On some properties of polynomials related to hypergeometric modular forms

Masanobu Kaneko and Naruya Niiho

Abstract

We give the discriminants, irreducibility result, and Galois groups of certain hypergeometric polynomials, which are closely related to modular forms and supersingular elliptic curves.

1. Introduction and Main Result.

The present article deals with a series of hypergeometric polynomials $P_m^{(r)}(x)$ $(m = 0, 1, 2, \ldots)$ which is defined, for each integer r with $0 \le r \le 5$, as follows. First define ν_0 and ν_1 by

$$\nu_0 = \begin{cases} \dfrac{1}{3}, & \text{if} \quad r \bmod 3 = 0, \\ -1, & \text{if} \quad r \bmod 3 = 1, \\ -\dfrac{1}{3}, & \text{if} \quad r \bmod 3 = 2, \end{cases} \qquad \nu_1 = \begin{cases} \dfrac{1}{2}, & \text{if} \quad r \bmod 2 = 0, \\ -\dfrac{1}{2}, & \text{if} \quad r \bmod 2 = 1. \end{cases}$$

Then the $P_m^{(r)}(x)$ is given by

$$P_m^{(r)}(x) = x^m \, F(-m, -m + \nu_0; -2m + \nu_0 + \nu_1; \frac{12^3}{x}),$$

where $F(a, b; c; x)$ is the classical Gauss hypergeometric series:

$$F(a, b; c; x) = 1 + \sum_{i=1}^{\infty} \frac{a(a+1)\cdots(a+i-1)b(b+1)\cdots(b+i-1)}{c(c+1)\cdots(c+i-1)} \frac{x^i}{i!}.$$

The $P_m^{(r)}(x)$ is a monic polynomial of degree m with rational coefficients.

In [2], we studied certain "hypergeometric modular forms" which are intimately connected to the j-invariants of supersingular elliptic curves. Our polynomials $P_m^{(r)}(x)$ for $r \bmod 3 = 0, 2$ are the ones describing the values of the elliptic modular j-function at the essential zeros of such modular forms and reduce modulo specific primes to the (essential factor of) supersingular j-polynomials in those characteristics. For instance, we have

$$P_2^{(2)}(x) = x^2 - \frac{48384}{23}x + \frac{334430208}{391},$$

which reduces modulo 29 to $(x - 2)(x + 4)$. The supersingular j-invariants in characteristic 29 are 0 ("trivial" one, coming from $j((-1 + \sqrt{-3})/2) = 0$), 2 and -4. For more details of this connection, we refer the reader to [2].

Our objective is to prove the following theorem.

2000 Mathematics Subject Classification: Primary 33C45; Secondary 11F11.
Key Words and Phrases: Hypergeometric modular forms, orthogonal polynomials.

Theorem. 1) *The discriminant of the polynomial* $P_m^{(r)}(x)$ *is given by*

$$12^{3m(m-1)}\prod_{i=1}^{m}\frac{i^i(i-\nu_0)^{i-1}(i-\nu_1)^{i-1}}{(m+i-\nu_0-\nu_1)^{m+i-2}}.$$

2) *If* $3m-1$ *(resp.* $3m+1$*) is prime, then* $P_m^{(0)}(x)$ *and* $P_m^{(3)}(x)$ *(resp.* $P_m^{(2)}(x)$ *and* $P_m^{(5)}(x)$*) are irreducible over the rationals.*

3) *The Galois group of* $P_m^{(r)}(x)$ *over the rationals is the full symmetric group for all* r *and* $m \le 150$*.*

Remarks. 1) By Dirichlet's theorem on primes in an arithmetic progression, there are infinitely many m such that $3m-1$ (resp. $3m+1$) is prime.

2) The theorem was essentially obtained in the bachelor's thesis by the second named author submitted to the Kyoto Institute of Technology in March 1996.

3) In a recent work by K. Mahlburg and K. Ono [3], done independently of the present work, the same subject is discussed. There, they use a modified polynomial instead of our $P_m^{(r)}(x)$ in order to avoid larger coefficients. Their Theorem 3.1 should be equivalent to our Theorem 1), whereas our Theorem 2) seems not to be covered by their Theorem 1.1 and 1.2 where a more extensive irreducibility results are obtained. They also discuss more the Galois groups of the polynomials.

2. Proof.

1) We adopt the method employed by I. Schur in [4]. By using the derivative formula and the contiguous relations of hypergeometric series (*cf.* [1]), we obtain the relation

$$\begin{aligned}
&(2m-\nu_0-\nu_1)^2(2m-1-\nu_0-\nu_1)x(x-12^3)P_m^{(r)\prime}(x)\\
=\;& m(2m-\nu_0-\nu_1)(2m-1-\nu_0-\nu_1)\left\{(2m-\nu_0-\nu_1)x-12^3(m-\nu_1)\right\}P_m^{(r)}(x)\\
&-12^6m(m-\nu_0)(m-\nu_1)(m-\nu_0-\nu_1)P_{m-1}^{(r)}(x).
\end{aligned}\tag{1}$$

Here, $P_m^{(r)\prime}(x)$ is the derivative of $P_m^{(r)}(x)$ with respect to x. Denote by $D_m^{(r)}$ and $R_m^{(r)}$ the discriminant of $P_m^{(r)}(x)$ and the resultant of $P_m^{(r)}(x)$ and $P_{m-1}^{(r)}(x)$, respectively. Let α_i $(1 \le i \le m)$ (resp. β_j $(1 \le j \le m-1)$) be the roots of $P_m^{(r)}(x)$ (resp. $P_{m-1}^{(r)}(x)$). Then we have

$$D_m^{(r)} = (-1)^{m(m-1)/2}\prod_{i=1}^{m}P_m^{(r)\prime}(\alpha_i),$$

and

$$R_m^{(r)} = \prod_{i=1}^{m}P_{m-1}^{(r)}(\alpha_i) = \prod_{j=1}^{m-1}P_m^{(r)}(\beta_j).$$

Setting $x=\alpha_i$ in (1) and taking the product $\prod_{i=1}^{m}$, we obtain

$$\begin{aligned}
&(-1)^{m(m-1)/2}(2m-\nu_0-\nu_1)^{2m}(2m-1-\nu_0-\nu_1)^m\prod_{i=1}^{m}\alpha_i(\alpha_i-12^3)\cdot D_m^{(r)}\\
=\;& (-1)^m12^{6m}m^m(m-\nu_0)^m(m-\nu_1)^m(m-\nu_0-\nu_1)^mR_m^{(r)}.
\end{aligned}\tag{2}$$

Since

$$\prod_{i=1}^{m}\alpha_i(\alpha_i-1728)=P_m^{(r)}(0)P_m^{(r)}(1728)=(-1)^m12^{6m}\prod_{i=1}^{m}\frac{(i-\nu_0)(i-\nu_1)}{(m+i-\nu_0-\nu_1)^2},$$

we have

$$\begin{aligned}&(-1)^{m(m-1)/2}(2m-\nu_0-\nu_1)^{2m}(2m-1-\nu_0-\nu_1)^m\prod_{i=1}^{m}\frac{(i-\nu_0)(i-\nu_1)}{(m+i-\nu_0-\nu_1)^2}\cdot D_m^{(r)}\\ =\;& m^m(m-\nu_0)^m(m-\nu_1)^m(m-\nu_0-\nu_1)^mR_m^{(r)}.\end{aligned}\tag{3}$$

On the other hand, by the recurrence relation ([2, Theorem 6])

$$P_m^{(r)}(x)=(x-(\lambda_{2m-2}+\lambda_{2m-1}))P_{m-1}^{(r)}(x)-\lambda_{2m-3}\lambda_{2m-2}P_{m-2}^{(r)}(x)\qquad(m\ge 2)$$

where

$$\lambda_n=12\left(6-(-1)^n\frac{3-6\nu_0}{n-\nu_0-\nu_1}\right)\left(6-(-1)^n\frac{3-6\nu_0}{n+1-\nu_0-\nu_1}\right),$$

we have

$$P_m^{(r)}(\beta_j)=-\lambda_{2m-3}\lambda_{2m-2}P_{m-2}^{(r)}(\beta_j)$$

and thus

$$R_m^{(r)}=(-\lambda_{2m-3}\lambda_{2m-2})^{m-1}R_{m-1}^{(r)}.$$

From this and $R_1^{(r)}=1$, we have

$$R_m^{(r)}=(-1)^{m(m-1)/2}\prod_{j=1}^{m-1}(\lambda_{2j-1}\lambda_{2j})^j.\tag{4}$$

Noting the identity

$$\begin{aligned}&m^m(m-\nu_0)^m(m-\nu_1)^m(m-\nu_0-\nu_1)^m\prod_{j=1}^{m-1}(\lambda_{2j-1}\lambda_{2j})^j\\ =\;& 12^{3m(m-1)}(2m-\nu_0-\nu_1)^{2m}(2m-1-\nu_0-\nu_1)^m\prod_{j=1}^{m}\frac{j^j(j-\nu_0)^{j-1}(j-\nu_1)^{j-1}}{(m+j-\nu_0-\nu_1)^{m+j-2}},\end{aligned}$$

we obtain from (4) and (3) the desired formula for $D_m^{(r)}$.

2) The coefficient of x^{m-i} in $P_m^{(r)}(x)$ is

$$\begin{aligned}&(-1)^i12^{3i}\frac{m(m-1)\cdots(m-i+1)(m-\nu_0)(m-\nu_0-1)\cdots(m-\nu_0-i+1)}{(2m-\nu_0-\nu_1)(2m-\nu_0-\nu_1-1)\cdots(2m-\nu_0-\nu_1-i+1)\cdot i!}\\ =\;&(-1)^i2^{7i}3^{3i}\frac{m(m-1)\cdots(m-i+1)(3m-3\nu_0)(3m-3\nu_0-3)\cdots(3m-3\nu_0-3i+3)}{(12m-6(\nu_0+\nu_1))(12m-6(\nu_0+\nu_1)-6)\cdots(12m-6(\nu_0+\nu_1)-6i+6)\cdot i!}.\end{aligned}$$

If $3m-3\nu_0=p$ is a prime, then the numerator of the last expression is divisible by p only once and the denominator is not divisible by p. The latter is because, when p is congruent to 1 (resp. -1) modulo 6, which is equivalent to ν_0 being equal to $-1/3$ (resp. $1/3$), any factor $12m-6(\nu_0+\nu_1)-6j$ $(0\le j\le i-1)$ is congruent to -1 (resp. 1) modulo 6, and thus if

$12m - 6(\nu_0 + \nu_1) - 6j$ is divisible by p then the quotient is congruent to -1 modulo 6 and in particular is at least 5. But we always have $5p = 15m - 15\nu_0 > 12m - 6(\nu_0 + \nu_1)$, so p does not divide any $12m - 6(\nu_0 + \nu_1) - 6j$. Hence, all the coefficients of x^{m-i} $(1 \geq i \geq m)$ are divisible by p exactly once and the Eisenstein criterion ensures that the $P_m^{(r)}(x)$ is irreducible.

3) We have calculated by computer (Mathematica and Pari-GP) the types of irreducible factorization of $P_m^{(r)}(x)$ modulo various primes and found for these values of r and m the primes p_1, p_2 and p_3 such that i) $P_m^{(r)}(x) \bmod p_1$ is irreducible, ii) $P_m^{(r)}(x) \bmod p_2$ decomposes as (linear)$\times$(irreducible of degree $m-1$), and iii) $P_m^{(r)}(x) \bmod p_3$ decomposes as (irreducible quadratic)$\times$(product of irreducibles of odd degrees). By i), the Galois group is transitive and by ii) and iii) it contains a cyclic permutation of length $m-1$ and a transposition. We therefore conclude the Galois group is the symmetric group of degree m once we find these three types of primes. For instance, the lease primes (which do not divide the denominators of the coefficients) satisfying i), ii), and iii) for $P_{100}^{(0)}(x)$ are $1489, 971$, and 109 respectively.

Acknowledgment. We should like to thank Ken Ono, whose paper [3] with Karl Mahlburg gave us an impetus to write up the present paper.

References

[1] C. F. Gauss : Disquisitiones generales circa seriem infinitam $1 + \frac{\alpha\beta}{1\cdot\gamma}\, x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1\cdot2\cdot\gamma(\gamma+1)}\, xx + \frac{\alpha(\alpha+1)(\alpha+1)\beta(\beta+1)(\beta+2)}{1\cdot2\cdot3\cdot\gamma(\gamma+1)(\gamma+2)}\, x^3 +$ etc. Pars prior, (1812), Werke III.

[2] M. Kaneko and D. Zagier : Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials, AMS/IP Studies in Advanced Mathematics, vol. 7 (1998), 97–126.

[3] K. Mahlburg and K. Ono : Arithmetic of certain hypergeometric modular forms, preprint, (2003).

[4] I. Schur : Gleichungen ohne Affekt, *Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalish-Mathematische Klasse*, (1930), 443–449. Gesammelte Abhandlungen, Band III, 191–197.

[5] H. Weber : *Lehrbuch der Algebra*, Vol. 1, Chelsea, New York.

[6] D. Zagier : Modular forms whose Fourier coefficients involve zeta functions of quadratic fields, in *Modular functions of one variable VI*, Lect. Notes in Math., no. 627, Springer-Verlag, (1977) 105–169.

Graduate School of Mathematics, Kyushu University 33,
Fukuoka, 812-8581, JAPAN
mkaneko@math.kyushu-u.ac.jp

Noda 2-49-12, Kuzuha, Hirakata,
Osaka 573-1103, JAPAN