ISSN 0914-675X

KUMAMOTO JOURNAL OF MATHEMATICS

Vol. 21

March 2008

DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
KUMAMOTO UNIVERSITY

KUMAMOTO JOURNAL OF MATHEMATICS

EDITORS

Susumu TANABÉ (Editor-in-Chief), Mikio FURUSHIMA, Yuji HAMANA,
Yoshishige HARAOKA, Hironobu KIMURA, Osamu KOBAYASHI,
Masashi MISAWA, Atsumi WATANABE

KUMAMOTO JOURNAL OF MATHEMATICS is the continuation of
KUMAMOTO JOURNAL OF SCIENCE (MATHEMATICS) Vol.1–Vol.17
and is edited by Department of Mathematics, Kumamoto University.

The paper submitted for publication should be double-spaced, and sent either on a disk, or via electronic mail to the address indicated below. The file will need to be in a TEX/LATEX/AMS-TEX file (LATEX 2_ε preferred). The author should indicate which versions of TEX and what operating system has been used to create the diskette. All figure files and any macro files used in the paper should be included. The first page should contain a short descriptive title, the name(s) of the author(s) followed by an abstract, not exceeding 200 words, which can be read independently of the paper. The AMS Mathematics Subject Classification Number for the primary and secondary subjects of the article together with several key words should appear at the bottom of the first page. The institutional affiliation and complete address (including e-mail if possible) of each author should be placed at the bottom of the last page.

Editor-in-Chief
Kumamoto Journal of Mathematics
Department of Mathematics
Faculty of Science
Kumamoto University
Kumamoto 860-8555, Japan
(e-mail: kjm@sci.kumamoto-u.ac.jp)

Kumamoto J. Math.
Vol.21 (2008), 1–9

On the Maillet determinant associated with a Dirichlet character

To the memory of Professor Kentaro Murata

Akira Endô

(Received January 31, 2008)

Abstract. The Maillet determinant associated with a Dirichlet character is considered.

1 Introduction

In this note we consider the Maillet determinant associated with a Dirichlet character. Let $m \geq 3$ be a natural number which is fixed, and a, b stand for rational integers which both are relatively prime to m. Assume that m is odd or divisible by 4. Denote by $R_m(a)$ the least positive residue of a modulo m: $a \equiv R_m(a) \pmod{m}, 1 \leq R_m(a) \leq m-1$. The Maillet determinant D_m is defined by

$$D_m = \det\Big(R_m(ab^{-1})\Big)_{a,b\in S},$$

where $S = \{1 \leq a < m/2 \mid (a,m) = 1\}$ and b^{-1} is the multiplicative inverse of b modulo m, and provides the formula for the relative class number h_m^- of the m-th cyclotomic number field K [2], [14], [16]:

$$D_m = \frac{(-m)^{\frac{\varphi(m)}{2}-1}}{Q_K} \prod_{\chi\in X^{(1)}} \prod_{p|m} \Big(1-\chi(p)\Big) h_m^-,$$

where Q_K is the unit index of K (cf. [13] Chap. 3), $\varphi(m)$ is the Euler function, $X^{(1)}$ is the set of primitive Dirichlet characters with conductors dividing m such that $\chi(-1) = -1$ and $\prod_{p|m}$ indicates the product taken over primes dividing m. Carlitz [1] and Fujisaki [6] generalized the Maillet determinant by using the Bernoulli polynomials of higher degree.

Mathematical Subject Classification (2000): 11R20 (primary); 11R29, 11C20 (secondary)

Key words: Maillet determinant, cyclotomic number field, relative class number.

On the other hand the determinant of the Demjanenko matrix, which is one having 0 and 1 as elements, also provides the formula for the relative class number of the cyclotomic number fields [8]. Tsumura [15] and Hirabayashi [10] unified the Maillet determinant and the Demjanenko matrix.

Now, denote by $R'_m(a)$ the absolutely least residue of a modulo m: $a \equiv R'_m(a) \pmod{m}, -m/2 < R'_m(a) < m/2$. Let

$$S'_m(a) = (-1)^{R'_m(a)},$$

$$T'_m(a) = \begin{cases} (-1)^{\frac{R'_m(a)}{2}} & \text{if } R'_m(a) \equiv 0 \pmod 2, \\ 0 & \text{if } R'_m(a) \equiv 1 \pmod 2, \end{cases}$$

$$U'_m(a) = \begin{cases} 0 & \text{if } R'_m(a) \equiv 0 \pmod 2, \\ (-1)^{\frac{R'_m(a)-1}{2}} & \text{if } R'_m(a) \equiv 1 \pmod 2. \end{cases}$$

Further for odd $m > 3$ denote by $R_m^{(3,k)}(a), k = 0, 1$, the residues of a modulo m which satisfy

$$-\frac{m}{3} < R_m^{(3.k)}(a) < \frac{m}{3}, \text{ or}$$

$$-\frac{2m}{3} < R_m^{(3,k)}(a) < \frac{2m}{3} \text{ and } R_m^{(3,k)}(a) \equiv k \pmod 2.$$

Let

$$S_m^{(3,0)}(a) = \frac{1}{2}(1 - (-1)^{R_m^{(3,0)}(a)}3)$$

$$= \begin{cases} -1 & \text{if } R_m^{(3,0)}(a) \equiv 0 \pmod 2, \\ 2 & \text{if } R_m^{(3,0)}(a) \equiv 1 \pmod 2, \end{cases}$$

$$U_m^{(3,1)}(a) = \begin{cases} 0 & \text{if } R_m^{(3,1)}(a) \equiv 0 \pmod 2, \\ (-1)^{\frac{R_m^{(3,1)}(a)-1}{2}} & \text{if } R_m^{(3,1)}(a) \equiv 1 \pmod 2. \end{cases}$$

2 Theorems

Let H be a subgroup of the multiplicative group $G_m = (Z/mZ)^\times$, Z being the ring of rational integers, with index n not containing -1; then H corresponds to an imaginary subfield of degree n in K. Further, let S be a subset of $\{1 \leq$

$a \leq m-1 \mid (a,m) = 1\}$ which forms a complete system of representatives of $G_m/(H,-1)$.

Now, let $B_k(x)$ be the Bernoulli polynomial of degree k: $B_1(x) = x - 1/2, B_2(x) = x^2 - x + 1/6, \ldots$. Let ψ be a real Dirichlet character modulo f, $(f,m) = 1$ and define a matrix $\Delta_{m,k,H}(\psi)$ of degree $n/2$ by

$$\Delta_{m,k,H}(\psi) = \Big(\sum_{c\in H}\sum_{d=0}^{f-1} \psi\Big(R_m(ab^{-1}c) + dm\Big) B_k\Big(\frac{R_m(ab^{-1}c)+dm}{fm}\Big)\Big)_{a,b\in S}.$$

Denote by X the set of primitive Dirichlet characters χ with conductors dividing m which satisfy $\chi(H) = 1$, and by $X^{(k)}$ the subset of X consisting of $\chi \in X$such that $\chi(-1) = (-1)^k$. For a Dirichlet character χ with conductor f_χ, let $B_{k,\chi}$ be the generalized Bernoulli number belonging to χ : $B_{k,\chi} = f_\chi^{k-1} \sum_{a=0}^{f_\chi - 1} \chi(a) B_k(a/f_\chi)$.

The following theorem can be proved in a way similar to the proof of Theorem 4 in [5] by using abelian group determinant relation:

Theorem 1. *If* $\psi(-1) = (-1)^{k'}$, *then*

$$\det \Delta_{m,k,H}(\psi) = \prod_{\chi\in X^{(k+k')}} \frac{1}{2(fm)^{k-1}} \prod_{p\mid m} \Big(1 - \chi\psi(p)p^{k-1}\Big) B_{k,\chi\psi}.$$

Let ψ_0 be the trivial character modulo f, and $\psi_D(a) = \left(\frac{D}{a}\right)$ the Kronecker character for the discriminant D of a quadratic number field.

By considering $\det \Delta_{m,1,\{1\}}(\psi)$ where $\psi = \psi_0$ with $f = 4, \psi = \psi_{-4}$, $\psi = \psi_{-8}$ and $\psi = \psi_8$ Theorem 1 together with Lemma in the next section allows us to calculate the determinants whose (a,b) entries are $R'_m(ab^{-1})$, $S'_m(ab^{-1}), T'_m(ab^{-1})$ and $U'_m(ab^{-1})$, respectively, because we see

$$R'_m(ab^{-1}) = \pm m \sum_{d=0}^{3} \psi_0\Big(R_m(a'b^{-1}) + dm\Big) B_1\Big(\frac{R_m(a'b^{-1})+dm}{4m}\Big),$$

$$S'_m(ab^{-1}) = -\psi_{-4}(m) 2 \sum_{d=0}^{3} \psi_{-4}\Big(R_m(a'b^{-1}) + dm\Big) B_1\Big(\frac{R_m(a'b^{-1})+dm}{4m}\Big),$$

$$T'_m(ab^{-1}) = -\psi_{-8}(m) \sum_{d=0}^{7} \psi_{-8}\Big(R_m(a'b^{-1}) + dm\Big) B_1\Big(\frac{R_m(a'b^{-1})+dm}{8m}\Big),$$

$$U'_m(ab^{-1}) = \pm(-1)^{\frac{m-1}{2}} \psi_8(m) \sum_{d=0}^{7} \psi_8\Big(R_m(a'b^{-1}) + dm\Big) B_1\Big(\frac{R_m(a'b^{-1})+dm}{8m}\Big),$$

where $2a \equiv \pm a' \pmod m, a' \in S$ (cf. [7], [11], [12]). When m is a power of an odd prime, these determinants have already been calculated up to sign in [3], [4].

From now on we assume that $H = \{1\}$. We obtain the following:

Theorem 2. *Assume that* $(m, 6) = 1$ *and* $H = \{1\}$.

(1) $$\det\Big(R_m^{(3,0)}(ab^{-1})\Big)_{a,b\in S} = \Big(-\frac{m}{2}\Big)^{\frac{\varphi(m)}{2}} \prod_{\chi\in X^{(1)}} \chi(2)\Big(1-\chi(3)\Big) \prod_{p|m}\Big(1-\chi(p)\Big) B_{1,\chi}.$$

(2) $$\det\Big(S_m^{(3,0)}(ab^{-1})\Big)_{a,b\in S} = \Big(\psi_{-3}(m)\frac{3}{2}\Big)^{\frac{\varphi(m)}{2}} \prod_{\chi\in X^{(0)}} \chi(6) \prod_{p|m}\Big(1-\chi\psi_{-3}(p)\Big) B_{1,\chi\psi_{-3}}.$$

(3) $$\det\Big(R_m^{(3,1)}(ab^{-1})\Big)_{a,b\in S} = \Big(-\frac{m}{2}\Big)^{\frac{\varphi(m)}{2}} \prod_{\chi\in X^{(1)}} \Big(1-\chi(2)\Big)\Big(1-\chi(3)\Big) \prod_{p|m}\Big(1-\chi(p)\Big) B_{1,\chi}.$$

(4) $$\det\Big(U_m^{(3,1)}(ab^{-1})\Big)_{a,b\in S} = \Big((-1)^{\frac{m-1}{2}}\psi_{12}(m)\frac{1}{2}\Big)^{\frac{\varphi(m)}{2}} \prod_{\chi\in X^{(1)}} \chi(3) \prod_{p|m}\Big(1-\chi\psi_{12}(p)\Big) B_{1,\chi\psi_{12}}.$$

In the particular case where $m = p > 3$ is a prime, we have the following:

Corollary. *For an integer* c *prime to* p *let* $f_p(c)$ *indicate the multiplicative order of* c *modulo* p.

(1) $\det\Big(R_p^{(3,0)}(ab^{-1})\Big) \neq 0$ *if and only if* $f_p(3) \equiv 0 \pmod 2$.

(2) $\det\Big(S_p^{(3,0)}(ab^{-1})\Big) \neq 0$ *if and only if* $p \equiv 2 \pmod 3$.

(3) $\det\Big(R_p^{(3,1)}(ab^{-1})\Big) \neq 0$ *if and only if* $f_p(2) \equiv f_p(3) \equiv 0 \pmod 2$.

(4) $\det\Big(U_p^{(3,1)}(ab^{-1})\Big) \neq 0$ *for all primes* $p > 3$.

3 Proof of Theorem 2

Let u be an integer prime to m. Then, for any $a \in S$ there exists $a' \in S$ such that $ua \equiv \pm a' \pmod{\text{m}}$; thus u induces a permutation σ_u of elements in S as follows: $ua \equiv \pm a' \pmod m, \sigma_u(a) = a' \in S$. Let μ_u be the number of $a \in S$ such that $ua \equiv -\sigma_u(a) \pmod m$, and $\mathrm{sgn}\sigma_u$ the signature of σ_u, that is, $\mathrm{sgn}\sigma_u = 1$ or -1 according as σ_u is even or odd.

Lemma. *For an integer* u *prime to* m, *we have*

$$\prod_{\chi\in X}\chi(u)=(-1)^{\mu_u}\ \textit{and}\ \prod_{\chi\in X^{(0)}}\chi(u)=\mathrm{sgn}\sigma_u.$$

Proof. The first is immediate from that $\prod_{\chi\in X}\chi(u)\equiv u^{\frac{\varphi(m)}{2}}\equiv(-1)^{\mu_u}\pmod m$, and for the second see Hirabayashi [10].

Proof of Theorem 2. (1) We consider the case $\psi=\psi_0$ with $f=3$. We have that if $3a\equiv\pm2a'\pmod m, a'=\sigma_{2^{-1}3}(a)\in S$, then

$$\begin{aligned}
&\sum_{d=0}^{2}\psi_0\Big(R_m(a'b^{-1})+dm\Big)B_1\Big(\frac{R_m(a'b^{-1})+dm}{3m}\Big)\\
&=\sum_{d=0}^{2}\psi_0\Big(R_m(a'b^{-1})+dm\Big)\Big(\frac{R_m(a'b^{-1})+dm}{3m}-\frac12\Big)\\
&=\begin{cases}\dfrac{2R_m(a'b^{-1})}{3m} & \text{if } R_m(a'b^{-1})\equiv0\pmod3,\\[2mm] \dfrac{2R_m(a'b^{-1})-2m}{3m} & \text{if } R_m(a'b^{-1})\equiv m\pmod3,\\[2mm] \dfrac{2R_m(a'b^{-1})-m}{3m} & \text{if } R_m(a'b^{-1})\equiv2m\pmod3\end{cases}\\
&=\pm\frac{R_m^{(3,0)}(ab^{-1})}{m},
\end{aligned}$$

which implies

$$\begin{aligned}
&\Big(R_m^{(3,0)}(ab^{-1})\Big)_{a,b\in S}\\
&=m\Big(\pm\sum_{d=0}^{2}\psi_0\Big(R_m(a'b^{-1})+dm\Big)B_1\Big(\frac{R_m(a'b^{-1})+dm}{3m}\Big)\Big)_{a,b\in S}.
\end{aligned}$$

Since $(-1)^{\mu_{2^{-1}3}}\mathrm{sgn}\sigma_{2^{-1}3}=\prod_{\chi\in X^{(1)}}\chi(6)$ by Lemma, it follows from Theorem 1 that

$$\begin{aligned}
&\det\Big(R_m^{(3,0)}(ab^{-1})\Big)_{a,b\in S}\\
&=m^{\frac{\varphi(m)}{2}}\prod_{\chi\in X^{(1)}}\chi(6)\det\Delta_{m,1,\{1\}}(\psi_0)\\
&=\Big(-\frac{m}{2}\Big)^{\frac{\varphi(m)}{2}}\prod_{\chi\in X^{(1)}}\chi(2)\Big(1-\chi(3)\Big)\prod_{p\mid m}\Big(1-\chi(p)\Big)B_{1,\chi},
\end{aligned}$$

because $B_{1,\chi\psi_0} = \Big(1-\chi(3)\Big)B_{1,\chi}$.

(2) In this case, $f=3$ and $\psi_{-3}(a) = \pm 1$ according as $a \equiv \pm 1 \pmod 3$ unless $a \equiv 0 \pmod 3$. We have that if $3a \equiv \pm 2a' \pmod m, a' = \sigma_{2^{-1}3}(a) \in S$, then

$$\sum_{d=0}^{2} \psi_{-3}\Big(R_m(a'b^{-1}) + dm\Big) B_1\Big(\frac{R_m(a'b^{-1})+dm}{3m}\Big)$$

$$= \frac{1}{3}\sum_{d=0}^{2} \psi_{-3}\Big(R_m(a'b^{-1}) + dm)\Big) d$$

$$= \begin{cases} -\dfrac{1}{3}\psi_{-3}(m) & \text{if } R_m(a'b^{-1}) \equiv 0, m \pmod 3, \\ \dfrac{2}{3}\psi_{-3}(m) & \text{if } R_m(a'b^{-1}) \equiv 2m \pmod 3 \end{cases}$$

$$= \frac{\psi_{-3}(m)}{3} S_m^{(3,0)}(ab^{-1}),$$

which yields

$$\Big(S_m^{(3,0)}(ab^{-1})\Big)_{a,b\in S}$$

$$= \psi_{-3}(m)3\Big(\sum_{d=0}^{2} \psi_{-3}\Big(R_m(a'b^{-1}) + dm\Big) B_1\Big(\frac{R_m(a'b^{-1})+dm}{3m}\Big)\Big)_{a,b\in S}.$$

Since $\operatorname{sgn}\sigma_{2^{-1}3} = \prod_{\chi\in X^{(0)}} \chi(6)$ by Lemma it follows from Theorem 1 that

$$\det\Big(S_m^{(3,0)}(ab^{-1})\Big)_{a,b\in S}$$

$$= \Big(\psi_{-3}(m)3\Big)^{\frac{\varphi(m)}{2}} \prod_{\chi\in X^{(0)}} \chi(6) \det \Delta_{m,1,\{1\}}(\psi_{-3})$$

$$= \Big(\psi_{-3}(m)\frac{3}{2}\Big)^{\frac{\varphi(m)}{2}} \prod_{\chi\in X^{(0)}} \chi(6) \prod_{p|m} \Big(1-\chi\psi_{-3}(p)\Big) B_{1,\chi\psi_{-3}}.$$

(3) We consider the case $\psi = \psi_0$ with $f = 12$. We have that if $3a \equiv \pm a' \pmod{12}, a' = \sigma_3(a) \in S$, then

$$\sum_{d=0}^{11} \psi_0\Big(R_m(a'b^{-1}) + dm\Big) B_1\Big(\frac{R_m(a'b^{-1})+dm}{12m}\Big)$$

$$= \sum_{d=0}^{11} \psi_0\Big(R_m(a'b^{-1}) + dm\Big)\Big(\frac{R_m(a'b^{-1})+dm}{12m} - \frac{1}{2}\Big)$$

$$= \begin{cases} \dfrac{R_m(a'b^{-1})}{3m} & \text{if } R_m(a'b^{-1}) \equiv 0 \bmod 3), \\ \dfrac{R_m(a'b^{-1}) - m}{3m} & \text{if } R_m(a'b^{-1}) \equiv m \pmod 3), \\ \dfrac{R_m(a'b^{-1}) + m}{3m} & \text{if } R_m(a'b^{-1}) \equiv 2m \pmod 6), \\ \dfrac{R_m(a'b^{-1}) - 2m}{3m} & \text{if } R_m(a'b^{-1}) \equiv 5m \pmod 6 \end{cases}$$

$$= \pm \frac{R_m^{(3,1)}(ab^{-1})}{m},$$

which implies

$$\Big(R_m^{(3,1)}(ab^{-1})\Big)_{a,b\in S}$$

$$= m\Big(\pm \sum_{d=0}^{11} \psi_0\Big(R_m(a'b^{-1}) + dm\Big) B_1\Big(\frac{R_m(a''b^{-1}) + dm}{12m}\Big)\Big)_{a,b\in S}.$$

Hence it follows from Theorem 1 and Lemma that

$$\det\Big(R_m^{(3,1)}(ab^{-1})\Big)_{a,b\in S}$$

$$= m^{\frac{\varphi(m)}{2}} \prod_{\chi\in X^{(1)}} \chi(3) \det \Delta_{m,1,\{1\}}(\psi_0)$$

$$= \Big(-\frac{m}{2}\Big)^{\frac{\varphi(m)}{2}} \prod_{\chi\in X^{(1)}} \Big(1-\chi(2)\Big)\Big(1-\chi(3)\Big) \prod_{p|m} \Big(1-\chi(p)\Big) B_{1.\chi},$$

because $B_{1,\chi\psi_0} = \Big(1-\chi(2)\Big)\Big(1-\chi(3)\Big)B_{1,\chi}$.

(4) In this case, $f = 12$ and $\psi_{12}(a) = 1$ or -1 according as $a \equiv 1, 11 \pmod{12}$ or $5, 7 \pmod{12}$ unless $(a, 12) \neq 1$. We have that if $3a \equiv \pm a', a' = \sigma_3(a) \in S$, then

$$\sum_{d=0}^{11} \psi_{12}\Big(R_m(a'b^{-1}) + dm\Big) B_1\Big(\frac{R_m(a'b^{-1}) + dm}{12m}\Big)$$

$$= \frac{1}{12} \sum_{d=0}^{11} \psi_{12}\Big(R_m(a'b^{-1}) + dm\Big) d$$

$$= \begin{cases} \psi_{12}(m) & \text{if } R_m(a'b^{-1}) \equiv 2m, 3m, 4m, 5m \pmod{12}, \\ -\psi_{12}(m) & \text{if } R_m(a'b^{-1}) \equiv 8m, 9m, 10m, 11m \pmod{12}, \\ 0 & \text{if } R_m(a'b^{-1}) \equiv 0, m \pmod 6 \end{cases}$$

$$= \pm(-1)^{\frac{m-1}{2}}\psi_{12}(m)U_m^{(3,1)}(ab^{-1}),$$

which yields

$$\Big(U_m^{(3,1)}(ab^{-1})\Big)_{a,b\in S}$$

$$= (-1)^{\frac{m-1}{2}}\psi_{12}(m)\Big(\pm\sum_{d=0}^{11}\psi_{12}\Big(R_m(a'b^{-1})+dm\Big)B_1\Big(\frac{R_m(a'b^{-1})+dm}{12m}\Big)\Big)_{a,b\in S}.$$

Therefore it follows from Theorem 1 and Lemma that

$$\det\Big(U_m^{(3,1)}(ab^{-1})\Big)_{a,b\in S}$$

$$=\Big((-1)^{\frac{m-1}{2}}\psi_{12}(m)\Big)^{\frac{\varphi(m)}{2}}\prod_{\chi\in X^{(1)}}\chi(3)\det\Delta_{m,1,\{1\}}(\psi_{12})$$

$$=\Big((-1)^{\frac{m-1}{2}}\psi_{12}(m)\frac{1}{2}\Big)^{\frac{\varphi(m)}{2}}\prod_{\chi\in X^{(1)}}\chi(3)\prod_{p|m}\Big(1-\chi\psi_{12}(p)\Big)B_{1,\chi\psi_{12}}.$$

We conclude this note by noting that the products $\det\Big(R_m^{(3,0)}(ab^{-1})\Big)\det\Big(S_m^{(3,0)}(ab^{-1})\Big)$ and $\det\Big(R_m^{(3,1)}(ab^{-1})\Big)\det\Big(U_m^{(3,1)}(ab^{-1})\Big)$, unless they vanish, give the formulae for the relative class numbers of the quadratic extensions $K(\sqrt{-3})$ and $K(\sqrt{3})$ of K, respectively.

Acknowldgement. The author thanks Professor Hirabayashi for pointing out errors in the original manuscript as well as sending a preprint of his paper [11].

References

[1] L. Carlitz, *A generalization of Maillet's determinant and a bound for the first factor of the class number*, Proc. Amer. Math. Soc. **12** (1961), 256–261.

[2] L. Carlitz and F. R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc. **6** (1955), 265–269.

[3] A. Endô, *The relative class numbers of certain imaginary abelian number fields and determinants*, J. Number Theory **34** (1990), 13–20.

[4] A. Endô, *On the Stickelberger ideal of (2,···,2)-extensions of a cyclotomic number field*, Manusc. Math. **69** (1990), 107–132.

[5] A. Endô, *A generalization of the Maillet determinant and the Demyanenko matrix*, Abh. Math. Sem. Univ. Hamburg **73** (2003), 181–193.

[6] G. Fujisaki, *A generalization of Carlitz's determinant*, Sci. Papers Coll. Arts Sci. Univ. Tokyo **40** (1990), 63–68.

[7] T. Funakura, *On Kronecker's limit formula for Dirichlet series with periodic coefficients*, Acta Arith. **55** (1990), 59–73.

[8] F. Hazama, *Demjanenko matrix, class number, and Hodge's group*, J. Number Theory **34** (1990), 174–177.

[9] M. Hirabayashi, *A generalization of Maillet and Demyanenko determinants*, Acta Arith. **85** (1998), 391–397.

[10] M. Hirabayashi, *A generalization of Maillet and Demyanenko determinants for the cyclotomic $\mathbf{Z}_p$-extensions*, Abh. Math. Sem. Univ. Hamburg **71** (2001), 15–27.

[11] M. Hirabayashi, *A determinant formula for the relative class number of an imaginary abelian number field*, preprint.

[12] S. Kanemitsu and T. Kuzumaki, *A generalization of the Maillet determinant*, in: Győry, Pethő and Sós (eds.), Number Theory–Diophantine, Computational and Algebraic Aspects, Proc. Int. Conf. Eger, Hungary 1996, Walter de Gruyter, 1998.

[13] S. Lang, *Cyclotomic Fields I and II*, Grad. Texts Math. 121, Springer-Verlag, 1990.

[14] K. Tateyama, *Maillet's determinant*, Sci. Papers College Gen. Educ. Univ. Tokyo **32** (1982), 97–100.

[15] H. Tsumura, *On Demjanenko's matrix and Maillet's determinant for imaginary abelian number fields*, J. Number Theory **60** (1996), 70–79.

[16] K. Wang, *On Maillet determinant*, J. Number Theory **18** (1984), 306–312.

Akira Endô
Department of Mathematics
Kumamoto University
Kumamoto 860-8555, Japan

Kumamoto J. Math.
Vol.21 (2008), 11-20

Logarithmic vector fields along smooth plane cubic curves

Kazushi Ueda and Masahiko Yoshinaga

(Received April 26, 2007)
(Accepted January 30, 2008)

Abstract. We study the sheaves of logarithmic vector fields along smooth cubic curves in the projective plane, and prove a Torelli-type theorem in the sense of Dolgachev–Kapranov [4] for those with non-vanishing j-invariants.

1 Introduction

K. Saito [6] introduced the notion of the sheaf of logarithmic vector fields along a divisor and proved that it is always reflexive. A divisor D in a variety S is said to be *free* if the sheaf of logarithmic vector field along D is a free $\mathcal{O}_S$-module. He proved that the discriminant in the parameter space of the semi-universal deformation of an isolated hypersurface singularity is always free.

When the ambient space is the projective space $\mathbb{P}^\ell$, an $\mathcal{O}_{\mathbb{P}^\ell}$-module is said to be free if it is the direct sum $\bigoplus_i \mathcal{O}_{\mathbb{P}^\ell}(a_i)$ of invertible sheaves. The problem of characterizing free divisors in projective spaces has attracted much attention, especially when the divisor is given as an arrangement of hyperplanes. See e.g. [7]. If a divisor in $\mathbb{P}^\ell$ is free, then the passage from the divisor to the sheaf of logarithmic vector fields causes loss of information; only the sequence $\{a_i\}_{i=1}^\ell$ of integers is left, and it is impossible to reconstruct the divisor from this finite amount of information.

In the opposite extreme, Dolgachev and Kapranov [4] asked when the the sheaf $\mathcal{T}(-\log D)$ contains enough information to reconstruct D. A divisor D in $\mathbb{P}^\ell$ is said to be *Torelli* if the isomorphism class of $\mathcal{T}(-\log D)$ as an $\mathcal{O}_{\mathbb{P}^\ell}$-module determines the divisor D. Their main result is the condition for an arrangement of sufficiently many hyperplanes in $\mathbb{P}^\ell$ to be Torelli.

In this paper, we discuss the case when $\ell = 2$ and D is a smooth cubic curve. Our main result asserts that D is Torelli precisely when the j-invariant of D is not zero. The strategy of our proof is the following:

1. The set of jumping lines of the sheaf of logarithmic vector fields along a smooth cubic curve coincides with its Cayleyan curve.

Mathematical Subject Classification (2000): 14J60 (primary); 14F05 (secondary)
Key words: logarithmic vector field, jumping line, Cayleyan curve.

2. For a smooth cubic curve with a non-vanishing j-invariant, the Cayleyan curve determines the original curve up to three possibilities.

3. The set of "jumping cubic curves" fixes this left-over ambiguity and the Torelli property holds.

4. When the j-invariant of D is zero, we can construct a family of divisors with isomorphic sheaves of logarithmic vector fields along them.

Smooth cubic curves with vanishing j-invariants provide examples of divisors which are neither free nor Torelli.

Acknowledgment: We thank Igor Dolgachev for a stimulating lecture in Kyoto in winter 2006 and Akira Ishii for valuable discussions and comments. K. U. is supported by Grant-in-Aid for Young Scientists (No.18840029). M. Y. is supported by JSPS Postdoctoral Fellowship for Research Abroad.

2 Preliminaries

2.1 de Rham–Saito's lemma

Let A be a Noetherian ring and $M = \bigoplus_{i=1}^{n} Ae_i$ be a free module over A generated by $e_1, \ldots, e_n$. For $\omega_1, \ldots, \omega_r \in M$, put

$$\omega_1 \wedge \cdots \wedge \omega_r = \sum_{1 \le i_1 < \cdots < i_r \le n} a_{i_1,\ldots,i_r} e_{i_1} \wedge \cdots \wedge e_{i_r}.$$

and define $\mathfrak{a}$ to be the ideal generated by $a_{i_1,\cdots,i_r}$ for $1 \le r \le n$ and $1 \le i_1 < \cdots < i_r \le n$. We also define as follows:

$$\begin{aligned} Z^p &= \{\varphi \in \wedge^p M \mid \omega_1 \wedge \cdots \wedge \omega_r \wedge \varphi = 0\}, \\ B^p &= \sum_{k=1}^{r} \omega_k \wedge (\wedge^{p-1} M), \\ H^p &= Z^p / B^p. \end{aligned}$$

Theorem 2.1 (de Rham–Saito's lemma [3, 5]) *(1) There exists an integer $\nu \in \mathbb{Z}_{\ge 0}$ such that $\mathfrak{a}^\nu H^p = 0$ for $0 \le p \le n$.*

(2) For $0 \le p < \operatorname{depth}_{\mathfrak{a}} A$, we have $H^p = 0$.

2.2 Sheaf of logarithmic vector fields

Let $A = \mathbb{C}[z_0, \ldots, z_\ell]$ be a polynomial ring and Der_A be the module of $\mathbb{C}$-derivations of A, which is a free module of rank $\ell + 1$;

$$\mathrm{Der}_A = \sum_{i=0}^{\ell} A \frac{\partial}{\partial z_i}.$$

Definition 2.1 For a homogeneous polynomial $f \in A$, we define

$$D(-\log f) = \{\delta \in \mathrm{Der}_A \mid \delta f \in (f)\},$$
$$D_0(-\log f) = \{\delta \in \mathrm{Der}_A \mid \delta f = 0\}.$$

We put $\deg z_i = 1$ and $\deg(\partial/\partial z_i) = -1$ for $i = 0, \ldots, l$. The degree k part of $D_0(-\log f)$ will be denoted by $D_0(-\log f)_k$.

We have the direct sum decomposition

$$D(-\log f) = D_0(-\log f) \oplus A \cdot E,$$

where

$$E = \sum_{i=0}^{\ell} z_i \partial/\partial z_i$$

is the Euler vector field. Let Ω_A be the module of differentials

$$\Omega_A^1 = \bigoplus_{i=0}^{\ell} A dz_i,$$

and Ω_A^k be its k-th exterior power for $k = 0, \ldots, \ell + 1$. We have an isomorphism of A-modules

$$D_0(-\log f) \cong \{\omega \in \Omega^\ell \mid df \wedge \omega = 0\}$$

under the identification

$$\begin{array}{ccc} \mathrm{Der}_A & \xrightarrow{\sim} & \Omega^\ell \\ \cup & & \cup \\ \sum_{i=0}^{\ell} f_i \frac{\partial}{\partial z_i} & \longmapsto & \sum_{i=0}^{\ell} (-1)^i f_i dz_0 \wedge \cdots \wedge \widehat{dz_i} \wedge \cdots \wedge dz_\ell. \end{array}$$

Let $D \subset \mathbb{P}^\ell$ be the hypersurface defined by f. If D is smooth, then the origin $0 \in \mathbb{C}^{l+1}$ is the only zero locus of the Jacobi ideal

$$J(f) = \left(\frac{\partial f}{\partial z_0}, \ldots, \frac{\partial f}{\partial z_\ell} \right),$$

and hence we have

$$\mathrm{depth}_{J(f)} A = \ell + 1.$$

Let H^p be the p-th cohomology of the complex

$$0 \longrightarrow \Omega_A^0 \xrightarrow{df\wedge} \Omega_A^1 \xrightarrow{df\wedge} \cdots \xrightarrow{df\wedge} \Omega_A^\ell \xrightarrow{df\wedge} \Omega_A^{\ell+1} \longrightarrow 0.$$

If D is smooth, then we have $H^p = 0$ for $p = 0, \ldots, \ell$ by de Rham–Saito's lemma. Since

$$D_0(-\log f) \cong \mathrm{Ker}\left(df\wedge : \Omega^\ell \to \Omega^{\ell+1}\right),$$

the sequence

$$0 \longrightarrow \Omega_A^0 \xrightarrow{df\wedge} \Omega_A^1 \xrightarrow{df\wedge} \cdots \xrightarrow{df\wedge} \Omega_A^{\ell-1} \xrightarrow{df\wedge} D_0(-\log f) \longrightarrow 0 \qquad (1)$$

gives a free resolution of $D_0(-\log f)$.

The Euler sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O} & \longrightarrow & \mathcal{O}(1)^{\ell+1} & \longrightarrow & \mathcal{T}_{\mathbb{P}^\ell} & \longrightarrow & 0, \\ & & \cup & & \cup & & & & \\ & & 1 & \mapsto & E & & & & \end{array}$$

shows that the sheafification $\mathcal{T}_{\mathbb{P}^\ell}(-\log f)$ of $D_0(-\log f)$ can be considered as a subsheaf of the tangent sheaf $\mathcal{T}_{\mathbb{P}^\ell}$;

$$\mathcal{T}_{\mathbb{P}^\ell}(-\log f) \subset \mathcal{T}_{\mathbb{P}^\ell}.$$

It is the sheaf of holomorphic vector fields tangent to the hypersurface D at smooth points of D. If D is smooth, we have the short exact sequence

$$0 \longrightarrow \mathcal{T}_{\mathbb{P}^\ell}(-\log f) \longrightarrow \mathcal{T}_{\mathbb{P}^\ell} \longrightarrow \mathcal{N}_{D/\mathbb{P}^\ell} \longrightarrow 0,$$

where $\mathcal{N}_{D/\mathbb{P}^\ell}$ is the normal bundle. We have an isomorphism

$$df|_D : \mathcal{N}_{D/\mathbb{P}^\ell} \xrightarrow{\sim} \mathcal{O}_D(d),$$

where

$$d = \deg f.$$

If D is smooth, then the sheaf $\mathcal{T}_{\mathbb{P}^\ell}(-\log f)$ has the resolution

$$0 \to \mathcal{O}(1-(d-1)\ell) \to \cdots \to \mathcal{O}(3-2d)^{\oplus\binom{\ell+1}{\ell-2}} \to \mathcal{O}(2-d)^{\oplus\binom{\ell+1}{\ell-1}} \to \mathcal{T}_{\mathbb{P}^\ell}(-\log f) \to 0 \tag{2}$$

obtained by sheafifying the exact sequence (1). We also have

$$\Gamma\left(\mathbb{P}^\ell, \mathcal{T}_{\mathbb{P}^\ell}(-\log f)(k)\right) = D_0(-\log f)_k$$

for $k \in \mathbb{Z}$.

3 Plane curves

Now we set $\ell = 2$ to focus our attention on plane curves. Let $f \in \mathbb{C}[z_0, z_1, z_2]$ be a homogeneous polynomial of degree d and $D \subset \mathbb{P}^2$ be the curve defined by f. Define $\mathcal{F}$ as the cokernel of $df\wedge : \mathcal{O}(3-2d) \to \mathcal{O}(2-d)^{\oplus 3}$ so that we have the exact sequence

$$0 \longrightarrow \mathcal{O}(3-2d) \xrightarrow{df\wedge} \mathcal{O}(2-d)^{\oplus 3} \longrightarrow \mathcal{F} \longrightarrow 0. \tag{3}$$

The Chern polynomial of $\mathcal{F}(k)$ is given by

$$\begin{aligned} c_t(\mathcal{F}(k)) &:= 1 + c_1(\mathcal{F}(k))t + c_2(\mathcal{F}(k))t^2 \\ &= c_t(\mathcal{O}(2-d+k))^3 c_t(\mathcal{O}(3-2d+k))^{-1} \\ &= 1 + (3-d+2k)t + (d^2 - 3d + 3 + k^2 + (3-d)k)t^2 \end{aligned}$$

for $k \in \mathbb{Z}$. If D is smooth, then we have

$$\begin{aligned}\mathcal{F} &:= \mathrm{Coker}(df\wedge : \mathcal{O}(3-2d) \to \mathcal{O}(2-d)^{\oplus 3}) \\ &\cong \mathrm{Coim}(df\wedge : \mathcal{O}(2-d)^{\oplus 3} \to \mathcal{O}(1)^{\oplus 3}) \\ &\cong \mathrm{Im}(df\wedge : \mathcal{O}(2-d)^{\oplus 3} \to \mathcal{O}(1)^{\oplus 3}) \\ &\cong \mathrm{Ker}(df\wedge : \mathcal{O}(1)^{\oplus 3} \to \mathcal{O}(d)) \\ &\cong \mathcal{T}_{\mathbb{P}^2}(-\log f).\end{aligned}$$

Lemma 3.1 *If D is smooth, then $\mathcal{T}_{\mathbb{P}^2}(-\log f)$ is stable.*

Proof. We consider $\mathcal{F}([(d-3)/2])$ instead of $\mathcal{T}_{\mathbb{P}^2}(-\log f)$ whose first Chern number is normalized to either 0 (when d is odd) or -1 (when d is even). Then $\mathcal{F}([(d-3)/2])$ is stable if and only if it has no global section. This follows from the cohomology long exact sequence associated with the short exact sequence (3) tensored with $\mathcal{O}_{\mathbb{P}^2}([(d-3)/2])$.

4 Smooth cubic curves

Let $f \in \mathbb{C}[z_0, z_1, z_2]$ be a homogeneous polynomial of degree three and $D \subset \mathbb{P}(V)$ be a cubic curve defined by f, where $V = \mathrm{Spec}\,\mathbb{C}[z_0, z_1, z_2]$. We assume that D is smooth.

4.1 Jumping lines

Let L be a point in the dual projective plane $\mathbb{P}(V^*)$ defined by a linear form $\alpha = \alpha_0 z_0 + \alpha_1 z_1 + \alpha_2 z_2 \in V^*$. We can think of L as a line in $\mathbb{P}(V)$. Restricting the short exact sequence (3) to L and taking the cohomology long exact sequence, we have

$$0 \longrightarrow H^0(\mathcal{F}|_L) \longrightarrow H^1(\mathcal{O}_L(-3)) \longrightarrow H^1(\mathcal{O}_L(-1))^3 \longrightarrow H^1(\mathcal{F}|_L) \longrightarrow 0.$$

Since

$$H^1(\mathcal{O}_L(-3)) \cong H^0(\mathcal{O}_L(1))^* \cong \mathbb{C}^2$$

and

$$H^1(\mathcal{O}_L(-1)) \cong H^0(\mathcal{O}_L(-1))^* = 0,$$

we have

$$\dim H^0(\mathcal{F}|_L) = 2.$$

Hence $\mathcal{F}|_L$ is either

$$\mathcal{F}|_L = \begin{cases} \mathcal{O}_L \oplus \mathcal{O}_L & L \text{ is generic,} \\ \mathcal{O}_L(-1) \oplus \mathcal{O}_L(1) & L \text{ is a jumping line.} \end{cases}$$

In particular,

$$L \text{ is a jumping line} \iff H^0(\mathcal{F}(-1)|_L) \neq 0.$$

By tensoring $\mathcal{O}_L(-1)$ with the short exact sequence (3) and taking the cohomology long exact sequence, we have

$$0 \to H^0(\mathcal{F}(-1)|_L) \to \underset{\wr\!\|}{H^1(\mathcal{O}_L(-4))} \xrightarrow{df\wedge} \underset{\wr\!\|}{H^1(\mathcal{O}_L(-2)^{\oplus 3})} \to H^0(\mathcal{F}(-1)|_L) \to ($$
$$H^0(\mathcal{O}_L(2))^* \qquad H^0(\mathcal{O}_L^{\oplus 3})^*.$$

Since $H^0(\mathcal{O}(2)|_L) \cong \mathrm{Sym}^2 V^*/(z_0\alpha, z_1\alpha, z_2\alpha)$, the set $S = S(\mathcal{T}_{\mathbb{P}^\ell}(-\log f)) \subset \mathbb{P}(V^*)$ of jumping lines is characterized as follows;

$$\begin{aligned} L \in S &\iff (df\wedge)^* : H^0(\mathcal{O}_L^{\oplus 3} \to H^0(\mathcal{O}_L(2))) \text{ is not an isomorphism} \\ &\iff z_0\alpha, z_1\alpha, z_2\alpha, \partial_0 f, \partial_1 f, \partial_2 f \text{ are linearly dependent in } \mathrm{Sym}^2 V^*. \quad (4) \end{aligned}$$

4.2 Cayleyan curves

Here we prove the following:

Proposition 4.1 *Let $D \subset \mathbb{P}(V)$ be a smooth cubic curve defined by a polynomial f. Then the set $S = S(\mathcal{T}_{\mathbb{P}^\ell}(-\log f)) \subset \mathbb{P}(V^*)$ of jumping lines of $\mathcal{T}_{\mathbb{P}^\ell}(-\log f)$ in the dual projective plane $\mathbb{P}(V^*)$ is the Cayleyan curve of D.*

First we recall the definition of the Cayleyan curve of a plane cubic curve following Artebani and Dolgachev [1]. The *first polar* of a plane curve $D = \{f = 0\}$ with respect to a point $q = [a_0 : a_1 : a_2] \in \mathbb{P}(V)$ is the curve $P_q(D)$ defined by the polynomial

$$g = a_0\partial_0 f + a_1\partial_1 f + a_2\partial_2 f,$$

whose degree is one less than that of f. A point $[x_0 : x_1 : x_2] \in P_q(D)$ is a singularity of the polar curve if

$$\partial_i g(x_0, x_1, x_2) = \sum_{j=0}^{2} a_j \partial_{ij} f(x_0, x_1, x_2) = 0$$

for $i = 0, 1, 2$. Here, ∂_i denotes the partial derivative with respect to x_i and $\partial_{ij} = \partial_i\partial_j$. When f is cubic, one has

$$\sum_{j=0}^{2} a_j \partial_{ij} f(x_0, x_1, x_2) = \sum_{j=0}^{2} x_j \partial_{ij} f(a_0, a_1, a_2)$$

and hence the polar curve $P_q(D)$ has a singularity if and only if q lies on the *Hessian curve* $\mathrm{He}(D) \subset \mathbb{P}(V)$ defined by

$$h = \det \begin{pmatrix} \partial_{00} f & \partial_{01} f & \partial_{02} f \\ \partial_{10} f & \partial_{11} f & \partial_{12} f \\ \partial_{20} f & \partial_{21} f & \partial_{22} f \end{pmatrix}.$$

For $q \in \mathrm{He}(D)$, the polar curve $P_q(D)$ decomposes into the union of two lines. Let $s_q \in \mathbb{P}(V)$ denote the singular point of $P_q(D)$ and $L_q \in \mathbb{P}(V^*)$ be the line connecting q and s_q. Since the equation

$$\sum_{j=0}^{2} a_j \partial_{ij} f(x_0, x_1, x_2) = 0$$

is symmetric with respect to q and s_q, the singularity s_q of $P_q(D)$ always lies on $\mathrm{He}(D)$ and the map

$$\begin{array}{ccccc} s & : & \mathrm{He}(D) & \longrightarrow & \mathrm{He}(D) \\ & & \cup & & \cup \\ & & q & \mapsto & s_q \end{array}$$

defines an involution on $\mathrm{He}(D)$. Since $q = s_q$ implies

$$\partial_i f(a_0, a_1, a_2) = 0, \qquad i = 0, 1, 2,$$

so that q is a singular point of D, the involution s has no fixed point. The image of the map

$$\begin{array}{ccc} \mathrm{He}(D) & \longrightarrow & \mathbb{P}(V^*) \\ \cup & & \cup \\ q & \mapsto & L_q \end{array}$$

is called the *Cayleyan curve* of D, which is known to be the quotient of $\mathrm{He}(D)$ by the involution s. A linear form $\alpha = \alpha_0 z_0 + \alpha_1 z_1 + \alpha_2 z_2 \in V^*$ represents a point in the Cayleyan curve of D if and only if there is a point $[a_0 : a_1 : a_2] \in \mathbb{P}^2$ such that

$$a_0 \partial_0 f + a_1 \partial_1 f + a_1 \partial_1 f \in \alpha \cdot V^*.$$

This is precisely the condition (4) for the line $[\alpha] \in \mathbb{P}(V^*)$ to be a jumping line of $\mathcal{T}_{\mathbb{P}^\ell}(-\log f)$.

4.3 The set of jumping lines and j-invariant

Here we prove the following:

Proposition 4.2 *Let D be the smooth cubic curve defined by a polynomial f. Then the set $S(\mathcal{T}_{\mathbb{P}^\ell}(-\log f))$ of jumping lines is singular if and only if the j-invariant of D is zero.*

Proof. Choose a coordinate of V so that f is a Hesse cubic

$$f_t(z_0, z_1, z_2) = z_0^3 + z_1^3 + z_2^3 - 3t z_0 z_1 z_2, \tag{5}$$

where $t \in \mathbb{C} \setminus \{1, \zeta, \zeta^2\}$ and $\zeta = \exp[2\pi\sqrt{-1}/3]$. Recall that $D = \{f_t = 0\} \subset \mathbb{P}^2$ is smooth if and only if $t^3 \neq 1$. The set $S = S(\mathcal{T}_{\mathbb{P}^\ell}(-\log f))$ of jumping lines, which coincides with the Cayleyan curve of D, is a Hesse cubic

$$t(\alpha_0^3 + \alpha_1^3 + \alpha_2^3) - (t^3 + 2)\alpha_0\alpha_1\alpha_2 = 0$$

in the dual projective plane. It is the union of three lines in general position if $t = 0$ or $(3t)^3 = (t^3+2)^3$. Since

$$(t^3+2)^3 - (3t)^3 = (t^3-1)^2(t^3+8)$$

and the j-invariant $j(D)$ of D is given by

$$j(D) = \frac{1}{64}t^3\frac{(t^3+8)^3}{(t^3-1)^3},$$

the Cayleyan curve of D is smooth if and only if $j(D) \neq 0$, and decomposes into the union of three lines in general position if $j(D) = 0$.

4.4 Restricting $\mathcal{T}_{\mathbb{P}^\ell}(-\log f)$ to other cubic curves

Here we consider the restriction of the sheaf $\mathcal{T}_{\mathbb{P}^\ell}(-\log f)$ to another cubic curve E defined by a polynomial g. ¿From the exact sequence (3), we have

$$0 \longrightarrow \mathcal{O}(-3)|_E \longrightarrow \mathcal{O}(-1)^{\oplus 3}|_E \longrightarrow \mathcal{F}|_E \longrightarrow 0.$$

Hence we have

$$\begin{array}{ccccccccc} 0 & \to & H^0(\mathcal{F}|_E) & \to & H^1(\mathcal{O}(-3)|_E) & \xrightarrow{df\wedge} & H^1(\mathcal{O}(-1)^{\oplus 3}|_E) & \to & H^0(\mathcal{F}|_E) & \to & 0 \\ & & & & \| & & \| & & & & \\ & & & & H^0(\mathcal{O}(3)|_E)^* & & H^0(\mathcal{O}(1)^{\oplus 3}|_E)^*. & & & & \end{array}$$

Since $H^0(\mathcal{O}(3)|_E) = \mathrm{Sym}^3 V^*/(g)$ and $H^0(\mathcal{O}(1)|_E)^3 = (V^*)^3$, the map $df\wedge$ is dual to the map induced by

$$\begin{array}{ccc} (V^*)^3 & \longrightarrow & \mathrm{Sym}^3 V^* \\ \cup & & \cup \\ (F_0, F_1, F_2) & \longrightarrow & F_0\partial_0 f + F_1\partial_1 f + F_2\partial_2 f. \end{array}$$

This map is injective due to de Rham–Saito's lemma, and the image can be identified with the degree 3 part $J(f)_3$ of the Jacobi ideal. Hence we have

$$H^0(\mathcal{F}|_E) = \begin{cases} \mathbb{C} & g \in J(f)_3, \\ 0 & g \notin J(f)_3. \end{cases}$$

By an explicit calculation, we obtain the following:

Proposition 4.3 *Let f_t be the Hesse cubic in (5) and put*

$$g = \sum_{0\le i\le j\le k\le 2} a_{ijk} z_i z_j z_k.$$

Then the hyperplane $J(f_t)_3 \subset \mathrm{Sym}^3 V^*$ is given by

$$J(f_t)_3 = \{g \mid a_{012} + t(a_{000} + a_{111} + a_{222}) = 0\}.$$

5 Torelli theorem

Here we prove our main result:

Theorem 5.1 *Let C and C' be smooth cubic curves with non-vanishing j-invariants. If $\mathcal{T}(-\log C)$ is isomorphic to $\mathcal{T}(-\log C')$ as an $\mathcal{O}_{\mathbf{P}^2}$-module, then $C = C'$.*

Proof. Take a homogeneous coordinate of the dual projective plane so that the set of jumping lines of $\mathcal{T}(-\log C)$ is a Hesse cubic. Since a smooth cubic whose Cayleyan curve is a smooth Hesse cubic must be a Hesse cubic, C and C' are Hesse cubics. Then Proposition 4.3 shows that C must coincide with C'.

Remark 5.1 *The Torelli theorem fails for cubic curves with vanishing j-invariants. Indeed, the family*

$$az_0^3 + bz_1^3 + cz_0^3 = 0, \qquad a, b, c \in \mathbb{C}^\times$$

consists of cubic curves with identical Cayleyan curves given by

$$\alpha_0\alpha_1\alpha_2 = 0.$$

Since the set of jumping lines determines a unique stable bundle if it consists of three lines in general position by Barth [2], the sheaf of logarithmic vector fields does not depend on a, b, and c.

References

[1] Michela Artebani and Igor Dolgachev, *The Hesse pencil of plane cubic curves*, arXiv:math.AG/0611590, 2006.

[2] Wolf Barth, *Moduli of vector bundles on the projective plane*, Invent. Math., vol.**42** (1977), 63–91.

[3] Georges de Rham, *Sur la division de formes et de courants par une forme linéaire*, Comment. Math. Helv., vol.**28** (1954), 346–352.

[4] Igor Dolgachev and Mikhail Kapranov, *Arrangements of hyperplanes and vector bundles on* $\mathbf{P}^n$, Duke Math. J., vol.**71**(3) (1993), 633–664.

[5] Kyoji Saito, *On a generalization of de-Rham lemma*, Ann. Inst. Fourier (Grenoble), vol.**26**(2) (1976), 165–170.

[6] Kyoji Saito, *Theory of logarithmic differential forms and logarithmic vector fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., vol.**27**(2) (1980), 265–291.

[7] Hiroaki Terao, *Generalized exponents of a free arrangement of hyperplanes and Shepherd-Todd-Brieskorn formula*, Invent. Math., vol.**63**(1) (1981), 159–179.

Kazushi Ueda
Department of Mathematics,
Graduate School of Science,
Osaka University,
Machikaneyama 1-1, Toyonaka, Osaka, 560-0043, Japan.
e-mail: kazushi@math.sci.osaka-u.ac.jp

Masahiko Yoshinaga
Department of Mathematics,
Graduate School of Science,
Kobe University,
1-1, Rokkodai, Nada-ku, Kobe 657-8501, Japan.
e-mail: myoshina@math.kobe-u.ac.jp

Kumamoto J. Math.
Vol.21 (2008), 21–28

$D_{p+1}(3)(p \geq 3)$ can be characterized by its order components*

Huaguo Shi and Guiyun Chen**

(Received September 18, 2007)
(Accepted December 29, 2007)

Abstract. It is proved that if $M = D_{p+1}(3)(p \geq 3)$, G is a finite group and has the same order components of M, then $G \cong M$.

1 Introduction

If G is a finite group, we define the prime graph $\Gamma(G)$ as follows: its vertices are the primes dividing the order of G, and two vertices p and q are joined by an edge if and only if there is an element in G of order pq. We denote the set of all the connected components of graph $\Gamma(G)$ by $T(G) = \{\pi_i(G), \text{ for } i = 1, 2, \cdots, t(G)\}$ where $t(G)$ is the number of connected components of $\Gamma(G)$, and if G is of even order we always assume that 2 belongs to $\pi_1(G)$. We denote by $\pi(n)$ the set of all primes dividing n where n is a natural number. Obviously $|G|$ can be expressed as a product of $m_1, m_2, \cdots, m_{t(G)}$, where m_i is a positive integer with $\pi(m_i) = \pi_i(G)$. All m_i are called the order components of G. Let $OC(G) = \{m_1, m_2, \cdots, m_{t(G)}\}$ be the set of order components of G. The order components of non-abelian simple groups having at least two prime graph components have been obtained in [3].

Professor J.G.Thompson proposed the following conjecture. Let M be a non-abelian simple group, if G is a finite group satisfying $Z(G) = 1$ and $N(G) = N(M)$, where $N(G) = \{n \in N | G \text{ has a conjugacy class } C, \text{ such that } |C| = n\}$, then $G \cong M$. To formulate another conjecture put forward by Professor W. J.Shi, let us introduce the notation $\pi_e(G)$ that denotes the set of orders of elements of G. After the conjecture, if both M and G are finite groups with properties $|G| = |M|$ and $\pi_e(G) = \pi_e(M)$ then $G \cong M$. In [5], we had proved that if M is a simple group with non-connected prime graph and G is a finite group satisfying the conditions of J.G. Thompson's conjecture then $OC(G) = OC(M)$. Obviously, if G is a finite group satisfying the conditions of W.J. Shi's conjecture, we have $OC(G) = OC(M)$. As a consequence, these two conjectures naturally hold for a

Mathematical Subject Classification (2000): 20D05, 20D60.
Key words: finite groups, prime graphs, order components.
*This work is supported by Natural Science Foundation of China(No. 10771172)
**corresponding author

simple group M characterized by its order components that consist at least of two elements. Hence, it is an important topic to find out those simple groups satisfying above mentioned properties.

We have established that the following simple groups have a non-connected prime graph and can be characterized by their order components: a finite simple group with at least three prime graph components [5], sporadic simple groups [3], Suzuki-Ree groups [6], $G_2(q)$ where $q \equiv 0 \pmod 3$ [4], $E_8(q)$ [1], $PSL_2(q)$ [7], ${}^3D_4(q)$ [8], ${}^2D_n(3), 9 \leq n = 2^m + 1 \neq p$ [9], ${}^2D_{p+1}(2)$, $5 \leq p \neq 2^m - 1$ [28], A_p where p and $p-2$ are primes [12], $PSL(5,q)$ [13], $PSL(3,q)$ where q is an odd prime power [14], $PSL(3,q)$ for $q = 2^n$ [15], $F_4(q)$ where q is even [16], $C_2(q)$ where $q > 5$ [17], $PSU_5(q)$ [18], $PSU(3,q)$ for $q > 5$ [19], ${}^2D_4(q)$ [20], ${}^2E_6(q)$ [22], $E_6(q)$ [21], $PSL(p,q)$.[23], $PSU(p,q)$[24], $PSL(p+1,q)$ [25], $PSU(p+1,q)$[26], $C_p(2)$[29].

In this paper we continue this work and will prove the following theorem:

Theorem 1 *Let $M = D_{p+1}(3)$ where p is an odd prime. If a finite group G satisfies the condition $OC(G) = OC(M)$, then $G \cong M$.*

2 Preliminary Results

Lemma 2 *[[3] Lemma 6] If $t(G) \geq 2$, H is a π_i subgroup of G, and $H \lhd G$, then $(\Pi_{j=1,j\neq i}^{t(G)} m_i) \mid (|H| - 1)$.*

Lemma 3 *[[2] Theorem 2] Let G be a 2-Frobenius group of even order. Then $t(G) = 2$, G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that $|K/H| = m_2, |H| \cdot |G/K| = m_1, |G/K| \mid (|K/H| - 1), |G/K| \mid \varphi(|K/H|)$, and H is nilpotent.*

Lemma 4 *[[30] Lemma 3]If M is a simple group with $t(M) = 2$, G is a finite group and $OC(G) = OC(M)$, then one of the following holds:*

(1) G is a Frobenius group or 2-Frobenius group.

(2) G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that H is a nilpotent π_1-group, K/H is a non-abelian simple group, the odd order component of M is equal to one of those of K/H, G/K is a cyclic π_1-group, and $|G/K| \mid |Out(K/H)|$.

Lemma 5 *[[11] Remark] The only solution of the equation $p^m - q^n = 1$, where p , q are primes and $m, n > 1$, is $3^2 - 2^3 = 1$.*

Lemma 6 *[31] Let p be a prime and n be a natural number, $n \geq 2$. Then there exists a prime divisor r of $p^n - 1$ which does not divide $p^m - 1$ for any natural number $m \leq n$, except $n = 6$, $p = 2$ or $n = 2$, $p + 1$ is a power of 2. Such r is called a primitive prime divisor of $p^n - 1$.*

Of course a primitive prime divisor of $p^n - 1$ can not divide $p^n + 1$ or $p^m - 1$ for $n \nmid m$.

Lemma 7 *[[27] Lemma 1] If $n \geq 6$ is a natural number then there exists at least $s(n)$ primes p_i such that $\frac{n+1}{2} < p_i < n$:*
$s(n) = 6$ for $n \geq 49$;
$s(n) = 5$ for $42 \leq n \leq 47$;
$s(n) = 4$ for $38 \leq n \leq 41$;
$s(n) = 3$ for $18 \leq n \leq 37$;
$s(n) = 2$ for $14 \leq n \leq 17$;
$s(n) = 1$ for $6 \leq n \leq 13$.

Suppose p is a prime number, a is a natural number, We denote the power of p in the standard factorization of a by a_p, and if $a_p = p^n$, then we write $p^n \parallel a$. Of course $p^n \parallel a$ denotes that $p^n | a$ and $p^{n+1} \nmid a$.

Lemma 8 *[[29] Lemma 7, Lemma 8, Lemma 9] Let p be a prime, $q > 1$ be a natural number $e = min\{d > 0 : p \mid (q^d - 1)\}$, $q^e = 1 + p^r k$, $p \nmid k$, $s = \prod_{i=1}^{n}(q^i - 1)$, t is a natural number and $p^u \parallel t$. If $p > 2$ or $r > 2$ then $p^{r+u} \parallel (q^{et} - 1)$, $s_p < q^{\frac{np}{p-1}}$ and $s_p < q^{1.5n}$ if $p = 2$.*

Definition 9 *Let a and f be expressions of integers with integral coefficients, if $f \mid a$ and $(f,\ a/f) = 1$, then we say that f is a hall factor of a.*

Lemma 10 *[[10] Theorem 1]If q is a power of a prime number, $c = \prod_{i=1}^{n}(q^{2i} - 1)$ or $(q^n \pm 1) \cdot \prod_{i=1}^{n-1}(q^{2i} - 1)$, then there exists a hall factor f of c satisfying:*
(1) If $n \geq 23$ then $f > q^{8n}$;
(2) If $n = 22$ then $f > q^{7n}$;
(3) If $18 \leq n \leq 21$ then $f > q^{6n}$;
(4) If $16 \leq n \leq 17$ then $f > q^{5n}$;
(5) If $14 \leq n \leq 15$ then $f > q^{4n}$.
And if the standard factorization of $f = \prod_{k=1}^{t} r_k^{\delta_k}$, then $r_k^{\delta_k} \leq \frac{q^{n-1}-1}{q-1}$.

3 Proof of the theorem

Proof: Because $M = D_{p+1}(3)$, $p \geq 3$, and G has the same order components with M, so the even order component of G is $m_1 = 2 \cdot 3^{p(p+1)}(3^{p+1} - 1)(3^p + 1)\prod_{i=1}^{p-1}(3^{2i} - 1)$, the odd order component of G is $m_2 = (3^p - 1)/2$.

We divide the proof into several cases based on Lemma 4 and Tables 1-4 in [3].

Case 1. G is not be a Frobenius group or a 2-Frobenius group.

Subcase 1.1 If G is a Frobenius group with Frobenius kernel H and complement K, then $|H| = m_1$, $|K| = m_2$ since $|K| \mid (|H|-1)$. There exists a primitive prime divisor r of $3^{2p}-1$ by Lemma 6. Set $S_r \in Syl_r(H)$, of course $|S_r| \mid (3^p+1)/4$ and $S_r \trianglelefteq G$ since H is nilpotent and so $S_r charH$. $|S_r| \equiv 1 \pmod{m_2}$ by Lemma 2, which is impossible.

Subcase 1.2 If G is a 2-Frobenius group , there is a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that H is a nilpotent π_1 group, $|K/H| = m_2$, $|G/K| \mid (|K/H|-1) = (3 \cdot (3^{p-1}-1))/2$. Hence $(3^p+1) \mid |H|$. Similarly to Subcase 1.1, we can show it's impossible.

From Subcase 1.1, Subcase 1.2 and Lemma 4 we have the following properties:

1. There is a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that K/H is a simple group, H and G/K are π_1 group and H is nilpotent.

2. The odd order component of G is one of those of K/H, consequently $t(K/H) \geq 2$. Hence K/H may be one of the simple groups listed in Tables 1-4 in [3].

Case 2. $K/H \ncong E_7(2)$, $E_7(3)$, $A_2(2)$, $A_2(4)$, ${}^2A_5(2)$, ${}^2E_6(2)$, ${}^2F_4(2)'$ or one of the sporadic simple groups.

Any odd order component of $E_7(2)$, $E_7(3)$, $A_2(2)$, $A_2(4)$, ${}^2A_5(2)$, or one of the sporadic simple groups(except Suz and F_{22}) can not be written into the form $(3^p-1)/2$ for $p \geq 3$. Though ${}^2E_6(2)$, Suz, F_{22} or ${}^2F_4(2)'$ has an order component 13 can be written into the form $(3^p-1)/2$ and $p=3$, but the order of ${}^2E_6(2)$, Suz, F_{22} or ${}^2F_4(2)'$ can not divides $|D_4(3)|$. So $K/H \ncong E_7(2)$, $E_7(3)$, $A_2(2)$, $A_2(4)$, ${}^2A_5(2)$, ${}^2E_6(2)$, ${}^2F_4(2)'$ or one of the sporadic simple groups.

Case 3. $K/H \ncong A_n$.

If $K/H \cong A_n$ then A_n has an odd component equal to $(3^p-1)/2$. Thus $|A_{(3^p-1)/2}| \mid |A_n|$ and $|A_n| \mid |D_{p+1}(3)|$. by Lemma 7, there exists at least six primes p_i satisfying $(3^p+1)/4 < p_i < (3^p-1)/2$ for $p \geq 5$,On the other hand there exists at most three prime divisors of $|D_{p+1}(3)|$ between $(3^p+1)/4$ and $(3^p-1)/2$ by Lemma 7, a contradiction.

By trivial calculation, we conclude that p can not be 3.

Case 4 $K/H \ncong A_n(q)$, ${}^2A_n(q)$, $E_6(q)$, $E_8(q)$, $F_4(q)$, ${}^2F_4(q)$ or ${}^2E_6(q)$.

Subcase 4.1 If $K/H \cong A_1(q)$, then $(3^p-1)/2 = q$, $(q \pm 1)/(2, q-1)$. Whenever in any case we have that $q \leq 3^{p+1}$, hence $|K/H| < 3^{3(p+1)}$. Assume $q = r^f$, we have that $|G/K| < 3^{p+1}$ since $2^{3^{p+1}/2} > 3^{p+1}$ and $|G/K| \mid |Out(K/H)| = 2f$. If $p \geq 14$ then there exists a hall factor g of $|G| = 3^{p(p+1)}(3^{p+1}-1)\prod_{i=1}^{p}(3^{2i}-1)$ satisfying that $g > 3^{4p}$ and for any prime number $r' \mid g$ we have that $g_{r'} < (3^p-1)/2$ by Lemma 10. Clearly $(g, |H|) \neq 1$. Let p' be a prime number satisfy $p' \mid (g, |H|)$ and $S_{p'} \in Syl_{p'}(G)$. $S_{p'}$ is a normal π_1–subgroup of G and $|S_{p'}| < (3^p-1)/2$, which contradicts Lemma 2.

By trivial calculation, we can show p can not be 3, 5, 7 or 11.

Subcase 4.2 If $K/H \cong A_{p'}(q)$, $q-1 \mid p'-1$ then $(3^p-1)/2 = (q^{p'}-1)/(q-1)$. Thus $q^{p'+1} \geq 3^p$.

If $p' > 7$ then $q^{p'(p'+1)/2} > 3^{3(p+1)}$, which implies q is a power of 3 by Lemma 8 and Lemma 8. It follows that $3^p - 3 = 2(q^{p'-1} + q^{p'-2} + \cdots + q)$, consequently $q = 3$ and $p = p'$, furthermore $3^p + 1 \mid |H|$. Similarly to Subcase 1.1, we can get a contradiction.

By trivial calculation we can show that p' can not be 3 or 5.

Similarly, we can show that $K/H \ncong {}^2A_n(q)$, $E_6(q)$, $E_8(q)$, $F_4(q)$, ${}^2F_4(q)$ or ${}^2E_6(q)$.

Subcase 4.3 If $K/H \cong A_{p'-1}(q)$ then $(q^{p'}-1)/(q-1)(p',\ q-1) = (3^p-1)/2$.

Similarly to Subcase 4.2, we can prove that p' can not be greater than 7. And similarly to Subcase 4.1, it is easy to prove that p' can not be 3, 5 or 7.

Case 5 $K/H \ncong B_n(q)$ or $C_n(q)$.

Subcase 5.1 If $K/H \cong C_{p'}(2)$, then $2^{p'} - 1 = (3^p - 1)/2$, $2^{p'+1} - 1 = 3^p$, which contradicts Lemma 5.

Subcase 5.2 If $K/H \cong B_{p'}(3)$ or $C_{p'}(3)$, then $(3^p-1)/2 = (3^{p'}-1)/2$, $p = p'$, $|B_p(3)|$ and $|C_p(3)|$ are divisors of $|D_{p+1}(3)|$, which is impossible.

Subcase 5.3 Similarly to Subcase 4.2, we can show that $K/H \cong B_n(q)$ or $C_n(q)(4 \leq n = 2^m)$.

Case 6 $K/H \ncong {}^2D_n(q)$.

Subcase 6.1 If $K/H \cong {}^2D_{p'}(3)(5 \leq p' \neq 2^k + 1)$, then $(3^p - 1)/2 = (3^{p'} + 1)/4\text{K2} \cdot 3^p - 3^{p'} = 3$ a contradiction. Similarly, we can prove that $K/H \ncong {}^2D_n(3)(9 \leq n = 2^k + 1$ is not a prime); $K/H \ncong {}^2D_{p'}(3)(5 \leq p' = 2^k + 1)$.

Subcase 6.2 If $K/H \cong {}^2D_{p'+1}(2)(p' \neq 2^m - 1)$, then $(3^p - 1)/2 = 2^{p'} - 1$, $3^p = 2^{p'+1} - 1$, which contradicts Lemma 5. Similarly we can prove $K/H \ncong {}^2D_{p'+1}(2)(3 \leq p' = 2^k - 1)$.

Subcase 6.3 Similarly to Subcase 4.2, we can prove that $K/H \ncong {}^2D_n(q)(2 \leq n = 2^k)$.

Case 7 $K/H \ncong G_2(q)$; $K/H \ncong {}^3D_4(q)$; $K/H \ncong {}^2G_2(q)(q = 3^{2k+1})$.

Subcase 7.1 If $K/H \cong G_2(q)(3 \mid q)$, then $(3^p-1)/2 = q^2 \pm q + 1$, $3^p - 3 = q^2 \pm q$, a contradiction. Similarly we have that $K/H \ncong {}^2G_2(q)(q = 3^{2k+1})$.

Subcase 7.2 Similarly to Subcase 4.1, we can prove that $K/H \ncong G_2(q)(3 \mid q \pm 1)$ or ${}^3D_4(q)$.

Case 8 $K/H \ncong {}^2B_2(q)(4 \leq q = 2^{2k+1})$.

If $K/H \cong {}^2B_2(q)(4 \leq q = 2^{2k+1})$, then $(3^p - 1)/2 = q \pm \sqrt{2q} + 1$ or $q - 1$. Clearly $(3^p - 1)/2 \neq q - 1\text{B}$

If $(3^p - 1)/2 = q + \sqrt{2q} + 1$, then $3(3^{p-1} - 1) = 2^{k+2}(2^k + 1)$, $2^k \mid p - 1$ by Lemma 8, furthermore, $2^{k+2}(2^k + 1) = 3(3^{p-1} - 1) > 3^{p-1} > 3^{2^k} > 2^{2^k} > 2^{2k+3} > 2^{k+2}(2^k + 1)$ for $k \geq 4$, a contradiction. By calculation we can prove that k can not be 1, 2 or 3.

Similarly we have $(3^p - 1)/2 \neq q - \sqrt{2q} + 1$.

Case 9 From Cases 1-8 and Lemma 4 we have K/H is isomorphic to one of $D_n(q)$.

If $K/H \cong D_{p'}(3)(p' \geq 5)$, then $(3^p - 1)/2 = (3^{p'} - 1)/2$, $p = p'$, hence $|G/K| \cdot |H| = 3^{2p}(3^p + 1)(3^{p+1} - 1)$, furthermore, $3^p + 1 \mid |H|$ since $|G/K| \mid |Out(K/H)| = 4$, similarly to Subcase 1.1 we can get a contradiction.

If $K/H \cong D_{P'}(5), p' \geq 5$, then $(5^{p'} - 1)/4 = (3^p - 1)/2$, $5^{p'} > 3^P$. Furthermore, $5^{p'(p'-1)} > 3^{3(p+1)}$, which contradicts Lemma 8.

So $K/H \cong D_{p'+1}(3)$, $(3^{p'} - 1)/2 = (3^p - 1)/2$, $p = p'$, hence $K/H = 1$, $H = 1$, $G \cong M$. □

References

[1] G.Y. Chen, *A new characterization of* $E_8(q)$, J. Southwest China Normal Uni., **21**(3) (1995), 215–217.

[2] G.Y. Chen, *On Frobenius and 2-Frobenius group*, J. Southwest China Normal Uni. in Chinese, **20**(5) (1995), 485–487.

[3] G.Y. Chen, *A new characterization of sporadic groups*, Algebra Colloq, **3**(1) (1996), 49–58.

[4] G.Y. Chen, *A new characterization of* $G_2(q)$, *[*$q \equiv 0$ *mod (3)]*, J. Southwest China Normal uni., **22**(1) (1996), 47–51.

[5] G.Y. Chen, *On Thompson's conjecture*, J. Algebra, **15** (1996), 184–193.

[6] G.Y. Chen, *A new characterization of Suzuki-Ree groups*, Sci. in China(ser A), **27**(5) (1997), 430–433.

[7] G.Y. Chen, *A new characterization of* $PSL_2(q)$, Southeast Asian Bulletin of Math, **22** (1998), 257–263.

[8] G.Y. Chen, *Characterization of* ${}^3D_4(q)$, Southeast Asian Bulletin of Math, **25** (2001), 389–401.

[9] G.Y. Chen and H.G. Shi, ${}^2D_n(3)(9 \leq n = 2^m + 1$ *not a prime) can be characterized by its order components*, Korean J.Comput.& Appl.Math., **19** (2005), no. 1-2, 353–362.

[10] G.Y. Chen and H.G. Shi, *On Hall factors of several Special Integeral expressions*, J. Southwest China Normal Uni., **30**(5) (2005), 763–770.

[11] P. Crescenzo, *A Diophantine equation which arises in the theory finite groups*, Advances in Math., **17** (1975), 25–29.

[12] A. Iranmanesh and S.H. Alavi, *A new characterization of* A_p *where* p *and* $p - 2$ *are primes*, Korean J.Comput.& Appl.Math., **8**(3) (2001), 665–673.

[13] A. Iranmanesh and S.H. Alavi, *A characterization of simple groups* $PSL(5,q)$, Bull. Austral Math. Soc., **65** (2002), 211–222.

[14] A. Iranmanesh, S.H. Alavi and Bz. Khosravi, *A characterization of* $PSL(3,q)$ *where* q *is an odd prime power*, J. Pure and Applied Algebra, **170**(2-3) (2002), 243–254.

[15] A. Iranmanesh, S.H. Alavi and Bz. Khosravi, *A characterization of* $PSL(3,q)$ *for* $q = 2^n$, Acta Math. Sinica, English series, **18**(3) (2002), 463–472.

[16] A. Iranmanesh and Bz. Khosravi, *A characterization of* $F_4(q)$ *where* q *is even*, Far East J. Math. Sci. (FJMS), **2**(6) (2000), 853–859.

[17] A. Iranmanesh and Bz. Khosravi, *A characterization of* $C_2(q)$ *where* $q > 5$, Comment Math. Univ. Carolinae, **43**(1) (2002), 9–21.

[18] A. Iranmanesh and Bz. Khosravi, *A characterization of* $PSU_5(q)$, International Mathematical Journal, **3**(2) (2003), 129–141.

[19] A. Iranmanesh, Bz. Khosravi and S.H. Alavi, *A characterization of* $PSU(3,q)$ *for* $q > 5$, Southeast Asian Bulletin Math, **26**(2) (2002), 33–44.

[20] Bz. Khosravi, *A characterization of* ${}^2D_4(q)$, Pure Math. Appl., **12**(4) (2001), 415–424.

[21] Bz. Khosravi and Bm. Khosravi, *A characterization of* $E_6(q)$, Algebras Groups and Geometries, **19**(2) (2002), 225–243.

[22] Bz. Khosravi and Bm. Khosravi, *A characterization of* ${}^2E_6(q)$, Kumamoto J.Math., **16** (2003) 1–11.

[23] A. Khosravi and Bz. Khosravi, *A new characterization of* $PSL(p,q)$, Communications in Algebra, **32** (6) (2004), 2325–2339.

[24] Bz. Khosravi, Bn. Khosravi and Bm. Khosravi, *A New Characterization of* $PSU(p,q)$, Acta Math. Hungarica, **107**(3) (2005), 235–252.

[25] Bz. Khosravi, Bn. Khosravi and Bm. Khosravi, *Characterizability of* $PSL(p+1,q)$ *by its order component(s)*, Houston J. Math., **32**(3) (2006), 683–700.

[26] A. Khosravi and Bz. Khosravi, *Characterizability of* $PSU(p+1,q)$ *by its order component(s)*, Rocky Mountain J. Math., **36**(5) (2006), 1555–1577.

[27] A. S. Kondtrat'ev and V. D. Mazurov, *Recognition of alternating groups if prime degree from their element orders*, Siberian Mathematical Journal, **41**(2) (2000) 294–302.

[28] H.G. Shi and G.Y. Chen, ${}^2D_{p+1}(2)(5 \leq p \neq 2^m - 1)$ *can be characterized by its order components*, Kumamoto J. Math. **18** (2005), 1–8.

[29] H.G. Shi and G.Y. Chen, $C_p(2)$ *can be characterized by its order components*, Far east J. math. sci. **27**(1) (2007), 205–216.

[30] J.S. Williams, *Prime Graph components of finite group*, J. Algebra **69** (1981), 487–513.

[31] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys., **3** (1892), 265–284.

Huaguo Shi
School of Mathematics and Statistics,
Southwest China University,
400715, Chongqing, P. R. China
and
Sichuan Vocational and Technical college,
629000 Sichuan, P. R. China.
e-mail: shihuaguo@126.com

Guiyun Chen
School of Mathematics and Statistics,
Southwest China University,
400715, Chongqing, P. R. China.
e-mail: gychen@swu.edu.cn

Kumamoto J. Math.
Vol.21 (2008), 29-39

Factorization in certain rings of arithmetical functions

Alexandru Zaharescu and Mohammad Zaki

(Received May 30, 2007)
(Accepted December 19, 2007)

Abstract. In this paper we show that certain subrings of the ring $A_r(F)$ of arithmetical functions in r variables over a given field F are factorial.

1 Introduction

The ring $(A, +, .)$ of complex valued arithmetical functions with Dirichlet convolution consists of all functions $\mathbb{N} \to \mathbb{C}$, where $\mathbb{N}$ is the set of positive integers. Cashwell and Everett [2] proved that $(A, +, .)$ is a unique factorization domain. Yokom [13] investigated the prime factorization of arithmetical functions in a certain subring of the regular convolution ring. He determined a discrete valuation subring of the unitary ring of arithmetical functions. Narkiewicz [4] introduced and studied in [4] the concept of regular convolution. Further work on regular convolutions has been done by Scheid [5], [6], [7], Sitaramaiah [12] and Haukkanen [3]. Schwab and Silberberg [10] constructed an extension of $(A, +, .)$ which is a discrete valuation ring. In [11], they showed that A is a quasi-noetherian ring. Further results have been obtained by Schwab in [8] and [9]. Alkan and the authors [1] studied absolute values and derivations on the ring of arithmetical functions in several variables having values in an integral domain, with the analogue of Dirichlet convolution as multiplication. If R is an integral domain and r is a positive integer, let $A_r(R) = \{f : \mathbb{N}^r \to R\}$. For any $f, g \in A_r(R)$, the convolution $f * g$ of f and g is defined by

$$(f * g)(n_1, ..., n_r) = \sum_{d_1 | n_1} \cdots \sum_{d_r | n_r} f(d_1, ..., d_r) g\left(\frac{n_1}{d_1}, ..., \frac{n_r}{d_r}\right). \tag{1.1}$$

In [14] a natural family of subrings $B_{r,k,p}(R)$ of $A_r(R)$ was considered. For any $k \in \{1, \ldots, r\}$, and any prime number p, $B_{r,k,p}(R)$ consists of all the functions $f \in A_r(R)$ with the property that for all $n_1, \ldots, n_r \in \mathbb{N}$ with p dividing n_k, one has $f(n_1, \ldots, n_r) = 0$. It was shown in [14] that the generating degree of$A_r(R)$

Mathematical Subject Classification (2000): 11K65, 13F99.
Key words: arithmetical functions, factorization, Dirichlet convolution.

with respect to each of the subrings $B_{r,k,p}(R)$ is equal to 1. For two commutative topological rings $A \subseteq B$, by the generating degree of B over A, one means the cardinality of the smallest subset M of B for which the ring $A[M]$ is dense in B. In the present paper we complement the results from [14] by showing that if R is a field, then all the subrings of $A_r(R)$ of the form $B_{r,k,p}(R)$ are factorial.

Theorem 1 *For any field F, any integer $r \geq 1$, any $k \in \{1, \ldots, r\}$, and any prime number p, the subring $B_{r,k,p}(F)$ of $A_r(F)$ is factorial.*

2 Valuations

Let r be a positive integer, let R be an integral domain, with identity 1_R, and let $A_r(R) = \{f : \mathbb{N}^r \to R\}$. Then R has a natural embedding in the ring $A_r(R)$, and $A_r(R)$ with addition and convolution defined as in the Introduction naturally becomes an R-algebra. We now recall the construction from [1] of a class of absolute values on $A_r(R)$. Fix $\underline{t} = (t_1, \ldots, t_r) \in \mathbb{R}^r$ with $t_1, \ldots, t_r$ linearly independent over $\mathbb{Q}$, and $t_i > 0, (i = 1, 2, \ldots, r)$. Given $n \in \mathbb{N}$, denote by $\Omega(n)$ the total number of prime factors of n, counting multiplicities. Thus, if $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ is the prime factorization of n, then $\Omega(n) = \alpha_1 + \ldots + \alpha_k$. Define also $\Omega_r : \mathbb{N}^r \to \mathbb{N}^r$ by

$$\Omega_r(n_1, \ldots, n_r) = (\Omega(n_1), \ldots, \Omega(n_r)).$$

For any $f \in A_r(R)$ denote $supp(f) = \{\underline{n} \in \mathbb{N}^r | f(\underline{n}) \neq 0\}$, and let

$$V_{\underline{t}}(f) = \min_{\underline{n} \in supp(f)} \underline{t} \cdot \Omega_r(\underline{n}),$$

with the convention $\min(\emptyset) = \infty$. It is shown in [1] that for any $f, g \in A_r(R)$ one has

$$V_{\underline{t}}(f + g) \geq \min(\{V_{\underline{t}}(f), V_{\underline{t}}(g)\}),$$

and

$$V_{\underline{t}}(f * g) = V_{\underline{t}}(f) + V_{\underline{t}}(g).$$

Next, one extends the valuation $V_{\underline{t}}$ to a valuation $\overline{V_{\underline{t}}}$ on the field of fractions $\mathbb{K} = \{\frac{f}{g} | f, g \in A_r(R), g \neq 0\}$ of $A_r(R)$ by letting $V_{\underline{t}}(\frac{f}{g}) = V_{\underline{t}}(f) - V_{\underline{t}}(g)$. The above valuation is nonarchimedean. From now on we will restrict to the case when $R = F$ is a field. One of the important features of this valuation, which will be used in the proof of Theorem 1, is the following. Let f be an element of $A_r(F)$. Then $V_{\underline{t}}(f) = 0$ if and only if f is a unit of $A_r(F)$. Indeed, if f is a unit of $A_r(F)$, then $f(1, 1, \ldots, 1)$ must be a nonzero element of F. Then $(1, 1, \ldots, 1)$ lies in $supp(f)$, and by the definition of $V_{\underline{t}}$ it follows that $V_{\underline{t}}(f) = 0$. Conversely, if $V_{\underline{t}}(f) = 0$, then by the definition of $V_{\underline{t}}$ there exists an $\underline{n} = (n_1, \ldots, n_r)$ in $supp(f)$ for which $(\Omega(n_1), \ldots, \Omega(n_r)) = (0, \ldots, 0)$. This forces each of $n_1, \ldots, n_r$ to equal 1, which in turn implies that $(1, 1, \ldots, 1)$ lies in $supp(f)$, and hence f is a unit of $A_r(F)$. Let us also remark, as another important feature of this valuation, that, although for $r \geq 2$ the image of $\mathbb{K}$ through $\overline{V_{\underline{t}}}$ is dense in $\mathbb{R}$, the image of $A_r(F)$ through $V_{\underline{t}}$ consists of a strictly increasing sequence of nonnegative real numbers

with limit infinity. Therefore any strictly decreasing sequence of such values, say $V_{\underline{t}}(\alpha_1) > V_{\underline{t}}(\alpha_2) > \ldots$, with $\alpha_1, \alpha_2, \ldots$ in $A_r(F)$, must terminate after finitely many steps.

3 Reduction to the full ring $A_r(F)$

Let F be a field. Fix an integer $r \geq 1$, a $k \in \{1, \ldots, r\}$, and a prime number p. Consider the subring $B_{r,k,p}(F)$ of $A_r(F)$ consisting of all the functions $f \in A_r(F)$ with the property that for all $n_1, \ldots, n_r \in \mathbb{N}$ with p dividing n_k, one has $f(n_1, \ldots, n_r) = 0$. As usual, by an irreducible element in a ring R we mean a nonzero, nonunit element a of R with the property that whenever a is written as a product of two elements b and c in the ring, then one of them is a unit.

In proving Theorem 1, our idea is to reduce the satement of the theorem about the subring $B_{r,k,p}(F)$ to the similar statement about the full ring $A_r(F)$, and separately to prove that $A_r(F)$ is factorial. In this section we present the reduction step, that is we show that if $A_r(F)$ is factorial, then $B_{r,k,p}(F)$ is factorial as well.

Lemma 1 *Let $u \in B_{r,k,p}(F)$ be nonzero. Then u is a unit in $B_{r,k,p}(F)$ if and only if u is a unit in $A_r(F)$.*

Proof: It is clear that if u is a unit in $B_{r,k,p}(F)$, then u is a unit in $A_r(F)$. Suppose now that u is a unit in $A_r(F)$. Then there exists $v \in A_r(F)$ such that $u * v = 1$, where 1 is the unity in $A_r(F)$, which as an arithmetical function, is given by

$$1(n_1, \ldots, n_r) = \begin{cases} 1 & \text{if } n_1 = \cdots = n_r = 1, \\ 0 & \text{else.} \end{cases}$$

for $n_1, \ldots, n_r \in \mathbb{N}$. We construct $w \in B_{r,k,p}(F)$ from v as follows. Let $n_1, \ldots, n_r \in \mathbb{N}$. Then we let

$$w(n_1, \ldots, n_r) = \begin{cases} 0 & \text{if } p | n_k, \\ v(n_1, \ldots, n_r) & \text{else.} \end{cases}$$

It follows that $u * w = 1$. To see this, first note that $u * w(1, \ldots, 1) = 1$. For $(n_1, \ldots, n_r) \neq (1, \ldots, 1)$, consider

$$(u * w)(n_1, ..., n_r) = \sum_{d_1 | n_1} \cdots \sum_{d_r | n_r} w(d_1, ..., d_r) u\left(\frac{n_1}{d_1}, ..., \frac{n_r}{d_r}\right). \tag{3.1}$$

If p does not divide n_k, then p does not divide any divisor d_k of n_k, and the above sum equals

$$\sum_{d_1 | n_1} \cdots \sum_{d_r | n_r} v(d_1, ..., d_r) u\left(\frac{n_1}{d_1}, ..., \frac{n_r}{d_r}\right) = (u * v)(n_1, ..., n_r) = 0.$$

So $(u * w)(n_1, ..., n_r) = 0$. Also, if p divides n_k, then each term in the sum on the right side of equation (3.1) is zero. This is because p divides either d_k or $\frac{n_k}{d_k}$ in

each of the terms. So again $(u * w)(n_1, ..., n_r) = 0$. We conclude that $u * w = 1$ and therefore u is a unit in $B_{r,k,p}(F)$.

Lemma 2 *Let $\pi \in B_{r,k,p}(F)$ be nonzero. Then π is an irreducible element of $B_{r,k,p}(F)$ if and only if π is an irreducible element of $A_r(F)$.*

Proof: Suppose that π is an irreducible element of $A_r(F)$. If π is not an irreducible element of $B_{r,k,p}(F)$, then there exist $a, b \in B_{r,k,p}(F)$ such that both a and b are nonunits in $B_{r,k,p}(F)$, and $\pi = a * b$. By Lemma 1 both a and b are nonunits in $A_r(F)$. This contradicts our assumption that π is irreducible in $A_r(F)$. Hence, π is an irreducible element of $B_{r,k,p}(F)$ as well.

Conversely, suppose that π is an irreducible element of $B_{r,k,p}(F)$. Assume $\pi = a * b$ with $a, b \in A_r(F)$. We construct $a', b' \in B_{r,k,p}(F)$ from a and b in the same way we constructed w from v in the proof of Lemma 1. That is, for $n_1, \ldots, n_r \in \mathbb{N}$ we let

$$a'(n_1, \ldots, n_r) = \begin{cases} 0 & \text{if } p | n_k, \\ a(n_1, \ldots, n_r) & \text{else.} \end{cases}$$

and

$$b'(n_1, \ldots, n_r) = \begin{cases} 0 & \text{if } p | n_k, \\ b(n_1, \ldots, n_r) & \text{else.} \end{cases}$$

Then one easily sees that $\pi = a' * b'$. Since π is irreducible in $B_{r,k,p}(F)$, either a' or b', say a', is a unit in $B_{r,k,p}(F)$. By Lemma 1, a' is also a unit in $A_r(F)$. We now show that a is a unit in $A_r(F)$. Write $a = a' + y$, where y is supported only on the set of all points $(n_1, \ldots, n_r) \in \mathbb{N}^r$ with the property that p divides n_k. Since a' is a unit in $B_{r,k,p}(F)$, there exists an element a'' of $B_{r,k,p}(F)$ such that $a' * a'' = 1$. Thus $a * a'' = a' * a'' + y * a'' = 1 + y * a''$. Define $f \in A_r(F)$ by $f = \sum_{m=0}^{\infty} (-1)^m (y * a'')^m = 1 - y * a'' + (y * a'')^2 - (y * a'')^3 + \ldots$. Note that f is a well defined element of $A_r(F)$ since for each fixed $(n_1, \ldots, n_r) \in \mathbb{N}^r$, there exists $n \in \mathbb{N}$ such that $(y * a'')^m (n_1, \ldots, n_r) = 0$ for all $m > n$. Observe that $a * a'' * f = 1$, and thus a is invertible in $A_r(F)$. This completes the proof of the lemma.

Lemma 3 *If $A_r(F)$ is factorial, then the subring $B_{r,k,p}(F)$ is factorial.*

Proof: First we show that each nonzero element $a \in B_{r,k,p}(F)$ can be expressed as a finite product of irreducible elements of $B_{r,k,p}(F)$. Indeed, if a is not irreducible in $B_{r,k,p}(F)$, then there exist nonunits $b, c \in B_{r,k,p}(F)$ such that $a = b * c$. By Lemma 1, b and c are also non units of $A_r(F)$. If any of the elements b and c is not irreducible in $B_{r,k,p}(F)$, then we may again write that element as a product of two elements in $B_{r,k,p}(F)$ which are nonunits in both $B_{r,k,p}(F)$ and $A_r(F)$. This process must stop after finitely many steps since otherwise we obtain a contradiction with the assumption that $A_r(F)$ is factorial. Hence we conclude that each element $a \in B_{r,k,p}(F)$ can be expressed as a finite product $a = a_1 * a_2 * \cdots * a_m$ of irreducible elements of $B_{r,k,p}(F)$.

Secondly we need to establish the uniqueness of the expressions $a = a_1 * a_2 * \cdots * a_m$ in $B_{r,k,p}(F)$ up to order and units. Suppose that $a = a_1 * a_2 * \cdots * a_m = b_1 * b_2 * \cdots * b_s$ $(m, s \in \mathbb{N})$ where a_i $(i = 1, \ldots, m)$ and b_j $(j = 1, \ldots, s)$ are irreducible elements of $B_{r,k,p}(F)$. By Lemma 2 and the assumption that $A_r(F)$ is factorial we have that $m = s$, and there exist w_i $(i = 1, \ldots, m)$ such that $a_i = b_i * w_i$ $(i = 1, \ldots, m)$ and w_i $(i = 1, \ldots, m)$ are units in $A_r(F)$. Let $n_1, \ldots, n_r \in \mathbb{N}$, and define $v_i \in B_{r,k,p}(F)$ $(i = 1, \ldots, m)$ as follows.

$$v_i(n_1, \ldots, n_r) = \begin{cases} 0 & \text{if } p | n_k, \\ w_i(n_1, \ldots, n_r) & \text{else.} \end{cases}$$

It is easily verified that for each $i \in \{1, \ldots, m\}$, one has $a_i = b_i * w_i = b_i * v_i$, and v_i is a unit in $A_r(F)$. But by Lemma 1, v_i is also a unit in $B_{r,k,p}(F)$. Hence the lemma is proved.

4 Completion of proof of Theorem 1

In order to complete the proof of Theorem 1, it remains to show that $A_r(F)$ is factorial. Let us fix a $\underline{t} = (t_1, \ldots, t_r) \in \mathbb{R}^r$ with $t_1, \ldots, t_r$ linearly independent over $\mathbb{Q}$, $t_i > 0, (i = 1, 2, \ldots, r)$, and consider the valuation $V_{\underline{t}}$ defined in Section 2.

Lemma 4 *Every $\alpha \in A_r(F)$ which is not zero and not a unit is expressible as a finite product of irreducible elements of $A_r(F)$.*

Proof: In order to prove the lemma, consider a nonzero element $\alpha \in A_r(F)$ which is not a unit. We need to show that α can be written as a finite product of irreducible elements of $A_r(F)$. If α is itself irreducible, there is nothing to prove. Let us assume that α is not irreducible. Then α can be written as $\alpha = \alpha_1 * \beta_1$, with α_1, β_1 nonunit elements of $A_r(F)$. By the results of Section 2 we know that $V_{\underline{t}}(\alpha_1) > 0$, $V_{\underline{t}}(\beta_1) > 0$, and

$$V_{\underline{t}}(\alpha) = V_{\underline{t}}(\alpha_1) + V_{\underline{t}}(\beta_1).$$

If α_1 and β_1 are both irreducibe then the lemma is proved. If not, we continue the same procedure with α replaced by α_1 or β_1. Note by the properties of the valuation $V_{\underline{t}}$ discussed Section 2, that since each of α_1 and β_1 has a valuation that is strictly smaller than the valuation of α, the above procedure must terminate after finitely many steps. This completes the proof of the lemma.

We now consider the ring of formal r-fold power series, which is defined as follows. Let us list the prime numbers in increasing order: $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$. Then every integer n may be written uniquely in the form $n = p_1^{\alpha_1(n)} p_2^{\alpha_2(n)} \cdots$ and uniquely described by a vector $(\alpha_1(n), \alpha_2(n), \ldots)$ with non-negative integral components where only finitely many of the components are nonzero. All such vectors are realized as n ranges over $\mathbb{N}$. Hence an arithmetic function $a = a(n) \in A_1(F)$

in one variable may be associated with a definite formal power series in a countably infinite number of indeterminates $y_{p_1}, y_{p_2}, y_{p_3}, \ldots$, having coefficients in F, by means of the correspondence

$$a \to P(a) = \sum_n a(n) y_{p_1}^{\alpha_1(n)} y_{p_2}^{\alpha_2(n)} \ldots .$$

Here, the summation extends over all $n = p_1^{\alpha_1(n)} p_2^{\alpha_2(n)} p_3^{\alpha_3(n)} \ldots$ in $\mathbb{N}$. Also, an arithmetic function $a = a(n_1, n_2) \in A_2(F)$ in two variables may be associated with a definite formal power series in a countably infinite number of indeterminates $x_{p_1}, x_{p_2}, x_{p_3}, \ldots$, $y_{p_1}, y_{p_2}, y_{p_3}, \ldots$ having coefficients in F, by means of the correspondence

$$a \to P(a) = \sum_n \sum_m a(n,m) x_{p_1}^{\alpha_1(n)} y_{p_1}^{\alpha_1(m)} x_{p_2}^{\alpha_2(n)} y_{p_2}^{\alpha_2(m)} \ldots .$$

Here, the summation extends over all

$$n = p_1^{\alpha_1(n)} p_2^{\alpha_2(n)} p_3^{\alpha_3(n)} \ldots$$

and

$$m = p_1^{\alpha_1(n)} p_2^{\alpha_2(n)} p_3^{\alpha_3(n)} \ldots$$

in $\mathbb{N}$. In general, an arithmetic function $a = a(n_1, \ldots, n_r) \in A_r(F)$ in r variables may be associated with a definite formal r-fold power series in a countably infinite number of indeterminates $x_{1p_1}, x_{1p_2}, \ldots, x_{2p_1}, x_{2p_2}, \ldots, \ldots, x_{rp_1}, x_{rp_2}, \ldots$, having coefficients in F, by means of the correspondence

$$a \to P(a) = \sum_{n_1} \sum_{n_2} \cdots \sum_{n_r} a(n_1, \ldots, n_r) x_{1p_1}^{\alpha_1(n_1)} x_{2p_1}^{\alpha_1(n_2)} \ldots x_{rp_1}^{\alpha_1(n_r)} x_{1p_2}^{\alpha_2(n_1)} x_{2p_2}^{\alpha_2(n_2)} \ldots x_{rp_2}^{\alpha_2(n_r)} \ldots .$$

Here, the summation extends over all

$$n_1 = p_1^{\alpha_1(n_1)} p_2^{\alpha_2(n_1)} p_3^{\alpha_3(n_1)} \ldots ,$$

$$n_2 = p_1^{\alpha_1(n_2)} p_2^{\alpha_2(n_2)} p_3^{\alpha_3(n_2)} \ldots ,$$

$$\ldots$$

$$n_r = p_1^{\alpha_1(n_r)} p_2^{\alpha_2(n_r)} p_3^{\alpha_3(n_r)} \ldots$$

of $\mathbb{N}$. This correspondence is clearly one to one on $A_r(F)$ to the set

$$F\{\ldots, x_{ip_j}, \ldots\} = F\{x_{1p_1}, x_{1p_2}, \ldots\}\{x_{2p_1}, x_{2p_2}, \ldots\} \ldots \{x_{rp_1}, x_{rp_2}, \ldots\}$$

of all such power series. Moreover, addition is preserved, and as we will see below $P(f * g) = P(f)P(g)$. The latter operation is the usual formal operation on power series involving multiplication and collection of finite number of like terms. Thus the ring $A_r(F)$ is isomorphic to the ring $F\{x_{ip_j}\}$ of all r-fold formal power series. We emphasize that only a finite number of x_{ip_j} actually appear (i.e., have

$\alpha_j(n_i) > 0$) in any term. However, infinitely many x_{ip_j} may well occur in the same series. We now prove that $P(f * g) = P(f)P(g)$. One has

$$P(f)P(g)$$

$$= \left(\sum_{n_1} \sum_{n_2} \cdots \sum_{n_r} f(n_1, \ldots, n_r) x_{1p_1}^{\alpha_1(n_1)} x_{2p_1}^{\alpha_1(n_2)} \cdots x_{rp_1}^{\alpha_1(n_r)} x_{1p_2}^{\alpha_2(n_1)} x_{2p_2}^{\alpha_2(n_2)} \cdots x_{rp_2}^{\alpha_2(n_r)} \cdots \right)$$

$$\left(\sum_{m_1} \sum_{m_2} \cdots \sum_{m_r} g(m_1, \ldots, m_r) x_{1p_1}^{\alpha_1(m_1)} x_{2p_1}^{\alpha_1(m_2)} \cdots x_{rp_1}^{\alpha_1(m_r)} x_{1p_2}^{\alpha_2(m_1)} x_{2p_2}^{\alpha_2(m_2)} \cdots x_{rp_2}^{\alpha_2(m_r)} \cdots \right)$$

$$= \sum_{\substack{n_1, \ldots, n_r \\ m_1, \ldots, m_r}} f(n_1, \ldots, n_r) g(m_1, \ldots, m_r)$$

$$x_{1p_1}^{\alpha_1(n_1)+\alpha_1(m_1)} x_{2p_1}^{\alpha_1(n_2)+\alpha_1(m_2)} \cdots x_{rp_1}^{\alpha_1(n_r)+\alpha_1(m_r)} x_{1p_2}^{\alpha_2(n_1)+\alpha_2(m_1)} x_{2p_2}^{\alpha_2(n_2)+\alpha_2(m_2)} \cdots x_{rp_2}^{\alpha_2(n_r)+\alpha_2(m_r)} \cdots$$

This further equals

$$\sum_{\substack{n_1, \ldots, n_r \\ m_1, \ldots, m_r}} f(n_1, \ldots, n_r) g(m_1, \ldots, m_r)$$

$$x_{1p_1}^{\alpha_1(n_1 m_1)} x_{2p_1}^{\alpha_1(n_2 m_2)} \cdots x_{rp_1}^{\alpha_1(n_r m_r)} x_{1p_2}^{\alpha_2(n_1 m_1)} x_{2p_2}^{\alpha_2(n_2 m_2)} \cdots x_{rp_2}^{\alpha_2(n_r m_r)} \cdots$$

$$= \sum_{k_1, \ldots, k_r} \left(\sum_{k_1 = m_1 n_1} \cdots \sum_{k_r = m_r n_r} f(n_1, \ldots, n_r) g(m_1, \ldots, m_r) \right)$$

$$x_{1p_1}^{\alpha_1(k_1)} x_{2p_1}^{\alpha_1(k_2)} \cdots x_{rp_1}^{\alpha_1(k_r)} x_{1p_2}^{\alpha_2(k_1)} x_{2p_2}^{\alpha_2(k_2)} \cdots x_{rp_2}^{\alpha_2(k_r)} \cdots$$

$$= \sum_{k_1, \ldots, k_r} (f * g)(k_1, \ldots, k_r) x_{1p_1}^{\alpha_1(k_1)} x_{2p_1}^{\alpha_1(k_2)} \cdots x_{rp_1}^{\alpha_1(k_r)} x_{1p_2}^{\alpha_2(k_1)} x_{2p_2}^{\alpha_2(k_2)} \cdots x_{rp_2}^{\alpha_2(k_r)} \cdots$$

$$= P(f * g).$$

Next, for any positive integer l, any $k \in \{1, \ldots, r\}$, and any power series $Q \in F\{\ldots, x_{ip_j}, \ldots\}$, denote by $deg_{x_{kp_l}}(Q)$ the supremum of the set of exponents of x_{kp_l} that appear in the terms of Q with nonzero coefficients. Also, for a positive integer l, and $k \in \{1, \ldots, r\}$, denote by $F\{\ldots, x_{ip_j}, \ldots\}_{(i,p_j) \neq (k,p_l)}$ the subring of $F\{\ldots, x_{ip_j}, \ldots\}$ which consists of all power series Q in $F\{\ldots, x_{ip_j}, \ldots\}$ such that $deg_{x_{kp_l}}(Q)$ is zero. Under the above isomorphism the ring $B_{r,k,p}(F)$ is isomorphic to the subring

$$F\{\ldots, x_{ip_j}, \ldots\}_{(i,p_j) \neq (k,p)}.$$

Cashwell and Everett [2] proved that $(A_1(\mathbb{C}), +, .)$, where $\mathbb{C}$ denotes the field of complex numbers, is a unique factorization domain by showing that the corresponding power series ring $\mathbb{C}\{x_{1p_1}, x_{1p_2}, \ldots\}$ is a unique factorization domain. Next, we show that for any positive integer r, $A_r(F)$ is a unique factorization domain by showing that the corresponding r-fold power series ring

$$F\{\ldots, x_{ip_j}, \ldots\} = F\{x_{1p_1}, x_{1p_2}, \ldots\}\{x_{2p_1}, x_{2p_2}, \ldots\} \ldots \{x_{rp_1}, x_{rp_2}, \ldots\}$$

is a unique factorization domain. We have already shown that every element of $(A_r(F), +, .)$ can be written as a finite product of irreducible elements. So we

need to establish the uniqueness of the expression of a non-zero, non-unit element of $A_r(F)$ as a product of irreducibles in $A_r(F)$ up to order and units. We first show that the uniqueness holds for the case $r = 2$. We proceed in several steps. Let $S[x_1, \ldots, x_l]$ denote the ring of formal power series in l indeterminates with coefficients in S, where S is any ring. Let $H = F\{x_{2p_1}, x_{2p_2}, \ldots x_{(2,p_j)}\}$. At the first step, we show that the ring $F\{x_{1p_1}, x_{1p_2}, \ldots\}\{x_{2p_1}, x_{2p_2}, \ldots\}$ is isomorphic to the ring $H\{x_{1p_1}, x_{1p_2}, \ldots\}$ of 1-fold formal power series with coefficents in H. Then we need to show that $H\{x_{1p_1}, x_{1p_2}, \ldots\}$ is a a unique factorization domain. By the proof of Cashwell and Everett [2], it is enough to show that for any positive integer l, $H[x_{1p_1}, x_{1p_2}, \ldots, x_{1p_l}]$ is a unique factorization domain. At the second step, we show that for any positive integer $l, H[x_{1p_1}, x_{1p_2}, \ldots, x_{1p_l}]$ is isomorphic to $F[x_{1p_1}, \ldots, x_{1p_l}]\{x_{2p_1}, x_{2p_2}, \ldots\}$. Again by the proof of Cashwell and Everett [2], $F[x_{1p_1}, \ldots, x_{1p_l}]\{x_{2p_1}, x_{2p_2}, \ldots\}$ is a unique factorization domain if for any positive integer l', $F[x_{1p_1}, \ldots, x_{1p_l}][x_{2p_1}, x_{2p_2}, \ldots, x_{2p_l'}]$ is isomorphic to $F[x_{1p_1}, \ldots, x_{1p_l}, x_{2p_1}, x_{2p_2}, \ldots, x_{2p_l'}]$. So, at the third step we establish the last isomorphism. We now proceed with the first step. To show that $F\{x_{1p_1}, x_{1p_2}, \ldots\}\{x_{2p_1}, x_{2p_2}, \ldots\}$ is isomorphic to the ring $H\{x_{1p_1}, x_{1p_2}, \ldots\}$, we first replace the set $x_{1p_1}, x_{1p_2}, \ldots$ of variables by the set $x_{p_1}, x_{p_2}, \ldots$, and the set $x_{2p_1}, x_{2p_2}, \ldots$ by $y_{p_1}, y_{p_2}, \ldots$. Given

$$f \in F\{x_{p_1}, x_{p_2}, \ldots\}\{y_{p_1}, y_{p_2}, \ldots\}, f = \sum_n \sum_m f(n,m) x_{p_1}^{\alpha_1(n)} y_{p_1}^{\alpha_1(m)} x_{p_2}^{\alpha_2(n)} y_{p_2}^{\alpha_2(m)} \ldots,$$

we define $f_H \in H\{x_{p_1}, x_{p_2}, \ldots\}$, where $H = F\{y_{p_1}, y_{p_2}, \ldots\}$, to be the series

$$f_H = \sum_n f_H(n) x_{p_1}^{\alpha_1(n)} x_{p_2}^{\alpha_2(n)} \ldots,$$

where

$$f_H(n) = \sum_m f(n,m) y_{p_1}^{\alpha_1(m)} y_{p_2}^{\alpha_2(m)} \ldots.$$

for each n. The map $f \to f_H$ is clearly a bijective map.

Also for $f, g \in F\{x_{p_1}, x_{p_2}, \ldots\}\{y_{p_1}, y_{p_2}, \ldots\}$, we have that

$$\begin{aligned}(fg) &= \sum_{n_1} \sum_{m_1} \sum_{n_2} \sum_{m_2} f(n_1, m_1) g(n_2, m_2) x_{p_1}^{\alpha_1(n_1 n_2)} y_{p_1}^{\alpha_1(m_1 m_2)} x_{p_2}^{\alpha_2(n_1 n_2)} y_{p_2}^{\alpha_2(m_1 m_2)} \ldots \\ &= \sum_n \sum_m \left(\sum_{n = n_1 n_2} \sum_{m = m_1 m_2} f(n_1, m_1) g(n_2, m_2) \right) x_{p_1}^{\alpha_1(n)} y_{p_1}^{\alpha_1(m)} x_{p_2}^{\alpha_2(n)} y_{p_2}^{\alpha_2(m)} \ldots.\end{aligned}$$

So,

$$
\begin{aligned}
(fg)_H &= \sum_n \left(\sum_m \left(\sum_{n=n_1n_2} \sum_{m=m_1m_2} f(n_1,m_1)g(n_2,m_2) \right) y_{p_1}^{\alpha_1(m)} y_{p_2}^{\alpha_2(m)} \dots \right) x_{p_1}^{\alpha_1(n)} x_{p_2}^{\alpha_2(n)} \dots \\
&= \left(\sum_{n_1} \left(\sum_{m_1} f(n_1,m_1) y_{p_1}^{\alpha_1(m_1)} y_{p_2}^{\alpha_2(m_1)} \dots \right) x_{p_1}^{\alpha_1(n_1)} x_{p_2}^{\alpha_2(n_1)} \dots \right) \\
&\quad \left(\sum_{n_2} \left(\sum_{m_2} f(n_2,m_2) y_{p_1}^{\alpha_1(m_2)} y_{p_2}^{\alpha_2(m_2)} \dots \right) x_{p_1}^{\alpha_1(n_2)} x_{p_2}^{\alpha_2(n_2)} \dots \right) \\
&= \left(\sum_{n_1} f_H(n_1) x_{p_1}^{\alpha_1(n_1)} x_{p_2}^{\alpha_2(n_1)} \dots \right) \left(\sum_{n_2} g_H(n_2) x_{p_1}^{\alpha_1(n_2)} x_{p_2}^{\alpha_2(n_2)} \dots \right) \\
&= f_H g_H .
\end{aligned}
$$

Thus, the map $f \to f_H$ is an isomorphism. This finishes step one.

Next, we prove the second step. To do so it suffices to prove that for any positive integer l, $H[x_{p_1}, x_{p_2}, \dots x_{p_l}]$ is isomorphic to $F[x_{p_1}, \dots, x_{p_l}]\{y_{p_1}, y_{p_2}, \dots\}$, where H is as in the proof of the first step. Let $a \in H[x_{p_1}, x_{p_2}, \dots, x_{p_l}]$. Let $a = \sum_n a_H(n) x_{p_1}^{\alpha_1(n)} \cdots x_{p_l}^{\alpha_l(n)}$, where for each n, $a_H(n) \in H$, and $a_H(n) = \sum_m a(n,m) y_{p_1}^{\alpha_1(m)} y_{p_2}^{\alpha_2(m)} \cdots$. Define $\overline{a} \in F[x_{p_1}, \dots, x_{p_l}]\{y_{p_1}, y_{p_2}, \dots\}$ by $\overline{a} = \sum_m \overline{a}(m) y_{p_1}^{\alpha_1(m)} y_{p_2}^{\alpha_2(m)} \cdots$, where for each m, $\overline{a}(m) = \sum_n a(n,m) x_{p_1}^{\alpha_1(n)} \cdots x_{p_l}^{\alpha_l(n)}$. The map $a \to \overline{a}(m)$ is a homomorphism. To see this let $a, b \in H[x_{p_1}, x_{p_2}, \dots, x_{p_l}]$, and let $c = ab$. Then $c_H(n) = \sum_{n=n_1n_2} a_H(n_1) b_H(n_2)$, and

$$
\begin{aligned}
a_H(n_1) b_H(n_2) &= \left(\sum_{m_1} a(n_1,m_1) y_{p_1}^{\alpha_1(m_1)} y_{p_2}^{\alpha_2(m_1)} \dots \right) \left(\sum_{m_2} b(n_2,m_2) y_{p_1}^{\alpha_1(m_2)} y_{p_2}^{\alpha_2(m_2)} \dots \right) \\
&= \sum_m \left(\sum_{m=m_1m_2} a(n_1,m_1) b(n_2,m_2) \right) y_{p_1}^{\alpha_1(m)} y_{p_2}^{\alpha_2(m)} \dots .
\end{aligned}
$$

So,

$$
\begin{aligned}
ab &= \left(\sum_{n_1} a_H(n_1) x_{p_1}^{\alpha_1(n_1)} \cdots x_{p_l}^{\alpha_l(n_1)} \right) \left(\sum_{n_2} b_H(n_2) x_{p_1}^{\alpha_1(n_2)} \cdots x_{p_l}^{\alpha_l(n_2)} \right) \\
&= \sum_n \left(\sum_{n=n_1n_2} a_H(n_1) b_H(n_2) \right) x_{p_1}^{\alpha_1(n)} \cdots x_{p_l}^{\alpha_l(n)}
\end{aligned}
$$

Thus,

$$\begin{aligned}
\overline{ab} &= \sum_m \left(\sum_n \left(\sum_{n=n_1 n_2} \sum_{m=m_1 m_2} a(n_1,m_1) b(n_2,m_2) \right) x_{p_1}^{\alpha_1(n)} \cdots x_{p_l}^{\alpha_l(n)} \right) y_{p_1}^{\alpha_1(m)} y_{p_2}^{\alpha_2(m)} \cdots \\
&= \left(\sum_{m_1} \left(\sum_{n_1} a(n_1,m_1) x_{p_1}^{\alpha_1(n_1)} \cdots x_{p_l}^{\alpha_l(n_1)} \right) y_{p_1}^{\alpha_1(m_1)} y_{p_2}^{\alpha_2(m_1)} \cdots \right) \\
&\left(\sum_{m_2} \left(\sum_{n_2} b(n_2,m_2) x_{p_1}^{\alpha_1(n_2)} \cdots x_{p_l}^{\alpha_2(n_2)} \right) y_{p_1}^{\alpha_1(m_2)} y_{p_2}^{\alpha_2(m_2)} \cdots \right) \\
&= \left(\sum_{m_1} \overline{a}(n_1) y_{p_1}^{\alpha_1(m_1)} y_{p_2}^{\alpha_2(m_1)} \cdots \right) \left(\sum_{m_2} \overline{b}(n_2) y_{p_1}^{\alpha_1(m_2)} y_{p_2}^{\alpha_2(m_2)} \cdots \right) \\
&= \overline{a}\,\overline{b}
\end{aligned}$$

Therefore, the map $a \to \overline{a}$ is a homomorphism. It is clear that this map is also a bijective map. Hence, $H[x_{p_1}, x_{p_2}, \ldots x_{p_l}]$ is isomorphic to $F[x_{p_1}, \ldots, x_{p_l}]\{y_{p_1}, y_{p_2}, \ldots\}$. This finishes step two. As for step three, one can argue similarly as above to conclude that the ring

$$F[x_{1p_1}, \ldots, x_{1p_l}][x_{2p_1}, x_{2p_2}, \ldots, x_{2p_l'}]$$

is isomorphic to the ring

$$F[x_{1p_1}, \ldots, x_{1p_l}, x_{2p_1}, x_{2p_2}, \ldots, x_{2p_l'}],$$

which finishes the proof in this case. The case of a general r is proved similarly, and with this the proof of Theorem 1 is complete.

References

[1] E. Alkan, A. Zaharescu, M. Zaki, *Arithmetical functions in several variables*, Int. J. Number Theory **1**, no. 3 (2005), 383–399.

[2] E.D. Cashwell, C.J. Everett, *The ring of number-theoretic functions*, Pacific J. Math. **9** (1959), 975–985.

[3] P. Haukkanen, *Comparison of regular convolutions*, Portugal. Math. **46**, no. 1 (1989), 59–69.

[4] W. Narkiewicz, *On a class of arithmetical convolutions*, Colloq. Math. **10** (1963), 81–94.

[5] H. Scheid, *Über ordnungstheoretische Funktionen*, J. Reine Angew. Math. **238** (1969), 1–13.

[6] H. Scheid, *Funktionen über lokal endlichen Halbordnungen. I*, Monatsh. Math. **74** (1970), 336–347.

[7] H. Scheid, *Funktionen über lokal endlichen Halbordnungen. II*, Monatsh. Math. **75** (1971), 44–56.

[8] E.D. Schwab, *Möbius categories as reduced standard division categories of combinatorial inverse monoids*, Semigroup Forum **69**,no. 1 (2004), 30–40.

[9] E.D. Schwab, *The Möbius category of some combinatorial inverse semigroups*, Semigroup Forum **69**, no. 1 (2004), 41–50.

[10] E.D. Schwab, G. Silberberg, *A note on some discrete valuation rings of arithmetical functions*, Arch. Math. (Brno), **36** (2000), 103-109.

[11] E.D. Schwab, G. Silberberg, *The Valuated ring of the Arithmetical Functions as a Power Series Ring*, Arch. Math. (Brno), **37** (2001), 77–80.

[12] V. Sitaramaiah, *Arithmetical sums in regular convolutions*, J. Reine Angew. Math. **303/304** (1978), 265–283.

[13] K.L. Yokom, *Totally multiplicative functions in regular convolution rings*, Canadian Math. Bulletin **16** (1973), 119–128.

[14] M. Zaki, A. Zaharescu, *Derivations and generating degrees in the ring of arithmetical functions*, to appear in Proc. Indian Acad. Sci. Math. Sci.

Alexandru Zaharescu
Department of Mathematics,
University of Illinois at Urbana-Champaign,
1409 W. Green Street, Urbana, IL, 61801, USA.
e-mail: zaharesc@math.uiuc.edu

Mohammad Zaki
Department of Mathematics,
University of Illinois at Urbana-Champaign,
1409 W. Green Street, Urbana, IL, 61801, USA.
e-mail: mzaki@math.uiuc.edu

CONTENTS

Author	Title	Page
Endô, A.	On the Maillet determinant associated with a Dirichlet character	1
Ueda, K. and Yoshinaga, M.	Logarithmic vector fields along smooth plane cubic curves	11
Shi, H.G. and Chen, G.Y.	$D_{p+1}(3)(p \geq 3)$ can be characterized by its order components	21
Zaharescu, A. and Zaki, M.	Factorization in certain rings of arithmetical functions	29