On generic polynomials for the modular 2-groups

By Yūichi RIKUNA

Department of Mathematical Sciences, Waseda University, 3-4-1, Ohkubo, Shinjuku-ku, Tokyo 169-8555

(Communicated by Heisuke HIRONAKA, M. J. A., March 12, 2002)

Abstract: We construct a generic polynomial for $\mathrm{Mod}_{2^{n+2}}$, the modular 2-group of order 2^{n+2}, with two parameters over the 2^n-th cyclotomic field k. Our construction is based on an explicit answer for linear Noether's problem. This polynomial, which has a remarkably simple expression, gives every $\mathrm{Mod}_{2^{n+2}}$-extension L/K with $K \supset k$, $\sharp K = \infty$ by specialization of the parameters. Moreover, we derive a new generic polynomial for the cyclic group of order 2^{n+1} from our construction.

Key words: Inverse Galois problem; Noether's problem; generic polynomials; modular 2-groups.

1. Introduction. Let n be a positive integer and k be a field whose characteristic is not two. We assume that the field k contains ζ, a primitive 2^n-th root of unity. Define α and β to be two k-automorphisms of $k(x_1, x_2)$, a rational function field over k with two variables x_1 and x_2, by the following

$$\begin{cases} \alpha(x_1) = x_2, \\ \alpha(x_2) = \zeta x_1, \end{cases} \quad \text{and} \quad \begin{cases} \beta(x_1) = x_1, \\ \beta(x_2) = -x_2. \end{cases} \tag{1}$$

Let G be a subgroup of $\mathrm{Aut}_k\, k(x_1, x_2)$ generated by α and β. This group is isomorphic to

$$\mathrm{Mod}_{2^{n+2}} := \langle a, b \mid a^{2^{n+1}} = b^2 = 1, ab = ba^{1+2^n} \rangle, \tag{2}$$

the modular 2-group of order 2^{n+2}.

In this paper, we construct a polynomial $F_n(t_1, t_2; X) \in k(t_1, t_2)[X]$ where t_1, t_2 are independent parameters, which has the following properties:

1. $F_n(t_1, t_2; X)$ is monic and has the Galois group $\mathrm{Mod}_{2^{n+2}}$ over $k(t_1, t_2)$,
2. for every $\mathrm{Mod}_{2^{n+2}}$-extension L/K with $K \supset k$ and $\sharp K = \infty$, there exist $a_1, a_2 \in K$ such that L is the splitting field of $F_n(a_1, a_2; X) \in K[X]$ over K.

The polynomial satisfying these properties is called k-*generic* for $\mathrm{Mod}_{2^{n+2}}$. It is an important problem for inverse Galois theory to construct explicit expressions for generic polynomials.

2. Generic $\mathbf{Mod_{2^{n+2}}}$-polynomial. We first consider the G-extension $k(x_1, x_2)/k(x_1, x_2)^G$ and find a generating set of $k(x_1, x_2)^G$ over k. Define S to be the scalar subgroup of the G-action on $k(x_1, x_2)$, i.e.,

$$S := \left\{ \tau \in G \;\middle|\; \tau\left(\frac{x_1}{x_2}\right) = \frac{x_1}{x_2} \right\} \lhd G. \tag{3}$$

Lemma 1. *We have $S = \langle \alpha^2 \rangle$ and $\sharp S = 2^n$.*

Proof. From $G = \{\alpha^{2j}, \alpha^{2j+1}, \alpha^{2j}\beta, \alpha^{2j+1}\beta \mid 0 \le j \le 2^n - 1\}$, the assertion is checked immediately. □

The quotient group G/S is isomorphic to $V_4 := (\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$, hence $k(x_1/x_2)/k(x_1/x_2)^G$ is a V_4-extension. By Lüroth's theorem, $k(x_1/x_2)^G$ is purely transcendental over k.

Proposition 2. *The invariant field $k(x_1/x_2)^G$ is generated over k by*

$$\eta := \frac{\zeta x_1^4 + \zeta^{-1} x_2^4}{(x_1 x_2)^2}. \tag{4}$$

Proof. Obviously we have $\eta \in k(x_1/x_2)^G$ and $[k(x_1/x_2) : k(\eta)] \ge \sharp V_4 = 4$. On the other hand, x_1/x_2 is a root of a biquadratic equation $X^4 - \zeta^{-1}\eta X^2 + \zeta^{-2} = 0$. Hence we obtain $[k(x_1/x_2) : k(\eta)] \le 4$. It follows that $k(x_1/x_2)^G = k(\eta)$. □

From [3, §1.1], every homogeneous rational function*) in $k(x_1, x_2)^G$ of degree $\sharp S = 2^n$ generates the invariant field $k(x_1, x_2)^G$ over $k(x_1/x_2)^G = k(\eta)$. Here, we choose as such function

$$\theta := \frac{(x_1 x_2)^{2^n}}{x_1^{2^n} + x_2^{2^n}} \tag{5}$$

2000 Mathematics Subject Classification. Primary 12F12; Secondary 13A50.

*) We call an element $f \in k(x_1, x_2)$ homogeneous of degree d if it can be written as $f = g/h$ with $g, h \in k[x_1, x_2]$ homogeneous and $\deg g - \deg h = d$.

so that $k(x_1, x_2)^G = k(\eta, \theta)$.

Since G is irreducible over k by regarding the inclusion $G \hookrightarrow \mathrm{Aut}_k\, k(x_1, x_2)$ as a linear representation, we obtain $k(x_1, x_2) = k(x_1, x_2)^G(R) = k(x_1, x_2)^G(x_1)$, where

$$(6)\quad R := \mathrm{Orb}_G(x_1) = \{\zeta^j x_1, \zeta^j x_2 \mid 0 \le j \le 2^n - 1\}.$$

Hence the minimal polynomial of x_1 over $k(x_1, x_2)^G$ is $\varphi(X) := \prod_{x \in R}(X - x)$ (cf. [6, Chap. 3]), and we have

$$(7)\quad \varphi(X) = X^{2^{n+1}} - (x_1^{2^n} + x_2^{2^n})X^{2^n} + (x_1 x_2)^{2^n}.$$

We next give the expression of $\varphi(X)$ as a polynomial over $k(\eta, \theta)$.

Lemma 3. *Define a sequance $\{E_j\}_{j=1}^{\infty}$ by $E_1 := \eta$ and $E_{j+1} := E_j^2 - 2$. Then we have*

$$(8)\qquad E_j = \frac{\zeta^{2^{j-1}} x_1^{2^{j+1}} + \zeta^{-2^{j-1}} x_2^{2^{j+1}}}{(x_1 x_2)^{2^j}}.$$

Proof. This follows by mathematical induction. □

Proposition 4. *The coefficients of $\varphi(X)$ have the following expressions*:

$$(9)\qquad x_1^{2^n} + x_2^{2^n} = (2 - E_n)\theta,$$

$$(10)\qquad (x_1 x_2)^{2^n} = (2 - E_n)\theta^2.$$

Proof. From $\zeta^{2^{n-1}} = -1$, we have

$$(11)\qquad E_n = -\frac{x_1^{2^{n+1}} + x_2^{2^{n+1}}}{(x_1 x_2)^{2^n}}.$$

Hence we obtain

$$(12)\qquad 2 - E_n = \frac{(x_1^{2^n} + x_2^{2^n})^2}{(x_1 x_2)^{2^n}}.$$

One can derive (9) and (10) from this. □

From Lemma 3, we obtain

$$(13)\quad E_n = (\cdots((\eta\underbrace{{}^2 - 2)^2 - 2)^2 \cdots - 2)^2 - 2}_{\text{square arises } n-1 \text{ times}}.$$

Hence we have

$$(14)\qquad E_n = \Phi^+_{2^{n+1}}(\eta),$$

where $\Phi^+_{2^{n+1}}(X)$ is the minimal polynomial of $2\cos(2\pi/2^{n+1})$ over $\mathbf{Q}$.

By regarding η and θ as new variables t_1 and t_2 in $\varphi(X)$, we see that

$$(15)\quad F(t_1, t_2; X) := X^{2^{n+1}} + (\Phi^+_{2^{n+1}}(t_1) - 2)t_2 X^{2^n} - (\Phi^+_{2^{n+1}}(t_1) - 2)t_2^2$$

gives a $\mathrm{Mod}_{2^{n+2}}$-extension over $k(t_1, t_2)$.

Remark. For any integer $m \ge 1$, we know the following identity in $\mathbf{Z}[X, Y]$:

$$(16)\qquad X^m + Y^m = \sum_{j=0}^{[m/2]} B(m, j)(-XY)^j (X + Y)^{m-2j},$$

where $B(m, j) := \binom{m-j-1}{j-1} + \binom{m-j}{j}$ and $[\cdot]$ is the Gauß symbol. By using this, we have an explicit expression of $\Phi^+_{2^{n+1}}(t_1)$ for $n \ge 2$;

$$(17)\quad \Phi^+_{2^{n+1}}(t_1) = \sum_{j=0}^{2^{n-2}} (-1)^j B(2^{n-1}, j) t_1^{2^{n-1}-2j}.$$

By the following theorem, this polynomial is generic over k:

Theorem (Kemper and Mattig cf. [4, Theorem 7])**.** *Let $\mathsf{k}(x_1, \ldots, x_m)$ be a rational function field over an arbitrary field k and G be a finite linear subgroup of $\mathrm{Aut}_{\mathsf{k}}\, \mathsf{k}(x_1, \ldots, x_m)$. And let $\mathsf{M} \subset \mathsf{k}(x_1, \ldots, x_m)$ be a finite G-stable subset with $\mathsf{k}(x_1, \ldots, x_m) = \mathsf{k}(x_1, \ldots, x_m)^{\mathsf{G}}(\mathsf{M})$. Suppose that the invariant field $\mathsf{k}(x_1, \ldots, x_m)^{\mathsf{G}}$ is purely transcendental over k and isomorphic to $\mathsf{k}(t_1, \ldots, t_m)$. By regarding $\prod_{y \in \mathsf{M}}(X - y) \in \mathsf{k}(x_1, \ldots, x_m)^{\mathsf{G}}[X]$ as a polynomial over $\mathsf{k}(t_1, \ldots, t_m)$, this polynomial is k-generic for G.*

We thus have the following

Theorem 5. *The polynomial $F(t_1, t_2; X)$ is k-generic for $\mathrm{Mod}_{2^{n+2}}$.*

Remark. For an even integer N, we define "modular type" finite group Mod_{4N} of order $4N$ by

$$\mathrm{Mod}_{4N} := \langle a, b \mid a^{2N} = b^2 = 1, ab = ba^{1+N} \rangle,$$

if $N = 2^n(2m - 1)$ $(m \ge 1)$. This generalizes the definition of $\mathrm{Mod}_{2^{n+2}}$, and we have

$$\mathrm{Mod}_{4N} \cong \mathrm{Mod}_{2^{n+2}} \oplus \mathbf{Z}/(2m - 1)\mathbf{Z}.$$

In addition to the assumption for k, suppose that the characteristic of k is prime to $2m - 1$ and that k contains $\mu + \mu^{-1}$, where μ is a primitive $(2m - 1)$-th root of unity. Then there exists a k-generic polynomial for $\mathbf{Z}/(2m - 1)\mathbf{Z}$ with one parameter asising from a linear Noether extension (cf. [1, 5]). Hence we can construct a k-generic polynomial for Mod_{4N} with three parameters.

3. Generic cyclic polynomial. Let $C_{2^{n+1}}$ be the cyclic group of order 2^{n+1}. A $\mathbf{Q}(\cos(2\pi/2^{n+1}))$-generic $C_{2^{n+1}}$-polynomial is given explicitly by [2, Theorem 1]. This result corresponds to a "degree-two descended" Kummer theory whose base field is descended to the maximal real subfield of the cyclotomic field. In the previous section, we have constructed a $\mathbf{Q}(\exp(2\pi\sqrt{-1}/2^n))$-generic $\mathrm{Mod}_{2^{n+2}}$-polynomial. Since $\mathrm{Mod}_{2^{n+2}}$ has a cyclic subgroup of order 2^{n+1}, we can construct a $\mathbf{Q}(\exp(2\pi\sqrt{-1}/2^n))$-generic $C_{2^{n+1}}$-polynomial. This gives a new "degree-two descended" Kummer theory.

Theorem 6. *The polynomial* $F(\zeta t_1^2 - 2, t_2; X)$ *is* k*-generic for* $C_{2^{n+1}}$.

Proof. A subgroup $H := \langle \alpha \rangle$ of G is cyclic of order 2^{n+1}. From Lemma 1, there exists $\lambda \in k(x_1/x_2)^H$ such that $k(x_1, x_2)^H = k(\lambda, \theta)$ and we can choose

$$\lambda := \frac{x_1^2 + \zeta^{-1} x_2^2}{x_1 x_2}. \tag{18}$$

Then we have

$$\eta = \zeta \lambda^2 - 2. \tag{19}$$

This completes the proof. □

Acknowledgements. 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.

References

[1] Hashimoto, K., and Mikake, K.: Inverse Galois problem for dihedral groups. Number Theory and Its Applications (Kyoto, 1997). Dev. Math. vol. 2, Kluwer, Dordrecht, pp. 165–181 (1999).

[2] Hashimoto, K., and Rikuna, Y.: On generic families of cyclic polynomials with even degree. Manuscripta Math. (To appear).

[3] Kemper, G.: A constructive approach to Noether's problem. Manuscripta Math., **90**, 343–363 (1996).

[4] Kemper, G., and Mattig, E.: Generic polynomials with few parameters. J. Symbolic Computation, **30**, 843–857 (2000).

[5] Rikuna, Y.: On simple families of cyclic polynomials. Proc. Amer. Math. Soc. (To appear).

[6] Smith, L.: Polynomial Invariants of Finite Groups. Res. Notes Math. vol. 6, A. K. Peters, Wellesley, MA (1995).