A Polynomial with Galois Group $\mathrm{SL}_2(11)$

JÜRGEN KLÜNERS

Universität Heidelberg, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany

We compute a polynomial with Galois group $\mathrm{SL}_2(11)$ over $\mathbb{Q}$. Furthermore we prove that $\mathrm{SL}_2(11)$ is the Galois group of a regular extension of $\mathbb{Q}(t)$.

1. Introduction

One way to construct a polynomial which has $\mathrm{SL}_2(11)$ as Galois group is to take a polynomial with Galois group $\mathrm{PSL}_2(11)$ and to solve the following embedding problem:

$$1 \to C_2 \to \mathrm{SL}_2(11) \to \mathrm{PSL}_2(11) \to 1.$$

This is a central embedding problem. Let $N/\mathbb{Q}$ be a normal extension with Galois group $\mathrm{PSL}_2(11)$. Since all elements of order 2 in $\mathrm{PSL}_2(11)$ lift to elements of order 4 in $\mathrm{SL}_2(11)$ a necessary condition for the solvabilty of this problem is that N is totally real. But this is not the only obstruction to the embedding problem. Böge (1990) has proved the following result, which is based on Serre's criterion (Serre, 1992, chapter 9).

THEOREM 1.1. *Let $N/\mathbb{Q}$ be a normal extension with Galois group $\mathrm{PSL}_2(l)$, where l is a prime number with $l \equiv 3 \bmod 8$ or $l \equiv 5 \bmod 8$. N is embeddable into an $\mathrm{SL}_2(l)$ extension over $\mathbb{Q}$ if and only if the following holds:*

(i) N is totally real.
(ii) For all odd prime numbers p with even ramification order we have: p has odd inertia degree if and only if $p \equiv 1 \bmod 4$.

2. Realization of $\mathrm{SL}_2(11)$

Using Theorem 1.1 it is easy to decide whether the given embedding problem is solvable or not. Malle (2000) has computed a $\mathrm{PSL}_2(11)$ polynomial of degree 11 over $\mathbb{Q}(a,t)$ with four ramification points with respect to t. Specializing a and t in a suitable way he gets the following totally real polynomial with Galois group $\mathrm{PSL}_2(11)$:
$f(x) = x^{11} - 4x^{10} - 25x^9 + 81x^8 + 237x^7 - 562x^6 - 1010x^5 + 1574x^4 + 1805x^3 - 1586x^2 - 847x + 579$.

Denote by L the stem field of f. Some computations with KASH (Daberkow *et al.*, 1997) show that the field discriminant of L is 74843^4 (where 74843 is prime). Denote by $\mathcal{O}_L$ the maximal order of L. The prime ideal factorization of (74843) equals

$$74843\mathcal{O}_L = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3^2\mathfrak{p}_4^2\mathfrak{p}_5,$$

where the inertia degrees of $\mathfrak{p}_4$ and $\mathfrak{p}_5$ are 2. The other inertia degrees are 1. In the splitting field N of $L/\mathbb{Q}$ no wild ramification can occur. Therefore all prime ideals of $\mathcal{O}_N$ lying over 74843 have ramification order 2 and inertia degree 2. Using Theorem 1.1, $N/\mathbb{Q}$ is embeddable into an $\mathrm{SL}_2(11)$ extension because $74843 \equiv 3 \bmod 4$.

Malle remarks that specializing $a = -5$ in his $\mathrm{PSL}_2(11)$-polynomial we get totally real specializations for $-716550 \leq t \leq -715599$. Specializing $a = -5$ we get:

$$g(t,x) := x^{11} - 74x^{10} + 1979x^9 - 22442x^8 + 93623x^7 - 68118x^6 + (t + 204139)x^5 + (-2t - 183370)x^4 + (t + 485462)x^3 - 2273900x^2 + 2760000x - 1000000.$$

The Galois group of g is $\mathrm{PSL}_2(11)$ and the branch cycle type description is $(2^4, 2^4, 2^4, 6 \cdot 3 \cdot 2)$, where all ramification points are real. Specializing $t = -715599$ or $t = -715600$ we get that the corresponding extension over $\mathbb{Q}$ is not embeddable into an $\mathrm{SL}_2(11)$ extension. For $t = -715601$ we get an extension which is only ramified in $p = 18496478981$ which is congruent 1 modulo 4. The corresponding prime ideal factorization yields that the inertia degree is 3 and the ramification degree is 2. Therefore this $\mathrm{PSL}_2(11)$-extension is embeddable into an $\mathrm{SL}_2(11)$ extension over $\mathbb{Q}$.

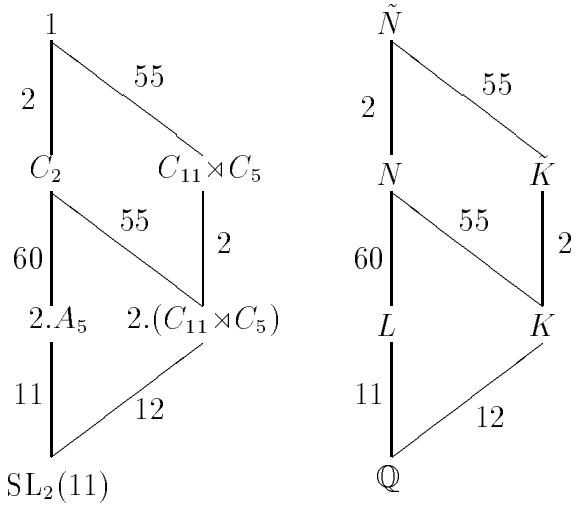
Since this embedding problem is a Brauer embedding problem and the number of ramified places is four, a result of Mestre (1994a) is applicable. This result has previously been applied to prove that $\mathrm{SL}_2(7)$ and $\mathrm{Aut}(M_{12})$ are Galois groups of regular extensions of $\mathbb{Q}(t)$ (Mestre, 1994b).

THEOREM 2.1. *$\mathrm{SL}_2(11)$ is a Galois group of a regular extension of $\mathbb{Q}(t)$.*

PROOF. The polynomial $g \in \mathbb{Q}(t)[x]$ is ramified in four places. We know that for one specialization the embedding problem is solvable. Therefore Theorem 2 of Mestre (1994a) is applicable, which states that there is a nonconstant rational function R of degree at most 8 such that the splitting field of $g(R(t), x)$ is embeddable into a regular $\mathrm{SL}_2(11)$ extension. □

3. The explicit construction

The Galois correspondence give the following diagram.



It remains to construct an explicit polynomial with Galois group $\mathrm{SL}_2(11)$. The smallest permutation representation of $\mathrm{SL}_2(11)$ is on 24 points. Denote this permutation group by G. The group G is imprimitive and has one non trivial block system with 12 blocks of size 2. Suppose we have an irreducible polynomial $\tilde{h} \in \mathbb{Q}[x]$ with $\mathrm{Gal}(\tilde{h}) = G$. Denote the stem field of $\tilde{h}$ by $\tilde{K}$. Then $\tilde{K}$ has one non trivial subfield K, which is of degree 12 and the Galois closure of K has Galois group $\mathrm{PSL}_2(11)$. The first step of the construction is to compute this field of degree 12, which can be done using the methods in Klüners and Malle (2000). Here we use the polynomial f and get the following polynomial as output:

$$\begin{aligned} h(x) := {} & x^{12} + 4x^{11} - 202x^{10} - 750x^9 + 14320x^8 + 57987x^7 - 420190x^6 - 2051347x^5 + \\ & 3470883x^4 + 27131426x^3 + 31354680x^2 + 1044099x - 6047919. \end{aligned}$$

Denote the stem field of h by K. Now we know that there exists an extension $\tilde{K} = K(\sqrt{\alpha})$ such that the splitting field of $\tilde{K}/\mathbb{Q}$ has Galois group $\mathrm{SL}_2(11)$. Since all elements of order 2 lift to elements of order 4, $\tilde{K}/K$ must be ramified in all of the ramified places of K. We want to look at those fields using class field theory. Assuming the generalized Riemann hypothesis (GRH) we are able to compute the class group of K. The class number is 5. We have the following prime ideal factorization:

$$74843\mathcal{O}_K = \mathfrak{P}_1^2\mathfrak{P}_2^2\mathfrak{P}_3^2.$$

All these prime ideals have inertia degree 2. Our first try is to compute the ray class group of $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$. Again, assuming GRH, we get that this ray class group is isomorphic to $C_5 \times C_{74842}$. Therefore there is a degree 2 extension, which is unramified outside $\{\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3\}$. We compute the conductor for this degree 2 extension and get that it equals $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$. Therefore this extension has the necessary properties, i.e. $\mathfrak{P}_1, \mathfrak{P}_2$, and $\mathfrak{P}_3$ are ramified in $\tilde{K}/K$. Using an algorithm of Fieker (2000) we compute this class field within a few minutes. Using reduction techniques based on the LLL algorithm (Lenstra *et al.*, 1982) we compute polynomials with smaller coefficients. The minimal polynomial of a primitive element over $\mathbb{Q}$ is

$$\begin{aligned} \tilde{h}(x) := {} & x^{24} - 224529x^{22} + 19626678634x^{20} - 856039761758776x^{18} + \\ & 19958084192689643991x^{16} - 252111992625681301495895x^{14} + \\ & 17541348715566511264209511113x^{12} - 664841471049673108949324536980 6x^{10} + \\ & 12991363853437959637044033680663051x^8 - \\ & 11401964598726978574279395625113924700x^6 + \\ & 32488962978549390891575601248550162700 80x^4 - \\ & 63286637850643001254855317664195057742 89x^2 + \\ & 22244433870746354272505452155294510342 4. \end{aligned}$$

4. Computing the Galois group of $\tilde{h}$

We now have a candidate for an $\mathrm{SL}_2(11)$ polynomial. Let $\tilde{K}$ be the stem field of $\tilde{h}$.

THEOREM 4.1. *The Galois group* $\mathrm{Gal}(\tilde{h})$ *is isomorphic to* $\mathrm{SL}_2(11)$.

PROOF. It is easy to see that $\tilde{K}$ has a subfield of degree 12. Using the subfield algorithm (Klüners, 1998) we get that this subfield is the only non trivial one. For a degree 12 field we compute the Galois group (Geißler and Klüners, 2000), which is $\mathrm{PSL}_2(11)$. From the subfield structure we know that $\mathrm{Gal}(\tilde{h})$ is a transitive subgroup of the wreath product $C_2 \wr \mathrm{PSL}_2(11) \cong C_2^{12} \rtimes \mathrm{PSL}_2(11)$.

Denote this wreath product by G_1. In the following we say that a group has the desired block structure, if there is only one non trivial block system and the action of the group on the blocks is isomorphic to $\mathrm{PSL}_2(11)$. Using MAGMA we compute up to conjugacy all maximal transitive subgroups of G_1 having the desired block structure. There is only one subgroup G_2 with this property. We get that $G_2 \cong C_2^{11} \rtimes \mathrm{PSL}_2(11)$. We repeat this process with G_2 and get two maximal non conjugate (in G_2) subgroups of G_2 with the desired block structure. We denote these groups by G_3 and G_4. Repeating this process with G_3 and G_4 we get that there are no transitive subgroups with the desired properties. We detect that G_3 and G_4 are conjugate in S_{24}. Both groups are isomorphic to $\mathrm{SL}_2(11)$.

Now we need an invariant which distinguishes $\mathrm{SL}_2(11)$ from the other groups. Denote by H_i the point stabilizer (of 1) in G_i $(1 \leq i \leq 4)$. The H_i are acting on $\Omega = \{1, \ldots, 24\}$. If we write Ω as a disjoint union of orbits of H_i $(1 \leq i \leq 4)$ we get three orbits of length 1,1,22 for H_1 and H_2. For H_3 and H_4 we get four orbits of lenght $1, 1, 11, 11$. It is well known that these orbit lenghts correspond to the degrees of the irreducible factors of $\tilde{h} \in \tilde{K}[x]$. Therefore $\mathrm{Gal}(\tilde{h}) \cong \mathrm{SL}_2(11)$ if and only if $\tilde{h}$ has four factors in $\tilde{K}[x]$. By computing the minimal polynomial of a zero of $\tilde{h}$ over K we get a degree 2 factor $\hat{h}$ of $\tilde{h}$. Therefore we have to factor the polynomial $\tilde{h}/\hat{h} \in \tilde{K}[x]$. Using KASH we get that the latter polynomial has two factors of degree 11. This proves that $\mathrm{Gal}(\tilde{h}) \cong \mathrm{SL}_2(11)$. □

Since our embedding problem is a central one we know that we can give all solutions, if we know one. Let $\tilde{K} = K(\sqrt{\alpha})$, then all solutions are given by $K(\sqrt{r\alpha})$, where $r \in \mathbb{Q}^\times$. Note that $\tilde{h}$ is an even polynomial, i.e. $\tilde{h}(x) = \bar{h}(x^2)$ with $\bar{h} \in \mathbb{Z}[x]$.

COROLLARY 4.1. *Let $\tilde{h}_t := \bar{h}(t \cdot x^2)$. The Galois group of $\tilde{h}_t$ over $\mathbb{Q}(t)$ is isomorphic to $\mathrm{SL}_2(11)$. The Galois group of $\tilde{h}_t$ over $\mathbb{C}(t)$ is isomorphic to C_2.*

PROOF. The proof is immediate from the fact that all extensions of the form $K(\sqrt{r\alpha})$ are solutions of the embedding problem. □

References

Böge, S. (1990). Witt-Invariante und ein gewisses Einbettungsproblem. *J. reine angew. Math.*, **410**:153–159.

Daberkow, M., Fieker, C., Klüners, J., Pohst, M., Roegner, K., Wildanger, K. (1997). KANT V4. *J. Symb. Comput.*, **24**(3):267–283.

Fieker, C. (2000). Computing class fields via the Artin map. to appear in Math.Comput.

Geißler, K., Klüners, J. (2000). Galois group computation of polynomials of degree up to 15. *J. Symb. Comput.*. same issue.

Klüners, J. (1998). On computing subfields - a detailed description of the algorithm. *Journal de Théorie des Nombres de Bordeaux*, **10**:243–271.

Klüners, J., Malle, G. (2000). Explicit Galois realization of transitive groups up to degree 15. *J. Symb. Comput.*. same issue.

Lenstra, A. K., Lenstra Jr., H. W., Lovász, L. (1982). Factoring polynomials with rational coefficients. *Math.Ann.*, **261**:515–534.

Malle, G. (2000). Some multi-parameter polynomials with given Galois group. *J. Symb. Comput.*. same issue.

Mestre, J. (1994a). Annulation, par changement de variable, d'éléments de $Br_2(k(x))$ ayant quatre poles. *C.R.Acad.Sci.Paris*, **319**:529–532.

Mestre, J. (1994b). Construction d'extensions régulières de $\mathbb{Q}(t)$ à groupes de Galois $SL_2(F_7)$ et $\tilde{M}_{12}$. *C.R.Acad.Sci.Paris*, **319**:781–782.

Serre, J.-P. (1992). *Topics in Galois Theory.* Research Notes in Mathematics. Jones and Bartlett Publishers.