SÉMINAIRE N. BOURBAKI

ROGER GODEMENT

Les travaux de E. Hecke, I

Séminaire N. Bourbaki, 1954, exp. n° 51, p. 13-19

<http://www.numdam.org/item?id=SB_1951-1954__2__13_0>

Séminaire BOURBAKI
(Décembre 1951)

LES TRAVAUX DE E. HECKE, I,

par Roger GODEMENT.

On se propose, dans cet exposé et les nombreux autres qui le suivront, de donner une idée de l'oeuvre de HECKE, relative à la théorie des nombres algébriques, à celle des fonctions modulaires, et aux rapports de ces deux théories entre elles. Cela n'implique pas que tous les résultats dont on parlera sont dûs à HECKE (contre-exemple : le théorème des unités dans les corps algébriques).

Dans ce premier exposé on va donner des résultats préliminaires destinés à conduire à la théorie des séries L (équation fonctionnelle).

1. Sommes de Gauss.

1. Classes modulo $\mathfrak{m}$. - Soient K un corps de nombres algébriques, A l'anneau des entiers de K, $\mathfrak{J}$ le groupe multiplicatif des idéaux (fractionnaires) non nuls de K, $\mathfrak{P}$ le sous-groupe des idéaux principaux de K. On sait que $G = \mathfrak{J}/\mathfrak{P}$ est un groupe fini, dont l'ordre se désigne par h. Pour $\mathfrak{a}, \mathfrak{b} \in \mathfrak{J}$, on écrit $\mathfrak{a} \sim \mathfrak{b}$ si $\mathfrak{a}$ et $\mathfrak{b}$ appartiennent à la même classe modulo $\mathfrak{P}$; cela veut dire qu'il existe $x, y \in A$ non nuls tels que $x.\mathfrak{b} = y.\mathfrak{a}$. Pour éviter des confusions par la suite, les classes modulo $\mathfrak{P}$ seront appelés grandes classes. Il est facile de voir que toute grande classe contient des idéaux entiers et même des idéaux entiers premiers à $\mathfrak{m}$, $\mathfrak{m}$ entier donné à l'avance.

Soit $\mathfrak{m}$ un idéal entier donné une fois pour toutes. Désignons par $\mathfrak{J}(\mathfrak{m})$ le sous-groupe des idéaux de la forme $\mathfrak{a}/\mathfrak{b}$ avec $\mathfrak{a}, \mathfrak{b}$ entiers premiers à $\mathfrak{m}$, et par $\mathfrak{P}(\mathfrak{m})$ le sous-groupe des idéaux principaux de la forme x/y où $x, y \in A$ sont $\equiv 1$ modulo $\mathfrak{m}$; il est clair que $\mathfrak{P}(\mathfrak{m})$ est un sous-groupe de $\mathfrak{J}(\mathfrak{m})$; la relation d'équivalence correspondante dans $\mathfrak{J}(\mathfrak{m})$ sera notée $\mathfrak{a} \sim \mathfrak{b}\ (\mathfrak{m})$; elle signifie encore qu'on a une relation $x.\mathfrak{b} = y.\mathfrak{a}$ avec x, y entiers, premiers à $\mathfrak{m}$, et $x \equiv y\ (\mathfrak{m})$; on parlera de classes modulo $\mathfrak{m}$. Le groupe $G(\mathfrak{m}) = \mathfrak{J}(\mathfrak{m})/\mathfrak{P}(\mathfrak{m})$ est aussi un groupe fini, d'ordre $h(\mathfrak{m})$.

Soit $\mathfrak{m}'$ un diviseur de $\mathfrak{m}$; tout idéal premier à $\mathfrak{m}$ l'est à $\mathfrak{m}'$, et $x \equiv 1\ (\mathfrak{m})$ implique $x \equiv 1\ (\mathfrak{m}')$; donc il existe un homomorphisme canonique, naturel et permis de $G(\mathfrak{m})$ dans $G(\mathfrak{m}')$; il n'est pas difficile de voir que :

1° cet homomorphisme applique $G(\mathfrak{m})$ sur $G(\mathfrak{m}')$;

2° si $\mathfrak{m}'$ et $\mathfrak{m}''$ sont deux diviseurs de $\mathfrak{m}$, et si $\mathfrak{m}'''$ est leur plus grand

commun diviseur , le noyau de $G(\mathfrak{m}) \longrightarrow G(\mathfrak{m}'')$ est (en tant que sous-groupe) engendré par les noyaux de $G(\mathfrak{m}) \longrightarrow G(\mathfrak{m}')$ et $G(\mathfrak{m}) \longrightarrow G(\mathfrak{m}'')$.

Si H est un sous-groupe quelconque de $G(\mathfrak{m})$ l'ensemble des diviseurs $\mathfrak{m}'$ de $\mathfrak{m}$ tels que H contienne le noyau de $G(\mathfrak{m}) \longrightarrow G(\mathfrak{m}')$ admet donc un <u>plus grand</u> élément, savoir le plus grand commun diviseur des $\mathfrak{m}'$ en question ; on l'appelle le <u>conducteur</u> de H , notation $\mathfrak{F}(H)$.

2.<u>Caractères modulo</u> $\mathfrak{m}$. - Si χ est un caractère de $G(\mathfrak{m})$ on note $\chi(\alpha)$ sa valeur sur la classe de α modulo $\mathfrak{m}$, en convenant de prendre $\chi(\alpha) = 0$ lorsque α est <u>entier</u> non premier à $\mathfrak{m}$ (l'expression 0/0 présentant des propriétés pathologiques, on ne peut pas définir de façon naturelle $\chi(\alpha)$ pour α non entier non dans $\mathfrak{J}(\mathfrak{m})$). On obtient ainsi les caractères modulo $\mathfrak{m}$. On a évidemment les propriétés suivantes où il s'agit d'idéaux premiers à $\mathfrak{m}$;

$$\chi(\alpha \cdot b) = \chi(\alpha) \cdot \chi(b) \quad ; \quad |\chi(\alpha)| = 1 \quad ;$$
$$\alpha \sim b \quad (\mathfrak{m}) \text{ implique } \chi(\alpha) = \chi(b) \ .$$

Si H est le sous-groupe de $G(\mathfrak{m})$ sur lequel χ prend la valeur 1, on note $\mathfrak{F}(\chi)$ le conducteur de H ; on peut alors regarder χ comme un caractère de $G(\mathfrak{F}(\chi))$ vu que ce groupe est canoniquement isomorphe à $G(\mathfrak{m})/H$. On dit que χ est un caractère <u>propre</u> modulo $\mathfrak{m}$ si $\mathfrak{F}(\chi) = \mathfrak{m}$; cela veut dire que pour tout diviseur non trivial $\mathfrak{m}'$ de $\mathfrak{m}$ il existe α entier vérifiant

$$\alpha \text{ premier à } \mathfrak{m} \ ; \ \alpha \sim (1) \ (\mathfrak{m}') \ ; \ \chi(\alpha) \neq 1 \ .$$

Si χ est un caractère modulo $\mathfrak{m}$, on pose $\chi(x) = \chi((x))$ pour x entier ; on a évidemment les propriétés suivantes :

$$\chi(xy) = \chi(x)\chi(y) \quad ; \quad \chi(x) = 1 \text{ si } x \text{ premier à } \mathfrak{m} \ ;$$
$$x \equiv y \ (\mathfrak{m}) \text{ implique } \chi(x) = \chi(y) \ ;$$
$$\chi(\varepsilon) = 1 \text{ pour toute unité de } K \ .$$

3. <u>Sommes de Gauss</u>. - Soient σ_i $(1 \leq i \leq n)$ les divers isomorphismes de K sur $\mathbb{Q}$; on note $T(x) = \sum \sigma_i(x)$ la trace d'un $x \in K$. Rappelons que les $x \in K$ tels que $T(xy)$ soient entier pour tout y entier forment l'inverse d'un idéal entier ∂ de K (<u>différente</u> de K) ; plus généralement, pour tout idéal α , l'idéal $1/\alpha \cdot \partial$ est l'ensemble des x tels que $T(xy)$ soit entier pour tout $y \in \alpha$. Si (y_i) est une base de α , $1/\alpha \cdot \partial$ admet une base (x_i) telle que $T(x_i\, y_j) = \delta_{ij}$ (base supplémentaire, ou duale, par rapport à la forme bilinéaire $T(xy)$) .

Soit χ un caractère modulo $\mathfrak{m}$. Si α est entier premier à $\mathfrak{m}$, et si $x \in 1/\alpha.\mathfrak{m}.\mathfrak{d}$ on a $xy \in 1/\mathfrak{d}$ dès que $y \in \alpha.\mathfrak{m} = \alpha \cap \mathfrak{m}$; il s'ensuit immédiatement que pour $y \in \alpha$ l'expression $\exp(T(xy))$ (où l'on pose en général $\exp(z) = e^{2\pi i z}$) ne dépend que de la classe de y modulo $\mathfrak{m}$ (pourvu que $x \in 1/\alpha.\mathfrak{m}.\mathfrak{d}$) ; comme il en est de même de $\chi(y) = \chi((y))$ on peut définir sans ambiguité le nombre

$$G(x\ ;\ \alpha) = \sum_{\substack{y \in \alpha \\ y \bmod \mathfrak{m}}} \chi(y).\exp(T(xy))\ ;$$

on va montrer que lorsque χ est un caractère <u>propre</u> modulo $\mathfrak{m}$ cette somme de Gauss est donnée par

$$(*) \qquad G(x\ ;\ \alpha) = C(\chi).\bar{\chi}(x.\mathfrak{m}.\mathfrak{d})$$

où $C(\chi)$ est indépendant de x et de α et où $\bar{\chi}$ est le caractère imaginaire conjugué de χ. Noter que $(*)$ montre que $G(x\ ,\ \alpha)$ ne dépend pas de α (modulo la condition $x \in 1/\alpha.\mathfrak{m}.\mathfrak{d}$).

DÉMONSTRATION.

a. Soit $z \in \alpha$ tel que $z.\alpha^{-1}$ soit entier premier à $\mathfrak{m}$ (ça existe car la grande classe de α^{-1} contient des idéaux entiers premiers à $\mathfrak{m}$) ; z est premier à $\mathfrak{m}$ de sorte que si y varie modulo $\mathfrak{m}$ il en est de même de yz ; donc on trouve immédiatement

$$(**) \qquad G(x\ ;\ \alpha) = \sum_{\substack{y \in (1) \\ y \bmod \mathfrak{m}}} \chi(yz).\exp(T(xyz) = \chi(z).G(xz)$$

où l'on pose

$$(***) \qquad G(x) = \sum_{\substack{y \in (1) \\ y \bmod \mathfrak{m}}} \chi(y).\exp(T(xy)) = G(x\ ;\ (1))\ ,$$

ceci supposant $x \in 1/\mathfrak{m}.\mathfrak{d}$.

b. Pour calculer $(***)$ posons $(x) = \mathfrak{b}/\mathfrak{m}.\mathfrak{d}$, avec $\mathfrak{b}$ entier, et supposons d'abord $\mathfrak{b}$ premier à $\mathfrak{m}$. Choisissons une fois pour toutes des entiers u , v tels que l'on ait des relations de la forme

$$(u) = \mathfrak{m}.\mathfrak{d}.\mathfrak{g}\ ,\quad (v) = \mathfrak{g}.\mathfrak{h}\ ,\ \text{avec}\ \mathfrak{g},\mathfrak{h}\ \text{entiers premiers à}\ \mathfrak{m}$$

(u , v existent : choisir $\mathfrak{g}$ dans la grande classe de $(\mathfrak{m}.\mathfrak{d}.)^{-1}$ etc.) et posons $w = ux$; on a $(w) = \mathfrak{b}.\mathfrak{g}$ de sorte que w est premier à $\mathfrak{m}$; donc il existe w' entier tel que $ww' \equiv v(\mathfrak{m})$; w' étant aussi premier à $\mathfrak{m}$ on

peut faire dans $(* * *)$ le changement de variable $y \longrightarrow w'y$ d'où

$$G(x) = \sum \chi(w'y).\exp(T(xw'y)) \ ;$$

mais comme $\mathfrak{g}$ divise v et w on a $ww' \equiv v(\mathfrak{g})$; cette relation étant aussi vraie modulo $\mathfrak{m}$ est vraie modulo $\mathfrak{m}.\mathfrak{g}$; donc on a

$$w'x - v/u = (ww' - v)/u \ , \quad \mathfrak{m}.\mathfrak{g}/(u) = \mathfrak{m}.\mathfrak{g}./\mathfrak{m}.\mathfrak{g}.\mathfrak{d} = \mathfrak{d}^{-1} \ ,$$

en sorte que

$$\exp(T(xw'y)) = \exp(T(yv/u)) \ ;$$

par suite

$$G(x) = \chi(w') \sum \chi(y).\exp(T(yv/u)) = G_1(\chi).\chi(w') \ ;$$

mais $ww' \equiv v(\mathfrak{m})$ donne

$$G(x) = C_2(\chi).\bar{\chi}(w) = C_2(\chi).\bar{\chi}(ux) = C_2(\chi).\chi(b/\mathfrak{g}) = C_3(\chi).\bar{\chi}(b)$$

d'où finalement

$$G(x)) = C(\chi).\bar{\chi}(x.\mathfrak{m}.\mathfrak{d}) \quad .$$

Revenant à $(* *)$ on voit que $(*)$ est démontré dans le cas où $xz = b'/\mathfrak{m}.\mathfrak{d}$ avec b' premier à $\mathfrak{m}$, ce qui veut dire, comme on le voit aisément, $(x) = b/\mathfrak{a}.\mathfrak{m}.\mathfrak{d}$ avec b (et $\mathfrak{a}$) premier à $\mathfrak{m}$.

c. Reste le cas où, dans $(* * *)$, on a $(x) = b/\mathfrak{m}.\mathfrak{d}$ avec b non premier à $\mathfrak{m}$; on va montrer qu'alors $G(x) = 0$. Soit en effet $\mathfrak{r} = (b , \mathfrak{m})$ le plus grand commun diviseur de b et de $\mathfrak{m}$, et posons $b = b'.\mathfrak{r}$, $\mathfrak{m} = \mathfrak{m}'.\mathfrak{r}$; $\mathfrak{m}'$ est un diviseur non trivial de $\mathfrak{m}$; puisque χ est <u>propre</u>, il existe c entier premier à $\mathfrak{m}$ vérifiant $c \equiv (1) \ (\mathfrak{m}')$ et $\chi(c) \neq 1$; on a évidemment $c = (u)$ avec u premier à $\mathfrak{m}$ et $u \equiv 1(\mathfrak{m}')$. Comme $(u , \mathfrak{m}) = 1$ on peut dans $(* * *)^*$ faire le changement de variable $y \longrightarrow uy$, ce qui donne visiblement la relation $G(x) = \chi(u)\ G(xu)$; mais pour y entier on a $xuy = x(u - 1)y + xy$, et $x(u - 1)y \in \mathfrak{d}^{-1}$ (car de $u - 1 = \mathfrak{m}'.1$, 1 entier, résulte

$$x(u - 1)y = y.\mathfrak{m}'.1.b/\mathfrak{m}.\mathfrak{d} = y.\mathfrak{m}'.1.b'.\mathfrak{r}/\mathfrak{m}.\mathfrak{d} = y.\mathfrak{m}.1.b'/\mathfrak{m}.\mathfrak{d} = y.1.b/\mathfrak{d} \ ,$$

C.Q.F.D.)

de sorte que $\exp(T(xuy)) = \exp(T(xy))$; donc $G(xu) = G(x)$, de sorte que $G(x) = \chi(u)\ G(x)$, ce qui, avec $\chi(u) \neq 1$, prouve que $G(x) = 0$.

Si l'on revient à $(* *)$ on voit que $G(x ; \mathfrak{a}) = 0$ lorsque $x.\mathfrak{m}.\mathfrak{d}$ n'est pas premier à $\mathfrak{m}$, de sorte que $(*)$ est aussi démontré dans ce cas.

d. Il faudrait encore examiner le cas où $x = 0$ (implicitement exclu dans ce qui précède).

REMARQUE. - Le calcul explicite de $C(\chi)$ peut se faire au moins si $K = Q$ mais même dans ce cas n'est pas trivial.

2. Fonctions thêta.

4. Formule sommatoire de Poisson. - Dans R^n soit $f(x)$ une fonction continue sommable par rapport à la mesure de Lebesgue dx ; supposons que la série

$$f^{\circ}(x) = \sum_{m \in Z^n} f(x + m)$$

converge absolument et uniformément sur tout compact. C'est alors une fonction périodique, dont les coefficients de Fourier sont les nombres

$$a(m) = \int_{R^n/Z^n} \sum_{p} f(x + p)\, e^{-2\pi i(m,x)}\, dx = \int_{R^n} f(x)\, e^{-2\pi i(m,x)}\, dx$$

i.e. $a(m) = \hat{f}(m)$, où $\hat{f}$ est la transformée de Fourier de f . Si donc on suppose $\sum |\hat{f}(m)| < +\infty$, il vient la formule de Poisson

$$\sum_{m \in Z^n} f(x + m) = \sum_{m \in Z^n} \hat{f}(m).e^{2\pi i(m,x)}$$

Bien entendu on pose d'une façon générale $(x , y) = \sum x_i y_i$.

5. Fonction θ d'une forme quadratique définie positive.

, Soit $Q(x) = (Hx , x) = \sum a_{ij} x_i x_j$ $(a_{ij} = a_{ji} = \overline{a_{ij}})$ une forme quadratique strictement positive dans R^n ; on pose

$$\theta(x ; Q) = \sum_{m \in Z^n} e^{-\pi Q(x+m)} \quad ;$$

Comme Q est définie, on a une relation $Q(x) \geqslant k.(x , x)$, $k > 0$, d'où la convergence absolue et uniforme sur tout compact.

Appliquons Poisson à $f(x) = e^{-\pi Q(x)}$; on a

$$\hat{f}(m) = \int e^{-\pi(Hx,x)-2\pi i(m,x)}\, dx = \int e^{-\pi(H^{\frac{1}{2}}x,H^{\frac{1}{2}}x)-2\pi i(m,x)}\, dx$$

d'où par le changement de variable $x \longrightarrow H^{\frac{1}{2}}x$:

$$\hat{f}(m) = \det(Q)^{-\frac{1}{2}} \int e^{-\pi(x,x)-2\pi i(p,x)}\, dx \qquad (\text{où } p = H^{-\frac{1}{2}} m)$$

$$= \det(Q)^{-\frac{1}{2}} \prod_{1 \leq k \leq n} \int_{-\infty}^{+\infty} e^{-\pi t^2 - 2\pi i p_k t}.dt \ ;$$

mais on a

$$\int e^{-\pi t^2 - 2\pi i x t} dt = \int e^{-\pi[(t+ix)^2+x^2]}\, dt = e^{-\pi x^2} \int e^{-\pi t^2}\, dt = e^{-\pi x^2}$$

(N.B. il faut tout de même se méfier du changement de variable $t \longrightarrow t - ix$ ...), d'où

$$\hat{f}(m) = \det(Q)^{-\frac{1}{2}} .e^{-\pi(p,p)} = \det(Q)^{-\frac{1}{2}} .e^{-\pi(H^{-1} m, m)} \ ;$$

si donc on désigne par $Q'(x)$ la forme quadratique associée à H^{-1} il vient

$$\hat{f}(m) = \det(Q)^{-\frac{1}{2}} .e^{-\pi Q'(m)}$$

Par suite on a le développement suivant de $\theta(x\ ;\ Q)$ en série trigonométrique :

$$\theta(x\ ;\ Q) = \det(Q)^{-\frac{1}{2}} \sum_{m \in Z^n} e^{-\pi Q'(m) + 2\pi i (m,x)} \ .$$

En particulier

$$\boxed{\theta(0\ ;\ Q) = \det(Q)^{-\frac{1}{2}} .\theta(0\ ;\ Q')}$$

EXEMPLE. - Prenons $n = 1$ et $Q(x) = tx^2$, $t > 0$; d'où $Q'(x) = x^2/t$, on trouve alors la formule bien connue

$$\sum e^{-\pi n^2 t} = t^{-\frac{1}{2}} . \sum e^{-\pi n^2/t} \ .$$

REMARQUE. - Les résultats précédents marchent encore pour Q complexe, à condition que la partie réelle de Q soit définie positive.

On verra dans le prochain exposé comment l'on peut définir des séries thêta à l'aide d'un corps algébrique K et d'un caractère χ modulo $\mathfrak{m}$.

BIBLIOGRAPHIE

[1] HECKE (Erich). - Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper, Nachr. königl. Gesellschaft Wiss., Göttingen, Math.-phys. Klasse, 1917, p. 299-318.

[2] HECKE (Erich). - Vorlesungen über die Theorie der algebraischen Zahlen, 2. Aufl. - Leipzig, Akademische Verlagsgesellschaft, 1954.

[3] LANDAU (Edmund). - Über Ideale und Primideale in Idealklassen, Math. Z., t. 2, 1918, p. 52-154.