L'ARITHMÉTIQUE des ALGÈBRES de QUATERNIONS

par

Jacques Martinet

Laboratoire A2X
Université Bordeaux 1
et
E.P.F.L

Lausanne
Avril 2002

L'arithmétique des algèbres de quaternions.

Ce texte rend compte de trois cours que j'ai donnés les 12, 19, et 26 avril 2002 à l'École Polytechnique Fédérale de Lausanne à la demande d'Eva Bayer. Il s'agissait d'expliquer en trois heures l'essentiel de ce que l'on sait sur la structure et sur l'ensemble des classes d'idéaux (à gauche) des corps de quaternions sur un corps de nombres.

Comme le lecteur le constatera à la lecture des paragraphes 11 et 13, seuls certains corps de quaternions se distinguent dans la catégorie de toutes les algèbres centrales simples. Mieux, on obtient des énoncés unifiés en associant à un corps de quaternions H l'algèbre $\mathcal{M}_2(H)$ des matrices 2×2 sur H. Pour ces raisons, j'ai préféré ne pas me limiter aux algèbres de quaternions, qui ne sont rien d'autre que les algèbres simples de rang 4 sur leur centre.

Vu le temps dont je disposais, il ne m'a pas été possible de donner des démonstrations ; tout au plus ai-je pu en esquisser quelques unes. La bibliographie commentée qui termine cette rédaction signale quelques ouvrages dans lesquels le lecteur pourra les lire. L'exposé oral a été enrichi de quelques exemples et du § 9'.

Je remercie Christian Maire pour ses remarques qui m'ont permis d'améliorer ce texte au fur et à mesure de sa rédaction, et Boas Erez pour la relecture détaillée qu'il en a faite.

Le texte présenté ici est une transcription en LaTeX de mai 2013 de la version d'origine en AmSTeX. J'ai profité de cette nouvelle édition pour corriger quelques fautes de style et ajouter la référence [Bo'] en dernière page.

Arithmétique des algèbres de quaternions, I

§ 1. Quaternions. Soit K un corps de caractéristique différente de 2, et soient a, $b \in K^*$. L'*algèbre de quaternions d'invariants a et b* est l'unique algèbre associative sur K ayant une base $(1, i, j, k)$ vérifiant les relations

$$i^2 = a,\ j^2 = b,\ ij = -ji = k\,.$$

On a alors en particulier $k^2 = -ab$. L'exemple historique, dû à Hamilton, est celui où $K = \mathbb{R}$ et $a = b = -1$, d'où $k^2 = -1$. On parle alors de *quaternions usuels*, quel que soit le corps de base K considéré. Hurwitz les a étudiés lorsque $K = \mathbb{Q}$, et a introduit l'*ordre de Hurwitz* $\mathfrak{O}$, anneau de base

$$(1, i, j, \omega) \quad \text{où} \quad \omega = \frac{-1 + i + j + k}{2}$$

sur $\mathbb{Z}$, sur lequel nous reviendrons.

[Pour être complet, signalons la définition en caractéristique 2 : on prend $a \in K$, $b \in K^*$, et les relations sont $i^2 = i + a$, $j^2 = b$, $ij = k$, $ji = k + j$, d'où $k^2 = ab$.]

§ 2. Algèbres simples et notions voisines. Soit K un corps. Une K-algèbre L (associative, de dimension finie) est dite *simple* si ses seuls idéaux bilatères sont $\{0\}$ et L, *semi-simple* si elle ne contient pas d'idéaux nilpotents non nuls, *centrale* si son centre est K. On montre en considérant les idéaux (à gauche) minimaux qu'une algèbre simple est isomorphe à une algèbre $\mathcal{M}_m(D)$ où D est un corps gauche de centre $C \supset K$, bien défini à isomorphisme près (ainsi que l'entier m) par L, et qu'une algèbre semi-simple est produit direct d'algèbres simples : $L = \prod_{i=1}^{r} L_i$. Lorsque les centres C_i des L_i sont des extensions séparables de K, on dit que L est une algèbre *séparable*.

L'arithmétique dans une telle algèbre s'étudie suivant quatre rubriques.

$\boxed{a}$ Structures des algèbres (semi-) simples sur un corps K arbitraire.

$\boxed{b}$ Arithmétique dans une algèbre séparable relativement à un anneau de Dedekind A de corps des fractions K.

$\boxed{c}$ Situation $\boxed{a}$ lorsque K est un corps local ou global, en pratique un corps de nombres ou l'un de ses complétés (théorie de Hasse).

$\boxed{d}$ Situation $\boxed{b}$ lorsque K est un corps global (théorie de Eichler).

Compléments sur les algèbres simples.
• Si L est centrale simple sur K, quelle que soit l'extension K' de K, la K'-algèbre étendue $L_{K'} = K' \otimes L$ est encore centrale simple. Le produit tensoriel de deux algèbres *centrales* simples est encore central simple. (Ces propriétés de stabilité entraînent les propriétés analogues pour les algèbres séparables.)
• Soit $\overline{K}$ une clôture algébrique de K. Comme $\overline{K} \otimes L$ ne peut être qu'une algèbre de matrices, le rang $[L : K]$ d'une algèbre centrale simple est un carré, soit m^2.
• Soit D un corps gauche de centre K, de rang m^2 sur K. Alors, tout sous-corps (commutatif) de D est contenu dans un *sous-corps commutatif maximal de* D, et un tel sous corps est de degré m sur K. En outre, il en existe qui sont séparables sur K.
• Soit L/K centrale simple. Pour $x \in L$, le polynôme caractéristique d'une matrice représentant x dans $\overline{K} \otimes L$ est à coefficients dans K, et ne dépend que de x. C'est le *polynôme caractéristique réduit de* x. Il est lié au polynôme caractéristique non réduit de x (celui de $y \mapsto xy$) par la relation $\chi_x(X) = \chi_{red,x}(X)^m$.
• Écrivons $\chi_{red,x}(X) = X^m - a_1 X^{m-1} + \cdots + (-1)^m a_m$. Le coefficient a_1 (resp. a_m) est la *trace réduite* (resp. la *norme réduite*) *de* x. Notations : $\mathrm{Trd}(x)$, $\mathrm{Nrd}(x)$.
• Dans une algèbre centrale simple, la forme bilinéaire $(x, y) \mapsto \mathrm{Trd}(xy)$ est non-dégénérée.
• Pour tout $x \in D$, et tout sous-corps commutatif maximal M de D contenant x, on a $\chi_{red,x} = \chi_{M/K,x}$, et en particulier $\mathrm{Trd}(x) = \mathrm{Tr}_{M/K}(x)$ et $\mathrm{Nrd}(x) = \mathrm{N}_{M/K}(x)$.
• Théorème de Skolem-Noether. Soit L/K une algèbre centrale simple, soit M une sous-algèbre simple de L, et soit $\sigma : M \to N \subset L$ un isomorphisme d'algèbres. Alors, σ est la restriction à M d'un automorphisme intérieur de L.

§ 3. Application aux algèbres de quaternions. Les notations sont celles du § 1.

D'abord, trace et norme réduites ont une interprétation simple en termes d'involution. Décrivons-la dans le cas où $\mathrm{Car}\, K \neq 2$. Pour $q = x + yi + zj + tk$, on pose $\bar{q} = x - yi - zj - tk$. L'application $q \mapsto \bar{q}$ est une *involution* (i.e., on a $\overline{q + q'} = \bar{q} + \bar{q}'$, $\overline{qq'} = \bar{q}'\bar{q}$, et $\bar{\lambda} = \lambda$ pour $\lambda \in K$). On a alors :

$$\mathrm{Trd}(q) = q + \bar{q} = 2x\,,\ \mathrm{Nrd}(q) = q\,\bar{q} = x^2 - ay^2 - bz^2 + abt^2\,,$$
$$\chi_{red,q}(X) = (X - q)\,(X - \bar{q}) = X^2 - \mathrm{Trd}(q)X + \mathrm{Nrd}(q)\,.$$

Remarque. La forme K-bilinéaire $(q, q') \mapsto \mathrm{Trd}(qq')$ a pour forme quadratique associée $q \mapsto 2\,\mathrm{Nrd}(q)$.

Le théorème de Skolem-Noether explique la raison d'être de la définition quelque peu artificielle d'une algèbre de quaternions. On vérifie facilement qu'une algèbre de quaternions est centrale simple.
Réciproquement :

Théorème. *Toute algèbre centrale simple de rang* 4 *est une algèbre de quaternions.*

Démonstration. Limitons-nous au cas d'un corps gauche H/K. Soit $M \subset H$ un sous-corps de degré 2, séparable sur K. Si $\mathrm{Car}\, K \neq 2$ (resp. si $\mathrm{Car}\, K = 2$), on peut écrire $M = K(i)$ où i est racine d'une équation de Kummer $X^2 - a = 0$ (resp. d'Artin-Schreier $X^2 - X - a = 0$). La conjugaison $i \mapsto -i$ (resp. $i \mapsto i + 1$) de $\mathrm{Gal}(M/K)$ est de la forme $i \mapsto jij^{-1}$. Mais $b = j^2$ commute avec i et j, donc est dans K, et la fin de la démonstration est alors immédiate.
[Le cas d'une algèbre de matrices relève d'un calcul explicite. Par exemple, si $\mathrm{Car}\, K \neq 2$, on peut prendre $i = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ et $j = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.] □

Les quaternions pour lesquels $x = 0$ (ceux qui sont dans le noyau de la trace réduite) sont appelés *quaternions purs*. Ils constituent un sous-espace vectoriel de dimension 3 de H, que nous notons V, supplémentaire orthogonal de K pour la forme $\mathrm{Trd}(q\bar{q}')$. On vérifie sans peine que l'on a $q^2 \in K$ si et seulement si $q \in K$ ou q est pur, et que *lorsque H est un corps*, l'égalité $q^2 = q'^2$ avec $q \in K$ et q' pur n'est possible que si $q = q' = 0$.

§ 4. Considérations géométriques. Soit H un corps de quaternions, muni ainsi que son sous-espace V des quaternions purs de la forme $\mathrm{Trd}(q\bar{q}')$. Pour tout $q \in H^*$, l'application $h \mapsto qhq^{-1}$ est une isométrie de H comme de V. On en déduit des homomorphismes de H^*/K^* dans les groupes orthogonaux $\mathrm{SO}(V)$ et $\mathrm{SO}(H)$. Le premier est surjectif (utiliser le fait que la réflexion le long de q est $h \mapsto -q\bar{h}\bar{q}^{-1}$).

Dans le cas des quaternions de Hamilton (sur $\mathbb{R}$), c'est la construction classique du revêtement universel $\mathrm{Spin}_3(\mathbb{R}) \simeq S^3 \to \mathrm{SO}_3(R)$.
[On peut de même construire $\mathrm{Spin}_4(\mathbb{R})$ à partir de $(q, r) \mapsto (h \mapsto qhr^{-1})$.]

On sait (voir par exemple H. Zassenhaus, *The theory of groups*) que les sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$ sont isomorphes à l'un des groupes suivants (qui sont uniques à conjugaison près) : le groupe cyclique C_n d'ordre n ($\forall n \geq 1$), le groupe diédral D_n d'ordre $2n$ ($\forall n \geq 2$), ou l'un des trois groupes A_4, S_4, A_5, d'ordres respectifs 12, 24, 60. (Ces trois

groupes sont associés aux polyèdres réguliers ; les groupes diédraux correspondent aux polygones réguliers.) Par relèvement dans la sphère S^3 identifiée au groupe des quaternions de norme 1, on obtient les groupes cycliques C_{2n}, les groupes quaternioniens H_{4n} d'ordre $4n \geq 8$, et trois groupes spéciaux $\widehat{A}_4$, $\widehat{S}_4$, $\widehat{A}_5$, d'ordres respectifs 24, 48, 120.
• Dans $\mathbb{R}(i) \simeq \mathbb{C}$, une racine de l'unité ζ d'ordre m engendre un groupe cyclique C_m.
• Soit $\zeta \in \mathbb{R}(i)$ d'ordre $2m$. Le groupe $\langle \zeta, j \rangle$ est quaternionien d'ordre $4m$. (On a $j\zeta j^{-1} = \bar{\zeta} = \zeta^{-1}$.) Le corps gauche $\mathbb{Q}(\zeta, j)$ est un corps de quaternions de centre $\mathbb{Q}(\zeta + \zeta^{-1})$, le sous-corps réel maximal de $\mathbb{Q}(\zeta)$; on obtient des quaternions sur $\mathbb{Q}$ si et seulement si $m = 2$ ou $m = 3$.
• À conjugaison près, on a les inclusions $\widehat{A}_4 \supset H_8$, $\widehat{S}_4 \supset \widehat{A}_4$, et $\widehat{A}_5 \supset \widehat{A}_4$.
• Le groupe $\widehat{A}_4$ s'obtient comme groupe des éléments inversibles de l'ordre de Hurwitz ; ses 24 éléments sont 1, -1 (d'ordre 2), $\pm i, \pm j, \pm k$ (d'ordre 4), $\frac{-1 \pm i \pm j \pm k}{2}$ (d'ordre 3), et $\frac{1 \pm i \pm j \pm k}{2}$ (d'ordre 6).
• On construit $\widehat{S}_4$ sur $\mathbb{Q}(\sqrt{2})$ comme groupe des élément inversibles de norme réduite 1 de l'anneau de base

$$(1, \frac{1+i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \omega = \frac{-1+i+j+k}{2})$$

sur $\mathbb{Z}[\sqrt{2}]$. On a $\widehat{S}_4 = \widehat{A}_4 \cup \frac{1+i}{\sqrt{2}} \widehat{A}_4$, et $\widehat{S}_4 \smallsetminus \widehat{A}_4$ contient 12 éléments de chacun des ordres 4 et 8.
• Finalement, soit $\tau = \frac{1+\sqrt{5}}{2}$. Le groupe $\widehat{A}_5$ est engendré par $\widehat{A}_4$ et $i + \tau j + \tau^{-1} k$. Les éléments de $\widehat{A}_5 \smallsetminus \widehat{A}_4$ sont d'ordre 5 ou 10.

§ 5. Ordres maximaux et discriminant. Étant donnés un anneau intègre, de corps des fractions K, et une K-algèbre L, un *ordre de A dans L* est un sous-anneau $\mathfrak{O}$ de L, qui est un A-module de rang $n = [L : K]$ dont les éléments sont entiers sur A. Si A est noethérien et intégralement clos, il revient au même de dire que $\mathfrak{O}$ est un anneau qui est un A-module de type fini et de rang n. On construit facilement des ordres par le procédé suivant : on part d'une base $(e_1 = 1, e_2, \ldots, e_n)$ de L sur K, et l'on prouve l'existence d'un $d \in A \smallsetminus \{0\}$ tel que $(e_1, de_2, \ldots, de_n)$ est une base d'un ordre.

Soit $L = \prod_{i=1}^{r} L_i$ semi-simple de facteurs simples L_i ayant pour centres C_i. La *trace réduite* est définie par

$$\mathrm{Trd}_{L/K} = \sum_i \mathrm{Tr}_{C_i/K} \circ \mathrm{Trd}_{L_i/C_i} \ .$$

Si $x \in L$ est entier sur A, alors $\mathrm{Trd}(x) \in K$ est aussi entier sur A.

À partir de maintenant, on suppose que L est séparable et que A est un anneau de Dedekind.

La forme bilinéaire $(x, y) \mapsto \mathrm{Trd}(xy)$ est non-dégénérée, ce qui permet d'associer à tout sous-A-module M de L de rang n son *dual*

$$M^\sharp = \{x \in L \mid \forall\, y \in M,\, \mathrm{Trd}(xy) \in A\}\,.$$

Dans le cas d'un ordre $\mathfrak{O}$, on a $\mathfrak{O}^\sharp \supset \mathfrak{O}$, et

$$\mathfrak{O} \subset \mathfrak{O}' \implies \mathfrak{O} \subset \mathfrak{O}' \subset \mathfrak{O}'^\sharp \subset \mathfrak{O}^\sharp\,,$$

ce qui prouve que tout ordre est contenu dans un *ordre maximal* (pour l'inclusion).

Étant donné un ordre $\mathfrak{O}$, son dual $\mathfrak{O}^\sharp$ est un $\mathfrak{O}$-module à gauche et à droite, la *codifférente de* $\mathfrak{O}$. Son inverse (dans un sens à définir, et sous réserve d'existence) est un idéal bilatère de $\mathfrak{O}$, la *différente*, notée $\mathcal{D}_\mathfrak{O}$.

Relativement à un ordre $\mathfrak{O}$, on a une notion naturelle d'*idéal fractionnaire* à gauche, à droite, ou bilatère : c'est un sous-$\mathfrak{O}$-module de L de type fini et de rang n ; un point de vue ne faisant pas référence à un ordre particulier sera donné plus loin.
Exemple : la codifférente et la différente sont des idéaux fractionnaires bilatères.

Du fait que la forme $\mathrm{Trd}(xy)$ est non-dégénérée, on a une notion de *discriminant réduit* d'abord pour une base de L/K (le déterminant $\det(\mathrm{Trd}(e_i e_j))$, puis pour un module de rang n. Cela se fait en utilisant des arguments locaux standards, ou en adaptant les méthodes utilisées par Serre dans le chapitre III de *Corps locaux*.

Arithmétique des algèbres de quaternions, II

§ 6. Idéaux inversibles. Les notations sont celles du § 5. Convenons d'appeler *idéal fractionnaire dans L* tout sous-A-module I de L de rang n. (Autrement dit, $K \otimes_A I$ est libre de rang 1 sur L.) Un tel module possède des ordres à gauche et à droite

$$\mathfrak{O}_g(I) = \{x \in L \mid xI \subset I\} \quad \text{et} \quad \mathfrak{O}_d(I) = \{x \in L \mid Ix \subset I\}\,.$$

Il est clair que I est un idéal fractionnaire à gauche au sens précédent pour un ordre $\mathfrak{O}$ si et seulement si $\mathfrak{O}_g(I) \supset \mathfrak{O}$. Alors, tout élément de $\mathfrak{O}_d(I)$ définit un $\mathfrak{O}$-endomorphisme de I, ce qui identifie $\mathrm{End}_{\mathfrak{O}}(I)$ à $\mathfrak{O}_d(I)^\circ$ (anneau opposé à $\mathfrak{O}_d(I)$). On peut multiplier les idéaux fractionnaires par $I\,J = \{\sum x_i y_i \mid x \in I,\, y \in J\}$.

Toutefois, sauf mention expresse du contraire, on n'effectuera un tel produit que lorsque $\mathfrak{O}_d(I) = \mathfrak{O}_g(J)$.

Soit $\mathfrak{O}$ un ordre, et soit I un idéal fractionnaire à gauche de $\mathfrak{O}$ (i.e., on a $\mathfrak{O} \subset \mathfrak{O}_g(I)$). On pose

$$I' = \{x \in L \mid Ix \subset \mathfrak{O}\}\,;$$

c'est un idéal à droite pour $\mathfrak{O}$ et à gauche pour $\mathfrak{O}_d(I)$, II' est un idéal bilatère de $\mathfrak{O}$, et $I'I$ est un idéal bilatère de $\mathfrak{O}_d(I)$ (on a $I\,(I'I) = (II')\,I \subset \mathfrak{O}I = I$, donc $I'I \subset \mathfrak{O}_d(I)$). On dit que I est *inversible* si $I'I = \mathfrak{O}_d(I)$. Exemple: un idéal fractionnaire *principal*, c'est-à-dire de la forme $I = \mathfrak{O}\,x$, est inversible. En effet,

$$I' = x^{-1}\mathfrak{O}\,,\ \mathfrak{O}_d(I) = x^{-1}\mathfrak{O}x\,,\ \text{ et }\ I'I = x^{-1}\mathfrak{O}\cdot\mathfrak{O}x = x^{-1}\mathfrak{O}x\,.$$

On peut caractériser les idéaux inversibles comme étant les idéaux projectifs. Leur structure peut être très compliquée. Les choses se simplifient dans le cas des ordres maximaux, dont de nombreuses propriétés les rapprochent des anneaux de Dedekind.

§ 7. Le groupoïde Brandt. Une étude des corps gauches sur les corps complets permet de montrer qu'un idéal fractionnaire à gauche sur un ordre maximal $\mathfrak{O}$ est localement libre, c'est-à-dire que $A_{\mathfrak{p}} \otimes I$ est libre sur $A_{\mathfrak{p}} \otimes \mathfrak{O}$ pour tout idéal premier $\mathfrak{p}$ de A ; en particulier, les idéaux fractionnaires des ordres maximaux sont inversibles. (N.B. $A_{\mathfrak{p}}$ désigne l'anneau local de A en $\mathfrak{p}$, non son complété.)

Comme le fait pour un ordre d'être maximal est une propriété de nature locale, cela entraîne que l'ordre à gauche d'un idéal fractionnaire est maximal si et seulement si son ordre à droite l'est (on parle alors d'*idéal normal*), et que les ordres maximaux sont localement conjugués.

Définition. On dit que deux idéaux à gauche I et J sur un même ordre maximal $\mathfrak{O}$ sont *équivalents* s'il existe $x \in L^*$ tel que $J = I\,x$; il revient au même de dire que ce sont des $\mathfrak{O}$-modules isomorphes. On dit que deux ordres maximaux sont du même *type* s'ils sont conjugués. On note h le nombre de classes à gauche de $\mathfrak{O}$, et t le nombre de types d'ordres maximaux de L. L'*idéal de distance* de deux ordres maximaux $\mathfrak{O}_1$ et $\mathfrak{O}_2$ est $\delta(\mathfrak{O}_1, \mathfrak{O}_2) = (\mathfrak{O}_2\,\mathfrak{O}_1)^{-1}$ (inverse par rapport à $\mathfrak{O}_1$ ou à $\mathfrak{O}_2$). [N.B. La finitude de h est vraie lorsque K est un corps de nombres. On ne s'en occupe pas ici. L'énoncé suivant a un sens même si la finitude n'est pas assurée.]

Théorème. Le nombre h ne dépend pas de $\mathfrak{O}$. C'est aussi le nombre de classes à droite de $\mathfrak{O}$, et l'on a $t \leq h$.

Démonstration. Si $\mathfrak{O}_1$ et $\mathfrak{O}_2$ sont deux ordres maximaux d'idéal de distance δ, l'application $J \mapsto \delta J$ met en bijection les classes à gauche de $\mathfrak{O}_2$ avec celles de $\mathfrak{O}_1$. En outre, pour tout ordre maximal $\mathfrak{O}$, l'application $I \mapsto I'$ met en bijection la classe à gauche de I avec la classe à droite de $\mathfrak{O}_d(I)$. Cela démontre les deux assertions relatives à h.

Si $\mathfrak{O}$ et $\mathfrak{O}'$ sont deux ordres maximaux, il existe des idéaux à gauche I de $\mathfrak{O}$ tels que $\mathfrak{O}_d(I) = \mathfrak{O}'$, par exemple leur idéal de distance. Comme $\mathfrak{O}_d(Ix) = x^{-1}\mathfrak{O}_d(I)x$, l'ensemble des images des idéaux de la classe de I est la classe de conjugaison de $\mathfrak{O}'$. On construit ainsi une surjection de l'ensemble des classes à gauche de $\mathfrak{O}$ sur l'ensemble des types d'ordres de L. □

Voici un exemple avec deux types d'ordres. Soit H l'algèbre des quaternions usuels sur $K = \mathbb{Q}(\sqrt{3})$. L'ordre de Hurwitz étendu à $\mathbb{Z}[\sqrt{3}]$ se plonge dans un ordre maximal $\mathfrak{M}_1$, dont le groupe U_1 des unités de norme réduite 1 contient le groupe $\widehat{A}_4$, et lui est en fait égal, car on doit exclure les groupes $\widehat{S}_4$ et $\widehat{A}_5$, vu que ni 2 ni 5 ne sont des carrés dans K. Comme K est le sous-corps réel maximal de $\mathbb{Q}(\zeta_{12})$, il existe un ordre maximal $\mathfrak{M}_2$ dont le groupe des unités de norme 1 est H_{24}. Il y a donc au moins deux types d'ordres maximaux dans H. (On peut montrer que l'on a $h = 2$, donc aussi $t = 2$, cf. partie III.)

La multiplication des idéaux normaux dans L est une loi associative, mais non partout définie, pour laquelle les «éléments unités» sont les ordres maximaux (un de chaque côté pour chaque idéal) et telle que

tout élément a un inverse à gauche et un inverse à droite. C'est le *groupoïde Brandt*.

Soit $\mathfrak{O}$ un ordre maximal. On dit qu'un $\mathfrak{O}$-module à gauche M est de rang r si $K\otimes_A M$ est libre de rang r sur L. Un tel module est isomorphe à une somme directe de r idéaux fractionnaires ($M \simeq I_1 \bigoplus \ldots \bigoplus I_r$), et l'on peut même réduire une telle somme sous la forme $M \simeq \mathfrak{O}^{r-1} \bigoplus I$. Toutefois, l'analogie avec la théorie des anneaux de Dedekind s'arrête là : il existe des cas dans lesquels deux idéaux I, J non isomorphes sont *stablement isomorphes*, c'est à dire tels que $\mathfrak{O}^{r-1} \bigoplus I$ et $\mathfrak{O}^{r-1} \bigoplus J$ sont isomorphes pour un $r > 1$ (ou pour $r = 1$, cela revient au même, cf. partie III). Autrement dit, on ne peut pas toujours *simplifier*.

Dans le cas d'un anneau de Dedekind, deux modules stablements isomorphes sont isomorphes (et la classe de I tel que $M \simeq A^{r-1} \bigoplus I$ est un invariant, appelé *classe de Steinitz de* M), mais cela se démontre en utilisant la théorie des déterminants, qui n'existe que sur les anneaux commutatifs.

§ 8. Corps gauches sur un corps complet. On suppose que A possède un unique idéal premier $\mathfrak{p}$ et qu'il est complet pour la valeur absolue $\mathfrak{p}$-adique. Soit D un corps gauche de centre K. Muni de n'importe quelle norme de K-espace vectoriel, D est complet.
Théorème. Soit m^2 le rang de D sur son centre.

(1) Le corps gauche D possède un unique ordre maximal $\mathfrak{O}$.
(2) $\mathfrak{O}$ contient un unique idéal maximal à gauche $\mathfrak{P}$, qui est bilatère et aussi maximal en tant qu'idéal à droite.
(3) Les idéaux fractionnaires de D sont bilatères, et ce sont les puissances $\mathfrak{P}^k$, $k \in \mathbb{Z}$ de $\mathfrak{P}$.
(4) $\mathfrak{O}/\mathfrak{P}$ est un corps gauche.

En outre, si le corps résiduel $A/\mathfrak{p}$ de K est fini, l'indice de ramification de $\mathfrak{P}$ et son degré résiduel sont tous deux égaux à m, i.e., on a

$$\mathfrak{p}\mathfrak{O} = \mathfrak{P}^m \quad \text{et} \quad [\mathfrak{O}/\mathfrak{P} : A/\mathfrak{p}] = m\,,$$

la différente de D est $\mathfrak{P}^{m-1}$ («une algèbre simple est modérément ramifiée sur son centre»), et son discriminant est donc égal à $\mathfrak{p}^{m(m-1)}$.

Revenons à la situation globale. Pour tout idéal $\mathfrak{p}$ de A, considérons les complétés $\widehat{A}_\mathfrak{p}$ de A et $\widehat{K}_\mathfrak{p}$ de K. Si L est une K-algèbre centrale simple, sa complétée $\widehat{L}_\mathfrak{p}$ en $\mathfrak{p}$ est isomorphe à $\widehat{K}_\mathfrak{p}\otimes_K L$. On a des isomorphismes

$$L \simeq \mathcal{M}_r(D),\ \widehat{L}_\mathfrak{p} \simeq \mathcal{M}_{r_\mathfrak{p}}(D(\mathfrak{p})),\ \text{ et }\ \widehat{D}_\mathfrak{p} \simeq \mathcal{M}_{s_\mathfrak{p}}(D(\mathfrak{p}))$$

où $D(\mathfrak{p})$ est un corps gauche de centre $\widehat{K}_\mathfrak{p}$, les rangs des diverses algèbres vérifiant (avec des notations évidentes) les relations $m = s_\mathfrak{p} m_\mathfrak{p}$ et $r\,m = r_\mathfrak{p} m_\mathfrak{p}$. Il existe une notion d'*idéal premier* (bilatère) rendant les services habituels. Dans ce cadre, la notion de ramification de $\mathfrak{p}$ dans L se traduit par le fait que l'on ait $m_\mathfrak{p} > 1$. Comme dans le cas commutatif, les idéaux premiers ramifiés sont exactement ceux qui divisent le discriminant réduit.

À côté des corps locaux du type $\widehat{K}_\mathfrak{p}$ comme ci-dessus, on doit aussi considérer les places v infinies, pour lesquelles $\widehat{K}_v$ est isomorphe à $\mathbb{R}$ ou à $\mathbb{C}$. Pour v complexe (resp. réelle), l'algèbre complétée est isomorphe à une algèbre $\mathcal{M}_r(\mathbb{C})$ (resp. $\mathcal{M}_r(\mathbb{R})$ ou $\mathcal{M}_r(\mathbb{H})$). Dans ce dernier cas, on dit que v est *ramifiée*.

§ 9. Résultats locaux et globaux. Le but de ce § est de donner la classification des corps gauches sur les extensions finies d'un corps p-adique $\mathbb{Q}_p$ (y compris sur $\mathbb{Q}_\infty = \mathbb{R}$), puis sur un corps de nombres.

Les corps gauches de centre un corps K de degré fini sur $\mathbb{Q}_p$ sont décrits à isomorphisme près par un invariant dans le groupe de torsion $\mathbb{Q}/\mathbb{Z}$. À un corps gauche D de rang m^2 correspond $\alpha \in \mathbb{Q}/\mathbb{Z}$ d'ordre m, de sorte qu'il y a exactement $\varphi(m)$ corps gauches de centre K et de rang m^2 sur K, cf. *infra*, § 9'. Pour toute extension K'/K finie, si $K' \otimes_K D$ est une algèbre de matrices sur un corps gauche D', l'invariant α' de D' est $[K' : K]\,\alpha$.

Sur $\mathbb{R}$, l'invariant α est à valeurs dans le sous-groupe $\{0, \frac{1}{2}\}$ de $\mathbb{Q}/\mathbb{Z}$ (0 pour $\mathbb{R}$, $\frac{1}{2}$ pour $\mathbb{H}$) ; sur $\mathbb{C}$, l'invariant α est nul.

Cas des corps de quaternions. Il y a dans chaque cas (sauf si $K = \mathbb{C}$) un unique corps de quaternions. La norme réduite correspond à l'unique classe de formes quadratiques quaternaires qui ne représente pas 0 sur K.

Lorsque p est impair, on peut le construire ainsi : on choisit un générateur π de $\mathfrak{p}$ et $a \in A \smallsetminus \mathfrak{p}$ qui n'est pas un carré modulo $\mathfrak{p}$, et l'algèbre $H_{a,\pi}$ convient. En effet, l'équation $\mathrm{Nrd}(q) = 0$ s'écrit $x^2 - ay^2 - \pi z^2 + a\pi t^2 = 0$, et l'on peut supposer que x, y, z, t ne sont pas tous divisibles par π. Elle entraîne $x^2 - ay^2 \equiv 0 \mod \mathfrak{p}$, donc $x \equiv y \equiv 0 \mod \mathfrak{p}$, puis $z \equiv t \equiv 0 \mod \mathfrak{p}$ en raisonnant modulo $\mathfrak{p}^2$, en contradiction avec l'hypothèse.

Lorsque $p = 2$, il faut travailler modulo $4\,\mathfrak{p}$. Lorsque le degré $[K : \mathbb{Q}_2]$ est impair, le corps des quaternions usuels convient.

Soit maintenant K un corps de nombres. À un corps gauche D, et à tout complété K_v de K, on associe l'invariant α_v de $D(v)$ tel que $\widehat{D}_v \simeq \mathcal{M}_{r_v}(D(v))$.

Théorème. Les classes d'isomorphismes de corps gauches de centre K sont en bijection avec les systèmes d'invariants locaux vérifiant les conditions suivantes :

(1) $\alpha_v = 0$ pour presque tout v.
(2) $\alpha_v = 0$ si v est complexe.
(3) $\alpha_v = 0$ ou $\alpha_v = \frac{1}{2}$ si v est réelle.
(4) $\sum_v \alpha_v = 0$

En outre, le corps gauche D correspondant à un système d'invariants α_v comme ci-dessus a pour rang m^2, où m est le PPCM des ordres des α_v.

[La condition (4) est connue sous le nom de «loi de réciprocité de Hasse». C'est une traduction dans le langage des algèbres simples de la loi de réciprocité d'Artin de la théorie du corps de classes.]

Cas des corps de quaternions. La loi de réciprocité de Hasse signifie simplement que le nombre de places ramifiées (y compris les places réelles ramifiées) doit être *pair*. Le discriminant est le carré $\mathfrak{d}^2$ d'un produit d'idéaux premiers distincts. Lorsque l'on se donne un tel produit, ainsi que le comportement des places réelles de façon que soit respectée la règle de parité, écrire le corps de quaternions sous la forme $H_{a,b}$ n'a rien évident.

Par exemple, il existe pour tout p premier un unique corps de quaternions H_p de centre $\mathbb{Q}$ ramifié exactement en p et ∞. La dernière condition équivaut à ce que H_p soit défini par des relations $i^2 = -a$ et $j^2 = -b$ avec a, $b > 0$. Le discriminant de H_p est p^2, celui de la base $(1, i, j, k)$ est $(4ab)^2$. Il faut donc faire en sorte que p divise $2ab$. Voici une recette de construction de H_p :

• Si $p = 2$, prendre $a = -1$ et $b = -1$ (ou $b = -2$) ; H_2 est le corps «usuel».
• Si $p \equiv 3 \mod 4$, prendre $a = -1$ et $b = -p$.
• Si $p \equiv 5 \mod 8$, prendre $a = -2$ et $b = -p$.
• Si $p \equiv 1 \mod 8$, prendre $a = q \equiv 7 \mod 8$ premier et $b = -p$ tel que $\left(\frac{q}{p}\right) = -1$.

[Justification dans le dernier cas : la forme $x^2 + pz^2$ (resp. $x^2 + qy^2$) représente 0 sur $\mathbb{Q}_q$ parce que $\left(\frac{-p}{q}\right) = +1$ (resp. sur $\mathbb{Q}_2$ parce que $-q \equiv +1 \mod 8$). L'ensemble des places ramifiées, que l'on sait être contenu dans $\{2, p, q, \infty\}$, est réduit à $\{p, \infty\}$ ou est vide, et ce dernier cas est exclu vu que la place infinie se ramifie.]

Pour être complet, il faudrait encore déterminer un ordre maximal, en modifiant la base $(1, i, j, k)$ par l'introduction de dénominateurs de façon à obtenir la bonne valeur du discriminant. Voici une possibilité pour chacun des trois premiers exemples :
• Dans le cas de H_2, on remplace k par $\omega = \frac{-1+i+j+k}{2}$; on obtient l'ordre de Hurwitz.
• Dans le cas de H_p, $p \equiv 3 \mod 4$, on remplace j par $\omega = \frac{-1+j}{2}$ et k par $\omega' = i\omega$. (On a $\omega'^2 = -1$.)
• Dans le cas de H_p, $p \equiv 5 \mod 8$, on remplace i par $\omega = \frac{i+k}{2}$ et j par $\omega' = \frac{1+i+j}{2}$.

On vérifie dans chaque cas que les produits deux à deux des éléments des nouvelles bases s'expriment sur ces bases, ce qui montre que l'on a bien défini des ordres. Le fait qu'ils soient maximaux résulte du calcul de leur discriminant, évident à partir de l'indice de l'ordre de base $(1, i, j, k)$.

Voici un exemple concernant les corps quadratiques réels. Il existe un unique corps de quaternions H ramifié aux deux places infinies de K et à aucune place finie. On peut le construire ainsi : on choisit un nombre premier p qui est inerte ou ramifié dans K ; alors, $H = K \otimes_{\mathbb{Q}} H_p$. [En effet, le degré local en p est égal à 2, donc l'extension des scalaires de $\mathbb{Q}$ à K «tue» la ramification en p ; variante globale : H n'est pas ramifié en-dehors de p, ∞_1, ∞_2 et l'est aux places infinies.]

§ 9'. Construction de l'invariant local. Avant d'entrer dans le vif du sujet, signalons que le fait que $\mathbb{Q}/\mathbb{Z}$ soit un groupe s'interprète en termes de *groupe de Brauer*. En fait, quel que soit le corps K, on multiplie les classes d'isomorphismes de corps gauches de centre K en posant $[D_1]\,[D_2] = [D']$ si $D_1 \otimes_K D_2 \simeq \mathcal{M}_r(D')$. C'est là une loi commutative et associative, pour laquelle $[K]$ est élément neutre, et l'inverse de $[D]$ est la classe du corps gauche opposé D°. Le groupe ainsi construit est le *groupe de Brauer de* K, noté $\mathrm{Br}(K)$.

Étant donnée une extension L/K, on note $\mathrm{Br}(L/K)$ le sous-groupe de $\mathrm{Br}(K)$ formé des classes de corps gauches *neutralisés* par L (c'est-à-dire tels que $L \otimes_K D$ soit une algèbre de matrices). Lorsque L/K est galoisienne finie de groupe G, on peut identifier $\mathrm{Br}(L/K)$ au groupe de cohomologie $H^2(G, L^*)$. Lorsque G est cyclique, les calculs sont très simples. C'est cette remarque que l'on va utiliser dans le cas local.

Soit donc K un corps complet pour une valuation discrète v, d'anneau de valuation A et d'idéal maximal $\mathfrak{p}$, à corps résiduel k fini avec q éléments. Rappelons qu'une clôture algébrique $\overline{K}$ de K contient pour tout n une unique extension non ramifiée L de degré n de K. Soit π un

générateur de $\mathfrak{p}$. C'est aussi un générateur de l'idéal maximal $\mathfrak{P}$ de L. Le choix de π identifie K^* au produit direct $\mathbb{Z} \times U_K$ (tout $x \in K^*$ s'écrit $x = \pi^{v(x)}\, u$ avec $u \in U_K = A \smallsetminus \mathfrak{p}$), et de même L^* à $\mathbb{Z} \times U_L$. Le groupe $\mathrm{Gal}(L/K)$ s'identifie canoniquement au groupe de Galois de l'extension résiduelle ℓ/k, lequel possède un générateur canonique, la *substitution de Frobenius* $x \mapsto x^q$. On note σ l'élément correspondant de $G = \mathrm{Gal}(L/K)$.

Soit D un corps gauche de centre K, de rang m^2 sur K. On commence par montrer que D contient un sous-corps commutatif maximal L non ramifié sur K (voir par exemple *Corps Locaux*, ch. XII). Le théorème de Skolem-Noether montre qu'il existe $e \in D^*$ tel que quel $\forall\, x \in L$, $\sigma\, x = exe^{-1}$. L'indépendance linéaire des éléments $1, \sigma, \ldots, \sigma^{m-1}$ de G montre que $1, e, \ldots, e^{m-1}$ sont indépendants sur L, et forment donc une base d'espace vectoriel de D sur L (opérant sur D par multiplication à gauche). Soit $a = e^m$. Comme a commute avec les éléments de L et les puissances de e, c'est un élément de K^* (et m est le plus petit entier tel que e^m soit dans K). Le choix de e est unique au produit près par un élément $x \in L$. On a $(xe)^2 = xexe^{-1}e^2 = (x\sigma x)\, e^2$, $(xe)^3 = (x\sigma x\sigma^2 x)\, e^3$, …, et finalement

$$(xe)^m = (x\sigma x \ldots \sigma^{m-1}x)e^m = \mathrm{N}_{L/K}(x)\, a\,.$$

Ainsi, on a associé à L un élément canonique $\bar{a} \in K^*/\,\mathrm{N}(L^*)$, et le théorème de Skolem-Noether montre que le résultat ne dépend pas du choix de $L \subset D$.

Il n'y a plus qu'à calculer des normes dans L/K. On a $\mathrm{N}(\pi) = \pi^m$ et $\mathrm{N}(U_L) = U_K$ (parce que L/K est non ramifiée ; c'est essentiellement une application du lemme de Hensel), et l'on peut ainsi identifier la norme à l'application $z \mapsto mz$ de $\mathbb{Z}$ dans $\mathbb{Z}$ par une identification indépendante du choix de π. On termine en identifiant $\mathbb{Z}/m\mathbb{Z}$ au sous-groupe $(\frac{1}{m}\,\mathbb{Z})/\mathbb{Z}$ de $\mathbb{Q}/\mathbb{Z}$, *quod erat demonstrandum.* (Et pour être tout à fait complet, on passe à la limite sur les extensions non ramifiées, obtenant $\mathbb{Q}/\mathbb{Z}$ comme réunion de ses sous-groupe $(\frac{1}{m}\,\mathbb{Z})/\mathbb{Z}$.)

La méthode de Hasse pour traiter le cas global repose aussi sur le fait qu'un corps gauche de centre un corps de nombres K possède un sous-corps commutatif maximal L qui est une extension cyclique de K, et sur le «théorème des normes de Hasse», qui affirme que dans une extension L/K cyclique, tout $x \in K^*$ qui est une norme dans toutes les extensions locales $\widehat{L}_{\mathfrak{P}}/\widehat{K}_{\mathfrak{p}}$ est une norme dans L/K.

Arithmétique des algèbres de quaternions, III

§ 10. Compléments sur la norme réduite. Soit L une algèbre centrale simple sur un corps K et soit $\mathfrak{O}$ un ordre maximal de L relativement à un anneau de Dedekind A de corps des fractions K. On définit la *norme réduite* d'un idéal fractionnaire (à gauche) I de $\mathfrak{O}$ comme étant l'idéal engendré par les normes réduites de ses éléments. C'est un idéal fractionnaire de K. Ses composantes locales sont les normes réduites des générateurs de ses localisés. La formule $\mathrm{Nrd}(IJ) = \mathrm{Nrd}(I)\,\mathrm{Nrd}(J)$ est vraie chaque fois que $\mathfrak{O}_d(I) = \mathfrak{O}_g(J)$. Par passages aux quotients, on obtient une application de l'ensemble des classes à gauche de $\mathfrak{O}$ dans le groupe des classes de A.

Étant donnés des idéaux fractionnaires $I_1, \ldots, I_r$, on associe à leur somme directe l'idéal I de $\mathcal{M}_r(L)$ formé des matrices dont la k-ième colonne est constituée d'éléments arbitraires de I_k. Dans l'algèbre $\mathcal{M}_r(L)$, on a $\mathrm{Nrd}(I) = \prod_{k=1}^{r} \mathrm{Nrd}(I_k)$.

Soit K un corps local. Si K est une extension finie d'un corps $\mathbb{Q}_p$ ou si $K = \mathbb{C}$, on a $\mathrm{Nrd}(L^*) = K^*$. Si $K = \mathbb{R}$, il y a deux possibilités : on a $\mathrm{Nrd}(L^*) = \mathbb{R}^*$ si L est une algèbre de matrices sur $\mathbb{R}$, et $\mathrm{Nrd}(L^*) = \mathbb{R}^*_{>0}$ si L est une algèbre de matrices sur $\mathbb{H}$. (Observer que $\mathcal{M}_r(\mathbb{H})$ est connexe par arcs.)

Soit maintenant K un corps de nombres. Rappelons qu'une place infinie $v : K \to \mathbb{C}$ est *ramifiée* dans L si elle est réelle, et si la norme réduite est positive en v. Il revient au même de dire que $\widehat{L}_v$ est de type $\mathcal{M}_r(\mathbb{H})$. On dit que l'algèbre L est *totalement définie* si toutes les places infinies de K se ramifient dans L.

Nous allons maintenant préciser la notion de norme réduite sur les classes. Rappelons qu'étant donné un ensemble S de places infinies de K, on définit le groupe Cl_A^S des classes d'idéaux de K (relativement à A) *au sens restreint pour* S comme le quotient du groupe I_A des idéaux fractionnaires de A par son sous-groupe P_A^S des idéaux principaux possédant un générateur positif à toutes les places réelles de S. On écrit Cl_A^+ (ou Cl_K^+) si $S = S_\infty$. À l'algèbre L, on associe le groupe Cl_A^S où S est l'ensemble des places infinies de K qui sont ramifiées dans L. La norme réduite induit une application de l'ensemble des classes de $\mathfrak{O}$ dans Cl_A^S.

§ 11. La condition d'Eichler. Sous forme restreinte, il s'agit d'une notion relative à une algèbre centrale simple sur un corps de nombres K, utilisée lorsque $A = \mathbb{Z}_K$:

L n'est pas un corps de quaternions totalement défini.

Soit S un ensemble fini de places de K contenant S_∞. À chaque place finie v de K, on associe la valuation $v_\mathfrak{p}$ de l'idéal premier correspondant. Soit alors

$$A_S = \{x \in K \mid \forall\, v \notin S,\, v_\mathfrak{p}(x) \geq 0\}\,.$$

(L'anneau des entiers $\mathbb{Z}_K$ de K correspond au cas où $S = S_\infty$.) La *condition d'Eichler relative à L et à un sous-anneau A de K de la forme A_S* est :

(CE) *$[L : K] > 4$, ou S contient une place qui ne se ramifie pas dans L.*

Il est clair que (CE) se réduit à la première condition lorsque $A = \mathbb{Z}_K$.

Théorème. *Soit $\mathfrak{O}$ un ordre maximal. Si (CE) est satisfaite, la norme réduite induit une bijection de l'ensemble des classes à gauche de $\mathfrak{O}$ sur l'ensemble Cl_A^S. En outre, le nombre t de types d'ordres divise h, le quotient étant le nombre de classes de $\mathfrak{O}$ représentées par des idéaux bilatères.*

La démonstration repose sur un *théorème d'approximation forte*, cas particulier d'un énoncé de Kneser s'appliquant à tous les groupes algébriques semi-simples simplement connexes, découvert par Eichler dans le cas des algèbres simples (avec $A = \mathbb{Z}_K$), qui l'a énoncé sous la forme suivante :
Si (CE) est satisfaite, tout élément de A est norme réduite d'un quaternion entier *sur A.*

Voici une première application du théorème d'Eichler. Disons que deux $\mathfrak{O}$-modules M et M' de type fini sans A-torsion sont *stablement isomorphes* s'il existe $k > 0$ tel que $\mathfrak{O}^k \bigoplus M \simeq \mathfrak{O}^k \bigoplus M'$.

Théorème. *Deux $\mathfrak{O}$-modules M et M' sont stablement isomorphes si et seulement si $\mathfrak{O} \bigoplus M \simeq \mathfrak{O} \bigoplus M'$. Si M et M' sont de rang $r \geq 2$, ou si le couple (L, A) vérifie (CE), deux sous-modules stablement isomorphes sont isomorphes.*

Démonstration. On écrit M et M' comme sommes directes $\mathfrak{O}^{r-1} \bigoplus I$ et $\mathfrak{O}^{r-1} \bigoplus I'$ où I et I' sont des idéaux fractionnaires. Par hypothèse, il existe $t \geq r$ tel que $\mathfrak{O}^{t-1} \bigoplus I \simeq \mathfrak{O}^{t-1} \bigoplus I'$. Comme la norme réduite sur les classes est la même pour toutes les algèbres $\mathcal{M}_t(L)$, et que (CE) est vérifiée pour tout $t \geq 2$, on a $\mathfrak{O} \bigoplus I \simeq \mathfrak{O} \bigoplus I'$, et même $I \simeq I'$ si L elle-même vérifie (CE). □

Lorsque L vérifie la condition d'Eichler, on peut transporter la structure de groupe de Cl_A^S à l'ensemble des classes de $\mathfrak{O}$. Le théorème ci-dessous va nous permettre en particulier d'expliciter cette structure de groupe.

Appelons *classes stables* les classes d'équivalence pour la relation suivante entre idéaux fractionnaires :

$$I \sim_s I' \iff \exists\, k > 0,\ \mathfrak{O}^k \bigoplus I \simeq \mathfrak{O}^k \bigoplus I' \iff \mathfrak{O} \bigoplus I \simeq \mathfrak{O} \bigoplus I'\,.$$

Étant donnés I_1 et I_2, la classe *stable* d'un idéal J tel que $I_1 \bigoplus I_2 \simeq \mathfrak{O} \bigoplus J$ est bien définie. On munit ainsi l'ensemble des classes stables d'une structure de groupe, dont l'élément neutre est la classe des idéaux *I stablement libres*, c'est-à-dire tels que $\mathfrak{O} \bigoplus I \simeq \mathfrak{O} \bigoplus \mathfrak{O}$. Ce groupe s'appelle le *groupe des classes de* $\mathfrak{O}$ ou *de* L, et se note Cl_L lorsqu'il n'y a pas d'ambiguité sur A. Le théorème précédent entraîne tout de suite :

Théorème. *Pour toute algèbre centrale simple L, la norme réduite induit un isomorphisme de Cl_L sur Cl_A^S, S désignant l'ensemble des places réelles de K ramifiées dans L.*

Il reste à calculer le nombre de classes des algèbres qui ne vérifient pas la condition d'Eichler. Des méthodes analytiques vont permettre d'effectuer ce calcul.

§ 12. Fonctions zêta. On définit la fonction zêta d'une algèbre simple L par la formule habituelle

$$\zeta_L(s) = \sum_{I \subset \mathfrak{O}} \frac{1}{\mathrm{Nrd}(I)^s}\,,$$

la somme étant étendue aux idéaux fractionnaires entier d'un ordre $\mathfrak{O}$ donné. La série converge pour $\Re(s) > 1$, et l'on a un produit eulérien $\zeta_L(s) = \prod_{\mathfrak{p}} \zeta_{L,\mathfrak{p}}(s)$ étendu aux idéaux premiers du centre. Posons $[L : K] = m^2$. Alors, la fonction zêta de L s'exprime en fonction de celle du centre par une formule de la forme

$$\zeta_L(s) = \prod_{i=0}^{m-1} \zeta_K(ns - i) \prod_{\mathfrak{p} \mid \mathfrak{d}(L/K)} \varphi_{\mathfrak{p}}(s)\,,$$

les termes $\varphi_{\mathfrak{p}}$ étant eux-mêmes des produits $\prod_{\mathfrak{p}} \left(1 - \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^{\alpha s + \beta}\right)^{\pm 1}$.

Dans le cas où L est une algèbre de quaternions H, notons $\mathfrak{d}$ le produit des idéaux premiers de K ramifiés dans H. La fonction zêta s'écrit alors simplement

$$\zeta_H(s) = \zeta_K(2s)\,\zeta_K(2s-1) \prod_{\mathfrak{p} \mid \mathfrak{d}(H/K)} (1 - \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})^s)$$

(on «débarasse» partiellement ζ_K de ses facteurs locaux aux places ramifiées).

On a besoin de considérer plus généralement les fonctions zêta partielles $\zeta_{L,c}$ obtenues en sommant sur les idéaux d'une classe c. On a $\zeta_L = \sum_c \zeta_{L,c}$. Contrairement à ce qui se passe dans le cas commutatif, le résidu de $\zeta_{L,c}$ en $s = 1$ peut maintenant dépendre de c. Ce résidu se calcule à l'aide d'un résidu en $s = 1$ et de valeurs en 2. En utilisant l'équation fonctionnelle de Hecke, qui relie $\zeta_K(s)$ et $\zeta_K(1-s)$, on se ramène à considérer des valeurs en 0 et -1.

§ 13. Une formule de masse. On considère maintenant une algèbre de quaternions totalement définie, de centre K (totalement réel). Les ordres maximaux que l'on considère sont relatifs à la clôture intégrale $\mathbb{Z}_K$ de $\mathbb{Z}$ dans K. L'énoncé ci-dessous, facile à démontrer, met en évidence une analogie entre corps de quaternions totalement définis et *corps de type C.M.* (extensions quadratiques totalement imaginaires d'un corps de nombres totalement réel). Les notations sont les suivantes : n est le degré de K, U_K est le groupe $\mathbb{Z}_K^*$ des unités de K (isomorphe à $\{\pm 1\} \times \mathbb{Z}^{n-1}$), $\mathfrak{O}$ est un ordre maximal de H, $U_{\mathfrak{O}}$ est le groupe des unités de $\mathfrak{O}$, et $\mu_{\mathfrak{O}}$ le sous-groupe de $U_{\mathfrak{O}}$ des unités de norme réduite 1. C'est un groupe fini, isomorphe à un sous-groupe fini de la sphère $S^3 \subset \mathbb{H}^*$.

Proposition. U_K est d'indice fini dans $U_{\mathfrak{O}}$. Plus précisément,

$$[U_{\mathfrak{O}} : \mu_{\mathfrak{O}}\, U_K] = 1,\ 2,\ \text{ou } 4\,.$$

[Dans le cas C.M., cet «indice de Hasse» vaut 1 ou 2.]

On considère maintenant des représentants $I_1, \ldots, I_h$ des idéaux à gauche de $\mathfrak{O}$, et l'on pose

$$\mathfrak{O}_k = \mathfrak{O}_d(I_k) \quad \text{et} \quad w_k = [U_{\mathfrak{O}_k} : \mu_{\mathfrak{O}_k}\, U_K]\,.$$

En évaluant les résidus des fonctions zêta partielles, on montre la formule suivante (comme dans le cas des corps abéliens de type C.M., les régulateurs disparaissent des formules) :

Théorème. (Eichler)

$$\sum_{k=1}^{h} \frac{1}{w_k} = \frac{1}{2^{n-1}}\, h_K\, \zeta_K(-1) \prod_{\mathfrak{p}\mid\mathfrak{d}} \big(1 - \mathrm{N}(\mathfrak{p})\big)\,.$$

[Noter que cette formule prouve que la fonction zêta au point -1 d'un corps de nombres totalement réel est un nombre rationnel non nul ; Siegel a montré que ce résultat s'étend à tous les entiers négatifs impairs.]

Examinons de plus près le cas où $K = \mathbb{Q}$, en notant d_H le produit des nombres premiers (en nombre impair) ramifiés dans H. On a $n = 1$, $U_K = \{\pm 1\}$, donc $w_k = \frac{|U_{f\mathfrak{O}_k}|}{2}$, $\zeta_{\mathbb{Q}}(-1) = -\frac{1}{12}$ (Euler !?), $h_{\mathbb{Q}} = 1$, et la formule se réduit à

$$\sum_{\mathfrak{O}} \frac{1}{|U_{\mathfrak{O}}|} = \frac{1}{24} \prod_{p|d_H} (p-1)\,.$$

On en déduit que $h = 1$ n'est possible que pour $d \leq 13$, donc $d \in \{2, 3, 5, 7, 11, 13\}$, et l'on doit exclure $d = 11$, valeur pour laquelle le membre de droite n'est pas l'inverse d'un entier. On vérifie en examinant les groupes susceptibles d'être des groupes d'unités que l'on a $h = 1$ si $p = 2$, 3, 5, 7 ou 13, les groupes $U_{\mathfrak{O}}$ étant isomorphes respectivement à $\widehat{A}_4$, H_{12}, C_6, C_4 et C_2. En revanche, la formule pour $p = 11$ ne peut être que $\dfrac{1}{|U_{\mathfrak{O}_1}|} + \dfrac{1}{|U_{\mathfrak{O}_2}|} = \dfrac{5}{12}$, mettant en évidence deux classes, associées aux groupes C_6 et C_4, et donc aussi deux types d'ordres.

Pour K quadratique de discriminant $d = 5$, 8 et 12, les valeurs respectives de $\zeta_K(-1)$ sont $\frac{1}{30}$, $\frac{1}{12}$ et $\frac{1}{6}$. Pour les algèbres non ramifiées en-dehors de l'infini, on trouve une classe dans chacun des deux premiers cas, avec groupe d'unité de norme réduite 1 isomorphe à $\widehat{A}_5$ (resp. à $\widehat{S}_4$). Dans le cas $d = 12$, on a vu qu'il y a au moins deux classes et deux types d'ordres. En fait, on a $h_K = 1$, mais $h_K^+ = 2$ (l'unité fondamentale est $\varepsilon = 2 + \sqrt{3}$, de norme $+1$), ce qui donne une autre preuve de la minoration $h \geq 2$. La formule de masse se réduit à $\frac{1}{12} + \frac{1}{12} = \frac{1}{6}$, d'où $h = t = 2$.

§ 14. Compléments.

14.1. Eichler a donné en 1955 des formules explicites pour le nombre de classes. Voici son résultat lorsque $K = \mathbb{Q}$, en écartant les cas singuliers $d_H = 2$ et $d_H = 3$. Les groupes d'unités sont alors cycliques d'ordre $2i = 2$, 4 ou 6, ce qui permet d'écrire $h = h_1 + h_2 + h_3$, h_i désignant le nombre de classes dont l'ordre à droite possède $2i$ unités. On a alors

$$h_2 = \frac{1}{2} \prod_{p|d_H} \left(1 - \left(\tfrac{-4}{p}\right)\right),\ h_3 = \frac{1}{2} \prod_{p|d_H} \left(1 - \left(\tfrac{-3}{p}\right)\right), \tag{1}$$

et

$$h = \frac{1}{12} \prod_{p|d_H} (p-1) + \frac{1}{2}\, h_2 + \frac{2}{3}\, h_3\,. \tag{2}$$

14.2. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de caractéristique p. Le groupe des points d'ordre p sur $\overline{\mathbb{F}}_q$ est alors d'ordre

p (cas *ordinaire*) ou est réduit à $\{0\}$ (cas *super-singulier*). Dans le premier cas, l'anneau des endomorphismes de E est un ordre d'un corps quadratique imaginaire. Dans le second cas, c'est un ordre maximal du corps de quaternions ramifié en p et l'infini. La formule du nombre de classes donne alors le nombre de courbes super-singulières. Une démonstration directe de ce résultat a été donnée par Igusa.

14.3. Soit à nouveau H une algèbre de quaternions totalement définie. Le cardinal de l'ensemble des classes stables est égal à h_K^+. La formule de masse montre que le nombre de classes tend vers l'infini avec le produit $\mathfrak{d}$ des places ramifiées dans H. Il en résulte que pour K donné, les ensembles de classes et de classes stables ne sont égaux que pour un nombre fini d'algèbres de quaternions (autrement dit, en général, la *simplification* n'est pas possible). M.-F. Vignéras a démontré beaucoup plus :

Théorème. La simplification n'est possible que pour un nombre fini de corps de quaternions totalement définis.

La démonstration se fait en majorant les discriminants d_K des corps K pour lesquels la simplification est possible. En utilisant les minorations des discriminants (issues de la géométrie des nombres) qui étaient connues lors de la rédaction de son travail, elle a en particulier prouvé la majoration $[K : \mathbb{Q}] \leq 33$. Elle a également classé toutes les algèbres posibles de centre un corps quadratique ou cubique cyclique. (Nous l'avons fait au § précédent dans le cas de $\mathbb{Q}$.) Or, postérieurement à la rédaction de son article, l'utilisation de méthodes analytiques a conduit à d'importants progrès sur les minorations des discriminants. Il serait intéressant de reprendre le problème de la simplification en tenant compte de ces nouvelles minorations. Peut-être est-il même possible d'obtenir la classification complète des algèbres à simplification.

.../...

Quelques références

La référence fondamentale est l'ouvrage

[De] Max Deuring, *Algebren*, Julius Springer, 1935,
dont il existe une édition anglaise. Il traite de tous les points abordés dans ce cours (y compris les fonctions zêta), à l'exception de la rubrique $\boxed{d}$, dont les résultats sont postérieurs à 1935.

Le livre

[Re] Irving Reiner, *Maximal orders*, Academic Press, 1975
contient tout ce qui est algébrique, mais laisse de côté le contenu des §§ 12 et 13 (la partie analytique de la théorie) ainsi que la théorie des modules.

Pour $\boxed{a}$ on peut aussi consulter

[Bo] Nicolas Bourbaki, *Algèbre, chapitre VIII*, Hermann, Paris, 1972,
dont la notice historique donne une bonne idée de l'évolution de la théorie, depuis les années 1900 aux États-Unis (Peirce, Wedderburn, ...) juqu'à l'Allemagne des années 1930 (E. Artin, R. Brauer, H. Hasse, E. Noether, ...), noms auxquels il convient d'adjoindre Th. Skolem et A. Albert, et mieux (mai 2013), la nouvelle édition refondue et étendue **[Bo']**, même titre, 2012, chez Springer.

Les résultats de $\boxed{b}$ ont été développés entre les deux guerres par H. Brandt, C. Chevalley et H. Hasse, et complétés en 1960 par M. Auslander et O. Goldman.

La théorie de $\boxed{c}$, essentiellement équivalente à la *théorie du corps de classes* qui décrit les extensions abéliennes d'un corps de nombres en termes du corps de base, est très largement l'œuvre de Hasse. Pour un exposé (très) formel, voir

[We], André Weil, *Basic Number Theory*, Springer, Heidelberg, 1967.

Les résultats de $\boxed{d}$ sont essentiellement dus à Martin Eichler (travaux de 1936–1938 et de 1955). Richard Swan et Marie-France Vigéras en ont modernisé la présentation. On doit à Swan de nombreux résultats sur les algèbres des groupes finis (notamment, le fait remarquable que sur un anneau de Dedekind A de caractéristique zéro, les modules projectifs de type fini sont localement libres dès lors que leur rang est défini, et il l'est lorsque les diviseurs premiers de l'ordre du groupe ne sont pas inversibles), ainsi que divers compléments concernant les groupes de type quaternioniens, et à Vignéras diverses variantes utiles des formules d'Eichler.

Pour la théorie de $\boxed{d}$, le livre de référence est

[Vi], Marie-France Vignéras, *Arithmétique des Algèbres de Quaternions*, Springer, Lecture Notes n° 800, 1980.