The complex polynomials $P(x)$ with $\text{Gal}(P(x) - t) \cong M_{23}$

Noam D. Elkies
The complex polynomials $P(x)$ with $\text{Gal}(P(x) - t) \cong M_{23}$

Noam D. Elkies

We find the polynomials $P \in \mathbb{C}[X]$ of degree 23 such that the Galois group of $P(x) - t$ over $\mathbb{C}(t)$ is the Mathieu group $M_{23}$. This completes the computation of polynomials $P$ for which the Galois group of $P(x) - t$ is among the exceptional groups listed by Müller.

1. Introduction

For $P \in \mathbb{C}[x]$ of degree $n > 0$, define $G_P$ to be the Galois group of $P(x) - t$ over $\mathbb{C}(t)$. Since $P(x) - t$ is irreducible, $G_P$ is a transitive subgroup of the symmetric group $S_n$. Generically, $G_P$ is all of $S_n$, but it can be as small as the cyclic or dihedral group for special choices such as $P = x^n$ or $P = T_n(x)$ (Chebyshev polynomial) respectively. If $P$ decomposes as $P(x) = P_1(P_2(x))$ with each $\deg(P_i) > 1$, then $G_P$ permutes the proper subsets $\{x : P_2(x) = u\}$ of the roots with $P_1(u) = t$, and is therefore imprimitive. The converse implication is shown in [8, Proposition 3.4]. Müller [12] determined all $G_P$ that can arise for indecomposable polynomials: they are the symmetric and alternating groups, the cyclic groups of prime order, the dihedral groups of order twice an odd prime, and twelve exceptional permutation groups with $n = 6, 7, \ldots, 23, 31$, the last two for the sporadic Mathieu group $M_{23}$ and the linear group $\text{GL}_5(\mathbb{Z}/2\mathbb{Z})$.

The proof uses covering-space methods and Riemann’s existence theorem, and thus does not yield explicit polynomials. But it is still a natural question to exhibit all $P$ that realize each possible group $G_P$, except for the cases of $A_n$ and $S_n$.

MSC2010: primary 12F12; secondary 20D08.

Keywords: Mathieu group $M_{23}$, Galois groups, Chebotarev density theorem.

In particular, $G_P = S_n$ if $dP/dx$ has $n - 1$ distinct roots at which $P$ takes distinct values; equivalently, if $\text{disc}_t(\text{disc}_x(P(x) - t)) \neq 0$. This sufficient (but far from necessary) condition was already noted by Hilbert ([10], see also [15, §4.4]); the formulation in terms of the discriminant of the discriminant is attributed to Davenport in [3, p. 422].
which occur in “many, not reasonably classifiable types” [12]. Say $P, Q \in \mathbb{C}[x]$ are equivalent if $Q(x) = L_1(P(L_2(x)))$ for some polynomials $L_1, L_2$ both of degree 1; then $G_P = G_Q$. Up to this equivalence, the cyclic and dihedral groups occur only for powers and Chebyshev polynomials respectively. Some of the exceptional groups were realized in [12], or earlier by Matzat [11]; most of the others were realized by Cassou-Noguès and Couveignes [4], leaving only $M_{23}$. Here we find the polynomials $P$ with $G_P \cong M_{23}$.

The main novelty here is not in the computation of $P$ but in the proof that $G_P \cong M_{23}$. The coefficients of $P$ were computed using a known $p$-adic method for finding polynomial identities by solving the equivalent system of nonlinear equations in the coefficients, though here the search for the initial approximation took several CPU-days. The difficulty was that these equations cannot distinguish between polynomials with Galois group $M_{23}$ and $A_{23}$, and there are four $M_{23}$-covers but numerous $A_{23}$-covers with the same cycle structure (with all the $A_{23}$-covers probably defined only over number fields of rather high degree). Once we found $P$ with coefficients in a quartic number field $F$, we quickly convinced ourselves that $G_P$ must be $M_{23}$ by factoring $P(x) - t_0$ mod $\lambda$ for many primes $\lambda$ of $F$ and choices of $t_0$ mod $\lambda$ at which $P(x) - t_0$ has distinct roots: in each case the degrees of the factors matched one of the 12 cycle structures of elements of $M_{23}$, out of the 632 that arise in $A_{23}$. Moreover, the fraction of $t_0$ values that yield each cycle structure was quite near to the fraction of elements of $M_{23}$ with that cycle structure, as promised by the Chebotarev density theorem for Galois extensions of function fields. (I later learned from Mark Watkins that Samir Siksek had independently used much the same technique to find $P$ and gather overwhelming evidence that $G_P \cong M_{23}$.)

Still this did not amount to a proof that $G_P \cong M_{23}$. However, if $G_P$ were actually $A_{23}$ then we would observe a very different distribution of cycle structures, which would contradict the Chebotarev theorem once the residue field of $\lambda$ got large enough. In our function-field setting such a calculation turns out to be feasible thanks to Weil’s proof of the Riemann hypothesis for curves over finite fields. We did this for a $\lambda$ whose residue field is prime of characteristic $l = 10^8 + 7$ (the smallest 9-digit prime, which happens to lie under a degree-1 prime of $F$). We showed that the resulting distribution of cycle structures implies that $G_P$ is not 5-transitive, which soon yields $G_P \cong M_{23}$ as desired.

The factorization of $10^8$ polynomials mod $\lambda$ was a somewhat extravagant computation (two days of CPU time in gp [13]). This is not the only way to prove that $G_P \cong M_{23}$; for example, one could do it also by numerically lifting monodromy generators to permutations of 23 preimages, as Granboulan did for the 24

\[2\text{Michael Zieve had already obtained but not published polynomials for a few of these cases, with groups } \text{PGL}_2(\mathbb{Z}/17\mathbb{Z}) (n = 8), \text{PGL}_2(\mathbb{F}_8) (n = 9, \text{ both classes}), \text{ and } M_{11} (n = 11) \text{; he also calculated that there are four } M_{23} \text{ polynomials up to equivalence, but was not able to exhibit such a polynomial.} \]
preimages of an $M_{24}$-cover [9]. Still our technique using Chebotarev plus Weil has some advantages over the monodromy computation: while our computation took rather long to run, it was very easy to code, whereas the monodromy calculation would require some careful estimates to guarantee that the precision was sufficient to obtain the correct permutations; and our technique works also for Galois groups of extensions in positive characteristic. This approach also raises the theoretical question of how large a residue field is necessary: perhaps it can be shown that the counts over a field of size much smaller than $10^8$ would have sufficed.

In the next section we exhibit $F$ and $P \in F[x]$ and give some details on its calculation. In the following section we report on the results of our computation mod $\lambda$, use them to prove that $G_P \not\cong A_{23}$, and deduce that a polynomial $P_1$ satisfies $G_{P_1} \cong M_{23}$ if and only if $P_1$ is equivalent to the image of our $P$ under one of the four embeddings of $F$ into $\mathbb{C}$.

2. Computation of $P$

Suppose $G_P \cong M_{23}$. By [12], the map $P : \mathbb{P}^1 \to \mathbb{P}^1$ is branched above only three points, with orders 23 (at $t = \infty$), 2, and 4. The group $M_{23}$ contains only one conjugacy class of order 2 and one of order 4. The corresponding monodromy generators $\gamma_2$ and $\gamma_4$ must have $\gamma_2 \gamma_4$ of order 23. Up to conjugation in $M_{23}$, there are four such pairs $(\gamma_2, \gamma_4)$, two for each of the two conjugacy classes of elements of order 23 in $M_{23}$, and in each case $\gamma_2$ and $\gamma_4$ generate $M_{23}$. Since $M_{23}$ is its own normalizer in $S_{23}$, we conclude that there are four equivalence classes of $M_{23}$ polynomials, each defined over a number field $F$ containing $\mathbb{Q}(\sqrt{-23})$ with degree 1 or 2. We eventually found that $F$ is the dihedral quartic field of discriminant $3 \cdot 23^3$ generated by a root of $g^4 + g^3 + 9g^2 - 10g + 8$, which indeed contains the square roots $\pm(2g^3 + 4g^2 + 16g - 7)/3$ of $-23$.

The permutations $\gamma_2$ and $\gamma_4$ of 23 objects have cycle structures $1^72^8$ and $1^32^24^4$. Thus $P$ is equivalent to a monic polynomial with two double and four quadruple roots. Then, if $\tau$ is the value of $P$ at its finite critical points other than zeros, we can write

$$P = P^2_2 P^3_3 P^4_4 = P_7 P_8^2 + \tau,$$

where the $P_i$ ($i = 2, 3, 4, 7, 8$) are pairwise coprime monic polynomials of degree $i$, and $\tau$ is a nonzero constant. It may seem that we have 10 coefficients to determine: the $2 + 3 + 4$ non-leading coefficients of $P_2, P_3, P_4$, together with $\tau$. We can reduce this to 8 variables using the remaining equivalences (translate $x$, and multiply $x$ by some nonzero $\mu$ and divide each $P_i$ by $\mu^i$). One further variable is eliminated using a familiar differentiation trick: $dP/dx$ has leading term $23x^{22}$ and is a

\footnote{The earliest published references I know of are [6; 2], but the trick must have been known and used long before that.}
multiple of $P_2P_4^3P_8$, so must equal $23P_2P_4^3P_8$; hence
\[ P_8 = \frac{1}{23} \frac{dP}{dx} \]  
\[ = \frac{1}{23} (2P_2'P_3P_4 + P_2P_3'P_4 + 4P_2P_3P_4'). \]  
(2)

Still the remaining nonlinear equations are too complicated to solve directly by

with techniques such as Gröbner bases, especially since they do not distinguish between

$M_{23}$- and $A_{23}$-covers.

Instead we use the following strategy. Suppose the solution is defined over a

number field $F$ with a prime $\pi$ of small residue field at which the cover $P : \mathbb{P}^1 \to \mathbb{P}^1$

has good reduction. We can then find our cover mod $\pi$ by exhaustive search. An

arbitrary lift to the $\pi$-adic numbers is then an approximate solution, which can be

improved by a multivariate Newton iteration. Once we have the solution to

high enough $\pi$-adic precision, we can recognize it as an $F$-rational point by lattice

reduction, and verify that it satisfies the equations exactly.

For a general system of nonlinear equations we could not know in advance

which $\pi$ satisfy the condition of good reduction. In our setting, we are seeking

a “Belyi map” (a cover of $\mathbb{P}^1$ ramified only above three points), so Beckmann’s

theorem [1] gives a sufficient condition: if the characteristic of the residue field of $\pi$
does not divide the order of the Galois group then the cover has good reduction

at $\pi$. But we do not know $F$ in advance, and thus do not know which residue fields
arise. We therefore tried small prime fields $\mathbb{Z}/p\mathbb{Z}$ in the hope that one would work.

But searches over $(\mathbb{Z}/p\mathbb{Z})^7$ became ever longer without finding the desired cover.

For example, a search mod 13 (the smallest prime not dividing $|M_{23}|$) found only

$P_2 = x^2 - 3x - 6, \quad P_3 = x^4 - 4x - 4, \quad P_4 = x^4 + 5x^2 - 5x - 1$

with $\tau = 5$; but the resulting $P = P_2^2P_3P_4^4$ cannot have Galois group $M_{23}$ because

there are $t_0 \neq 0, 5$ for which the factorization of $P - t_0$ mod 13 has degrees not

seen in any of the $M_{23}$ cycle structures — for instance, $P - 1$ has an irreducible

factor of degree 19. In retrospect we know there is no $M_{23}$ polynomial over $\mathbb{Z}/13\mathbb{Z}$,

because $F$ has no prime of degree 1 above 13 (even though 13 does split in the

quadratic subfield $\mathbb{Q}(\sqrt{-23})$).

To bring larger $p$ within reach, we applied the following refinement. For $j \geq 0$

and any $Q \in \mathbb{C}[x]$, denote by $c_j(Q)$ the $x^j$ coefficient of $Q$; for example $c_1(P_l) = 1$

for each $l = 2, 3, 4, 7, 8$. For any monic $P_2, P_3, P_4$, let $R$ be the remainder

when $P_{23}$ is divided by $P_8^2$, where $P_{23}$ and $P_8$ are defined by (1) and (2). Then $R$

has degree $\deg(P_8^2) - 1 = 15$ generically, but must vanish at the desired solution.

We noticed that if we hold all but $c_0(P_4)$ and $c_1(P_4)$ fixed then $c_{15}(R)$ and

$c_{14}(R)$ are polynomials of degree only 2 in $c_0(P_4)$ and of degree 3 in $c_1(P_4)$;

in fact, $c_{15}(R)$ and $c_{14}(R)$ have degrees 2 and 3 respectively in $(c_0(P_4), c_1(P_4))$
together. We could have solved the simultaneous equations $c_{15}(R) = c_{14}(R) = 0$ in
(c_0(P_4), c_1(P_4)), reducing the search from O(p^7) to O(p^5) but with quite a large O-constant. Instead we opted for the following strategy, which is still O(p^7) but with a much smaller constant. Having fixed all but c_0(P_4) and c_1(P_4), compute R at the 12 sample points with c_0(P_4) = 0, 1, 2 and c_1(P_4) = 0, 1, 2, 3, and then use the fact that both c_{15}(R) and c_{14}(R) are quadratic in c_0(P_4) and cubic in c_1(P_4) to recursively evaluate them at all other choices of c_0(P_4) and c_1(P_4). If both vanish, test whether \text{deg}(R) = 0. This way, instead of computing p^2 polynomial remainders we need on average only 13: twelve sample points, and one more for the expected number of solutions of c_{15}(R) = c_{14}(R) = 0.

We implemented this search in \text{gp} (which we used also for the earlier O(p^7) method), and finally succeeded at \( p = 29 \). We assumed that \( c_2(P_3) = 0 \), and that \( c_0(P_3) = c_1(P_3) \) if both \( c_0(P_3) \) and \( c_0(P_1) \) are nonzero; every choice of \( P_2, P_3, P_4 \) with \( c_0(P_3)c_1(P_3) \neq 0 \) is equivalent to exactly one satisfying these conditions. (One can also make a unique choice if \( c_0(P_3) = 0 \) or \( c_1(P_3) = 0 \), but here this was not necessary.) The search took 46 CPU-hours, compressed to less than five hours by running on 10 heads in parallel, which is an order of magnitude smaller than the time to compute some 29^7 polynomial remainders. The resulting list of solutions contained two for which every \( P(x) - t_0 \) has a factorization consistent with \( G_P \cong M_{23} \). One of these was

\[
P_2 = x^2 - x - 3, \quad P_3 = x^3 - 3x - 3, \quad P_4 = x^4 - 3x^3 - 11x^2 + 13x + 7
\]

with \( \tau = 5 \). Lifting to \( \mathbb{Z}/p^{128}\mathbb{Z} \) (while retaining the conditions \( c_2(P_3) = 0 \) and \( c_0(P_3) = c_1(P_3) \)) gave more than enough precision to identify all the coefficients as elements of the quartic field \( F = \mathbb{Q}[g]/(g^4 + g^3 + 9g^2 - 10g + 8) \).

These elements of \( F \) are quite complicated because of the normalization \( c_0(P_3) = c_1(P_3) \). Once we have found one choice of \( P_2, P_3, P_4 \in F[x] \) that works, we can find equivalent but simpler ones by removing this normalization and the spurious bad reduction that it entails. One reasonably simple choice we found (dropping also the condition that the \( P_i \) be monic) is as follows:

\[
P_2 = (8g^3 + 16g^2 - 20g + 20)x^2 - (7g^3 + 17g^2 - 7g + 76)x
\]

\[
-13g^3 + 25g^2 - 107g + 596;
\]

\[
P_3 = 8(31g^3 + 405g^2 - 459g + 333)x^3 + (941g^3 + 1303g^2 - 1853g + 1772)x
\]

\[
+ 85g^3 - 385g^2 + 395g - 220;
\]

\[
P_4 = 32(4g^3 - 69g^2 + 74g - 49)x^4 + 32(21g^3 + 53g^2 - 68g + 58)x^3
\]

\[
- 8(97g^3 + 95g^2 - 145g + 148)x^2 + 8(41g^3 - 89g^2 - g + 140)x
\]

\[
- 123g^3 + 391g^2 - 93g + 3228.
\]
With this choice,
\[ \tau = \frac{2^{38}3^{17}}{23^3} \left( 47323g^3 - 1084897g^2 + 7751g - 711002 \right), \]
the last factor having norm \(2^{27}3^{23}5^{10}\).

3. Proof of \( \text{Gal}(P(x) - t) \cong M_{23} \)

We chose the degree-1 prime \( \lambda \) of \( F \) above the rational prime \( l = 10^8 + 7 \) at which \( g \equiv 36436770 \mod l \). We reduced \( P \) mod \( \lambda \) to obtain a polynomial \( \bar{P} \) with coefficients in \( F_\lambda = \mathbb{Z}/l\mathbb{Z} \), and factored \( \bar{P} - t_0 \) for each of the \( l - 2 \) values of \( t_0 \mod l \) for which \( \bar{P} - t_0 \) has no repeated roots. In each case the degrees of the irreducible factors, and thus the cycle structure of the action of Frobenius at \( t = t_0 \), agreed with the cycle structure of one or two of the conjugacy classes of \( M_{23} \).

Table 1 lists the key information for each class or pair of classes \( c \subset M_{23} \), including the difference between the expected and the actual number of occurrences of \( c \)’s cycle structure. The agreement is quite close: the discrepancy never exceeds twice the square root of the expected value.

In particular, because each of the \( M_{23} \) cycle structures occurs (and \( G_P \subset A_{23} \) because \( \text{disc}_x(P(x) - t) \) is a square) we know that \( G_P \) is a transitive subgroup of \( A_{23} \) containing elements of order \( p \) for each of the prime factors \( p = 2, 3, 5, 7, 11, 23 \).

| ATLAS label | Cycle structure | \(|c|/|M_{23}|\) | Expected | Actual | \(\Delta\) |
|-------------|-----------------|----------------|----------|--------|--------|
| 1A          | \(1^{23}\)      | 1/|\(M_{23}\)| | 10       | 9      | -1     |
| 2A          | \(1^72^8\)      | 1/2688        | 37202    | 37235  | 33     |
| 3A          | \(1^53^6\)      | 1/180         | 555556   | 556547 | 991    |
| 4A          | \(1^32^24^4\)   | 1/32          | 3125000  | 3123317| -1683  |
| 5A          | \(1^35^4\)      | 1/15          | 6666667  | 6665816| -851   |
| 6A          | \(1^23^26^2\)   | 1/12          | 8333334  | 8329354| -3980  |
| 7A, 7B      | \(1^27^3\)      | 2/14          | 14285715 | 14290600| 4885   |
| 8A          | \(1^24^8^2\)    | 1/8           | 12500001 | 12493007| -6994  |
| 11A, 11B    | \(11^2\)        | 2/11          | 18181819 | 18185450| 3631   |
| 14A, 14B    | \(2714\)        | 2/14          | 14285715 | 14289505| 3790   |
| 15A, 15B    | \(3515\)        | 2/15          | 13333334 | 13331689| -1645  |
| 23A, 23B    | 23              | 2/23          | 8695653  | 8697476| 1823   |

Table 1. Data on conjugacy classes. For each class or pair of classes \( c \subset M_{23} \), we list the ATLAS label [5, p. 71], the cycle structure, the fraction \(|c|/|M_{23}|\), the integer nearest to \(|c|/|M_{23}|(l - 2)\) (which is the expected number of occurrences of this cycle structure), the actual number of times it appeared, and the difference between the actual and expected counts.
of \(|M_{23}| = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 10200960\). This shows that \(G_P\) is either \(M_{23}\) or \(A_{23}\).

One could try various strategies for deducing \(G_P \neq A_{23}\) from the counts in Table 1. The following approach was the one that worked most easily. We shall take \(C_0\) and \(C_1\) to be the projective \(t\)- and \(x\)-lines in the following general setup.

Suppose \(C_1/C_0\) is a degree-\(n\) covering of curves over some finite field \(F_\lambda\). Let \(\tilde{C}\) be the Galois closure, with Galois group \(G \subseteq S_n\). Assume that \(G\) is \(k\)-transitive. Let \(G_k\) be the stabilizer of a \(k\)-element set, so the action of \(G_k\) on that set gives a surjective homomorphism \(G_k \to S_k\) whose kernel is the \(k\)-point stabilizer; write \(C_k = \tilde{C}/G_k\), so \(C_k/C_0\) is a cover of degree \(\binom{n}{k}\). If the cover \(C_1/C_0\) is given by a polynomial \(Q\) of degree \(n\), then with finitely many exceptions a point of \(C_k\) corresponds to a degree-\(k\) factor of a specialization of \(Q\).

Let \(N_k\) be the number of \(F_\lambda\)-rational points of \(C_k\). For an unramified \(F_\lambda\)-rational point \(t_0\) on \(C_0\), let \(N_k(t_0)\) be the number of \(F_\lambda\)-rational points of \(C_k\) lying over \(t_0\).

We next express \(N_k(t_0)\) in terms of the Galois structure of the preimage of \(t_0\) in \(C_1\). Let \(\phi\) be the Frobenius permutation of the preimage of \(t_0\) in \(C_1\).

**Lemma.** Let \(c_1, c_2, \ldots, c_m\) (with \(\sum_{i=1}^{m} c_m = n\)) be the cycle lengths of \(\phi\). Then \(N_k(t_0)\) is the \(X^k\) coefficient of the polynomial \(\prod_{i=1}^{m} (1 + X_{c_i})\).

**Proof.** A \(k\)-element subset of the preimage of \(t_0\) yields a rational point of \(C_k\) if and only if it is taken to itself by \(\phi\); equivalently, if and only if it is the union of orbits of \(\phi\). Since these orbits have sizes \(c_i\), the expansion of \(\prod_{i=1}^{m} (1 + X_{c_i})\) yields a sum of \(2^m\) monomials, with each monomial \(X^k\) corresponding to a \(k\)-element subset. \(\square\)

We now take \(C_0\) and \(C_1\) to be the \(t\)- and \(x\)-lines. Then \(G = G_P\) by Beckmann’s criterion [1] (since \(l\) is too large to be a factor of \(|G|\) even if \(G = A_{23}\)). Using the entries in Table 1, we find for each \(k = 1, 2, \ldots, 22\) the sum of \(\prod_{i=1}^{m} (1 + X_{c_i})\) over the \(l - 2\) unramified points \(t_0\). The sum is invariant under \(k \leftrightarrow n - k\), so we need only tabulate up to \(k = 11\). In each case we write \(\sum_{t_0} N_k(t_0) = Al - B\) with \(A \in \mathbb{Z}\) minimizing \(|B|\); the results are given in Table 2.

In each case \(Al - B\) is a lower bound for \(N_k\), with the difference coming from the counts above the three ramified points. If \(G\) acts \(k\)-transitively then \(C_k\) is an

<table>
<thead>
<tr>
<th>(k)</th>
<th>(A)</th>
<th>(B)</th>
<th>(k)</th>
<th>(A)</th>
<th>(B)</th>
<th>(k)</th>
<th>(A)</th>
<th>(B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>10</td>
<td>5</td>
<td>2</td>
<td>10892</td>
<td>9</td>
<td>5</td>
<td>487620</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>6592</td>
<td>6</td>
<td>3</td>
<td>60120</td>
<td>10</td>
<td>5</td>
<td>742744</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>19784</td>
<td>7</td>
<td>4</td>
<td>109978</td>
<td>11</td>
<td>7</td>
<td>883854</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>2326</td>
<td>8</td>
<td>5</td>
<td>243430</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 2.** Integers \(A\) and \(B\) such that \(\sum_{t_0} N_k(t_0) = Al - B\), with \(|B|\) minimal.
irreducible curve, and then the Weil bound gives \( |N_k - (l + 1)| \leq 2l^{1/2} g(C_k) \). Table 2 suggests that this might happen for \( k \leq 4 \) but not for \( k = 5 \) (and indeed \( C_5 \) has two components, one for each of the orbits of the action of \( M_{23} \) on 5-element subsets). We next prove that \( G \) is not 5-transitive by bounding \( g(C_5) \). If \( G_P = A_{23} \) then \( C_k \) has genus at most

\[
1 + \frac{1}{2} \left( \frac{1}{2} - \frac{1}{2} - \frac{1}{4} - \frac{1}{23} \right) [C_k : C_0] = 1 + \frac{1}{2} \frac{19}{24} \left( \frac{23}{k} \right)
\]

by the Riemann-Hurwitz formula. For \( k = 5 \) this gives \( 27805/8 \), so \( g(C_5) < 3476 \). Therefore

\[
|N_5 - (l + 1)| < 2l^{1/2} \cdot 3476 < 7 \cdot 10^7.
\]

But the \( k = 5 \) row of Table 2 gives

\[
N_5 - (l + 1) > l - 10893 > 9 \cdot 10^7,
\]

even without including the preimages of the ramified points. The conflict between inequalities (3) and (4) refutes the hypothesis that \( G_P = A_{23} \) and completes the proof that \( G_P \cong M_{23} \).

Acknowledgments

I thank Michael Zieve for telling me of the remaining \( M_{23} \) case in Müller’s list, and of the earlier work of himself and of Cassou-Noguès and Couveignes on the other groups. I also thank: the referee, for a careful reading resulting in several local corrections and improvements; John Voight, for the reference [2]; Mark Watkins, for apprising me of Siksek’s independent work on this problem; and Watkins, Voight, and Zieve also for other helpful correspondence on this and similar problems.

This research was supported in part by NSF grants DMS-0501029 and DMS-1100511.

References


**Noam D. Elkies**: elkies@math.harvard.edu

*Department of Mathematics, Harvard University, Cambridge, MA 02138, United States*
Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography. This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS

1 Deterministic elliptic curve primality proving for a special sequence of numbers — Alexander Abatzoglou, Alice Silverberg, Andrew V. Sutherland, and Angela Wong

2 Imaginary quadratic fields with isomorphic abelian Galois groups — Athanasios Angelakis and Peter Stevenhagen

41 Iterated Coleman integration for hyperelliptic curves — Jennifer S. Balakrishnan

63 Finding ECM-friendly curves through a study of Galois properties — Razvan Barbulescu, Joppe W. Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter L. Montgomery

113 Improved techniques for computing the ideal class group and a system of fundamental units in number fields — Jean-François Biasse and Claus Fieker

135 Conditionally bounding analytic ranks of elliptic curves — Jonathan W. Bober


167 Finding simultaneous Diophantine approximations with prescribed quality — Wieb Bosma and Ionica Smeets

187 Success and challenges in determining the rational points on curves — Nils Bruin

213 Solving quadratic equations in dimension 5 or more without factoring — Pierre Castel

235 Counting value sets: algorithm and complexity — Qi Cheng, Joshua E. Hill, and Daqing Wan

249 Haberland’s formula and numerical computation of Petersson scalar products — Henri Cohen

271 Approximate common divisors via lattices — Henry Cohn and Nadia Heninger

295 Explicit descent in the Picard group of a cyclic cover of the projective line — Brendan Creutz

317 Computing equations of curves with many points — Virgile Ducet and Claus Fieker

335 Computing the unit group, class group, and compact representations in algebraic function fields — Kirsten Eisenträger and Sean Hallgren

359 The complex polynomials $P(x)$ with $\text{Gal}(P(x) - 1) \cong M_{23}$ — Noam D. Elkies

369 Experiments with the transcendental Brauer-Manin obstruction — Andreas-Stephan Elsenhans and Jörg Jahnel

395 Explicit 5-descent on elliptic curves — Tom Fisher

413 On the density of abelian surfaces with Tate-Shafarevich group of order five times a square — Stefan Keil and Remke Kloosterman

437 Improved CRT algorithm for class polynomials in genus 2 — Kristin E. Lauter and Damien Robert

463 Fast computation of isomorphisms of hyperelliptic curves and explicit Galois descent — Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling

487 Elliptic factors in Jacobians of hyperelliptic curves with certain automorphism groups — Jennifer Paulhus

507 Isogeny volcanoes — Andrew V. Sutherland

531 On the evaluation of modular polynomials — Andrew V. Sutherland

557 Constructing and tabulating dihedral function fields — Colin Weir, Renate Scheidler, and Everett W. Howe