Computational Verification of M_{11} and M_{12} as Galois Groups over Q

Henri Darmon
Department of Mathematics
Harvard University
Cambridge, Massachusetts 02138
U.S.A.

David Ford
Department of Computer Science
Concordia University
Montreal, Quebec H3G 1M8
Canada

1. The Theory

For $n = 11$ and $n = 12$ we exhibit $f(x) \in \mathbf{Z}[x]$ monic, irreducible of degree n, which can be seen by the standard techniques of [1] to have $M_n \subseteq \mathrm{Gal}_{\mathbb{Q}} f \subseteq A_n$. We prove $\mathrm{Gal}_{\mathbb{Q}} f = M_n$ by demonstrating that $\mathrm{Gal}_{\mathbb{Q}} f$ is not transitive on sets of roots taken $n-6$ at a time. The example polynomials are derived from [5].

We assume the prime p has been chosen so that $f(x)$ has n distinct p-adic integer roots. We let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ in $\mathbf{Z}_p$, $\beta_1, \ldots, \beta_n$ the roots of $f(x)$ in $\mathbf{C}$, and R_n a complete set of coset representatives of M_n in A_n.

We define

$$F(x_1, \ldots x_n) = \sum_{\theta} \prod_{j \in \theta} x_j,$$

the subscripts in each term being taken from a distinct $(n-6)$-tuple θ of the Steiner system $S(n-7, n-6, n)$. By definition, $F(x_1, \ldots x_n)$ is fixed by any $\sigma \in M_n$. We assume the values of $\sigma F(\alpha_1, \ldots, \alpha_n)$ are known to be distinct as σ ranges over R_n. Then $\mathrm{Gal}_{\mathbb{Q}} f \neq A_n$ if and only if there is a labelling of the roots for which $F(\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}$.

We define

$$g(x) = \prod_{\sigma \in R_n} (x - \sigma F(\alpha_1, \ldots, \alpha_n)) = \prod_{\sigma \in R_n} (x - \sigma F(\beta_1, \ldots, \beta_n)) \in \mathbf{Z}[x].$$

It is enough to show that $g(v) = 0$ for some $v \in \mathbf{Z}$. Taking B an upper bound on the absolute values of the conjugates of $F(\beta_1, \ldots, \beta_n)$, $h = |R_n|$, and k sufficiently large, we have

$$|g(v)| \leq (|v| + B)^h < p^k.$$

If we can produce a labelling of the roots for which

$$F(\alpha_1, \ldots, \alpha_n) \equiv v \pmod{p^k} \tag{1}$$

it will follow that $g(v) \equiv 0 \pmod{p^k}$, so that $g(v) = 0$, and the proof will be complete.

2. The Method

The value of v is discovered by examination of the values of $\sigma F(\beta_1, \ldots, \beta_n)$, $\sigma \in R_n$, using sufficiently precise approximations of $\beta_1, \ldots, \beta_n$.

By testing whether $f(x)$ divides $x^p - x$ mod p we discover the smallest prime modulus p for which $f(x)$ has n distinct roots. It follows that $f(x)$ has n distinct roots $\alpha_1, \ldots, \alpha_n$ in $\mathbf{Z}_p$.

We confirm that $\sigma F(\alpha_1, \ldots, \alpha_n)$ assumes distinct values mod p^2 for $\sigma \in R_n$ (the values are *not* distinct mod p). In the process we discover a "correct" labelling of the roots, so that $F(\alpha_1, \ldots, \alpha_n) \equiv v \pmod{p^2}$.

When the roots are correctly labelled we apply Hensel lifting to obtain sufficiently precise rational integer approximations of the p-adic integer roots so that (1) can be confirmed.

The search for the splitting prime p and the enumeration of the distinct values of

$$\sigma F(\alpha_1, \ldots, \alpha_n) \pmod{p^2}$$

were programmed in PASCAL and VAX MACRO assembler. The Hensel lifting was done by a program in the ALGEB language (see [2]). All computations were performed on a VAX 8550 computer at the Computer Centre of Concordia University.

3. An example for M_{11}

The Steiner system $S(4,5,11)$ is described in [3], from which we take

$$\begin{aligned} f(x) = x^{11} &+ 101x^{10} + 4151x^9 + 87851x^8 + 976826x^7 + 4621826x^6 \\ &- 5948674x^5 - 113111674x^4 - 12236299x^3 + 1119536201x^2 \\ &- 1660753125x - 332150625. \end{aligned}$$

We find:

$$h = 2520; \quad v = -688814; \quad B = 111000000; \quad p = 37061; \quad k = 4439.$$

A correct labelling of the p-adic integer roots is given by

$$\begin{array}{llll} \alpha_1 \equiv 3562 & \alpha_4 \equiv 6490 & \alpha_7 \equiv 9100 & \alpha_{10} \equiv 15236 \\ \alpha_2 \equiv 3891 & \alpha_5 \equiv -17375 & \alpha_8 \equiv -5956 & \alpha_{11} \equiv 7030 \\ \alpha_3 \equiv 4847 & \alpha_6 \equiv -18529 & \alpha_9 \equiv -8397 & \end{array}$$

The Hensel lifting for this example required 7 hours, 32 minutes of CPU time.

4. An example for M_{12}

The Steiner system $S(5,6,12)$ is described in [4], from which we take

$$\begin{aligned} f(x) = x^{12} &+ 100x^{11} + 4050x^{10} + 83700x^9 + 888975x^8 + 3645000x^7 \\ &- 10570500x^6 - 107163000x^5 + 100875375x^4 + 1131772500x^3 \\ &- 329614375x^2 + 1328602500x + 332150625. \end{aligned}$$

We find:

$$h = 2520; \quad v = -7508700; \quad B = 2843000000; \quad p = 1044479; \quad k = 3959.$$

A correct labelling of the p-adic integer roots is given by

$$\begin{array}{llll} \alpha_1 \equiv -480839 & \alpha_4 \equiv -199074 & \alpha_7 \equiv 216720 & \alpha_{10} \equiv 394385 \\ \alpha_2 \equiv -319442 & \alpha_5 \equiv -116833 & \alpha_8 \equiv 392842 & \alpha_{11} \equiv -100630 \\ \alpha_3 \equiv -292338 & \alpha_6 \equiv {-54522} & \alpha_9 \equiv 425417 & \alpha_{12} \equiv 134214 \end{array}$$

The Hensel lifting for this example required 14 hours, 12 minutes of CPU time.

References

1. D. W. Erbach, J. Fischer, & J. McKay. Polynomials with PSL(2,7) as Galois Group. *Journal of Number Theory 11* (1979), 69–75.
2. D. Ford. On the Computation of the Maximal Order in a Dedekind Domain. Ph.D. Dissertation, Ohio State University (1978).
3. D. Ford & J. McKay. From Polynomials to Galois Groups. *Lecture Notes in Computer Science 204* (1985), 535–536. Proc. Eurocal '85 (Linz).
4. D. Ford & J. McKay. Computation of Galois Groups from Polynomials over the Rationals. In *COMPUTER ALGEBRA,* D. Chudnovsky & R. Jenks, editors, pp. 145–150. Marcel Dekker, New York (1988).
5. B. H. Matzat & A. Zeh-Marschke. Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über **Q**. *Journal of Number Theory 23* (1986), 195–202.