PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 130, Number 8, Pages 2215–2218
S 0002-9939(02)06414-6
Article electronically published on January 17, 2002

ON SIMPLE FAMILIES OF CYCLIC POLYNOMIALS

YŪICHI RIKUNA

(Communicated by David E. Rohrlich)

ABSTRACT. We study polynomials giving cyclic extensions over rational function fields with one variable satisfying some conditions. By using them, we construct families of cyclic polynomials over some algebraic number fields. And these families give non-Kummer (or non-Artin–Schreier) cyclic extensions. In this paper, we see that our polynomials have two nice arithmetic properties. One is simplicity: our polynomials and their discriminants have more simple expressions than previous results, e.g. Dentzer (1995), Malle and Mazat (1999) and Smith (1991), etc. The other is a "systematic" property: if one of our polynomials f gives an extension L/K, then for every intermediate field M we can easily find polynomials giving M/K from f systematically.

1. INTRODUCTION

For a finite group G and a field k, a polynomial whose Galois group over k is isomorphic to G is called a (G,k)-*polynomial*. It is an important problem for inverse Galois theory to find a family of (G,k)-polynomials.

We construct a family of $(\mathbb{Z}/m\mathbb{Z}, k_m)$-polynomials with one parameter for each integer $m \geq 3$ and a suitable field k_m. If k_m includes a primitive m-th root of unity, then these polynomials give Kummer (or Artin–Schreier) cyclic extensions over k_m and we easily have a generic family of such polynomials. So it is important to make the assumption on k_m weaker. Our results give a family of non-Kummer (or non-Artin–Schreier) cyclic polynomials.

We know that $\mathrm{Aut}_{k_m} k_m(T)$, where $k_m(T)$ is the rational function field with one variable, is isomorphic to $\mathrm{PGL}_2(k_m)$, the group of the linear fractional transformations over k_m. Suppose that $\mathrm{Aut}_{k_m} k_m(T)$ has a cyclic subgroup C_m of order m; then the extension $k_m(T)/k_m(T)^{C_m}$ is cyclic of degree m, which gives a $(\mathbb{Z}/m\mathbb{Z}, k_m(T)^{C_m})$-polynomial. By using Lüroth's theorem, one can regard a generator of $k_m(T)^{C_m}$ as a variable Y over k_m. So one has a $(\mathbb{Z}/m\mathbb{Z}, k_m(Y))$-polynomial. Hilbert's irreducibility theorem assures that we get an infinite set of $(\mathbb{Z}/m\mathbb{Z}, k_m)$-polynomials by a specialization of the variable, $Y \mapsto t \in k_m$.

It is, however, difficult to execute this method to obtain a reasonable expression for the $(\mathbb{Z}/m\mathbb{Z}, k_m(Y))$-polynomial because of the hard calculation. There were only a few examples for small groups such as $\mathbb{Z}/3\mathbb{Z}$ (by Shanks [6]), $\mathbb{Z}/4\mathbb{Z}$ and

Received by the editors February 26, 2001.
2000 *Mathematics Subject Classification.* Primary 12F12; Secondary 11R20, 12E10.
Key words and phrases. Inverse Galois problem, cyclic groups, cyclic polynomials.
The author is a Research Fellow of the Japan Society for the Promotion of Science, and this study was supported by Grant-in-Aid for JSPS Fellows.

$\mathbb{Z}/6\mathbb{Z}$ (by Gras [2]), etc., until recently when Miyake [5] and Hashimoto–Miyake [3] overcame the difficulty for every cyclic group of *odd* degree:

Theorem 1.1 (Hashimoto–Miyake)**.** *Let $m \geq 3$ be an odd integer and k a field of characteristic zero. Assume that k contains $\omega = \zeta + \zeta^{-1}$, where ζ is a primitive m-th root of unity. Then $((X-\zeta)^m + (X-\zeta^{-1})^m)/2 - Y\prod_{j=0}^{m-1}(-\xi_j X + \xi_{j+1})$, where $\xi_j = (\zeta^j - \zeta^{-j})/(\zeta - \zeta^{-1})$, is a $(\mathbb{Z}/m\mathbb{Z}, k(Y))$-polynomial.*

In this paper, we expand their result for every cyclic group and find more simple expressions of $(\mathbb{Z}/m\mathbb{Z}, k_m(Y))$-polynomials.

2. Cyclic polynomials

Let $n \geq 2$ be an integer and K a field whose characteristic does not divide $2n$. We assume that K contains $\omega = \zeta + \zeta^{-1}$, where ζ is a primitive n-th (resp. $2n$-th) root of unity if n is odd (resp. even). We put

$$A := \begin{pmatrix} 1 & -1 \\ 1 & 1-\omega \end{pmatrix} \in \mathrm{GL}_2(K), \qquad \nu_j := \frac{(1-\zeta)^j - (1-\zeta^{-1})^j}{(1-\zeta) - (1-\zeta^{-1})}$$

for $j \in \mathbb{Z}$. It is clearly seen that $\nu_j \in K$. The matrix A is diagonalized as

$$A = \begin{pmatrix} \zeta^{-1} & \zeta \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1-\zeta & 0 \\ 0 & 1-\zeta^{-1} \end{pmatrix} \begin{pmatrix} \zeta^{-1} & \zeta \\ 1 & 1 \end{pmatrix}^{-1},$$

from which we easily obtain

$$A^j = \begin{pmatrix} -(2-\omega)\nu_{j-2} & -\nu_j \\ \nu_j & (2-\omega)^{-1}\nu_{j+2} \end{pmatrix}. \tag{2.1}$$

Observe that A^j is a scalar matrix if and only if $(1-\zeta)^j = (1-\zeta^{-1})^j$, or $j \equiv 0 \bmod 2n$. Hence we obtain the following:

Proposition 2.1. *The order of $A \bmod K^\times$ in $\mathrm{PGL}_2(K)$ is equal to $2n$. In other words, the projective representation $\rho_{2n} : \mathbb{Z}/2n\mathbb{Z} \to \mathrm{PGL}_2(K) : j \bmod 2n \mapsto A^j \bmod K^\times$ is faithful.*

Remark 2.2. Suppose that n is odd. The homomorphism $\varphi_n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/2n\mathbb{Z} : j \bmod n \mapsto 2j \bmod 2n$ is injective. Hence the projective representation $\rho_n = \rho_{2n} \circ \varphi_n$ is faithful. This covers the case treated by Miyake [5] and Hashimoto–Miyake [3].

Keep the above notation and put $N := 2n$. Let $K(T)$ be the rational function field over K with one variable T. The automorphism group $\mathrm{Aut}_K K(T)$ is naturally identified with $\mathrm{PGL}_2(K)$. Thus we associate $A \bmod K^\times$ with the linear fractional transformation $\tau \in \mathrm{Aut}_K K(T)$ given by

$$\tau : T \mapsto \frac{T-1}{T+1-\omega}.$$

It follows from Proposition 2.1 that $\langle\tau\rangle$ is a cyclic subgroup of $\mathrm{Aut}_K K(T)$ of order N, that is, the extension $K(T)/K(T)^{\langle\tau\rangle}$ is cyclic of degree N with the Galois group $\langle\tau\rangle$. We consider a defining polynomial of this extension. For this purpose, we choose the following:

$$u(T) := \frac{1}{N}\sum_{j=0}^{N-1} \tau^j(T) \in K(T).$$

From (2.1) we have

$$\tau^j(T) = \frac{-(2-\omega)\nu_{j-2}T - \nu_j}{\nu_j T + (2-\omega)^{-1}\nu_{j+2}}. \tag{2.2}$$

Then we define $p(T)$ and $q(T) \in K[T]$ by

$$\begin{cases} p(T) = \displaystyle\sum_{j=0}^{N-1} (-(2-\omega)\nu_{j-2}T - \nu_j) \prod_{k\neq j} (\nu_k T + (2-\omega)^{-1}\nu_{k+2}), \\ q(T) = N \displaystyle\prod_{j=0}^{N-1} (\nu_j T + (2-\omega)^{-1}\nu_{j+2}), \end{cases}$$

so that $u(T) = p(T)/q(T)$. By the definition of $u(T)$ and (2.2), $Nu(T) - N\zeta^{\pm 1}$ have the following power series expansions in $T - \zeta^{\pm 1}$:

$$Nu(T) - N\zeta^{\pm 1} = \sum_{k=0}^{\infty} \frac{(T-\zeta^{\pm 1})^{k+1}}{(\zeta^{-1}-\zeta)^k} \sum_{j=0}^{N-1} (-\zeta^{\pm 1})^j (1 - (-\zeta^{\pm 1})^j)^k.$$

Because $(-\zeta^{\pm 1})^{l+1}$ are non-trivial N-th roots of unity for every integer $0 \leq l \leq N-2$, we obtain

$$\sum_{j=0}^{N-1} (-\zeta^{\pm 1})^j (1 - (-\zeta^{\pm 1})^j)^k = \sum_{l=0}^{k} \binom{k}{l} (-1)^l \sum_{j=0}^{N-1} (-\zeta^{\pm 1})^{(l+1)j} = 0.$$

Therefore one has

$$Nu(T) - N\zeta^{\pm 1} = \sum_{k=N-1}^{\infty} \frac{(T-\zeta^{\pm 1})^{k+1}}{(\zeta^{-1}-\zeta)^k} \sum_{j=0}^{N-1} (-\zeta^{\pm 1})^j (1 - (-\zeta^{\pm 1})^j)^k,$$

which shows that $p(T) - \zeta^{\pm 1} q(T)$ is divisible by $(T - \zeta^{\pm 1})^N$; hence it is a constant multiple of $(T - \zeta^{\pm 1})^N$. Hence we obtain the following remarkably simple expressions of $p(T)$ and $q(T)$:

Proposition 2.3. *Put* $\Pi := \prod_{k=1}^{N-1} \nu_k$. *Then we have* $\Pi \neq 0$ *and*

$$\begin{cases} p(T) = \dfrac{\Pi}{\zeta^{-1}-\zeta}(\zeta^{-1}(T-\zeta)^N - \zeta(T-\zeta^{-1})^N), \\ q(T) = \dfrac{\Pi}{\zeta^{-1}-\zeta}((T-\zeta)^N - (T-\zeta^{-1})^N), \\ u(T) = \dfrac{\zeta^{-1}(T-\zeta)^N - \zeta(T-\zeta^{-1})^N}{(T-\zeta)^N - (T-\zeta^{-1})^N}. \end{cases}$$

Proposition 2.4. $K(u(T)) = K(T)^{\langle\tau\rangle}$.

Proof. Obviously we obtain $[K(T) : K(T)^{\langle\tau\rangle}] = N$ and $K(T)^{\langle\tau\rangle} \supset K(u(T))$ by the definition of $u(T)$. On the other hand, the above result shows that the degree of $p(X) - u(T)q(X) \in K(u(T))[X]$ with respect to X is N, and has a root $X = T$. So we have $[K(T) : K(u(T))] \leq N$. Hence we have $K(u(T)) = K(T)^{\langle\tau\rangle}$. This completes the proof. □

The above discussion concludes the even part of our first main result. This result extends Theorem 1.1 to general degree.

Theorem 2.5. *Let $N \geq 3$ be an integer and K a field whose characteristic does not divide N. Assume that K contains $\omega = \zeta + \zeta^{-1}$, where ζ is a primitive $N/2$-th (resp. N-th) root of unity if $N \equiv 2 \bmod 4$ (resp. $N \not\equiv 2 \bmod 4$). Define $\tau \in \mathrm{Aut}_K K(T)$ to be the following linear fractional transformation of order N:*

$$\tau(T) = \begin{cases} \dfrac{-1}{T-\omega} & \text{if } N \text{ is odd,} \\ \dfrac{T-1}{T+1-\omega} & \text{otherwise.} \end{cases}$$

Then

$$P(X) - u(T)Q(X) = \prod_{j=0}^{N-1} (X - \tau^j(T)) \in K(u(T))[X],$$

where

$$\begin{cases} P(X) := (\zeta^{-1} - \zeta)^{-1}(\zeta^{-1}(X-\zeta)^N - \zeta(X-\zeta^{-1})^N), \\ Q(X) := (\zeta^{-1} - \zeta)^{-1}((X-\zeta)^N - (X-\zeta^{-1})^N), \end{cases}$$

is an irreducible $(\mathbb{Z}/N\mathbb{Z}, K(u(T)))$-polynomial with the Galois group $\langle \tau \rangle$.

We can improve the above discussion for a divisor d of N, so we obtain defining polynomials for every intermediate field of $K(T)/K(u(T))$ systematically. By Lüroth's theorem, $K(u(T))$ is a purely transcendental extension of K of dimension one, so we regard $u(T)$ as a variable Y and hence $K(u(T)) = K(Y)$.

Corollary 2.6. *For $d \mid N$, let*

$$F^{(d)}(X) := \frac{(\zeta^{-1} - Y)(X-\zeta)^d - (\zeta - Y)(X-\zeta^{-1})^d}{\zeta^{-1} - \zeta} \in K(Y)[X]$$

and define $L^{(d)}$ to be the splitting field of $F^{(d)}(X)$ over $K(Y)$. Then $F^{(d)}(X)$ is a monic irreducible $(\mathbb{Z}/d\mathbb{Z}, K(Y))$-polynomial and $K(Y) \subset L^{(d)} \subset L^{(N)}$.

Remark 2.7. The discriminant of $F^{(d)}(X)$ with respect to X is

$$d^d (4 - \omega^2)^{(d-1)(d-2)/2} (Y^2 - \omega Y + 1)^{d-1}.$$

References

1. R. Dentzer, *Polynomials with cyclic Galois group*, Comm. Algebra, **23** (1995), no. 4, 1593–1603. MR **96a:**12006
2. M.-N. Gras, *Special units in real cyclic sextic fields*, Math. Comp., **48** (1987), no. 177, 179–182. MR **88m:**11092
3. K. Hashimoto and K. Miyake, *Inverse Galois problem for dihedral groups*, Number theory and its applications (Kyoto, 1997), 165–181, Dev. Math., 2, Kluwer Acad. Publ., Doredrecht, 1999. MR **2001a:**12010
4. G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999. MR **2000k:**12004
5. K. Miyake, *Linear Fractional Transformations and Cyclic Polynomials*, Algebraic number theory (Hapcheon/Saga, 1996). Adv. Stud. Contemp. Math. (Pusan), **1**, (1999), 137–142. MR **2000j:**11159
6. D. Shanks, *The simplest cubic fields*, Math. Comp., **28** (1974), 1137–1152. MR **50:**4537
7. G. W. Smith, *Generic cyclic polynomials of odd degree*, Comm. Algebra, **19** (1991), no. 12, 3367–3391. MR **93d:**12004

Department of Mathematical Sciences, School of Science and Engineering, Waseda University, 3–4–1 Ohkubo, Shinjuku-ku, Tokyo 169–8555, Japan

E-mail address: rikuna@gm.math.waseda.ac.jp