

FAMILIES OF CYCLIC POLYNOMIALS OBTAINED FROM GEOMETRIC GENERALIZATION OF GAUSSIAN PERIOD RELATIONS

KI-ICHIRO HASHIMOTO AND AKINARI HOSHI

ABSTRACT. A general method of constructing families of cyclic polynomials over \mathbb{Q} with more than one parameter will be discussed, which may be called a geometric generalization of the Gaussian period relations. Using this, we obtain explicit multi-parametric families of cyclic polynomials over \mathbb{Q} of degree $3 \leq e \leq 7$. We also give a simple family of cyclic polynomials with one parameter in each case, by specializing our parameters.

1. INTRODUCTION

Let p be a rational prime which is written in the form $p = n^4 + 5n^3 + 15n^2 + 25n + 25$ for some integer n . Using such n , Emma Lehmer [9] discovered the following “simple” family of cyclic quintic polynomials using technical transformations of Gaussian periods. She showed that certain linear transformations of Gaussian periods in the cyclotomic field $\mathbb{Q}(\zeta_p)$ are roots of the polynomial

$$f(X) = X^5 + n^2X^4 - (2n^3 + 6n^2 + 10n + 10)X^3 \\ + (n^4 + 5n^3 + 11n^2 + 15n + 5)X^2 + (n^3 + 4n^2 + 10n + 10)X + 1.$$

Note that since $f(X)$ is a monic polynomial with integral coefficients and constant term *one*, the roots of $f(X)$ are units of the splitting field which is cyclic of degree 5 over \mathbb{Q} . Schoof and Washington [14] showed that they generate the full group of units of the ring of integers of this field. Similar polynomials have been constructed for cubic, quartic and sextic cases in [9]. This method of constructing units of cyclic extensions of rationals is known as the “Lehmer project” [8]. Recently, Thaine [19, 20] made an extensive study of irreducible polynomials of Gaussian periods of arbitrary degree e and constructed new one-parameter families of cyclic polynomials explicitly for degree 7, 9 and 12. His method, which uses cyclotomic numbers, Jacobi sums, and Stickelberger’s theorem for a rational prime which is the norm of a certain number $\alpha \in \mathbb{Z}[\zeta_e]$, seems to be very interesting from the viewpoint of the Lehmer project. However, “simple” families of cyclic polynomials expected in the project are not constructed yet even in the septic case.

As another important view for the above $f(X)$, we note that if one regards n as a variable, then $f(X)$ is still a quintic cyclic polynomial over the rational function field $\mathbb{Q}(n)$. This fact is applied also to other one-parameter families of

Received by the editor November 13, 2002 and, in revised form, May 19, 2004.

2000 *Mathematics Subject Classification*. Primary 11R18, 11R27, 11T22, 12F10, 12F12.

Key words and phrases. Inverse Galois theory, generic polynomials, cyclic polynomials, Gaussian periods, Jacobi sums, cyclotomic numbers.

cyclic polynomials obtained from polynomials of Gaussian periods in [9],[19],[20]. Based on this observation, one can expect a new method of systematic construction of cyclic polynomials, which is essentially different from those described in the literature of the inverse Galois problem, such as [15], [11].

The purpose of this paper is to develop a similar but more general method of constructing cyclic polynomials over \mathbb{Q} which have more than one parameter. Our main idea, which we describe here briefly, may be called a geometric generalization of Gaussian period relations. This means that we take, among the various algebraic relations satisfied by Gaussian periods η_j , the following system of relations and regard it as the axiom for our theory:

$$\eta_m \eta_{m+i} = \sum_{j=0}^{e-1} c_{i,j} \eta_{m+j},$$

where the $c_{i,j}$ are a slight modification of the cyclotomic numbers of order e (see (2.1)). Now replace $\eta_0, \eta_1, \dots, \eta_{e-1}$ by independent variables y_0, y_1, \dots, y_{e-1} . Let R be the $e \times e$ matrix given by $R = [y_{i+j}]_{0 \leq i, j \leq e-1}$, where the subscripts are taken modulo e . Then the above relation can be rephrased to the equality

$$U = R D R^{-1},$$

where we have replaced $[c_{i,j}]_{0 \leq i, j \leq e-1}$ by the matrix $U = [u_{i,j}]_{0 \leq i, j \leq e-1}$ and D is the diagonal matrix $\text{diag}(y_0, y_1, \dots, y_{e-1})$. Let σ be the cyclic permutation of y_0, y_1, \dots, y_{e-1} . The following lemma plays a key role in this paper.

Key Lemma. *We have $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})^{(\sigma)} = \mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq e-1)$. Hence $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})/\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq e-1)$ is a cyclic extension of degree e . Moreover $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})$ is a root field of the characteristic polynomial of the matrix U .*

Therefore it is important to ask whether the fixed field $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})^{(\sigma)} = \mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq e-1)$ is again a rational function field or not, which is called Noether's problem in Galois theory. For $3 \leq e \leq 5$, we shall give an affirmative answer to Noether's problem with explicit generators of the fixed field, which is quite different from that given in [12, 13]. To construct families of simple cyclic polynomials, we introduce some more relations for y_0, y_1, \dots, y_{e-1} . In this way, for $4 \leq e \leq 7$, we shall obtain families of cyclic polynomials with $e - \lfloor \frac{e-2}{2} \rfloor$ parameters. Moreover, we shall also give some simple families of cyclic polynomials with one parameter. In particular we find the following new simple family of septic cyclic polynomials with parameter a whose constant term is a^7 :

$$\begin{aligned} X^7 &- (a^3 + a^2 + 5a + 6)X^6 + 3(3a^3 + 3a^2 + 8a + 4)X^5 \\ &+ (a^7 + a^6 + 9a^5 - 5a^4 - 15a^3 - 22a^2 - 36a - 8)X^4 \\ &- a(a^7 + 5a^6 + 12a^5 + 24a^4 - 6a^3 + 2a^2 - 20a - 16)X^3 \\ &+ a^2(2a^6 + 7a^5 + 19a^4 + 14a^3 + 2a^2 + 8a - 8)X^2 \\ &- a^4(a^4 + 4a^3 + 8a^2 + 4)X + a^7. \end{aligned}$$

This paper consists of four sections. In Section 2, we review some basic facts of Gaussian periods and cyclotomic numbers. In Section 3, we generalize polynomials of Gaussian periods geometrically. This will give a family of cyclic polynomials of

degree e with e parameters over \mathbb{Q} for small degree. In Section 4, we specialize our polynomials to obtain families of simple cyclic polynomials for $4 \leq e \leq 7$.

2. GAUSSIAN PERIODS AND CYCLOTOMIC NUMBERS

In this section, we review some basic facts of Gaussian periods, period polynomials and cyclotomic numbers which are the main ingredients of our construction of multi-parametric families of cyclic polynomials over \mathbb{Q} . Let $e \geq 2$ be a positive integer and let p be a rational prime $\equiv 1 \pmod{e}$. Write $p = ef + 1$. Let ζ_p be a p -th primitive root of 1 and g a primitive root modulo p . Gaussian periods $\eta_0, \eta_1, \dots, \eta_{e-1}$ of degree e in $\mathbb{Q}(\zeta_p)$ are defined as

$$\eta_i = \sum_{j=0}^{f-1} \zeta_p^{g^{ej+i}},$$

which are mutually conjugate over \mathbb{Q} , so that $\mathbb{Q}(\eta_i) = \mathbb{Q}(\eta_0)$ for $1 \leq i \leq e - 1$. The field $\mathbb{Q}(\eta_0)$ is the unique subfield of $\mathbb{Q}(\zeta_p)$ of degree e over \mathbb{Q} . Moreover the set $\{\eta_0, \eta_1, \dots, \eta_{e-1}\}$, which forms a normal basis of $\mathbb{Q}(\eta_0)/\mathbb{Q}$, is an integral basis of $\mathbb{Q}(\eta_0)$. The period polynomial $P_e(X) \in \mathbb{Q}[X]$ of degree e is given by $P_e(X) = \prod_{i=0}^{e-1} (X - \eta_i)$.

A classical important problem which has been studied over centuries is to determine the coefficients of $P_e(X)$ and to ask how they depend on p . Note that the coefficient of X^{e-1} of $P_e(X)$ is always 1 since $\sum_{i=0}^{e-1} \eta_i = -1$. The determination of $P_3(X)$ was established by Gauss [3] in terms of the solutions of the diophantine system $4p = L^2 + 27M^2, L \equiv 1 \pmod{3}$:

$$P_3(X) = X^3 + X^2 - \frac{p-1}{3}X - \frac{p(L+3)-1}{27}.$$

In 1935, period polynomials were again taken up by Dickson [2] with cyclotomic numbers in connection with Waring’s problem. The cyclotomic numbers (i, j) of order e are defined to be the number of pairs of integers (u_1, u_2) , for $0 \leq u_1, u_2 \leq f - 1$, satisfying $1 + g^{eu_1+i} \equiv g^{eu_2+j} \pmod{p}$. They are related to Gaussian periods in the following equalities, which are of fundamental importance in our study:

$$(2.1) \quad \eta_m \eta_{m+i} = \sum_{j=0}^{e-1} \left((i, j) - D_i f \right) \eta_{m+j}, \quad D_i = \begin{cases} \delta_{0,i} & \text{if } f \text{ is even,} \\ \delta_{\frac{e}{2},i} & \text{if } f \text{ is odd,} \end{cases}$$

where $\delta_{i,j}$ is Kronecker’s delta. It follows that the Gaussian periods are eigenvalues of the $e \times e$ matrix $[(i, j) - D_i f]_{0 \leq i, j \leq e-1}$. Hence if we have the cyclotomic numbers of order e , then we can obtain the period polynomial $P_e(X)$ as the characteristic polynomial of the matrix $[(i, j) - D_i f]_{0 \leq i, j \leq e-1}$. We also have the following properties of Gaussian periods:

$$(2.2) \quad \sum_{m=0}^{e-1} \eta_m \eta_{m+i} = pD_i - f.$$

Cyclotomic numbers are also deeply related to Jacobi sums. For these topics we refer to the book [1] and papers [7], [17], [18], [19], [20].

3. GEOMETRIC GENERALIZATION OF GAUSSIAN PERIOD RELATIONS

We shall generalize polynomials of Gaussian periods geometrically. Let $e \geq 2$ be a positive integer and let y_0, y_1, \dots, y_{e-1} be independent variables, where we are taking the subscript of y modulo e . Define the $e \times e$ matrix R by

$$R = \begin{bmatrix} y_0 & y_1 & \cdots & y_{e-1} \\ y_1 & y_2 & \cdots & y_0 \\ \vdots & \vdots & \ddots & \vdots \\ y_{e-1} & y_0 & \cdots & y_{e-2} \end{bmatrix}$$

and the diagonal matrix D by $D = \text{diag}(y_0, y_1, \dots, y_{e-1})$. Also we number the rows and columns of the matrices from 0 to $e-1$ to allow the use of residue classes modulo e . Since we regard y_i as the geometric generalization of Gaussian periods η_i , we also need a generalization of cyclotomic numbers (i, j) and a system of relations similar to (2.1) between them. Therefore we introduce an $e \times e$ matrix $U = [u_{i,j}]_{0 \leq i, j \leq e-1}$ and require that it satisfy the relation

$$(3.1) \quad RD = UR.$$

It should be noted that (3.1) is equivalent to the equalities

$$(3.2) \quad y_m y_{m+i} = \sum_{j=0}^{e-1} u_{i,j} y_{m+j}, \quad \text{for } 0 \leq m, i \leq e-1.$$

Hence the matrix $U = [u_{i,j}]$ corresponds to the matrix $[(i, j) - D_{i,j}]$ in (2.1). We shall use the following version of Kronecker's delta:

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i \equiv j \pmod{e}, \\ 0 & \text{if } i \not\equiv j \pmod{e}. \end{cases}$$

Observe that if we put $P := [\delta_{i,-j}]_{0 \leq i, j \leq e-1}$, then PR is a circulant matrix. Hence the matrix R is invertible and by (3.1) we obtain

$$(3.3) \quad U = RDR^{-1}.$$

Thus the matrix U is uniquely determined and its entries are in $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})$, the rational function field over \mathbb{Q} with e variables. Let σ be the cyclic permutation of y_0, y_1, \dots, y_{e-1} so that $\sigma(y_0) = y_1, \sigma(y_1) = y_2, \dots, \sigma(y_{e-1}) = y_0$, and let $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})^{\langle \sigma \rangle}$ be the subfield of $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})$ consisting of elements fixed under the cyclic group $\langle \sigma \rangle$ of order e . We have the following lemma which plays a key role in our study of the geometric generalization of Gaussian period relations.

Key Lemma. *We have $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})^{\langle \sigma \rangle} = \mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq e-1)$. Hence $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})/\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq e-1)$ is a cyclic extension of degree e . Moreover $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})$ is a root field of the characteristic polynomial of the matrix U .*

Proof. Apply σ to (3.2) and replace $m+1$ by m . Since the left-hand side is fixed by this, we have

$$\sum_{j=0}^{e-1} (\sigma(u_{i,j}) - u_{i,j}) y_{m+j} = 0 \quad (0 \leq m, i \leq e-1).$$

These equalities are rephrased to a single equality $(\sigma(U) - U)R = O$; hence $U = \sigma(U)$. Let $L := \mathbb{Q}(y_0, y_1, \dots, y_{e-1})$ and $M := \mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq e-1)$. Then $M \subseteq L^{(\sigma)} \subset L = L^{(\sigma)}(y_0)$ and $[L : L^{(\sigma)}] = e$. Since y_0, y_1, \dots, y_{e-1} are the eigenvalues of U whose characteristic polynomial belongs to $M[X]$, we have $[M(y_0) : M] = e$. So it suffices to show $L = M(y_0)$ to obtain $L^{(\sigma)} = M$. Put $m = 0$ in (3.2). Then we have $-u_{i,0} y_0 = \sum_{j=1}^{e-1} (u_{i,j} - \delta_{i,j} y_0) y_j$. Namely,

$$\begin{bmatrix} u_{1,1} - y_0 & u_{1,2} & \dots & u_{1,e-1} \\ u_{2,1} & u_{2,2} - y_0 & \dots & u_{2,e-1} \\ \vdots & \vdots & \ddots & \vdots \\ u_{e-1,1} & u_{e-1,2} & \dots & u_{e-1,e-1} - y_0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{e-1} \end{bmatrix} = \begin{bmatrix} -u_{1,0} y_0 \\ -u_{2,0} y_0 \\ \vdots \\ -u_{e-1,0} y_0 \end{bmatrix}.$$

Since y_0 is of degree e over M , we have $\det[u_{i,j} - \delta_{i,j} y_0]_{1 \leq i, j \leq e-1} \neq 0$, and hence $y_1, y_2, \dots, y_{e-1} \in M(y_0)$. This shows $L = M(y_0)$. \square

Remark 3.1. The last part of the above proof of the Key Lemma can be viewed as giving an expression of the action of σ on y_0, y_1, \dots, y_{e-1} explicitly as elements of the field $\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq e-1)(y_0)$.

From the Key Lemma we obtain the C_e -extension (i.e., the cyclic extension of degree e) $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})/\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq e-1)$. This leads us to the well-known Noether problem for cyclic groups which questions the rationality of the fixed field $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})^{(\sigma)}$ over \mathbb{Q} . If we have $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})^{(\sigma)} = \mathbb{Q}(\mathbf{t})$ with explicit generators $\mathbf{t} = (t_1, t_2, \dots, t_e)$, then we obtain a generating polynomial $g_e(\mathbf{t}; X)$ for the above C_e -extension. In such a case $g_e(\mathbf{t}; X)$ is a \mathbb{Q} -generic C_e -polynomial, i.e., every C_e -extension L/M with $M \supset \mathbb{Q}$ is the splitting field of a polynomial $g(\mathbf{a}; X)$ for some $\mathbf{a} \in M^n$ (cf. [6]). It is known that Noether’s problem for C_e has a positive answer for $e \leq 7$, although it has in many cases negative answers (see [16], [10], [6]).

Proposition 3.2. *The matrix $U = [u_{i,j}]$ defined by (3.1) satisfies the following properties:*

- (i) $u_{i,j} = u_{-i,j-i} \quad (0 \leq i, j \leq e-1)$,
- (ii) $\sum_{i=0}^{e-1} u_{i,j} = \begin{cases} y_0 + y_1 + \dots + y_{e-1} & \text{if } j \equiv 0 \pmod{e}, \\ 0 & \text{if } j \not\equiv 0 \pmod{e}, \end{cases}$
- (iii) $\sum_{j=0}^{e-1} u_{i,j} = \frac{1}{y_0 + \dots + y_{e-1}} \sum_{m=0}^{e-1} y_m y_{m+i}$,
- (iv) $\sum_{k=0}^{e-1} u_{i,k} u_{j-k,l-k} = \sum_{k=0}^{e-1} u_{j,k} u_{i-k,l-k} \quad (0 \leq i, j, l \leq e-1)$.

Proof. From the definition of U , we see $y_m y_i = \sum_{j=0}^{e-1} u_{i-m,j-m} y_j$. Thus we have $\sum_{j=0}^{e-1} u_{i,j} y_j = y_0 y_i = y_i y_0 = \sum_{j=0}^{e-1} u_{-i,j-i} y_j$. Assertion (i) follows from this, since y_0, y_1, \dots, y_{e-1} are linearly independent over $\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq e-1)$. Setting $R^{-1} = [s_{i,j}]_{0 \leq i, j \leq e-1}$, we have $(RR^{-1})_{i,j} = \sum_{k=0}^{e-1} y_{i+k} s_{k,j} = \delta_{i,j}$. Then by (3.3) we have

$$\sum_{i=0}^{e-1} u_{i,j} = \sum_{i=0}^{e-1} \sum_{k,h=0}^{e-1} y_{i+k} \delta_{k,h} y_k s_{h,j} = \sum_{i=0}^{e-1} \sum_{k=0}^{e-1} y_{i+k} y_k s_{k,j} = \delta_{0,j} \sum_{i=0}^{e-1} y_i.$$

Hence (ii) follows. Summing both sides of (3.2) over m , we obtain (iii). Finally we have

$$y_0 y_i y_j = \left(\sum_{k=0}^{e-1} u_{i,k} y_k \right) y_j = \sum_{l=0}^{e-1} \left(\sum_{k=0}^{e-1} u_{i,k} u_{j-k,l-k} \right) y_l.$$

Replacing i, j by each other and equating the right-hand sides, we obtain (iv). This completes the proof. \square

We shall now make the case study on the fixed field $\mathbb{Q}(y_0, y_1, \dots, y_{e-1})^{(\sigma)}$.

The cubic case. From (i) of Proposition 3.2, the matrix $U = [u_{i,j}]$ is of the form

$$U = \begin{bmatrix} A' & B' & C' \\ B & C & D \\ C & D & B \end{bmatrix}.$$

We can calculate the entries of the matrix U by (3.3). For example, we have

$$\begin{aligned} B &= (-y_0^3 y_1 + y_0^2 y_1 y_2 + y_0 y_1^2 y_2 - y_1^3 y_2 + y_0 y_1 y_2^2 - y_0 y_2^3) / \det R, \\ C &= (-y_0 y_1^3 - y_0^3 y_2 + y_0^2 y_1 y_2 + y_0 y_1^2 y_2 + y_0 y_1 y_2^2 - y_1 y_2^3) / \det R, \\ D &= (y_0^2 y_1^2 - y_0^2 y_1 y_2 - y_0 y_1^2 y_2 + y_0^2 y_2^2 - y_0 y_1 y_2^2 + y_1^2 y_2^2) / \det R, \\ \det R &= -(y_0 + y_1 + y_2)(y_0^2 - y_0 y_1 + y_1^2 - y_0 y_2 - y_1 y_2 + y_2^2). \end{aligned}$$

From (ii) and (iv) of Proposition 3.2, we obtain that

$$(3.4) \quad A' = -(B^2 + C^2 + D^2 - BC) / D, \quad B' = -(C + D), \quad C' = -(B + D).$$

This shows that the field $\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq 2) = \mathbb{Q}(B, C, D)$ is purely transcendental over \mathbb{Q} . We thus obtain a new approach to Noether’s problem for the cyclic group of order 3. Indeed we have $\mathbb{Q}(y_0, y_1, y_2)^{(\sigma)} = \mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq 2)$. By the Key Lemma and (3.4), we have a generating polynomial $g_3(B, C, D; X)$ for the cyclic cubic extension $\mathbb{Q}(y_0, y_1, y_2) / \mathbb{Q}(B, C, D)$ as the characteristic polynomial of U :

$$g_3(B, C, D; X) = X^3 - SX^2 + S(B + C + D)X + S(D^2 - BC),$$

where $S = -(B^2 + C^2 + D^2 - BC - CD - DB) / D$. The discriminant of $g_3(B, C, D; X)$ is equal to $(B - C)^2 S^2 (S - 3(B + C + D))^2$. We make the bi-rational transformation

$$\begin{cases} s = -(B^2 + C^2 + D^2 - BC - CD - DB) / D, \\ t = B - D, \\ u = C - D, \end{cases} \quad \begin{cases} B = t + (t^2 + tu + u^2) / s, \\ C = u + (t^2 + tu + u^2) / s, \\ D = (t^2 + tu + u^2) / s. \end{cases}$$

Then we have $\mathbb{Q}(y_0, y_1, y_2)^{(\sigma)} = \mathbb{Q}(s, t, u)$, where $s = y_0 + y_1 + y_2$,

$$t = \frac{y_0^2 y_1 + y_1^2 y_2 + y_2^2 y_0 - 3y_0 y_1 y_2}{y_0^2 + y_1^2 + y_2^2 - y_0 y_1 - y_1 y_2 - y_2 y_0}, \quad u = \frac{y_0 y_1^2 + y_1 y_2^2 + y_2 y_0^2 - 3y_0 y_1 y_2}{y_0^2 + y_1^2 + y_2^2 - y_0 y_1 - y_1 y_2 - y_2 y_0}.$$

We thus obtain a \mathbb{Q} -generic C_3 -polynomial over $\mathbb{Q}(s, t, u)$:

$$g_3(s, t, u; X) = X^3 - sX^2 + (s(t + u) - 3(t^2 - tu + u^2))X + t^3 - stu + u^3.$$

Moreover, by specializing the parameters s, t, u , we find simple cubic polynomials including Shanks' simplest cubic:

$$\begin{aligned} g_3(n, 0, -1; X) &= X^3 - nX^2 - (n+3)X - 1, \\ g_3(n^2, n, 1; X) &= X^3 - n^2X^2 + (n^3 - 2n^2 + 3n - 3)X + 1. \end{aligned}$$

The quartic case. From (i) of Proposition 3.2, the matrix $U = [u_{i,j}]$ has the form

$$(3.5) \quad U = \begin{bmatrix} A' & B' & C' & D' \\ B & D & E_1 & E_2 \\ C & E_3 & C & E_3 \\ D & E_1 & E_2 & B \end{bmatrix}.$$

From (ii) of Proposition 3.2, we have $B', C', D' \in \mathbb{Q}(B, C, D, E_1, E_2, E_3)$. Using this and (iv) of Proposition 3.2, one can show that

$$\begin{aligned} BE_1 + E_1^2 - DE_2 - E_2^2 - BE_3 + DE_3 + E_1E_3 - E_2E_3 &= 0, \\ CE_1 + E_1^2 + CE_2 - DE_2 - BE_3 - E_2E_3 &= 0, \\ A'E_2 + B^2 - BC + CD + DE_1 - CE_2 + BE_3 + E_2E_3 &= 0. \end{aligned}$$

From this we have $A', C, E_3 \in \mathbb{Q}(B, D, E_1, E_2)$ which gives an explicit solution of Noether's problem: $\mathbb{Q}(y_0, y_1, y_2, y_3)^{(\sigma)} = \mathbb{Q}(B, D, E_1, E_2)$. Thus we obtain a \mathbb{Q} -generic C_4 -polynomial $g_4(B, D, E_1, E_2; X)$. We use the following transformation of the variables:

$$\begin{cases} s = B + D + E_1 + E_2, \\ t = B - D + E_1 - E_2, \\ u = B - D - E_1 + E_2, \\ v = B + D - E_1 - E_2, \end{cases} \quad \begin{cases} B = (s + t + u + v)/4, \\ D = (s - t - u + v)/4, \\ E_1 = (s + t - u - v)/4, \\ E_2 = (s - t + u - v)/4. \end{cases}$$

Then we have $\mathbb{Q}(B, D, E_1, E_2) = \mathbb{Q}(s, t, u, v)$, where

$$\begin{aligned} s &= \frac{(y_0 + y_2)(y_1 + y_3)}{y_0 + y_1 + y_2 + y_3}, & u &= \frac{(y_0 - y_2)(y_1 - y_3)(y_0 - y_1 + y_2 - y_3)}{(y_0 - y_2)^2 + (y_1 - y_3)^2}, \\ t &= \frac{(y_0 - y_2)(y_1 - y_3)}{y_0 - y_1 + y_2 - y_3}, & v &= \frac{(y_0 + y_2)(y_1 - y_3)^2 + (y_0 - y_2)^2(y_1 + y_3)}{(y_0 - y_2)^2 + (y_1 - y_3)^2}. \end{aligned}$$

Hence we obtain a \mathbb{Q} -generic C_4 -polynomial with parameters s, t, u, v :

$$\begin{aligned} X^4 &+ \frac{u^2 + v^2}{s - v} X^3 - \frac{(u^2 + v^2)(4s^2t + 2s^2u + tu^2 - u^3 - 4stv - 2suv + tv^2 - uv^2)}{4u(s - v)^2} X^2 \\ &+ \frac{(u^2 + v^2)(-su^3 + 4s^2tv + tu^2v - 4stv^2 - suv^2 + tv^3)}{4u(s - v)^2} X \\ &+ \frac{u^2 + v^2}{16u(s - v)^2} \left(4s^2t^2u - 4s^2tu^2 + s^2u^3 + t^2u^3 - tu^4 - 4st^2uv + 4stu^2v \right. \\ &\quad \left. - 4s^2tv^2 + s^2uv^2 + t^2uv^2 - 2tu^2v^2 + 4stv^3 - tv^4 \right). \end{aligned}$$

Now we consider the specialization

$$s := \frac{4u^2 + u^4 - 4v^2 + 2u^2v^2 + v^4}{2v(u^2 + v^2 - 4)}, \quad t := \frac{u^2 + v^2 - 4}{2u}.$$

Then we get the following C_4 -polynomial with two parameters:

$$h_4(u, v; X) = X^4 + \frac{2v(u^2 + v^2 - 4)}{u^2 - v^2 + 4}X^3 + \frac{-2u^2 - u^4 + 2v^2 - 2u^2v^2 - v^4 + 8}{u^2 - v^2 + 4}X^2 + \frac{2v(u^2 + v^2 - 4)}{u^2 - v^2 + 4}X + 1.$$

We find simple cyclic polynomials by specializing parameters u, v as follows:

$$\begin{aligned} h_4(n, n; X) &= X^4 + n(n^2 - 2)X^3 - (n^4 - 2)X^2 + n(n^2 - 2)X + 1, \\ h_4(n, 2; X) &= X^4 + 4X^3 - (n^2 + 10)X^2 + 4X + 1, \\ h_4(n - 2, n; X) &= X^4 - n^2X^3 + (n^3 - 2n^2 + 4n - 2)X^2 - n^2X + 1. \end{aligned}$$

The quintic case. Again from (i) of Proposition 3.2, the matrix $U = [u_{i,j}]$ can be written as

$$U = \begin{bmatrix} A' & B' & C' & D' & E' \\ B & E & F_1 & G_1 & F_2 \\ C & F_3 & D & G_2 & G_3 \\ D & G_2 & G_3 & C & F_3 \\ E & F_1 & G_1 & F_2 & B \end{bmatrix}.$$

Using (ii), (iv) of Proposition 3.2, one can show that $\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq 4) = \mathbb{Q}(F_1, F_2, F_3, G_1, G_2, G_3)$ and $F_1, F_2, F_3, G_1, G_2, G_3$ satisfy the relation

$$\begin{aligned} &F_1^2F_2^2 - 2F_1F_2F_3^2 + F_3^4 + F_1F_2F_3G_1 - F_3^3G_1 - 2F_1F_2G_1^2 + F_3^2G_1^2 \\ &- F_3G_1^3 + G_1^4 - F_2^2G_2 + F_1^2F_3G_2 + F_1^2G_1G_2 + F_2F_3G_2^2 + F_2G_1G_2^2 \\ &- F_1G_2^3 - F_1^3G_3 + F_2^2F_3G_3 - F_1F_2G_2G_3 + F_2^2G_1G_3 - 2F_3^2G_2G_3 \\ &+ F_3G_1G_2G_3 - 2G_1^2G_2G_3 + F_1F_3G_3^2 + F_1G_1G_3^2 + G_2^2G_3^2 - F_2G_3^3 = 0. \end{aligned}$$

Note that this is a cubic equation for each variable. Here we make the following technical transformation:

$$t_1 := F_2 - F_1, \quad t_2 := F_3 - F_1, \quad t_3 := G_1 - F_1, \quad t_4 := G_2 - F_1, \quad t_5 := G_3 - F_1.$$

Then the above relation is transformed to one which is linear in F_1 , so that we have $F_1 \in \mathbb{Q}(t_1, t_2, t_3, t_4, t_5)$. Thus we have an explicit solution to Noether’s problem: $\mathbb{Q}(y_0, y_1, \dots, y_4)^{(\sigma)} = \mathbb{Q}(t_1, t_2, t_3, t_4, t_5)$, as well as a \mathbb{Q} -generic C_5 -polynomial $g_5(t_1, t_2, t_3, t_4, t_5; X)$.

4. SPECIALIZATION AND CONSTRUCTION OF SIMPLE CYCLIC POLYNOMIALS

To construct families of simple cyclic polynomials, we specialize the polynomials obtained in Section 3, by requiring our parameters to satisfy some further relations satisfied by Gaussian periods. Although we cannot obtain \mathbb{Q} -generic C_e -polynomials in this way, we expect the resulting polynomials to be much simpler to the extent that one can apply them to algebraic number theory. A typical example of this approach is the Lehmer project as mentioned in Section 1.

In this section, we require that the quantities y_0, y_1, \dots, y_{e-1} ($e \geq 4$) are subject to the $\lfloor \frac{e-2}{2} \rfloor$ quadratic relations

$$(*) \quad \sum_{m=0}^{e-1} y_m y_{m+1} = \sum_{m=0}^{e-1} y_m y_{m+i} \quad (2 \leq i \leq \lfloor \frac{e}{2} \rfloor).$$

Note that Gaussian periods $\{\eta_i\}$ have the same property in the case where f is even (cf. (2.1)). We shall see that if we require the condition $(*)$, then the resulting polynomial becomes closer to the polynomial of Gaussian periods. Indeed we can show that the matrix U becomes the same form as the matrix $[(i, j) - D_i f]$ in Section 2. Now we shall make the case study for each degree.

The quartic case. The quadratic relation $(*)$ we assume is

$$(4.1) \quad y_0 y_1 + y_1 y_2 + y_2 y_3 + y_3 y_0 - 2(y_0 y_2 + y_1 y_3) = 0.$$

It follows that $\mathbb{Q}(y_0, y_1, y_2, y_3) = \mathbb{Q}(y_0, y_1, y_2)$. From Section 3, we have that $\mathbb{Q}(y_0, y_1, y_2)/\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq 3)$ is a quartic cyclic extension and the action of σ is

$$\sigma(y_0) = y_1, \sigma(y_1) = y_2, \sigma(y_2) = y_3 = \frac{2y_0 y_2 - y_0 y_1 - y_1 y_2}{y_0 - 2y_1 + y_2}$$

$(\sigma(y_3) = y_0)$. We know that the matrix U is of the form as in (3.5). Moreover, using (4.1), we can show that $B - B' = C - C' = D - D'$ and $E_1 = E_2 = E_3$. Thus if we put $f := B - B'$ and $A := A' + f$, then U has the form

$$U = \begin{bmatrix} A - f & B - f & C - f & D - f \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{bmatrix}.$$

From Proposition 3.2, we can show that $A, B, C \in \mathbb{Q}(D, E, f)$, and hence we have $\mathbb{Q}(y_0, y_1, y_2)^{(\sigma)} = \mathbb{Q}(D, E, f)$. Therefore we obtain a generating polynomial $f_4(D, E, f; X)$ for the quartic cyclic extension $\mathbb{Q}(y_0, y_1, y_2)/\mathbb{Q}(D, E, f)$. If we specialize variables D, E, f as $D := (-n - 1)/n, E := -1/n, f := -4/n$, then we can find a simple family of cyclic quartic polynomials over $\mathbb{Q}(n)$

$$f_4\left(\frac{-n - 1}{n}, \frac{-1}{n}, \frac{-4}{n}; X\right) = X^4 - nX^3 - 6X^2 + nX + 1,$$

with discriminant $4(n^2 + 16)^3$ (cf. [4], [15]).

The quintic case. The assumption $(*)$ is written as

$$y_0 y_1 + y_1 y_2 + y_2 y_3 + y_3 y_4 + y_4 y_0 - (y_0 y_2 + y_1 y_3 + y_2 y_4 + y_3 y_0 + y_4 y_1) = 0,$$

so we have $\mathbb{Q}(y_0, y_1, y_2, y_3, y_4) = \mathbb{Q}(y_0, y_1, y_2, y_3)$. As in the quartic case, we put $f := B - B'$ and $A := A' + f$ and we see that the matrix U has the form

$$(4.2) \quad U = \begin{bmatrix} A - f & B - f & C - f & D - f & E - f \\ B & E & F & G & F \\ C & F & D & G & G \\ D & G & G & C & F \\ E & F & G & F & B \end{bmatrix}.$$

From Proposition 3.2, we see that $A, B, C \in \mathbb{Q}(D, E, F, G, f)$ and D, E, F, G, f satisfy a certain cubic relation. Using the transformation $s_1 := D - F, s_2 := E - F, s_3 := G - F, s_4 := f - 5F$, we obtain $\mathbb{Q}(y_0, y_1, y_2, y_3)^{(\sigma)} = \mathbb{Q}(s_1, s_2, s_3, s_4)$. Therefore we have a generating polynomial $f_5(s_1, s_2, s_3, s_4; X)$ for a quintic cyclic

extension. Here we specialize variables s_1, s_2, s_3, s_4 as $s_1 := n + 1, s_2 := n + 2, s_3 := 1, s_4 := n + 3$. Then entries of the matrix U in (4.2) are written as

$$\begin{aligned} A &= -(n^2 + n + 1)(n + 1)(n - 1)/n^2, & B &= C = F = (n + 1)/n^2, \\ D &= (n^2 + 1)(n + 1)/n^2, & E &= (n^3 + 2n^2 + n + 1)/n^2, \\ G &= (n^2 + n + 1)/n^2, & f &= (n^3 + 3n^2 + 5n + 5)/n^2. \end{aligned}$$

Hence we get a simple family of quintic cyclic polynomials over $\mathbb{Q}(n)$ as the characteristic polynomial of the matrix U :

$$\begin{aligned} &X^5 + n^2X^4 - (2n^3 + 6n^2 + 10n + 10)X^3 \\ &+ (n^4 + 5n^3 + 11n^2 + 15n + 5)X^2 + (n^3 + 4n^2 + 10n + 10)X + 1, \end{aligned}$$

with discriminant $(n^3 + 5n^2 + 10n + 7)^2(n^4 + 5n^3 + 15n^2 + 25n + 25)^4$. This is exactly Lehmer’s simplest quintic [9].

The sextic case. Assuming the two quadratic relations (*), we see that the matrix U has the form

$$U = \begin{bmatrix} A - f & B - f & C - f & D - f & E - f & F - f \\ B & F & G & H & I & G \\ C & G & E & I & J & H \\ D & H & I & D & H & I \\ E & I & J & H & C & G \\ F & G & H & I & G & B \end{bmatrix}.$$

We can show that $\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq 5) = \mathbb{Q}(D, F, G, H)$ using Proposition 3.2. Hence we can obtain a generating polynomial $f_6(D, F, G, H; X)$ for a cyclic sextic extension. Here we specialize variables D, F, G, H as $D := (-n + 1)/2n, F := (2n + 1)/2n, G := 1/2n, H := 1/2n$. Then we get the following simple family of sextic cyclic polynomials over $\mathbb{Q}(n)$:

$$X^6 + 2nX^5 + 5(n - 3)X^4 - 20X^3 - 5nX^2 - 2(n - 3)X + 1,$$

with discriminant $6^6(n^2 - 3n + 9)^5$ (cf. [4]).

The septic case. We shall give a new simple family of cyclic septic polynomials. By using (*), we can show that the matrix U has the form

$$U = \begin{bmatrix} A - f & B - f & C - f & D - f & E - f & F - f & G - f \\ B & G & H & I & J & K & H \\ C & H & F & K & L & L & I \\ D & I & K & E & J & L & J \\ E & J & L & J & D & I & K \\ F & K & L & L & I & C & H \\ G & H & I & J & K & H & B \end{bmatrix}.$$

Using Proposition 3.2, one can show that $\mathbb{Q}(u_{i,j} \mid 0 \leq i, j \leq 6) = \mathbb{Q}(v_1, v_2, v_3, v_4, v_5)$, where $v_1 := H - G, v_2 := I - G, v_3 := J - G, v_4 := K - G, v_5 := L - G$. Hence we have a generating polynomial $f_7(v_1, v_2, v_3, v_4, v_5; X)$ for our cyclic septic extension

$\mathbb{Q}(y_0, \dots, y_6)/\mathbb{Q}(v_1, \dots, v_5)$. If we specialize the parameters as $v_1 := -1, v_2 := -1, v_3 := -1, v_4 := 0, v_5 := -a - 1$, then we find a simple family of cyclic septic polynomials over $\mathbb{Q}(a)$:

$$\begin{aligned} X^7 &- (a^3 + a^2 + 5a + 6)X^6 + 3(3a^3 + 3a^2 + 8a + 4)X^5 \\ &+ (a^7 + a^6 + 9a^5 - 5a^4 - 15a^3 - 22a^2 - 36a - 8)X^4 \\ &- a(a^7 + 5a^6 + 12a^5 + 24a^4 - 6a^3 + 2a^2 - 20a - 16)X^3 \\ &+ a^2(2a^6 + 7a^5 + 19a^4 + 14a^3 + 2a^2 + 8a - 8)X^2 \\ &- a^4(a^4 + 4a^3 + 8a^2 + 4)X + a^7. \end{aligned}$$

The discriminant of this polynomial is equal to

$$\begin{aligned} &a^{22}(2a^4 - 2a^3 + 6a^2 - 3a + 4)^2(a^5 + a^4 + a^3 + 2a^2 + a + 1)^2 \\ &\times (a^6 + 2a^5 + 11a^4 + a^3 + 16a^2 + 4a + 8)^6. \end{aligned}$$

If we let a run over the units of an algebraic number field, then we obtain new units of septic cyclic extensions of this field. It would be an interesting problem to study the properties of these units.

Added remark (26 July 2004). As this paper was going to print, the authors learned of the recent paper [21] by Thaine which has closely related material. We also refer to our paper [5] which extends the idea of this paper to meta-cyclic groups.

REFERENCES

- [1] B.C. Berndt and R.J. Evans and K.S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, 1998. MR1625181 (99d:11092)
- [2] L.E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.
- [3] C.F. Gauss, *Disquisitiones Arithmeticae*, Section 358. MR0197380 (33:5545)
- [4] M.-N. Gras, *Special units in real cyclic sextic fields*, Math. Comp. **48** (1987), 179–182. MR0866107 (88m:11092)
- [5] K. Hashimoto and A. Hoshi *Geometric generalization of Gaussian period relations with application to Noether's problem for meta-cyclic groups*, to appear in Tokyo J. Math.
- [6] C. Jensen, A. Ledet and N. Yui, *Generic polynomials, constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, Cambridge, 2002. MR1969648 (2004d:12007)
- [7] S.A. Katre and A.R. Rajwade, *Complete solution of the cyclotomic problem in \mathbb{F}_q^* for any prime modulus l , $q = p^\alpha$, $p \equiv 1 \pmod{l}$* , Acta Arith. **45** (1985), 183–199. MR0808019 (87d:11095)
- [8] D.H. Lehmer and E. Lehmer, *The Lehmer project*, Math. Comp. **61** (1993), 313–317. MR1189521 (93k:11100)
- [9] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), 535–541. MR0929551 (89h:11067a)
- [10] H.W. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325. MR0347788 (50:289)
- [11] G. Malle and B.H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, Springer-Verlag, 1999. MR1711577 (2000k:12004)
- [12] K. Masuda, *On a problem of Chevalley*, Nagoya Math. J. **8** (1955), 59–63. MR0069159 (16:993c)
- [13] K. Masuda, *Application of theory of the group of classes of projective modules to existence problem of independent parameters of invariant*, J. Math. Soc. Japan **20** (1968), 223–232. MR0223345 (36:6393)
- [14] R. Schoof and L.C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), 543–556. MR0929552 (89h:11067b)

- [15] J.-P. Serre, *Topics in Galois Theory*, Research notes in mathematics (Boston, Mass.); 1 (1991). MR1162313 (94d:12006)
- [16] R.G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969), 148–158. MR0244215 (39:5532)
- [17] F. Thaine, *Properties that characterize Gaussian periods and cyclotomic numbers*, Proc. Amer. Math. Soc. **124** (1996), 35–45. MR1301532 (96d:11115)
- [18] F. Thaine, *On the coefficients of Jacobi sums in prime cyclotomic fields*, Trans. Amer. Math. Soc. **351** (1999), 4769–4790. MR1475696 (2000c:11181)
- [19] F. Thaine, *Families of irreducible polynomials of Gaussian periods and matrices of cyclotomic numbers*, Math. Comp. **69** (2000), 1653–1666. MR1653998 (2001a:11179)
- [20] F. Thaine, *Jacobi sums and new families of irreducible polynomials of Gaussian periods*, Math. Comp. **70** (2001), 1617–1640. MR1836923 (2003c:11141)
- [21] F. Thaine, *Cyclic polynomials and the multiplication matrices of their roots*, J. Pure Appl. Algebra **188** (2004), 247–286. MR2030817

DEPARTMENT OF MATHEMATICAL SCIENCES, SCHOOL OF SCIENCE AND ENGINEERING, WASEDA UNIVERSITY, 3-4-1 OHKUBO, SHINJUKU-KU, TOKYO 169-8555, JAPAN
E-mail address: khasimot@waseda.jp

DEPARTMENT OF MATHEMATICAL SCIENCES, SCHOOL OF SCIENCE AND ENGINEERING, WASEDA UNIVERSITY, 3-4-1 OHKUBO, SHINJUKU-KU, TOKYO 169-8555, JAPAN
E-mail address: hoshi@ruri.waseda.jp