SÉMINAIRE N. BOURBAKI

ROGER GODEMENT

# Les fonctions ζ des algèbres simples, I

*Séminaire N. Bourbaki*, 1960, exp. n° 171, p. 27-49

<http://www.numdam.org/item?id=SB_1958-1960__5__27_0>

Séminaire BOURBAKI
(Décembre 1958)

# LES FONCTIONS $\zeta$ DES ALGÈBRES SIMPLES, I.

par Roger GODEMENT

On sait, depuis HECKE, attacher à tout corps de nombres algébriques des séries de Dirichlet à équation fonctionnelle, séries dont les propriétés analytiques (résidu en $s = 1$ par exemple) traduisent certaines propriétés arithmétiques des corps considérés. Comme on peut aussi considérer un corps de nombres comme une algèbre simple commutative sur le corps des rationnels, on a cherché après HECKE à attacher de même des fonctions $\zeta$ aux algèbres simples non commutatives sur le corps des rationnels ; les résultats classiques dans cette voie sont dûs à K. HEY dont la Dissertation (Hambourg, 1929) est résumée au chapitre VII, paragraphe 8 de l'ouvrage classique de DEURING [1].

La théorie de HECKE a fait l'objet récemment d'un exposé beaucoup plus beau dû à J. TATE [3], exposé basé sur l'analyse harmonique dans le groupe des idèles d'un corps de nombres. En utilisant un article récent de G. FUJISAKI [2], on se propose dans cet exposé et le suivant d'étendre la méthode de TATE (qu'il faudrait aussi, sans doute, attribuer également à IWASAWA) au cas non commutatif.

Dans ce premier exposé on se bornera à traiter des préliminaires arithmétiques indispensables, la partie "analytique" devant être étudiée dans le second exposé.

## 1. La théorie élémentaire des réseaux.

Dans ce numéro on se donne une fois pour toutes un anneau de Dedekind $A$ dont on désigne le corps des fractions par $K$.

(1.1). - Soit $L$ un espace vectoriel de dimension finie sur $K$. On appelle réseau de $L$ (ou même $A$-réseau si l'on veut préciser $A$) toute partie $\mathfrak{o}$ de $L$ qui est un sous-$A$-module de type fini de $L$ et qui contient une base de $L$ sur $K$, ce qui veut dire que tout $x \in L$ a un multiple non nul dans $\mathfrak{o}$, ou encore que l'homomorphisme évident $K \otimes_A \mathfrak{o} \to L$ est bijectif. Si $A$ est principal, $\mathfrak{o}$ est libre.

(1.2). - Si $\mathfrak{o}'$ et $\mathfrak{o}''$ sont des réseaux de $L$ il en est de même de $\mathfrak{o}' + \mathfrak{o}''$ et de $\mathfrak{o}' \cap \mathfrak{o}''$ ; si $\mathfrak{o}$ est un réseau de $L$, alors $\mathfrak{o} \cap L'$ est un réseau de $L'$ pour tout sous-espace $L'$ de $L$ ; si $\mathfrak{o}'$ et $\mathfrak{o}''$ sont des réseaux

dans $L'$ et $L''$, alors les $u \in L = \mathrm{Hom}_K(L', L'')$ tels que $u(\mathfrak{a}') \subset \mathfrak{a}''$ forment un réseau de $L$ ; enfin l'image d'un réseau par un homomorphisme surjectif est un réseau. Ces propriétés triviales résultent du fait que $A$ est noethérien.

(1.3). - Soient $\mathfrak{a}$ un réseau d'un vectoriel $L$, et $\mathfrak{a}^*$ l'ensemble des $u \in L^*$, dual de $L$, tels que $u(\mathfrak{a}) \subset A$ ; alors $\mathfrak{a}^*$ est un réseau de $L^*$ d'après (1.2), et, comme $A$-module, s'identifie canoniquement au dual du $A$-module $\mathfrak{a}$ d'après (1.1). Vu la théorie des modules sans torsion de type fini sur un anneau de Dedekind on en déduit qu'inversement

$$\mathfrak{a} = (\mathfrak{a}^*)^*$$

modulo l'isomorphisme de bidualité pour $L$. Une démonstration élémentaire (qui ne diffère d'ailleurs pas de la démonstration "supérieure") s'obtient en se ramenant, par "localisation" - voir ci-dessous - au cas trivial d'un anneau de base principal.

(1.4). - Soit $\mathfrak{p}$ un idéal premier non nul (i. e. maximal) de $A$, et remplaçons $A$ par l'anneau de fractions $A_{\mathfrak{p}} \subset K$, qui est local et principal. Pour tout $A$-réseau $\mathfrak{a}$ d'un vectoriel $L$ sur $K$, le localisé

$$\mathfrak{a}_{\mathfrak{p}} = A_{\mathfrak{p}} \underset{A}{\otimes} \mathfrak{a}$$

du $a$-module $\mathfrak{a}$ s'identifie canoniquement au sous-$A_{\mathfrak{p}}$-module de $L$ engendré par $\mathfrak{a}$, ce que nous écrirons

$$\mathfrak{a}_{\mathfrak{p}} = A_{\mathfrak{p}} \cdot \mathfrak{a} \quad .$$

On vérifie alors que l'application $\mathfrak{a} \longrightarrow \mathfrak{a}_{\mathfrak{p}}$ envoie l'ensemble des $A$-réseaux de $L$ sur l'ensemble des $A_{\mathfrak{p}}$-réseaux de $L$ (en effet un réseau pour $A_{\mathfrak{p}}$ est engendré par une base de $L$ sur $K$, donc s'obtient en localisant le $A$-réseau engendré par la même base). De plus la localisation $\mathfrak{a} \longrightarrow \mathfrak{a}_{\mathfrak{p}}$ est compatible avec toutes les opérations sur les réseaux définies en (1.2) et (1.3). Il est bien connu enfin (et ceci n'a rien à voir avec les anneaux de Dedekind...) que l'on a

$$\mathfrak{a} = \bigcap_{\mathfrak{p}} \mathfrak{a}_{\mathfrak{p}}$$

pour tout $A$-réseau $\mathfrak{a}$ de $L$.

(1.5). - Cette propriété montre qu'un $A$-réseau de $L$ est déterminé par la donnée de ses localisés $\mathfrak{a}_{\mathfrak{p}}$ ; il y a plus : il existe toujours un $A$-réseau $\mathfrak{b}$ dont les localisés sont donnés d'avance, pourvu que ceux-ci coïncident pour presque tout $\mathfrak{p}$ avec les localisés d'un $A$-réseau donné. La démonstration, élémentaire, repose

sur le théorème d'approximation dans les anneaux de Dedekind (existence d'un élément de $K$ ayant des "parties polaires" données en un nombre fini de "places" données de $A$).

(1.6). - Considérons toujours $A$ , $K$ , $L$ , comme ci-dessus, et un idéal premier $\mathfrak{p}$ de $A$ . On sait que $A_{\mathfrak{p}}$ est l'anneau d'une valuation discrète normée $v_{\mathfrak{p}}$ du corps $K$ , ce qui permet d'introduire le complété $\hat{K}_{\mathfrak{p}}$ de $K$ relativement à cette valuation, laquelle se prolonge d'ailleurs au corps $\hat{K}_{\mathfrak{p}}$ . En identifiant $L$ à $K^n$ à l'aide d'une base de $L$ , on déduit de la topologie $\mathfrak{p}$-adique de $K$ une topologie (dite encore $\mathfrak{p}$-adique) sur $L$ , indépendante évidemment du choix de la base. Le complété de $L$ pour cette topologie s'identifie canoniquement à

$$\hat{L}_{\mathfrak{p}} = \hat{K}_{\mathfrak{p}} \underset{K}{\otimes} L$$

muni de l'unique topologie qui en fait un espace vectoriel topologique (E. V. T.) sur $\hat{K}_{\mathfrak{p}}$ . Tout cela est bien connu, et d'ailleurs immédiat.

(1.7). - Soit alors $\mathfrak{a}$ un $A$-réseau dans $L$ et soit $\hat{A}_{\mathfrak{p}}$ l'anneau des entiers de $\hat{K}_{\mathfrak{p}}$ , qui est local et principal. Alors l'adhérence de $\mathfrak{a}$ dans $\hat{L}_{\mathfrak{p}}$ n'est autre que

$$\hat{\mathfrak{a}}_{\mathfrak{p}} = \hat{A}_{\mathfrak{p}} \cdot \mathfrak{a} = \hat{A}_{\mathfrak{p}} \underset{A}{\otimes} \mathfrak{a} \quad ,$$

et c'est un $\hat{A}_{\mathfrak{p}}$ -réseau de $\hat{L}_{\mathfrak{p}}$ ; on a en outre la relation

$$\hat{\mathfrak{a}}_{\mathfrak{p}} \cap L = \mathfrak{a}_{\mathfrak{p}} \quad .$$

Ces propriétés résultent essentiellement des propriétés de "platitude" du complété d'un anneau de valuation discrète (ou plus généralement d'un "anneau de ZARISKI").

(1.8). - On déduit de là que le passage d'un $A_{\mathfrak{p}}$ -réseau de $L$ à son complété est une bijection de l'ensemble des réseaux de $L$ (pour $A_{\mathfrak{p}}$ ) sur l'ensemble des $\hat{A}_{\mathfrak{p}}$ -réseaux de $\hat{L}_{\mathfrak{p}}$ , bijection compatible avec les opérations algébriques définies en (1.2) et (1.3). Ceci permet de transformer (1.5) en un énoncé où les localisés $\mathfrak{b}_{\mathfrak{p}}$ sont remplacés par les complétés $\hat{\mathfrak{b}}_{\mathfrak{p}}$ , résultat fort utile.

2. Ordres maximaux d'une algèbre semi-simple.

Pour éviter des difficultés (d'ailleurs peu sérieuses) on suppose maintenant que $K$ est de caractéristique 0 , et on va s'intéresser aux algèbres $L$ de dimension finie sur $K$ ; on les supposera semi-simples, ce qui veut dire que, sur une telle

algèbre, la forme bilinéaire $\mathrm{Tr}_{L/K}(xy)$ est non dégénérée (il s'agit ici de la trace usuelle, calculée dans la représentation régulière) ; on sait qu'alors L reste semi-simple par toute extension du corps de base.

(2.1). - Si $\mathfrak{a}'$ et $\mathfrak{a}''$ sont des réseaux de L, il en est de même de $\mathfrak{a}'\mathfrak{a}''$ (sous-groupe engendré par les produits $x'x''$, avec $x' \in \mathfrak{a}'$ et $x'' \in \mathfrak{a}''$) ; de même les $x \in L$ tels que $x.\mathfrak{a}' \subset \mathfrak{a}''$ (resp. $\mathfrak{a}'x \subset \mathfrak{a}''$) forment un réseau ; en particulier, on appelle inverse d'un réseau $\mathfrak{a}$ le réseau $\mathfrak{a}^{-1}$ (la terminologie et la notation adoptées ici sont parfois justifiées ...) formé des $x \in L$ tels que $\mathfrak{a}.x.\mathfrak{a} \subset \mathfrak{a}$ ; enfin on appelle complémentaire d'un réseau $\mathfrak{a}$ de L le réseau $\tilde{\mathfrak{a}}$ formé des $x \in L$ tels que

$$\mathrm{Tr}(xy) \in A \quad \text{pour tout} \quad y \in \mathfrak{a} \quad ;$$

le résultat énoncé en (1.3) donne immédiatement la relation

$$\tilde{\tilde{\mathfrak{a}}} = \mathfrak{a}$$

pour tout réseau de L.

(2.2). - On appelle ordre de L tout réseau B de L tel que l'on ait

$$A \subset B \quad , \quad B.B \subset B \quad ;$$

par exemple, pour tout réseau $\mathfrak{a}$ les $x \in L$ tels que $x.\mathfrak{a} \subset \mathfrak{a}$ forment un ordre.

(2.3). - Soit B un ordre de L ; pour tout $x \in B$, l'anneau $A[x]$ est contenu dans B, donc est un A-module de type fini, de sorte que tout $x \in B$ est entier sur A. Inversement, soit B un sous-anneau de L, contenant A, formé d'entiers sur A, et contenant une base $(x_i)$ de L sur K ; pour tout $x \in B$ les éléments $x_i x$ sont entiers sur A, donc leurs traces sont dans A, et par suite B est contenu dans le complémentaire du réseau engendré par les $x_i$ : ainsi B est un A-module de type fini, donc un ordre. Ce résultat implique immédiatement (Zorn) que tout ordre de L est contenu dans un ordre maximal.

Si L est commutative, il y a un seul ordre maximal : l'ensemble de tous les entiers de L ; il n'en est plus de même dans le cas non commutatif (sauf - cf. ci-dessous - si L est une algèbre à division et si A est l'anneau d'une valuation complète).

(2.4). - Soit B un ordre de L ; alors pour tout idéal premier $\mathfrak{p}$ de A il

est clair que $\hat{B}_{\mathfrak{p}}$ est un ordre de l'algèbre $\hat{L}_{\mathfrak{p}}$ relativement à l'anneau de base $\hat{A}_{\mathfrak{p}}$ ; et ceci caractérise les ordres parmi les réseaux de L . Comme on peut, d'après (1.8), modifier un nombre fini de composantes $\hat{B}_{\mathfrak{p}}$ de B , on en déduit que l'ordre B est maximal si et seulement si l'ordre $\hat{B}_{\mathfrak{p}}$ est maximal pour tout $\mathfrak{p}$ .

(2.5). - Soit B un ordre maximal de L ; on appelle B-réseau ("zweiseitige ideal" dans DEURING) tout A-réseau $\mathfrak{a}$ tel que $B.\mathfrak{a}.B \subset \mathfrak{a}$ . Comme B est maximal on voit alors trivialement que

$$x \in B \Leftrightarrow x.\mathfrak{a} \subset \mathfrak{a} \Leftrightarrow \mathfrak{a}.x \subset \mathfrak{a}$$

(car les x vérifiant la seconde, ou la troisième propriété, forment un ordre contenant B), et on déduit de là que

$$x \in \mathfrak{a}^{-1} \Leftrightarrow x.\mathfrak{a} \subset B \Leftrightarrow \mathfrak{a}.x \subset B \quad .$$

Bien entendu les opérations algébriques (somme, produit, intersection, complémentaire, etc.) conservent l'ensemble des B-réseaux. Il est non moins clair qu'un réseau $\mathfrak{a}$ est un B-réseau si et seulement si $\hat{\mathfrak{a}}_{\mathfrak{p}}$ est un $\hat{B}_{\mathfrak{p}}$ -réseau pour tout $\mathfrak{p}$ .

(2.6). - Un B-réseau $\mathfrak{a}$ est dit premier si c'est en même temps un idéal bilatère maximal de l'anneau B . Les B-réseaux premiers ne sont autres évidemment que les idéaux bilatères maximaux $\mathfrak{a}$ de B tels que

$$A \cap \mathfrak{a} \neq 0$$

(cette propriété signifie en effet que $\mathfrak{a}$ engendre L sur K) ; ce sont aussi les éléments maximaux dans l'ensemble des B-réseaux contenus dans B (i. e. "entiers") et distincts de B . De là et de (1.8) résulte qu'un B-réseau $\mathfrak{a}$ est premier si et seulement si l'on peut trouver un idéal premier $\mathfrak{p}_0$ de A tel que $\hat{\mathfrak{a}}_{\mathfrak{p}} = \hat{B}_{\mathfrak{p}}$ pour tout $\mathfrak{p} \neq \mathfrak{p}_0$ et tel que $\hat{\mathfrak{a}}_{\mathfrak{p}_0}$ soit premier.

Il s'ensuit que l'ensemble des B-réseaux premiers s'identifie canoniquement à la somme des ensembles analogues relatifs aux divers ordres maximaux $\hat{B}_{\mathfrak{p}}$ .

(2.7). - Enonçons maintenant le théorème suivant :

THÉORÈME 1. - Soit B un ordre maximal de L ; alors le monoïde multiplicatif des B-réseaux est un groupe abélien, dont B est l'élément neutre, l'inverse dans ce groupe d'un B-réseau $\mathfrak{a}$ étant le B-réseau $\mathfrak{a}^{-1}$ . En outre, ce groupe admet pour base l'ensemble des B-réseaux premiers.

Les résultats énoncés en (1.8) et (2.6) permettent trivialement de se ramener au cas local-complet..D'autre part, si $L$ est somme directe d'algèbres simples $L_i$ il est clair que tout ordre maximal de $L$ est somme directe de ses projections dans les $L_i$ , qui sont aussi des ordres maximaux. Ainsi on peut se borner à établir le théorème dans le cas où $A$ est l'anneau d'une valuation discrète $v$ pour laquelle $K$ est complet et où $L$ est une algèbre simple sur $K$ , donc de la forme

$$L = M_n(L_o)$$

où $L_o$ est un corps gauche sur $K$ .

(2.8). - On commence d'abord par le cas où $L = L_o$ . On voit d'abord que

$$x \text{ entier} \iff N_{L_o/K}(x) \in A$$

(le cas commutatif est bien connu, le cas non commutatif s'y ramène en observant que tout $x \in L_o$ appartient à un sous-corps commutatif de $L_o$). Il s'ensuit (pour un corps gauche) que les $x \in L_o$ entiers sur $A$ forment un sous-anneau de $L_o$ , qui est donc l'unique ordre maximal $B_o$ de $L_o$ . Il est en effet trivial que $x \in B_o$ , $y \in B_o$ implique $xy \in B_o$ ; supposons de plus $x^{-1}y$ de norme entière (sinon permuter $x$ et $y$ ...) ; alors $x^{-1}y$ est entier, donc aussi $1 + x^{-1}y$ puisque $1$ commute à $x^{-1}y$ , donc aussi $x(1 + x^{-1}y) = x + y$ , d'où notre assertion.

Soit donc $B_o$ l'anneau des entiers de $L_o$ et soit $\mathfrak{a} \subset L_o$ un $B_o$-réseau ; comme $\mathfrak{a}_o$ est, à une homothétie près, contenu dans $B_o$ , les entiers $v(N(x))$ restent bornés inférieurement quand $x \in \mathfrak{a}$ ; si $x_o \in \mathfrak{a}$ est tel que $v(N(x_o))$ soit minimum il est clair que

$$\mathfrak{a} = x_o.B_o = B_o.x_o \quad ,$$

que $x \in \mathfrak{a}^{-1}$ signifie que $x_o\, x \in B_o$ , donc que

$$\mathfrak{a}^{-1} = x_o^{-1}.B_o = B_o.x_o^{-1} \quad ,$$

d'où la relation $\mathfrak{a}.\mathfrak{a}^{-1} = \mathfrak{a}^{-1}.\mathfrak{a} = B_o$ ; comme pour tout $x \in L_o$ on a trivialement $B_o\, x = xB_o$ , la relation $\mathfrak{a}.\mathfrak{b} = \mathfrak{b}.\mathfrak{a}$ s'obtient aussitôt dans l'ensemble des $B_o$-réseaux, qui est donc bien un groupe abélien. De plus l'ensemble $v(N(x)) > 0$ des éléments non inversibles de l'anneau $B_o$ est un idéal bilatère (même démonstration que pour montrer que les entiers forment un anneau), forcément maximal et unique maximal, donc seul et unique $B_o$-réseau premier ; si $x$ est un

générateur de celui-ci il est immédiat de voir (division euclidienne ...) que les entiers $v(N(y))$ , $y \in L_o$ , sont les multiples de $v(N(x))$ , d'où résulte que le $B_o$-réseau premier engendre le groupe des $B_o$-réseaux, qui est donc cyclique infini.

(2.9). - Le corps gauche $L_o$ étant liquidé il reste à examiner $L = M_n(L_o)$ . Soit $B$ un ordre maximal de $L$ ; considérant $L$ comme l'anneau des endomorphismes d'un vectoriel à droite $V$ de dimension $n$ sur $L_o$ , et observant que pour tout $x \in V$ non nul les $u(x)$ , $u \in B$ , forment un réseau de $V$ considéré comme vectoriel sur $K$ (image d'un réseau par un homomorphisme surjectif), on voit qu'il existe un $A$-réseau $\mathfrak{a}$ de $V$ tel que les $u \in B$ vérifiant $u(\mathfrak{a}) \subset \mathfrak{a}$ ; mais comme cette propriété définit un ordre dans $L$ , elle caractérise les $u \in B$ puisque $B$ est maximal ; de plus rien n'est changé si l'on remplace le réseau $\mathfrak{a}$ par le réseau $\mathfrak{a}.B_o$ (où $B_o$ est l'anneau des entiers du corps gauche $L_o$), i. e. on peut supposer que $B$ est l'ensemble des $u \in L$ qui conservent un réseau de $V$ invariant à droite par $B_o$ . Or les résultats obtenus dans (2.8) montrent que $B_o$ est un anneau principal (à ceci près qu'il n'est pas commutatif ...), d'où l'on déduit, par une extension triviale de la méthode valable pour les anneaux principaux commutatifs, que tout réseau $\mathfrak{a}$ de $V$ invariant par $B_o$ est un module libre sur $B_o$ , i. e. est engendré sur $B_o$ par une base de $V$ sur le corps $L_o$ . On a ainsi démontré que l'algèbre de matrices $L = M_n(L_o)$ possède, à un automorphisme intérieur près, un seul ordre maximal, à savoir $M_n(B_o)$ .

(2.10). - Pour établir le théorème 1 pour $L = M_n(L_o)$ on peut donc supposer que $B = M_n(B_o)$ . Soit alors $\mathfrak{a}$ un $B$-réseau de $L$ ; soit $u_{ij} \in L$ la matrice dont tous les termes sont nuls sauf celui d'indices $i$ , $j$ , qui est égal à $1$ ; on a donc $u = \sum u_{ij}\, d_{ij}(u) = \sum d_{ij}(u)\, u_{ij}$ pour tout $u \in L$ , avec des coefficients $d_{ij}(u) \in L_o$ ; pour $u \in \mathfrak{a}$ on a aussi $u_{ij}\, u \in \mathfrak{a}$ , $u u_{ij} \in \mathfrak{a}$ , d'où résulte que

$$u \in \mathfrak{a} \quad \text{implique} \quad u_{ij}\, d_{pq}(u) \in \mathfrak{a}$$

quels que soient $i$ , $j$ , $p$ , $q$ ; la réciproque est triviale ; or pour $i$ , $j$ donnés il est clair que les $d \in L_o$ tels que $u_{ij}\, d \in \mathfrak{a}$ forment dans $L_o$ un $B_o$-réseau $\mathfrak{a}_{ij}$ qui, d'après ce qui précède, est en fait indépendant des indices $i$ et $j$ ; autrement dit, $\mathfrak{a}$ est l'ensemble des matrices à coefficients dans un $B_o$-réseau donné de $L_o$ , i. e.

$$\mathfrak{a} = B.d = d.B \quad \text{pour un } d \in L_o \quad ,$$

ce qui donne une construction explicite de tous les $B$-réseaux de $L$ .

La démonstration du théorème 1 est naturellement triviale à partir de ce résultat, et l'on voit que le groupe abélien des B-réseaux est encore cyclique infini; le seul B-réseau premier étant formé des matrices à coefficients dans l'unique idéal bilatère maximal de $B_o$ .

(2.11). - Si l'on revient maintenant au "cas global" d'un anneau de Dedekind A quelconque, on obtient évidemment, modulo (1.8), le résultat que voici : soit B un ordre maximal d'une alfèbre semi-simple L sur K ; alors le groupe abélien des B-réseaux s'identifie canoniquement à la somme directe des groupes analogues relatifs aux ordres maximaux $\hat{B}_\mathfrak{p}$ des diverses algèbres $\hat{L}_\mathfrak{p}$ ; et le groupe des $\hat{B}_\mathfrak{p}$ -réseaux est abélien libre, et de rang égal au nombre de composantes simples de l'algèbre $\hat{L}_\mathfrak{p}$ (donc est cyclique infini dans le cas où L est une algèbre centrale simple sur K

(2.12). - La théorie classique des réseaux comporte encore d'autres résultats (cf. DEURING, chap. VI, paragraphe 2). Soit B un ordre maximal d'une algèbre semi-simple L sur K (A de Dedekind quelconque) ; on s'est jusqu'ici intéressé aux réseaux $\mathfrak{a}$ de L tels que $B.\mathfrak{a}.B = \mathfrak{a}$ ; on peut aussi étudier les réseaux tels que l'on ait seulement $B.\mathfrak{a} = \mathfrak{a}$ (resp. $\mathfrak{a}.B = \mathfrak{a}$) ; partons plus généralement d'un réseau $\mathfrak{a}$ de L et soit B' (resp. B") l'ensemble des $x \in L$ tels que $x.\mathfrak{a} \subset \mathfrak{a}$ (resp. $\mathfrak{a}.x \subset \mathfrak{a}$) ; alors B' et B" sont des ordres (trivial) et si l'un de ces ordres est maximal il en est de même de l'autre - on dit alors que $\mathfrak{a}$ est un réseau normal. On montre alors que les réseaux normaux de L forment un groupoïde au sens de BRANDT, à condition de ne considérer le produit $\mathfrak{a}'.\mathfrak{a}''$ de deux réseaux normaux que dans le cas où l'ordre maximal qui opère à droite sur $\mathfrak{a}'$ est identique à l'ordre maximal qui opère à gauche sur $\mathfrak{a}''$ . De plus ce groupoïde est engendré par les réseaux normaux $\mathfrak{a}$ possédant la propriété suivante : $\mathfrak{a}$ est un idéal à gauche maximal de l'ordre maximal B' qui opère à gauche sur $\mathfrak{a}$ (auquel cas $\mathfrak{a}$ est aussi un idéal à droite maximal de l'ordre maximal qui opère à droite sur $\mathfrak{a}$). Evidemment toutes ces propriétés - qui font l'objet dans DEURING de démonstrations directes fort ingénieuses mais peu transparentes - peuvent se démontrer en passant aux algèbres $\hat{L}_\mathfrak{p}$ et en donnant explicitement, dans ce cas, la structure des réseaux normaux.

## 3. Norme d'un réseau ; relation des degrés.

On conserve les hypothèses et notations des numéros précédents ; A est un anneau de Dedekind quelconque jusqu'à nouvel ordre (à ceci près que K est supposé être de caractéristique 0), et L est une algèbre semi-simple sur K .

(3.1). - Il est bien connu que l'on peut attacher à tout A-module de torsion et de type fini M un idéal $\chi(M)$ de l'anneau de Dedekind A , de telle sorte que : $\chi(M) = \chi(N)$ si M et N sont isomorphes ; $\chi(M) = \mathfrak{a}$ si $M = A/\mathfrak{a}$ où $\mathfrak{a}$ est un idéal de A ; $\chi(M) = \chi(M')\,\chi(M'')$ toutes les fois qu'on a une suite exacte $0 \to M' \to M \to M'' \to 0$ . Ces propriétés caractérisent la "fonction" $\chi$ .

(3.2). - Soit B un ordre maximal de L . Pour tout B-réseau $\mathfrak{a}$ entier (i. e. contenu dans B), on peut regarder $B/\mathfrak{a}$ comme un A-module de type fini ; son annulateur est l'idéal non nul $A \cap \mathfrak{a}$ de A , c'est donc un A-module de torsion ; ainsi on peut définir

$$N(\mathfrak{a}) = \chi(B/\mathfrak{a}) \quad .$$

On a alors la relation

$$N(\mathfrak{a}'.\mathfrak{a}'') = N(\mathfrak{a}').N(\mathfrak{a}'')$$

quels que soient les B-réseaux entiers $\mathfrak{a}'$ et $\mathfrak{a}''$ (ce qui permettra de définir la norme d'un B-réseau non nécessairement entier). Pour établir ce résultat il suffit (vu la multiplicativité de la fonction $\chi$ ) de prouver que les A-modules $B/\mathfrak{a}'$ et $\mathfrak{a}''/\mathfrak{a}'\,\mathfrak{a}''$ sont isomorphes ou du moins ont le même $\chi$ . Mais évidemment $\chi(M)$ dépend uniquement des localisés $M_{\mathfrak{p}}$ de M , et même uniquement des complétés $\hat{M}_{\mathfrak{p}}$ ; comme le foncteur

$$\mathfrak{a} \longrightarrow \hat{\mathfrak{a}}_{\mathfrak{p}}$$

est compatible avec la multiplication des réseaux, on est ramené à faire la démonstration dans le cas local-complet ; mais c'est alors à peu près évident, puisque dans ce cas les B-réseaux sont "principaux" comme on l'a vu en (2.10).

(3.3). - Soit en particulier $\mathfrak{a}$ un B-réseau premier ; alors $A \cap \mathfrak{a} = \mathfrak{p}$ est un idéal premier de l'anneau A (soit $x \in A$ ; les $y \in B$ tels que $xy \in \mathfrak{a}$ forment un B-réseau entier contenant $\mathfrak{a}$ , donc égal à B ou au B-réseau $\mathfrak{a}$ ; donc les $y \in A$ tels que $xy \in \mathfrak{p}$ forment soit l'idéal $\mathfrak{p}$ soit l'anneau A tout entier). Il est clair qu'alors

$$N(\mathfrak{a}) = \mathfrak{p}^f \quad \text{où} \quad f = [B/\mathfrak{a} : A/\mathfrak{p}]$$

- on regarde $B/\mathfrak{a}$ comme un espace vectoriel sur le corps $A/\mathfrak{p}$ .

(3.4). - Soit $\mathfrak{p}$ un idéal premier de A ; comme les éléments de A commutent à ceux de B , l'ensemble $B.\mathfrak{p}$ est un B-réseau entier, qui a donc une décomposition unique

$$B.\mathfrak{p} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \qquad (e_i \geqslant 1)$$

avec des B-réseaux premiers $\mathfrak{P}_i$ , de degrés $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$ ; il est du reste facile de voir que les $\mathfrak{P}_i$ sont tous les B-réseaux premiers qui contiennent $\mathfrak{p}$ . D'après (3.2) et (3.3) on a alors

$$\chi(B/B.\mathfrak{p}) = \mathfrak{p}^{e_1 f_1 + \ldots + e_r f_r} \quad ;$$

pour déduire de là la classique relation des degrés

$$e_1 f_1 + \ldots + e_r f_r = n = [L : K]$$

il suffit donc de montrer que $B/B.\mathfrak{p}$ est de dimension $n$ sur le corps $A/\mathfrak{p}$ ; pour cela on remarque que $B/B.\mathfrak{p}$ ne change pas si l'on se localise en $\mathfrak{p}$ , ce qui ramène au cas où $A$ est un anneau local, donc principal ; mais alors $B$ est libre de rang $n$ et $\mathfrak{p}.B = \pi.B$ où $\pi$ est un générateur de l'idéal $\mathfrak{p}$ de $A$ , d'où immédiatement le résultat cherché.

(3.5). - Conservons les hypothèses et notations de (3.4) ; on va déterminer les $\mathfrak{p}$ qui se "ramifient" dans $B$ , i. e. pour lesquels les indices de ramification $e_i$ ne sont pas tous égaux à 1 . Cela signifie évidemment que l'anneau d'Artin $B/B.\mathfrak{p}$ n'est pas semi-simple, i. e. possède des idéaux nilpotents non nuls. Une condition nécessaire pour qu'il en soit ainsi est que la forme $Tr(xy)$ de $B/B.\mathfrak{p}$ (regardé comme algèbre sur le corps $A/\mathfrak{p}$) soit dégénérée. Or comme $B_{\mathfrak{p}}$ est un module libre de rang $n$ sur l'anneau $A_{\mathfrak{p}}$ , il existe dans $B$ une base $(x_i)$ de $L$ sur $K$ qui est aussi une base du $A_{\mathfrak{p}}$-module $B_{\mathfrak{p}}$ ; alors les images des $x_i$ dans $B/B.\mathfrak{p}$ forment une base de cette algèbre ; comme pour $x \in L$ on a

$$Tr_{L/K}(x) = \sum \lambda_{ii} \quad \text{où} \quad xx_i = \sum \lambda_{ij} x_j$$

on déduit immédiatement de là que la forme $Tr(xy)$ sur $B$ passe au quotient et donne la forme $Tr(xy)$ de l'algèbre $B/B.\mathfrak{p}$ . Si donc $\mathfrak{p}$ est ramifié dans $B$ , il existe

$$x \in B \ , \quad x \notin B.\mathfrak{p} \quad \text{tel que} \quad Tr(xy) \in \mathfrak{p} \quad \text{pour tout} \quad y \in B \ .$$

Or considérons dans $L$ le réseau complémentaire de $B$ (cf. (2.1)) ; c'est évidemment un $B$-réseau de $L$ qui contient $B$ , donc de la forme

$$\delta(B)^{-1}$$

où $\delta(B)$ , différente de l'ordre maximal $B$ , est un $B$-réseau entier. Il est immédiat de voir (en se localisant, de sorte que $\mathfrak{p}$ devient principal) que les $y \in L$ tels que $Tr(xy) \in \mathfrak{p}$ pour tout $x \in B$ forment le $B$-réseau $\mathfrak{p}.\delta(B)^{-1}$ - on a d'ailleurs la formule

$$\tilde{a} = a^{-1}.\delta(B)^{-1}$$

pour tout B-réseau $a$ . Ceci dit, on voit que si $\mathfrak{p}$ se ramifie dans B on a la relation

$$B \cap \mathfrak{p} \cdot \delta(B)^{-1} \neq \mathfrak{p}.B$$

(le premier membre contient toujours le second). Ecrivant les décompositions de $\mathfrak{p}.B$ et de $\delta(B)$ en B-réseaux premiers, on voit que la relation précédente équivaut à l'existence de "facteurs premiers" communs à $B.\mathfrak{p}$ et à $\delta(B)$ ; autrement dit si $\mathfrak{p}$ se ramifie dans B , on a la relation

$$\delta(B) \cap A \subset \mathfrak{p} \quad ,$$

ce qui prouve qu'il n'existe qu'un nombre fini d'idéaux premiers de A qui se ramifient dans B . On notera que la condition qu'on vient de trouver s'écrit encore

$$\mathfrak{p} \supset N(\delta(B)) \quad .$$

L'idéal $N(\delta(B))$ s'appelle le discriminant de l'algèbre L ; il ne dépend pas du choix de l'ordre maximal B (en effet il est clair que pour tout idéal premier $\mathfrak{p}$ de A la $\mathfrak{p}$-composante de ce discriminant s'obtient en remplaçant L par $\hat{L}_{\mathfrak{p}}$ et B par $\hat{B}_{\mathfrak{p}}$ ; or les ordres maximaux sont conjugués dans le cas local-complet, d'où le résultat). On montrera plus loin comment le calculer.

(3.6). - On vient de montrer que, si un idéal premier $\mathfrak{p}$ de A se ramifie dans B (i. e. admet des facteurs premiers multiples), alors il divise l'idéal $N(\delta(B))$ . La réciproque de cette propriété n'est pas exacte ; en effet la relation $\mathfrak{p} \supset N(\delta(B))$ exprime simplement, comme on l'a vu, que la forme bilinéaire Tr(xy) de l'algèbre $B/B.\mathfrak{p}$ sur le corps $A/\mathfrak{p}$ est dégénérée - mais cela peut fort bien se produire même si $B/B.\mathfrak{p}$ est semi-simple (exemple : si $A/\mathfrak{p} = k$ est de caractéristique p , alors la forme Tr(xy) de l'algèbre $M_p(k)$ est identiquement nulle ...). Pour aller plus loin il faudrait, au lieu d'utiliser sur les algèbres considérées les traces usuelles (calculées dans la représentation régulière), se servir des traces réduites (étant donnée une algèbre L sur un corps K , la trace réduite Sp dans L est la somme des caractères des diverses représentations irréductibles de l'algèbre déduite de L par extension des scalaires à la clôture algébrique de K ; rappelons que la forme Sp(xy) sur L est non dégénérée si et seulement si L est absolument semi-simple, i. e. reste semi-simple par extension à la clôture algèbrique de K). En remplaçant sur L la trace Tr par la trace réduite Sp , on remplace la différente $\delta(B)$ de l'ordre maximal B par la différente "réduite" $\delta'(B)$ . On démontre alors (DEURING, chap. VI, paragraphe 5, Satz 3) que pour qu'un idéal premier $\mathfrak{p}$ de A divise $N(\delta'(B))$ il faut et il suffit

que l'un des B-réseaux premiers qui divisent $B.\mathfrak{p}$, soit $\mathfrak{q}$, vérifie l'une des deux conditions suivantes : ou bien $\mathfrak{q}$ intervient dans la décomposition de $\mathfrak{p}.B$ avec une multiplicité $\geqslant 2$, ou bien $B/\mathfrak{q}$, considérée comme algèbre sur le corps $A/\mathfrak{p}$, n'est pas absolument semi-simple. (Cette dernière circonstance ne saurait d'ailleurs se produire dans les situations "arithmétiques", puisqu'alors les corps $A/\mathfrak{p}$ sont finis et n'ont donc que des extensions séparables). Pour le cas des extensions commutatives de K, voir aussi SAMUEL-ZARISKI [5], chap. V, paragraphe 11.

(3.7). - Pour conclure, indiquons un procédé "pratique" de calcul de la norme $N(\mathfrak{a})$ d'un B-réseau. Il suffit d'en calculer la $\mathfrak{p}$-composante pour tout $\mathfrak{p}$, ce qui permet de se ramener au cas d'un anneau A principal. Il y a alors une base $(b_i)$ du A-module B et une base $(a_i)$ du A-module $\mathfrak{a}$, et on a

$$a_i = \sum \lambda_{ij}\, b_j \qquad , \qquad \lambda_{ij} \in K \qquad ;$$

ceci dit, $N(\mathfrak{a})$ est l'idéal de A engendré par $\det(\lambda_{ij})$. En effet on peut d'abord supposer $\mathfrak{a} \subset B$ à l'aide d'une homothétie. Par ailleurs l'idéal $\det(\lambda_{ij})$ ne dépend évidemment pas du choix des bases de B et de $\mathfrak{a}$ ; on peut donc (diviseurs élémentaires) supposer la matrice $(\lambda_{ij})$ diagonale ; mais alors on a un isomorphisme de A-modules

$$B/\mathfrak{a} = \prod A/\lambda_{ii}\, A \qquad ,$$

d'où trivialement le résultat cherché.

Ceci permet par exemple de calculer le discriminant $N(\delta(B))$ ; en effet $\delta(B)^{-1}$ est le complémentaire $\tilde{B}$ du réseau B, donc a une base $(\tilde{x}_i)$ telle que

$$\mathrm{Tr}(x_i\, \tilde{x}_j) = \delta_{ij} \qquad ;$$

posant $\tilde{x}_i = \sum \lambda_{ij}\, x_j$ on voit donc que les matrices $(\lambda_{ij})$ et $(\mathrm{Tr}(x_i\, x_j))$ sont inverses l'une de l'autre, d'où

$$N(\delta(B)) = \det(\mathrm{Tr}(x_i\, x_j))$$

dans le cas d'un anneau A principal. Le cas général s'y ramène par localisation, et montre que le discriminant de B est l'idéal de A engendré par les éléments $\det(\mathrm{Tr}(x_i\, x_j))$, où $(x_i)$ parcourt l'ensemble des suites de $n = [L : K]$ éléments de B. Ce résultat remonte naturellement à Dedekind (modulo la non-commutativité).

4. L'anneau des adèles d'une algèbre semi-simple sur les rationnels.

Dans tout le reste de cet exposé on suppose que $A = \underset{\sim}{Z}$ , $K = \underset{\sim}{Q}$ . On pourrait "plus généralement" examiner le cas où $A$ est l'anneau des entiers d'un corps de nombres algébriques, mais ce cas se ramène visiblement au précédent ...

(4.1). - Pour tout nombre premier $p$ on considère la valeur absolue p-adique, donnée par

$$|x|_p = p^{-v_p(x)}$$

où $v_p$ est la valuation p-adique normée ; on introduit aussi la valeur absolue usuelle

$$|x|_\infty = |x| \quad ;$$

l'ensemble de ces valeurs absolues est appelé l'ensemble des <u>places</u> de $K$ ; les places $|x|_p$ sont dites "finies", la place $|x|_\infty$ est qualifiée, sans doute pour des raisons d'ordre psychanalytique, de "place à l'infini". Pour chaque $p$ (fini ou infini) on notera $\hat{K}_p$ le complété de $K$ pour la valeur absolue correspondante ; c'est le corps $\underset{\sim}{Q}_p$ des nombres p-adiques si $p$ est fini, et le corps $\underset{\sim}{R}$ des nombres réels si $p$ est infini. Pour $p$ fini, l'anneau $\hat{A}_p = \underset{\sim}{Z}_p$ est formé des entiers p-adiques ; comme chacun sait ou peut démontrer, le groupe additif topologique $\hat{K}_p$ est localement compact pour tout $p$ (même infini) et, pour $p$ fini, le sous-groupe $\hat{A}_p$ est compact (donc fermé) et de plus ouvert dans $\hat{K}_p$ .

(4.2). - Soit maintenant $L$ un espace vectoriel de dimension finie sur le corps $K$ . En plus des complétés p-adiques $\hat{L}_p$ introduits au numéro (1.6), pour $p$ fini, on définit

$$\hat{L}_\infty = \hat{K}_\infty \underset{K}{\otimes} L \quad ,$$

vectoriel déduit de $L$ pae extension à $\underset{\sim}{R}$ du corps de base. Tous les groupes additifs $\hat{L}_p$ ($p$ fini ou non) sont localement compacts. Pour $p$ fini il est clair que tout <u>réseau</u> de $\hat{L}_p$ constitue un sous-groupe ouvert et compact de $\hat{L}_p$ ; par contre, $\hat{L}_\infty$ est excessivement connexe.

(4.3). - Les notations étant comme en (4.2), choisissons un $A$-réseau $\alpha$ dans $L$ , d'où un $\hat{A}_p$-réseau $\hat{\alpha}_p$ dans $\hat{L}_p$ pour tout $p$ fini. Nous appelerons <u>adèles</u> de $L$ les

$$\underline{x} = (x_p) \in \prod \hat{L}_p$$

tels que l'on ait

$$x_p \in \mathfrak{a}_p \quad \text{pour presque tout } p \text{ fini ;}$$

cette condition est évidemment indépendante du choix du réseau $\mathfrak{a}$ dans $L$ - cf. (1.5) et (1.8). Il est clair que les adèles forment un sous-groupe $\hat{L}$ du produit direct des complétés $\hat{L}_p$. Comme $\hat{\mathfrak{a}}_p$ est un sous-groupe ouvert compact de $\hat{L}_p$ pour tout $p$ fini, il est facile de voir qu'il existe sur $L$ une et une seule topologie de groupe telle que

$$\hat{L}_\infty \times \prod_{p \text{ fini}} \hat{\mathfrak{a}}_p$$

soit, avec sa topologie naturelle (produit de groupes localement compacts presque tous compacts), un sous-groupe ouvert de $\hat{L}$. Si l'on remplace $\mathfrak{a}$ par un autre réseau $\mathfrak{b}$, on a d'abord $\mathfrak{a}_p = \mathfrak{b}_p$ pour presque tout $p$ ; et pour les $p$ finis exceptionnels, il est clair que $\mathfrak{a}_p \cap \mathfrak{b}_p$ est compact et d'indice fini à la fois dans $\mathfrak{a}_p$ et dans $\mathfrak{b}_p$ ; on en déduit que la topologie qu'on vient de définir sur $\hat{L}$ ne dépend pas du choix de $\mathfrak{a}$.

Si $L = K$ il est clair que $\hat{K}$ est un sous-anneau de $\prod \hat{K}_p$, et que la topologie de $\hat{L}$ fait de $\hat{L}$ un anneau topologique localement compact. Dans le cas général, chaque $\hat{L}_p$ est un espace vectoriel topologique sur le corps $\hat{K}_p$ correspondant ; comme le "transporteur" d'un réseau dans un réseau est encore un réseau, on voit immédiatement qu'on peut regarder $\hat{L}$ comme un module topologique sur l'anneau topologique $\hat{K}$.

(4.4). - Considérons toujours un vectoriel $L$ sur $K$ ; les injections canoniques $L \to \hat{L}_p$ définissent une injection

$$L \to \prod \hat{L}_p \quad ,$$

et en fait, évidemment, une injection

$$L \to \hat{L} \quad ;$$

regardés comme éléments de $\hat{L}$, les $x \in L$ s'appellent les adèles principaux. Le premier résultat important (mais très facile ...) est que $L$ est un sous-groupe discret de $\hat{L}$, le quotient $\hat{L}/L$ étant de plus compact.

Pour prouver que $L$ est discret il faut montrer que, pour tout réseau $\mathfrak{a}$ de $L$, les $x \in L$ tels que $x \in \mathfrak{a}_p$ pour tout $p$ (ce qui veut dire $x \in \mathfrak{a}$ simplement ...) et qui sont assez voisins de 0 dans $\hat{L}_\infty$ forment un ensemble fini - autrement dit que les réseaux de $L$ sont aussi des sous-groupes discrets de $\hat{L}_\infty$,

ce qui est assez clair. Pour établir la compacité de $\hat{L}/L$ on considère le sous-groupe ouvert

$$U(\mathfrak{a}) = \hat{L}_\infty \times \prod_{p \text{ fini}} \hat{\mathfrak{a}}_p$$

de $\hat{L}$, où $\mathfrak{a}$ est un réseau de $L$ ; on vérifie d'abord, grâce à un théorème "chisnois", que $\hat{L} = L + U(\mathfrak{a})$ ; il reste alors à établir que $U(\mathfrak{a})/L \cap U(\mathfrak{a})$ est compact ; or $U(\mathfrak{a})$ est produit d'un groupe compact et de $\hat{L}_\infty$ ; par ailleurs $L \cap U(\mathfrak{a}) = \mathfrak{a}$ est à quotient compact dans $\hat{L}_\infty$, d'où immédiatement le résultat.

5. Le groupe des idèles d'une algèbre.

Les hypothèses faites au début du numéro 4 restent valables ; on désigne maintenant par $L$ une algèbre semi-simple sur $K$.

(5.1). - On appelle idèles de $L$ les éléments inversibles de l'anneau $\hat{L}$ des adèles de $L$ ; ils forment donc un groupe multiplicatif $I^*(L)$, qui contient canoniquement le groupe des unités $L^*$ de l'algèbre $L$. Noter que si $\underline{x} = (x_p)$ est un idèle de $L$, et si $B$ est un ordre maximal de $L$, on a $x_p \in \hat{B}_p$ pour presque tout $p$ fini, et par conséquent $x_p$ est une unité de l'anneau $\hat{B}_p$ pour presque tout $p$.

(5.2). - On peut munir $I^*(L)$ d'une topologie, à savoir la moins fine qui rende continues les injections $x \to x$ et $x \to x^{-1}$ de $I^*(L)$ dans $\hat{L}$. Il est clair (pour tout anneau topologique :) que c'est bien une topologie de groupe ; elle est en outre localement compacte. Soient en effet $B$ un ordre maximal de $L$ et $U_\infty$ un voisinage compact de 0 dans $\hat{L}_\infty$ ; les idèles $\underline{x}$ vérifiant

$$\underline{x} \in 1 + U_\infty \quad , \quad \underline{x}^{-1} \in 1 + U_\infty \quad , \quad x_p \in \hat{B}_p \quad , \quad x_p^{-1} \in \hat{B}_p$$

forment un voisinage de l'unité dans $I^*(L)$ par définition ; pour voir qu'un tel voisinage est compact il suffit évidemment de montrer que dans $\hat{L}_p$ ($p$ fini) l'ensemble $U_p(B)$ des unités de $\hat{B}_p$ est compact ; or $\hat{B}_p$ est compact ; il suffit donc de faire voir que les éléments non inversibles de $\hat{B}_p$ forment un sous-groupe ouvert de $\hat{B}_p$ ; mais ce sous-ensemble (et non pas sous-groupe !) est la réunion des idéaux (à gauche ou à droite) maximaux de l'anneau $\hat{B}_p$, lesquels sont des réseaux du vectoriel $\hat{L}_p$ et sont par suite ouverts dans $\hat{B}_p$, d'où le résultat.

Il est clair que $L^*$ se plonge comme sous-groupe discret dans $I^*(L)$ ; les éléments de $L^*$ sont aussi appelés les idèles principaux de $L$.

(5.3). - On va maintenant définir et calculer la valeur absolue $|\underline{x}|$ d'un idèle $\underline{x}$.

Pour cela on considère sur le groupe additif $\hat{L}$ une mesure de Haar $dm^+(\underline{y})$ ; évidemment $dm^+(\underline{x}.\underline{y})$ est encore une mesure de Haar de $\hat{L}$ puisque $\underline{x}$ est inversible, et par suite

$$dm^+(\underline{x}.\underline{y}) = |\underline{x}|.dm^+(\underline{y})$$

avec un facteur $|\underline{x}|$ réel strictement positif; c'est la valeur absolue cherchée.

La valeur absolue est donc encore définie par le fait que l'on a

$$m^+(\underline{x}.K) = |\underline{x}|.m^+(K)$$

pour tout compact $K \subset \hat{L}$ .On va en déduire le calcul de $|x|$ .

Soit $dm_p^+$ la mesure de Haar de $\hat{L}_p$ additif, normée pour $p$ fini par la condition que

$$m_p^+(\hat{B}_p) = 1$$

pour un ordre maximal donné $B$ de $L$ (il résultera des calculs qui vont suivre que cette condition est alors vérifiée pour tout autre ordre maximal de $L$ , vu que les ordres maximaux de $\hat{L}_p$ sont deux à deux conjugués). Comme $\hat{L}_\infty \times \prod \hat{B}_p$ est ouvert dans $\hat{L}$ , la mesure de Haar de $\hat{L}$ induit sur ce sous-groupe le produit (qui a un sens ...) des mesures de Haar des groupes additifs $\hat{L}_\infty$ et $\hat{B}_p$ ; on peut donc prendre

$$K = K_\infty \times \prod_{p \text{ fini}} \hat{B}_p$$

et alors

$$|\underline{x}| = \frac{m_\infty^+(\underline{x}_\infty.K_\infty)}{m_\infty^+(K_\infty)} \cdot \prod_{p \text{ fini}} \frac{m_p^+(\underline{x}_p.\hat{B}_p)}{m_p^+(\hat{B}_p)} \quad .$$

Vu les propriétés connues des déterminants il est clair que

$$m_\infty^+(\underline{x}_\infty.K_\infty) = |N(\underline{x}_\infty)|.m_\infty^+(K_\infty)$$

où la norme est calculée à la façon usuelle, i. e. dans la représentation régulière de l'algèbre $\hat{L}_\infty$ . Supposons maintenant provisoirement $\underline{x}_p \in \hat{B}_p$ pour tout $p$ fini ; alors $\underline{x}_p.\hat{B}_p$ est un réseau de $\hat{L}_p$ contenu dans $\hat{B}_p$ , donc un sous-groupe d'indice fini de $\hat{B}_p$ ; par suite

$$m_p^+(\underline{x}_p.\hat{B}_p) = m_p^+(\hat{B}_p).(\hat{B}_p : \underline{x}_p.\hat{B}_p)^{-1}$$

où figure au second membre l'indice de $\underline{x}_p.\hat{B}_p$ dans $\hat{B}_p$ . Or soit $(b_{p,i})$ une base

de $\hat{B}_p$ sur $\hat{A}_p$, donc aussi de $\hat{L}_p$ sur $\hat{K}_p$ et posons

$$\underline{x}_p \cdot b_{p,i} = \sum a_{p,ij}\, b_{p,j} \quad , \quad a_{p,ij} \in \hat{A}_p \quad ;$$

comme l'idéal maximal de $\hat{A}_p$ est engendré par $p$ on a une relation

$$N(\underline{x}_p) = \det(a_{p,ij}) = p^{r_p} \quad ,$$

où $N(\underline{x}_p)$ est ici encore la norme usuelle dans l'algèbre $\hat{L}_p$ sur $\hat{K}_p$ ; ceci dit le raisonnement fait en (3.7) montre que $\chi(\hat{B}_p/\underline{x}_p.\hat{B}_p)$ est l'idéal $p^{rp^p}$ de $\hat{A}_p$ ; comme $\hat{A}_p/p\hat{A}_p$ a $p$ éléments on en déduit que

$$(\hat{B}_p : \underline{x}_p.\hat{B}_p) = p^{r_p} = |N(\underline{x}_p)|_p^{-1}$$

vu la normalisation adoptée pour les valeurs absolues p-adiques de $K$. Ceci fait, il est clair qu'on a en définitive la formule

$$|\underline{x}| = \prod |N(\underline{x}_p)|_p \quad ,$$

le produit étant étendu à tous les $p$ (finis ou non) et convergeant trivialement vu que $N(\underline{x}_p)$ est une unité pour presque tout $p$.

A vrai dire la démonstration suppose $\underline{x}_p \in \hat{B}_p$ pour tout $p$ fini, mais le passage au cas général est trivial vu d'une part la multiplicativité des deux membres de la relation précédente, et, d'autre part, le fait que tout idèle est quotient de deux idèles vérifiant les hypothèses faites dans la démonstration.

(5.4). - Prenons en particulier un $x \in L^*$ et regardons-le comme un élément de $I^*(L)$ ; comme la norme se conserve par extension du corps de base il est clair qu'on prouve

$$|x| = \prod |N_{L/K}(x)|_p = 1$$

en vertu de la formule "du produit", à savoir

$$\prod |\lambda|_p = 1 \quad \text{pour tout} \quad \lambda \in K \, .$$

On est donc conduit à introduire le sous-groupe

$$I_o^*(L) \, : \, |\underline{x}| = 1$$

de $I^*(L)$, et on voit que $L^*$ se plonge comme sous-groupe discret de $I_o^*(L)$. Le quotient $I^*(L)/I_o^*(L)$ est naturellement isomorphe à $\mathbf{R}_+^*$.

(5.5). - On va maintenant démontrer le théorème suivant :

THÉORÈME 2. - Si L est une algèbre à division, l'espace homogène $I_o^*(L)/L^*$ est compact.

Il suffit de prouver le résultat suivant :

Soit M un anneau topolologique localement compact contenant un sous-corps L discret dans M et tel que le quotient M/L soit compact. Soit $M_o^*$ le groupe multiplicatif formé des $a \in M^*$ tels que $x \to ax$ laisse invariante la mesure de Haar additive $dm^+(x)$ de M. Alors :

(i) on a $L^* \subset M_o^*$

(ii) $L^*$ est un sous-groupe discret à quotient compact de $M_o^*$ (muni de la topologie la moins fine qui rend continues les injections $x \to x$ et $x \to x^{-1}$ de $M_o^*$ dans M).

DÉMONSTRATION. - (FUJISAKI. - A. WEIL).

Soit $\xi \in L^*$ ; l'automorphisme $x \to \xi x$ du groupe additif M laisse invariante la mesure de Haar de L (trivialement) ainsi que celle de M/L puisque ce quotient est compact ; d'où (i).

Posons d'une manière générale

$$dm^+(ax) = |a|.dm^+(x) \quad .$$

On a d'abord le lemme suivant :

LEMME de Minkowski. - Soit V un voisinage compact de 0 dans M ; il existe une constante $c(V) > 0$ telle que les relations

$$x \in M^* \quad , \quad |x| > c(V)$$

impliquent

$$x.V \cap L^* = \emptyset \quad .$$

En effet soit $W = -W$ un second voisinage compact de 0 tel que $W + W \subset V$ ; si $x.V$ ne rencontre L qu'en 0 il est clair que les ensembles $x.W + y (y \in L)$ sont deux à deux disjoints, et par suite que

$$m^+(x.W) \leq m^+(M/L) \quad ;$$

il suffit donc de prendre $c(V) = m^+(M/L)/m^+(W)$ .

Le lemme de Minkowski étant établi, prenons un voisinage compact V de 0 tel que

$c(V) < 1$ , ce qui est évidemment possible ; alors

$$x \in M_o^* \Rightarrow x.V \cap L^* \text{ non vide,}$$

ce qui prouve que

$$(1) \qquad M_o^* = L^*.(M_o^* \cap V)^{-1} = (M_o^* \cap V).\ L^* \quad ;$$

il reste à prouver que $M_o^* \cap V$ est un compact du groupe <u>multiplicatif</u> $M_o^*$ , et pour cela il suffit de montrer que $(M_o^* \cap V)^{-1}$ est relativement compact dans le groupe <u>additif</u> M . Or (1) montre que pour tout $x \in M_o^* \cap V$ il existe $\xi \in L^*$ tel que $x = \xi v^{-1}$ pour un $v \in M_o^* \cap V$ ; il s'ensuit que $\xi = x.v \in V.V$ , partie compacte de M , d'où un nombre fini seulement de possibilités pour $\xi$ , soit $\{\xi_1, \dots, \xi_r\}$ ; ainsi

$$x \in M_o^* \cap V \text{ implique } x^{-1} \in \bigcup_{i=1} V\,\xi_i^{-1} \quad ,$$

ce qui achève la démonstration.

COROLLAIRE. - <u>Soient</u> L <u>une algèbre à division sur</u> $K = \underset{\sim}{Q}$ , <u>le groupe multiplicatif des éléments de norme</u> 1 <u>de</u> $\hat{L}_\infty$ , <u>et</u> $\Gamma \subset G$ <u>le groupe des unités d'un ordre maximal</u> B <u>de</u> L . <u>Alors</u> $\Gamma$ <u>est un sous-groupe discret</u> à quotient compact <u>du groupe de Lie</u> G.

Pour p fini, notons $U_p(B)$ le groupe des unités de l'anneau $\hat{B}_p \subset \hat{L}_p$ ; il est visible que c'est un sous-groupe ouvert et compact de $\hat{L}_p^*$ , et que

$$U = \hat{L}_\infty^* \times \prod_{p \text{ fini}} U_p(B) \quad ,$$

muni de sa topologie-produit, est un sous-groupe <u>ouvert</u> de $I^*(L)$ . De là et par des raisonnements assez triviaux de théorie des groupes topologiques, on déduit que

$$U \cap I_o^*(L)/U \cap L^*$$

est compact. Or

$$U \cap I_o^*(L) = G \times \prod_{p \text{ fini}} U_p(B)$$

avec la topologie-produit, et d'autre part $U \cap L^* = \Gamma$ puisque le fait pour un $x \in L$ d'être une unité de B est évidemment une propriété locale. Comme le facteur "parasite" $\prod U_p(B)$ est compact, on obtient immédiatement le corollaire.

Rappelons que dans le cas classique (L = corps de nombres) le corollaire précédent

est essentiellement équivalent au théorème des unités de Dirichlet, qui vaut donc pour tout algèbre à division sur le rationnels. Naturellement le corollaire montre que le groupe $\Gamma$ est à engendrement fini (comme quotient du groupe fondamental d'une variété compacte).

(5.6). - Dans le théorème 2, l'hypothèse que L est un corps gauche ne peut pas être évitée ; en effet, avec les notations du corollaire précédent, le quotient $\Gamma\backslash G$ est compact ; on en déduit par un raisonnement facile (communiqué à l'auteur par A. SELBERG) que pour tout $\gamma \in \Gamma$ les $g\gamma g^{-1} (g \in G)$ forment dans G un ensemble fermé ; de là résulte (propriété générale des groupes semi-simples) que tout $\gamma \in \Gamma$ est semi-simple, donc que ni $\Gamma$, ni par conséquent $L^*$, ne possèdent d'élément unipotent $\neq e$, ce qui est trivialement faux si L n'est pas un corps.

(5.7). - Dans le cas où L est seulement semi-simple, on a encore des résultats importants. Considérons comme ci-dessus le sous-groupe ouvert

$$U = L^*_{\infty} \times \prod_{p \text{ fini}} U_p(B)$$

de $I^*(L)$ .

THÉORÈME 3. - $I^*(L)$ est réunion finie de classes bilatères

$$L^*.x.U$$

THÉORÈME 4. - L'espace homogène $L^*\backslash I^*(L)$ est de volume fini.

Pour établir ces résultats, écrivons $L = M_n(K)$ , où K est un corps gauche. Si A est un ordre maximal de K on peut supposer $B = M_n(A)$ . Posons

$$I^+(K) = \hat{K} \quad ;$$

il est clair que

$$I^+(L) = M_n(\hat{K}) \quad ; \quad I^*(L) = GL(n , \hat{K}) \quad .$$

Si on considère dans $\hat{K}$ le sous-anneau ouvert

$$\hat{A} = K_{\infty} \times \prod_{p \text{ fini}} A_p$$

il est aussi clair que

$$U = GL(n , \hat{A}) \quad .$$

Formons dans $I^*(L) = GL(n , \hat{K})$ le sous-groupe

$$T : \text{matrices } t = \begin{pmatrix} t_1 & * \\ 0 & t_2 \end{pmatrix}$$

avec $t_1 \in I^*(K)$ , $t_2 \in GL(n-1 , \hat{K})$ . On a tout d'abord

$$GL(n , \hat{K}) = T.U = U.T$$

(il suffit de vérifier $gl(n , K_p) = T_p.U_p$ pour chaque $p$ fini, ce qui résulte du fait que l'anneau $A_p$ est "principal"). Pour prouve le théorème 3 il suffit donc de montrer que $T$ est recouvert par un nombre fini de classes ; si $n = 1$ c'est trivial ($U$ est ouvert, $L^* \setminus I^*(L)$ est compact) ; si $n > 1$ le résultat s'obtient facilement par récurrence sur $n$ ; car $T$ est produit semi-direct de $GL(1 , \hat{K}) \times GL(n-1 , \hat{K})$ et d'un groupe additif $\hat{K}^{n-1}$ .

Pour le théorème 4, choisissons dans $L^*_\infty$ un sous-groupe compact maximal $W_\infty$ et posons

$$W = W_\infty \times \prod U_p(B) \quad ,$$

sous-groupe compact de $I^*(L)$ ; on a encore

$$I^*(L) = GL(n , \hat{K}) = W.T \quad .$$

Regardons les $g \in I^*(L)$ comme des automorphismes du $\hat{K}$-module à droite $\hat{K}^n$ . Le raisonnement de Minkowski (démonstration du théorème 2) montre que $\hat{K}^n$ contient un compact $C$ tel que pour tout $g \in I^*_o(L)$ on ait

$$g(C) \cap K^n \neq \{0\} \quad ;$$

or tout $\xi \in K^n$ non nul est de la forme $\gamma(e_1)$ , avec $\gamma \in L^* = GL(n , K)$ , $e_1$ premier vecteur de base de $\hat{K}^n$ . Donc pour tout $g \in I^*_o(L)$ il existe $\gamma \in L^*$ tel que $g\gamma(e_1)$ appartienne à un compact fixe $C$ de $K^n$ . Pour tout $\varepsilon > 0$ définissons

$$T^\varepsilon_o : \text{matrices } t = \begin{pmatrix} t_1 & * \\ 0 & t_2 \end{pmatrix} \in T$$

$$\text{telles que } |t_1| \leqslant \varepsilon \quad , \ |t| = 1 \quad ;$$

le résultat précédent prouve que

$$I^*_o(L) = W.T^\varepsilon_o.L^*$$

pour un $\varepsilon > 0$ bien choisi. Il reste donc à montrer que

$$W.(T_o^{\varepsilon}/T_o^{\xi} \cap L^*)$$

est de volume fini dans $I_o^*(L)$ . Or la décomposition $I_o^*(L) = W.T_o$ donne une décomposition de la mesure invariante de $I_o^*(L)$ :

$$dm_o^*(g) = dm^*(w)\ dm_o^*(t) \quad \text{pour} \quad g = wt$$

où $dm_o^*(t)$ est la mesure invariante à droite de $T_o$ ; il suffit donc de prouver que $T_o^{\xi}/T_o^{\varepsilon} \cap L^*$ est de volume (invariant à droite) fini. Or $T_o$ est produit semi-direct des sous-groupes

$$H : \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-\frac{1}{n-1}} \end{pmatrix} \qquad (\lambda \in \underset{\sim}{R}^*_+)$$

$$N : \begin{pmatrix} t_1 & t_1 x \\ 0 & t_2 \end{pmatrix} \quad \text{avec} \quad \begin{cases} t_1 \in I_o^*(K) , & x \in \hat{K}^{n-1} \\ t_2 \in GL(n-1 , \hat{K}) , & |t_2| = 1 \end{cases} .$$

L'hypothèse de récurrence montre que $N/T_o' \cap L^*$ est de volume fini ; par ailleurs, la décomposition $T_o = H.N$ montre que $dm_o^* t)$ est produit de la mesure invariante de $N$ et de la mesure

$$\lambda^{(1+\frac{1}{n-1})(n-1)d}\ \frac{d\lambda}{\lambda} \quad \text{où} \quad d = [K : Q] \quad ;$$

il reste donc à prouver que

$$\int_0^{\xi} \lambda^{(1+\frac{1}{n-1})(n-1)d}\ \frac{d\lambda}{\lambda} < +\infty : \quad ,$$

ce qui est clair.

COROLLAIRE. - (Mêmes notations que dans le corollaire au théorème 2 ; mais on ne suppose plus que $L$ soit un corps gauche.) L'espace homogène $G/\Gamma$ est de volume fini.

Ce résultat a été démontré par C.-L. SIEGEL [4] à l'aide de la théorie de la réduction de Minkowski. La démonstration précédente (rédigée en Juin 1959 et inspirée d'une démonstration de A. WEIL pour les groupes orthogonaux et similaires) n'utilise

que la partie triviale de cette théorie, ainsi que les techniques standard de calcul des mesures de Haar.

## BIBLIOGRAPHIE

[1] DEURING (Max). - Algebren. - Berlin, Springer, 1935 (Ergebnisse der Mathematik, Vierter Band, 1).

[2] FUJISAKI (Genjiro). - On the zeta-function of the simple algebra over the field of rational numbers, J. Fac. Sc. Univ. Tokyo, Sect. 1, t. 7, 1954-58, p. 567-604.

[3] SIEGEL (Carl Ludwig). - Discontinuous groups, Annals of Math., Series 2, t. 44, 1943, p. 674-689.

[4] TATE (John). - Fourier analysis in number fields and Hecke's zeta-functions [Ce travail a été publié récemment sous forme multigraphiée] (Thèse Sc. math. Princeton University. 1950).

[5] ZARISKI (O.) and SAMUEL (P.). - Commutative algebra. Princeton, D. Van Nostrand, 1958.