On the eigenvalues of the Hecke operator T_2.

KEVIN BUZZARD*

Department of Pure Mathematics and Mathematical Statistics,
16 Mill Lane,
Cambridge, CB2 1SB, UK

ABSTRACT: Let K be the splitting field of the characteristic polynomial of the Hecke operator T_2 acting on the d-dimensional space of cusp forms of weight k and level 1. We show, for various values of k, that the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is the full symmetric group on d symbols.

Let $k \geq 2$ be a fixed even integer and S_k the complex vector space of cusp forms of weight k for the full modular group $SL_2(\mathbb{Z})$. Say the dimension of S_k is d. Let $f \in S_k$ be an eigenvector for all the Hecke operators T_p as p runs through every rational prime. It is well-known that the eigenvalues a_p of T_p generate a number field L_f. Moreover, it is easy to check that if the characteristic polynomial of T_p acting on S_k is irreducible over $\mathbb{Q}$, then its splitting field K is the compositum of the L_fs for f running through the d eigenforms in S_k, and K is also the Galois closure of any L_f over $\mathbb{Q}$.

Because the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts faithfully on the d roots of the characteristic polynomial of T_p, we can identify $\mathrm{Gal}(K/\mathbb{Q})$ with a subgroup of the symmetric group Σ_d on d symbols. We restrict now to the case where $k = 12l$ for some prime l. Then the dimension of S_k is l.

Theorem. If $l \in \{2, 3, 5, 7, 11, 13, 17, 19\}$ and $k = 12l$ then the characteristic polynomial of T_2 on S_k is irreducible and if K is its splitting field over $\mathbb{Q}$ then $\mathrm{Gal}(K/\mathbb{Q}) \cong \Sigma_l$.

Remarks.

i) If $l \leq 7$ then the Galois group of the splitting field of an irreducible polynomial of degree l can be evaluated using standard computer algebra packages like PARI-GP or MAPLE. For $l > 7$ the packages available at present, to my knowledge, are unable to deal with polynomoials of degree l, so one has to use a trick.

ii) One has $\dim_{\mathbb{C}} S_k \leq 7$ for $2 \leq k \leq 98$, $k \neq 96$, and in these cases the referee has calculated $\mathrm{Gal}(K/\mathbb{Q})$, using the cited computer algebra packages, and has observed that it is isomorphic to the full symmetric group.

Corollary. If $l \in \{2, 3, 5, 7, 11, 13, 17, 19\}$ and $k = 12l$, then for any cusp eigenform $f = \Sigma a_n q^n$ of weight k for $SL_2(\mathbb{Z})$ with $a_1 = 1$, the field L_f generated over $\mathbb{Q}$ by the a_n has degree l over $\mathbb{Q}$ and the Galois closure K of L_f over $\mathbb{Q}$ satisfies $\mathrm{Gal}(K/\mathbb{Q}) \cong \Sigma_l$.

Proof of corollary. This comes from the fact that for these k we have $L_f = \mathbb{Q}(a_2)$. □

The proof of the theorem uses the following lemma.

Lemma. Let $l \in \mathbb{Z}$ be a prime, and let $P \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree l, with splitting field K over $\mathbb{Q}$. Say q is a prime such that the mod q reduction $\overline{P} \in \mathbb{F}_q[X]$ of P satisfies

$$\overline{P} = \prod_{i=0}^{r} h_i$$

for distinct irreducible polynomials h_i in $\mathbb{F}_q[X]$ with the following properties:

i) The degree of h_0 is 2

ii) The degree of h_i is odd, for $1 \leq i \leq r$.

Then $\mathrm{Gal}(K/\mathbb{Q}) \cong \Sigma_l$.

Proof of lemma. Let G be $\mathrm{Gal}(K/\mathbb{Q})$ identified as a subgroup of Σ_l. Now P has distinct roots modulo q and hence if $\wp$ is a prime of K above q, there is a unique element $\mathrm{Frob}_\wp \in G$, the Frobenius element at

* Research supported by the Science and Engineering Research Council.

$\wp$. Moreover, if d_i is the degree of h_i, we see that $\mathrm{Frob}_\wp$ is the product of $r+1$ disjoint cycles of lengths $d_0, d_1, \ldots, d_r$. Hence if $t = \prod_{i=1}^r d_i$ then $(\mathrm{Frob}_\wp)^t$ is a transposition in G. So the transitive subgroup G of Σ_l contains a transposition. This forces G to be the whole of Σ_l as can be seen thus: Put an equivalence relation $\sim$ on the roots of P by setting $a \sim b$ if either $a = b$ or the transposition (a, b) is an element of G. Then because the action is transitive on the roots, all equivalence classes have the same size, and because l is a prime there can be either 1 or l of them. But there is some transposition in G, and hence there is only 1 equivalence class and so G contains all transpositions and is thus Σ_l.

□

Proof of theorem. Clearly it suffices to show that the characteristic polynomial of T_2 acting on S_k for $k = 12l$, $l \in \{2, 3, 5, 7, 11, 13, 17, 19\}$ satisfies the conditions of the lemma for some q. As remarked earlier, for $l \leq 7$ the characteristic polynomial of T_2 acting on S_k can be easily checked to be irreducible and the Galois group of its splitting field over $\mathbb{Q}$ can also easily checked to be the full symmetric group. We shall restrict ourselves to the case $l > 7$. Let χ_k be the characteristic polynomial of T_2 acting on S_k. To prove that χ_k for $k = 12l$ is irreducible, it suffices to show that it is irreducible mod p for some prime p. So we have reduced the theorem to finding, for all k in question, primes p and q for which χ_k is irreducible modulo p and satisfies the conditions of the lemma modulo q.

The first calculations of χ_k for $k \leq 158$ were done by Maeda in [1]. For larger k we calculated χ_k modulo many primes without actually calculating χ_k itself. The following table of results finishes the proof.

l	prime	Complete factorisation of χ_{12l} modulo this prime.
11	$q = 37$	$(X^2+30X+34)(X+4)(X+6)(X+11)(X+14)$ $(X+15)(X+21)(X+26)(X+31)(X+33)$
11	$p = 479$	$X^{11}+189X^{10}+343X^9+43X^8+424X^7+323X^6+$ $+58X^5+100X^4+131X^3+307X^2+192X+133$
13	$q = 29$	$(X^2+24X+26)(X+9)(X+11)(X+13)(X+14)$ $(X+16)(X+17)(X+22)(X+24)(X+26)(X+27)(X+28)$
13	$p = 353$	$X^{13}+287X^{12}+288X^{11}+304X^{10}+252X^9+76X^8+139X^7+$ $+218X^6+62X^5+350X^4+249X^3+299X^2+307X+73$
17	$p = 263$	$X^{17}+123X^{16}+97X^{15}+194X^{14}+30X^{13}+60X^{12}+99X^{11}+2X^{10}+$ $+94X^9+209X^8+203X^7+157X^6+46X^5+8X^4+83X^3+209X^2+204X+4$
17	$q = 317$	$(X^2+123X+261)(X^{15}+91X^{14}+66X^{13}+205X^{12}+71X^{11}+191X^{10}+77X^9+$ $+43X^8+295X^7+28X^6+168X^5+253X^4+18X^3+54X^2+186X+4)$
19	$q = 53$	$(X^2+41X+6)(X+13)(X+17)(X+21)(X+23)(X+37)(X+45)(X+46)(X+49)$ $(X^3+47X^2+7X+21)(X^3+35X^2+36X+52)(X^3+18X^2+35X+25)$
19	$p = 251$	$X^{19}+186X^{18}+5X^{17}+86X^{16}+71X^{15}+237X^{14}+15X^{13}+145X^{12}+113X^{11}+$ $+30X^{10}+155X^8+162X^7+70X^6+89X^5+241X^4+188X^3+52X^2+217X+199$

□

Reference.

1. Y. MAEDA, Table of characteristic polynomials for the Hecke operator $T(2)$ on $S_k(SL_2(\mathbb{Z}))$. Hokkaido University, Sapporo, Japan.