THE ADMISSIBILITY OF M_{11} OVER NUMBER FIELDS

JOACHIM KÖNIG AND DANNY NEFTIN

Abstract. A group G is $\mathbb{Q}$-admissible if there exists a G-crossed product division algebra over $\mathbb{Q}$. The $\mathbb{Q}$-admissibility conjecture asserts that every group with metacyclic Sylow subgroups is $\mathbb{Q}$-admissible. We prove that the Mathieu group M_{11} is $\mathbb{Q}$-admissible, in contrast to any other sporadic group.

1. Introduction and statement of the main result

A finite dimensional division algebra D over its center k is *a G-crossed product* if it admits a maximal subfield L that is Galois over k with $\mathrm{Gal}(L|k) \cong G$. A G-crossed product division algebra is equipped with an explicit structure, which has a key role in the theory of division algebras, cf. [20, Chapter 14-19]. A classical problem originating in [23] is to understand for which groups G there exists a G-crossed product division algebra with center k. Such groups G are said to be *k-admissible.* A Galois extension $L|k$ with Galois group G such that L is a maximal subfield of a G-crossed product division algebra is called *adequate.*

For $k = \mathbb{Q}$, it is known that every $\mathbb{Q}$-admissible group G has metacyclic Sylow subgroups [23]. The converse of this statement is known as the long standing open *$\mathbb{Q}$-admissibility* conjecture, cf. [2, Problem 11.2]. The conjecture is proved for solvable groups G by Sonn in a series of papers [25, 4, 26], which moreover show that such groups G are *strongly $\mathbb{Q}$-admissible.* That is for every $m \in \mathbb{N}$, there exists an adequate Galois extension $L|k$ with Galois group G such that $L \cap \mathbb{Q}(\mu_m) = \mathbb{Q}$. Moreover, the conjecture is reduced in [4] to proving the strong $\mathbb{Q}$-admissibility of an explicit list of five families of groups. The last family in this list is the Mathieu group M_{11}, the only sporadic group whose Sylow subgroups are metacyclic.

Analogues and generalisations of the $\mathbb{Q}$-admissibility conjecture were proved over various fields, including over fields such as $\mathbb{C}((x))(t)$ by Harbater–Hartmann–Krashen [8], $\mathbb{C}((x,y))$ by Neftin-Paran [16], and $\mathbb{Q}_p(t)$ by Surendranath–Suresh [27]. Over number fields, the conjecture was further generalized and studied in the works of Liedahl [19], and the second author and Vishne [17], [15, Question 1.2]. These suggest that every group whose Sylow subgroups are metacyclic and furthermore admit a certain presentation depending only on the maximal abelian subextension $k_{ab}|\mathbb{Q}$ in $k|\mathbb{Q}$, is k-admissible *infinitely often* in the sense of [1], that is, there exist infinitely many linearly disjoint adequate Galois extensions $L|k$ with Galois group G. In the case $G = M_{11}$, this amounts to G being k-admissible infinitely often over every number field k that does not contain any of the fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-1})$.

We prove this strong form of admissibility for $G = M_{11}$ over the following fields:

Theorem 1. *Let k be a number field in which at least one of the primes 2 and 11 splits completely. Then M_{11} is infinitely often k-admissible.*

Date: February 9, 2017.

Key words and phrases. Galois theory; admissibility.

Via Schacher's criterion (Theorem 3), the admissibilty of $G = M_{11}$ reduces to realizing G infinitely often as a Galois group of an extension $L|k$ such that the noncyclic Sylow subgroups of M_{11} (the generalized dihedral group and $C_3 \times C_3$) are contained in a decomposition group over at least two primes of k. To do so, we apply Hilbert's irreducibility theorem, weak approximation, and a specialization result of Beckmann which connects the inertia group of primes of $\mathbb{Q}(t)$ in a regular extension $E|\mathbb{Q}(t)$ with inertia groups of primes of $\mathbb{Q}$ in a specialization $E_a|\mathbb{Q}$, for $t = a$. The combination of these results gives us (infinitely many linearly disjoint) specializations of a regular Galois extension $E|\mathbb{Q}(t)$ with Galois group M_{11} which satisfy Schacher's criterion.

The group M_{11} has been realized as a Galois group of a regular Galois extension of $\mathbb{Q}(t)$ in several different ways. Explicit polynomials can be found in [11, Chapter I, Cor. 9.11], [10, Cor. 10.2]. However, we were unable to obtain specializations of these polynomials with the required decomposition groups, since their inertia subgroups over $\mathbb{Q}(t)$ are not well-suited for applying the above methods; in particular, none of them has order divisible by 3. We use the recently constructed genus 0 polynomial from [9, Thm. 5], which admits both geometric inertia groups of order 4 and of order 3. We find specializations of it with inertia groups of order divisible by 8, and decomposition groups of order divisible by 16 and 9, as necessary for Schacher's critertion.

This research was supported by the Israel Science Foundation (grant No. 577/15).

2. Preliminaries and notation

2.1.1. *Dedekind domains.* The following facts about primes in Dedekind domains are well known, c.f. [24]. Let K be the fraction field of a Dedekind domain O, and $\mathfrak{p}$ a prime of O. Denote the *residue field* at $\mathfrak{p}$ by $K_\mathfrak{p} := O/\mathfrak{p}$, and the *completion* of K at $\mathfrak{p}$ by $\hat{K}_\mathfrak{p}$. For a Galois extension $L|K$, the completions $\hat{L}_{\mathfrak{P}_i}$ (resp. residue fields $L_{\mathfrak{P}_i}$) are Galois (resp. normal) over $\hat{K}_\mathfrak{p}$ (resp. $K_\mathfrak{p}$) and are isomorphic $\hat{L}_{\mathfrak{P}_1} \cong \hat{L}_{\mathfrak{P}_2}$ (resp. $L_{\mathfrak{P}_1} \cong L_{\mathfrak{P}_2}$), for every two primes $\mathfrak{P}_i$, $i = 1, 2$ of L lying over $\mathfrak{p}$. Put $\hat{L}_\mathfrak{p} := \hat{L}_\mathfrak{P}$ (resp. $L_\mathfrak{p} := L_\mathfrak{P}$), which up to isomorphism are independent of the choice of a prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$. The *decomposition groups* $D(\mathfrak{P}_i|\mathfrak{p}) := \{\sigma \in \mathrm{Gal}(L|K) \,|\, \sigma(\mathfrak{P}_i) \subseteq \mathfrak{P}_i\}$ are conjugate for every two primes $\mathfrak{P}_i$, $i = 1, 2$ of L lying over $\mathfrak{p}$. Put $D_\mathfrak{p} := D(\mathfrak{P}|\mathfrak{p})$ for some prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$. The restriction map $D_\mathfrak{p} \rightarrow \mathrm{Gal}(L_\mathfrak{p}|K_\mathfrak{p})$ is then surjective and its kernel is the *inertia group* $I_\mathfrak{p}$ at $\mathfrak{p}$. The prime $\mathfrak{p}$ *ramifies* in $L|K$ if $I_\mathfrak{p} \neq 0$, otherwise *unramified.*

Let $f \in K[X]$ be a polynomial and L its splitting field. The polynomial f is called *integral* at $\mathfrak{p}$ if it is an element of $O_\mathfrak{p}[X]$ whose leading coefficient is a unit, where $O_\mathfrak{p}$ denotes the localization at $\mathfrak{p}$. For such f, the reduction $\overline{f} := f \pmod{\mathfrak{p}}$ is defined, of degree $\deg f$, and its roots $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$ are contained in $L_\mathfrak{p}$. Furthermore:

Lemma 2. *Let K be the fraction field of a Dedekind domain O, and $\mathfrak{p} \lhd O$ a prime. Let $f \in O[X]$ be a monic polynomial with splitting field L such that $D(f) \notin \mathfrak{p}$. Then the splitting field of $\overline{f}$ is $L_\mathfrak{p}$.*

Proof. Let $O_\mathfrak{P}$ be the valuation ring of a prime $\mathfrak{P}$ lying over $\mathfrak{p}$. Let $\alpha_1, \ldots, \alpha_n$ denote the roots of f in L. The residue of $D(f) \cdot O_\mathfrak{P}$ mod $\mathfrak{P}$ is contained in the $K_\mathfrak{p}$-vector space A generated by $\overline{\alpha}_1, \ldots, \overline{\alpha}_n$. As $D(f)$ is invertible mod $\mathfrak{p}$, the entire field $L_\mathfrak{p} = O_\mathfrak{P}/\mathfrak{P}$ is contained in A. □

A polynomial $f(x) := \sum_{i=0}^{n} a_i X^i \in O[X]$ such that $a_j \in \mathfrak{p}$ for $j = 0, \ldots, n-1$, $a_0 \notin \mathfrak{p}^2$, and $a_n \notin \mathfrak{p}$, is called an *Eisenstein polynomial.* Such a polynomial is irreducible over K, and moreover the completion at $\mathfrak{p}$ of $K(\alpha)|K$, where α is a root of f, is of degree $[\hat{K}(\alpha)_\mathfrak{P} : \hat{K}_\mathfrak{p}] = n$, for a (unique) prime $\mathfrak{P}$ over $\mathfrak{p}$ [24, Chapter I, Proposition 17].

2.1.2. *Number fields and admissibility.* For a number field k, we say that $\mathfrak{p}$ is a prime of k if it is a prime ideal of the ring of integers of k. The following criterion then reduces the problem of determining whether a group is admissible to a realization problem with local constraints:

Theorem 3. *(Schacher* [23]*) Let $L|k$ be a Galois extension of number fields with Galois group G. Then L is k-adequate if and only if for every prime p dividing $|G|$, there are at least two primes $\mathfrak{q}_i$ of k such that the decomposition group $D_{\mathfrak{q}_i}$ contains a p-Sylow subgroup of G, for $i = 1, 2$.*

We note that by Chebotarev density theorem there are infinitely many primes $\mathfrak{q}$ of a number field k such that $D_{\mathfrak{q}}$ is isomorphic to any prescribed cyclic subgroup of $\mathrm{Gal}(L|k)$. It therefore suffices to verify Schacher's criterion for primes p such that the p-Sylow subgroup of G is noncyclic. The noncyclic Sylow subgroups of M_{11} are $C_3 \times C_3$ and the semidihedral group $SD_{16} \cong C_8 \rtimes C_2$.

For a Galois extension of number fields $L|k$ and a prime $\mathfrak{p}$ of k, the ramification of $\mathfrak{p}$ in $L|k$ is *tame* if the characteristic of $L_{\mathfrak{p}}$ is prime to $|I_{\mathfrak{p}}|$. In this case, $I_{\mathfrak{p}}$ is known to be cyclic of order dividing the cardinality $|L_{\mathfrak{p}}^{\times}|$ of the multiplicative group of the residue field [24, Chapter IV, Corollary 1].

2.1.3. *Function fields and specializations.* Let $k(t)$ be the rational function field over a number field k and $E|k(t)$ a finite Galois extension. These are also fraction fields of Dedekind domains. The extension $E|k(t)$ is *regular* if k is algebraically closed in E. Denote the place corresponding to the ideal $(t-a) \lhd k[t]$ by $t \to a$, and the place corresponding to $(1/t) \lhd k[1/t]$ by $t \to \infty$. For brevity, denote the residue field $E_{(t-a)}$ by E_a, the inertia group $I_{(t-a)}$ in $E|k(t)$ by I_a, and say a is a *branch point* if $I_a \neq 0$, for $a \in k \cup \{\infty\}$.

The following theorem and proposition are the key to finding the desired specializations in Theorem 1. Denote by $\mathrm{ord}_{\mathfrak{p}}(a)$ the multiplicity of $\mathfrak{p}$ in the factorization of the fractional ideal (a), for $a \in k$.

Theorem 4. *(Beckmann* [3, Theorem 1.2]*) Let k be a number field and $E|k(t)$ a regular Galois extension with Galois group G. Then for all but finitely many primes $\mathfrak{p}$ of k, the following holds: If $a \in k$ is not a branch point of $E|k(t)$ and $e := \mathrm{ord}_{\mathfrak{p}}(a-b) > 0$ for some branch point $b \in k$, then the inertia group $I_{\mathfrak{p}}$ in the specialization $E_a|k$ is conjugate in G to $\langle \tau^e \rangle$, where $I_b = \langle \tau \rangle$.*

Theorem 4 follows from [3] by increasing the finite set of exceptional primes to ensure that $\mathrm{ord}_{\mathfrak{p}}(b) \geq 0$ for all branch points $b \in k$. In case the latter condition does not hold at $\mathfrak{p}$, the theorem can still be applied but with a differently defined exponent e.

Proposition 5. *(*[21, Prop. 2.1]*) Let k be a number field, and $E|k(t)$ be a finite regular Galois extension with Galois group G. Let S be a finite set of primes of k. For each $\mathfrak{p} \in S$, choose $t_{\mathfrak{p}} \in k$ and let $E(\mathfrak{p})$ denote the completion at $\mathfrak{p}$ of $E_{t_{\mathfrak{p}}}$. Then there exists $t_0 \in k$ such that $E_{t_0}|k$ has Galois group G and its completion at $\mathfrak{p}$ is isomorphic to $E(\mathfrak{p})|\hat{k}_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$.*

2.1.4. *Genus* 0 *extensions.* Let k be a field and $k(t)$ the rational function field over k. For a separable polynomial $f \in k(t)[X]$, let $\mathrm{Gal}(f|k(t))$ be the Galois group of the splitting field E of f over $k(t)$. Then $\mathrm{Gal}(f|k(t))$ is a permutation group on n letters via its action on the roots of f in E. Moreover, it is transitive if and only if f is irreducible. We focus on polynomials of the form $f(t,X) = f_1(X) - tf_2(X)$ which correspond to (rational) genus 0 extensions and make use of the following lemma to ensure 2-transitivity.

Lemma 6. *Assume $f_1, f_2 \in k[X]$ are such that $f(t,X) := f_1(X) - tf_2(X) \in k(t)[X]$ is a separable polynomial. Then* $\mathrm{Gal}(f|k(t))$ *is* 2*-transitive if the following* 2*-variable polynomial is* *irreducible:*

$$F_f(X,Y) := \frac{f_1(X)f_2(Y) - f_2(X)f_1(Y)}{X - Y} \in k[X,Y].$$

Proof. By [13, Lemma 9.24], $f \in k(t)[X]$ is irreducible, so $G := \mathrm{Gal}(f|k(t))$ is transitive on the set S of roots of f. Let $y \in S$, so that $f_1(y)/f_2(y) = t$. Then $H := \mathrm{Gal}(f|k(y))$ is the stabilizer of $y \in S$ under the G-action. Since $F_f(X,Y) \in k[X,Y]$ is irreducible, $F_f(X,y) \in k(y)[X]$ is irreducible by Gauss's lemma. Since $F_f(X,y) = f_2(y)\cdot f(t,X)/(X-y)$, we get that $f(t,X)/(X-y) \in k(y)[X]$ is irreducible. Hence H acts transitively on $S \setminus \{y\}$ and G is 2-transitive. □

The following statement describes the ramification in rational genus 0 extensions and is well known, cf. [14, Lemma 3.1]. Let $\tilde{k}$ denote the algebraic closure of k. We write $\tilde{k} \cup \{\infty\}$ for the projective line over $\tilde{k}$, so that a rational function $u \in \tilde{k}(x)$ defines a map $u : \tilde{k} \cup \{\infty\} \to \tilde{k} \cup \{\infty\}$. If $u(\infty) = \alpha \in \tilde{k}$ then the multiplicity of ∞ is defined as $\deg u_2 - \deg u_1$, where u_1, u_2 are the numerator and denumerator of $u(X) - \alpha \in \tilde{k}(X)$. If $u(\infty) = \infty$ then the multiplicity of ∞ is its multiplicity in $(1/u)^{-1}(0)$.

Lemma 7. *Assume $f(t,X) := f_1(X) - tf_2(X) \in k(t)[X]$ is separable, and L the splitting field of f over $k(t)$. For $\alpha \in \tilde{k} \cup \{\infty\}$, denote by $m_1, \ldots, m_r$ the multiplicities of the elements in $(\frac{f_1}{f_2})^{-1}(\alpha) \subseteq \tilde{k} \cup \{\infty\}$. Then the orbits of the (cyclic) inertia group I_α in $L|k(t)$ on the roots of $f(t,X)$ are of length $m_1, \ldots, m_r$.*

Proof. Let x be a root of $f(t,X) \in \tilde{k}(t)[X]$, and $\alpha_i \in \tilde{k} \cup \{\infty\}$ the preimages in $(\frac{f_1}{f_2})^{-1}(\alpha)$ with multiplicity m_i, $i = 1, \ldots, r$. Then the places $x \to \alpha_1, \ldots, x \to \alpha_r$ lie over $t \to \alpha$ and have ramification indices $m_1, \ldots, m_r$, respectively. The ramification indices over $t \to \alpha$ then correspond to the lengths of orbits of I_α, e.g. by [11, Thm. I.9.1]. □

3. Polynomials with regular Galois group M_{11}

We begin with proving that the polynomials in [9, Thm. 5] have Galois group M_{11}.

Proposition 8. *Let*

$$f_1(X) := (77X^3 + 10989X^2 + 129816X + 496368)^3(77X^2 + 2376X + 15472), \quad \textit{and}$$
$$f_2(X) := (11X^2 - 1296)^4(11X^2 + 143X + 621) \in \mathbb{Q}[X].$$

Furthermore, let

$$g_1(X) := (X^2 + 6X + 91/11)^3(X^3 - 3/4X^2 - 285/22X + 951/44), \quad \textit{and}$$
$$g_2(X) := (X^2 + 2X - 89/11)^4(X^2 + 5X + 113/22)^2.$$

Then the polynomials $f(t,X) := f_1(X) - tf_2(X)$ and $g(t,X) := g_1(X) - tg_2(X) \in \mathbb{Q}(t)[X]$ have Galois group M_{11} over $\mathbb{Q}(t)$.

Proof. In the rational function field $\mathbb{Q}(x)$, let $w := w(x) := (-9x^2 - 30x + 44)/(x^2 - 11)$ and $t := f_1(w)/f_2(w)$. Then $t = \frac{h_1(x)}{h_2(x)}$ is a rational function of degree 22 with

$$\begin{aligned} h_1(x) = {} & 2^{12} \cdot 5^5 \cdot 13 \cdot (x^3 - \tfrac{11}{8}x^2 - \tfrac{11}{3}x - \tfrac{121}{9})^3(x^3 + \tfrac{21}{2}x^2 + \tfrac{154}{3}x + \tfrac{814}{9})^3 \cdot \\ & (x^2 - 88x - 264)(x^2 - \tfrac{44}{13}x - \tfrac{132}{13}), \text{ and} \\ h_2(x) = {} & 3^6 \cdot (x^2 - \tfrac{44}{3}x - \tfrac{616}{9})^4(x^2 - \tfrac{44}{9})^4(x^2 + \tfrac{11}{3}x + 11)^2(x^2 - 11). \end{aligned}$$

Let L be the Galois closure of $\mathbb{Q}(w)$ over $\mathbb{Q}(t)$, and let E be the Galois closure of $\mathbb{Q}(x)$ over $\mathbb{Q}(t)$. (In fact, the proof will show that $L = E$.) Let $G := \mathrm{Gal}(L|\mathbb{Q}(t)) = \mathrm{Gal}(f(t,X)|\mathbb{Q}(t))$, and let $H := \mathrm{Gal}(E|\mathbb{Q}(t)) = \mathrm{Gal}(h_1(X) - th_2(X)|\mathbb{Q}(t))$. As $[\mathbb{Q}(w) : \mathbb{Q}(t)] = 11$ and $[\mathbb{Q}(x) : \mathbb{Q}(t)] = 22$, G acts transitively on 11 points, and H acts transitively on 22 points, cf. Section 2.1.4.

Lemma 7 shows that G contains an element of order 4 (namely, an inertia group generator over $t \mapsto \infty$). The transitive groups of degree 11 are well-known, and the only ones containing an element of order 4 are M_{11}, A_{11} and S_{11}. To exclude the latter two groups, let $\widehat{g_2}(X) := \frac{11^3}{7^3.5^{10}}g_2(X)$ and let y be a root of $g_1 - t\widehat{g_2}$ over $\mathbb{Q}(t)$ (i.e. $t = g_1(y)/\widehat{g_2}(y)$).
A verification using Magma (cf. Remark 2) shows that $(g_1(X)\widehat{g_2}(y) - \widehat{g_2}(X)g_1(y))/(X - y)$ is irreducible over $\mathbb{Q}(y)$. Hence, $\hat{G} := \mathrm{Gal}(g_1(X) - t\widehat{g_2}(X)|\mathbb{Q}(t))$ is 2-transitive by Lemma 6, and in particular primitive. The point stabilizer of $\hat{G}$ is therefore a maximal subgroup, and hence $\mathbb{Q}(y)|\mathbb{Q}(t)$ has no proper intermediate fields. This means that either $\mathbb{Q}(y) \cap E$ is $\mathbb{Q}(t)$ or $\mathbb{Q}(y) \subset E$. We claim that the latter holds.

Set $p(X, y) := \widehat{g_2}(y)h_1(X) - g_1(y)h_2(X) = \widehat{g_2}(y) \cdot (h_1(X) - th_2(X)) \in \mathbb{Q}(y)[X]$. A straightforward verification using Magma shows that p is reducible over $\mathbb{Q}(y)$. More precisely, it factors into a product of two polynomials of degree 11 in X. In particular, $h_1(X) - th_2(X)$ is reducible over $\mathbb{Q}(y)$. This means that $\mathrm{Gal}(\mathbb{Q}(y)E|\mathbb{Q}(y))$ acts intransitively on the roots of $h_1(X) - th_2(X)$. Then however, $\mathrm{Gal}(E|\mathbb{Q}(y) \cap E)$ also acts intransitively on these roots, since the restriction of $\mathrm{Gal}(\mathbb{Q}(y)E|\mathbb{Q}(y))$ to E yields a permutation isomorphism of these two groups. This shows that $\mathbb{Q}(y) \cap E$ is strictly larger than $\mathbb{Q}(t)$. Since $\mathbb{Q}(y)/\mathbb{Q}(t)$ is minimal, we get $\mathbb{Q}(y) \subset E$. Furthermore, we obtain that H must have an intransitive subgroup U (in the degree 22 action on the roots of $h_1(X) - th_2(X)$) of index 12, namely the group fixing $\mathbb{Q}(y)$.

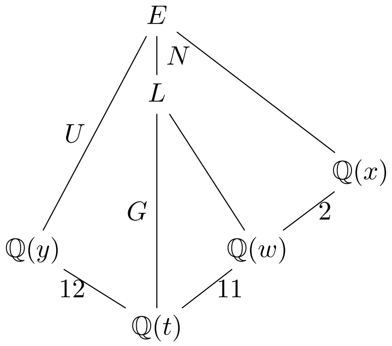

FIGURE 1. The tower of field extensions of $\mathbb{Q}(t)$

Now $N := \mathrm{Gal}(E|L)$ is a 2-group, as $E|L$ is generated by the Galois conjugates of $L(x)$, all of which are (Galois) of degree at most 2 over L. Therefore $|NU|$ equals $|U| \cdot 2^k$ with some $k \in \mathbb{N}_0$. In particular, the fixed field $\mathbb{Q}(y) \cap L$ of NU is strictly larger than $\mathbb{Q}(t)$, as $[\mathbb{Q}(y) : \mathbb{Q}(t)]$ is divisible by 3. Since $\mathbb{Q}(y)|\mathbb{Q}(t)$ is minimal, once more either $\mathbb{Q}(y) \cap L = \mathbb{Q}(y)$ or $\mathbb{Q}(y) \subseteq L$. Thus, G has a subgroup of index 12, and among our three candidate groups, only $G = M_{11}$ has this property. Therefore, M_{11} is the Galois group of f as well as of $g_1(X) - t\widehat{g_2}(X)$, and thus also of $g(t, X)$.

□

Remark 1.

(a) The main idea behind the above proof is that the field E^V is of genus 0 not only for the index 11 subgroup $V \leq M_{11}$, but also for the index 12 maximal subgroup $V \leq M_{11}$, and the index 22 nonmaximal subgroup $V \leq M_{11}$. The polynomials appearing in the proof arise from an explicit parameterization of the corresponding rational function fields.

(b) The general idea of using the reducibility of a variable separated equation to show that two polynomials have the same Galois closure, is in the spirit of Fried's result [7, Prop. 2].

(c) Let $2A, 3A, 4A$ be the unique conjugacy class of M_{11} of order $2, 3, 4$, respectively. The Galois extension $E|\mathbb{Q}(t)$ is obtained by descending a Galois extension of $\mathbb{C}(t)$ that has four branch points over which its inertia groups are $2A, 2A, 3A$, and $4A$.[1] In fact one can show that, up to equivalence of coverings, f is the *only* polynomial in the M_{11}-family of type $(2A, 2A, 3A, 4A)$ which is defined over $\mathbb{Q}$.
The reason is that the reduced Hurwitz space of this family is a genus-2 curve and (through explicit computations) turns out to be birationally equivalent to the hyperelliptic curve given by $y^2 = (x^2 - x + 3)(x^2 + 1)(x^2 + x + 1)$. For such curves, there are methods to explicitly determine, under a few assumptions, the complete set of rational points. Using Magma, we found that the Jacobian of the above curve is of rank 1, and Chabauty's method (as described e.g. in [12]) then yields that there are exactly four rational points; only one of these corresponds to a nondegenerate (i.e. 4 branch points) cover. See [9] for more details on the computation of such families, as well as [22] for general information on Hurwitz spaces.

4. Specializations with prescribed decomposition groups: Proof of Theorem 1

In this section, we prove Theorem 1. Let $f = f(t, X) \in \mathbb{Q}[t, X]$ be the polynomial from Proposition 8 and E its splitting field over $k(t)$. The proof of Theorem 1 is by finding specializations $f(t_0, X) \in \mathbb{Q}[X]$, $t_0 \in k$, such that the splitting field L of $f(t_0, X)$ satisfies Schacher's criterion. The following two lemmas give specializations $f(t_p, X)$, $t_p \in k$, the splitting field of which satisfies Schacher's criterion for each of the primes $p = 2, 3$ (but not necessarily simultaneously).

Lemma 9. *Assume that* $f_0(X) := 77X^3 + 10989X^2 + 129816X + 496368 \in k(t)[X]$ *is irreducible. There are infinitely many primes* $\mathfrak{p}$ *of* k *such that for all but finitely many* $t_0 \in k \setminus \{0\}$ *with* $\mathrm{ord}_{\mathfrak{p}}(t_0) > 0$ *and* $\mathrm{ord}_{\mathfrak{p}}(t_0) \neq 0$ *mod* 3*, the decomposition group of the splitting field of* $f(t_0, X)$ *over* $\mathfrak{p}$ *contains a* 3*-Sylow subgroup of* M_{11}*.*

Proof. For a prime $\mathfrak{p}$ of k, let $T_{\mathfrak{p}}$ be the set of $t_0 \in k \setminus \{0\}$ such that $\mathrm{ord}_{\mathfrak{p}}(t_0) > 0$, $\mathrm{ord}_{\mathfrak{p}}(t_0)$ is prime to 3, and t_0 is not a branch point of $E|k(t)$. By Lemma 2, the splitting field of $f(t_0, X) \in k[X]$ is E_{t_0}, for all $t_0 \in T_{\mathfrak{p}}$.

Let $\tau \in M_{11}$ be a generator of an inertia group over $t \to 0$, so that τ is of order 3 by Lemma 7. Since M_{11} is simple and $E|k(t)$ is nonconstant, it is a regular extension, so we can apply Theorem 4. By Theorem 4 with $t \to 0$, there is a set S_1 containing all but finitely many primes of k, such that the inertia subgroup $I_{\mathfrak{p}} \leq \mathrm{Gal}(E_{t_0}|\mathbb{Q})$ of a prime $\mathfrak{P}$ over $\mathfrak{p}$ is generated by a conjugate of $\tau^{ord_{\mathfrak{p}}(t_0)}$, for all $t_0 \in T_{\mathfrak{p}}$, $\mathfrak{p} \in S_1$. Since τ is of order 3, and $\mathrm{ord}_{\mathfrak{p}}(t_0)$ is prime to 3, we get $|I_{\mathfrak{p}}| = |\langle \tau^{ord_{\mathfrak{p}}(t_0)} \rangle| = 3$ for $t_0 \in T_{\mathfrak{p}}$, $\mathfrak{p} \in S_1$.

For $\mathfrak{p} \in S_1$, let $D_{\mathfrak{p}}$ be the decomposition group of $\mathfrak{P}$ in $E_{t_0}|k$, so that $|D_{\mathfrak{p}}/I_{\mathfrak{p}}| = [(E_{t_0})_{\mathfrak{P}} : k_{\mathfrak{p}}]$. We claim that there is an infinite set $S_2 \subseteq S_1$ such that $|D_{\mathfrak{p}}/I_{\mathfrak{p}}|$ is divisible by 3 for every $t_0 \in T_{\mathfrak{p}}$,

[1] The classes of the inertia groups follow immediately via factoring the corresponding specializations of $f(t, X)$ and applying Lemma 7.

$\mathfrak{p} \in S_2$. For each $\mathfrak{p} \in S_2$, we then have $|I_{\mathfrak{p}}| = 3$ and $3 \,|\, |D_{\mathfrak{p}}/I_{\mathfrak{p}}|$, so $9 \,|\, |D_{\mathfrak{p}}|$ and hence $D_{\mathfrak{p}}$ contains a 3-Sylow subgroup of M_{11}, proving the theorem.

To prove the claim, note that for all t_0 with $\operatorname{ord}_{\mathfrak{p}}(t_0) > 0$, we have

$$f(t_0, X) \equiv f(0, X) = (77X^3 + 10989X^2 + 129816X + 496368)^3(77X^2 + 2376X + 15472) \bmod \mathfrak{p}.$$

Since f is integral at the place $t{\to}0$, the splitting field F of $f_0 \in k[X]$ is contained in the residue extension $E_0|k$.

Let S_3 be the set of primes $\mathfrak{p}$ of k for which $f_{0,\mathfrak{p}} := f_0 \bmod \mathfrak{p}$ is separable, so that S_3 contains all but finitely many primes of k. By Lemma 2, the splitting field of $f_{0,\mathfrak{p}}$ is the residue field $F_{\mathfrak{p}}$, and hence contained in $(E_0)_{\mathfrak{p}}|k_{\mathfrak{p}}$, for all $\mathfrak{p} \in S_3$. Since $f(t_0, X) = f(0, X) \bmod \mathfrak{p}$, the same argument shows that the splitting field of $f(t_0, X) \bmod \mathfrak{p}$ is $F_{\mathfrak{p}}$ and hence contained in $(E_{t_0})_{\mathfrak{p}}|k_{\mathfrak{p}}$, for all $\mathfrak{p} \in S_3$, $t_0 \in T_{\mathfrak{p}}$.

By Chebotarev's density theorem, as f_0 is irreducible over $\mathbb{Q}$ and S_1, S_3 contain all but finitely many primes of k, there is an inifinite subset $S_2 \subseteq S_1 \cap S_3$ of primes $\mathfrak{p}$ such that f_0 remains irreducible mod $\mathfrak{p}$. Therefore 3 divides $[F_{\mathfrak{p}} : k_{\mathfrak{p}}]$ and hence also $[(E_{t_0})_{\mathfrak{p}} : k_{\mathfrak{p}}] = |D_{\mathfrak{p}}/I_{\mathfrak{p}}|$ for all $\mathfrak{p} \in S_2$, $t_0 \in T_{\mathfrak{p}}$, proving the claim, and hence the theorem. □

The above proof relies on the fact that inertia group at the place $t \mapsto 0$ has order 3, and that its index in the decomposition group is again divisible by 3. This method can and will be generalized in a more general context of Grunwald problems. However, this argument does not apply to the 2-Sylow subgroups of M_{11}, since $E|k(t)$ has no inertia group of order 8, and the 2-Sylow subgroups of M_{11} can only be written as metacyclic groups of the form $C_8.C_2$.

Lemma 10. *Let $p \in \{2, 11\}$ and assume p splits completely in k. There exists $t_0 \in k$ such that the decomposition groups of the splitting field L of $f_0(X) := f(t_0, X) \in k[X]$ over primes dividing p, are of order divisible by* 16.

Proof. Let $\mathfrak{p}$ be a prime of k over p. Since $\hat{k}_{\mathfrak{p}} \cong \hat{\mathbb{Q}}_p$, it suffices to show that the completions $\hat{L}_p|\hat{\mathbb{Q}}_p$ have degree divisible by 16. To do so, we factor the polynomial f_0 (multiplied by a suitable scalar, if necessary) mod p^k, with some fixed precision k. Assuming that this precision is sufficiently high, Hensel's lemma then yields that f_0 factors over $\hat{\mathbb{Q}}_p$ into polynomials of the same degrees as the mod p^k factors.

For $p = 2$, set $t_0 := 2$. One finds that f_0 factors into polynomials of degrees 8 and 3. This shows that $\operatorname{Gal}(\hat{L}_2|\hat{\mathbb{Q}}_2)$ is a subgroup of M_{11} with orbit lengths 8 and 3. A verification using Magma shows that there are only two classes of such subgroups in M_{11}, one of order 48 and one of order 24 isomorphic to $\mathrm{SL}_2(3)$.

To exclude the latter group, we replace X by $X + 1$, so that the second factor takes the form $u(X) := X^3 + a_2X^2 + a_1X + a_0$, with 2-adic valuation $\nu_2(a_i) = 1$ for all $i = 0, 1, 2$. Since the latter is an Eisenstein polynomial, its root field is a totally tamely ramified degree-3 extension of $\hat{\mathbb{Q}}_2$, cf. Section 2.1.1. Since $\hat{\mathbb{Q}}_2$ has no totally tamely ramified Galois extension of degree 3, the splitting field F of u is of degree $[F : \hat{\mathbb{Q}}_2] = 6$. If $\operatorname{Gal}(\hat{L}_2|\hat{\mathbb{Q}}_2) \cong \mathrm{SL}_2(3)$, then the degree 6 Galois subextension $F|\hat{\mathbb{Q}}_2$ yields a degree 6 quotient of $\mathrm{SL}_2(3)$. As $\mathrm{SL}_2(3)$ has no such quotient, we deduce that $|\operatorname{Gal}(\hat{L}_2|\hat{\mathbb{Q}}_2)| = 48$.

For $p = 11$, set $t_0 := 1/11^2$. Then f_0 factors into degrees $8, 2$, and 1. Again, one verifies that there are only two classes of subgroups of M_{11} with these orbit lengths: 2-Sylow subgroups, and cyclic subgroups of order 8.

Assume on the contrary that $\mathrm{Gal}(\hat{L}_{11}|\hat{\mathbb{Q}}_{11}) \cong C_8$. The degree-2 factor of f_0 takes the form $X^2 + b_1X + b_0$, with 11-adic valuations $\nu_{11}(b_1) = 0$ and $\nu_{11}(b_0) = -1$. Upon substituting $X/11$ for X (and multiplying by 11^2), this becomes an Eisenstein polynomial $u(X) \in \hat{\mathbb{Q}}_{11}[X]$. The splitting field of u is a ramified degree-2 subextension of $\hat{L}_{11}|\hat{\mathbb{Q}}_{11}$. As $\hat{L}_{11}|\hat{\mathbb{Q}}_{11}$ is cyclic of order 8, it follows that $\hat{L}_{11}|\hat{\mathbb{Q}}_{11}$ is totally ramified. This contradicts the fact that $\hat{\mathbb{Q}}_{11}$ has no totally ramified cyclic degree 8 extension. Thus $|\,\mathrm{Gal}(\hat{L}_{11}|\hat{\mathbb{Q}}_{11})| = 16$. □

Proof of Theorem 1. Recall that E is the splitting field of f over $k(t)$. By assumption there are at least two degree 1 primes $\mathfrak{q}_1, \mathfrak{q}_2$ of k whose restriction to $\mathbb{Q}$ is in $\{2, 11\}$. Also note that in a root field of the factor $f_0(X) = 77X^3 + 10989X^2 + 129816X + 496368$ from Lemma 9, both 2 and 11 do not split completely. As 2 and 11 split completely in k, the factor f_0 has to remain irreducible over k, and hence we may apply Lemma 9.

By Lemmas 9 and 10, there are primes $\mathfrak{p}_1, \mathfrak{p}_2$ of k and specializations $t{\to}t_i$, $t{\to}s_i$, for $t_i, s_i \in k$, $i = 1, 2$, such that the decomposition groups of $E_{t_i}|k$ (resp. $E_{s_i}|k$) over $\mathfrak{p}_i$ (resp. $\mathfrak{q}_i$) contain 3-Sylow (resp. 2-Sylow) subgroups of M_{11}. By Proposition 5, there exists $t_0 \in k$ such that $\mathrm{Gal}(E_{t_0}|k) \cong M_{11}$, the completion of E_{t_0} at $\mathfrak{p}_i$ identifies with the completion of E_{t_i} at $\mathfrak{p}_i$, and its completion at $\mathfrak{q}_i$ identifies with the completion of E_{s_i} at $\mathfrak{q}_i$, for $i = 1, 2$. Since every p-Sylow subgroup of M_{11} is cyclic for $p \neq 2, 3$, each such group appears as a decomposition group of $E_{t_0}|k$ over infinitely many primes. Thus, E_{t_0} is k-adequate by Schacher's criterion.

Since Lemma 9 gives infinitely many choices for the primes $\mathfrak{p}_1, \mathfrak{p}_2$, and each resulting specialization $E_{t_0}|k$ has only finitely many primes with decomposition group containing a 3-Sylow subgroup (as it has only finitely many ramified primes), by varying the the primes $\mathfrak{p}_1, \mathfrak{p}_2$ we get infinitely many distinct k-adequate Galois extensions with Galois group M_{11}. Since M_{11} is simple and nonabelian these extensions are linearly disjoint over k.

□

Remark 2. It should be emphasized that while computer calculations were used in some of the proofs, no "black-box" algorithms are needed. Rather, all that is needed is polynomial factorization over $\mathbb{Q}(y)$ (in Proposition 8) and over a p-adic field given to a sufficient precision (in Lemma 10), as well as information about the subgroups of M_{11} and their orbits (accessible e.g. in Magma via the `Subgroups` command).
For p-adic polynomial factorization, the Magma command `Factorization(f)` was used for a polynomial f in the structure `PolynomialRing(pAdicField(p,k))`, with a prime p and a precision k (precisions much larger than 100 may be used). To verify the irreducibility of a monic factor $g \in \mathbb{Z}_p[X]$ returned by this procedure, we used the following method. One may assume a factorization $g \equiv h_1 \cdot h_2 \bmod p^r$, where $r \leq k$, $h_1 = \sum_{i=0}^{n_1} \alpha_i X^i$ and $h_2 = \sum_{i=0}^{n_2} \beta_i X^i$. Now the existence of such a factorization may be excluded by a Groebner basis computation in the ring $\mathbb{Z}[\alpha_1, ..., \alpha_{n_1}, \beta_1, ..., \beta_{n_2}]$ (with the α's and β's viewed as transcendentals). This approach was successfully used to verify irreducibility of the (2-adic and 11-adic) degree 8 factors occurring in Lemma 10, by showing that these factors are irreducible mod 2^8 and mod 11^5, respectively.

References

[1] E. S. Allman, M. M. Schacher, *Division algebras with* $\mathrm{PSL}(2,q)$*-Galois maximal subfields.* J. Algebra 240 (2001), 808–821.

[2] A. Auel, E. Brussel, S. Garibaldi, and U. Vishne, *Open problems on central simple algebras.* Transform. Groups 16 (2011), 219–264.

[3] S. Beckmann, *On extensions of number fields obtained by specializing branched coverings.* J. reine angew. Math. 419 (1991), 27–53.

[4] D. Chillag, J. Sonn, *Sylow metacyclic groups and $\mathbb{Q}$-admissibility.* Israel Journal of Mathematics 40 (3) (1981), 307–323.

[5] W. Feit, P. Vojta, *Examples of some $\mathbb{Q}$-admissible groups.* J. Number Theory 26 (1987), 210–226.

[6] W. Feit, $SL_2(11)$ *is $\mathbb{Q}$-admissible.* J. Algebra 257 (2002), 244–248.

[7] M. D. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables.* Illinois J. Math. 17 (1973), 128–146.

[8] D. Harbater, J. Hartmann, D. Krashen, *Patching subfields of division algebras.* Trans. Amer. Math. Soc. 363 (2011), no. 6, 3335–3349.

[9] J. König, *On rational functions with monodromy group M_{11}.* J. Symb. Comput. 79 (2017), 372–383.

[10] G. Malle, *Multi-parameter polynomials with given Galois group.* J. Symb. Comput. 21 (2000), 1–15.

[11] G. Malle, B.H. Matzat, *Inverse Galois Theory.* Springer Monographs in Mathematics, Berlin-Heidelberg (1999).

[12] W. McCallum, B. Poonen, *The Method of Chabauty and Coleman.* Explicit Methods in Number Theory, Panor. Synthèses 36, Soc. Math. France, Paris (2012), 99–117.

[13] J.S. Milne *Fields and Galois theory.* Course notes, Version 4.51.

[14] P. Müller, *Finiteness Results for Hilbert's Irreducibility Theorem.* Ann. Inst. Fourier 52 (2002), 983–1015.

[15] D. Neftin, *Tamely ramified subfields of division algebras.* J. Algebra 378 (2013), 184–195.

[16] D. Neftin, E. Paran, *Patching and admissibility over two dimensional complete local domains.* Algebra and Number Theory 4, no. 6 (2010), 743–762.

[17] D. Neftin, U. Vishne, *Admissibility under extension of number fields.* Doc. Math. 18 (2013), 359–382.

[18] J. Neukirch, *Algebraic Number Theory.* Springer Verlag, Berlin-Heidelberg (1999).

[19] S. Liedahl, *Presentations of metacylic p-groups with applications to K-admissibility questions.* J. Algebra 169 (1994) 965–983.

[20] R. S. Pierce, *Associative Algebras.* Springer-Verlag (1982).

[21] B. Plans, N. Vila, *Galois covers of $\mathbb{P}^1$ over $\mathbb{Q}$ with prescribed local or global behavior by specialization.* J. Théor. Nombres Bordeaux 17 (2005), 271–282.

[22] M. Romagny, S. Wewers, *Hurwitz spaces.* Groupes de Galois arithmétiques et différentiels, Sémin. Congr., vol. 13, Soc. Math. France, Paris (2006), 313–341.

[23] M. Schacher, *Subfields of division rings, I.* J. Algebra 9 (1968) 451–477.

[24] J. P. Serre, *Local fields.* Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[25] J. Sonn, *Rational division algebras as solvable crossed products.* Israel J. Math. 37 (1980), 246–250.

[26] J. Sonn, *$\mathbb{Q}$-admissibility of solvable groups.* J. Algebra 84 (1983), 411–419.

[27] B. Surendranath Reddy, V. Suresh, *Admissibility of groups over function fields of p-adic curves.* Adv. Math. 237 (2013), 316–330.

Technion, Israel Institute of Technology, Haifa 3200, Israel.

E-mail address: `koenig.joach@tx.technion.ac.il`

Technion, Israel Institute of Technology, Haifa 3200, Israel.

E-mail address: `dneftin@tx.technion.ac.il`