SÉMINAIRE DE MATHÉMATIQUES

CHARLES PISOT

Fonction $\zeta(s)$ d'un corps de fonctions algébriques de caractéristique p

Séminaire de Mathématiques (Julia), tome 5 (1937-1938), exp. n° 5, p. 1-21

<http://www.numdam.org/item?id=SMJ_1937-1938__5__A5_0>

V.- K.

SEMINAIRE DE MATHEMATIQUES

Cinquième année 1937 -1938

LES FONCTIONS ALGEBRIQUES

Fonction $\zeta(s)$ d'un corps de fonctions algébriques de caractéristique p

Exposé fait par M. Charles PISOT, le lundi 16 Mai 1938

Exemplaire n° 3

Introduction

L'étude algébrique des fonctions algébriques s'est souvent développée par analogie avec la théorie des corps de nombres algébriques . Or, quoiqu'elle soit d'origine bien plus récente que cette dernière, on a constaté souvent que les résultats s'y présentaient plus simplement. On peut donc penser que l'étude algébrique des corps de fonctions algébriques, outre son intérêt propre, peut encore nous suggérer des idées pour attaquer les problèmes de la théorie des nombres .

Or, on sait toute l'importance de la fonction $\zeta(s)$ introduite par Riemann dans l'étude du corps de nombres rationnels, et généralisé plus tard par Dedekind pour tout corps de nombres algébriques . Ces fonctions sont d'une étude très difficile et beaucoup de problèmes restent encore sans réponse. La fonction $\zeta(s)$ de Riemann est définie comme fonction analytique de la variable complexe s par l'expression :

$$\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_{n=0}^{\infty} \frac{1}{n^s}$$

lorsque la partie réelle $\mathcal{R}(s) > 1$, p parcourant tous les nombres premiers. On montre que $\zeta(s)$ est régulier et uniforme dans tout le plan des s , sauf au point $s = 1$ où il y a un pôle simple de résidu $+1$. Si l'on fixe la partie réelle de s , $\zeta(s)$ est presque-périodique . La fonction

$$\xi(s) = \frac{s(s-1)}{2}\, \pi^{-\frac{s}{2}}\, \Gamma\left(\frac{s}{2}\right)\, \zeta(s)$$

est une fonction entière invariante par le changement de s en $1-s$. $\xi(s)$ s'annule pour $s = -2, -4, \ldots$; elle n'a aucun zéro à partie réelle ≥ 1 comme le montre immédiatement le produit infini. En exceptant les zéros réels et négatifs, on montre que $\xi(s)$ a une infinité de zéros dans la "bande critique" $0 < \Re(s) < 1$ symétriques deux à deux par rapport à la droite $\Re(s) = \frac{1}{2}$ et par rapport à l'axe réel. Il n'y a pas de zéros sur les deux droites limites $\Re(s) = 0$ et $\Re(s) = 1$ et ce théorème est équivalent au théorème des nombres premiers qui dit que le nombre de nombres premiers inférieurs à N est asymptotiquement équivalent à $\frac{N}{\log N}$. Le nombre $N(T)$ de zéros de $\xi(s)$ dont la partie imaginaire est comprise entre 0 et T est

$$N(T) = \frac{1}{2\pi}\, T \log T \;-\; \frac{1+\log 2\pi}{2\pi}\, T + \mathcal{O}(\log T)$$

On sait même qu'il y a une infinité de zéros sur la droite $\Re(s) = \frac{1}{2}$ et que leur nombre est supérieur à cT, c étant une certaine constante. La célèbre "hypothèse de Riemann" consiste à affirmer que tous les zéros de $\xi(s)$ de la bande critique se trouvent sur la droite $\Re(s) = \frac{1}{2}$. La démonstration de cette hypothèse permettrait d'approfondir considérablement nos connaissances sur les nombres premiers, mais malgré tous les efforts faits dans ce sens, on n'a pas encore pu y parvenir.

Dedekind a généralisé la fonction $\zeta(s)$ à un corps de nombres algébriques k de la façon suivante :

$$\zeta(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{|\mathfrak{p}|^s}} = \sum_{\mathfrak{a}} \frac{1}{|\mathfrak{a}|^s}$$

$\mathfrak{p}$ parcourant tous les idéaux premiers de k et $\mathfrak{a}$ tous les idéaux entiers . $|\mathfrak{a}|$ est la norme de l'idéal $\mathfrak{a}$, c'est à-dire le nombre de classes d'entiers de k différents mod. $\mathfrak{a}$ Cette fonction $\zeta(s)$ jouit de propriétés analogues à la fonction de Riemann . Son intérêt principal consiste dans la relation qui la lie au nombre h de classes d'idéaux . Rappelons que l'on dit que deux idéaux appartiennent à une même classe si leur quotient est un nombre de k . Le résidu de $\zeta(s)$ au pôle $s=1$ est alors ah , a étant une constante dépendant des unités et du discriminant de k . Cette fonction $\zeta(s)$ de Dedekind est encore plus compliquée que celle de Riemann et on ne sait même pas s'il y a une infinité de zéros sur la droite $\mathcal{R}(s) = \frac{1}{2}$.

La fonction de Dedekind nous montre comment on peut passer à une fonction $\zeta(s)$ relative à un corps K de fonctions algébriques . En effet, ce qui correspond à un idéal, c'est un diviseur entier . Nous chercherons alors à définir la norme $|A|$ d'un diviseur entier A de façon analogue à celle d'un idéal . Les entiers du corps devront être remplacés par les éléments de K entiers par rapport à A , c'est à

dire dont le diviseur dénominateur ne contient aucun diviseur premier figurant dans A . En particulier, soit P un diviseur premier de K, u une uniformisante locale correspondant à P, tout élément z de K entier par rapport à P, peut se mettre sous la forme $z = \alpha_0 + \alpha_1 u + \ldots$ ne contenant aucune puissance négative de u , $\alpha_0, \alpha_1, \ldots$ appartenant à une extension k^* finie du corps k des constantes de K . On a alors $z \equiv \alpha_0 \pmod{P}$ et il y a autant de classes (mod P) de tels éléments z qu'il y a d'éléments dans le corps k^* . Pour que ce nombre ne soit pas infini et que l'on puisse définir convenablement $|P|$ il faudra supposer k^* formé d'un nombre fini d'éléments. Il faut par suite que k^* , et donc k , soient de caractéristique $p \neq 0$, et il suffit que k soit lui-même formé d'un nombre fini $q = p^{\ell}$ d'éléments. Si f est alors le degré $(k^* : k)$ de l'extension k^* / k c'est-à-dire par définition le degré de P , il y aura q^f classes (mod P) d'éléments de K entiers par rapport à P et nous conviendrons de poser

$$|P| = q^f$$

De façon générale, n étant le degré du diviseur entier A, nous poserons $|A| = q^n$. Avec ces conventions, nous définirons formellement

$$\zeta(s) = \prod_P \frac{1}{1 - \frac{1}{|P|^s}} = \sum_A \frac{1}{|A|^s}$$

P parcourant tous les diviseurs premiers de K, et A tous les diviseurs entiers .

Ces fonctions $\zeta(s)$ ont été étudiées pour la première fois par M.Artin dans sa thèse en 1924, dans le cas où K était un corps de fonctions hyperelliptiques. Sa définition non invariante par les transformations birationnelles de K , a été remplacée par celle que nous venons de donner par M. F.K Schmidt en 1931 et étendue par là à un corps K quelconque. Nous allons étudier cette fonction $\zeta(s)$ et nous verrons que l'analogie avec les fonctions de Riemann et de Dedekind est très grande, tout en étant bien plus simple que ces dernières fonctions . On peut d'ailleurs en déduire des résultats analogues pour le nombre de diviseurs premiers et le nombre de classes de diviseurs du corps K . Mais , il y a plus, et c'est là un résultat découvert par M.Hasse, dans le cas où K est de genre $g=1$, on peut démontrer l'hypothèse de Riemann et montrer ainsi que tous les zéros se trouvent sur la droite $\mathcal{R}(s) = \frac{1}{2}$. La démonstration consiste essentiellement à établir l'identité entre un polynôme du second degré, dont dépendent les zéros de $\zeta(s)$ dans ce cas, et l'équation du second degré vérifiée par un méromorphisme particulier Π de K , celui qui transforme tout élément de K en sa puissance $q^{\text{ième}}$. On obtient ainsi une signification des zéros de la fonction $\zeta(s)$ qui peut nous

suggérer des tentatives semblables dans l'étude des fonctions de Riemann et de Dedekind .

Les diviseurs de K.

Pour étudier la fonction $\zeta(s)$ nous sommes conduits à examiner d'abord les diviseurs entiers d'un corps K dont le corps de constantes k est de caractéristique $p \neq 0$ et ne contient qu'un nombre fini $q = p^{\ell}$ d'éléments . Un tel corps est une extension finie de degré ℓ du corps des entiers (mod p) et par suite, est parfait .

Le nombre de diviseurs entiers d'un degré n donné est fini .

En effet, soit $A = \prod_i P_i^{e_i}$ un diviseur entier de degré n . Si f_i est le degré de P_i , on a donc $n = \sum_i e_i f_i$ avec $e_i \geq 0$. Soit z une fonction de K . Si P_i figure au diviseur dénominateur de z , $\frac{1}{z^{e_i}}$ est divisible par P_i . Si P_i ne figure pas au diviseur dénominateur de z , il y a un polynôme $c_i(z)$ de $k[z]$ de degré au plus $e_i f_i$ divisible par $P_i^{e_i}$. Donc, A divise le diviseur d'un élément de la forme $(\frac{1}{z})^{e} c(z)$ où $e \leq n$ et où $c(z)$ est un polynôme en z de degré au plus égal à n-e . Or k n'ayant qu'un nombre fini d'éléments, le nombre d'éléments de la forme précédente est fini et par suite aussi le nombre de diviseurs entiers A qui les divisent .

Le nombre des classes de diviseurs de degré 0 est fini. Nous désignons ce nombre par h .

Soit encore z une fonction de K et $m = (K:k(z))$. Prenons $n = \overline{n}\, m$ multiple de m suffisamment grand pour que $n \geq 2g - 2$, g étant le genre de K . Le diviseur numérateur d'un polynôme $c(z)$ de $k[z]$, de degré $\overline{n}$ en z , est alors exactement de degré $\overline{n}.m = n$, soit C_n ce diviseur . Désignons par C_o un diviseur de degré 0, le diviseur C_oC_n est de degré n . Comme $n \geq 2g - 2$, le théorème de Riemann-Roch nous apprend que la dimension de la classe de C_oC_n est positive, c'est-à-dire , il y a au moins un élément de K multiple de $\frac{1}{C_oC_n}$, donc dont le diviseur est de la forme $\frac{C'_n}{C_oC_n}$ où C'_n est un diviseur entier de degré n . Il en résulte que C_o appartient à la classe du diviseur $\frac{C'_n}{C_n}$ Or le nombre de tels diviseurs est fini , car C_n et C'_n sont entiers, il en est donc ainsi a fortiori du nombre de leurs classes . Nous désignerons par h le nombre fini des classes de diviseurs de degré 0 .

Les degrés des diviseurs de K sont multiples d'un certain entier d . et lorsque n est multiple de d , le nombre des classes de diviseurs de degré n est h .

Les degrés des diviseurs de K sont des nombres entiers il y a donc un diviseur B dans K dont le degré est minimum ,

soit $d > 0$, ce degré . Il en résulte que les degrés des diviseurs de K sont des multiples de d . Soit alors C_n un diviseur de degré $n = m\,d$, le diviseur $C_n B^{-m} = C_o$ sera de degré 0 . Tout diviseur C_n de K peut donc se mettre sous la forme $C_o B^m$, B étant un diviseur fixe, ce qui démontre la deuxième partie de la proposition .

Le nombre de diviseurs entiers d'une classe $\mathcal{L}$ de dimension r est $\frac{q^r - 1}{q - 1}$

Soit A un diviseur entier de la classe $\mathcal{L}$, par hypothèse le module des éléments z de K multiples de A^{-1} est de dimension r , c'est-à-dire , on a $z = \lambda_1 z_1 + \ldots + \lambda_r z_r$ avec λ_i dans k . Il y a donc $q^r - 1$ tels éléments non identiquement nuls . Or, avec z , les éléments λz , et ceux-là seulement, ont même diviseur, λ étant un élément non nul de k . Il y a donc $\frac{q^r-1}{q-1}$ diviseurs entiers dans la classe $\mathcal{L}$ donnée .

Etude analytique de la fonction $\zeta(s)$.

$\zeta(s)$ est une fonction analytique et régulière dans tout le plan des s sauf aux points 0 et 1 (mod $\frac{2\pi i}{\log q^d}$) où elle a des pôles simples avec les résidus respectifs $-\frac{h}{(q-1)\log q^d}$ et $\frac{h}{(q-1)\,q^{g-1}\log q^d}$. Elle est périodique de période $\frac{2\pi i}{\log q^d}$.

Dans la formule $\zeta(s) = \sum_A \frac{1}{|A|^s}$ où A parcourt tous les diviseurs entiers de K , nous allons faire la sommation en groupant les A d'abord par degré et ensuite par classes . Nous désignerons par $\mathcal{L}_n$ une classe de degré n et de dimension r_n . En tenant compte de ce qu'il y a h classes d'un degré donné, on aura :

$$\zeta(s) = \sum_{dn=0}^{\infty} \left(\sum_{\mathcal{L}_{dn}} \frac{q^{r_{dn}}-1}{q-1} \frac{1}{q^{dns}} \right) = \frac{1}{q-1} \sum_{dn=0}^{\infty} \left(\sum_{\mathcal{L}_{dn}} \frac{q^{r_{dn}}}{q^{dns}} \right) + \frac{h}{q-1} \cdot \frac{1}{q^{-ds}-1}$$

lorsque $\Re(s) > 1$. Les diviseurs des différentielles de K sont de degré $2g-2$, donc $2g-2$ est multiple de d . Or si $dn > 2g-2$, le théorème de Riemann-Roch nous indique que $r_{dn} = dn - g + 1$. La série $\sum_A \frac{1}{|A|^s}$ converge donc pour $\Re(s) > 1$ et on a :

$$\zeta(s) = \frac{1}{q-1} \sum_{dn=0}^{2g-2} \left(\sum_{\mathcal{L}_{dn}} \frac{q^{r_{dn}}}{q^{dns}} \right) + \frac{h}{q-1} \sum_{dn=2g-2+d}^{\infty} \frac{q^{dn-g+1}}{q^{dns}} + \frac{h}{q-1} \frac{1}{q^{-ds}-1}$$

$$\zeta(s) = U\left(\frac{1}{q^{ds}}\right) + \frac{h}{q-1} \frac{q^{g-1}}{q^{2(g-1)s}} \frac{1}{q^{d(s-1)}-1} + \frac{h}{q-1} \frac{1}{q^{-ds}-1}$$

où $U\left(\frac{1}{q^{ds}}\right)$ est un polynôme en $\frac{1}{q^s}$ de degré $2g-2$.

Le théorème énoncé s'en déduit immédiatement .

Comme la série $\sum_A \frac{1}{|A|^s}$ converge pour $\Re(s) > 1$, et représente $\zeta(s)$, il en est a fortiori ainsi pour le

produit $\prod_P \frac{1}{1-\frac{1}{|P|^s}}$. Nous en déduirons le théorème suivant:

Le corps K contient des diviseurs de degré 1 , c'est-à-dire $d = 1$.

En effet, soit k^* une extension de degré d de k k^* aura alors q^d éléments . Soit $K^* = K k^*$ le corps de fonctions algébriques correspondant . Comme le degré f de tout diviseur premier P de k est divisible par d , le corps des restes σ de $k \pmod P$ contiendra un corps isomorphe à k^* . Dans l'extension de K à K^* , σ deviendra une somme directe de d corps de degré $\frac{f}{d}$ sur k^* , donc P se décompose dans K^* en d diviseurs premiers P_i^* de degrés $\frac{f}{d}$. On a ainsi $|P_i^*| = (q^d)^{\frac{f}{d}} = q^f = |P|$ et la formule $\zeta^*(s) = \prod_P \frac{1}{1-\frac{1}{|P^*|^s}}$ montre que $\zeta^*(s) = [\zeta(s)]^d$

Or les pôles de $\zeta^*(s)$ sont aussi simples, donc $d = 1$.

La fonction $q^{(g-1)s}\,\zeta(s)$ est invariante si on change s en 1-s .

Prenons d'abord le cas du genre $g = 0$, alors $h = 1$; en effet, il n'y a pas de différentielle entière et $r_n = n+1$, donc la dimension d'une classe de degré 0 est 1. Par suite, il y a un élément de K , multiple de tout diviseur de degré 0, c'est-à-dire dont le diviseur est précisément le

diviseur de degré 0 considéré . On a donc

$$\zeta_0(s) = \sum_{n=0}^{\infty} \frac{q^{n+1}-1}{q-1} \frac{1}{q^{ns}} = \sum_{n=0}^{\infty} (1+q+\ldots+q^n) \frac{1}{q^{ns}} =$$

$$= \sum_{n=0}^{\infty} \frac{1}{q^{ns}} + \frac{q}{q^s} \sum_{n=0}^{\infty} \frac{1}{q^{ns}} + \ldots = \sum_{n=0}^{\infty} \frac{1}{q^{ns}} \sum_{n=0}^{\infty} \frac{q^n}{q^{ns}}$$

$$\zeta_0(s) = \frac{1}{1-\frac{1}{q^s}} \quad \frac{1}{1-\frac{q}{q^s}} \quad \text{et} \quad q^{-s}\zeta_0(s) = \frac{-1}{q^s-1} \quad \frac{1}{q^{1-s}-1}$$

Sous cette forme l'invariance de $q^{-s}\zeta_0(s)$ par la transformation de s en $1-s$ est en évidence .

Soit maintenant le cas $g \geq 1$. On aura :

$$q^{(g-1)s}\zeta(s) = q^{(g-1)s} U\left(\frac{1}{q^s}\right) + \frac{h}{q-1}\left[\frac{q^{(g-1)(1-s)}}{q^{-(1-s)}-1} + \frac{q^{(g-1)s}}{q^{-s}-1}\right]$$

L'invariance en question est en évidence sur le crochet . Dans le polynôme $U\left(\frac{1}{q^s}\right)$ elle résultera du théorème de Riemann-Roch . Désignons par $\mathcal{L}'_{n'}$ la classe complémentaire de $\mathcal{L}_n$, par n' son degré et par $r'_{n'}$ sa dimension . le théorème de Riemann-Roch nous apprend que $r_n = r'_{n'} + n - g + 1$ avec $n + n' = 2g - 2$, ou sous une forme plus symétrique $n - g + 1 = -(n' - g + 1)$ et $r_n - \frac{n}{2} = r' - \frac{n'}{2}$

On a

$$q^{(g-1)s} U\left(\frac{1}{q^s}\right) = \frac{q^{(g-1)s}}{q-1} \sum_{n=0}^{2g-2} \left(\sum_{\mathcal{L}_n} \frac{q^{r_n}}{q^{ns}} \right) =$$

$$= \frac{q^{\frac{g-1}{2}}}{q-1} \sum_{n=0}^{2g-2} \left(\sum_{\mathfrak{L}_n} \frac{q^{r_n - \frac{n}{2}}}{q^{(n-g+1)(s-\frac{1}{2})}} \right)$$

ce qui démontre l'invariance, le changement de s en $1-s$ faisant passer d'une classe à la classe complémentaire .

Les zéros de $\zeta(s)$.

La fonction $\zeta(s)$ ne peut s'annuler que dans la "bande critique" définie par $0 < \Re(s) < 1$.

L'invariance de $q^{(g-1)s}\ (s)$ par le changement de s en $1-s$ montre que les zéros de $\zeta(s)$ sont deux à deux symétriques par rapport à la droite $\Re(s) = \frac{1}{2}$. Il suffit donc de considérer le demi-plan $\Re(s) \geq \frac{1}{2}$. L'expression $\zeta(s) = \prod_P \left(\frac{1}{1 - \frac{1}{|P|^s}} \right)$ montre que $\zeta(s) \neq 0$ si $\Re(s) > 1$

Il en résulte donc aussi $\zeta(s) \neq 0$ pour $\Re(s) < 0$.

Le fait que $\zeta(s) \neq 0$ pour $\Re(s) = 1$ se démontre comme pour les fonctions $\zeta(s)$ de la théorie classique. Pour une fonction analytique $f(z)$ on a :

$$\lim_{z=z_0} (z-z_0) \frac{f'(z)}{f(z)} = \text{ordre de } f(z) \text{ en } z_0 .$$

ε et t étant alors des nombres réels, $\varepsilon > 0$, et k un entier positif, on peut écrire :

$$\lim_{\varepsilon=0} \varepsilon \Re \left[\frac{\zeta'(1+\varepsilon)}{\zeta(1+\varepsilon)} \right] = -1 \quad \text{et} \quad \lim_{\varepsilon=0} \varepsilon \Re \left[\frac{\zeta'(1+ikt+\varepsilon)}{\zeta(1+ikt+\varepsilon)} \right] = \lambda_k$$

λ_k étant l'ordre de la fonction $\zeta(s)$ pour $s = 1 + ikt$.

Or $$\log \zeta(s) = -\sum_P \log\left(1 - \frac{1}{|P|^s}\right) = \sum_{m=1}^{\infty} \sum_P \frac{1}{m\,|P|^{ms}}$$

En posant $s = \sigma + it$ il vient :

$$\Re\left[\frac{\zeta'(s)}{\zeta(s)}\right] = -\Re\left[\sum_{m=1}^{\infty} \sum_P \frac{\log|P|}{|P|^{ms}}\right] = -\left[\sum_{m=1} \sum_P \frac{\log|P|}{|P|^{m\sigma}} \cos(mt\log|P|)\right]$$

On peut donc écrire :

$$\frac{3}{2} - 2\lambda_1 - \frac{1}{2}\lambda_2 = \lim_{\varepsilon=0} \varepsilon\left[\sum_{m=1}^{\infty} \sum_P \frac{\log|P|}{|P|^{m(1+\varepsilon)}} \left(\frac{3}{2} + 2\cos\varphi_m + \frac{1}{2}\cos 2\varphi_m\right)\right]$$

où $\varphi_m = mt \log|P|$.

Or $$\frac{3}{2} + 2\cos\varphi_m + \frac{1}{2}\cos 2\varphi_m = (1+\cos\varphi_m)^2 \geq 0$$

donc : $$\frac{3}{2} - 2\lambda_1 - \frac{1}{2}\lambda_2 \geq 0 .$$

Si alors $\zeta(s)$ avait un zéro pour $\Re(s) = 1$, en vertu de la périodicité il y aurait aussi un zéro $1+it$ tel que $0 < t < \frac{2\pi}{\log q}$. Si alors le point $1+2it$ n'est pas un pôle, on aurait $\lambda_2 \geq 0$ et $\lambda_1 > 0$, ce qui est impossible . D'autre part, si $1+2it$ est un pôle, le point $1-it$ conjugué de $1+it$, coinciderait avec le point déduit de $1+it$ en retranchant la période $\frac{2\pi i}{\log q}$, ce serait donc un zéro double de $\zeta(s)$ et $\lambda_1 \geq 2$. $\lambda_2 = -1$. On voit qu'il y a encore impossibilité .

Jusqu'ici la théorie exposée de la fonction $\zeta_3(s)$ est tout à fait analogue à la théorie des fonctions ζ classiques . Nous allons maintenant développer d'autres résultats et nous commencerons par démontrer le fait suivant :

<u>On a</u> $\zeta_3(s) = \zeta_{3_0}(s)\, L(s)$. $\zeta_{3_0}(s)$ <u>est la fonction</u> ζ_3 <u>correspondant au genre</u> $g = 0$ <u>et</u> $L(s)$ <u>un polynôme en</u> $\frac{1}{q^s}$ <u>de degré</u> $2g$ <u>de la forme suivante :</u>

$$L(s) = 1 + \frac{N_1 - (q+1)}{q^s} + \ldots + \frac{q^g}{q^{2gs}}$$

<u>N_1 est le nombre de diviseurs entiers du 1er degré de K (ce sont des diviseurs premiers)</u>.

En effet, on a :

$$\frac{1}{\zeta_{3_0}(s)} = 1 - \frac{q+1}{q^s} + \frac{q}{q^{2s}} = \frac{q}{q^s}\,(q^{s-1}-1)(q^{-s}-1)$$

En multipliant par

$$\zeta_3(s) = \frac{1}{q-1}\sum_{n=0}^{2g-2}\left(\sum_{\mathcal{L}_n}\frac{q^{r_n}}{q^{ns}}\right) + \frac{h}{q-1}\,\frac{q^{g-1}}{q^{2(g-1)s}}\,\frac{1}{q^{s-1}-1} + \frac{h}{q-1}\,\frac{1}{q^{-s}-1}$$

on voit bien que l'on obtient un polynôme $L(s)$ en $\frac{1}{q^s}$ de degré $2g$.

Le coefficient du terme $\frac{1}{q^{2gs}}$ est $\frac{q}{q-1}\sum_{\mathcal{L}_{2g-2}} q^{r_{2g-2}} - \frac{h}{q-1}\, q^g$

Or si $\mathcal{L}_{2g-2}$ est la classe des différentielles, $r_{2g-2} = g$, tandis que pour les $h-1$ autres classes $\mathcal{L}_{2g-2}$, on a

$r_{2g-2} = g-1$. Le coefficient cherché est donc

$$\frac{q}{q-1}\, q^g + (h-1)\frac{q}{q-1}\, q^{g-1} - h\,\frac{q^g}{q-1} = q^g$$

D'autre part

$$\zeta(s) = \sum_A \frac{1}{|A|^s} = 1 + \frac{N_1}{q^s} + \ldots .$$

ce qui, avec la formule :

$$\frac{1}{\zeta_0(s)} = 1 - \frac{q+1}{q^s} + \frac{q}{q^{2s}}$$

donne l'expression indiquée pour $L(s)$.

Enfin $q^{(g-1)s}\,\zeta(s)$ et $q^{-s}\,\zeta_0(s)$ sont invariants par la transformation de s en $1-s$. Il en sera donc de même pour $q^{gs}\,L(s)$, d'où une certaine symétrie dans les coefficients de $L(s)$. Comme $\zeta_0(s) \neq 0$ quel que soit s les racines de $\zeta(s) = 0$ sont celles de $L(s) = 0$. Si l'on pose alors $z = q^{-s}$, $q^{2gs}\,L(s)$ devient un polynôme $P(z) \equiv z^{2g} - \left[N_1 - (q+1)\right] z^{2g-1} + \ldots + q^g$ de degré $2g$ en z. Nous désignerons ses $2g$ racines par $\omega_\nu = q^{\beta_\nu}$. $\zeta(s) = 0$ admet donc dans la bande critique $2g$ séries des racines les racines d'une série se déduisant de l'une d'elles par la période $\frac{2\pi i}{\log q}$. Comme on ne peut avoir ni $\Re(s) = 0$, ni $\Re(s) = 1$, on aura pour toutes les $2g$ racines $1 < |\omega_\nu| < q$ Il y a donc un exposant $\frac{1}{2} \leq \vartheta < 1$ tel que $|\omega_\nu| = q^{\vartheta}$ donc tel que $1-\vartheta \leq \Re(s) \leq \vartheta$.

On a en particulier

$$N_1 - (q+1) = -\sum_{\nu=1}^{2g} \omega_\nu \qquad \text{d'où} \quad \left|N_1 - (q+1)\right| \leq 2g\, q^{\theta} .$$

D'autre part en calculant les résidus de $\zeta(s)$ aux pôles $s = 0$ et $s = 1$ avec la forme $\zeta_0(s)\, L(s)$ $\left(L(s) = \frac{1}{q^{2gs}} \prod_{\nu=1}^{2g} (q^s - \omega_\nu) \right)$, et en les égalant aux valeurs trouvées plus haut, on obtient :

$$h = \prod_{\nu=1}^{2g} (1 - \omega_\nu) = \frac{1}{q^g} \prod_{\nu=1}^{2g} (q - \omega_\nu)$$

Ces deux formules relient les deux nombres h et N_1, caractéristiques de K, aux zéros de sa fonction $\zeta(s)$.

Fonction $\zeta^{(r)}(s)$ de l'extension $K^{(r)} = K k^{(r)}$ de k de degré r.

Le corps $k^{(r)}$ contiendra q^r éléments. Soit P un diviseur premier de degré n de K et soit d le p.g.c.d. de n et de r. Posons $n = d\, n_0$, $r = d\, r_0$, n_0 et r_0 seront premiers entre eux. Le corps des restes de K par rapport à P est une extension de degré n de k, il se décompose en somme directe de d corps de degré n_0 dans l'extension $K^{(r)}$. Donc P se décompose dans $K^{(r)}$ en d diviseurs premiers P_i, chacun de degré n_0 et on aura $|P_i| = (q^r)^{n_0} = |P|^{r_0}$ car $|P| = q^n$ et $nr_0 = rn_0 = dr_0 n_0$

On a par suite :

$$\prod_{P_1} \left(1 - \frac{1}{|P_1|^s}\right) = \left(1 - \frac{1}{|P|^{r_0 s}}\right)^d$$

Or désignons par ε les racines $r^{\text{ièmes}}$ de l'unité, alors

$$\prod_{\varepsilon} \left(1 - \frac{\varepsilon^n}{z}\right) = \left(1 - \frac{1}{z^{r_0}}\right)^d \quad , \text{ d'où}$$

$$\prod_{P_1} \left(1 - \frac{1}{|P_1|^s}\right) = \prod_{\varepsilon} \left(1 - \frac{\varepsilon^n}{q^{ns}}\right) = \prod \left(1 - \frac{1}{q^n\left(s - \frac{\log}{\log q}\right)}\right)$$

Mais $\varepsilon = e^{i\frac{2\pi}{r}\rho}$ $\rho = 0, 1, \ldots, r-1$, on en déduit :

$$\zeta^{(r)}(s) = \prod_{\rho=0}^{r-1} \zeta\left(s - \frac{2\pi i \rho}{r \log q}\right)$$

Par suite les racines se déduisent des $2g$ racines de $L(s)$ par la période $\frac{2\pi i}{r \log q}$ qui est la $r^{\text{ième}}$ partie de la période $\frac{2\pi i}{\log q}$, elles sont donc aussi connues . En particulier, elles sont dans la bande $0 < 1-\theta \leq \Re(s) \leq \theta < 1$ et est indépendant de r .

Hypothèse de Riemann dans le cas du genre $g=1$.

L'étude précédente nous a montré que pour étudier les racines de $\zeta(s) = 0$, on pouvait prendre comme corps de constantes k une extension finie quelconque du corps des entiers (mod p) . Désignons d'autre part par $\bar{K}$ un corps de

fonctions algébriques dont le corps de constantes $\bar{k}$ est algébriquement fermé, mais est toujours de caractéristique p. $\bar{k}$ contient alors une infinité d'éléments. Dans la dernière conférence, où l'on trouvera les démonstrations des faits utilisés, on a vu que si $\bar{K}$ est de genre $g=1$, il existait dans $\bar{K}$ une multiplication complexe, c'est-à-dire des transformations λ, de $\bar{K}$ en un sous-corps $\bar{K}_\lambda$ laissant fixe un certain diviseur premier $\mathcal{O}$ de degré 1. On dit que λ est alors un méromorphisme normé par rapport à $\mathcal{O}$ de K. L'ensemble de ces méromorphismes λ est isomorphe à un ordre, soit 1°) de l'ensemble des entiers rationnels, 2°) de l'ensemble des entiers d'un corps quadratique complexe, 3°) d'une algèbre de quaternions. Dans chacun de ces cas λ vérifie une équation $\lambda^2 - u\lambda + v = 0$, où u est aussi un méromorphisme normé et $v = N(\lambda)$ est le degré de l'extension $\bar{K} / \bar{K}_\lambda$.

Si $1, x, y$ est une base du module des multiples de $\mathcal{O}^{-3}$ telle que le diviseur dénominateur de x soit $\mathcal{O}^2$ et $\mathcal{O}^3$ celui de y, on aura $\bar{K} = \bar{k}(x,y)$ et cette génération de $\bar{K}$ est dite normée par rapport à $\mathcal{O}$. Soit $f(x,y)=0$ l'équation reliant x à y, ses coefficients seront dans un certain sous-corps de $\bar{k}$ à un nombre fini d'éléments, et c'est ce sous-corps que nous prendrons pour corps k. Nous désignons par K le corps algébrique, dont k est le corps de constantes, et par q le nombre des éléments de k.

La classe des différentielles de $\overline{K}$ est de dimension $g=1$, c'est-à-dire le rapport de deux différentielles entières de $\overline{K}$ est une constante de $\overline{k}$. $du = \frac{dx}{f'_y(x,y)}$ est une différentielle entière et un méromorphisme λ la transforme en une différentielle $c_\lambda du$ où c_λ est dans $\overline{k}$. On démontre alors que $c_{\lambda_1\lambda_2} = c_{\lambda_1} c_{\lambda_2}$ et $c_{\lambda_1+\lambda_2} = c_{\lambda_1} + c_{\lambda_2}$ et que d'autre part la condition $c_\lambda \neq 0$ est équivalente au fait que l'extension $\overline{K} / \overline{K}_\lambda$ est séparable .

Soit alors Π la transformation de $\overline{K}$ obtenue en remplaçant chaque élément de $\overline{K}$ par sa puissance $q^{\text{ième}}$. On obtient ainsi un corps $\overline{K}_\Pi = \overline{K}^q$ contenu dans $\overline{K}$ et Π laisse $\mathfrak{k}$ invariant, donc Π est un méromorphisme normé de $\overline{K}$. On voit facilement que l'extension $\overline{K} / \overline{K}_\Pi$ n'est pas séparable et que son degré est q . Il en résulte que $c_\Pi = 0$, et que Π vérifie une équation $\Pi^2 - \ell\Pi + q = 0$. Désignons alors par $\overline{\Pi}$ le méromorphisme conjugué normé $\ell - \Pi$ et posons $Q(z) \equiv z^2 - \ell z + q = (z-\Pi)(z-\overline{\Pi})$. D'après la définition de Π , Π est échangeable avec tout méromorphisme normé λ de $\overline{K}$, donc si $\Pi \neq \overline{\Pi}$, Π est un entier quadratique complexe . Les racines de $Q(z) = 0$ sont donc toujours de même module $q^{\frac{1}{2}}$.

Montrons maintenant l'identité de $Q(z)$ et du polynôme $P(z) \equiv z^2 - \left[N_1 - (q+1)\right] z + q$ qui provient de $\zeta(s)$.

L'hypothèse de Riemann sera alors démontrée , et cela, d'après la remarque de tout à l'heure, quel que soit le corps de constantes fini k . Pour démontrer cette identité il suffit de montrer que $Q(1) = P(1)$.

On a $Q(1) = (1-\Pi)(1-\overline{\Pi}) = N(\Pi-1)$. Or $c_\pi = 0$ et $c_1 \neq 0$ donc $c_{\pi-1} = c_\pi - c_1 \neq 0$ et l'extension $\overline{K} / \overline{K}_{\pi-1}$ est séparable . On montre que dans un tel cas , $N(\Pi-1)$ est aussi le nombre de solutions de $(\Pi-1)\, P = \mathcal{O}$, c'est-à-dire le nombre de diviseurs premiers P de $\overline{K}$ transformés en $\mathcal{O}$ par le méromorphisme $\Pi-1$.

D'autre part $P(1) = N_1$ est le nombre de diviseurs premiers de degré 1 de K , c'est donc le nombre des diviseurs premiers de $\overline{K}$ de degré 1 qui sont déjà diviseurs premiers de K . Or si on a $x \equiv a \pmod P$ et $y = b \pmod P$ où a et b appartiennent à $\overline{k}$ et où P est un diviseur premier de $\overline{K}$, on a $f(a,b) = 0$. On montre que la réciproque est vraie c'est-à-dire à tout couple (a,b) de constantes de $\overline{k}$ telles que $f(a,b) = 0$ on peut associer un diviseur premier de degré 1 , P de $\overline{K}$ et un seul pour lequel $x \equiv a \pmod P$ et $y \equiv b \pmod P$. D'autre part, si $(\lambda a, \lambda b)$ est le couple correspondant aux transformés λx , λy (mod P) de x, y, par un méromorphisme normé λ , le diviseur premier correspondant à $(\lambda a, \lambda b)$ est le transformé λP de P par λ .

Si alors P est diviseur premier de K, le couple associé (a,b) est dans k, et par suite $a = a^q$, $b = b^q$, donc $(a,b) = (\pi a, \pi' b)$. Il en résulte que $P = \mathfrak{N} P$, et en vertu de la loi d'addition des méromorphismes normés $(\pi - 1) P = \mathcal{O}$. Il y a donc exactement autant de diviseurs premiers de degré 1 dans K que de solutions dans $\mathbb{K}$ de la relation $(\pi - 1) P = \mathcal{O}$, ce qui démontre l'identité associée et par suite l'hypothèse de Riemann.

En particulier, on peut identifier formellement les deux séries de zéros $\rho' = \rho_1 + \frac{2\pi i m}{\log q}$ et $\rho'' = \rho_2 + \frac{2\pi i m}{\log q}$ $(m = \ldots, -2, -1, 0, 1, 2, \ldots)$ aux deux méromorphismes π et $\bar{\pi}$ par les formules

$$\omega_1 = q^{\rho'} = \pi \quad \text{et} \quad \omega_2 = q^{\rho''} = \bar{\pi}$$

BIBLIOGRAPHIE

E.ARTIN — Quadratische Körper im Gebiet der höheren Kongruenzen I et II
Math.Zeitschr. 19 (1924) p.153-206 et 207-246

F.K.SCHMIDT — Analytische Zahlentheorie in Körpern der Characteristik p - Math.Zeitschr.33 (1931) p.1-32

H.HASSE — Uber die Kongruenzzetafunctionen
Sitzungsberichte der preus.Akad.Wiss.(1934) p.250-263

H.HASSE — Zur Theorie der abstracten elliptischen Funktionenkörper III
Journal f.d.reine u.ang.Math.175 (1936) p.193-207
