SÉMINAIRE N. BOURBAKI

CLAUDE CHEVALLEY

L'hypothèse de Riemann pour les corps de fonctions algébriques de caractéristique p, I

Séminaire N. Bourbaki, 1952, exp. n° 3, p. 17-19

<http://www.numdam.org/item?id=SB_1948-1951__1__17_0>

Séminaire BOURBAKI
(Décembre 1948)

L'HYPOTHÈSE DE RIEMANN POUR LES CORPS DE FONCTIONS ALGÉBRIQUES DE CARACTÉRISTIQUE p , I.

par Claude CHEVALLEY

On dit que R est un corps de fonctions algébriques (d'une variable) sur un corps de constantes K lorsque les conditions suivantes sont satisfaites :

a) K est un sous-corps de R , et tout élément de R qui est algébrique sur K est dans K ;

b) R contient un élément x non situé dans K (donc transcendant par rapport à K) et est algébrique de degré fini sur K(x) .

Un anneau de valuation dans R est un sous-anneau A de R , contenant K , distinct de R et tel que l'inverse de tout élément de R non situé dans A soit dans A . Les éléments de A qui n'ont pas d'inverse dans A forment alors un idéal P dans A , qui est appelé la place de l'anneau A . L'anneau A/P est un corps qu'on appelle le corps des résidus de la place P ; ce corps contient K et est algébrique de degré fini d(P) sur K ; le nombre d(P) s'appelle le degré de la place P . L'idéal P est principal ; un générateur t de cet idéal est appelé une variable uniformisante en P ; tout $x \neq 0$ de R se met, et d'une seule manière, sous la forme $ut^{\nu(P\,;\,x)}$, où $\nu(P\,;\,x)$ est un entier qui ne dépend que de x et de P (non de t), et qui s'appelle l'ordre de x en P , et où u est un élément de A non dans P . On pose $\nu(P\,;\,0) = +\infty$ et on a

$$\nu(P\,;\,xy) = \nu(P\,;\,x) + \nu(P\,;\,y) \quad ,$$

$$\nu(P\,;\,x \pm y) \geqslant \min \left\{ \nu(P\,;\,x) \ , \ \nu(P\,;\,y) \right\}$$

Les combinaisons linéaires formelles de places à coefficients entiers s'appellent les diviseurs. Un diviseur $\mathfrak{a}$ s'écrit donc sous la forme $\sum a(P)P$, les a(P) étant des entiers presque tous nuls. Le nombre $\sum_P a(P)d(P)$ s'appelle le degré du diviseur $\mathfrak{a}$ et se note $d(\mathfrak{a})$; si $\mathfrak{a}$ et $\mathfrak{b}$ sont des diviseurs, on a $d(\mathfrak{a} + \mathfrak{b}) = d(\mathfrak{a}) + d(\mathfrak{b})$. Si les nombres a(P) sont tous $\geqslant 0$, on dit que $\mathfrak{a}$ est un diviseur entier ou positif. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des diviseurs tels que $\mathfrak{a} - \mathfrak{b}$ soit positif, on dit que $\mathfrak{a}$ est multiple de $\mathfrak{b}$.

Si x est un élément $\neq 0$ de R , $\sum_P \nu(P\,;\,x)P$ est un diviseur qu'on appelle le diviseur de x et qu'on note $\mathfrak{d}(x)$; le degré de ce diviseur est toujours 0 , mais le diviseur lui-même n'est le diviseur nul que si x est dans K . On a

$\mathfrak{d}(xy) = \mathfrak{d}(x) + \mathfrak{d}(y)$. Deux diviseurs sont dits équivalents si leur différence est le diviseur d'un élément de R . On obtient ainsi une décomposition de l'ensemble des diviseurs en classes de diviseurs ; tous les diviseurs d'une même classe ont le même degré, appelé degré de la classe.

On dit qu'un élément x de R est multiple du diviseur $\mathfrak{a}$ si le diviseur de x est multiple de $\mathfrak{a}$ (ou si $x = 0$). Les multiples de $\mathfrak{a}$ forment un espace vectoriel $\mathfrak{L}(\mathfrak{a})$ de dimension finie sur K ; la dimension de cet espace se note $\ell(\mathfrak{a})$; elle ne dépend que de la classe de $\mathfrak{a}$. Le théorème de Riemann affirme que le nombre $\ell(\mathfrak{a}) + d(\mathfrak{a}) - 1$ reste borné inférieurement quand $\mathfrak{a}$ décrit l'ensemble des diviseurs de R ; si on désigne son minimum par $-g$, g est appelé le genre du corps R ; c'est un entier $\geqslant 0$. On pose $\delta(\mathfrak{a}) = \ell(-\mathfrak{a}) + d(-\mathfrak{a}) + g - 1$; cet entier est donc toujours $\geqslant 0$. Le théorème de Riemann-Roch affirme qu'il existe une classe de diviseurs, dite classe canonique, telle que, si $\mathfrak{c}$ est un diviseur de cette classe, on ait, pour tout diviseur $\mathfrak{a}$, $\delta(\mathfrak{a}) = \ell(\mathfrak{a} - \mathfrak{c})$. Les diviseurs de la classe canonique sont de degré $2g-2$.

Supposons maintenant que K soit un corps parfait, et soit L un sur-corps quelconque de K . On peut alors former un corps R(L) de fonctions algébriques dont le corps des constantes soit L et qui s'obtienne par adjonction à L des éléments de R . La structure de ce corps est uniquement déterminée quand R et L sont donnés ; le genre de R(L) est égal à celui de R . Soient P une place de R et A son anneau de valuation. Il existe alors un nombre fini de places Q de R(L) dont les anneaux de valuation contiennent A ; on dit que ces places sont les places de R(L) au-dessus de P . La somme des degrés de ces places est égale au degré de P , toute variable uniformisante en P l'est aussi en chacune de ces places. Soit $\mathfrak{a} = \sum_P a(P)P$ un diviseur de R ; si on y remplace chaque place P par la somme des places de R(L) qui se trouvent au-dessus d'elle, on obtient un diviseur de R(L) qu'on identifie souvent avec $\mathfrak{a}$ lui-même. Cette identification préserve les degrés et identifie le diviseur d'un élément x de R avec le diviseur du même x dans R(L) . Les éléments de R(L) qui sont multiples de $\mathfrak{a}$ sont les combinaisons linéaires à coefficients dans L d'éléments de R multiples de $\mathfrak{a}$. Le nombre $\ell(\mathfrak{a})$ est le même que l'on considère $\mathfrak{a}$ comme un diviseur dans R ou dans R(L) . En particulier, si L est algébriquement fermé, on voit qu'au-dessus de toute place P de R il y a exactement d(P) places de R(L) , qui sont naturellement de degré 1 .

Supposons maintenant que K soit un corps fini, dont on désignera le nombre d'éléments par q . Si une classe de diviseurs contient un diviseur entier $\mathfrak{a}$,

le nombre des diviseurs entiers de cette classe est $(q^{\ell(-\alpha)}-1)/(q-1)$. Il n'y a par ailleurs qu'un nombre fini de places (et donc aussi de diviseurs entiers) de degré donné. En s'appuyant sur ces faits et sur le théorème de Riemann, on trouve que la série

$$Z(u) = \sum u^{d(\alpha)}$$

(la somme étant étendue à tous les diviseurs entiers) converge pour $|u| < q^{-1}$ et représente une fonction rationnelle de u qui possède un pôle simple au point q^{-1} . Cette fonction est appelée la fonction dzêta du corps R . L'hypothèse de Riemann est que tous les zéros de cette fonction sont de valeur absolue $q^{-1/2}$. En comparant les fonctions dzêta de R et de $R(L)$, où L est un sur-corps fini convenable de K , on trouve qu'il existe au moins un diviseur de degré 1 , d'où on déduit que les seuls pôles de la fonction dzêta sont q^{-1} et 1 . En faisant usage du théorème de Riemann-Roch, on montre que la fonction dzêta satisfait à l'équation fonctionnelle suivante :

$$Z(1/qu) = q^{1-g}u^{2-2g}\, Z(u) \quad .$$

On peut aussi représenter (pour $|u| < q^{-1}$) la fonction dzêta par un produit infini

$$Z(u) = \Pi_P (1 - u^{d(P)})^{-1}$$

le produit étant étendu à toutes les places. On en déduit :

$$\frac{Z'(u)}{Z(u)} = u^{-1} \sum_{n=1}^{\infty} c_n u^n$$

où c_n est le nombre des places de degré 1 de $R(K_n)$ si K_n est l'extension de degré n de K . On indiquera dans la suite de cet exposé le principe de la méthode par laquelle A. WEIL est parvenu à démontrer l'inégalité $(1+q^n - c_n)^2 \leqslant (2g)^2 q^n$; l'hypothèse de Riemann résulte immédiatement de cette inégalité, car cette dernière entraîne que la série qui représente la dérivée logarithmique de $Z(u)(1-qu)$ converge pour $|u| < q^{-1/2}$.