comme k est algébriquement clos, on peut trouver une valeur de X qui annule ce polynôme. On obtient ainsi un zéro non trivial. Réciproquement, on utilise le résultat suivant :

Théorème 1.1. *Si un corps k admet une extension K de degré $n \geqslant 2$, alors il existe un polynôme homogène à coefficients dans k de degré n et en n variables n'ayant que le zéro trivial.*

Démonstration. Soit $(v_1, \ldots, v_n)$ une base de K/k, la norme convient, à savoir le polynôme homogène défini comme le déterminant de l'endomorphisme du k-espace vectoriel K défini par la multiplication par l'élément $X_1 v_1 + \cdots + X_n v_n$. Ce polynôme ne s'annule qu'en 0 dans la mesure où la multiplication par l'inverse donne l'endomorphisme réciproque (qui est donc inversible et alors de déterminant non nul).

Ainsi, si k n'est pas algébriquement clos, il admet une extension de degré $n \geqslant 2$, et donc n'est pas C_0. □

Dans toute la suite, i désigne un entier naturel non nul.

Définition 1.2. Un corps k est dit C_i si tout polynôme homogène de degré d en n variables, avec $n > d^i$, a un zéro non trivial.

Historiquement, les corps C_1 (alors appelés corps quasi-algébriquement clos), ont été constuits comme généralisation la propriété d'être algébriquement clos suivante : Si un corps algébriquement clos n'admet d'extension finie stricte, il n'existe pas, pour un corps quasi-algébriquement clos k, de k-algèbre à division finie . En effet, il existe un analogue du théorème 1.1, à savoir que si un corps k admet une extension K non commutative (mais de centre contenant k), alors il existe un polynôme homogènes à coefficients dans k n'ayant pour zéro que le zéro trivial. Ce résultat se montre en reprenant la démonstration du théorème 1.1 et en ne changeant que le mot «norme» en «norme réduite» (nous construirons celle-ci par la suite).

Maintenant, on a imposé des conditions sur les polynômes homogènes, mais on peut aussi considérer tous les polynômes sans terme constant :

Définition 1.3. On dit qu'un corps k est fortement C_i si tout polynôme à coefficients dans k et sans terme constant avec $n > d^i$ a un zéro non trivial.

Malheureusement, un corps C_i n'est pas toujours fortement C_i. En revanche, en écrivant un polynôme sans terme constant comme une somme de polynômes homogènes, et d'après le théorème 1.7 qui donnera un zéro simultané pour ces polynômes homogènes, un corps C_i est souvent fortement C_{i+1}.

Après ces défintions, montrons un résultat usuel sur les corps algébriquement clos.

Théorème 1.2. *Soit k un corps algébriquement clos et soient $f_1, \dots, f_p$ p polynômes homogènes sur k de degré $d_1, \dots, d_p > 0$ et en n variables. Alors si $n > p$, ils possèdent un zéro commun non trivial.*

Démonstration. Par l'absurde, on suppose que $(0, \dots, 0)$ est le seul zéro commun à tous ces polynômes.

On note $\mathfrak{J}$ l'idéal engendré par les $f_1, \dots, f_p$, comme $V(\mathfrak{J}) = \{0\}$, on a, par le *Nullstellensatz* $rad(\mathfrak{J}) = (x_1, \dots, x_n)$ (les idéaux maximaux sont en bijection avec les points de k^n et sont de la forme $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ avec les $\alpha_i \in k$ et où $rad(\mathfrak{J}) = \{P \in k[x_1, \dots, x_n] : \exists s \in \mathbb{N}, P^s \in \mathfrak{J}\}$). Donc en particulier, pour chaque x_i, il existe $n_i \in \mathbb{N}$ tel que $x_i^{n_i} \in \mathfrak{J}$ et donc si on prend $r \geqslant \sum_{i=1}^{n} n_i$, on a que tout monôme de degré total $\geqslant r$ est dans $\mathfrak{J}$. Soit m un tel monôme, alors m s'écrit $m = \sum_{i=1}^{m} p_i f_i$ où les p_i sont des polynômes. Seulement, comme les f_i sont homogènes et que m est un monôme de degré total $d > r$, on peut pour les p_i supprimer tous les monômes sauf ceux de degré total $d - d_i$. On se ramène donc à exprimer m comme une somme de monômes de degré $< d$ multipliés par les f_i.

Lemme 1.3. *Tout monôme s'écrit $g(x_1, \dots, x_n)$ où g est un polynôme à coefficients dans $k[f_1, \dots, f_p]$ de degré total $< r$.*

Preuve du lemme. On va effectuer une récurrence pour montrer que tout monôme peut s'exprimer ainsi. La propriété est trivialement vraie pour les monômes de degré total $< r$. On la considère vraie pour les monômes de degré $< d$. Alors un monôme de degré d s'exprime d'après ce qui précède comme une somme de monôme (p_i) de degré strictement plus petit multipliés par certains f_i avec les mêmes notations qu'avant, on applique alors l'hypothèse de récurrence à ces nouveaux monômes et on obtient des $p_i(x_1, \dots, x_n) = g_i(x_1, \dots, x_n)$, où les g_i sont des polynômes de degré total $< r$ et à coefficients dans $k[f_1, \dots, f_p]$. Comme on les multiplie par des f_i, ils ne changent pas de degré total (les f_i s'intègrent dans leurs coefficients) et restent à coefficients dans $k[f_1, \dots, f_p]$. On a donc montré cette propriété. □

On note maintenant $K = k(f_1, \dots, f_p)$ le corps des fractions de cet anneau intègre, vu dans $k(x_1, \dots, x_n)$ et on va montrer que $K[x_1, \dots, x_n]$ (polynômes en les x_i et à coefficients dans K) est de dimension finie sur K. En effet, les monômes de degré total $< r$ forment une famille génératrice de $K[x_1, \dots, x_n]$ (on considère encore tous les anneaux dans $k(x_1, \dots, x_n)$). Par conséquent, $K[x_1, \dots, x_n]$ est un corps, qui contient les x_i donc aussi $k[x_1, \dots, x_n]$ donc $k(x_1, \dots, x_n)$. On en conclut que l'extension $k(x_1, \dots, x_n)/K$ est algébrique finie car de type fini comme corps, ce qui implique que le degré de transcendance de chacun de ces corps sur k est le même, or ce degré est n pour $k(x_1, \dots, x_n)$ et $\leqslant p$ pour K, donc $n \leqslant p$. □

Le degré du polynôme n'est pas pertinent lorsque le corps est algébriquement clos, cependant, pour les corps $C_i, i > 0$ ce ne sera pas le cas et il faut introduire encore quelques notions. On suppose de plus $d > 0$.

Définition 1.4. On dit qu'un polynôme homogène est une forme normique d'ordre i si $n = d^i$ et s'il n'admet que le zéro trivial.

De même, on dit qu'un polynôme est normique d'ordre i, s'il n'a pas de terme constant, vérifie $n = d^i$, et n'a que le zéro trivial.

La plupart des théorèmes sur les corps C_i seront encore vrais en replaçant «corps C_i» par «corps fortement C_i» et «polynôme homogène» par «polynôme sans terme constant».

Remarquons enfin que le cas $d = 1$ est trivial, de même que le cas $i = 0$. Les théorèmes 1.4, 1.7, 1.8 se réduisent au théorème 1.2 pour $i = 0$. Nous supposerons donc $i \geqslant 1$ à partir de maintenant, et nous exclurons le cas $d = 1$.

Théorème 1.4. *Soit k un corps C_i admettant au moins une forme normique d'ordre i. Soient r un entier naturel non nul, et $f_1, \ldots, f_r$ r polynômes homogènes en n variables communes, et chacun de degré d. Alors, si $n > rd^i$, ces polynômes ont un zéro non trivial en commun.*

Démonstration.

Lemme 1.5. *Si un corps k admet une forme normique d'ordre $i \geqslant 1$, alors il admet des formes normiques d'ordre i de degré arbitrairement grand.*

Démonstration. Soit φ une forme normique d'ordre i en n variables et de degré d. Alors $\varphi(\varphi|\ldots|\varphi)(x_1, \ldots, x_{n^2}) = \varphi(\varphi(x_1, \ldots, x_n), \ldots, \varphi(x_{n^2-n+1} \ldots, x_{n^2})$ ($|$ signifie que l'on prend de nouvelles variables pour φ) est une forme normique de degré d^2 en $n^2 = (d^2)^i$ variables. En effet, elle ne s'annule que si tous les $\varphi(x_i, \ldots, x_{i+n-1})$ s'annulent soit si tous les x_i sont nuls. □

D'après le lemme, on peut choisir une forme normique N d'ordre i de degré D suffisamment grand, que nous préciserons par la suite.

Posons $\varphi = N(f_1, \ldots, f_r|f_1, \ldots, f_r|\ldots|f_1, \ldots, f_r|0, \ldots, 0)$ où l'on a placé autant de $f_1, \ldots, f_r$ que possible — en mettant de nouvelles variables à chaque $|$ (comme dans le lemme) — à savoir $s = \lfloor D^i/r \rfloor$, puis comblé par $t = D^i - r\lfloor D^i/r \rfloor$ zéros. On a que φ a sn variables et est de degré Dd. Choisissons alors D tel que $sn > (Dd)^i$ *i.e.* tel que $D^i/\lfloor D^i/r \rfloor < n/d^i$. C'est bien possible car le membre de droite est strictement plus grand que r, et celui de gauche tend vers r quand D tend vers l'infini. Pour un D choisi tel que l'inégalité voulue soit vérifiée, φ admet un zéro non trivial car le corps est C_i. Alors chacune des s occurences respectives des f_i ($1 \leqslant i \leqslant r$) s'annule car N est normique. Et l'un de ces s «paquets» de polynômes admet un zéro non trivial. □

Dans le cas $i = 1$, l'hypothèse d'existence est superflue, comme l'exprime le corollaire :

Corollaire 1.6. *Soit k un corps C_1. Soient r un entier naturel non nul, et $f_1, \ldots, f_r$ r polynômes homogènes en n variables communes, et chacun de degré $d \geqslant 1$. Alors, si $n > rd$, ces polynômes ont un zéro non trivial en commun.*

En effet, il suffit d'utiliser le théorème 1.2 si k est C_0, et sinon, k admet une extension de degré supérieur ou égal à 2. Alors le théorème 1.1 assure l'existence d'une forme normique d'ordre 1.

Théorème 1.7. *Soit k un corps C_i admettant au moins une forme normique d'ordre i et de degré d pour tout d entier naturel non nul. Soient $f_1, \ldots, f_r$ r polynômes homogènes en n variables commmunes de degré $d_1, \ldots, d_r$ respectivement. Alors si $n > \sum_{j=1}^{r} d_j^i$, ces polynômes ont un zéro non trivial en commun.*

Démonstration. Ramenons-nous au théorème précédent.

Soit, pour tout $1 \leqslant i \leqslant r$, N_i une forme normique de degré $\prod_{j=1, j\neq i}^{r} d_j$.

On considère les r systèmes d'équations :

$$\begin{array}{lccccc}
1) & N_1(f_1|f_1|\ldots|f_1) = 0 & | & \ldots & | & N_1(f_1|f_1|\ldots|f_1) = 0 \quad (d_1^i \text{ équations}) \\
 & & & \ldots & & \\
r) & N_r(f_r|f_r|\ldots|f_r) = 0 & | & \ldots & | & N_r(f_r|f_r|\ldots|f_r) = 0 \quad (d_r^i \text{ équations})
\end{array}$$

On donne de nouvelles variables à chaque f_1 précédé d'une barre verticale, et on réutilise les mêmes pour les $r - 1$ systèmes restants.

On a alors affaire à $\sum_{j=1}^{r} d_j^i$ polynômes homogènes de degré $\prod_{j=1}^{r} d_j^i$ chacun et à $n(\prod_{j=1}^{r} d_j)^i$ variables en tout.

$n(\prod_{j=1}^{r} d_j)^i > \sum_{j=1}^{r} d_j^i . \prod_{j=1}^{r} d_j^i$ par hypothèse, et donc d'après le théorème précédent, ces $\sum_{j=1}^{r} d_j^i$ polynômes ont un zéro en commun. Comme on a utilisé les mêmes variables pour les r systèmes, on a notre zéro en commun pour $f_1, \ldots, f_r$. □

Théorème 1.8. *Soit k un corps C_i qui admet au moins une forme normique d'ordre i. Alors toute extension finie K de k est aussi C_i.*

Démonstration. Soit f un polynôme homogène en n variables à coefficients dans K, tel que $n > d^i$. On note r le degré de K/k, et $(w_1, \ldots, w_r)$ une base de K/k.

On introduit nr nouvelles variables par

$X_j = X_{j1}w_1 + \cdots + X_{jr}w_r$ pour $1 \leqslant j \leqslant r$

On décompose alors f en :

$f(X_1, \ldots, X_n) = f_1(X_{kj}, 1 \leqslant j \leqslant r, 1 \leqslant k \leqslant n)w_1 + \cdots + f_r(X_{kj}, 1 \leqslant j \leqslant r, 1 \leqslant k \leqslant n)w_r$

où les f_j $(1 \leqslant j \leqslant r)$ sont des polynômes homogènes en nr variables à coefficients dans k, et de degré d. Par hypothèse, $nr > rd^i$ Donc le théorème 1.4 permet de conclure. □

Corollaire 1.9. *Si k est C_1, toute extension finie est aussi C_1.*

Démonstration. Si k est algébriquement clos, toute extension finie est k lui-même. Sinon, on conclut encore avec le théorème 1.1. □

2 Exemples de corps C_1

2.1 Corps finis

Théorème 2.1 (Chevalley-Warning). *Les corps finis sont fortement C_1.*

Démonstration. Soit $\mathbb{F}_q$ le corps fini à q éléments (où $q = p^n$ avec p premier). On va prouver un résultat un peu plus fort, à savoir que le nombre de zéro d'un polynôme est congru à 0 modulo p. Soit P un polynôme de degré d et en n variables avec $n > d$. On pose alors :

$$\Sigma(P) = \sum_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{F}_q^n} (P(\alpha_1,\ldots,\alpha_n))^{q-1}$$

Et on note $N(P)$ le nombre de zéros de P dans $\mathbb{F}_q^n$, comme $\alpha^{q-1} = 1$ pour tout α non nul de $\mathbb{F}_q^n$ on en déduit qu'en fait, $\Sigma(P)$ est un élément de $\mathbb{F}_p \subset \mathbb{F}_q$ et de plus,

$$q^n - \Sigma(P) = \sum_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{F}_q^n} (1 - (P(\alpha_1,\ldots,\alpha_n))^{q-1}) \equiv N(P) \bmod p$$

On va montrer que $\Sigma(P) = 0$ ce qui impliquera directement le résultat (et même qu'il y a au moins p zéro si P est homogène comme il y a déjà le zéro trivial). Écrivons pour cela P^{q-1} comme une somme de monômes $x_1^{r_1}\ldots x_n^{r_n}$. Si un des r_i est nul on a clairement $\Sigma(x_1^{r_1}\ldots x_n^{r_n}) = 0$ (on somme q fois le même terme). Si aucun des r_i n'est nul, comme le degré de P est $d < n$ par hypothèse, un des r_i est plus petit que $q-1$, par exemple r_1. On fixe alors $(\alpha_2,\ldots,\alpha_n) \in \mathbb{F}_q^{n-1}$ et on prend ω un générateur de $\mathbb{F}_q^\times$, alors :

$$\sum_{\alpha\in\mathbb{F}_q} \alpha^{r_1}\alpha_2^{r_2}\ldots\alpha_n^{r_n} = \alpha_2^{r_2}\ldots\alpha_n^{r_n}\sum_{i=0}^{n}\omega^{ir_1} = \alpha_2^{r_2}\ldots\alpha_n^{r_n}\frac{(\omega^{r_1})^{q-1}-1}{\omega^{r_1}-1}$$

Et le dernier terme est égal à zéro, donc en parcourant $\mathbb{F}_q^{n-1}$ pour $(\alpha_2,\ldots,\alpha_n)$, on obtient bien que $\Sigma(x_1^{r_1}\ldots x_n^{r_n}) = 0$, d'où le résultat par linéarité. □

2.2 Anneaux de valuation discrète

Définition 2.1. Soit A un anneau principal, A est dit de valuation discrète s'il possède un idéal premier non nul et un seul, noté $\mathfrak{m}(A)$ ou juste $\mathfrak{m}$.

Le corps $A/\mathfrak{m}(A)$ s'appelle le corps résiduel de l'anneau A.

Les idéaux premiers non nuls d'un anneau principal sont de la forme πA où π est un élément irréductible. Être un anneau de valuation discrète revient donc à n'avoir, à multiplication par un élément inversible près, qu'un seul élément irréductible.

Proposition 2.2. *Soit A un anneau de valuation discrète, et π un élément irréductible de A, alors les idéaux de A sont de la forme $\pi^n A$.*

Démonstration. Comme A est un anneau principal, les idéaux sont de la forme xA, or on peut décomposer x en produit de facteurs irréductibles soit $x = \pi^n u$ où u est inversible comme π est le seul élément irréductible de A, on a donc bien $xA = \pi^n A$ □

Remarque 2.2.1. L'entier n ainsi défini s'appelle la valuation de x et est noté $\nu(x)$, sa valeur ne dépend clairement pas du choix de π. On peut de façon générale poser $\nu(x) = \sup\{n \in \mathbb{N}; x \in \pi^n A\}$ et on a alors $\nu(0) = +\infty$

On peut ensuite étudier le corps k des fractions de A. Ses éléments se notent $a/b,\ a, b \in A,\ b \neq 0$ et on peut étendre la valuation à tout k en posant $\nu(a/b) = \nu(a) - \nu(b)$. Cette définition est indépendante du choix de a et de b.

Proposition 2.3. *L'application $\nu : k^* \to \mathbb{Z}$ ainsi définie est un morphisme surjectif et vérifie $\nu(x + y) \geqslant \inf(\nu(x), \nu(y))$*

Démonstration. Le caractère de morphisme surjectif est évident et pour $a, b, c, d \in A$ $(b, c \neq 0)$, on a $a/b + c/d = (ad + bc)/bd$ soit en écrivant $i = \pi^{n_i} u_i,\ u \in A^*$ et en supposant $\alpha = n_a + n_d - n_c - n_b \geqslant 0$ *i.e.* $\nu(a/b) \geqslant \nu(c/d)$, $(\pi^{n_a+n_d} u_a u_d + \pi^{n_c+n_b} u_c u_d)/\pi^{n_b+n_d} u_b u_d = \pi^{n_a-n_b}(u_a u_d + u_c u_b \pi^\alpha) u_b^{-1} u_d^{-1}$ où $(u_a u_d + u_c u_b \pi^\alpha) u_b^{-1} u_d^{-1} \in A$, d'où la seconde propriété. □

On peut alors effectuer le raisonnement inverse :

Proposition 2.4. *Soit k un corps muni d'une application ν vérifiant les propriétés précédentes, alors $A = \{a \in k : \nu(a) \geqslant 0\}$ est un anneau de valuation discrète tel que $\mathfrak{m}(A) = \{a \in k : \nu(a) > 0\}$*

Démonstration. Soit $\pi \in A$ tel que $\nu(\pi) = 1$ alors tout élément de A peut s'écrire sous la forme $\pi^n u$ où u est inversible dans A (en effet, $\nu(u) = 0 \Rightarrow \nu(u^{-1}) = 0$ dans k^* du fait du caractère de morphisme de ν soit u inversible dans A) et π est irréductible dans A (un diviseur non inversible lui est associé) donc A n'a qu'un seul élément irréductible, de plus, si $\mathfrak{m}$ est un idéal de A,

et si $x \in \mathfrak{m}$ est un élément de valuation minimale, on a $\pi^n A \subset \mathfrak{m} \subset \pi^n A$ soit $\mathfrak{m}$ est un idéal principal de A, donc A est principal (il est intègre comme sous-anneau de k) n'ayant qu'un seul élément irréductible. □

Exemple Si on considère $k(X)$ muni de la valuation usuelle des fractions rationnelles, on est dans le cas précédent et le corps résiduel est k, avec X comme unique élément irréductible.

2.3 Formes normiques

Proposition 2.5. *Soit K un corps muni d'une valuation discrète, de corps résiduel κ. si κ a une forme normique N^* d'ordre i, alors K a une forme normique N d'ordre $i+1$.*

Démonstration. En effet, N^* est un polynôme homogène sur κ, en n variables et de degré d ($d^i = n$), on étend alors cette forme en relevant les coefficients de ce polynôme (qui sont dans κ) dans K, on obtient alors un polynôme homogène $P \in K[X]$. Soit alors $\pi \in K$ un élément de valuation 1, on pose $N(x_1, \ldots, x_{nd}) = P(x_1, \ldots, x_n) + \pi P(x_{n+1}, \ldots, x_{2n}) + \cdots + \pi^{d-1} P(x_{n(d-1)+1}, \ldots, x_{nd})$ et cette application convient. Elle est en effet de degré d, en $nd = d^{i+1}$ variables et si on suppose que $(x_1, \ldots, x_{nd})$ est un zéro de N alors on peut montrer qu'il est trivial.

On le suppose en effet non trivial et on procède par récurrence sur le maximum des valuations des x_i non nuls. Comme N^* est un polynôme homogène, on peut supposer que toutes les valuations sont positives, sinon, si par exemple x_1 est de valuation strictement négative, on va utiliser le fait que $x_1^{-d} N(x_1, \ldots, x_{nd}) = N(1, x_1^{-1} x_2, \ldots, x_1^{-1} x_{nd})$ comme N est un polynôme homogène de degré d et en faisant la même opération pour tous les éléments de valuation strictement négative, on obtient un zéro dont toutes les projections sont dans A l'anneau de valuation discrète associé à K.

Notons φ la projection sur κ, le corps résiduel de A. On a alors :

$$N^*(\varphi(x_1), \ldots, \varphi(x_n)) = 0$$

Donc comme N^* est une forme normique, on a $\varphi(x_1) = \cdots = \varphi(x_n) = 0$. On peut donc écrire $x_1 = \pi x_1', \ldots, x_n = \pi x_n'$ où les x_i' sont de valuations positives, et inférieure à 1 de celle de x_i quand $x_i \neq 0$. En conséquence, on a $\pi^d P(x_1', \ldots, x_n') + \pi P(x_{n+1}, \ldots, x_{2n}) + \cdots + \pi^{d-1} P(x_{n(d-1)+1}, \ldots, x_{nd}) = 0$ soit en simplifiant par π qui est non nul, on obtient un nouveau zéro $(x_{n+1}, \ldots, x_{nd}, x_1', \ldots, x_n')$ avec les derniers éléments qui ont perdu 1 en valuation (sauf s'ils sont déjà nuls). On peut recommencer avec $x_{n+1}, \ldots, x_{2n}$ et ainsi de suite jusqu'à avoir diminué le maximum de valuation des x_i non nuls de 1. Par conséquent et d'après ce qui précède, tous les x_i sont de valuations infinie donc nuls, donc la forme est bien normique. □

Remarque 2.5.1. On peut donc déduire de cela que si κ est C_0 alors K possède une forme normique d'ordre 1 (en prenant $N^*(x) = x^d$) et que dans le cas contraire, il existe une forme normique d'ordre 2 (la forme normique d'ordre 1 sur κ étant donnée par la norme sur une extension algébrique de κ).

2.4 Théorème de Tsen

Soit k un corps C_i possédant une forme normique d'ordre i, alors récursivement, $k(X_1, \ldots, X_k)$ possède une forme normique d'ordre $i+k$. On peut donc en déduire le lemme suivant :

Lemme 2.6. *Soit k un corps C_i possédant au moins une forme normique d'ordre i alors $k(t)$ est C_{i+1}.*

Démonstration. Soit $P(x_1, \ldots, x_n)$ un polynôme homogène en n variables et de degré d sur $k(t)$ vérifiant $n > d^{i+1}$. Nous allons montrer que P admet un zéro non trivial.

Soit

$$\begin{aligned} x_1 &= \xi_{10} + \xi_{11}t + \cdots + \xi_{1s}t^s \\ x_2 &= \xi_{20} + \xi_{21}t + \cdots + \xi_{2s}t^s \\ &\cdots \\ x_n &= \xi_{n0} + \xi_{n1}t + \cdots + \xi_{ns}t^s \end{aligned}$$

Où les ξ_{ij} sont des éléments de k et s non déterminé pour l'instant mais pouvant être arbitrairement grand. Soit r le degré le plus élevé des coefficients de P, on peut alors réécrire P sous la forme :

$$P(x_1, \ldots, x_n) = P_0(\xi_{10}, \ldots, \xi_{ns}) + P_1(\xi_{10}, \ldots, \xi_{ns})t + \cdots + P_{ds+r}(\xi_{10}, \ldots, \xi_{ns})t^{ds+r}$$

Où les P_i sont tous des polynômes homogènes de degré d en $n(s+1)$ variables. Pour les avoir tous nuls en même temps, on utilise le théorème 1.4 en satisfaisant l'inéquation

$$n(s+1) > d^i(ds + r + 1) \Leftrightarrow n - d^{i+1} > (d^i(r+1) - n)/s$$

qui est satisfaite pour s assez grand. □

Théorème 2.7 (Théorème de Tsen). *Soit k un corps C_i possédant au moins une forme normique d'ordre i, alors le corps $k(X_1, \ldots, X_k)$ est C_{i+k}.*

Démonstration. Ce théorème se démontre directement par récurence en utilisant le lemme. □

Citons enfin d'autres exemples de corps C_1, nous renvoyons à [1] et [2] pour une démonstration de ces théorèmes et à [3] pour des détails sur les ramifications. Rappelons auparavant quelques définitions :

Définition 2.2. Soit K/k une extension de corps munis d'une valuation discrète (on suppose que celle de K prolonge celle de k) et de corps résiduels λ, κ alors κ s'identifie avec un sous-corps de λ et l'extension K/k est dite non ramifiée si $[K : k] = [\lambda : \kappa]$. De plus, si on fixe une clôture algébrique $\bar{\kappa}$ de κ alors il existe une extension maximale non ramifiée de k qui correspond à la limite inductive des extensions de k correspondant aux extensions séparables de κ.

Exemple $\mathbb{C}((t))$ est l'extension maximale non ramifiée de $\mathbb{R}((t))$

Théorème 2.8. *L'extension maximale non ramifiée d'un corps complet pour une valuation discrète et dont le corps résiduel est parfait est C_1, il en va de même $k((t))$, le corps des séries de Laurent sur k où k est algébriquement clos.*

Une fois établies ces propiétés générales sur les corps C_i, nous allons nous pencher sur les propriétés des algèbres simples centrales et leur classification en général puis plus particulièrement au sujet des corps C_1 pour constater qu'ils n'ont pas d'extensions simples centrales non triviales (différentes de $M_n(k)$).

3 Algèbres simples centrales

3.1 Théorème de Wedderburn

Une k-algèbre A est dite centrale si son centre est réduit à k. Elle est dite simple si ses seuls idéaux bilatères sont 0 et A. Par exemple une algèbre à division est centrale sur son centre $Z(D)$ (qui est un corps), et est évidemment simple. Donnons un autre exemple d'algèbre simple centrale qui nous sera utile par la suite :

Exemple Soit D une algèbre à division sur un corps k, et $n \geqslant 1$. L'anneau de matrices $M_n(D)$ est simple, et de plus son centre est constitué des homothéties de rapport appartenant à $Z(D)$. Donc $M_n(D)$ est simple centrale sur le corps $Z(D)$.

Idéaux à gauche de $M_n(D)$ Soit pour $1 \leqslant r \leqslant n$, $I_r \subseteq M_n(D)$ l'idéal à gauche constitué des matrices n'ayant des éléments non nuls que sur la r^e colonne. On montre grâce aux matrices élémentaires que tout idéal à gauche contient l'un de ces idéaux. Ces n idéaux sont donc exactement les idéaux à gauche minimaux de $M_n(D)$. Remarquons qu'on a : $I_r \simeq D^n$ en tant que $M_n(D)$-modules. En fait, on montre de la même manière que tout idéal à gauche de $M_n(D)$ est somme directe de certains de ces n idéaux.

Théorème 3.1 (Théorème de Wedderburn). *Soit A une algèbre simple de dimension finie sur un corps k. Alors il existe un entier $n \geqslant 1$ et une algèbre à division $D \supset k$ telle que A soit isomorphe à l'anneau $M_n(D)$. De plus, D est unique à isomorphisme près.*

Lemme 3.2 (Schur). *Soit M un module simple sur une k-algèbre A. Alors* $\mathrm{End}_A(M)$ *est une algèbre à division.*

Démonstration. Soit f un endomorphisme non nul de M. Son noyau est un sous-A-module différent de M donc réduit à 0. De même, son image ne peut être que M tout entier. C'est donc un isomorphisme, qui a donc un inverse dans $\mathrm{End}_A(M)$. □

Soit maintenant M un A-module à gauche, on note $D = \mathrm{End}_A(M)$. On munit naturellement M d'une structure de D-module à gauche par la loi :

$\forall \varphi \in \mathrm{End}_A(M), \forall x \in M, \varphi.x = \varphi(x)$.

On considère alors $\mathrm{End}_D(M)$, et on définit un homomorphisme d'anneau par :

$\lambda_M : A \to \mathrm{End}_D(M)$ $a \longmapsto (x \in M \mapsto ax \in M)$

$x \in M \mapsto ax \in M$ est bien un D-endormorphisme de M, puisque si φ est un élement de D, $a\varphi.x = a\varphi(x) = \varphi(ax) = \varphi.ax$.

Lemme 3.3 (Rieffel). *Soit L un idéal à gauche non réduit à zéro d'une k-algèbre simple A. alors l'application λ_L définie ci-dessus est un isomorphisme.*

Remarquons qu'un idéal à gauche n'est autre qu'un sous-module du A-module à gauche A.

Démonstration. Comme $\lambda_L \neq 0$, son noyau est un idéal bilatère propre de A. Mais A est simple donc λ_L est injective. Pour montrer la surjectivité, prouvons d'abord que $\lambda_L(L)$ est un idéal à gauche de $\mathrm{End}_D(L)$. Soit $\varphi \in \mathrm{End}_D(L)$, et $l \in L$. Alors $\varphi\lambda_L(l)$ est le D-endomorphisme de L suivant : $x \mapsto \varphi(lx) = \varphi(l)x$, car $y \mapsto yx$ est A-endomorphisme de L. Donc $\varphi\lambda_L(l) = \lambda_L(\varphi(l))$, et $\lambda_L(L)$ est un idéal à gauche. Alors l'idéal à droite LA engendré par L est un idéal bilatère, et donc $LA = A$. En particulier, on peut écrire : $1 = \sum l_i a_i$ avec $l_i \in L$, $a_i \in A$. Donc si $\varphi \in \mathrm{End}_D(L)$, on a $\varphi = \varphi\lambda_L(1) = \sum \varphi\lambda_L(l_i)\lambda_L(a_i)$.

Or, comme $\lambda_L(L)$ est un idéal à gauche, on a : $\forall i, \varphi\lambda_L(l_i) \in \lambda_L(L)$, donc $\varphi \in \lambda_L(A)$. □

Preuve du théorème de Wedderburn. Comme A est de dimension finie, une suite décroissante d'idéaux à gauche doit être stationnaire (ce sont des sous-espaces vectoriels). Soit donc L un idéal à gauche minimal : c'est un A-module simple. Alors, d'après le lemme de Schur, $D = \mathrm{End}_A(L)$ est une algèbre à division, et d'après le lemme de Rieffel, on dispose d'un isomorphisme $A \simeq \mathrm{End}_D(L) \simeq M_n(D)$, où n est la dimension de L sur D (L est

de dimension finie sur k donc sur D), le dernier isomorphisme étant obtenu par le choix d'une base.

Pour l'unicité, supposons que D et D' sont deux algèbres à division telles que $A \simeq M_n(D) \simeq M_m(D')$ où m et n sont deux entiers. Alors, comme on l'a déjà remarqué, $L \simeq D^n \simeq D'^m$, d'où $D \simeq \mathrm{End}_A(D^n) \simeq \mathrm{End}_A(L) \simeq \mathrm{End}_A(D'^m) \simeq D'$. □

Corollaire 3.4. *Soit k un corps algébriquement clos. Alors toute k-algèbre simple centrale est isomorphe à $M_n(k)$ pour un certain $n \geqslant 1$.*

Démonstration. D'après le théorème de Wedderburn, il suffit de voir qu'il n'existe pas d'algèbre à division $D \supset k$ de dimension finie sur k autre que k. Soit donc d un élément non nul de D. La famille $(d^i)_{i\in\mathbb{N}}$ est liée, et donc il existe un polynôme annulateur de d, et comme D est une algèbre à division, et donc n'admet pas de diviseur de zéro, on peut le supposer irréductible. Alors $k[d]$ est un corps de dimension finie sur k (pour la stabilité par passage à l'inverse, il suffit d'utiliser Bézout), donc c'est k, car k est algébriquement clos. Ainsi $d \in k$, et $D = k$. □

3.2 Corps de déploiement

Théorème 3.5. *Soient k un corps et A une k-algèbre de dimension finie. Alors A est une algèbre simple centrale si et seulement s'il existe un entier $n \geqslant 1$ et une extension de corps finie $K \supseteq k$ telle que $A \otimes_k K$ est isomorphe à $M_n(K)$.*

Lemme 3.6. *Avec les mêmes notations que précédemment, A est une algèbre simple centrale si et seulement si $A \otimes_k K$ est une algèbre simple centrale pour une certaine extension de corps $K \supseteq k$.*

Démonstration. Si I est un idéal bilatère non trivial de A, alors $I \otimes_k K$ est un idéal bilatère non trivial de $A \otimes_k K$. De même, si A n'est pas centrale, $A \otimes_k K$ ne l'est pas non plus. Donc si $A \otimes_k K$ est simple centrale, A aussi.

En utilisant le théorème de Wedderburn pour la réciproque, il suffit de considérer le cas où $A = D$ est une algèbre à division (qui est centrale comme A). Soit alors une k-base de K : $(w_1, \ldots, w_n)$. $(1 \otimes w_1, \ldots, 1 \otimes w_n)$ est une D-base de $D \otimes_k K$ vu comme D-espace vectoriel à gauche. Soit alors $x = \sum \alpha_i(1 \otimes w_i)$ un élement du centre de $D \otimes_k K$. On a pour tout $d \in D$, $x = (d^{-1} \otimes 1)x(d \otimes 1) = \sum(d^{-1}\alpha_i d)(1 \otimes w_i)$, donc $d^{-1}\alpha_i d = \alpha i$ pour tout $1 \leqslant i \leqslant n$ et pour tout $d \in D$, car la famille $(1 \otimes w_i)_{1\leqslant i\leqslant n}$ est libre. Comme D est centrale sur k, les α_i sont nécessairement dans k et donc $D \otimes_k K$ est centrale sur K.

Soit maintenant J un idéal bilatère non nul de $D \otimes_k K$ engendré par des éléments $z_1, \ldots, z_r$ que l'on peut supposer D-linéairement indépendants

et compléter en une base en ajoutant des éléments de $(1 \otimes w_1, \ldots, 1 \otimes w_n)$, disons $1 \otimes w_{r+1}, \ldots, 1 \otimes w_n$. Alors pour $1 \leqslant i \leqslant r$, on peut écrire :

$$1 \otimes w_i = \sum_{j=r+1}^{n} \alpha_{ij}(1 \otimes w_j) + y_i$$

où les α_{ij} sont dans D et les y_i sont des combinaisons linéaires des z_i, donc des éléments de J.

Les y_i sont alors linéairement indépendants du fait de la liberté des $1 \otimes w_j (1 \leqslant j \leqslant n)$, donc forment une base de J. De plus, comme J est un idéal bilatère, on a pour tout $d \in D$ et pour tout $1 \leqslant i \leqslant r$, $d^{-1} y_i d \in J$, et donc il existe $(\beta_{il})_{1 \leqslant i \leqslant r, 1 \leqslant l \leqslant r}$ telle que : $d^{-1} y_i d = \sum_{l=1}^{r} \beta_{il} y_l$. Alors,

$$1 \otimes w_i - \sum_{j=r+1}^{n} (d^{-1}\alpha_{ij}d)(1 \otimes w_j) = \sum_{l=1}^{r} \beta_{il} 1 \otimes w_l - \sum_{l=1}^{r} \beta_{il} \sum_{j=r+1}^{n} \alpha_{lj}(1 \otimes w_j)$$

La liberté des $1 \otimes w_j (1 \leqslant j \leqslant n)$ implique alors que $\beta_{il} = \delta_{il}$ où δ est le symbole de Kronecker, soit y_i central, puis $d^{-1}\alpha_{ij}d = \alpha_{ij}$, donc $\alpha_{ij} \in k$, car D est centrale ($k \subseteq D \otimes_k K$ via l'injection $w \mapsto 1 \otimes w$). Donc J est engendré par des éléments de K. Comme K est un corps, on a $J \cap K = K$, donc $J = D \otimes_k K$. Donc $D \otimes_k K$ est simple.

□

Preuve du théorème 3.5. Montrons d'abord le sens $\Leftarrow$. Comme on l'a déjà vu, $M_n(K)$ est une algèbre simple centrale sur le corps K, donc $A \otimes_k K$ aussi, et d'après le lemme, A est une algèbre simple centrale sur le corps k.

Montrons maintenant le sens $\Rightarrow$. Soit $\bar{k}$ une clôture algébrique de k. D'après le lemme et le corollaire 3.4, on a $A \otimes_k \bar{k} \simeq M_n(\bar{k})$ pour un certain n. Remarquons maintenant que pour toute extension finie $K \supseteq k$ incluse dans $\bar{k}$, l'injection canonique $K \hookrightarrow \bar{k}$ induit une injection $A \otimes_k K \to A \otimes_k \bar{k}$, et que donc $A \otimes_k \bar{k}$ apparaît comme l'union des $A \otimes_k K$, sur les $K \supseteq k$ extensions finies incluse dans $\bar{k}$. Alors, pour une extension finie de k assez grande $K \subset \bar{k}$ l'algèbre $A \otimes_k K$ contient les n^2 éléments $e_1, \ldots, e_{n^2} \in A \otimes_k \bar{k}$ correspondant aux matrices élémentaires de $M_n(\bar{k}) \simeq A \otimes_k \bar{k}$, et tous les coefficients a_{ijk} définissant le produit

$$e_i e_j = \sum a_{ijk} e_k$$

sont dans K. On obtient alors un K-isomorphisme $A \otimes_k K \simeq M_n(K)$ en envoyant chaque e_i sur la matrice élémentaire de $M_n(K)$ correspondant (le même que pour la correspondance $M_n(\bar{k}) \simeq A \otimes_k \bar{k}$) □

Corollaire 3.7. *Si A est une k-algèbre centrale simple, sa dimension sur k est un carré.*

Définition 3.1. Un corps K comme dans le théorème ($A \otimes_k K \simeq M_n(K)$ pour un certain n) est appelé corps de déploiement de A. On dit que A est déployé par k. Enfin, l'entier $\sqrt{dim_k(A)}$ est appelé degré de A.

Terminons enfin cette partie par une proposition cruciale pour la suite.

Théorème 3.8 (Noether, Köthe). *Une k-algèbre simple centrale a un corps de déploiement séparable sur k.*

Démonstration. Supposons qu'il existe une k-algèbre simple centrale A qui ne soit déployée par aucune extension finie séparable $K \supseteq k$. Soient alors $k^s \subseteq \bar{k}$ des clôtures séparable et algébrique de k. Alors, par le même argument que dans la preuve du théorème 3.5, la k^s-algèbre $A \otimes_k k^s$ n'est pas déployée par k^s (sinon A serait déployée par une extension finie incluse dans k^s), donc est isomorphe, par le théorème de Wedderburn, à une certaine algèbre de matrice $M_n(D)$ où D est une algèbre à division sur k^s différente de k^s. Soit d la dimension de D sur k^s. On a $d > 1$ et par le corollaire 3.4, on a $D \otimes_{k^s} \bar{k} \simeq M_d(\bar{k})$. En considérant les éléments de $M_n(\bar{k})$ comme les points d'un espace affine sur $\bar{k}$ de dimension d^2, on remarque que D correspond aux éléments définis sur k^s. Or D est algèbre à division, donc ses éléments non nuls sont envoyés sur des matrices inversibles de $M_n(\bar{k})$, en particulier, elles ont un déterminant non nul. Or le déterminant d'une matrice est un polynôme P en d^2 variables, à coefficients dans $-1, 1$ et irréductible. *A fortiori*, $P \in k^s[x_1, \ldots, x_{d^2}]$, et P a pour unique zéro dans $(k^s)^{d^2}$ le zéro trivial. L'hypersurface de l'espace affine définie comme les points d'annulation de P ne contient pour élement défini sur k^s que zéro. Ceci contredit un point fondamental de la géométrie algébrique (voir [2] pour plus de détails). □

Corollaire 3.9. *Une k-algèbre A de dimension finie est simple centrale si et seulement s'il existe un entier $n \geqslant 1$ et une extension $K \supseteq k$ galoisienne de groupe de Galois fini, tels que $A \otimes_k K$ est isomorphe à l'algèbre de matrices $M_n(K)$*

Démonstration. Cela découle du théorème 3.5, du théorème précédent, et du fait que toute extension finie séparable est incluse dans une extension galoisienne finie du corps de base.

□

Terminons par une remarque, qui nous invitera à être prudent par la suite : Si A est une k-algèbre simple centrale qui n'est pas déployée par k mais par une extension finie galoisienne $K \supseteq k$ de groupe de Galois G, et que l'on munit $M_n(K)$ et $A \otimes_k K$ des actions de G naturelles, l'isomorphisme $A \otimes_k K \simeq M_n(K)$ est incompatible avec l'action de G. Sinon, on aurait $A \simeq (A \otimes_k K)^G \simeq (M_n(K))^G \simeq M_n(k)$.

4 Groupe de Brauer

4.1 Construction

Le but dans la suite va être de classer les algèbres simples centrales sur un corps k en prenant en compte un corps K de déploiement.

Lemme 4.1. *Si A et B sont des k-algèbres simples centrales déployées par K, alors il en est de même de $A \otimes_k B$.*

Démonstration. On va utiliser pour cela l'isomorphisme $(A \otimes_k B) \otimes_k K \simeq (A \otimes_k K) \otimes_K (B \otimes_k K)$. Alors le résultat découle immédiatement du fait que $M_n(K) \otimes_K M_m(K) \simeq M_{nm}(K)$. □

Pour effectuer notre classification, on va considérer les classes d'isomorphisme de k-algèbres déployées par K et de degré n. En effet, une k-algèbre de dimension finie n'est jamais qu'un espace vectoriel V sur k, de dimension n^2 (soit k^{n^2}) et muni d'une application bilinéaire de $V \times V \to V$ qui correspond à la multiplication et que l'on peut assimiler à un élément de $V^* \otimes_k V^* \otimes_k V$. Donc à isomorphisme près, on peut toujours se ramener à un tel cas. On note $ASC_K(n)$ une telle classe d'algèbres simples centrales de degré n déployées par un même corps K. On peut envoyer $ASC_K(n)$ $ASC_K(nm)$ en tensorisant chaque algèbre par $M_m(k)$.

Proposition 4.2. *Une telle application est injective.*

Démonstration. Supposons que nous ayons A et A' deux algèbres simples centrales sur k avec $A \otimes_k M_m(k) \simeq A' \otimes_k M_m(k)$ alors, par le théorème de Wedderburn, A et A' sont des algèbres de matrices sur des algèbres à division D et D' respectivement, et par conséquent, $A \otimes_k M_m(k)$ et $A' \otimes_k M_m(k)$ aussi. Seulement, on a unicité par le théorème de Wedderburn, donc $D \simeq D'$ et donc $A \simeq A'$ pour des raisons dimensionnelles. □

Considérons $\bar{k}$ une clôture algébrique de k. Nous pouvons d'après ce que nous avons dit précédemment considérer l'ensemble des classes d'isomorphisme d'algèbres simples centrales sur k. On obtient alors des classes regroupant des algèbres de même degré, nous allons maintenant rajouter une condition d'équivalence pour construire le groupe de Brauer de k.

Définition 4.1. Soient A et A' deux k-algèbres simples centrales, on dit qu'elles sont équivalentes au sens de Brauer (ou semblables) s'il existe $m, m' \in \mathbb{N}$ tels que $A \otimes_k M_m(k) \simeq A' \otimes_k M_{m'}(k)$. C'est une relation d'équivalence et on note $\mathrm{Br}(k)$ l'ensemble des classes d'équivalences.

Remarque 4.2.1. La première chose que l'on peut constater, c'est que l'on peut très bien se restreindre aux algèbres simples centrales déployées par une même extension galoisienne K/k (en faisant une union sur les degrés,

c'est cohérent par l'injectivité de la proposition précédente) et considérer les classes d'équivalences (que l'on note $\mathrm{Br}(K|k)$), puis ensuite faire une union sur les extensions galoisiennes de k dans $\bar{k}$ en faisant attention à ne pas prendre plusieurs fois les mêmes algèbres (une algèbre déployée par une extension l'est par les extensions de cette extension).

Ensuite, chaque classe d'équivalence contient (à isomorphisme près) une unique algèbre à division (évidemment cenrale sur k). C'est une conséquence directe du théorème de Wedderburn. En conséquence, on peut dire que $\mathrm{Br}(k)$ est une classification des algèbres à division centrales sur k et que $\mathrm{Br}(K|k)$ est une classification des algèbres à division centrales sur k et déployées par K.

Enfin, le produit tensoriel respecte manifestement l'équivalence au sens de Brauer et passe donc aux classes, de plus par le lemme 4.1, $\mathrm{Br}(K|k)$ est stable par ce produit (tout comme $\mathrm{Br}(k)$) et donc, par les propriétés du produit tensoriel, ce sont des monoïdes commutatifs munis de ce produit avec pour élément neutre la classe de k.

Théorème 4.3. *Les ensembles* $\mathrm{Br}(K|k)$ *et* $\mathrm{Br}(k)$ *munis du produit tensoriel sont des groupes abéliens, appelés groupe de Brauer de* k *relatif à* K *ou juste groupe de Brauer de* k*.*

Démonstration. Commençons par définir l'algèbre opposée à une algèbre A, notée A°, c'est l'algèbre qui possède le même ensemble sous-jacent, la même structure d'espace vectoriel mais dont la multiplication est donnée par $(x, y) \mapsto yx$ au lieu de xy, où xy est le produit dans A. Si A est simple centrale déployée par K, il en est de même de A°.

On va montrer que la classe de A° constitue un inverse pour la classe de A. A est muni d'une structure de $A \otimes_k A^\circ$-module par $a \otimes b \cdot \alpha = a\alpha b, \alpha \in A$. Un endomorphisme φ de A doit vérifier $\varphi(1)a = 1 \otimes a \cdot \varphi(1) = \varphi(1 \otimes a \cdot 1) = \varphi(a) = \varphi(a \otimes 1 \cdot 1) = a \otimes 1 \cdot \varphi(1) = a\varphi(1)$, autrement dit, un tel endomorphisme est donné par la multiplication par un élément du centre de A soit par un élément de k. On a donc $\mathrm{End}_{A \otimes A^\circ}(A) \simeq k$ et comme $A \otimes A^\circ$ est simple par le lemme 4.1, le lemme de Rieffel donne $A \otimes A^\circ \simeq \mathrm{End}_k(A) \simeq M_{n^2}(k)$ où $n^2 = \dim_k A$. □

4.2 Norme réduite

Proposition 4.4. *Soit* K *un corps, les automorphismes de* $M_n(K)$ *sont intérieurs,* i.e. *donnés par* $M \mapsto C^{-1}MC$ *pour une matrice* $C \in \mathrm{GL}_n(K)$*.*

Démonstration. Considérons les idéaux à gauche I_r de $M_n(K)$ qui sont donnés par les matrices n'ayant des termes non nuls que sur une colonne fixée. Alors ceux-ci sont permutés par l'action de $\lambda \in \mathrm{Aut}(M_n(K))$, par une permutation σ. On peut supposer, en composant λ avec l'automorphisme intérieur donnée par $M \mapsto S^{-1}MS$ où $S = (\delta_{i\sigma(j)})_{i,j}$ que $\lambda(I_r) = I_r$. De plus, en

prenant $e_1, \ldots, e_n$ une base de K^n et en associant à chaque $M \in I_1$ le vecteur Me_1, on obtient un isomorphisme entre I_1 et K^n, ainsi, λ s'interprète comme un automorphisme *lambda* de K^n, *via* $\bar{\lambda} Me_1 = \lambda(M)e_1$ qui est donc défini par $C \in \mathrm{GL}_n(K)$. On a alors pour toute matrice $M \in M_n(K)$ et $H \in I_1$, comme $MH \in I_1$, $CMH = \lambda(MH) = \lambda(M)\lambda(H) = \lambda(M)CH$ soit $(CM - \lambda(M)C)H = 0$ d'où en multipliant à droite par e_1, $CM - \lambda(M)C = 0$ *i.e.* $\lambda(M) = CMC^{-1}$. □

Corollaire 4.5. *Le groupe des automorphismes de $M_n(K)$ est* $\mathrm{PGL}_n(K)$.

Démonstration. D'après ce qui précède, on a un homomorphisme surjectif de $\mathrm{GL}_n(K)$ dans $\mathrm{Aut}(M_n(K))$, dont le noyau est le centre de $M_n(K)$, soit KI_n. □

Soit A une algèbre simple centrale sur k de degré n et soit K une extension galoisienne de k qui déploie A et de groupe de Galois G. Alors on peut choisir φ, isomorphisme de K-algèbres : $A \otimes_k K \simeq M_n(K)$. Il faut faire très attention au fait qu'un tel isomorphisme n'est pas compatible avec l'action de G, nous allons donc le tordre par un cocycle pour obtenir une meilleure action de G sur $M_n(K)$.

Rappelons d'abord quelques points sur les cocycles.

Définition 4.2. Soit G un groupe, A un autre groupe sur lequel G agit (avec $\forall a, b \in A, \forall \sigma \in G, \sigma(ab) = \sigma(a)\sigma(b)$) et X un ensemble sur lequel G et A agissent, on appelle cocycle de G à valeur dans A une application $a : \sigma \mapsto a_\sigma$ telle que $a_{\sigma\tau} = a_\sigma \sigma(a_\tau)$.

Lemme 4.6. *Sous les mêmes hypothèses, alors l'application qui va de $G \times X$ dans X et qui à (σ, x) associe $a_\sigma(\sigma(x))$ est une action de G sur X, qui est dite tordue par le cocycle a.*

Démonstration. En effet, $a_{\sigma\tau}(\sigma\tau(x)) = a_\sigma \sigma(a_\tau)(\sigma\tau(x)) = a_\sigma \sigma(a_\tau(\tau(x)))$. □

On note désormais ${}_aX$ l'ensemble X muni de cette action tordue de G.

On considère alors $\mathrm{Gal}(K/k)$ pour G, $\mathrm{Aut}(M_n(K))$ pour A, muni pour l'action de G de la conjugaison ($\sigma \cdot a = \sigma \circ a \circ \sigma^{-1}$), et pour X on prend $M_n(K)$ muni de l'action usuelle de G sur K.

On cherche à construire un cocycle qui tordrait l'action de G sur $M_n(K)$ de façon à rendre φ équivariante, c'est-à-dire à avoir $a_\sigma(\sigma(\varphi(x))) = \varphi(\sigma(x))$ un calcul rapide donne :

$$\forall z \in M_n(K), a_\sigma(z) = \varphi \circ \sigma \circ \varphi^{-1} \circ \sigma^{-1}(z)$$

Vérifions qu'il s'agit bien d'un cocycle.

$$\begin{aligned} a_{\sigma\tau} &= \varphi \circ \sigma \circ \tau \circ \varphi^{-1} \circ \tau^{-1} \circ \sigma^{-1} \\ &= \varphi \circ \sigma \circ \varphi^{-1} \circ \sigma^{-1} \circ \sigma \circ \varphi \circ \tau \circ \varphi^{-1} \circ \tau^{-1} \circ \sigma^{-1} \\ &= a_\sigma \circ \sigma(a_\tau) \text{ car } \varphi \circ \tau \circ \varphi^{-1} \circ \tau^{-1} \in \mathrm{Aut}(M_n(K)) \end{aligned}$$

On a donc construit une action de G sur $M_n(K)$ qui est compatible avec φ, on peut donc écrire $A \otimes_k K \simeq_a M_n(K)$ par φ et on dispose alors aussi de $A \simeq ({}_aM_n(K))^G$ en prenant les invariants.

Comme a_σ est un automorphisme de $M_n(K)$, il est intérieur et correspond donc à la conjugaison par une certaine matrice que nous noterons aussi a_σ et l'on note $\sigma \cdot x$ l'action de G sur $M_n(K)$ tordue par le cocycle a.

Considérons maintenant le déterminant : $M_n(K) \to K$. Alors on a :

$$\begin{aligned} \forall \sigma \in G, \forall M \in M_n(K), \det(\sigma \cdot M) &= \det(a_\sigma \sigma(M) a_\sigma^{-1}) \\ &= \det(\sigma(M)) \\ &= \sigma(\det(M)) \end{aligned}$$

Le déterminant est compatible avec l'action de G, donc en considérant les invariants pour G, on obtient une application Nrd de A dans k, appelée norme réduite.

Remarque 4.6.1. Tout d'abord, la valeur de Nrd ne dépend pas du choix de φ, en effet, si on prend un autre isomorphisme, on obtient un cocycle conjugé à a qui ne fait que conjuguer les matrices des automorphismes a_σ, ce qui laisse invariant le déterminant. Enfin, la construction ne dépend pas de K non plus, il suffit en effet de l'effectuer dans le corps engendré par deux corps de déploiement pour obtenir le même résultat pour les deux.

Proposition 4.7. *Si A est une k-algèbre simple centrale, alors un élément $a \in A$ est inversible si et seulement si* $\mathrm{Nrd}(a) \neq 0$. *En particulier, A est un algèbre à division si et seulement si* Nrd *ne s'annule qu'en 0.*

Démonstration. Si a est inversible, pour tout isomorphisme $\varphi : A \otimes_k K \to M_n(K)$, $\varphi(a)$ est inversible et a donc un déterminant non nul. À l'inverse, si on considère un tel φ est si on suppose que $\varphi(a)$ est inversible (de déterminant non nul), alors il existe $B \in M_n(K)$ telle que $\varphi(a)B = B\varphi(a) = I_n$. En appliquant ensuite $\sigma \in G$, on obtient $\varphi(a)\sigma \cdot B = \sigma \cdot B\varphi(a) = I_n$ et par unicité de l'inverse, on en tire $\forall \sigma \in G, \sigma \cdot B = B$ soit $B \in ({}_aM_n(K))^G$ ce qui signifie que B est l'image d'un élément de A, qui est donc l'inverse de a dans A. □

4.3 Groupe de Brauer d'un corps C_1

Proposition 4.8. *Le groupe de Brauer d'un corps C_1 est réduit à $\{0\}$.*

Démonstration. Soit D une algèbre à division centrale sur un corps k qui est C_1, et soit n son degré. Considérons $v_1, \ldots, v_{n^2}$ une k-base de D, alors $\mathrm{Nrd}(x_1v_1 + \cdots + x_{n^2}v_{n^2}) = f(x_1, \ldots, x_{n^2})$ est un polynôme homogène de degré n en n^2 variables. Par conséquent, si $n > 1$, il possède un zéro non-trivial, ce qui contredit la proposition 4.7. On a alors $n = 1$ et donc il n'existe, à isomorphisme près, que k comme algèbre à division centrale sur k, ce qui signifie, d'après la remarque 4.2.1 que $\mathrm{Br}(k) = \{0\}$. □

Remarque 4.8.1. Nous avons montré qu'il n'existe pas d'algèbres à division finies et centrale sur un corps C_1, ce résultat s'étend aux algèbres dont le centre n'est pas réduit à k dans la mesure où le centre d'une telle algèbre est une extension algébrique (car finie) de k qui est donc aussi C_1

Signalons qu'il existe des corps dont le groupe de Brauer est réduit à $\{0\}$ et qui ne sont pas C_1.

Corollaire 4.9 (Petit théorème de Wedderburn). *Les algèbres à division finies sont des corps.*

Démonstration. Soit D une algèbre à division finie, alors D est centrale sur son centre $Z(D)$, qui est un corps, fini donc C_1 par le théorème de Chevalley et donc par la proposition 4.8 $D \simeq Z(D)$, qui est un corps. □

Nous terminerons donc avec ce résultat qui paraît anecdotique, mais qui montre la puissance de la théorie que nous avons développée dans cette dernière partie. Nous avons dégagé quelques propriétés des corps C_i, notamment l'existence de zéros simultanés pour des polynômes homogènes sous certaines conditions, aux conséquences sur les polynômes non nécessairement homogènes, en ne quittant l'optique de généralisation de la notion de corps algébriquement clos. Nous avons, après quelques exemples, étudié la conservation des propriétés de type C_i lors du passage à une extension, ou d'un corps de constantes à un corps de fractions rationnelles. Nous avons ensuite examiné les algèbres simples centrales, et notamment leur propriétés de déploiement, pour ensuite construire le groupe de Brauer qui classifie les algèbres à division centrales sur un corps (et déployées par une extension). Après la construction de la norme réduite, déjà évoquée au début, nous avons pu montrer que le groupe de Brauer d'un corps C_1 est nul, généralisant ainsi la propriété de non-existence d'extension algébrique stricte pour un corps algébriquement clos.

Références

[1] Serge Lang, *On quasi algebraic closures*, Annals of Mathematics, vol. 55, n°2, mars 1952.

[2] Phillipe Gille, Tamàs Szamuely, *Central simple algebras and Galois cohomology*, `http://www.renyi.hu/~szamuely/publ.html`.

[3] Jean-Pierre Serre, *Corps locaux*, Hermann, 1968.