MATHEMATICS OF COMPUTATION
VOLUME 51, NUMBER 184
OCTOBER 1988, PAGES 761-768

Polynomials with Galois Groups $\mathrm{Aut}(M_{22})$, M_{22}, and $\mathrm{PSL}_3(\mathbb{F}_4) \cdot 2_2$ Over $\mathbb{Q}$

By Gunter Malle

Dedicated to Prof. Dr. H. W. Leopoldt on the occasion of his 60th birthday

Abstract. In this paper the construction of infinite families of polynomials with Galois groups $\mathrm{Aut}(M_{22})$, M_{22} and $\mathrm{PSL}_3(\mathbb{F}_4) \cdot 2$ over $\mathbb{Q}$ is achieved. The determination of these polynomials leads to a system of nonlinear algebraic equations in 22 unknowns. The solutions belonging to the Galois extensions with the desired Galois groups are computed with a p-modular version of the Buchberger algorithm. The application of this method, which is described in some detail, turns out to be feasible even for relatively large systems of nonlinear equations.

0. Introduction. Recently there has been a certain interest in the construction of polynomials having a given nonabelian simple group as Galois group. In [5] for example, the task of determining polynomials over $\mathbb{Q}(t)$ having a given nonsolvable group with a faithful primitive permutation representation of degree at most fifteen as Galois groups was completed. Of the sporadic simple groups, the Mathieu groups seem to be the easiest cases, owing to their small permutation representations. Hoyden and Matzat [3] gave polynomials having M_{24} and M_{23} (for the latter, see the remark in [8]) as Galois group over $\mathbb{Q}(t)(\sqrt{-23})$. Also in [2], polynomials with groups M_{24} and M_{23} over $\mathbb{Q}(t)(\sqrt{-7})$ were calculated. Matzat and Zeh [7], [8] published polynomials with Galois groups M_{12} and M_{11} over $\mathbb{Q}(t)$. As for the fifth Mathieu group, M_{22}, in [6, Bemerkung 8.5] the existence of a regular $\mathrm{Aut}(M_{22})$-extension of $\mathbb{Q}(y)$ for the ramification structure $\mathfrak{C}^* = (2B, 4C, 11A)^*$ was proved. Moreover, in Satz 8.6 the fixed field of M_{22} in this extension was recognized to be a rational function field $\mathbb{Q}(t)$.—Since a stem field of degree 22 (i.e., the fixed field in the extension of the stabilizer of a point in the permutation representation of degree 22) also is a rational function field, the method used in [2]–[7] to calculate a generating polynomial should be applicable to the $\mathrm{Aut}(M_{22})$-extension. In this paper, infinite families of polynomials with Galois groups $\mathrm{Aut}(M_{22})$, M_{22} and $\mathrm{PSL}_3(\mathbb{F}_4) \cdot 2_2$ are constructed. Considerable computational problems arise on the way, coming from a system of nonlinear equations in 22 unknows for which solutions have to be found in a certain number field. These are determined with a p-modular version of the Buchberger algorithm [10], showing the feasibility of this p-modular approach even for relatively large systems of nonlinear equations.

1. The Theoretical Solution. Let K be a stem field (see above) of degree 22 of the $\mathrm{Aut}(M_{22})$-extension $N/\mathbb{Q}(y)$ for $\mathfrak{C}^*$ whose existence was proved in [6]. The elements of the classes $2B, 4C, 11A$ have permutation types $(2)^7(1)^8, (4)^4(2)^3, (11)^2$,

Received July 15, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12F10, 12E10, 65H10.

respectively, in the permutation representation of degree 22 of $\mathrm{Aut}(M_{22})$. From this ramification behavior of $K/\mathbb{Q}(y)$ the genus of K can be calculated, using the Hurwitz relative genus formula, as

$$g(K) = 1 - 22 + \frac{1}{2}(7 + 15 + 20) = 0.$$

We can now choose the ramification of $K/\mathbb{Q}(y)$ to occur exactly in the numerator and denominator divisors of y and $y-1$. In $K\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(y)$, by Satz B in [4], one then has

$$\bar{\mathfrak{p}}_\infty = \overline{\mathfrak{P}}_\infty^{11}\overline{\mathfrak{P}}_0^{11}, \quad \bar{\mathfrak{p}}_0 = \overline{\mathfrak{P}}^2\overline{\mathfrak{Q}}, \quad \bar{\mathfrak{p}}_1 = \overline{\mathfrak{R}}^4\overline{\mathfrak{S}}^2, \tag{1}$$

with divisors of degrees $\partial(\overline{\mathfrak{Q}}) = 8$, $\partial(\overline{\mathfrak{P}}) = 7$, $\partial(\overline{\mathfrak{R}}) = 4$ and $\partial(\overline{\mathfrak{S}}) = 3$. The divisors $\overline{\mathfrak{P}}, \overline{\mathfrak{Q}}, \overline{\mathfrak{R}}$ and $\overline{\mathfrak{S}}$ are now already defined over $\mathbb{Q}$ and as the degree of $\overline{\mathfrak{P}}$ is odd, K is a rational function field. On the other hand, the normalizer $\mathcal{N}_G(Z_{11}) \cong 11.10$ of a Sylow 11-subgroup of $\mathrm{Aut}(M_{22})$ acts transitively on the 22 points, so we only know that the product $\overline{\mathfrak{P}}_\infty\overline{\mathfrak{P}}_0$ is defined over $\mathbb{Q}$.

PROPOSITION 1. *The prime divisors $\overline{\mathfrak{P}}_\infty$ and $\overline{\mathfrak{P}}_0$ are defined over $\mathbb{Q}(\sqrt{-11})$.*

Proof. Let $N^* = N(\sqrt{-11})$ and define $M^* = N^{*M_{22}}$ to be the fixed field of M_{22} in $N^*/\mathbb{Q}(y)(\sqrt{-11})$. Then according to [6, Satz 8.6], N^*/M^* has the ramification structure $\mathfrak{C}_1^* = (2A, 11A, 11B)^*$, and the ramified prime divisors are defined over $\mathbb{Q}(\sqrt{-11})$ by [6, Bemerkung 5.3]. The field KM^* is a stem field of N^*/M^* of degree 22, and in this extension the two divisors $\wp_2$ and $\wp_3$ of $\bar{\mathfrak{p}}_\infty$ are ramified as follows:

$$\wp_2 = \mathfrak{L}_3^{11}\mathfrak{L}_4^{11}, \qquad \wp_3 = \mathfrak{L}_5^{11}\mathfrak{L}_6^{11}.$$

This can be seen from the permutation types of elements of order eleven in M_{22}. The normalizer $\mathcal{N}_{M_{22}}(Z_{11}) \cong 11.5$ of a Sylow 11-subgroup has two orbits on the 22 points, consequently all the divisors $\mathfrak{L}_3, \mathfrak{L}_4, \mathfrak{L}_5$ and $\mathfrak{L}_6$ are already defined over $\mathbb{Q}(\sqrt{-11})$. Finally, the divisors $\overline{\mathfrak{P}}_\infty$ and $\overline{\mathfrak{P}}_0$ split in $\overline{K}M^*/\overline{K}$ as $\overline{\mathfrak{P}}_\infty\overline{\mathfrak{P}}_0 = \overline{\mathfrak{L}}_3 \cdot \overline{\mathfrak{L}}_4 \cdot \overline{\mathfrak{L}}_5 \cdot \overline{\mathfrak{L}}_6$, with the divisors $\mathfrak{L}_i$ of degree one on the right-hand side all defined over $\mathbb{Q}(\sqrt{-11})$. Thus the same is true for $\overline{\mathfrak{P}}_\infty$ and $\overline{\mathfrak{P}}_0$. □

Now let x be a generating function of $K^* = K(\sqrt{-11})$ over $\mathbb{Q}(\sqrt{-11})$ with $(x) = \mathfrak{P}_\infty^{-1}\mathfrak{P}_0$. As K^* is a rational function field, there exist monic polynomials $\overline{p}, \overline{q}, \overline{r}, \overline{s} \in \mathbb{Q}(\sqrt{-11})[x]$ with divisors

$$(\overline{p}(x)) = \frac{\mathfrak{P}}{\mathfrak{P}_\infty^7}, \quad (\overline{q}(x)) = \frac{\mathfrak{Q}}{\mathfrak{P}_\infty^8}, \quad (\overline{r}(x)) = \frac{\mathfrak{R}}{\mathfrak{P}_\infty^4}, \quad (\overline{s}(x)) = \frac{\mathfrak{S}}{\mathfrak{P}_\infty^3}.$$

From (1) the following equality of divisors is deduced:

$$(y) = \left(\frac{\overline{p}(x)^2\overline{q}(x)}{x^{11}}\right), \qquad (y-1) = \left(\frac{\overline{r}(x)^4\overline{s}(x)^2}{x^{11}}\right). \tag{2}$$

So there are constants $\eta, \eta' \in \mathbb{Q}(\sqrt{-11})$ such that

$$x^{11}y = \eta\overline{p}(x)^2\overline{q}(x), \qquad x^{11}(y-1) = \eta'\overline{r}(x)^4\overline{s}(x)^2.$$

Subtracting the second equation from the first, one gets a formal identity over the polynomial ring $\mathbb{Q}(\sqrt{-11})[x]$ (remember x is transcendental over $\mathbb{Q}$). Comparing the coefficients at x^{22}, one has $\eta = \eta'$ and

$$x^{11} = \eta(\overline{p}^2\overline{q} - \overline{r}^4\overline{s}^2). \tag{3}$$

A further simplification can be obtained by differentiating with respect to x and eliminating η from the two equations, yielding

$$11(\overline{p}^2\overline{q} - \overline{r}^4\overline{s}^2) = x(2\overline{p}\overline{p}'\overline{q} + \overline{p}^2\overline{q}' - 4\overline{r}^3\overline{r}'\overline{s}^2 - 2\overline{r}^4\overline{s}\overline{s}').$$

This can be rewritten as

$$\overline{p}(11\overline{p}\overline{q} - 2x\overline{p}'\overline{q} - x\overline{p}\overline{q}') = \overline{r}^3\overline{s}(11\overline{r}\overline{s} - 4x\overline{r}'\overline{s} - 2x\overline{r}\overline{s}').$$

By definition, $\overline{p}$ and $\overline{r}^3\overline{s}$ are prime to each other. This finally allows the splitting into the two equalities

$$\begin{aligned} 11\overline{p}(x) + 11\overline{r}(x)\overline{s}(x) - 4x\overline{r}(x)'\overline{s}(x) - 2x\overline{r}(x)\overline{s}(x)' = 0, \\ 11\overline{r}(x)^3\overline{s}(x) + 11\overline{p}(x)\overline{q}(x) - 2x\overline{p}(x)'\overline{q}(x) - x\overline{p}(x)\overline{q}(x)' = 0. \end{aligned} \tag{4}$$

Comparing the coefficients at the transcendental x leads to a nonlinear system of 22 equations in the 22 unknown coefficients of the monic polynomials $\overline{p}, \overline{q}, \overline{r}$ and $\overline{s}$. As x was fixed only up to constant multiples, we can finally choose the second-highest coefficient of $\overline{s}(x)$ to be equal to 3, say. (If this coefficient were equal to zero, we would get an imprimitive solution, i.e., an imprimitive Galois group.)

All that is left to be done is to find the common zeros of this system of equations, which is possible, say, by Buchberger's algorithm. So from a theoretical point of view, the problem is solved.

2. Solving the Nonlinear System of Equations. The nonlinear system of equations was first treated with the Buchberger algorithm [9]. But it turns out that the coefficients and the number of monomials in the intermediate polynomials grow too quickly to get through with this method over a global field. Here, as in other computational problems in number theory, a local version of the algorithm seems to be needed [10]. If p is a prime for which -11 is a square mod p, any solution of the original system in $\mathbb{Q}(\sqrt{-11})$ will correspond to a solution in the p-adic field $\mathbb{Q}_p$. Moreover, reducing mod p gives a solution in the finite field $\mathbb{F}_p$ if the solution was an integer in $\mathbb{Q}_p$. (This last restriction can be removed if one looks at the homogeneous form of the equations over $\mathbb{F}_p$, determining the 'solutions at infinity' as well.) But even over finite fields, the complexity of the polynomials is too large to compute a Gröbner basis by elimination. Instead, the following method was used: Ten of the unknowns occurred linearly in at least one of the equations and could be eliminated by substitution (namely all of the coefficients of $\overline{p}(x)$ and three of the coefficients of $\overline{q}(x)$). This left 12 equations in 11 unknowns. Then the system was reduced modulo the prime 23. (This is the smallest 'good' prime for the problem, i.e., the smallest prime $p \nmid |\mathrm{Aut}(M_{22})|$ with $(\frac{-11}{p}) = 1$.) Then some of the unknowns were chosen such that the system of equations obtained by specializing these unknowns to elements of $\mathbb{F}_{23}$ could be solved entirely. This was done for all possible specializations of those variables, thus giving all solutions of the system over $\mathbb{F}_{23}$. Exactly four solutions were found:

μ_5	μ_4	μ_3	μ_2	μ_1	ρ_3	ρ_2	ρ_1	ρ_0	σ_1	σ_0
8	11	2	9	11	3	1	10	12	1	19
22	20	22	13	15	13	12	5	3	7	18
15	0	22	4	4	3	9	9	4	14	1
9	0	8	12	15	5	6	7	12	8	17

with $\overline{q}(x) = \sum \mu_i x^i$, $\overline{r}(x) = \sum \rho_i x^i$ and $\overline{s}(x) = \sum \sigma_i x^i$. (The variables not figuring in the above table were eliminated before.) This step needed 23 hours and one minute computing time on a SUN 3/50 (Motorola 68020 CPU at 8 MHz). On a larger computer like a Siemens S7880 it should have taken about $6\frac{1}{2}$ hours.

Now there is a problem: by constructive Galois theory, only two of the solutions can belong to $\mathrm{Aut}(M_{22})$-polynomials, the other two must come from another permutation group of degree 22 having a $(2, 4, 11)$-system. But it is known that the factoring of a polynomial reduced modulo a prime gives possible cycle shapes of the Galois group. And indeed, we already know the reduction modulo the prime 23 of the polynomial we look for. By substituting different values (mod 23) for the indeterminate t in the reduced polynomial and looking at the factoring, we can exclude the last two solutions, because they lead to cycle types not contained in $\mathrm{Aut}(M_{22})$ (only in S_{22}). An application of Newton's method to the remaining solutions mod 23 should give approximations in $\mathbb{Q}_{23}$. It turns out that this is possible for both solutions (i.e., the Jacobian of the system is nonsingular), yielding the following approximations in $\mathbb{Z}_{23}$ (the 23-adic number $\sum_{i\geq 0} a_i p^i$ is given as $a_0, a_1 a_2 \ldots$):

μ_5	=	8,	19	1	0	22	7	20	5	14	9	1	18 ...
μ_4	=	11,	17	22	11	17	2	5	10	5	16	4	14 ...
μ_3	=	2,	11	7	2	9	1	4	2	18	2	5	3 ...
μ_2	=	9,	20	19	17	9	7	0	5	5	16	7	14 ...
μ_1	=	11,	3	18	1	20	22	4	14	6	20	18	10 ...
ρ_3	=	3,	8	21	6	7	16	12	17	4	0	4	8 ...
ρ_2	=	1,	7	20	16	15	8	6	18	6	7	5	21 ...
ρ_1	=	10,	1	7	18	21	21	4	4	12	6	9	11 ...
ρ_0	=	12,	12	15	0	0	22	3	20	8	10	20	16 ...
σ_1	=	1,	10	7	7	5	11	10	14	10	2	19	1 ...
σ_0	=	19,	13	2	16	8	4	21	0	1	19	0	5 ...

and

μ_5	=	22,	12	5	13	7	8	3	4	0	4	7	20 ...
μ_4	=	20,	16	3	16	10	2	8	11	13	14	3	6 ...
μ_3	=	22,	20	5	21	19	1	5	17	19	9	21	8 ...
μ_2	=	13,	21	19	3	20	7	8	16	14	16	0	16 ...
μ_1	=	15,	17	1	5	8	1	19	6	5	7	14	5 ...
ρ_3	=	13,	5	9	5	1	9	8	2	16	10	19	9 ...
ρ_2	=	12,	1	18	1	19	13	12	10	9	15	8	16 ...
ρ_1	=	5,	13	1	6	12	5	14	18	11	14	4	14 ...
ρ_0	=	3,	2	9	0	13	19	15	19	17	21	14	16 ...
σ_1	=	7,	3	11	22	16	17	10	19	20	0	5	5 ...
σ_0	=	18,	19	13	11	5	6	15	8	19	21	3	9 ...

The amount of time needed for this step is negligible in comparison with the time needed for finding the solutions mod 23. So we are left with two sets of 23-adic numbers (which must be contained in $\mathbb{Q}(\sqrt{-11}) \subset \mathbb{Q}_{23}$). How do we recognize the algebraic numbers? As the solutions must be conjugate over $\mathbb{Q}(\sqrt{-11})$, the sum of the two solutions for any of the variables must be a rational number. Rational

numbers can be detected by the method of continued fractions, as described in [10]. So we can 'guess': $\rho_3 + \rho_3' = 402/97$. One finds out that the values are easier to handle if one replaces x by a suitable multiple such that $\overline{s}(X) = X^3 + \frac{1}{2}(17 \pm 3\sqrt{-11})X^2 + \cdots$. Then with $\theta = \pm\sqrt{-11}$ the correct solutions are:

$$\begin{aligned}
\overline{p}(X) &= X^7 + \tfrac{1}{2}(19+5\theta)X^6 + \tfrac{1}{2}(9+19\theta)X^5 + \tfrac{1}{2}(29+5\theta)X^4 \\
&\quad - \tfrac{1}{2}(29-5\theta)X^3 - \tfrac{1}{2}(9-19\theta)X^2 - \tfrac{1}{2}(19-5\theta)X - 1, \\
\overline{q}(X) &= X^8 + (14+6\theta)X^7 + (-82+52\theta)X^6 + (-408-52\theta)X^5 + 1379X^4 \\
&\quad + (-408+52\theta)X^3 + (-82-52\theta)X^2 + (14-6\theta)X + 1, \\
\overline{r}(X) &= X^4 + (4+2\theta)X^3 - 5X^2 + (4-2\theta)X + 1, \\
\overline{s}(X) &= X^3 + \tfrac{1}{2}(17+3\theta)X^2 + \tfrac{1}{2}(17-3\theta)X + 1,
\end{aligned}$$

as is verified immediately by substituting the values into the original nonlinear equations for the coefficients.

THEOREM 1. *The polynomial* $\overline{p}(X)^2\overline{q}(X)+2^{22}yX^{11}$ *has Galois group* $\mathrm{Aut}(M_{22})$ *over* $\mathbb{Q}(\sqrt{-11})(y)$.

The only thing left to be calculated is the value of η, but this is easily found from (3).

3. Finding the Polynomial over $\mathbb{Q}$. The irrationality $\sqrt{-11}$ was introduced by working over the field of definition of $\overline{\mathfrak{P}}_\infty$ and $\overline{\mathfrak{P}}_0$. But the product of these two divisors is already defined over $\mathbb{Q}$. So to pass to a rational polynomial we have to choose a new generator $\overline{x}$ such that $\overline{\mathfrak{P}}_\infty \cdot \overline{\mathfrak{P}}_0$ is the divisor of the numerator of $\overline{x}^2 + 11$. This means that x has the form $\alpha\frac{\overline{x}-\theta}{\overline{x}+\theta}$ for some constant α. It turns out that all polynomials become rational after the substitution $X \mapsto \frac{\overline{X}-\theta}{\overline{X}+\theta}$. More precisely, one gets:

$$\begin{aligned}
&(\overline{X}+\theta)^7\overline{p}\left(\frac{\overline{X}-\theta}{\overline{X}+\theta}\right) \\
&\quad = \theta(29\overline{X}^7 - 165\overline{X}^6 - 539\overline{X}^5 + 363\overline{X}^4 - 12705\overline{X}^3 + 3993\overline{X}^2 - 35937\overline{X} - 49247) \\
&\quad =: \theta p(\overline{X}),
\end{aligned}$$

$$\begin{aligned}
(\overline{X}+\theta)^8\overline{q}\left(\frac{\overline{X}-\theta}{\overline{X}+\theta}\right) &= 429\overline{X}^8 + 3080\overline{X}^7 + 45012\overline{X}^6 - 45496\overline{X}^5 + 1216534\overline{X}^4 \\
&\quad - 1607848\overline{X}^3 + 10834340\overline{X}^2 - 8081832\overline{X} + 29355205 \\
&=: q(\overline{X}),
\end{aligned}$$

$$(\overline{X}+\theta)^4\overline{r}\left(\frac{\overline{X}-\theta}{\overline{X}+\theta}\right) = 5\overline{X}^4 + 88\overline{X}^3 - 242\overline{X}^2 + 968\overline{X} - 1331 =: r(\overline{X}),$$

$$(\overline{X}+\theta)^3\overline{s}\left(\frac{\overline{X}-\theta}{\overline{X}+\theta}\right) = 19\overline{X}^3 + 33\overline{X}^2 + 121\overline{X} + 363 =: s(\overline{X}).$$

The Galois group of the new polynomial has $\mathrm{Aut}(M_{22})$ as a subgroup. But as $\mathrm{Aut}(M_{22})$ is a complete group (i.e., it has no outer automorphisms), the Galois group of the transformed polynomial actually must be the same as the original one,

showing:

THEOREM 2. *The Galois group of the polynomial*

$$g(X,y) = 11p(X)^2q(X) - 2^{22}y(X^2+11)^{11}$$

over $\mathbb{Q}(y)$ *is isomorphic to* $\mathrm{Aut}(M_{22})$. *The polynomial* $g(X,\omega)$ *obtained by specializing* y *to* $\omega \equiv 2 \pmod{17\cdot 19}, \omega \in \mathbb{Z}$, *has the same Galois group* $\mathrm{Aut}(M_{22})$ *over* $\mathbb{Q}$.

Proof. Only the second statement about the specialization remains to be proved. The polynomial $g(X,2)$ has decomposition type $(14)(7)(1)$ modulo 17 and $(11)^2$ modulo 19 (i.e., it factors into irreducible polynomials of those degrees when reduced modulo the indicated primes). No proper subgroup of $\mathrm{Aut}(M_{22})$ contains elements of order 14 and 11. So we have $\mathrm{Gal}(g(X,2)) = \mathrm{Aut}(M_{22})$, and this holds true for all polynomials congruent to $g(X,2)$ as stated in the theorem. □

THEOREM 3. *The Galois group of the polynomial*

$$h(X,x) = \frac{p(X)^2q(X)(x^2+11)^{11} - p(x)^2q(x)(X^2+11)^{11}}{X-x}$$

over $\mathbb{Q}(x)$ *is isomorphic to* $\mathrm{PSL}_3(\mathbb{F}_4)\cdot 2_2$. *The polynomial* $h(X,\xi)$ *obtained by specializing* x *to* $\xi \equiv 2 \pmod{13\cdot 43}, \xi \in \mathbb{Z}$, *has the same Galois group* $\mathrm{PSL}_3(\mathbb{F}_4)\cdot 2_2$ *over* $\mathbb{Q}$.

Proof. The first part is just the fact that the stabilizer of a point in the permutation representation of degree 22 of $\mathrm{Aut}(M_{22})$, that is, the Galois group of $N/K = N/\mathbb{Q}(x)$, is isomorphic to $\mathrm{PSL}_3(\mathbb{F}_4)\cdot 2_2$. (The notation for that particular extension of $\mathrm{PSL}_3(\mathbb{F}_4)$ is taken from the Atlas [1].) For the second part one finds the decomposition types $(5)^4(1)$ modulo 13 and $(14)(7)$ modulo 43 of $h(X,2)$. Therefore, the Galois group of $h(X,2)$ must be the full group. Obviously, this remains true for the stated congruences for ξ. □

4. Descent to the Mathieu Group M_{22}. Let again M denote the fixed field of M_{22} in $N/\mathbb{Q}(y)$. Then $M/\mathbb{Q}(y)$ is an extension of degree two ramified at two places, whence M is a rational function field. The ramification behavior of the three original ramified prime divisors is given by

$$\mathfrak{p}_\infty = \wp, \quad \mathfrak{p}_0 = \wp_\infty^2, \quad \mathfrak{p}_1 = \wp_0^2,$$

with $\partial(\wp) = 2$. Here $\wp$ splits over $\mathbb{Q}(\sqrt{-11})$ into $\wp_2\cdot\wp_3$ (see Section 1). A generating function t of M can be chosen such that $(t) = \wp_\infty^{-1}\wp_0$, and we conclude

$$(y) = \left(\frac{1}{t^2+at+b}\right), \qquad (y-1) = \left(\frac{t^2}{t^2+at+b}\right).$$

By calculations similar to those in the second section this forces $a = 0$ and $y(t^2+b) = b$. As $\wp$ splits over $\mathbb{Q}(\sqrt{-11})$, the function t can be fixed by taking $b = 11$.

THEOREM 4. *The polynomial*

$$f(X,t) = 2^{22}(X^2+11)^{11} - (t^2+11)p(X)^2q(X)$$

has Galois group M_{22} over $\mathbb{Q}(t)$. The polynomial $f(X,\tau)$ obtained by specializing t to $\tau \equiv 1 \pmod{7 \cdot 31}, \tau \in \mathbb{Z}$, has the same Galois group M_{22} over $\mathbb{Q}$.

Proof. $f(X,1)$ has decomposition types $(11)^2$ modulo 7 and $(7)^3(1)$ modulo 31. But no proper subgroup of M_{22} has order divisible by 7 and 11, so the Galois group of $f(X,\tau)$ is M_{22} for all $\tau \equiv 1 \pmod{217}$. □

The stabilizer of a point in the permutation representation of degree 22 of $\mathrm{Aut}(M_{22})$ contains the simple group $\mathrm{PSL}_3(\mathbb{F}_4)$ as a subgroup of index two. It would be interesting to get this group as a Galois group over $\mathbb{Q}$ as well. From the ramification of $L := K \cdot M$ one readily calculates the genus $g(L) = 3$, and one has:

PROPOSITION 2. *The field $L = K \cdot M$ with $\mathrm{Gal}(N/L) = \mathrm{PSL}_3(\mathbb{F}_4)$ has genus three and is generated over K by a root T of the equation $e(x,T) = T^2 - q(x)$.*

To get Galois realizations of $\mathrm{PSL}_3(\mathbb{F}_4)$ over $\mathbb{Q}$, one has to find rational points on that curve of genus three. No such point was found by a first search.

The following number theoretical result might be of interest:

PROPOSITION 3. (a) *The Galois group of $q(X)$ over $\mathbb{Q}$ is isomorphic to $\mathrm{Hol}(E_8)$.* (b) *The Galois group of $p(X)$ over $\mathbb{Q}$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$.*

Proof. These groups originate from the fact that the centralizer of an element in the class $2B$ in $\mathrm{Aut}(M_{22})$ is isomorphic to $\mathrm{Hol}(E_8) \times Z_2$. This centralizer must contain the decomposition group at the prime divisor $\mathfrak{p}_0$. Both $\mathrm{Hol}(E_8)$ and $\mathrm{PSL}_2(\mathbb{F}_7)$ are factor groups of the decomposition group. The correct Galois group can be determined from the decomposition types of the polynomials reduced modulo some small primes. □

Acknowledgment. Thanks are due to W. Leister from the Department of Computer Science at the University of Karlsruhe for providing me with the necessary computer facilities and to the Deutsche Forschungsgemeinschaft for financial support.

Fachbereich 3 Mathematik
Technische Universität Berlin
Strasse des 17. Juni 135
D-1000 Berlin 12, West Germany

1. J. H. CONWAY, R. T. CURTIS, S. P. NORTON, R. A. PARKER & R. A. WILSON, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

2. F. HÄFNER, *Realisierung der Mathieugruppen M_{24} und M_{23} als Galoisgruppen*, Diplomarbeit, Universität Karlsruhe, 1987.

3. G. HOYDEN-SIEDERSLEBEN & B. H. MATZAT, "Realisierung sporadischer einfacher Gruppen als Galoisgruppen über Kreisteilungskörpen," *J. Algebra*, v. 101, 1986, pp. 273 285.

4. G. MALLE & B. H. MATZAT, "Realisierung von Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$," *Math. Ann.*, v. 272, 1985, pp. 549 565.

5. G. MALLE, "Polynomials for primitive nonsolvable permutation groups of degree $d \leq 15$," *J. Symb. Comput.*, v. 4, 1987, pp. 83 92.

6. B. H. MATZAT, "Zwei Aspekte konstruktiver Galoistheorie," *J. Algebra*, v. 96, 1985, pp. 499 531.

7. B. H. MATZAT & A. ZEH-MARSCHKE, "Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbb{Q}$," *J. Number Theory*, v. 23, 1986, pp. 195 202.

8. B. H. MATZAT & A. ZEH-MARSCHKE, "Polynome mit der Mathieugruppe M_{11} als Galoisgruppe über $\mathbb{Q}$," *J. Symb. Comput.*, v. 4, 1987, pp. 93–98.

9. W. TRINKS, "Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen," *J. Number Theory*, v. 10, 1978, pp. 475–488.

10. W. TRINKS, "On improving approximate results of Buchberger's algorithm by Newton's method," *ACM SIGSAM Bull.*, v. 18, 1984, pp. 7–11.