数理解析研究所講究録
589巻 1986年 79-92

On some properties of the universal power series for Jacobi sums

Yasutaka Ihara (伊原康隆) 東大・理 ★

In our previous work [PGC], we associated to each element ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ an ℓ-adic power series $F_\rho(u,v)$ in two variables and studied its connection with Jacobi sums, Coleman power series etc., as a first step in the study of the Galois representation in $\mathrm{Aut}\,\pi_1^{\text{pro-}\ell}(\mathbb{P}^1 \setminus \{0,1,\infty\})$. In this paper, we shall prove some symmetricity properties of the power series F_ρ (for $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{\ell^\infty}))$), in particular, $\mathfrak{S}_4$-symmetricity of the amalgamated product

$$F_\rho(u,v)F_\rho(u',v') \in \mathbb{Z}_\ell[[u,v,u',v']]/[(1+u)(1+v)(1+u')(1+v')-1].$$

This is based on the corresponding $\mathfrak{S}_4$-symmetricity of Jacobi sums on 4 parameters $a,b,a',b' \in (\mathbb{Z}/\ell^n)$ with $a+b+a'+b'=0$ $(n \geqslant 1)$; cf. Theorem A_1 below. As a consequence, we conclude that, although there are $m+1$ coefficients of $F_\rho(u,v)$ in degree m, they are "essentially the same" for each m (Theorem A_2).

This study was motivated by a recent communication with P.Deligne, who explained me his idea to use amalgamation of two copies of $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\})$ along $\pi_1(S^1)$ (in the context of algebraic geometry) to obtain a similar type of restriction to the Galois image in $\mathrm{Aut}\,\pi_1^{\text{pro-}\ell}(\mathbb{P}^1 \setminus \{0,1,\infty\})$.*) In the present situation, it is carried out by arithmetical means.

The author learned that G.Anderson [A] has also obtained various results on F_ρ, including similar symmetricity, by a different method.

---

*) The author wishes to thank P.Deligne for this valuable communication.

★) この論文は，その後 行成敦・金子昌信 両氏（いずれも東大・理）によって得られた結果も加えて三人の共著として出版する予定です。

We shall present our main results in §1, and their proofs in §2. In §3, we discuss some open questions related to the image of $\rho \to F_\rho \pmod{\ell}$.

1 The main statements

Let ℓ be a fixed rational prime, Z_ℓ be the ring of ℓ-adic integers, and $\mathcal{A}$ be the commutative Z_ℓ-algebra of formal power series:

$$(1) \qquad \mathcal{A} = Z_\ell[[u,v]] = Z_\ell[[u,v,w]]/[(1+u)(1+v)(1+w)-1] ,$$

equipped with the Krull topology. An element of $\mathcal{A}$ will be denoted by $F = F(u,v)$, and also as $F(u,v,w)$ (a representative modulo the ideal $[(1+u)(1+v)(1+w)-1]$). Let $G_Q = Gal(\overline{Q}/Q)$ be the absolute Galois group over Q, $\chi : G_Q \to Z_\ell^\times$ be the ℓ-cyclotomic character describing the action of G_Q on the group μ_{ℓ^∞} of ℓ-power roots of unity in $\overline{Q}$, and let G_Q act on $\mathcal{A}$ via

$$J_\rho \; : \; 1+u \to (1+u)^{\chi(\rho)}, \quad 1+v \to (1+v)^{\chi(\rho)}, \quad 1+w \to (1+w)^{\chi(\rho)}$$

($\rho \in G_Q$). In [PGC], we constructed a continuous 1-cocycle

$$(2) \qquad G_Q \longrightarrow \mathcal{A}^\times \qquad (\rho \to F_\rho = F_\rho(u,v,w)).$$

It is unramified outside ℓ, and is "universal" for Jacobi sums on 3 parameters $a,b,c \in (Z/\ell^n)$ with $a+b+c=0$. This 1-cocycle depends on the choice of a "coordinate system ι" related to $\pi_1^{\text{pro-}\ell}(\mathbf{P}^1 \setminus \{0,1,\infty\})$ (loc.cit I§2), but its restriction to $G_{Q(\mu_{\ell^\infty})}$

$= \mathrm{Gal}(\overline{Q}/Q(\mu_{\ell^\infty}))$, which is a continuous homomorphism

(3) $$G_{Q(\mu_{\ell^\infty})} \longrightarrow 1+uvw\mathcal{A} \subset \mathcal{A}^\times ,$$

depends only on the choice of a basis $(\zeta_n)_{n\geq 1}$ of $T_\ell(\mathbb{G}_m) = \varprojlim_n \mu_{\ell^n}$ (which is subject to ℓ).

For each $F = F(u,v) \in \mathcal{A}$, define $F * F$ to be the element of

(4) $$\mathcal{A} * \mathcal{A} = Z_\ell[[u,v,u',v']] /[(1+u)(1+v)(1+u')(1+v')-1]$$

represented by the product $F(u,v)F(u',v')$. (This algebra $\mathcal{A}*\mathcal{A}$ is a sort of "completed amalgamated free product $\mathcal{A} \mathop{\hat{*}}_{Z_\ell[[w]]} \mathcal{A}$ ", but we denote it simply as $\mathcal{A}*\mathcal{A}$, for brevity of notations.) The first formulation of our theorem is as follows.

Theorem A_1. Let $\rho \in G_{Q(\mu_{\ell^\infty})}$. Then $F_\rho \in \mathcal{A}$ is symmetric in $u,v,w,$ and $F_\rho * F_\rho \in \mathcal{A}*\mathcal{A}$ is symmetric in u,v,u',v'.

We shall show that these symmetricities w.r.t. $\mathfrak{S}_3$ and $\mathfrak{S}_4$ follow from corresponding symmetricities of Jacobi sums (§2). The first symmetricity also allows a direct proof based on the definition of F_ρ . As for the second, the author learned that G.Anderson recently obtained it independently by a totally different method. Further symmetricities of Jacobi sums ($\mathfrak{S}_{r+1}$-symmetricity of the Jacobi sum on $r+1$ parameters $a_0,\ldots,a_r \in (Z/\ell^n)$ for $r \geq 4$) do not give any more new functional equations for F_ρ .

To state the second formulation of the theorem, change varibles as

(4) $\quad 1+u=\exp U,\quad 1+v=\exp V,\quad 1+w=\exp W \quad (U+V+W=0)$.

Then

<u>Theorem A_2</u> Let $\rho \in G_{Q(\mu_{\ell^\infty})}$. Then F_ρ has an expansion of the form

(5) $$F_\rho(u,v,w) = \exp \sum_{\substack{m\geq 3\\ \text{odd}}} \frac{\beta_m(\rho)}{m!}(U^m+V^m+W^m)$$

with $\beta_m(\rho) \in Z_\ell$ $(m\geq 3$, odd$)$.

This is in accordance with the results of [PGC] IV (Theorem 10 and its Corollary). Combining this with a formula of Deligne[D] (cf. also [PGC] IV) which, in our terminology, determines the coefficients of $U^{m-1}V$ and UV^{m-1} in $\log F_\rho$ (at least for $m<\ell$), we conclude that

(6) $$\beta_m(\rho) = (1-\ell^{m-1})^{-1}\chi_m(\rho)$$

for $m \geq 3$,odd (and at least for $m<\ell$). Here, χ_m is a Kummer character w.r.t. some system of circular ℓ-units of $Q(\mu_{\ell^\infty})$ ([PGC] IV). From this follows in particular that the Vandiver conjecture for ℓ ("the class number of $Q(\cos \frac{2\pi}{\ell})$ is not divisible by ℓ") is valid if and only if $\beta_m : G_{Q(\mu_{\ell^\infty})} \to Z_\ell$ is surjective for all $m = 3,5,\ldots, \ell-2$; $(\ell>3)$.

2 Proofs.

Proof of Theorem A_1. Let $(\zeta_n)_{n\geq 1}$ be the basis of $T_\ell(G_m)$ which determines the homomorphism (3) of §1. (Each ζ_n is a primitive element of μ_{ℓ^n}, and $\zeta_{n+1}^{\ell} = \zeta_n$ $(n\geq 1)$.) For each $n\geq 1$, denote by $\mathcal{L}_n$ the set of all ordered triples (a,b,c) such that $a,b,c \in (Z/\ell^n) \setminus (0)$, $a+b+c=0$, and such that at least one of a,b,c belongs to $(Z/\ell^n)^\times$. For $F = F(u,v,w) \in \mathcal{A}$ and $(a,b,c) \in \mathcal{L}_n$ $(n\geq 1)$, the special value

(1) $$F(\zeta_n^a-1,\ \zeta_n^b-1,\ \zeta_n^c-1)$$

is well-defined, because $a+b+c=0$ (and the series obviously converge. We shall first prove the following two statements (I), (II) for any $\rho \in G_{Q(\mu_{\ell^\infty})}$ and $n\geq 1$:

(I) $F_\rho(\zeta_n^a-1,\zeta_n^b-1,\zeta_n^c-1)$, for $(a,b,c)\in\mathcal{L}_n$, is symmetric in a,b,c.

(II) Let $a, a', b, b' \in (Z/\ell^n)$ be such that

$$a + a' + b + b' = 0,$$
$$b\ ,\ b' \not\equiv 0 \pmod{\ell},$$
$$a\ ,\ a' \equiv 0 \pmod{\ell},\quad \text{but}\quad a\ ,\ a' \neq 0;$$

(hence necessarily $n\geq 2$). Then

(2) $$F_\rho(\zeta_n^a-1,\zeta_n^b-1)F_\rho(\zeta_n^{a'}-1,\zeta_n^{b'}-1) = F_\rho(\zeta_n^{a'}-1,\zeta_n^b-1)F_\rho(\zeta_n^a-1,\zeta_n^{b'}-1).$$

In fact, for each fixed $n\geq 1$, we shall prove the statements of (I)(II) for all $\rho \in G_{Q(\mu_{\ell^n})}$ (resp. $G_{Q(\mu_{\ell^{n+1}})}$ when $\ell = 2$). By continuity, it suffices to prove them when ρ is a Frobenius element of a prime divisor $\mathfrak{p}$ of $Q(\mu_{\ell^n})$ such that $\mathfrak{p}\nmid\ell$. But for such ρ , $F_\rho(\zeta_n^a-1,\zeta_n^b-1,\zeta_n^c-1)$ $((a,b,c)\in\mathcal{L}_n)$ is, by Theorem 7 of [PGC] II§6, the Jacobi sum:

$$(3)\qquad F_\rho(\zeta_n^a-1,\zeta_n^b-1,\zeta_n^c-1) = -\sum_{\substack{x,y\in F_q^\times\\ x+y+1=0}} \chi_n(x)^a\chi_n(y)^b$$
$$= \frac{-1}{q-1}\sum_{\substack{x,y,z\in F_q^\times\\ x+y+z=0}} \chi_n(x)^a\chi_n(y)^b\chi_n(z)^c,$$

where $q = N(\mathfrak{p})$, F_q is the finite field $Z[\zeta_n]/\mathfrak{p}$, and $\chi_n : F_q^\times \to \mu_{\ell^n}$ is the Teichmüller character determined by

$$\chi_n(x) \equiv x^{\frac{q-1}{\ell^n}} \pmod{\mathfrak{p}} \qquad (x\in F_q^\times).$$

Note that $\chi_n(-1)=1$, because when $\ell = 2$, we assumed $\rho\in G_{Q(\mu_{\ell^{n+1}})}$ and hence $q\equiv 1 \pmod{\ell^{n+1}}$. Since the right side of (3) is symmetric in a,b,c, (I) follows.

Now, to prove (II) when ρ is a Frobenius element of $\mathfrak{p}$, let a,b,a',b' be as in (II). Then all the 4 triples

$$(a,b,-a-b),(a',b',-a'-b'),(a',b,-a'-b),(a,b',-a-b')$$

belong to $\mathcal{L}_n$, because $a+b,a'+b',a'+b,a+b'\not\equiv 0 \pmod{\ell}$; hence in particular $\neq 0$. Therefore, the formula

$$(4)\qquad F_\rho(\zeta_n^\alpha-1,\zeta_n^\beta-1) = -\sum_{\substack{x,y\in F_q^\times\\ x+y+1=0}} \chi_n(x)^\alpha\chi_n(y)^\beta$$

is valid for $(\alpha,\beta)=(a,b),(a',b'),(a',b),(a,b')$. On the other hand,

$$(5)\qquad \sum_{\substack{x,y,x',y'\in F_q^\times\\ x+y+x'+y'=0}} \chi_n(x)^a\chi_n(y)^b\chi_n(x')^{a'}\chi_n(y')^{b'}$$
$$= \sum_{z\in F_q}\left\{ \sum_{\substack{x+y=z\\ x,y\neq 0}} \chi_n(x)^a\chi_n(y)^b \cdot \sum_{\substack{x'+y'=-z\\ x',y'\neq 0}} \chi_n(x')^{a'}\chi_n(y')^{b'}\right\}.$$

Since χ_n is surjective and $a+b,a'+b'\neq 0$, the summand for $z=0$

vanishes; hence (5) is equal to the sum over $z \in F_q^\times$. The summand for each $z \in F_q^\times$ may be rewritten as

$$\sum_{\substack{x+y=-1\\ x,y\neq 0}} \chi_n(-xz)^a \chi_n(-yz)^b \cdot \sum_{\substack{x'+y'=-1\\ x',y'\neq 0}} \chi_n(x'z)^{a'} \chi_n(y'z)^{b'},$$

which is independent of z, as $a+b+a'+b'=0$. And since $\chi_n(-1)=1$, (5) is equal to

$$(5') \qquad (q-1) \sum_{\substack{x+y=-1\\ x,y\neq 0}} \chi_n(x)^a \chi_n(y)^b \cdot \sum_{\substack{x'+y'=-1\\ x',y'\neq 0}} \chi_n(x')^{a'} \chi_n(y')^{b'}$$

$$= (q-1) F_\rho(\zeta_n^a - 1, \zeta_n^b - 1) F_\rho(\zeta_n^{a'} - 1, \zeta_n^{b'} - 1).$$

Since (5) is a priori symmetric in a,b,a',b', and (4) holds for $(\alpha,\beta)=(a',b),(a,b')$, we deduce that (5') is also equal to

$$(5'') \qquad (q-1) F_\rho(\zeta_n^{a'} - 1, \zeta_n^b - 1) F_\rho(\zeta_n^{a} - 1, \zeta_n^{b'} - 1).$$

This gives the proof of (II).

$\mathfrak{S}_3$-<u>symmetricity</u>. In [PGC] II, we studied the ideals

$$(6) \qquad \mathfrak{A}_m = \left\{ F=F(u,v,w) \in \mathcal{A} \;;\; F(\zeta-1,\zeta'-1,\zeta''-1)=0, \text{for all } \zeta,\zeta',\zeta'' \in \mu_{\ell^m} \setminus \{1\} \text{ with } \zeta\zeta'\zeta''=1 \right\}$$

$(m \geq 1)$ of $\mathcal{A}$ and in particular proved that $\bigcap_{m\geq 1} \mathfrak{A}_m = (0)$ (cf. II§4(14), §1(16)). Now the property (I) proved above for all $n \leq m$ implies that if $\rho \in G_{Q(\mu_{\ell^\infty})}$ and σ is any substitution of three letters u,v,w, then

$$F_\rho(u,v,w) - F_\rho(\sigma u, \sigma v, \sigma w)$$

belongs to $\mathfrak{A}_m$. Since $m \geq 1$ is arbitrary, this must vanish. Therefore, $F_\rho(u,v,w)$, as an element of $\mathcal{A}$, is symmetric in u,v,w.

$\mathfrak{S}_4$-<u>symmetricity</u>. Let u,u',v be 3 independent variables, and define $v' \in Z_\ell[[u,u',v]]$ by the equality

$$(1+u)(1+u')(1+v)(1+v')=1.$$

(Note that v' has no constant term.) To prove the $\mathfrak{S}_4$-symmetricity of $F_\rho * F_\rho$ (for $\rho \in G_{Q(\mu_{\ell^\infty})}$), it suffices to prove that

(7) $$F_\rho(u,v)F_\rho(u',v') = F_\rho(u',v)F_\rho(u,v') \qquad (\rho \in G_{Q(\mu_{\ell^\infty})})$$

holds in $Z_\ell[[u,u',v]]$, because $\mathfrak{S}_4$ (on u,u',v,v') is generated by 3 transpositions $u \leftrightarrow v$, $u' \leftrightarrow v'$, and $u \leftrightarrow u'$. (These transpositions generate a transitive subgroup containing "$\mathfrak{S}_3$ on u,u',v", the full stabilizer of v'.) Now, to prove (7), fix ρ and put

$$\begin{aligned} G(u,u',v) &= F_\rho(u,v)F_\rho(u',v')-F_\rho(u',v)F_\rho(u,v') \\ &= \sum_{i=0}^{\infty} H_i(u,u')v^i, \end{aligned}$$

with $H_i(u,u') \in Z_\ell[[u,u']]$. Then, by (II),

$$G(\zeta_n^a-1, \zeta_n^{a'}-1, \zeta_n^b-1) = 0$$

holds as long as $a, a' \in (Z/\ell^n) \setminus (0)$, $b \in (Z/\ell^n)^\times$ and $a, a' \equiv 0 \pmod{\ell}$. (Note that $b'=-a-a'-b \not\equiv 0 \pmod{\ell}$.) So, if we fix $m \geqslant 1$ and $\alpha, \alpha' \in (Z/\ell^m) \setminus (0)$, and take $n=m+k$ $(k=1,2,\dots)$ and $a=\ell^k\alpha$, $a'=\ell^k\alpha'$ (the image of α, α' by the ℓ^k-multiplication map $(Z/\ell^m) \to (Z/\ell^n)$), then

$$G(\zeta_m^\alpha-1, \zeta_m^{\alpha'}-1, \zeta_{m+k}^b-1) = 0$$

for all $k \geqslant 1$ and $b \in (Z/\ell^{m+k})^\times$. But then, $G(\zeta_m^\alpha-1, \zeta_m^{\alpha'}-1, v)$ vanishes at $v = \zeta-1$ for infinitely many distinct values of $\zeta \in \mu_{\ell^\infty}$. By lemma 1 below, this implies that $G(\zeta_m^\alpha-1, \zeta_m^{\alpha'}-1, v) = 0$, i.e., $H_i(\zeta_m^\alpha-1, \zeta_m^{\alpha'}-1) = 0$ for each $i \geqslant 0$. This implies in particular that $H_i \in \mathfrak{A}_m$. Since $m \geqslant 1$ is arbitrary, this gives $H_i \in \bigcap_{m\geq 1} \mathfrak{A}_m = (0)$, all i. Therefore, $G = 0$. This gives (7), and hence completes the proof of Theorem A_1.

<u>lemma 1</u>. Let k be a finite extension of Q_ℓ, $\mathcal{O}$ be the ring of integers of k, and $G(u) \in \mathcal{O}[[u]]$ be a formal power series of one variable over $\mathcal{O}$. Suppose $G(\zeta-1) = 0$ for infinitely many distinct elements ζ of μ_{ℓ^∞}. Then $G = 0$.

<u>Proof</u> This is well-known, and can be verified immediately as follows. Suppose on the contrary that $G(u) = \sum_{i \geq 0} a_i u^i \neq 0$ $(a_i \in \mathcal{O})$, and let i_0 be the smallest integer ≥ 0 such that $\mathrm{ord}_k(a_{i_0}) = \mathrm{Min}_i\, \mathrm{ord}_k(a_i)$ (ord_k : the normalized additive valuation of k). Take n (≥ 1) so large that $\ell^{n-1} > i_0(\ell-1)^{-1}\mathrm{ord}_k \ell$, and let $\zeta \in \mu_{\ell^\infty}$ be of order exactly ℓ^n. Then $\mathrm{ord}_k(\zeta-1)^{i_0} = i_0(\ell^n-\ell^{n-1})^{-1}\mathrm{ord}_k \ell < 1$. But then, it is easy to see that

(8) $$\mathrm{ord}_k(a_{i_0}(\zeta-1)^{i_0}) < \mathrm{ord}_k(a_i(\zeta-1)^i), \quad \text{all } i \neq i_0.$$

Therefore, $G(\zeta-1) \neq 0$ for all such ζ, a contradiction. <u>q.e.d.</u>

<u>Proof of Theorem A_2</u>. For each $F = F(u,v) \in \mathcal{A}$ with $F(0,0) = 1$, define its logarithm by $\log F = \sum_{m \geq 1} (-1)^{m-1}(F-1)^m/m$, and consider it as an element of $Q_\ell[[U,V]]$, where $U = \log(1+u)$, $V = \log(1+v)$. The involutive automorphism of $\mathcal{A}$ defined by $1+u \to (1+u)^{-1}$, $1+v \to (1+v)^{-1}$ (i.e., $U \to -U$, $V \to -V$) is denoted by the bar sign $* \to \bar{*}$. We shall reduce Theorem A_1 to:

<u>Proposition 1</u> Let $F = F(u,v) \in \mathcal{A}$. Then the following conditions (i) (ii) are equivalent;

(i) $$F \equiv 1 \pmod{uvw},$$

$$F \cdot \bar{F} = 1,$$

$$F \text{ is symmetric in } u,v,w,$$

$$F{*}F \text{ is symmetric in } u,v,u',v';$$

(ii) $\log F$ is of the form

$$\log F = \sum_{\substack{m \geq 3 \\ \text{odd}}} \frac{\beta_m}{m!}(U^m+V^m+W^m), \tag{9}$$

where $W = -(U+V)$, $\beta_m \in \mathbb{Z}_\ell$.

Remark. As the following proof shows, (i) is also equivalent to an apparently weaker condition:

(i)' $$F \equiv 1 \pmod{uv},$$

$$F(u,v)F(u',v') \equiv F(u',v)F(u,v') \quad \mathrm{mod}[(1+u)(1+v)(1+u')(1+v')-1].$$

When $F = F_\rho$ ($\rho \in G_{\mathbb{Q}(\mu_{\ell^\infty})}$), the first two properties in (i) are proved in [PGC], and the last two are given by Theorem A_1. Thus, Theorem A_2 is reduced to Proposition 1.

Proof of Proposition 1. We shall only prove the implication (i)' $\to$ (ii) (the implication (ii)$\to$(i)$\to$(i)' is obvious). From the first congruence of (i)' follows that $\log F$ is divisible by UV. Hence $\log F$ is of the form

(10) $$-\sum_{i,j\geq 1} \frac{\beta_{ij}}{i!j!} u^i v^j ,$$

with $\beta_{ij} \in Z_\ell$. (That β_{ij} is integral follows automatically from the integrality of the coefficients of $F(u,v)$; cf.[PGC] IV§2.) So, it remains to show, from the second congruence of (i)',that β_{ij} depends only on $m = i+j$ and vanishes when m is even.

This is immediately reduced to the following

lemma 2 Let m be a positive integer, and $g(x,y)$ be a homogeneous polynomial of degree m over a field of characteristic 0. Then, if m is odd, the following two conditions (i)(ii) are equivalent;

(i) $g(x,y)$ satisfies

(*) $$g(x,0) = g(0,y) = 0,$$

(**) $$g(x,y)+g(x',y') \equiv g(x',y)+g(x,y') \mod (x+x'+y+y');$$

(ii) $g(x,y)$ is a constant multiple of $(x+y)^m-x^m-y^m$.

If m is even, the condition (i) implies $g(x,y) = 0$.

Proof The implication (ii)$\rightarrow$(i) (for m:odd) is straightforward. To prove the rest, let $g(x,y)$ satisfy (i), and write

(11) $$g(x,y) = \sum_{\substack{i,j\geq 0\\ i+j=m}} b_j x^i y^j, \quad \text{and} \quad \beta_j = i!j!b_j.$$

Then $b_0 = b_m = 0$, by (*). The congruence (**) says that the polynomial

(12) $$g(x,y) + g(x',-x-x'-y)$$

is symmetric in x,x'. Therefore, the coefficient of y^j in (12) for each j, given by the formula below, is symmetric in x,x'.

(13) $$b_j x^i + \sum_{j\le \ell\le m} b_\ell (-1)^\ell \binom{\ell}{j}(x+x')^{\ell-j}x'^{m-\ell}$$

$$= b_j x^i + \sum_{0\le p\le i}\left\{ b_{j+p}(-1)^{j+p}\binom{j+p}{j}\cdot\sum_{\mu=0}^{p}\binom{p}{\mu}x^\mu x'^{i-\mu}\right\}$$

(put $\ell = j+p$). For $\mu,\nu \geqslant 0$, $\mu+\nu = i$, the coefficient of $x^\mu x'^\nu$ in the second term of (13) is given by

(14) $$\sum_{\mu\le p\le i} (-1)^{j+p}\binom{j+p}{j}\binom{p}{\mu} b_{j+p} \qquad \text{(put } q=i-p)$$

$$= \sum_{0\le q\le \nu} (-1)^{m-q}\binom{m-q}{j}\binom{i-q}{\mu} b_{m-q} = \frac{(-1)^m}{j!\mu!\nu!}\gamma_\nu ,$$

with

(15) $$\gamma_\nu = \sum_{0\le q\le \nu} (-1)^q \binom{\nu}{q}\beta_{m-q}$$

(β_{m-q}, as in (11).) But since (13) is symmetric in x, x', (14) must be symmetric in μ, ν, unless μ or $\nu = 0$ (this exception, as we have not yet taken the first term $b_j x^i$ in (13) into account). Therefore, $\gamma_\nu = \gamma_{i-\nu}$ for all ν, with $0<\nu< i$. Therefore, $\gamma_1 = \gamma_{i-1}$ for $2\le i\le m$; hence

(16) $$\gamma_1 = \gamma_2 = \dots = \gamma_{m-1} \overset{\text{put}}{=} \gamma .$$

Moreover, the coefficients of x^i and of x'^i in (13) must be equal; hence we obtain (noting that $b_0=b_m=0$):

$$b_j = \frac{(-1)^m}{i!j!}\gamma_i \qquad (i,j>0,\ i+j=m).$$

Therefore,

(17) $$\beta_j = (-1)^m \gamma_i \quad (0 < i < m).$$

Therefore, (16) gives

(18) $$\beta_1 = \beta_2 = \dots = \beta_{m-1} \overset{\text{put}}{=} \beta.$$

Since $\beta_0 = \beta_m = 0$, we obtain

$$g(x,y) = \beta \cdot \sum_{\substack{i,j\geq 1\\ i+j=m}} \frac{x^i y^j}{i!j!} = \frac{\beta}{m!}((x+y)^m - x^m - y^m).$$

On the other hand, (15) and (18) gives $\gamma = -\beta$, and (17) gives $\beta = (-1)^m \gamma$. Therefore, $\beta = 0$ when m is even. <u>q.e.d.</u>

3 Some open questions

We have thus proved that F_ρ $(\rho \in G_{\mathbb{Q}(\mu_{\ell^\infty})})$ satisfies the equivalent conditions of Proposition 1. It is natural to ask whether these conditions characterize the image of $G_{\mathbb{Q}(\mu_{\ell^\infty})}$ in $\mathcal{A}^\times$. More plausible would be a similar characterization of the image modulo ℓ. As we have seen above, it is closely connected with the Vandiver conjecture at ℓ. It also seems to be an interesting question to construct all power series in $(\mathbb{Z}/\ell)[[u,v]]$ satisfying the conditions analogous to those of Proposition 1 (i). Here, we meet with the study of the power series $h(u) \in (\mathbb{Z}/\ell)[[u]]$ satisfying the differential equations of the form

$$D^{\ell-1}(h) - D^{\ell-1}(h)_{u=0} = h - h^\ell,$$

where $D = (u+1)\frac{d}{du}$. (Such $h(u)$ appears in the v-adic expansion of $F(u,v)$ as

$$F(u,v) = 1 + h(u)v + \dots\quad .)$$

Is there a totally different approach (e.g. from topology) to construct such power series in $(\mathbb{Z}/\ell)[[u,v]]$?

[References]

[A] G.Anderson, Letters, August-September, 1985.

[D] P.Deligne, A letter to S.Bloch, February, 1984.

[PGC] Y.Ihara, Profinite braid groups, Galois representations, and complex multiplications, (to appear in Annals of Math.)