数理解析研究所講究録
41巻 1968年 18-22

楕円曲線の群法則と
ゼーターー函数

阪大　理　　本田　平

Rが単位元をもつ可換環のとき，R係数の2変数の整級数 $F(x,y)$ で

(1)　　$F(x,0)=x, \quad F(0,y)=y$

(2)　　$F(F(x,y),z)=F(x,F(y,z))$

をみたすものをR上の（1次元）形式群という。GをR上の他の形式群とするとき，R上の整級数 $f(x)=x+\cdots$ で

$$f(F(x,y))= G(f(x),f(y))$$

をみたすものがあればGはFに（強い意味で）同値であるという。Rが標数0の整域のときはFはつねに可換

(3)　　$F(x,y)=F(y,x)$

であり，Rの商体Kでは加法群 $G(x,y)=x+y$ に同値であることが知られている．従ってF（の同値類）をあたえるには

$$f(F(x,y))= f(x)+f(y)$$

となる(K係数の) f をあたえればよい。あるいはF上の不変微分形式は $f'(x)dx$ を底にもつから、Fを知ればF上の不変微分形式を知ればよいことになる。

今 Gauss の整数環 $\mathbb{Z}[\sqrt{-1}]$ 上の乗法群 $F(x,y)=x+y-\sqrt{-4}\,xy$ を考えるとF上の不変微分形式は $(1-\sqrt{-4}\,x)^{-1}dx$ である。ここで $x=t/(1+\sqrt{-1}\,t)$ なる変換をほどこすと

$$(1-\sqrt{-4}\,x)^{-1}\,dx=(1+t^2)^{-1}dt$$

となるからFは $(1+x^2)^{-1}dx$ を不変微分形式とする $\mathbb{Z}$ 上の形式群(その群法則は tan の加法定理!)に $\mathbb{Z}[\sqrt{-1}]$ 上同値である。ところで

$$(1+x^2)^{-1}dx=\sum_{n=1}^{\infty}a_n x^{n-1}dx$$

とおいてヂリクレ級数 $\sum_{n=1}^{\infty}a_n n^{-s}$ を作るとこれは $\mathbb{Q}(\sqrt{-1})$ に対応するヂリクレのL函数に他ならない。このように可換な群多様体の群法則とゼーター函数の間には密接な関係があるが、以下 $\mathbb{Q}$ 上の1次元アーベル多様体(以下楕円曲線とよぶ)についてこの関係をのべたい。

$\mathbb{Q}$ 上の楕円曲線Eの方程式は

$$(4)\quad Y^2+\lambda XY+\mu Y=X^3+\alpha X^2+\beta X+\gamma \qquad (\lambda,\mu,\alpha,\beta,\gamma\in\mathbb{Z})$$

の形にかける。Néron はEのモデルとして(4)の判別式を

出来るだけ小さくしたもの（極小モデル）が本質的に一意に存在することを示した。以下Eは(4)の極小モデルとする。無限遠点 ∞ を原点にとり，$t = X/Y$ を ∞ における局所助変数としてtでEの群法則を展開すると $\mathbb{Z}$ 上の形式群 $\hat{E}$ をうる。

p を素数としモデル(4)について $E_p = E \bmod p$ を考えるとこれは $GF(p)$ 上の代数群となるが，その単位元の連結成分は (i) E_p が特異点をもたないときは楕円曲線，(ii) E_p が結節点をもちその点での接線が（$GF(p)$上）有理的のときは $GF(p)$ 上乗法群に同型，(iii) E_p が結節点をもちその点での接線が有理的でないときは $GF(p^2)$ 上（はじめて）乗法群に同型，(iv) E_p が尖点をもつときは加法群に同型となることが知られている。この各の場合に対し E_p の局所L函数 $L_p(s)$ を次のように定義する。(i) E_p のゼーター函数の分子を $U^2 - a_p U + p$ とするとき $L_p(s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$，(ii) $L_p(s) = (1 - p^{-s})^{-1}$，(iii) $L_p(s) = (1 + p^{-s})^{-1}$，(iv) $L_p(s) = 1$。

そしてEの大局的L函数を $L(s) = \prod_p L_p(s)$ と定義する。

このとき次の定理が成立する：

［定理］ Sを条件

(*) $p \mid a_p$ かつ $a_p \neq 0$ ならば Sは p を含まない

をみたす素数の任意の集合とし，

$$L_S(s) = \prod_{p \in S} L_p(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

とおくとき $\sum_{n=1}^{\infty} a_n x^{n-1} dx$ を不変微分形式とする形式群は $\mathbb{Z}$ 係数で，$\mathbb{Z}_S$ 上 $\hat{E}$ に同値である。ここで $\mathbb{Z}_S$ は分母が S にぞくする素数でわれないような有理数全体の作る環とする。

（注意：$p \mid a_p$ かつ $a_p \neq 0$ が起きるのは $p=2$ または 3 の場合にかぎり，このとき $L_p(s) = 1 \pm p^{1-s} + p^{1-2s}$ となることが Riemann 予想から容易にたしかめられる。条件(*)を除いても定理は正しいと予想されるがまだ証明は出来ていない。）

この定理は保型函数で一意化される代数曲線のゼーター函数に関する Eichler－志村の定理から着想を得たもので，局所的または大局的整数環上ある種の重要な形式群の具体的な構成をあたえる一般的な定理から導かれるのであるが，ここではその詳細は省く。この定理は，楕円曲線の L 函数の係数がその楕円曲線の群法則の 1 つの標準形をあたえることを述べるもので，また S は（条件(*)があれば）任意でよいことから楕円曲線の群法則がその局所整数環上の群法則のいわば"直積"になっていることを示すものである。これからいくつかの興味ある結果が得られ，またいくつかの問題が生ずる。たとえば E_1 と E_2 を $\mathbb{Q}$ 上の楕円曲線とするとき，$\hat{E}_1$ と $\hat{E}_2$ が $\mathbb{Z}$ 上同値（あるいは isogenous）のとき E_1 と E_2 の間にはどのような関係があるのであろうか？ これなどはアー

ベル多様体の準同型に関するTate予想とも関連して解明が待たれる問題である。

以上