Generic polynomials over $\boldsymbol{Q}$ with two parameters for the transitive groups of degree five

By Ki-ichiro HASHIMOTO*) and Hiroshi TSUNOGAI**)

(Communicated by Heisuke HIRONAKA, M. J. A., Nov. 12, 2003)

Abstract: In this article, we construct generic polynomials over $\boldsymbol{Q}$ with two parameters for all transitive subgroups of the symmetric group of degree 5 by considering the action on the moduli space of the projective line with ordered five marked points. Although polynomials having such properties are already known, our device is unifying through all the cases, and in some cases we obtain polynomials with much simpler coefficients.

Key words: Constructive Galois theory; generic polynomials.

1. Introduction. All the transivite subgroups of the symmetric group $\mathfrak{S}_5$ of degree 5 are the cyclic group C_5 of order 5, the dihedral group D_5 of order 10, the Frobenius group $F_{20} = F_{5,4}$ of order 20, the alternating group $\mathfrak{A}_5$ of order 60, and $\mathfrak{S}_5$ itself. In this article, we give generic polynomials for all of these subgroups over $\boldsymbol{Q}$ with two parameters by considering the action on the moduli space of the projective line with ordered five marked points.

While polynomials having such properties are already known [1–3, 5, 6], the main features of this article are that our device is unifying through all the cases, and that our polynomials have much simpler coefficients for the cases of C_5 and $\mathfrak{A}_5$. We remark that, for any group G listed above, it is known that the essential dimension of G over $\boldsymbol{Q}$ is two, which is the minimum number of parameters for generic polynomial ([2, 5]).

2. The action of $\mathfrak{S}_5$ on $\mathcal{M}_{0,5}$. Let $\mathcal{M}_{0,5}$ be the moduli space of projective lines with ordered five marked points:

$$\begin{aligned}\mathcal{M}_{0,5} &= \left((\mathbf{P}^1)^5 \smallsetminus (\text{weak diagonal})\right)/\mathrm{PGL}(2)\\ &= \{(x_1,\dots,x_5) | x_i \in \mathbf{P}^1, x_i \neq x_j (i \neq j)\}/\mathrm{PGL}(2),\end{aligned}$$

where $\mathrm{PGL}(2) = \mathrm{Aut}(\mathbf{P}^1)$ acts diagonally. We denote the class of $(x_1,\dots,x_5)$ by $[x_1,\dots,x_5]$. The function field

$$K := \boldsymbol{Q}(\mathcal{M}_{0,5}) = \boldsymbol{Q}(x_1,\dots,x_5)^{\mathrm{PGL}(2)}$$

is purely transcendental over $\boldsymbol{Q}$ of degree two and generated by the cross-ratios

$$\frac{x_i - x_k}{x_i - x_l} \Big/ \frac{x_j - x_k}{x_j - x_l}\,.$$

The symmetric group $\mathfrak{S}_5$ of degree 5 acts on $\mathcal{M}_{0,5}$ by permutation of components:

$$\sigma \cdot [x_1,\dots,x_5] := [x_{\sigma^{-1}(1)},\dots,x_{\sigma^{-1}(5)}]$$

($\sigma \in \mathfrak{S}_5$), and also on the function field K by $\sigma \cdot \varphi := \varphi \circ \sigma^{-1}$ ($\sigma \in \mathfrak{S}_5$, $\varphi \in K$). This action is faithful and can be described concretely. A point $P = [x_1,\dots,x_5] \in \mathcal{M}_{0,5}$ can be normalized to the form $[0, xy, x, 1, \infty]$ by a unique element of PGL(2), where

$$(1)\qquad \begin{cases} x = \dfrac{x_3 - x_1}{x_3 - x_5} \Big/ \dfrac{x_4 - x_1}{x_4 - x_5}\,, \\[2ex] y = \dfrac{x_2 - x_1}{x_2 - x_5} \Big/ \dfrac{x_3 - x_1}{x_3 - x_5} \end{cases}$$

can be regarded as local coordinate functions on $\mathcal{M}_{0,5}$. By the use of x, y, we identify $\mathcal{M}_{0,5}$ with $\left(\mathbf{P}^1 \smallsetminus \{0,1,\infty\}\right)^2 \smallsetminus \{xy = 1\}$. Then we have $K = \boldsymbol{Q}(\mathcal{M}_{0,5}) = \boldsymbol{Q}(x,y)$. The action of $\mathfrak{S}_5$ on $\boldsymbol{Q}(x,y)$ is described as follows: For example, consider the action of the element $\alpha = (1\ 2\ 3\ 4\ 5)$. Put $P = [x_1,\dots,x_5] = [0, xy, x, 1, \infty]$. Then $\alpha^{-1}(P) = [x_2, x_3, x_4, x_5, x_1] = [xy, x, 1, \infty, 0] = [0, 1-y, 1-xy, 1, \infty]$, where the renormalization is given by $\xi \mapsto (\xi - xy)/\xi$. Thus we obtain

$$(2)\qquad \alpha : \begin{cases} x \longmapsto 1 - xy \\[1ex] y \longmapsto \dfrac{1-y}{1-xy}. \end{cases}$$

2000 Mathematics Subject Classification. Primary 12F12; Secondary 13A50, 20B25.

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

**) Department of Mathematics, Sophia University, 7-1, Kioi-cho, Chiyoda-ku, Tokyo 102-8554.

In the following sections, for each subgroup G listed above, we give a polynomial $f^G(X) \in K^G[X]$ whose splitting field coincides with K. Our main task to obtain a generic polynomial over $\boldsymbol{Q}$ from $f^G[X]$ is to show that K^G is rational over $\boldsymbol{Q}$ of transcendental degree two. (We carried out this calculation with Maple with `grobner` package).

3. Dihedral group $\boldsymbol{D_5}$ of order 10. Let D_5 be the subgroup of $\mathfrak{S}_5$ generated by $\alpha = (1\ 2\ 3\ 4\ 5)$ and $\beta = (1\ 3)(4\ 5)$. Then D_5 is a dihedral group of degree 5, and is the stabilizer of a necklace permutation ("juzu-junretsu" in Japanese) $(1, 2, 3, 4, 5)$. The action of α on $K = \boldsymbol{Q}(x, y)$ is described in (2). That of β on K is given by

$$\beta : \begin{cases} x \longmapsto x \\ y \longmapsto \dfrac{1-y}{1-xy}. \end{cases}$$

Let $S = \mathrm{Orb}_{D_5}(x)$ be the D_5-orbit of x:

$$S = \left\{ x, 1-xy, y, \frac{1-y}{1-xy}, \frac{1-x}{1-xy} \right\},$$

and put $f(X) := \prod_{u \in S}(X - u) =: X^5 + c_4X^4 + c_3X^3 + c_2X^2 + c_1X + c_0 \in K^{D_5}[X]$. Since the stabilizer of S in $\mathrm{Aut}(K/\boldsymbol{Q})$ is D_5, K^{D_5} coincides with $K(c_0, \ldots, c_4)$ and $f(X)$ is a D_5-polynomial over K^{D_5}.

Theorem 1. (1) *The fixed field* $K^{D_5} = K(c_0, \ldots, c_4)$ *of* D_5 *is rational* (*i.e. purely transcendental over* $\boldsymbol{Q}$ *with degree* 2). *Indeed we have* $K^{D_5} = \boldsymbol{Q}(a, b)$ *where*

$$c_0 = a, \quad c_1 = b, \quad c_2 = a^2 - a - 1 - 2b, \quad c_3 = b - a - 3, \quad c_4 = a - 3.$$

(2) (*reconstruction of Brumer* [1], *Hashimoto* [4]) *The polynomial*

$$\begin{aligned} &f^{D_5}(a, b; X) \\ &\quad := X^5 + (-3 + a)X^4 + (3 + b - a)X^3 \\ &\qquad + (-1 - a - 2b + a^2)X^2 + bX + a \end{aligned}$$

is a generic polynomial for D_5 *over* $\boldsymbol{Q}$.

Proof. (1) Write $c_0, \ldots, c_4$ in terms of x, y. Then the equations among c_i's can be verified by straight forward calculation with computer. To find the equations, one can do with Gröbner basis algorithm. We may find them by hand if we use a remarkable relation $u + \alpha(u)\alpha^{-1}(u) = 1$ for any $u \in S$.

(2) Let $L \supset K \supset \boldsymbol{Q}$ be any field extention with $\mathrm{Gal}(L/K) \simeq D_5$. By the normal basis theorem, L is isomorphic to $K[D_5]$ as $K[D_5]$-modules. Hence there exists a sub-$K[D_5]$-module $W = \bigoplus_{i=1}^5 Kx_i$ of L isomorphic to the permutation representation, i.e. $\sigma(x_i) = x_{\sigma(i)}$. Let x, y be as in (1) and define a, b as above. When $x \neq y$, D_5 acts on the roots of $f^{D_5}(a, b; X) \in K[X]$ and L is the splitting field of $f^{D_5}(a, b; X)$ over K. (When $x = y (= (-1 \pm \sqrt{5})/2)$, we need a suitable change to W, but we omit the detail here.) $\square$

4. Cyclic group $\boldsymbol{C_5}$ of order 5. Consider the cyclic subgroup $C_5 = \langle \alpha = (1\ 2\ 3\ 4\ 5) \rangle$ of D_5. We show the rationality of the fixed field K^{C_5}, which is a quadratic extension of $K^{D_5} = \boldsymbol{Q}(a, b)$ (a, b are as in Theorem 1).

Let $c = \prod_{i \in \boldsymbol{Z}/5\boldsymbol{Z}}(\alpha^i(x) - \alpha^{i+1}(x)) = \prod_{u \in S}(u - \alpha(u))$. Then, we have $\alpha(c) = c, \beta(c) = -c$, from which follows $K^{C_5} = K^{D_5}(c) = \boldsymbol{Q}(a, b, c)$ and $c^2 \in K^{D_5}$. Writing c^2, a, b in terms of x, y, we have the following relation among them:

$$\begin{aligned} (3) \quad &H(a, b, c) \\ &\quad := c^2 + 4b^3 + (-a^2 + 30a - 1)b^2 \\ &\qquad + (-24a^3 + 34a^2 + 14a)b \\ &\qquad + (4a^5 - 4a^4 - 40a^3 + 91a^2 - 4a) = 0. \end{aligned}$$

Remark. The equation (3) defines an elliptic surface with a base curve $\mathbf{P}_a^1$ with singularity. By the theory of elliptic surfaces, we know that (3) is rational over $\overline{\boldsymbol{Q}}$. The crucial point of our argument is to show that it is rational over $\boldsymbol{Q}$.

The defining ideal I of the singular locus of $H(a, b, c) = 0$ is

$$\left(H, \frac{\partial H}{\partial a}, \frac{\partial H}{\partial b}, \frac{\partial H}{\partial c} \right) = (a^2 - 11a - 1, b - 3a - 1, c).$$

One can desingularize $H(a, b, c) = 0$ by blowing up along I successively. Then after blowing up four times, we obtain a smooth model birational to $\mathbf{P}^2$ over $\boldsymbol{Q}$.

Theorem 2. *The* C_5*-fixed field* $K^{C_5} = \boldsymbol{Q}(a, b, c)$ *is rational over* $\boldsymbol{Q}$. *Indeed we have* $K^{C_5} = \boldsymbol{Q}(A, B)$, *where*

$$(4) \qquad \begin{cases} A = -\dfrac{2a^3 - 2a^2 + 13a - 7ab + b}{8a^2 - 33a - ab - 7b + 2} \\ B = -\dfrac{c}{8a^2 - 33a - ab - 7b + 2}. \end{cases}$$

Indeed we have $a = a_{\mathrm{num}}/Q$, $b = b_{\mathrm{num}}/Q^2$, $c = c_{\mathrm{num}}/Q^3$, *where*

$$\begin{cases} a_{\mathrm{num}} := -A^3 - A^2 - 7B^2A + B^2 \\ b_{\mathrm{num}} := 2A^5 - 2A^4 - 8B^2A^4 + 36A^3B^2 - 145B^4A^2 \\ \qquad + 3A^2 - 22B^2A^2 + 4B^2A + 120B^4A \\ \qquad - 2A - 13B^2 - 180B^4 - 625B^6 \\ c_{\mathrm{num}} := -2BP^2 \\ \quad P := A^4 - 2A^3 + 25B^2A^2 - A^2 + 2A + 1 \\ \qquad + 25B^2 + 125B^4, \\ \quad Q := -A + 1 + B^2A + 7B^2. \end{cases}$$

Corollary 3. *The polynomial* $f_1^{C_5}(A,B;X) := f^{D_5}(a,b;X)$ *is a generic polynomial for* C_5 *over* $\boldsymbol{Q}$. *The polynomials*

$$\begin{aligned} &f_2^{C_5}(A,B;X) \\ &\quad = X^5 - \frac{(2-2A+A^2+15B^2)P}{Q^2}X^3 \\ &\qquad + \frac{2BP^2}{Q^3}X^2 + \frac{(1-A)P^2}{Q^3}X - \frac{2BP^2}{Q^3}, \\ &f_3^{C_5}(A,B;X) \\ &\quad = X^5 - \frac{P(A^2+1+10B^2)}{Q^2}X^3 \\ &\qquad + \frac{(A^2+3B^2+3B^2A^2+25B^4)P^2}{Q^4}X \\ &\qquad + \frac{2(A^3+A^2+7B^2A-B^2)BP^2}{Q^4}, \end{aligned}$$

are also generic polynomials for C_5 *over* $\boldsymbol{Q}$.

Proof. The transformation of variables are obtained in the process of desingularization. To show the genericity, let $L \supset K \supset \boldsymbol{Q}$ be any field extention with $\mathrm{Gal}(L/K) \simeq C_5$. By the normal basis theorem, L is isomorphic to $K[C_5]$ as $K[C_5]$-modules. Take $x_i \in L$ such that $L = \bigoplus_{i=1}^5 Kx_i$ with $\sigma(x_i) = x_{\sigma(i)}$, and put x, y as in (1) and define a, b, c as above (If $x = y$, make a similar modification to the case of D_5). Since $\mathrm{Gal}(L/K) \simeq C_5$, c must belong to K. Define $A, B \in K$ by (4). Then the splitting field of $f_1^{C_5}(A,B;X) \in K[X]$ over K coincides with L.

Put $x' := x - \alpha(x)$ and denote its C_5-orbit by $S' = \mathrm{Orb}_{C_5}(x')$. Then the coefficients of $f(X) := \prod_{u \in S'}(X-u)$ is contained in K^{C_5}, and the splitting field of $f(X)$ over K^{C_5} is K. By expressing the coefficients in terms of A, B, we obtain $f_2^{C_5}(A,B;X)$. If we do the same work with $x'' := x - \alpha^2(x)$ instead of x', we obtain $f_3^{C_5}(A,B;X)$. $\square$

5. Frobenius group $F_{5,4}$ of order 20. Let $\alpha = (1\ 2\ 3\ 4\ 5)$ and $\gamma = (1\ 5\ 3\ 4)$. They generate a Frobenius group $F_{5,4} = \langle \alpha, \gamma \rangle$ of order 20. The action of γ on K is given by

$$\gamma : \begin{cases} x \longmapsto \dfrac{x}{x-1} \\ y \longmapsto \dfrac{x-1}{x(1-y)}. \end{cases}$$

The stabilizer of x in $F_{5,4}$ is $\langle \gamma^2 \rangle$. Then $u_0 := x + \gamma(x) = x^2/(x-1)$ is γ-invariant and its $F_{5,4}$-orbit $S' := \mathrm{Orb}_{F_{5,4}}(u_0)$ is

$$\begin{aligned} &\mathrm{Orb}_{\langle\alpha\rangle}(u_0) \\ &\quad = \left\{ \frac{x^2}{x-1}, -\frac{(1-xy)^2}{xy}, \frac{y^2}{y-1}, \right. \\ &\qquad \left. -\frac{(1-y)^2}{y(1-x)(1-xy)}, -\frac{(1-x)^2}{x(1-y)(1-xy)} \right\}. \end{aligned}$$

We obtain a generic polynomial for $F_{5,4}$ over $\boldsymbol{Q}$ by taking the monic polynomial whose roots are S'. The following polynomial of Lecacheux is obtained after a variable change $X \mapsto 1/X$.

Theorem 4 (Lecacheux [6])**.** *The polynomial*

$$\begin{aligned} &f^{F_{5,4}}(s,t;X) \\ &\quad = X^5 + \left(t^2d - 2s - \frac{17}{4}\right)X^4 \\ &\qquad + \left(3td + d + \frac{13s}{2} + 1\right)X^3 \\ &\qquad - \left(td + \frac{11s}{2} - 8\right)X^2 + (s-6)X + 1 \end{aligned}$$

where $d = s^2 + 4$, *is a generic polynomial for* $F_{5,4}$ *over* $\boldsymbol{Q}$.

6. The alternative group $\mathfrak{A}_5$ of order 60. Let $\alpha = (1\ 2\ 3\ 4\ 5)$ and $\omega = (1\ 5\ 4)$. They generate the alternative group $\mathfrak{A}_5 = \langle \alpha, \omega \rangle$ of order 60. The action of ω on K is given by

$$\omega : \begin{cases} x \longmapsto \dfrac{1}{1-x} \\ y \longmapsto \dfrac{1-x}{1-xy}. \end{cases} \tag{5}$$

The stabilizer of x in $\mathfrak{A}_5$ is $\langle (1\ 3)(4\ 5), (1\ 4)(3\ 5) \rangle \simeq V_4$ (Klein's four group). Then the stabilizer of $v_0 := x + \omega(x) + \omega^2(x) = (1 - 3x + x^3)/x(x-1)$ in $\mathfrak{A}_5$ is of order 12, and the $\mathfrak{A}_5$-orbit $S'' := \mathrm{Orb}_{\mathfrak{A}_5}(v_0)$ of v_0 coincides with

$$\mathrm{Orb}_{\langle\alpha\rangle}(v_0) = \left\{ \frac{1-3x+x^3}{x(x-1)}, \frac{1-3x^2y^2+x^3y^3}{xy(1-xy)}, \frac{1-3y+y^3}{y(y-1)}, \frac{1-3xy-3y^2+6xy^2+y^3-3x^2y^3+x^3y^3}{y(1-x)(1-y)(1-xy)}, \frac{1-3xy-3x^2+6x^2y+x^3-3x^3y^2+x^3y^3}{x(1-x)(1-y)(1-xy)} \right\}.$$

Taking the monic polynomial whose roots are S'', we obtain the following polynomial.

Theorem 5. (1) *The fixed field* $K^{\mathfrak{A}_5}$ *of* $\mathfrak{A}_5$ *is rational. Indeed we have* $K^{\mathfrak{A}_5} = \boldsymbol{Q}(u,v)$ *where*

$$\begin{cases} u = (a^2-10a+1-b)/a \\ v = ((2a^5+18a^4-140a^3+13a^2-2a) \\ \qquad -(4a^3+20a^2+6a)b-a^2b^2)/a^3. \end{cases}$$

(2) *The polynomial*

$$f^{\mathfrak{A}_5}(u,v;X) = X^5+uX^4+(-6u-10)X^3+vX^2 + (-u^2+12u+25-3v)X+(u^3+24u^2+27u-24+9v)$$

is a generic polynomial for $\mathfrak{A}_5$ *over* $\boldsymbol{Q}$*, whose discriminant is the square of*

$$(24000-109600u-54720u^2+91032u^3 + 68280u^4+13624u^5+840u^6+16u^7) + (-28400+36240u+44284u^2+9240u^3+332u^4)v + (6480+1386u-90u^2-4u^3)v^2-27v^3.$$

Remark. It would be worth remarking that the discriminant is a square of an irreducible polynomial. In the case that the discriminant is a square of a prime number p for $u,v \in \boldsymbol{Z}$, the only prime p ramifies in the splitting field of $f^{\mathfrak{A}_5}(u,v;X)$. Hence, composing it with a quadratic field K in which p ramifies, we obtain an unramified $\mathfrak{A}_5$-extension of K. The following table is a list of values $u,v \in \boldsymbol{Z}$ for which the discriminant of $f^{\mathfrak{A}_5}(u,v;X) = X^5 + c_4X^4+c_3X^3+c_2X^2+c_1X+c_0$ is a square of a small prime p.

u	v	$\left(\frac{-1}{p}\right)p$	c_4	c_3	c_2	c_1	c_0
-7	-75	653	-7	32	-75	117	-55
0	1	2053	0	-10	1	22	-15
-7	-77	-2083	-7	32	-77	123	-73
-7	-79	3329	-7	32	-79	129	-91
-5	-39	5413	-5	20	-39	57	-35
-6	-55	7433	-6	26	-55	82	-33
1	-7	-8311	1	-16	-7	57	-35

7. The symmetric group $\mathfrak{S}_5$ of order 120.

By a similar method, one can obtain a generic polynomial for $\mathfrak{S}_5$ over $\boldsymbol{Q}$. We omit a detail.

Theorem 6. (1) *The fixed field* $K^{\mathfrak{S}_5}$ *of* $\mathfrak{S}_5$ *is rational. Indeed we have* $K^{\mathfrak{S}_5} = \boldsymbol{Q}(U,V)$ *where*

$$\begin{cases} U = -u^2-15u-57 \\ V = \dfrac{v+90}{2u+15} - 13. \end{cases}$$

(2) *The polynomial*

$$f^{\mathfrak{S}_5}(U,V;X) = X^5+(U-8)X^4+(4UV+3V+15)X^3 + (4UV^2+3V^2-4UV-3V-2U^2-22U-26)X^2 + (-4U^2V-15UV-9V+3U^2+23U+19)X+U^3$$

is a generic polynomial for $\mathfrak{S}_5$ *over* $\boldsymbol{Q}$*.*

References

[1] Brumer, A.: Curves with real multiplications. (In preparation).

[2] Buhler, J., and Reichstein, Z.: Versal cyclic polynomials. (Unpublished manuscript).

[3] Hermite, C.: Sur l'invariant du dix-huitième ordre des formes du cinquième degré et sur le role qu'il joue dans la résolution de l'équation de cinquième degré. (extrait de deux lettres à M. Borchardt), J. Reine Angew. Math., **59**, 304–305, (œuvre II, 107–108). (1861).

[4] Hashimoto, K.: On Brumer's family of RM-curves of genus two. Tohoku Math. J. (2), **52** (4), 475–488 (2000).

[5] Jensen, C. U., Ledet, A., and Yui, N.: Generic polynomial, contructive aspects of the inverse Galois problem. Mathematical Sciences Reasearch Institute Publications, vol. 45, Cambridge University Press, Cambridge (2002).

[6] Lecacheux, O.: Construction de polynômes génériques à groupe de Galois résoluble. Acta Arith., **86**, 207–216 (1998).