J. Symbolic Computation (1987) **4**, 83–92

Polynomials for Primitive Nonsolvable Permutation Groups of Degree $d \leqslant 15$

GUNTER MALLE

Mathematisches Institut II, Lehrstuhl Professor Leopoldt, Englerstraße 2, D-7500 Karlsruhe 1, F.R.G.

The determination of polynomials over $\mathbb{Q}(t)$ with a given primitive nonsolvable permutation group of degree $d \leqslant 15$ as Galois group is completed. Sections 1–3 deal with the remaining three cases $\mathrm{Hol}(E_8)$, $\mathrm{PGL}_2(\mathbb{F}_{11})$ and $\mathrm{PSL}_3(\mathbb{F}_3)$. In section 4 the same methods are applied to calculate polynomials with the maximal transitive subgroups of the symmetric group S_6 as Galois groups. In all cases infinitely many specialisations $t \mapsto \tau \in \mathbb{Q}$ preserving the Galois group of the original polynomial are found according to the Hilbert irreducibility theorem.

Introduction

All nonsolvable groups having a faithful primitive permutation representation of degree $d \leqslant 15$ are known to occur as Galois groups over the rationals $\mathbb{Q}$ (see Matzat, 1984; Matzat & Zeh, 1986). A constructive way to obtain polynomials having one of these groups as Galois groups was also presented in Matzat (1984). The construction depends on solving a system of nonlinear algebraic equations in as many variables as the degree of the permutation group. This remained an obstacle to computing polynomials with the aforementioned groups as Galois groups. Still a comparison of the list of primitive permutation groups in Sims (1970) with the cases treated in Matzat (1984), Malle & Matzat (1985) and Matzat & Zeh (1986) shows that only polynomials with Galois groups $\mathrm{Hol}(E_8)$, $\mathrm{PGL}_2(\mathbb{F}_{11})$ and $\mathrm{PSL}_3(\mathbb{F}_3)$ over $\mathbb{Q}(t)$ remain to be determined. Using mainly the methods of Matzat (1984) we will construct the fixed fields of the stabiliser of a point in the primitive permutation representations of these groups (Stammkörper). This yields generating polynomials of the Galois extensions whose existence was shown in Matzat (1984). For the first time the case of a fixed field of genus different from zero (i.e. $g = 1$) will be treated. The systems of nonlinear algebraic equations were solved using a p-modular version of the Buchberger algorithm according to Malle & Trinks (1985).

In the last section the determination of extensions over $\mathbb{Q}(t)$ with a fixed ramification structure (Verzweigungsstruktur) of S_6 will permit the realisation of the maximal transitive subgroups of S_6 as Galois groups.

According to the Hilbert irreducibility theorem specialisations $t \mapsto \tau \in \mathbb{Q}$ preserving the Galois group will be given for each polynomial.

1. Polynomials with the Galois group $\mathrm{Hol}(E_8)$

By Matzat (1984), Lemma 10.1, there exists a Galois extension $N/\mathbb{Q}(t)$ with Galois group $G = \mathrm{Hol}(E_8)$ and ramification structure $\mathscr{C}^* = (C_4, C_4', C_6)^*$. (For the notation we

0747-7171/87/040083+10 $03.00/0

refer to Matzat (1984).) In this section a polynomial $f(t, X) \in \mathbb{Q}(t)[X]$ of degree eight with splitting field equal to N will be calculated.

Let L be the fixed field of the stabiliser in G of a point in a permutation representation of degree eight. Then L has degree eight over $\mathbb{Q}(t)$. The ramification structure $\mathscr{C}^* = (C_4, C_4', C_6)^*$ of $N/\mathbb{Q}(t)$ implies that three prime divisors $\bar{\mathfrak{p}}_1, \bar{\mathfrak{p}}_2, \bar{\mathfrak{p}}_3$ of residue class degree one are ramified in $\bar{L} := \bar{\mathbb{Q}}L$ over $\bar{\mathbb{Q}}(t)$ with ramification orders $e_1 = e_2 = 4$, $e_3 = 6$. In a transitive permutation representation of G of degree eight the elements of C_4 have the type (4, 2, 1, 1), those of C_6 the type (6, 2). So according to Satz B in Malle & Matzat (1985) the divisors $\bar{\mathfrak{p}}_1$, $\bar{\mathfrak{p}}_2$ and $\bar{\mathfrak{p}}_3$ ramify as follows

$$\bar{\mathfrak{p}}_i = \bar{\mathfrak{P}}_{i,1}^4 \cdot \bar{\mathfrak{P}}_{i,2}^2 \cdot \bar{\mathfrak{P}}_{i,3} \quad \text{for } i = 1, 2 \quad \text{and} \quad \bar{\mathfrak{p}}_3 = \bar{\mathfrak{P}}_{3,1}^6 \cdot \bar{\mathfrak{P}}_{3,2}^2,$$

with $\partial(\bar{\mathfrak{P}}_{i,j}) = 1$ for $j \leqslant 2$ and $\partial(\bar{\mathfrak{P}}_{1,3}) = \partial(\bar{\mathfrak{P}}_{2,3}) = 2$. Using the Hurwitz formula the genus of $\bar{L}$ and L is calculated as

$$g(\bar{L}) = g(L) = 1 - 8 + \tfrac{1}{2}(4+4+6) = 0.$$

While $\bar{\mathfrak{p}}_3$ is defined over $\mathbb{Q}(t)$, Lemma 10.1 in Matzat (1984) shows that the divisors $\bar{\mathfrak{p}}_1$ and $\bar{\mathfrak{p}}_2$ are permuted by $\mathrm{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$. Therefore one prime divisor $\mathfrak{p}_3$ of degree one and one divisor $\mathfrak{p}$ of degree two are ramified in $L/\mathbb{Q}(t)$ with respective ramification order 6 and 4. Choose a generating function t of $\mathbb{Q}(t)$ over $\mathbb{Q}$ with $\mathfrak{p} \cdot \mathfrak{p}_3^{-2} = (t^2 - \pi)$, $\pi \in \mathbb{Q}$. This determines t up to rational multiples. As $\mathfrak{p}_3 = \mathfrak{P}_{3,1}^6 \cdot \mathfrak{P}_{3,2}^2$ in $L/\mathbb{Q}(t)$, the field L contains prime divisors of degree one and therefore is a rational function field. A generating function x of L over $\mathbb{Q}$ will be determined up to rational multiples by $(x) = \mathfrak{P}_{3,2} \cdot \mathfrak{P}_{3,1}^{-1}$. In the splitting field $k(t)$ of $\mathfrak{p}$ with $(k : \mathbb{Q}) = 2$ the divisor $\mathfrak{p}$ splits into the product of $\tilde{\mathfrak{p}}_1$ and $\tilde{\mathfrak{p}}_2$, and the following equalities of divisors hold:

$$\frac{\tilde{\mathfrak{p}}_1}{\tilde{\mathfrak{p}}_3} = (t+\omega), \qquad \frac{\tilde{\mathfrak{p}}_2}{\tilde{\mathfrak{p}}_3} = (t-\omega), \quad \text{with } \omega^2 = \pi \in \mathbb{Q}.$$

In $\tilde{L} := kL$ over $k(t)$ the two divisors of $\mathfrak{p}$ split further to

$$\tilde{\mathfrak{p}}_i = \tilde{\mathfrak{P}}_{i,1}^4 \cdot \tilde{\mathfrak{P}}_{i,2}^2 \cdot \tilde{\mathfrak{P}}_{i,3} \quad \text{for } i = 1, 2.$$

Let $\tilde{\mathfrak{P}}_{3,j}$ be a prime divisor of $\mathfrak{P}_{3,j}$ in $\tilde{L}$. Then rational numbers α, β, γ and δ are determined by $\tilde{\mathfrak{P}}_{1,1} \cdot \tilde{\mathfrak{P}}_{3,1}^{-1} = (x+\alpha)$, $\tilde{\mathfrak{P}}_{1,2} \cdot \tilde{\mathfrak{P}}_{3,1}^{-1} = (x+\beta)$ and $\tilde{\mathfrak{P}}_{1,3} \cdot \tilde{\mathfrak{P}}_{3,1}^{-2} = (x^2+\gamma x+\delta)$. Writing $\bar{}$: $k \to k$, $\kappa \mapsto \bar{\kappa}$ for the generating automorphism of $k/\mathbb{Q}$ we have $\tilde{\mathfrak{P}}_{2,1} \cdot \tilde{\mathfrak{P}}_{3,1}^{-1} = \overline{(x+\alpha)} = (x+\bar{\alpha})$, $\tilde{\mathfrak{P}}_{2,2} \cdot \tilde{\mathfrak{P}}_{3,1}^{-1} = (x+\bar{\beta})$ and $\tilde{\mathfrak{P}}_{2,3} \cdot \tilde{\mathfrak{P}}_{3,1}^{-2} = (x^2+\bar{\gamma}x+\bar{\delta})$. This leads to

$$(t+\omega) = \frac{\tilde{\mathfrak{p}}_1}{\tilde{\mathfrak{p}}_3} = \frac{\tilde{\mathfrak{P}}_{1,1}^4 \cdot \tilde{\mathfrak{P}}_{1,2}^2 \cdot \tilde{\mathfrak{P}}_{1,3}}{\tilde{\mathfrak{P}}_{3,1}^6 \cdot \tilde{\mathfrak{P}}_{3,2}^2} = \left(\frac{(x+\alpha)^4(x+\beta)^2(x^2+\gamma x+\delta)}{x^2}\right)$$

and the equation of divisors conjugate to this in $\bar{L}/L$. So there exists $\eta \in k^\times$ with

$$\begin{aligned} x^2(t+\omega) &= \eta(x+\alpha)^4(x+\beta)^2(x^2+\gamma x+\delta) \\ x^2(t-\omega) &= \bar{\eta}(x+\bar{\alpha})^4(x+\bar{\beta})^2(x^2+\bar{\gamma}x+\bar{\delta}). \end{aligned} \tag{1}$$

Eliminating t from (1) we obtain

$$2\omega x^2 = \eta(x+\alpha)^4(x+\beta)^2(x^2+\gamma x+\delta) - \bar{\eta}(x+\bar{\alpha})^4(x+\bar{\beta})^2(x^2+\bar{\gamma}x+\bar{\delta}). \tag{2}$$

The generating element x of L is transcendent over k, so the last equation can be regarded as a polynomial identity in x, which gives $\eta = \bar{\eta}$. Subtracting (2) differentiated with

respect to x and multiplied by x from (2) multiplied by two, we have

$$p^3q(2pqr-x(4qr+2pr+pqr')) = \bar{p}^3\bar{q}(2\bar{p}\bar{q}\bar{r}-x(4\bar{q}\bar{r}+2\bar{p}\bar{r}+\bar{p}\bar{q}\bar{r}')) \tag{3}$$

with $p = x+\alpha$, $q = x+\beta$ and $r = x^2+\gamma x+\delta$. As $\tilde{\mathscr{P}}^3_{1,1}\cdot\tilde{\mathscr{P}}_{1,2}$ and $\tilde{\mathscr{P}}^3_{2,1}\cdot\tilde{\mathscr{P}}_{2,2}$ do not have a common factor, the same holds for the polynomials p^3q and $\bar{p}^3\bar{q}$, and (3) can be divided up into

$$6p^3q+2\bar{p}\bar{q}\bar{r}-x(4\bar{q}\bar{r}+2\bar{p}\bar{r}+\bar{p}\bar{q}\bar{r}') = 0$$

$$6\bar{p}^3\bar{q}+2pqr-x(4qr+2pr+pqr') = 0.$$

Comparing coefficients this leads to a system of eight nonlinear equations in eight unknowns. The generating function x which was determined only up to rational multiples can be fixed by one additional condition. Setting $\alpha+\bar{\alpha} = 0$ does not lead to a solution of the system of equations, so let $\alpha+\bar{\alpha} = 2$. Using the modular algorithm of Malle & Trinks (1985) one finds exactly two solutions in a quadratic extension field of $\mathbb{Q}$; with $\theta = \pm\sqrt{7}$ they are $\alpha = 1-\theta$, $\beta = -13-\theta$, $\gamma = -2+6\theta$ and $\delta = 32+10\theta$. As $\omega \in k$ we may choose $\omega = \theta$ and thereby fix t. From (1) it follows

THEOREM 1: *The splitting field N of the polynomial*

$$f(X,t) = X^8-24X^7+2128X^5+2184X^4-66528X^3 \\ -28672X^2-243648X+104976-87808X^2t$$

has the Galois group $\mathrm{Hol}(E_8)$ *over* $\mathbb{Q}(t)$ *and the ramification structure* $\mathscr{C}^* = (C_4, C_4', C_6)^*$.

According to the Hilbert irreducibility theorem there exist infinitely many specialisations $t \mapsto \tau \in \mathbb{Q}$ such that $f(X,\tau)$ still has the Galois group $\mathrm{Hol}(E_8)$. A series of such specialisations shall now be found.

COROLLARY 1: *The polynomial $f(X,\tau)$ has the Galois group* $\mathrm{Hol}(E_8)$ *over* $\mathbb{Q}$ *for all values* $\tau \in \mathbb{Z}$ *with*

$$\tau \equiv 2 \pmod{715}.$$

PROOF: The Galois group of $f(X,\tau)$ is isomorphic to a subgroup of $\mathrm{Gal}(f(X,t))$. For $\tau \equiv 2 \pmod{715}$ the polynomial $f(X,\tau)$ has the following factorisations

$$f(X,\tau) \equiv (X+1)(X+2)(X^2+2X+3)(X^4+X^3+4X^2+4X+1) \pmod 5,$$
$$f(X,\tau) \equiv (X^2+8X+9)(X^6+X^5+5X^4+5X^2+4X+4) \pmod{11},$$
$$f(X,\tau) \equiv (X+5)(X^7+10X^6+2X^5+12X^4+5X^3+7X^2+11X+8) \pmod{13}.$$

Therefore $\mathrm{Gal}(f(X,\tau))$ contains elements of cycle shapes (4, 2, 1, 1), (6, 2) and (7, 1) and so is isomorphic to $\mathrm{Hol}(E_8)$. ■

The Galois group of $N/L = N/\mathbb{Q}(x)$ with $f(x,t) = 0$ has index eight in $\mathrm{Gal}(N/\mathbb{Q}(t)) \cong \mathrm{Hol}(E_8)$. Thus it is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$. By setting $f(X,t) =: g(X)+t\cdot h(X)$ a generating polynomial of N/L can be obtained as in Matzat & Zeh (1986), Bemerkung 4:

THEOREM 2: *N is the splitting field of*

$$f_1(X,x) = \frac{g(X)h(x)-g(x)h(X)}{X-x}$$

over $\mathbb{Q}(x)$ *with the Galois group* $\mathrm{Gal}(N/\mathbb{Q}(x)) \cong \mathrm{PSL}_2(\mathbb{F}_7)$ *and ramification structure* $\mathscr{C}^* = (C_2, C_2, C_4, C_4, C_4, C_4, C_3)^*$.

2. Polynomials with the Galois groups $\mathrm{PGL}_2(\mathbb{F}_{11})$ and $\mathrm{PSL}_2(\mathbb{F}_{11})$

In Matzat (1984), Satz 7.2, the existence of a Galois extension $N/\mathbb{Q}(t)$ with the group $G = \mathrm{PGL}_2(\mathbb{F}_{11})$ and the ramification structure $\mathscr{C}^* = (C_2^-, C_4, C_{11})^*$ was proved. Let L be the fixed field in N of a one point stabiliser in a permutation representation of G of degree twelve. In such a permutation representation the elements in C_2^- have the permutation type (2, 2, 2, 2, 2, 1, 1), the elements in C_4 have the type (4, 4, 4) and those in C_{11} have the type (11, 1). The Hurwitz genus formula then yields $g(L) = 1-12+\frac{1}{2}(5+9+10) = 1$. Denote by $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ the three prime divisors of degree one ramified in $L/\mathbb{Q}(t)$. By Satz B in Malle & Matzat (1985) they ramify as follows

$$\mathfrak{p}_1 = \mathscr{P}_{1,1}^2 \cdot \mathscr{P}_{1,2}, \qquad \mathfrak{p}_2 = \mathscr{P}_2^4, \qquad \mathfrak{p}_3 = \mathscr{P}_{3,1}^{11} \cdot \mathscr{P}_{3,2},$$

with $\partial(\mathscr{P}_{3,1}) = \partial(\mathscr{P}_{3,2}) = 1$, $\partial(\mathscr{P}_2) = 3$, $\partial(\mathscr{P}_{1,1}) = 5$ and $\partial(\mathscr{P}_{1,2}) = 2$. So L contains prime divisors of degree one and is a disclosed elliptic function field. Choose a function $u \in L$ with divisor of poles equal to $\mathscr{P}_{3,1}^2$ according to the theorem of Riemann–Roch. Then the extension $L/\mathbb{Q}(u)$ has degree two. Denote by $\bar{}: L \to L$ the generating automorphism of that field extension. A generating function t of $\mathbb{Q}(t)$ is determined by $\mathfrak{p}_2 \cdot \mathfrak{p}_3^{-1} = (t)$ and $\mathfrak{p}_1 \cdot \mathfrak{p}_3^{-1} = (t-1)$. Suppose $t \in K := \mathbb{Q}(u)$. Then to K as a subfield of $N/\mathbb{Q}(t)$ would correspond a subgroup of $G = \mathrm{PGL}_2(\mathbb{F}_{11})$ of index six. But G does not have such a subgroup. So t generates L over K. The ramification of $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{p}_3$ now yields

$$(t\bar{t}) = \frac{\mathscr{P}_2^4 \cdot \bar{\mathscr{P}}_2^4}{\mathscr{P}_{3,1}^{22} \cdot \mathscr{P}_{3,2} \cdot \bar{\mathscr{P}}_{3,2}} = \frac{\mathscr{R}_2^4}{\mathscr{R}_{3,1}^{11} \cdot \mathscr{R}_{3,2}}, \qquad (t-1)(\bar{t}-1) = \frac{\mathscr{R}_{1,1}^2 \cdot \mathscr{R}_{1,2}}{\mathscr{R}_{3,1}^{11} \cdot \mathscr{R}_{3,2}}$$

where the divisors $\mathscr{R}_{1,1}$, $\mathscr{R}_{1,2}$, $\mathscr{R}_2$, $\mathscr{R}_{3,1} = \mathscr{P}_{3,1}^2$ and $\mathscr{R}_{3,2}$ are defined over K. (The extension L/K is ramified in $\mathscr{R}_{3,1}$ because of the choice of u.)

Let finally x be a generating function of $K = \mathbb{Q}(u)$ with $\mathscr{R}_{3,1}$ as divisor of poles and the condition $\mathscr{R}_2 \cdot \mathscr{R}_{3,1}^{-3} = (b(x)) = (x^3+\beta_1 x+\beta_0)$. Define μ_i, ν_i and λ in $\mathbb{Q}$ by $\mathscr{R}_{1,1} \cdot \mathscr{R}_{3,1}^{-5} = (m(x)) = (x^5+\mu_4 x^4+\mu_3 x^3+\mu_2 x^2+\mu_1 x+\mu_0)$, $\mathscr{R}_{1,2} \cdot \mathscr{R}_{3,1}^{-2} = (n(x)) = (x^2+\nu_1 x+\nu_0)$ and $\mathscr{R}_{3,2} \cdot \mathscr{R}_{3,1}^{-1} = (x+\lambda)$. Then there exist $\eta, \pi \in \mathbb{Q}$ with

$$t\bar{t}(x+\lambda) = \eta b(x)^4 \quad \text{and} \quad (t-1)(\bar{t}-1)(x+\lambda) = \pi m(x)^2 n(x).$$

From this the minimal polynomial of t over K is $F(t) = (x+\lambda)t^2 - a(x)t + \eta b(x)^4$ with $a(x) := x+\lambda+\eta b(x)^4 - \pi m(x)^2 n(x)$. The extension L/K is ramified in precisely three places apart from $\mathscr{R}_{3,1}$. So the discriminant $D(F) = a(x)^2 - 4\eta b(x)^4(x+\lambda)$ of F has to be of the form $\kappa c(x)^2 d(x)$ with a polynomial $d(x)$ of degree three in x and $\kappa \in \mathbb{Q}$. In particular the degree in x of the discriminant is odd, so the above formula for $D(F)$ shows $\eta = \pi$, $\kappa = -4\eta$ and $\partial(c(x)) = 5$. As x is transcendental over $\mathbb{Q}$, the equation $D(F) = -4\eta c(x)^2 d(x)$ can be regarded as an equality in the polynomial ring $\mathbb{Q}[x]$. Comparing the coefficients in x leads to a nonlinear system of 24 equations in 19 variables. The function x may now be determined by setting $\nu_1 = 8$, because the choice $\nu_1 = 0$ does not give a solution. For every solution of the original problem, the polynomials $a(x)$, $b(x)$, $m(x)$, $n(x)$ and $(x+\lambda)$ may not have a common factor. Under this condition with the algorithm described in Malle & Trinks (1985) only one solution of the system of equations is found: $\beta_1 = -66$, $\beta_0 = -308$, $\mu_4 = -4$, $\mu_3 = -152$, $\mu_2 = 280$, $\mu_1 = 8204$, $\mu_0 = -29888$, $\nu_0 = 88$, $\lambda = -11$ and $\eta = -2^{-16}3^{-11}$. To simplify the result, set $T := 2^8 3^5 t$.

THEOREM 3: (*a*) *The splitting field N of the polynomial*

$$f(X, T) = (X^3 - 66X - 308)^4 - 9T(11X^5 - 44X^4 - 1573X^3 + 1892X^2 + 57358X + 103763) - 3T^2(X - 11)$$

has the Galois group $\mathrm{PGL}_2(\mathbb{F}_{11})$ *over* $\mathbb{Q}(t)$ *and ramification structure* $\mathscr{C}^* = (C_2^-, C_4, C_{11})^*$.

(*b*) *N is the splitting field of*

$$f(X, 62208/(11y^2+1)) \in \mathbb{Q}(y)[X]$$

over $\mathbb{Q}(y)$ *with the Galois group* $\mathrm{Gal}(N/\mathbb{Q}(y)) \cong \mathrm{PSL}_2(\mathbb{F}_{11})$ *and ramification structure* $\mathscr{C}^* = (C_2^+, C_{11}, C_{11}')^*$.

PROOF: In Satz 7.2 of Matzat (1984) the fixed field M of $\mathrm{PSL}_2(\mathbb{F}_{11})$ in N is shown to be a rational function field $\mathbb{Q}(y)$. Precisely the two prime divisors $\mathfrak{p}_1 = \mathfrak{P}_1^2$ and $\mathfrak{p}_2 = \mathfrak{P}_2^2$ are ramified in $M/\mathbb{Q}(t)$. So a generating function y of M may be chosen with $(y) = \mathfrak{P}_1 \cdot \mathfrak{P}_2^{-1}$. This determines y up to rational multiples and the following holds

$$\left(\frac{t-1}{t}\right) = \frac{\mathfrak{p}_1}{\mathfrak{p}_2} = \frac{\mathfrak{P}_1^2}{\mathfrak{P}_2^2} = (y^2).$$

Consequently there exists $\alpha \in \mathbb{Q}^\times$ with $\alpha(t-1) = ty^2$. The discriminant of f with respect to X is equal to $-11(t-1)t^{-1}$ up to a square. As this discriminant has to become a square in M, we may choose $\alpha = -1/11$, thereby fixing y. With $T = 2^8 3^5 t = 2^8 3^5/(11y^2+1)$ part (b) follows. ■

COROLLARY 2: (*a*) *The polynomial* $f(X, \tau)$ *has the Galois group* $\mathrm{PGL}_2(\mathbb{F}_{11})$ *over* $\mathbb{Q}$ *for all values* $\tau \in \mathbb{Z}$ *with*

$$\tau \equiv 1 \pmod{10}.$$

(*b*) *The polynomial* $f(X, 66208/(11\tau^2+1))$ *has the Galois group* $\mathrm{PSL}_2(\mathbb{F}_{11})$ *over* $\mathbb{Q}$ *for all values* $\tau \in \mathbb{Z}$ *with*

$$\tau \equiv 1 \pmod{65}.$$

PROOF: The polynomial $f(X, 1)$ remains irreducible modulo the prime 5 and has factors of degrees 10, 1 and 1 modulo two. So as $\mathrm{Gal}(f(X, 1))$ contains elements of orders ten and twelve it is already equal to $\mathrm{Gal}(f(X, T)) \cong \mathrm{PGL}_2(\mathbb{F}_{11})$. The congruences remain valid for all $\tau \equiv 1 \pmod{10}$, so (a) follows.

$f(X, 5184)$ has two irreducible factors of degree six modulo 5 and two factors of degrees 11 and 1 modulo 13. As $\mathrm{PSL}_2(\mathbb{F}_{11})$ does not have a proper subgroup containing elements of orders six and eleven, this shows (b). ■

3. Polynomials with the Galois group $\mathrm{PSL}_3(\mathbb{F}_3)$

By Matzat (1984), Satz 10.4, there exists a regular Galois extension $N/\mathbb{Q}(t)$ with Galois group $G = \mathrm{PSL}_3(\mathbb{F}_3)$ and ramification structure $\mathscr{C}^* = (C_2, C_8, C_8')^*$. In a permutation representation of G of degree thirteen, elements of the class C_2 have the permutation type (2, 2, 2, 2, 1, 1, 1, 1, 1), elements of the classes C_8 and C_8' have the type (8, 4, 1). Let L be the fixed field in N of the stabiliser of a point in that permutation representation. If x denotes a generating element of $L/\mathbb{Q}(t)$ then the minimal polynomial of x has splitting field N and its Galois group is equal to G.

According to the ramification structure of $N/\mathbb{Q}(t)$ three prime divisors $\bar{\mathfrak{p}}_1$, $\bar{\mathfrak{p}}_2$, $\bar{\mathfrak{p}}_3$ of residue class degree one are ramified in $\bar{L} := \bar{\mathbb{Q}}L$ over $\bar{\mathbb{Q}}(t)$ with ramification order $e_1 = 2$, $e_2 = e_3 = 8$ respectively. The cycle shapes of elements in the three classes of $\mathscr{C}$ yield the ramification

$$\bar{\mathfrak{p}}_1 = \bar{\mathfrak{Q}}_{1,1}^2 \cdot \bar{\mathfrak{Q}}_{1,2} \quad \text{and} \quad \bar{\mathfrak{p}}_i = \bar{\mathfrak{P}}_{i,1}^8 \cdot \bar{\mathfrak{P}}_{i,2}^4 \cdot \bar{\mathfrak{P}}_{i,3} \quad \text{for } i = 2, 3,$$

with $\partial(\bar{\mathfrak{Q}}_{1,1}) = 4$, $\partial(\bar{\mathfrak{Q}}_{1,2}) = 5$ and $\partial(\bar{\mathfrak{P}}_{i,j}) = 1$ for $i \geqslant 2$. The genus of $\bar{L}$ and L is equal to $g(\bar{L}) = g(L) = 1 - 13 + \frac{1}{2}(4 + 10 + 10) = 0$.

The divisor $\bar{\mathfrak{p}}_1$ is defined over $\mathbb{Q}(t)$, while $\bar{\mathfrak{p}}_2$ and $\bar{\mathfrak{p}}_3$ are permuted by $\mathrm{Gal}(\bar{\mathbb{Q}}(t)/\mathbb{Q}(t))$ (Matzat, 1984). So in $L/\mathbb{Q}(t)$ one prime divisor $\mathfrak{p}_1$ of degree one and one divisor $\mathfrak{q}$ of degree two are ramified with respective ramification orders 2 and 8. A generating function t of $\mathbb{Q}(t)$ is determined up to rational multiples by $\mathfrak{q} \cdot \mathfrak{p}_1^{-2} = (t^2 - \pi)$ with $\pi \in \mathbb{Q}$. The centraliser of an involution in $\mathrm{PSL}_3(\mathbb{F}_3)$ is contained in the stabiliser of a point in the permutation representation of degree thirteen. So it does not act transitively on the five prime divisors of $\bar{\mathfrak{Q}}_{1,2}$ in $\mathbb{P}(\bar{\mathbb{Q}}L/\bar{\mathbb{Q}})$. This gives the ramification

$$\mathfrak{p}_1 = \mathfrak{P}_{1,1}^2 \cdot \mathfrak{P}_{1,2} \cdot \mathfrak{P}_{1,3}$$

with $\partial(\mathfrak{P}_{1,1}) = \partial(\mathfrak{P}_{1,2}) = 4$, $\partial(\mathfrak{P}_{1,3}) = 1$ in $L/\mathbb{Q}(t)$. Let x be a generating function of the rational function field L with divisor of poles $\mathfrak{P}_{1,3}$. Define μ_i, $\nu_i \in \mathbb{Q}$ by $\mathfrak{P}_{1,1} \cdot \mathfrak{P}_{1,3}^{-4} =: (x^4 + \mu_3 x^3 + \mu_2 x^2 + \mu_1 x + \mu_0) =: (p(x))$ and $\mathfrak{P}_{1,2} \cdot \mathfrak{P}_{1,3}^{-4} =: (x^4 + \nu_3 x^3 + \nu_2 x^2 + \nu_1 x + \nu_0) =: (q(x))$. By a theorem of Shih (1974) the splitting field of $\mathfrak{q}$ is $k(t) = \mathbb{Q}(\sqrt{-2})(t)$ (compare Bemerkung 5.3 in Matzat (1985) for a more general version). We have

$$\frac{\tilde{\mathfrak{p}}_2}{\tilde{\mathfrak{p}}_1} = (t + \omega), \qquad \frac{\tilde{\mathfrak{p}}_3}{\tilde{\mathfrak{p}}_1} = (t - \omega) \quad \text{with } \omega^2 = \pi \in \mathbb{Q},$$

for the three divisors $\tilde{\mathfrak{p}}_2$, $\tilde{\mathfrak{p}}_3$ of $\mathfrak{q}$ and $\tilde{\mathfrak{p}}_1$ of $\mathfrak{p}_1$ in $k(t)$. In $\bar{L} := kL$ over $k(t)$, the first two divisors split further into

$$\tilde{\mathfrak{p}}_i = \tilde{\mathfrak{P}}_{i,1}^8 \cdot \tilde{\mathfrak{P}}_{i,2}^4 \cdot \tilde{\mathfrak{P}}_{i,3} \quad \text{for } i = 2, 3.$$

Let κ, λ, $\rho \in k$ be defined by $\tilde{\mathfrak{P}}_{2,1} \cdot \tilde{\mathfrak{P}}_{1,3}^{-1} = (x + \kappa)$, $\tilde{\mathfrak{P}}_{2,2} \cdot \tilde{\mathfrak{P}}_{1,3}^{-1} = (x + \lambda)$ and $\tilde{\mathfrak{P}}_{2,3} \cdot \tilde{\mathfrak{P}}_{1,3}^{-1} = (x + \rho)$. Then we have $\tilde{\mathfrak{P}}_{3,1} \cdot \tilde{\mathfrak{P}}_{1,3}^{-1} = (x + \bar{\kappa})$, $\tilde{\mathfrak{P}}_{3,2} \cdot \tilde{\mathfrak{P}}_{1,3}^{-1} = (x + \bar{\lambda})$ and $\tilde{\mathfrak{P}}_{3,3} \cdot \tilde{\mathfrak{P}}_{1,3}^{-1} = (x + \bar{\rho})$ with the generating automorphism $\bar{}: k \to k$, $\alpha \mapsto \bar{\alpha}$ of $k/\mathbb{Q}$. So we get the equation

$$(t + \omega) = \frac{\tilde{\mathfrak{p}}_2}{\tilde{\mathfrak{p}}_1} = \frac{\tilde{\mathfrak{P}}_{2,1}^8 \cdot \tilde{\mathfrak{P}}_{2,2}^4 \cdot \tilde{\mathfrak{P}}_{2,3}}{\tilde{\mathfrak{P}}_{1,1}^2 \cdot \tilde{\mathfrak{P}}_{1,2} \cdot \tilde{\mathfrak{P}}_{1,3}} = \left(\frac{(x+\kappa)^8 (x+\lambda)^4 (x+\rho)}{p(x)^2 q(x)} \right)$$

and the conjugate of it in $\tilde{L}/L$. By the equality of divisors there exists a $\eta \in k^\times$ with

$$\begin{aligned} p(x)^2 q(x)(t + \omega) &= \eta (x+\kappa)^8 (x+\lambda)^4 (x+\rho), \\ p(x)^2 q(x)(t - \omega) &= \bar{\eta} (x+\bar{\kappa})^8 (x+\bar{\lambda})^4 (x+\bar{\rho}). \end{aligned} \tag{1}$$

Eliminating t from (1) yields the polynomial identity in X

$$2\omega p(X)^2 q(X) = \eta (X+\kappa)^8 (X+\lambda)^4 (X+\rho) - \bar{\eta} (X+\bar{\kappa})^8 (X+\bar{\lambda})^4 (X+\bar{\rho}), \tag{2}$$

showing $\eta = \bar{\eta}$. Subtract equation (2) differentiated with respect to X multiplied by $p(X)q(X)$ from (2) multiplied by $2p(X)'q(X) + p(X)q(X)'$ to get

$$\begin{aligned} u^7 v^3 (uvw(2p'q + pq') - pq(8vw + 4uw + uv)) \\ = \bar{u}^7 \bar{v}^3 (\bar{u}\bar{v}\bar{w}(2p'q + pq') - pq(8\bar{v}\bar{w} + 4\bar{u}\bar{w} + \bar{u}\bar{v})) \end{aligned} \tag{3}$$

with $u = X+\kappa$, $v = X+\lambda$ and $w = X+\rho$. The divisors $\tilde{\mathscr{P}}^7_{2,1}\cdot\tilde{\mathscr{P}}^3_{2,2}$ and $\tilde{\mathscr{P}}^7_{3,1}\cdot\tilde{\mathscr{P}}^3_{3,2}$ do not have a common factor, so neither do u^7v^3 and $\bar{u}^7\bar{v}^3$. So (3) may be divided up into

$$u^7v^3+\bar{u}\bar{v}\bar{w}(2p'q+pq')-pq(8\bar{v}\bar{w}+4\bar{u}\bar{w}+\bar{u}\bar{v}) = 0,$$

$$\bar{u}^7\bar{v}^3+uvw(2p'q+pq')-pq(8vw+4uw+uv) = 0.$$

Comparison of coefficients leads to a system of twenty nonlinear equations in fourteen unknowns. Because x was determined only up to linear substitutions, we may choose $\lambda+\bar{\lambda} = 0$ and (as $\kappa+\bar{\kappa} = 0$ does not give a solution) $\kappa+\bar{\kappa} = 4$. The resulting system of equations has exactly two solutions in $k = \mathbb{Q}(\sqrt{-2})$, which were found with the algorithm in Malle & Trinks (1985); with $\theta = \pm\sqrt{-2}$ they are $\mu_3 = -\frac{4}{3}$, $\mu_2 = 4$, $\mu_1 = -8$, $\mu_0 = -\frac{68}{3}$, $\nu_3 = 16$, $\nu_2 = 72$, $\nu_1 = 128$, $\nu_0 = 188$, $\kappa = 2+3\theta$, $\lambda = -\theta$ and $\rho = -2\theta$.

Now t may be fixed by setting $\eta = 1$.

THEOREM 4: *The splitting field N of the polynomial*

$$\begin{aligned} f(X,t) = {} & X^{13}+16X^{12}-132X^{11}-2016X^{10}-9060X^9-43776X^8-144096X^7 \\ & -377088X^6-1015056X^5-1743616X^4-3388480X^3-3177984X^2-3311040X \\ & +989184-t(3X^4-4X^3+12X^2-24X-68)^2(X^4+16X^3+72X^2+128X+188) \end{aligned}$$

has the Galois group $\mathrm{PSL}_3(\mathbb{F}_3)$ *over* $\mathbb{Q}(t)$ *and ramification structure* $\mathscr{C}^* = (C_2, C_8, C_8')^*$.

COROLLARY 3: *The polynomial $f(X,\tau)$ has the Galois group* $\mathrm{PSL}_3(\mathbb{F}_3)$ *over* $\mathbb{Q}$ *for all values* $\tau \in \mathbb{Z}$ *with*

$$\tau \equiv 1 \pmod{385}.$$

PROOF: The Galois group of $f(X,\tau)$ is isomorphic to a subgroup of $\mathrm{Gal}(f(X,t))$. For $\tau \equiv 1 \pmod{385}$ the polynomial $f(X,\tau)$ has the factorisations

$$\begin{aligned} f(X,\tau) \equiv {} & (X+6)(X^4+5X^3+4X^2+3) \\ & (X^8+3X^7+3X^6+6X^4+4X^3+4X^2+1) \pmod 7, \end{aligned}$$

$$\begin{aligned} f(X,\tau) \equiv {} & (X+1)(X^3+5X^2+9X+8)(X^3+5X^2+4X+3) \\ & (X^3+3X^2+5X+7)(X^3+4X^2+2X+9) \pmod{11}, \end{aligned}$$

and remains irreducible modulo 5. So $\mathrm{Gal}(f(X,\tau))$ contains elements of orders 3, 8 and 13 and is isomorphic to $\mathrm{PSL}_3(\mathbb{F}_3)$. ■

4. Transitive subgroups of S_6 as Galois groups

Apart from A_6 and S_5, the symmetric group S_6 on six symbols possesses two further maximal subgroups; these are G_{72} (imprimitive on two sets of three symbols each) of index ten and G_{48} (imprimitive on three sets of two symbols each) of index fifteen. Clearly by the result of Shafarevich these solvable groups are known to occur as Galois groups over the rationals. Here polynomials of degree six with corresponding Galois groups will be given.

In Matzat (1984), Lemma 6.1, the existence of a regular field extension $N/\mathbb{Q}(t)$ having Galois group S_6 and ramification structure $\mathscr{C}^* = (C_2, C_5, C_6)^*$ was proved. Denote by L_0 the fixed field in N of an intransitive subgroup S_5 in a permutation representation of S_6 of degree six. In Matzat (1984) L_0 was shown to be a rational function field and a generating

trinomial of degree six for $N/\mathbb{Q}(t)$ was calculated. The outer automorphism of S_6 transforms $\mathscr{C}^*$ into $\mathscr{C}_1^* = (C_2', C_5, C_6')^*$ where C_2' and C_6' contain elements of cycle shapes (2, 2, 2) and (3, 2, 1) respectively. The fixed field L_1 of a transitive subgroup S_5 in S_6 is a rational function field. Using the primitive permutation representations of S_6 of degrees ten and fifteen in Sims (1970) and Satz B in Malle & Matzat (1985) the fixed fields L_2, L_3 of subgroups G_{72} and G_{48} are seen to be rational function fields, of degrees ten and fifteen over $\mathbb{Q}(t)$. So with the methods of the preceding sections generating polynomials of degrees six, ten and fifteen for $N/\mathbb{Q}(t)$ may be calculated.

THEOREM 5: *The splitting field of each of the four polynomials*

$$f_0(X, T) = X^6 - 6X^5 + T,$$
$$f_1(W, T) = W^6 - 120W^5 + 64(W+8)^2(W+5)T,$$
$$f_2(Y, T) = (Y^2 - 14Y + 4)^5 - 27(Y-16)Y^3T,$$
$$f_3(Z, T) = (Z^2-45)^5Z^5 - \tfrac{27}{4}(2Z+15)^2(Z-6)(Z^2-2Z-15)^3T$$

is equal to N and the orders of ramification in the ramified places ∞, 0 *and* 5^5 *are* 6, 5 *and* 2 *respectively.*

PROOF: The polynomial $f_0(X, T)$ is obtained from $f(x, t)$ in Matzat (1984) by the transformation $X := 5x$, $T := 5^5t$. The remaining three polynomials are calculated along the lines of the first three sections, with only the last case leading to a moderately complicated system of nonlinear equations which can be solved with the algorithm of Malle & Trinks (1985). ■

We can now find trinomials having Galois groups $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$, G_{72} and G_{48}. For this let w, y, z be zeros in N of $f_1(W, T)$, $f_2(Y, T)$, $f_3(Z, T)$ respectively. So without loss of generality $L_1 = \mathbb{Q}(w)$, $L_2 = \mathbb{Q}(y)$, $L_3 = \mathbb{Q}(z)$ and we have:

THEOREM 6: (*a*) *N is the splitting field over* $\mathbb{Q}(w)$ *of*

$$g_1(X, w) = X^6 - 6X^5 - \frac{w^5(w-120)}{64(w+8)^2(w+5)}$$

and has the Galois group $\mathrm{PGL}_2(\mathbb{F}_5)$ *and the ramification structure* $\mathscr{C}_2^* = (C_2, C_3, C_5, C_6)^*$.

(*b*) *N is the splitting field over* $\mathbb{Q}(v)$ *of*

$$g_1(X, v^2-5) \in \mathbb{Q}(v)[X]$$

with the Galois group $\mathrm{PSL}_2(\mathbb{F}_5)$ *and the ramification structure* $\mathscr{C}_3^* = (C_3, C_3, C_3, C_5, C_5)^*$.

(*c*) *The splitting field N of the polynomial*

$$g_2(X, y) = X^6 - 6X^5 + \frac{(y^2-14y+4)^5}{27(y-16)y^3}$$

has the Galois group G_{72} *over* $\mathbb{Q}(y)$ *and the ramification structure* $\mathscr{C}_4^* = (4 \cdot C_2, C_2', C_6)^*$.

(*d*) *The splitting field N of the polynomial*

$$g_3(X, z) = X^6 - 6X^5 + \frac{4z^5(z^2-45)^5}{27(2z+15)^2(z-6)(z^2-2z-15)^3}$$

has the Galois group G_{48} *over* $\mathbb{Q}(z)$ *and the ramification structure* $\mathscr{C}_5^* = (3 \cdot C_2, 2 \cdot C_2', C_3, C_6)^*$.

(*e*) *N is the splitting field of*

$$g_3(X, 3(5u^2-1)/(3u^2+1)) \in \mathbb{Q}(u)[X]$$

over $\mathbb{Q}(u)$ *with the Galois group* $Z_2 \times A_4 \cong G_{24} < G_{48}$ *and ramification structure* $\mathscr{C}_6^* = (6 \cdot C_2, C_3, C_3, C_6, C_6)^*$.

PROOF: By definition $\mathbb{Q}(w)$, $\mathbb{Q}(y)$, $\mathbb{Q}(z)$ are the fixed fields of $\mathrm{PGL}_2(\mathbb{F}_5)$, G_{72} and G_{48} in $N/\mathbb{Q}(t)$, so the polynomials in (a), (c) and (d) may be obtained from Theorem 5. The precise ramification in $L_i/\mathbb{Q}(t)$ yields the stated ramification structures. The fixed fields of $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$ in N/L_1 and of G_{24} in N/L_3 turn out to be rational function fields $\mathbb{Q}(v)$ and $\mathbb{Q}(u)$. So generating equations for $N/\mathbb{Q}(v)$ and $N/\mathbb{Q}(u)$ may be calculated from the ones for N/L_1 and N/L_3 as in the case of $\mathrm{PSL}_2(\mathbb{F}_{11})$ in section 2. ■

COROLLARY 4: (*a*) *The polynomial* $g_1(X, \omega)$ *has the Galois group* $\mathrm{PGL}_2(\mathbb{F}_5)$ *over* $\mathbb{Q}$ *for all values* $\omega \in \mathbb{Z}$ *with*

$$\omega \equiv 1 \pmod{209}.$$

(*b*) *For* $v \in \mathbb{Z}$ *with*

$$v \equiv 1 \pmod{35}$$

the Galois group of $g_1(X, v^2-5)$ *over* $\mathbb{Q}$ *is isomorphic to* $\mathrm{PSL}_2(\mathbb{F}_5)$.

(*c*) *For* $\gamma \in \mathbb{Z}$ *with*

$$\gamma \equiv 1 \pmod{187}$$

the Galois group of $g_2(X, \gamma)$ *over* $\mathbb{Q}$ *is isomorphic to* G_{72}.

(*d*) *For* $\zeta \in \mathbb{Z}$ *with*

$$\zeta \equiv 1 \pmod{247}$$

the Galois group of $g_3(X, \zeta)$ *over* $\mathbb{Q}$ *is isomorphic to* G_{48}.

(*e*) *For* $\xi \in \mathbb{Z}$ *with*

$$\xi \equiv 1 \pmod{143}$$

the Galois group of $g_3(X, 3(5\xi^2-1)/(3\xi^2+1))$ *over* $\mathbb{Q}$ *is isomorphic to* G_{24}.

To prove Corollary 4, the factorisations of the g_i modulo certain primes must be studied, similar to the way in the preceding sections.

Theorem 6 gives trinomials for all the transitive subgroups of S_6 with rational fixed field in N, as can be seen from the ramification structures. For certain exceptional specialisations of the parameters, three further transitive subgroups of S_6 can be obtained as Galois groups of trinomials over $\mathbb{Q}$:

EXAMPLE:

(a) $g_2(X, 2) = X^6 - 6X^5 + 2^6 5^5 3^{-3} 7^{-1}$ has the Galois group $G_{36} < G_{72}$.

(b) $g_3(X, 10) = X^6 - 6X^5 + 2^5 5^5 11^5 3^{-3} 7^{-2} 13^{-3}$ has the Galois group $G_{24}^2 \cong S_4$ (acting on the subgroups of type Z_4).

(c) $g_2(X, -2/7) = g_3(X, -15/7) = X^6 - 6X^5 + 2^6 3^6 11^5 7^{-6} 19^{-1}$ has the Galois group Z_6.

Finally I want to thank Priv. Doz. Dr. B. H. Matzat for the constant encouragement without which this work probably would not have been completed.

References

Malle, G., Matzat, B. H. (1985). Realisierung von Gruppen $PSL_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$. *Math. Ann.* **272,** 549–565.

Malle, G., Trinks, W. (1985). Zur Behandlung algebraischer Gleichungssysteme mit dem Computer. Preprint.

Matzat, B. H. (1984). Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe. *J. reine angew. Math.* **349,** 179–220.

Matzat, B. H. (1985). Zwei Aspekte konstruktiver Galoistheorie. *J. Algebra* **96,** 499–531.

Matzat, B. H., Zeh-Marschke, A. (1986). Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbb{Q}$. *J. Number Theory* **23,** 195–202.

Shih, K. (1974). On the construction of Galois extensions of function fields and number fields. *Math. Ann.* **207,** 99–120.

Sims, C. C. (1970). The primitive permutation groups of degree not exceeding 20. *Computational Problems in Abstract Algebra,* pp. 169–183. New York: Pergamon Press.