Math. Res. Lett. **20** (2013), *no.* 5, 985–993

AN APPLICATION OF MAEDA'S CONJECTURE TO THE INVERSE GALOIS PROBLEM

Gabor Wiese

Abstract. It is shown that Maeda's conjecture on eigenforms of level 1 implies that for every positive even d and every p in a density-one set of primes, the simple group $\mathrm{PSL}_2(\mathbb{F}_{p^d})$ occurs as the Galois group of a number field ramifying only at p.

1. Introduction

The purpose of this paper is to support the approach to the inverse Galois problem for certain finite groups of Lie type through automorphic forms. There have been a number of promising results in the recent past, e.g., [2, 11] for groups of the type $\mathrm{PSL}_2(\mathbb{F}_{\ell^d})$, and [1, 6, 7] for more general groups. The general idea is to take varying automorphic forms over $\mathbb{Q}$ and to study the images of the residual Galois representations attached to them. Currently, one only obtains positive-density or infinity results. The main technical obstacle to improving the mentioned results to density 1 seems to be the lack of control on the fields of coefficients of the automorphic forms involved.

In the easiest case, that of 'classical' modular forms, i.e., of automorphic forms for GL_2 over $\mathbb{Q}$, there is a strong conjecture due to Maeda on the coefficient fields of level 1 modular forms. In order to demonstrate the potential of the modular approach to the inverse Galois problem, we show that the control on the coefficient fields provided by Maeda's conjecture suffices to yield the following strong result on the inverse Galois problem.

Theorem 1.1. *Assume the following form of* Maeda's conjecture *on level 1 modular forms:*

> *For any k and any normalised eigenform $f \in S_k(1)$ (the space of cuspidal modular forms of weight k and level 1), the coefficient field $\mathbb{Q}_f := \mathbb{Q}(a_n(f) \mid n \in \mathbb{N})$ has degree equal to $d_k := \dim_{\mathbb{C}} S_k(1)$ and the Galois group of its normal closure over $\mathbb{Q}$ is the symmetric group S_{d_k}.*

(a) *Let $2 \leq d \in \mathbb{N}$ be even. Then the set of primes p such that there is a number field $K/\mathbb{Q}$ ramified only at p with Galois group isomorphic to* $\mathrm{PSL}_2(\mathbb{F}_{p^d})$ *has density* 1.

(b) *Let $1 \leq d \in \mathbb{N}$ be odd. Then the set of primes p such that there is a number field $K/\mathbb{Q}$ ramified only at p with Galois group isomorphic to* $\mathrm{PGL}_2(\mathbb{F}_{p^d})$ *has density* 1.

Received by the editors December 7, 2012.

1991 *Mathematics Subject Classification.* MSC (2010): 11F11 (primary); 11F80, 11R32, 12F12 (secondary).

Maeda's conjecture was formulated as Conjecture 1.2 in [5]. It has been checked up to weight 12000 (see [4]). We also mention that a generalization of a weaker form of Maeda's conjecture to square-free levels has recently been proposed by Tsaknias [9].

Throughout the paper the notion of density can be taken to be either natural density or Dirichlet density.

It is certainly possible to give an effective version of Theorem 1.1. Suppose that Maeda's conjecture has been checked for weights up to B. Then for all $d \leq \dim_{\mathbb{C}} S_B(1)$ one can work out an explicit lower bound for the density of the sets in the theorem, depending on B.

The proof of Theorem 1.1 is given in the remainder of the paper. It is based on a meanwhile classical 'big image result' of Ribet [8], Chebotarev's density theorem, some combinatorics in symmetric groups, and Galois theory.

2. Proof

In this section, the main result is proved. We use the convention that the symmetric group S_n is the group of permutations of the set $\{1, 2, \ldots, n\}$.

2.1. Splitting of primes in extensions with symmetric Galois group.

In this part, we give a possibly non-standard proof of the well-known fact that the splitting behaviour of unramified primes in a simple extension $K(a)/K$ can be read off from the cycle type of the Frobenius, seen as an element of the permutation group of the roots of the minimal polynomial of a. (A more 'standard' proof would consider the factorization into irreducibles of the reduction of the minimal polynomial of a, as in [10], p. 198).

Let M/K be a separable field extension of degree n and let L/M be the Galois closure of M over K. By the theorem of the primitive element there is $a \in M$ such that $M = K(a)$. Let $f \in K[X]$ be the minimal polynomial of a over K and let $a = a_1, a_2, \ldots, a_n$ be the roots of f in L. The map $\psi : G := \mathrm{Gal}(L/K) \to S_n$, sending σ to the permutation $\psi(\sigma)$ given by $\sigma(a_i) = a_{\psi(\sigma)(i)}$ is an injective group homomorphism, which maps $H := \mathrm{Gal}(L/M)$ onto $\mathrm{Stab}_{S_n}(1) \cap \psi(G)$.

Proposition 2.1. *Assume the preceding set-up with K a number field. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ a prime of L dividing $\mathfrak{p}$. We suppose that $\mathfrak{P}/\mathfrak{p}$ is unramified. Then the cycle lengths in the cycle decomposition of $\psi(\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}) \in S_n$ are precisely the residue degrees of the primes of M lying above $\mathfrak{p}$.*

Proof. Let $g \in \mathrm{Gal}(L/K)$. Denote by $\mathrm{Frob}_{g\mathfrak{P}/\mathfrak{p}}$ the Frobenius element of $g\mathfrak{P}/\mathfrak{p}$ in $\mathrm{Gal}(L/K)$ and by $f_{(g\mathfrak{P}\cap M)/\mathfrak{p}}$ the inertial degree of the prime $g\mathfrak{P} \cap M$ of M over $\mathfrak{p}$. Write $\varphi := \mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ for short. We have

$$f_{(g\mathfrak{P}\cap M)/\mathfrak{p}} = \min_{i\in\mathbb{N}}(\mathrm{Frob}^i_{g\mathfrak{P}/\mathfrak{p}} \in H) = \min_{i\in\mathbb{N}}(\varphi^i \in g^{-1}Hg).$$

From this we obtain the equivalences:

$$\begin{aligned} & \exists g \in G : \ f_{(g\mathfrak{P}\cap M)/\mathfrak{p}} = d, \\ \Leftrightarrow \quad & \exists g \in G : \ \varphi^d \in g^{-1}Hg \text{ and } \forall\, 1 \leq i < d : \varphi^i \notin g^{-1}Hg, \end{aligned}$$

$$\begin{aligned}
&\Leftrightarrow\ \exists g \in G:\ \psi(\varphi^d) \in \mathrm{Stab}_{S_n}(\psi(g^{-1})(1))\\
&\qquad \text{and } \forall\, 1 \le i < d : \psi(\varphi^i) \notin \mathrm{Stab}_{S_n}(\psi(g^{-1})(1)),\\
&\Leftrightarrow\ \exists j \in \{1,\dots,n\}:\ \psi(\varphi^d) \in \mathrm{Stab}_{S_n}(j) \text{ and } \forall\, 1 \le i < d : \psi(\varphi^i) \notin \mathrm{Stab}_{S_n}(j)\\
&\Leftrightarrow\ \psi(\varphi) \text{ contains a } d\text{-cycle.}
\end{aligned}$$

This proves the proposition. □

2.2. Combinatorics in symmetric groups. We will eventually be interested in primes of a fixed residue degree d in an extension with symmetric Galois group. The results of the previous part hence lead us to consider elements in symmetric groups having a d-cycle, which we do in this part.

The contents of this part is presumably also well-known. Since the techniques are very simple and straight forward, I decided to include the proofs rather than to look for suitable references. Let $d \ge 1$ be a fixed integer. Define recursively for $i \ge 1$ and $1 \le j \le i$

$$a(0) := 0, \quad b(i,j) := \frac{1}{j!d^j}(1 - a(i-j)), \quad a(i) := \sum_{k=1}^{i} b(i,k).$$

Lemma 2.2. *With the preceding definitions we have*

$$a(i) = \sum_{j=1}^{i} \frac{(-1)^{j+1}}{j!d^j} = 1 - \exp\left(\frac{-1}{d}\right) + \sum_{j=i+1}^{\infty} \frac{(-1)^j}{j!d^j}.$$

Proof. This is a simple induction. For the convenience of the reader, we include the inductive step:

$$\begin{aligned}
a(i+1) &= \sum_{k=1}^{i+1} b(i+1,k) = \sum_{k=1}^{i+1} \frac{1}{k!d^k}(1 - a(i+1-k))\\
&= \sum_{k=1}^{i+1} \frac{1}{k!d^k}\left(1 - \sum_{j=1}^{i+1-k} \frac{(-1)^{j+1}}{j!d^j}\right) = \sum_{k=1}^{i+1}\left(\frac{1}{k!d^k} - \sum_{j=1}^{i+1-k} \frac{(-1)^{j+1}}{k!j!d^{j+k}}\right)\\
&= \sum_{m=1}^{i+1} \frac{1}{m!d^m} + \sum_{m=2}^{i+1} \frac{1}{m!d^m} \sum_{j=1}^{m-1} \binom{m}{j}(-1)^j = \sum_{m=1}^{i+1} \frac{(-1)^{m+1}}{m!d^m}.
\end{aligned}$$

□

For $i \to \infty$ the convergence $a(i) \to 1 - \exp(\frac{-1}{d})$ is very quick because of the simple estimate of the error term $\left|\sum_{j=i+1}^{\infty} \frac{1}{j!d^j}\right| \le \frac{2}{(i+1)!d^{i+1}}$.

We now relate the quantities $a(i)$ and $b(i,j)$ to proportions in the symmetric group. Let $n, j \in \mathbb{N}$. Define

$$\begin{aligned}
\mathcal{A}_n(d) &:= \{g \in S_n \mid g \text{ contains at least one } d\text{-cycle}\},\\
\mathcal{B}_n(d,j) &:= \{g \in S_n \mid g \text{ contains precisely } j\ d\text{-cycles}\}.
\end{aligned}$$

Lemma 2.3. *For all $n \ge 2d$ the following formulae hold, where $i := \lfloor \frac{n}{d} \rfloor$:*

(a) $n! \cdot a(i) = \#\mathcal{A}_n(d)$,

(b) $n! \cdot b(i,j) = \#\mathcal{B}_n(d,j)$,

(c) $n! \cdot \frac{2n-d-1}{n(n-1)}(1-a(i-1)) = \#\{g \in \mathcal{B}_n(d,1) \mid$ *the unique d-cycle contains* 1 *or* $2\}$,

(d) $n! \cdot \frac{1}{n(n-1)}(1-a(i-2)) = \#\{g \in \mathcal{B}_n(d,2) \mid$ *one d-cycle contains* 1*, the other* $2\}$.

Proof. (a) and (b) are proved by induction for $n \geq 1$. For $n < d$ (i.e., $i = 0$), the equalities are trivially true. Now we describe the induction step:

$$\begin{aligned}\#\mathcal{B}_n(d,j) = \frac{1}{j!} \cdot &\left(\binom{n}{d} \cdot (d-1)!\right) \cdot \left(\binom{n-d}{d} \cdot (d-1)!\right) \cdots \\ &\times \left(\binom{n-(j-1)d}{d} \cdot (d-1)!\right) \\ &\times (n-jd)! \cdot (1-a(i-j)) = \frac{n!}{j!d^j}(1-a(i-j)).\end{aligned}$$

The first equality can be seen as follows: there are $j!$ ways of ordering the j d-cycles. The number of choices for the first d-cycle is given by $\binom{n}{d} \cdot (d-1)!$, the one for the second is $\binom{n-d}{d} \cdot (d-1)!$, and so on. After having chosen j d-cycles, $n-jd$ elements remain. Among these remaining elements we may only take those that do not contain any d-cycle; their number is $(n-jd)! \cdot (1-a(i-j))$ by induction hypothesis.

(c) The number of elements in the set in question is

$$\left(2\binom{n-1}{d-1} - \binom{n-2}{d-2}\right)(d-1)! \cdot (n-d)! \cdot (1-a(i-1)) = n!\frac{2n-d-1}{n(n-1)}(1-a(i-1))$$

because $\binom{n-1}{d-1} \cdot (d-1)!$ is the number of choices for a d-cycle with one previously chosen element (i.e., 1 or 2) and $\binom{n-2}{d-2} \cdot (d-1)!$ is the number of choices for a d-cycle containing 1 and 2.

(d) The number of elements in the set in question is

$$\begin{aligned}&\binom{n-2}{d-1}(d-1)! \cdot \binom{n-2-(d-1)}{d-1}(d-1)! \cdot (n-2d)! \cdot (1-a(i-2)) \\ &= n!\frac{1}{n(n-1)}(1-a(i-2))\end{aligned}$$

because $\binom{n-2}{d-1} \cdot (d-1)!$ is the number of choices for a d-cycle containing 1 and not containing 2 and $\binom{n-2-(d-1)}{d-1} \cdot (d-1)!$ is the number of choices for a d-cycle containing 2 among the elements remaining after the first choice, and again $(n-2d)! \cdot (1-a(i-2))$ is the number of elements remaining after the two choices such that they do not contain any d-cycle. □

We write $\mathcal{A}_n^{\pm}(d)$ for the subsets of $\mathcal{A}_n(d)$ consisting of the elements having positive or negative signs.

Corollary 2.4. *Let $d, n \in \mathbb{N}$, $n \geq 2d \geq 2$ and put $i := \lfloor \frac{n}{d} \rfloor$. Then the estimates*

$$\begin{aligned}\left|\#\mathcal{A}_n^+(d) - \#\mathcal{A}_n^-(d)\right| &\leq n! \cdot \left(\frac{2n-d-1}{n(n-1)}(1-a(i-1)) + \frac{1}{n(n-1)}(1-a(i-2))\right) \\ &\leq n! \cdot \frac{2}{n-1}\end{aligned}$$

and

$$\left|\frac{\#\mathcal{A}_n^+(d)-\#\mathcal{A}_n^-(d)}{\#\mathcal{A}_n(d)}\right| \le \frac{1}{n-1}\cdot\frac{2}{1-\exp(-\frac{1}{d})-\frac{2}{(i+1)!d^{i+1}}}$$

hold.

Proof. Consider the bijection $\phi : S_n \xrightarrow{g\mapsto g\circ(12)} S_n$. For $j>2$ the image of $\mathcal{A}_n^+(d)\cap\mathcal{B}_n(d,j)$ under ϕ lands in $\mathcal{A}_n^-(d)$ because the multiplication with $(1\ 2)$ can at most remove two d-cycles. Now consider $g\in\mathcal{A}_n^+(d)\cap\mathcal{B}_n(d,2)$. Clearly $\phi(g)\in\mathcal{A}_n^-(d)$ unless one of the d-cycles contains 1 and the other one contains 2. For $g\in\mathcal{A}_n^+(d)\cap\mathcal{B}_n(d,1)$ we find that $\phi(g)\in\mathcal{A}_n^-(d)$ unless the single d-cycle of g contains 1 or 2. In view of Lemma 2.3, we thus obtain the inequality

$$\begin{aligned}\#\mathcal{A}_n^+(d)-\#\mathcal{A}_n^-(d) &\le n!\cdot\left(\frac{2n-d-1}{n(n-1)}(1-a(i-1))+\frac{1}{n(n-1)}(1-a(i-2))\right)\\ &\le n!\cdot\frac{2}{n-1}.\end{aligned}$$

By exchanging the roles of + and − we obtain the first estimate. The second estimate then is an immediate consequence of Lemma 2.2 and the trivial estimate of the error term mentioned after it. □

2.3. Density of primes with prescribed residue degree in composites of field extensions with symmetric Galois groups.

Lemma 2.5. *Let* $1\le d\in\mathbb{N}$, *K be a field and L/K, F/K be two finite Galois extensions such that* $\mathrm{Gal}(L/K)\cong S_n$ *with* $n\ge\max(5,2d)$ *and L is not a subfield of F. Let* $C\subseteq G:=\mathrm{Gal}(F/K)$ *be a subset and put* $c:=\frac{\#C}{\#G}$ *and* $a:=\frac{\#\mathcal{A}_n(d)}{\#S_n}=a(\lfloor\frac{n}{d}\rfloor)$.

Let $X:=\mathrm{Gal}(LF/K)$ *and Y be the subset of X consisting of those elements that project to an element in* $\mathcal{A}_n(d)\subseteq S_n\cong\mathrm{Gal}(L/K)$ *or to an element in* $C\subseteq\mathrm{Gal}(F/K)$ *under the natural projections. Then*

$$\frac{\#Y}{\#X}=a+c-(1+\delta)ac,$$

where

$$\begin{cases}\delta=0, & \textit{if } L\cap F=K,\\ |\delta|\le\frac{1}{n-1}\cdot\frac{2}{1-\exp(-\frac{1}{d})-\frac{2}{(1+\lceil\frac{n}{d}\rceil)!d^{1+\lceil\frac{n}{d}\rceil}}}, & \textit{otherwise.}\end{cases}$$

Proof. The intersection $L\cap F$ is a Galois extension of K which is contained in L. The group structure of S_n (more precisely, the fact that the alternating group A_n is the only non-trivial normal subgroup of S_n) hence implies that $[L\cap F:K]\le 2$; for, if $L\cap F$ were equal to L, then L would be a subfield of F, which is excluded by assumption.

Assume first $L\cap F=K$, then $\mathrm{Gal}(LF/K)\cong\mathrm{Gal}(L/K)\times\mathrm{Gal}(F/K)$ and thus

$$\#Y=\#\mathcal{A}_n(d)\cdot\#G+\#S_n\cdot\#C-\#\mathcal{A}_n(d)\cdot\#C,$$

from which the claimed formula follows by dividing by $\#X=\#G\cdot\#S_n$.

Assume now that $L\cap F=:N$ is a quadratic extension of K. Then X is isomorphic to the index 2 subgroup of $\mathrm{Gal}(L/K)\times\mathrm{Gal}(F/K)$ consisting of those pairs of elements (g,h) such that g and h project to the same element in $\mathrm{Gal}(N/K)$. The elements of

$\mathcal{A}_n(d)$ that project to the identity of $\mathrm{Gal}(N/K)$ are precisely those in $\mathcal{A}_n^+(d)$. In a similar way, we denote by C^+ those elements of C projecting to the identity of $\mathrm{Gal}(N/K)$, and by C^- the others. Then we have

$$\#Y = \#\mathcal{A}_n(d) \cdot \frac{\#G}{2} + \frac{\#S_n}{2} \cdot \#C - \#\mathcal{A}_n^+(d) \cdot \#C^+ - \#\mathcal{A}_n^-(d) \cdot \#C^-.$$

Dividing by $\#X = \frac{\#S_n \cdot \#G}{2}$ we obtain

$$\frac{\#Y}{\#X} = a + c - (1+\delta)ac, \text{ where } \delta = \frac{\#C^+ - \#C^-}{\#C} \cdot \frac{\#\mathcal{A}_n^+(d) - \#\mathcal{A}_n^-(d)}{\#\mathcal{A}_n(d)}.$$

The claim is now a consequence of Corollary 2.4. □

Lemma 2.6. *Let $(a_n)_{n\geq 1}$ be a sequence of non-negative real numbers such that $\sum_{n=1}^\infty a_n$ diverges.*

(a) *Let $\gamma > 0$, $b_0 \in \mathbb{R}$. Assume that $a_n < \frac{1}{\gamma}$ for all $n \geq 1$. We define a sequence $(b_n)_{n\geq 0}$ by the rule*

$$b_n := b_{n-1} + a_n - \gamma b_{n-1} a_n$$

for all $n \geq 1$. Then the sequence $(b_n)_{n\geq 1}$ tends to $1/\gamma$ for $n \to \infty$.

(b) *Let $(\delta_n)_{n\geq 1}$ be a sequence of real numbers tending to 0 and let $c_0 \in \mathbb{R}$. Assume that* $\limsup_{n\to\infty} a_n < 1$. *We define the (modified)* inclusion–exclusion sequence *as*

$$c_n := c_{n-1} + a_n - (1+\delta_n) c_{n-1} a_n \text{ for } n \geq 1.$$

Then the sequence $(c_n)_{n\geq 1}$ tends to 1.

Proof. (a) We let

$$\begin{aligned} r_n &:= 1 - \gamma b_n = 1 - \gamma(b_{n-1} + a_n - \gamma b_{n-1} a_n) = (1 - \gamma b_{n-1})(1 - \gamma a_n) \\ &= (1 - \gamma b_0)(1 - \gamma a_1)(1 - \gamma a_2) \cdots (1 - \gamma a_n). \end{aligned}$$

To see that the limit of $(\gamma b_n)_{n\geq 0}$ is 1, we take the logarithm of $(1 - \gamma a_1)(1 - \gamma a_2) \cdots (1 - \gamma a_n)$:

$$\sum_{i=1}^n \log(1 - \gamma a_i) = -\gamma \sum_{i=1}^n a_i - \sum_{i=1}^n \sum_{j=2}^\infty \frac{(\gamma a_i)^j}{j} \leq -\gamma \sum_{i=1}^n a_i.$$

By our assumption this diverges to $-\infty$ for $n \to \infty$, so that $\lim_{n\to\infty} r_n = 0$, proving the lemma.

(b) Let $\min\left(1, \frac{1}{\limsup_{n\to\infty} a_n} - 1\right) > \epsilon > 0$. There is N such that $|\delta_n| < \epsilon$ and $a_n < \frac{1}{1+\epsilon}$ for all $n \geq N$. By enlarging N if necessary we may also assume that $c_N \geq 0$. The reason for the latter is that $c_{N+n} > c_N + \sum_{i=1}^n a_{N+i}$ if $c_{N+i} < 0$ for all $0 \leq i \leq n$.

We consider the two sequences

$$b_N := c_N \text{ and } b_n = b_{n-1} + a_n - (1+\epsilon) b_{n-1} a_n, \text{ for } n > N$$

and

$$d_N := c_N \text{ and } d_n = d_{n-1} + a_n - (1-\epsilon) d_{n-1} a_n, \text{ for } n > N.$$

By (a) we know $\lim_{n\to\infty} b_n = \frac{1}{1+\epsilon}$ and $\lim_{n\to\infty} d_n = \frac{1}{1-\epsilon}$. For $n \geq N$ by induction we obtain the estimate:

$$0 \leq b_n \leq c_n \leq d_n.$$

Thus, there is M such that $\frac{1}{1+\epsilon} - \epsilon \le c_n \le \frac{1}{1-\epsilon} + \epsilon$ for all $n \ge M$. As ϵ is arbitrary, we find $\lim_{n\to\infty} c_n = 1$. □

Proposition 2.7. *Let $1 \le d \in \mathbb{N}$, K be a field and let L_n for $n \in \mathbb{N}$ be Galois extensions of K with Galois group $\mathrm{Gal}(L_n/K) \cong S_{N_n}$ such that $N_n < N_{n+1}$ for all $n \ge 1$. Denote by G_n the Galois group of the composite field $L_1 L_2 \cdots L_n$ over K and for $1 \le i \le n$ denote by $\pi_i : G_n \to \mathrm{Gal}(L_i/K)$ the natural projection. Consider*

$$c_n := \frac{\#\{g \in G_n \mid \exists i \in \{1,\dots,n\} : \pi_i(g) \in \mathrm{Gal}(L_i/K) \cong S_{N_i} \text{ contains a } d\text{-cycle}\}}{\#G_n}.$$

Then the sequence c_n tends to 1 for $n \to \infty$.

Proof. Without loss of generality we can assume that $\max(5, 2d) \le N_1$. Let $c_0 := 0$ and $a_n := a(\lfloor \frac{N_n}{d} \rfloor) = \frac{\#\mathcal{A}_{N_n}(d)}{\#S_{N_n}}$. By Lemmas 2.2 and 2.3 it is clear that $\sum_{n=1}^{\infty} a_n$ diverges.

If we call K_i the unique quadratic extension of K inside L_i, then Lemma 18.3.9 of [3] shows that $\mathrm{Gal}(L_1 \dots L_n/K_1 \cdots K_n) \cong A_{N_1} \times \cdots \times A_{N_n}$, for all $n \ge 1$. This implies that L_n cannot be a subfield of $L_1 \cdots L_{n-1}$ for any $n \ge 2$.

Lemma 2.5 inductively gives the formula $c_n = a_n + c_{n-1} - (1+\delta_n) a_n c_{n-1}$ for $n \ge 1$, where δ_n is bounded by

$$|\delta_n| \le \frac{1}{N_n - 1} \cdot \frac{2}{1 - \exp(-\frac{1}{d}) - \frac{2}{(1+\lceil \frac{N_n}{d} \rceil)! d^{1+\lceil \frac{N_n}{d} \rceil}}},$$

which clearly tends to 0 for $n \to \infty$. Lemma 2.6 yields the claim on the limit. □

By applying Chebotarev's density theorem and noting that the set in the proposition is conjugation invariant, we obtain the following corollary.

Corollary 2.8. *Let $1 \le d \in \mathbb{N}$, K be a number field and let L_n for $n \in \mathbb{N}$ be Galois extensions of K with Galois group $\mathrm{Gal}(L_n/K) \cong S_{N_n}$ such that $N_n < N_{n+1}$ for all $n \ge 1$.*

Then the set of primes of K

$$\{\mathfrak{p} \mid \exists i \in \{1,\dots,n\} : \pi_i(\mathrm{Frob}_{\mathfrak{p}}) \in \mathrm{Gal}(L_i/K) \cong S_{N_i} \text{ contains at least one } d\text{-cycle}\}$$

has a density, and the density is equal to c_n from Proposition 2.7 and hence tends to 1 for $n \to \infty$. Here $\mathrm{Frob}_{\mathfrak{p}} = \mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ for any prime $\mathfrak{P}$ of the composite field $L_1 L_2 \cdots L_n$ above $\mathfrak{p}$.

The following is the main theorem of this paper concerning the density of primes with prescribed residue degree in a composite of field extensions with symmetric Galois groups.

Theorem 2.9. *Let $1 \le d \in \mathbb{N}$, K be a number field and let M_n for $n \in \mathbb{N}$ be field extensions of K with splitting field L_n over K having Galois group $\mathrm{Gal}(L_n/K) \cong S_{N_n}$ such that $N_n < N_{n+1}$ for all $n \ge 1$.*

Then the set of primes of K

$$\{\mathfrak{p} \mid \exists i \in \{1,\dots,n\}, \exists \mathfrak{P}/\mathfrak{p} \text{ prime of } M_i \text{ of residue degree } d\}$$

has a density, and the density is equal to c_n from Proposition 2.7 and hence tends to 1 for $n \to \infty$.

Proof. Because of Proposition 2.1 the set of primes in the theorem is the same as the set in Corollary 2.8. □

2.4. End of the proof.

Proof of Theorem 1.1. Since $\dim_{\mathbb{C}} S_k(1)$ tends to ∞ for $k \to \infty$ (for even k), Maeda's conjecture implies the existence of newforms f_n of level one and increasing weight (automatically without complex multiplication because of level 1) such that their coefficient fields $M_n := \mathbb{Q}_{f_n}$ satisfy the assumptions of Theorem 2.9.

For each n and each prime $\mathfrak{P}$ of M_n consider the Galois representation $\rho^{\mathrm{proj}}_{f_n,\mathfrak{P}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ attached to f_n. Theorem 3.1 of Ribet [8] implies that for each f_n and all but possibly finitely many $\mathfrak{P}$, its image is equal to $\mathrm{PGL}_2(\mathbb{F}_{\mathfrak{P}})$, if the residue field $\mathbb{F}_{\mathfrak{P}}$ of $\mathfrak{P}$ has odd degree over its prime field, and equal to $\mathrm{PSL}_2(\mathbb{F}_{\mathfrak{P}})$ if the residue degree is even. We will abbreviate this by $\mathrm{PXL}_2(\mathbb{F}_{\mathfrak{P}})$.

Consequently, the set of primes (of $\mathbb{Q}$)

$$\{p \mid \exists i \in \{1, \ldots, n\}, \exists \mathfrak{P}/p \text{ prime of } M_i \text{ s.t. } \rho^{\mathrm{proj}}_{f_i,\mathfrak{P}} \cong \mathrm{PXL}_2(\mathbb{F}_{p^d})\}$$

has the same density as the corresponding set in Theorem 2.9, implying Theorem 1.1. □

Acknowledgments

I wish to thank Sara Arias-de-Reyna for reading an earlier version of this paper and her corrections and valuable remarks. I also thank Jürgen Klüners for the reference to van der Waerden. I acknowledge partial support by the Priority Program 1489 of the Deutsche Forschungsgemeinschaft (DFG) and by the Fonds National de la Recherche Luxembourg (INTER/DFG/12/10).

References

[1] S. Arias-de Reyna, L. Dieulefait, S.W. Shin and G. Wiese, *Compatible systems of symplectic Galois representations and the inverse Galois problem III. Automorphic construction of compatible systems with suitable local properties*, 2013, arXiv:1308.2192.

[2] L. Dieulefait and G. Wiese, *On modular forms and the inverse Galois problem*, Trans. Amer. Math. Soc. **363**(9) (2011), 4569–4584.

[3] M.D. Fried and M. Jarden, *Field arithmetic*, Vol. 11 of Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], Springer-Verlag, Berlin, 3rd ed., 2008, ISBN 978-3-540-77269-9. Revised by Jarden.

[4] A. Ghitza and A. McAndrew, *Experimental evidence for Maeda's conjecture on modular forms*, Tbil. Math. J. **5**(2) (2012), 55–69.

[5] H. Hida and Y. Maeda, *Non-abelian base change for totally real fields*, Pacific J. Math. (Special Issue) (1997), 189–217, Olga Taussky–Todd: in memoriam.

[6] C. Khare, M. Larsen and G. Savin, *Functoriality and the inverse Galois problem*, Compos. Math. **144**(3) (2008), 541–564.

[7] ———, *Functoriality and the inverse Galois problem. II. Groups of type B_n and G_2*, Ann. Fac. Sci. Toulouse Math. (6) **19**(1) (2010), 37–70.

[8] K.A. Ribet, *On l-adic representations attached to modular forms. II*, Glasgow Math. J. **27** (1985) 185–194.

[9] P. Tsaknias, *A possible generalization of Maeda's conjecture*, in G. Böckle, G. Wiese (eds.), *Computations with Modular Forms*, Contributions in Mathematical and Computational Sciences 6, Springer International Publishing Switzerland, 2014, 317–329.

[10] B.L. van der Waerden, *Moderne Algebra I*, Vol. XXXIII of Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Springer-Verlag, Berlin, 3rd edn., 1950.

[11] G. Wiese, *On projective linear groups over finite fields as Galois groups over the rational numbers*, in Modular forms on Schiermonnikoog, Cambridge University Press, Cambridge, 2008, 343–350.

Université du Luxembourg, Faculté des Sciences, de la Technologie et de la Communication,
6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg
Luxembourg

E-mail address: gabor.wiese@uni.lu