FIELDS OF MODULAR FUNCTIONS OF GENUS 0

BY
JOSEPH B. DENNIN, JR.

1. Introduction

Let Γ be the group of linear fractional transformations

$$w \to (aw + b)/(cw + d)$$

of the upper half plane into itself with integer coefficients and determinant 1. Γ is isomorphic to the 2×2 modular group, i.e. the group of 2×2 matrices with integer entries and determinant 1 in which a matrix is identified with its negative. Let $\Gamma(n)$, the principal congruence subgroup of level n, be the subgroup of Γ consisting of those elements for which $a \equiv d \equiv 1 \ (n)$ and $b \equiv c \equiv 0 \ (n)$. G is called a congruence subgroup of level n if G contains $\Gamma(n)$ and n is the smallest such integer. G has a fundamental domain in the upper half plane which can be compactified to a Riemann surface and then the genus of G can be defined to be the genus of the Riemann surface. H. Rademacher has conjectured that the number of congruence subgroups of genus 0 is finite. D. McQuillan [6] has shown that if n is relatively prime to $2 \cdot 3 \cdot 5$, then the conjecture is true. In this paper, we show that the number of subgroups of levels 5^n and 3^n, $n \geq 1$, of genus 0 is finite and list explicitly which ones they are.

Consider $M_{\Gamma(n)}$, the Riemann surface associated with $\Gamma(n)$. The field of meromorphic functions on $M_{\Gamma(n)}$ is called the field of modular functions of level n and is denoted by $K(n)$. If j is the absolute Weierstrass invariant, $K(n)$ is a finite Galois extension of $C(j)$ with $\Gamma/\Gamma(n)$ for Galois group. Let $SL(2, n)$ be the special linear group of degree two with coefficients in Z/nZ and let $LF(2, n) = SL(2, n)/ \pm \mathrm{Id}$. Then $\Gamma/\Gamma(n)$ is isomorphic to $LF(2, n)$. If $\Gamma(n) \subset G \subset \Gamma$ and H is the corresponding subgroup of $LF(2, n)$, then by Galois theory H corresponds to a subfield F of $K(n)$ and the genus of F equals the genus of G.

The following notation will be standard. A matrix

$$\pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

will be written $\pm(a, b, c, d)$.

$$T = \pm(0, -1, 1, 0); \quad S = \pm(1, 1, 0, 1); \quad R = \pm(0, -1, 1, 1).$$

T and S generate $LF(2, n)$ and $R = TS$. F will be a subfield of $K(n)$ containing $C(j)$ and H, the corresponding subgroup of $LF(2, n)$. $g(H)$ = the genus of H and h or $|H|$ = the order of H. $[A]$ or $[\pm(a, b, c, d)]$ will denote the group generated by A or $\pm(a, b, c, d)$ respectively.

Received February 4, 1969.

We now concentrate on $LF(2, p^n)$, $p > 2$, whose order is $p^{3n-2}(p^2 - 1)/2$. McQuillan [6] obtained the following formula for the genus of H.

Let r, t and $s(p^r)$ be the number of distinct cyclic subgroups of H generated by a conjugate in $LF(2, p^n)$ of R, T and S^{p^r} respectively where $1 \leq p^r < p^n$. Then

$$g(H) = 1 + p^{2n-2}(p^2 - 1)(p^n - 6)/24h - p^{n-1}(p - (-3/p))r/3h \\ - p^{n-1}(p - (-1/p))t/4h - p^{2n-2}(p - 1)^2 W/4h \tag{1.1}$$

where $W = \sum s(p^r)$. One immediate consequence of this is that if two groups are conjugate, they have the same genus.

We also need the following results from Gierster [2] which is a chief source of information on $LF(2, p^n)$, $p > 2$.

LEMMA 1.1. *Suppose $p > 2$. An element of $LF(2, p^n)$ is conjugate to T if and only if its trace is 0. Consequently every element of order 2 is conjugate to T and has the form $\pm (a, b, c, -a)$ where $-a^2 - bc \equiv 1\ (p^n)$. An element of $LF(2, p^n)$ is conjugate to R if and only if its trace is 1.*

Let f_r^n be the natural homomorphism from $LF(2, p^n)$ to $LF(2, p^r)$, $0 < r < n$, given by reducing an element mod p^r. The kernel of this homomorphism is denoted by K_r^n and has order $p^{3(n-r)}$.

PROPOSITION 1.1. *If $H \cap K_{n-1}^n$ is the identity, $H \cap K_r^n$ is the identity for $r = 1, \cdots, n-2$.*

PROPOSITION 1.2. *If $| H \cap K_{n-1}^n | = p$, then $H \cap K_1^n$ is cyclic and*

$$| H \cap K_1^n | \leq p^{n-1}.$$

PROPOSITION 1.3. *If $| H \cap K_{n-1}^n | = p^2$, then $H \cap K_1^n$ is generated by two transformations U and U' of order p^{n-r} and $p^{n-r'}$ respectively and*

$$| H \cap K_1^n | = p^{2n-r-r'}.$$

So $| H \cap K_1^n | \leq p^{2n-2}$.

We use the groups K_r^n to define the concept of level for H. H is of level p^r if H contains K_r^n and does not contain K_{r-1}^n. Similarly we say a subfield F of $K(p^n)$ is of level p^r if F is a subfield of $K(p^r)$ and not a subfield of $K(p^{r-1})$. Note that F is of level p^r if and only if its Galois group is of level p^r.

For each r, K_r^n is a normal subgroup of $LF(2, p^n)$ and if $p > 3$, these are all the normal subgroups of $LF(2, p^n)$ [5]. Since K_r^n is normal, $H \cdot K_r^n$ is a subgroup of $LF(2, p^n)$ and we have the following useful formulas:

$$| H \cdot K_r^n | = | H |\, | K_r^n | / | H \cap K_r^n | \tag{1.2}$$

$$| H \cap K_r^n | = | H |\, | K_r^n | / | H \cdot K_r^n | . \tag{1.3}$$

In addition to the propositions from Gierster [2], we also use his tables extensively and when we use the phrase "by Gierster" we are referring to this paper. Gierster writes an element of K_r^n :

$$U_r = \varphi(\mu, \nu, \rho)_r \equiv (u + p^r\mu, p^r\nu, p^r\rho, u - p^r\mu) \bmod p^n$$

where μ, ν, ρ belong to the set of residues mod p^{n-r},

$$u^2 \equiv 1 + 2^{2r}(\mu^2 + \nu\rho) \quad \bmod p^n \quad \text{and} \quad u \equiv 1 \quad (p).$$

A final group we find useful is the one generated by K_1^n and S which we denote by E and which has order p^{3n-2}.

To compute the genus of H, we have to calculate r, t and $s(p^r)$. Lemma 1.1 and the Sylow theorems are very useful in calculating r and t. We now give a method for calculating $s(p^r)$. Note a conjugate of S^{p^r} has the form

$$\pm(1 - p^rac, p^ra^2, -p^rc^2, 1 + p^rac).$$

LEMMA 1.2.

$$(1 - pac, pa^2, -pc^2, 1 + pac)^k = (1 - kpac, kpa^2, -kpc^2, 1 + kpac).$$

Proof. Induction on k.

LEMMA 1.3. *Suppose A is a subgroup of $LF(2, p^n)$ and A is conjugate to $[S^{p^r}]$ where $0 \leq r \leq n - 1$. Then A contains an element conjugate to S^{p^r},*

$$\alpha = \pm(1 - p^rac, p^ra^2, -p^rc^2, 1 + p^rac).$$

If $(a, p^n) = 1$, then A contains one and only one element of the form $\pm (x, p^r, y, z)$.

Proof. Consider

$$\{\alpha^k\} = \{\pm(1 - kp^rac, kp^ra^2, -kp^rc^2, 1 + kp^rac)\}, \qquad 1 \leq k \leq p^{n-r}.$$

Since $(a^2, p^n) = 1$, the set $\{ka^2\}$ consists of the p^{n-r} different elements of $Z/p^{n-r}Z$ and so $ka^2 = 1$ for exactly one k.

LEMMA 1.4. *Suppose $\pm(x, p^r, y, z)$ belongs to a group conjugate to $[S^{p^r}]$. Then $\pm(x, p^r, y, z)$ is conjugate to S^{p^r} and further if*

$$\pm(a, b, c, d) \cdot \pm(1, p^r, 0, 1) \cdot \pm(a, b, c, d)^{-1} = \pm(x, p^r, y, z),$$

then $(a, p^n) = 1$.

Proof. If $\pm(x, p^r, y, z)$ is conjugate to $\pm(1, s_0 p^r, 0, 1)$, then

$$p^r \equiv s_0a^2p^r \ (p^n)$$

for some a. Thus $(a, p) = 1$ and s_0 is a quadratic residue mod p^{n-r}. But $\pm(1, s_0p^r, 0, 1)$ is conjugate to S^{p^r} if and only if s_0 is a quadratic residue mod p^{n-r}.

PROPOSITION 1.4 *Any group A conjugate to $[S^{p^r}]$, where*

$$\pm(1 - p^rac, p^ra^2, -p^rc^2, 1 + p^rac)$$

is an element of A *and* $(a, p^n) = 1$, *contains one and only one element of the form* $\pm(x, p^r, y, z)$ *and it is conjugate to* S^{p^r}.

Thus if it is known that, for conjugates of $\pm(1, p^r, 0, 1)$, $(a, p) = 1$, to calculate $s(p^r)$ it is sufficient to set $a = 1$ and see how many choices of c yield distinct elements of $LF(2, p^n)$. In particular, this is the case if it can be shown that p divides c since $ad - bc \equiv 1\ (p^n)$.

2. $LF(2, 5^n)$

Let $H' = \{\pm(x, y, 0, z)\}$ where x, y, z belong to the set of residues mod 25 and $xz \equiv 1\ (25)$.

THEOREM 1. *The only subfields of* $K(5^n)$, $n \geq 1$, *which have genus* 0 *are the subfields of* $K(5)$ *and the following two classes of subfields of* $K(25)$ *of level* 25: (1) $\{k_1\}$ *where* $G(K(25) \mid k_1)$ *has order* 250 *and is conjugate to* H'; (2) $\{k_2\}$ *where* $G(K(25) \mid k_2)$ *has order* 125 *and is conjugate to* $H' \cap E$.

Note that all subfields of $K(5)$ have genus 0 since a subfield of a field of genus 0 has genus 0. The rest of the proof will follow from propositions 2.1 and 2.2.

Suppose that H is a subgroup of $LF(2, 5^2)$ of level 25. Then $|H \cap K_1^2| \leq 5^2$ and so $|H \cdot K_1^2| \geq |H| \cdot 5$ which implies that $|H| \leq 5^3 \cdot 12$. By using formula 1.1, Sylow to get upper bounds on t and r, Sylow and Gierster to get upper bounds on W and the fact that $g(H) \geq 0$, we calculate that $g(H) > 0$ if $|H| = 2, 3, 4, 5, 6, 10, 12, 15, 20, 25, 30, 50, 60$ or 75. In this section, r_0 will denote a fixed non-zero residue mod 5.

LEMMA 2.1. *If* $|H| = 5^2 \cdot 12$ *or* $5^3 \cdot 12$, *then* $g(H) \neq 0$.

Proof. Suppose $|H| = 5^2 \cdot 12$. Then, by formula 1.2, $|H \cap K_1^2| \geq 5$. If $|H \cap K_1^2| = 5$, then $H \cdot K_1^2 = \mathrm{LF}(2, 25)$ and H (mod 5) $= LF(2, 5)$. So H contains K_1^2 [6,484] which is a contradiction. If $|H \cap K_1^2| = 25$, H is of the third type [2,353]; but there are no groups of order $12 \cdot 5^2$ of the third type [2,357–360]. Suppose $|H| = 5^3 \cdot 12$. Then $|H \cap K_1^2| = 25$ which implies that $|H \cdot K_1^2| = 5^4 \cdot 12$. So H (mod 5) $= LF(2, 5)$ implying H contains K_1^2, a contradiction.

LEMMA 2.2 *If* $|H| = 5^3 \cdot k$, $k = 3, 4, 6$ *or* 10, *then* $g(H) \neq 0$.

Proof. Since, if $|H \cap K_1^2| < 25$, $|H \cdot K_1^2|$ would be greater than $|LF(2, 5^2)|$, $|H \cap K_1^2| = 25$. If $|H| = 5^3 \cdot 3$ or $5^3 \cdot 4$, $|H \cdot K_1^2| = 5^4 \cdot 3$ or $5^4 \cdot 4$ and so H(mod 5) $= 15$ or 20. But $LF(2, 5)$ has no subgroups of order 15 or 20. If $|H| = 5^3 \cdot 6$ or $5^3 \cdot 10$, then $|H \cdot K_1^2| = 5^4 \cdot 6$ or $5^4 \cdot 10$. But $LF(2, 5^2)$ has no such subgroups.

LEMMA 2.3. *If* $|H| = 5^2 \cdot 4$, $g(H) \neq 0$.

Proof. Note that $|H \cap K_1^2| = 5$ or 25. If $|H \cap K_1^2| = 5$, $|H \cdot K_1^2| = 5^4 \cdot 4$

and so $|H \pmod 5)| = 20$ which is impossible. If $|H \cap K_1^2| = 25$, then $g(H) = (115\text{-}t\text{-}20W)/20$. By Sylow, $t \leq 75$ and by Gierster pp. 329–330, $W \leq 2$. Thus $g(H) = 0$ if and only if $W = 2$ and $t = 75$. We show that $t < 75$.

Let $B = \{\text{identity}, T, \pm (7, 0, 0, -7), \pm (0, 7, 7, 0)\}$ and let A be a subgroup of H of order 4. Since, by Sylow, A and B are conjugate and since conjugate groups have the same genus, we may assume that, by conjugating H, B is a subgroup of H. Further note that $(H \cap K_1^2)\cdot B$ has 100 elements and so $H = (H \cap K_1^2)\cdot B$. So in order to obtain 75 elements of order 2 in H, it is necessary that each element ($\neq$ identity) of B yield 25 elements of order 2 when multiplied by $(H \cap K_1^2)$.

$$K_1^2\cdot T = \{\pm(-5y, 1 - 5x, 1 + 5x, 5z)\}$$

where x, y, z describe all values mod 5. The 25 elements of order 2 in this set are given by $y \equiv z(5)$; so

$$(H \cap K_1^2) = \{\pm(1 - 5x, 5y, 5y, 1 + 5x)\}.$$

But then

$$(H \cap K_1^2)\cdot \pm (0, 7, 7, 0) = \{\pm(10y, 7 - 10x, 7 + 10x, 10y)\}$$

yields only 5 more elements of order 2 given by $y = 0$. So $t < 75$.

LEMMA 2.4. *If* $|H| = 5^2\cdot 6, g(H) \neq 0$.

Proof. $|H \cap K_1^2| = 5$ or 25. If $|H \cap K_1^2| = 5$, then $|H\cdot K_1^2| = 5^4\cdot 6$ which is impossible. If $|H \cap K_1^2| = 25$,

$$W \leq 2[2,329\text{–}330] \quad \text{and} \quad g(H) = (125\text{-}r\text{-}t\text{-}20W)/30.$$

So if $g(H) = 0$ we have 3 possibilities: $W = 0$ and $r + t = 125$; $W = 1$ and $r + t = 105$; $W = 2$ and $r + t = 85$. But by Sylow, $r + t \neq 105$ or 85 and if $r + t = 125$, $t = 75$ and $r = 50$. Thus if $g(H) = 0$, the only possible orders for elements of H are 2, 3 and 5. But $H \pmod 5)$ is a dihedral group of order 6 containing 3 elements of order 2. So each element of order 2 in $H \pmod 5)$ must have 25 elements of order 2 in its pre-image in H. Therefore in H, any element of order 2 multiplied by $H \cap K_1^2$ has to yield 25 elements of order 2.

As in Lemma 2.3, we may assume T is in H and so to get 25 elements of order 2 from $(H \cap K_1^2)\cdot T$, $H \cap K_1^2$ has to be

$$\{\pm(1 - 5x, 5y, 5y, 1 + 5x)\}.$$

To get $t = 75$, we must find 2 elements of order 2 in addition to T which, when multiplied by $H \cap K_1^2$, will yield 25 elements of order 2 different from those in $(H \cap K_1^2)\cdot T$. Now

$$\begin{aligned}(H \cap K_1^2)\cdot &\pm (a, b, c, -a)\\ &= \{a - 5ax + 5yc, b - 5bx - 5ya, 5ya + c + 5ax, -a-5ax + 5yb)\}.\end{aligned}$$

So we wish to find a, b, c such that $-10ax + 5yc + 5yb \equiv 0\ (25)$ for $x, y = 0, \cdots, 4$. If $x = 0$, we need $(c + b) \equiv 0\ (5)$. If $y = 0$, we need $a \equiv 0\ (5)$. Further, from the determinant, we need $a^2 + bc \equiv -1\ (25)$. So we have to solve simultaneously $(c + b) \equiv 0\ (5)$ and $-bc \equiv 1\ (25)$. The only solutions are the pairs $\{1, -1\}$, $\{4, 6\}$, $\{9, 11\}$ and their negatives. The elements of order 2 corresponding to these pairs all belong to $(H \cap K_1^2) \cdot T$. So $t < 75$ and $g(H) > 0$.

LEMMA 2.5. *If* $|H| = 5^3 \cdot 2$, *then* $g(H) = 0$ *if and only if* H *is conjugate to* H'.

Proof. Note $|H'| = 5^3 \cdot 2$ and $g(H') = 0$ since $t = 25$ and $W = 6$, the 25 elements of order 2 being given by $\{\pm(7, y, 0, -7)\}$ where $0 \leq y \leq 24$ and the 6 groups contributing to W being generated by

$$\pm(-4, 1, 0, 6), \quad \pm(-9, 1, 0, 11), \quad \pm(11, 1, 0, -9),$$
$$\pm(6, 1, 0, -4), \quad \pm(1, 1, 0, 1) \quad \text{and} \quad \pm(1, 5, 0, 1).$$

In general if $|H| = 5^3 \cdot 2$, $|H \cap K_1^2| = 25$ and so H is of type 3. So there are 2 possibilities for H, [2,357–360]. First H could be one of 30 conjugate $G''_{250}(I, I)_0$ containing $1(1, 2)(I, I)_0$ and 25 $G_{10} \cdot H'$ is an example of this type and so all these groups have genus 0.

Second, H could belong to one of 4 types of 30 conjugate $G''_{250}(I, I', 1)_0$ containing $1(1, 2)(I, I', 1)$ and 25 G_{10}. So to calculate W, it is necessary to investigate $a(1, 2)(I, I', 1)$. In $LF(2, 5^2)$, there are 4 given by

$$\{\pm(1 + 5(\xi + z), \xi, 5r_0\xi, 1 - 5(\xi + z))\}$$

where z describes all values mod 5 and ξ all values mod 25. The 4 different groups correspond to choices for r_0.

Recall a conjugate of S^r has the form

$$\pm(1 - 5^r ac, 5^r a^2, -5^r c^2, 1 + 5^r ac)$$

where at least one of a and c is not congruent to 0 mod 5. So if a conjugate of S belongs to $(1, 2)(I, I', 1)_0$, $-c^2 \equiv 5r_0\xi\ (25)$ so that 5 divides c so that $-c^2 \equiv 0\ (25)$ so that $5r_0\xi \equiv 0\ (25)$ which, together with $r_0 \not\equiv 0\ (5)$ implies that $\xi \equiv 0\ (5)$ so that $a^2 \equiv 0\ (5)$ which is a contradiction since then 5 divides both a and c. If a conjugate of S^5 belongs to $(1, 2)(I, I', 1)_0$, $5r_0\xi \equiv -5c^2$ (25) and $5a^2 \equiv \xi\ (25)$ so that $0 \equiv 25r_0a^2 \equiv -5c^2\ (25)$. Thus 5 divides c so that $(a, 5) = 1$. By Proposition 1.4, we let $a = 1$ and find there is only one conjugate of $[S^5]$ in $(1, 2)(I, I', 1)_0$, namely $[S^5]$ itself. Thus $W = 1$ and $g(H) = (125\text{-}t)/50 = 0$ if and only if $t = 125$. But H contains 124 elements of order divisible by 5 in $(1, 2)(I, I', 1)_0$ and at least one element of order 10 in G_{10}. Since $|H| = 250$, $t \neq 125$ and $g(H) \neq 0$.

LEMMA 2.6. *Suppose* $|H| = 5^3$ *and* $H \neq K_1^2$. *Then* $g(H) = 0$ *if and only if* H *is conjugate to* $H' \cap E$.

Proof. First observe that $g(H) = (24 - 4W)/5$. Also note, from Gierster, pp. 345–352, that any group of order 5^3 $(\neq K_1^2)$ can be gotten by intersecting a group of order 250 with E. So we must consider a $(1, 2)(I, I)_0$ and a $(1, 2)(I, I', 1)_0$. From Lemma 2.5, we see that $H' \cap E$ is an example of the first type so that $W = 6$ and $g(H) = 0$. We also see that in the second case $W = 1$ and $g(H) = 4$.

From Lemmas 2.1 to 2.6, we now have

PROPOSITION 2.1. *There exist two classes of subfields of $K(25)$ of level 25, $\{k_1\}$ and $\{k_2\}$, which have genus 0. These are distinguished by the fact that $G(K(25) \mid k_1)$ has order 250 and is conjugate to H' and that $G(K(25) \mid k_2)$ has order 125 and is conjugate to $H' \cap E$.*

LEMMA 2.7. *If F is a subfield of $K(125)$ and $F_1 = F \cap K(25)$ is contained in K (5), then F is contained in K (5).*

Proof. Note that since F_1 is a subfield of $K(5)$, F_1 equals $F \cap K(5)$ so that

$$H \cdot K_1^3 = H \cdot K_2^3 = G(K(125) \mid F_1).$$

Also $G(K(5) \mid F_1)$ has order $5^k \cdot m$ where $k = 0$; $m = 1, 2, 3, 4, 6$ or 12 or $k = 1$; $m = 1, 2, 12$. We show that F is a subfield of $K(25)$ which is sufficient since $F \cap K(25)$ is a subfield of $K(5)$. If F is not a subfield of $K(25)$, then

$$| H \cap K_2^3 | = | (H \cap K_1^3) \cap K_2^3 | = 1, 5 \text{ or } 25.$$

Using the fact that $| H \cdot K_2^3 | = | H \cdot K_1^3 | = 5^6 \cdot 5^k \cdot m$ and formula 1.2, we see that $| H | = 5^3 \cdot 5^k \cdot m$, $5^4 \cdot 5^k \cdot m$ or $5^5 \cdot 5^k \cdot m$ as $| H \cap K_2^3 | = 1, 5$ or 25. But then by formula 1.3, $| H \cap K_1^3 | = 5^3, 5^4$ or 5^5 which contradicts Proposition 1.1, 1.2, or 1.3 respectively.

Remark. This type of argument, using the orders of the various groups obtained from H and K_r^n, formulas 1.2 and 1.3 and Propositions 1.1–1.3, will be used frequently and will be referred to as the usual argument using Propositions 1.1–1.3.

LEMMA 2.8. *Suppose F is a subfield of $K(125)$ of genus 0 so that $F_1 = F \cap K(25)$ also has genus 0. If the level of F_1 is 25, F is contained in $K(25)$.*

Proof. Since the level of F_1 is 25, $H_1 = G(K(25) \mid F_1)$ is conjugate to H' or $H' \cap E$. If F is not a subfield of $K(25)$, $| H \cap K_2^3 | = 1, 5$ or 25. If $| H \cap K_2^3 | = 1$ or 5, the usual argument using Proposition 1.1 or 1.2 leads to a contradiction. If $| H \cap K_2^3 | = 25$, then $| H \cap K_1^3 | = 5^4$ by the standard calculations using formulas 1.2 and 1.3.

Suppose H_1 is conjugate to $H \cap E$. Then $| H | = 5^5$ and H is either a $(2, 3)(I, I)_0$ or a $(2, 3)(I, I', 1)_0$ [2, pp. 345–352]. An example of the first is given by $\{\pm(u + 5z, \xi, 0, u - 5z)\}$ where ξ describes all values mod 125 and z all values mod 25. Using Proposition 1.4, we see that H contains 5 conjugates of $[S]$ (given by $a = 1$ and $c = 0, 25, 50, 75, 100$); 5 conjugates of $[S^5]$ given by $a = 1$ and $c = 0, 5, 10, 15, 20$) and 1 conjugate of $[S^{25}]$ ($a = 1$, $c = 0$). So $W = 11$ and $g(H) = 16$. An example of the second is given by $\{\pm(u + 5z, \xi, 5r_0\xi, u - 5z)\}$ where ξ, z are as above. For conjugates of $[S]$, consider $-c^2 \equiv 25r_0\xi$ (125) which implies that 5 divides c and $(a, 5) = 1$. Applying Proposition 1.4, we let $a = 1$ and get $-c^2 \equiv 25r_0$ (125). If r_0 is a quadratic residue mod 5, there are 10 choices for c; if not, there are none. For conjugates of $[S^5]$, $5a^2 \equiv \xi$ (125) and so

$$-5c^2 \equiv 25r_0\xi \equiv 125r_0a^2 \equiv 0 \ (125)$$

which implies that 5 divides c and we see there are 5 choices for c regardless of what r_0 is. Similarly there is only one conjugate of $[S^{25}]$ regardless of what r_0 is. So $W = 16$ or 6 and $g(H) = 12$ or 20 depending on whether r_0 is a quadratic residue or not.

Suppose H_1 is conjugate to H'. Then $|H| = 5^5 \cdot 2$ and H is either a $G''_{6250}(I, I)_0$ or one of 4 types of $G''_{6250}(I, I', 1)$. An example of the first is given by $\{\pm(x, y, 0, z)\}$ where x, y, z describe all values mod 125 and $xz \equiv 1$ (125). Then $H \cap E$ is a $(2, 3)(I, I)_0$ and so $W = 11$. Further $t = 125$ since the only elements of order 2 in H are $\pm(43, \xi, 0, -43)$. So $g(H) = 8$. In an example of the second case, $H \cap E$ is a $(2, 3)(I, I', 1)_0$ so $W = 16$ or 6. Then $g(H) = (1625 - t)/250$ or $(2625 - t)/250$. But by Sylow, t has to be a power of 5 and neither 1625 nor 2625 is. Hence $g(H) \neq 0$.

Remark. This type of argument, also seen in Lemma 2.5, using Proposition 1.4 to count conjugates of $[S^r]$ will be used frequently and will be referred to as the usual argument using proposition 1.4.

PROPOSITION 2.2. *Suppose F is a subfield of $K(5^n)$, $n \geq 3$, which has genus 0. Then F is a subfield of $K(25)$.*

Proof. Lemmas 2.7 and 2.8 show that the proposition is true for $n = 3$ and we proceed by induction, i.e. we suppose that a subfield of $K(5^{n-1})$, $n \geq 4$, of genus 0 is a subfield of $K(25)$. Consider F a subfield of $K(5^n)$. If F is a subfield of $K(5^{n-1})$, we are done by the induction hypothesis. If not, $F_1 = F \cap K(5^{n-1})$ has genus 0 and by the induction hypothesis is a subfield of $K(25)$. Considering the two cases, F_1 a subfield of $K(5)$ and F_1 a subfield of $K(25)$ of level 25 separately, we get a contradiction by the usual argument using Propositions 1.1–1.3.

3. $LF(2, 3^n)$

THEOREM 2. *The only subfields of $K(3^n)$, $n \geq 1$, which have genus 0 are a subfield of $K(3)$; a subfield of $K(9)$ of level 9 whose Galois group belongs to one of the 5 following classes: (1) H has order 9 and is either a subgroup of K_1^2 with $W = 2$, a $\Gamma_9^1(1)$ or a conjugate of $[S]$, (2) H has order 12, (3) H has order 18 and is either a $G''_{18}\{(III, a)\}$ or the right kind of $G''_{18}\{(II, b)\}$, (4) H has order*

27, (5) *H has order* 36; *and a subfield of* $K(27)$ *of level* 27 *whose Galois group is the right kind of* $(2, 3)(I, I', 1)_0$.

First note that any subfield of $K(3)$ has genus 0 and the rest of the proof will follow from Propositions 3.1 to 3.3. Second note that Gierster denotes a conjugate of T by Γ_3. Now suppose H is a subgroup of $LF(2, 9)$ of level 9. Simple calculations show that 3^3 is the highest power of 3 which can divide the order of H and that if $|H| = 2, 3, 4$ or 6, $g(H) \neq 0$. It also follows from easy calculations plus Gierster, pp. 356–360, that if $|H| = 3^3 \cdot 2$ or $3^3 \cdot 4$, H contains K_1^2. In this section r_0 will denote any fixed non-zero residue mod 3.

LEMMA 3.1. *If* $|H| = 9$, *there are* 3 *cases in which* $g(H) = 0$: (1) *H is a subgroup of K_1^2 with* $W = 2$, (2) *H is a* $\Gamma_9'(1)$ *or* (3) *H is a conjugate of* $[S]$.

Proof. If $|H \cap K_1^2| = 1$, $|H \cdot K_1^2| = 3^5$ which is impossible. If $|H \cap K_1^2| = 9$, H is a subgroup of K_1^2 and $g(H) = (18 - 9W)/9$. So $g(H) = 0$ if and only if $W = 2$. If $|H \cap K_1^2| = 3$, $g(H) = (18 - 3 \cdot r - 9W)/9$. So $g(H) = 0$ if and only if (1) $W = 0$ and $r = 6$ which is impossible since then $|H| > 9$; (2) $W = 1$ and $r = 3$ which says H is a $\Gamma_9'(1)$; (3) $W = 2$ in which case H is a conjugate of $[S]$ since $|H \cap K_1^2| = 3$ implies there is at most 1 conjugate of $[S^3]$ in H.

LEMMA 3.2. *Any group of order* 12 *has genus* 0.

Proof. If $|H \cap K_1^2| = 1$, H is a tetrahedral group so $r = 4$, $t = 3$ and $g(H) = 0$. If $|H \cap K_1^2| = 3$, H is one of 9 $G_{12}^1\{III\}$ [2,356] so $t = 7$. Hence $g(H) \leq (21 - 21)/12 = 0$ and since $g(H)$ is always non-negative, $g(H) = 0$.

LEMMA 3.3. *If* $|H| = 18$, *there are two cases for which* $g(H) = 0$: (1) *H is one of* 3 *conjugate* $G_{18}''\{(III, a)\}$ *or* (2) *H is one of* 18 *conjugate* $G_{18}''\{(II, \mathrm{b})\}$ *of the right kind.*

Proof. By Sylow H has one subgroup of order 9 and $t = 1$, 3 or 9. $|H \cap K_1^2| = 1$ or 3 yields an impossible order for $|H \cdot K_1^2|$. So $|H \cap K_1^2| = 9$ which says that $r = 0$ since no Γ_3 belongs to K_1^2 and that $W = 0$, 1 or 2. $g(H) = (27 - 3t - 9W)/18$ so that $g(H) = 0$ if and only if $W = 0$, $t = 9$; $W = 2$, $t = 3$. The first occurs if H is one of 3 conjugate $G_{18}''\{III, a)\}$ containing $1(1, 1)\{III\}$ and $9G_2$; the second if H is one of 18 conjugate $G_{18}''\{(II, b)\}$ containing $1(1, 1)\{II\}$ and $3G_6$. That not all groups of order 18 have genus 0 is shown by the existence of 18 $G_{18}''\{(III, b)\}$ containing $1(1, 1)\{III\}$ and $3G_6$ so that $g(H) = 1$.

LEMMA 3.4. *Any subgroup of order* 36 *has genus* 0.

Proof. $|H \cap K_1^2| \neq 1$ since then $|H \cdot K_1^2|$ would be too large and $|H \cap K_1^2| \neq 3$ since there are no such groups [2,356]. So $|H \cap K_1^2| = 9$ and there are two possibilities. H may be one of 9 conjugate $G_{36}''\{III, c\}$ or one of two types of $G_{36}''\{III, III, d\}$, each containing $1(1, 1)\{(III)\}$, $6G_6$ and $9G_2$. So in either case $W = 0$, $t = 15$ and $g(H) = 0$.

LEMMA 3.5. *Any subgroup of order* 27 *has genus* 0.

Proof. First if $H = K_1^2$, then $H = G(K(9) \mid K(3))$ and $g(H) = 0$. Otherwise $|H \cap K_1^2| = 9$ since, if not, $|H \cdot K_1^2|$ will be too large. So H may be one of 4 conjugate $\Gamma''_{27}(I, a)$ containing $1(1, 1)(I)$ and $9\Gamma_3$ so that $r = 9$, $W = 1$ and $g(H) = 0$. On the other hand, H may be a $(1, 2)(I, I)_0$ an example of which is given by

$$\{\pm(1 - 3(\xi + z), \xi, 0, 1 + 3(\xi + z))\}$$

where ξ describes all values mod 9 and z all values mod 3. By the usual argument using Proposition 1.4, $W = 3 + 1 = 4$ and $g(H) = 0$.

So we now have

PROPOSITION 3.1. *Suppose F is a subfield of $K(9)$ of level* 9. *Then F has genus* 0 *if and only if $G(K(9) \mid F) = H$ belongs to one of the following classes*:

(1) *H has order* 9 *and is either a subgroup of K_1^2 with $W = 2$, a $\Gamma'_9(1)$ or a conjugate of* $[S]$;

(2) *H has order* 12;

(3) *H has order* 18 *and is either a $G''_{18}\{III, a\}$ or the right kind of $G''_{18}\{II, b\}$*;

(4) *H has order* 27;

(5) *H has order* 36.

Now we consider subfields F of $K(27)$ and let $F_1 = F \cap K(9)$ and $H_1 = G(K(9) \mid F_1)$.

LEMMA 3.6. *Suppose F is a subfield of $K(27)$ of genus* 0 *and H_1 has order* 9. *Then F is a subfield of $K(9)$.*

Proof. If $|H \cap K_2^3| = 1$, $|H \cap K_1^3| \geq 3$ contradicting Proposition 1.1. Since F_1 has genus 0, there are 3 possibilities for H_1. First suppose H_1 is a subgroup of K_1^2. Then F_1 contains $K(3)$ and so $F \cap K(3) = K(3)$. Thus F contains $K(3)$, H is a subgroup of K_1^3, $|H \cap K_2^3| = 9$ and $|H| = 81$. H
H is either a

$$(2, 2)(I) \quad \text{or} \quad (2, 2)(I', 1)[2,338\text{–}339].$$

So H is conjugate to either

$$\{\pm(u - 3x, 3y, 0, u + 3x)\} \quad \text{or} \quad \{\pm(u - 3x, 3y, -9r_0y, u + 3x)\}$$

where x, y describe all values mod 9. Then by the usual argument using Proposition 1.4 either $W = 0 + 3 + 1 = 4$ and $g(H) = 4$ or $W = 0 + 0 + 1 = 1$ and $g(H) = 7$.

Suppose H_1 is conjugate to $[S]$. If $|H \cap K_2^3| = 3$, $|H| = 27$ and $H \cap K_1^3$ is cyclic of order 9. A conjugate of S has the form $\pm(a, b, c, d)$ where

$$((a + d)/2)^2 - 1 \equiv 0 \quad (3^n) \quad \text{and} \quad ad - bc \equiv 1 \quad (3^n).$$

So H_1 contains an element of this form and hence H contains an element

$$\alpha = \pm(a', b', c', d')$$

where $a'd' - b'c' \equiv 1$ (27) and $a' = a + 9k_1$, $b' = b + 9k_2$, $c' = c + 9k_3$, $d' = d + 9k_4$ where the k_i are integers. Then

$$\Delta' = ((a' + d')/2)^2 - 1 \equiv 9s_0 \quad (27)$$

where $s_0 = 0, 1, 2$. So $[\alpha]$ is either a $G_{27}(I)$ or $G_{27}(I, 1)$ and has order 27. Thus H is cyclic, $W \leq 3$ and $g(H) \geq 13$. If $|H \cap K_2^3| = 9$, $|H| = 81$ and $|H \cap K_1^3| = 27$. If $W = 0$, $g(H) > 0$. If $W > 0$, H is either a $(1, 3)(I, I)_0$ or one of 2 types of $(1, 3)(I, I', \epsilon)$, $\epsilon = 1$ or 2 [2,345–351]. As a $(1, 3)(I, I)_0$ H is conjugate to

$$\{\pm(u + 3\xi + 9z, \xi, -9\xi, u-(3\xi + 9z))\}$$

and as a $(1, 3)(I, I', 1)_0$ H is conjugate to one of

$$\{\pm(u + 3\xi + 9z, \xi, 9r_0\xi, u-(3\xi + 9z))\}$$

where ξ describes all values mod 27, z all values mod 3. In either case $W = 3 + 3 + 1 = 7$ so that $g(H) = 1$. As a $(1, 3)(I, I', 2)_0$, H is conjugate to one of

$$\{\pm(u + 3\xi + 9z, \xi, 3r_0\xi - 9\xi, u-(3\xi + 9z))\}$$

with ξ, z as above. Here $W = 0 + 0 + 1$ and $g(H) = 7$.

Suppose $H_1 = \Gamma_9'(1)$. If $|H \cap K_2^3| = 3$, $|H| = 27$ and $H \cap K_1^3$ is cyclic of order 9. So [2,364–366] H is one of 3 types of 108 $\Gamma_{27}'(I', 2)$, $W \leq 2$, $r = 3$ and $g(H) \geq 15$. If $|H \cap K_2^3| = 9$, $|H| = 3^4$ and $|H \cap K_1^3| = 27$. So [2,364–366], H contains either a $(1, 2)(I, I)$ or a $(1, 2')(I, I', 1)$. An example of a $(1, 2)(I, I)$ is given by

$$\{\pm(u + 9(\xi + z), 3\xi, 0, u - 9(\xi + z))\}$$

with ξ, z as above and $W = 0 + 3 + 1 = 4$. An example of a $(1, 2)(I, I', 1)$ is given by

$$\{\pm(u + 9(\xi + z), 3\xi, 9\xi r_0, u - 9(\xi + z))\}$$

with ξ, z as above and so $W = 0 + 0 + 1 = 1$. Now H itself belongs to one of the following classes and has the genus indicated: (1) H is one of 36 conjugate $\Gamma_{81}''(I, I)$, $W = 4$, $r = 9$ and $g(H) = 3$; (2) H is one of 12 conjugate $\Gamma_{81}''(I, I', 1, a)$, $W = 1$, $r = 27$ and $g(H) = 4$; (3) H is one of 2 types of 12 $\Gamma_{81}''(I, I', 1, b)$, $W = 1$, $r = 0$, $g(H) = 7$; (4) H is one of 36 conjugate $\Gamma_{81}''(I, I', 1, c)$, $W = 1$, $r = 9$ and $g(H) = 6$. So $g(H) > 0$ in all cases.

LEMMA 3.7. *Suppose F is a subfield of $K(27)$ of genus 0 and H_1 has order 12, 18 or 36. Then F is a subfield of $K(9)$.*

Proof. Suppose $|H_1| = 12$. If $|H \cap K_2^3| = 1$, H is a tetrahedral group and $g(H) = 43$. If $|H \cap K_2^3| = 3$, $|H| = 36$ and $H \cap K_1^3$ is cyclic of order 9. Then $W \leq 2$ and by Sylow, $t \leq 27$ so that $g(H) \geq 22/4$. If $|H \cap K_2^3| = 9$, $|H| = 3^3 \cdot 4$ and $|H \cap K_1^3| = 27$. So [2, pp. 345–352], H is one of 2 types of 81 $G_{108}''\{(III, III, d)\}$ for which $W = 0$ and $t \leq 39$ so that $g(H) \geq 4$.

Suppose $|H_1| = 18$ or 36. If $|H \cap K_2^3| = 1$ or 3, one gets a contradiction to Proposition 1.1 or 1.2. If $|H \cap K_2^3| = 9$, then $|H| = 3^4 \cdot k$ where $k = 2$ or 4 and $|H \cap K_1^3| = 3^4$. So $H \cap K_1^3$ is either a $(2, 2)(I)$ or a $(2, 2)(I', 1)$. But [2, pp. 351–361] there are no groups of order $3^4 \cdot k$ containing either of these.

LEMMA 3.8. *Suppose F is a subfield of $K(27)$ of genus 0 and H_1 has order 27. Then either F is a subfield of $K(9)$ or H belongs to the right kind of $(2, 3)(I, I', 1)_0$.*

Proof. If $|H \cap K_2^3| = 1$ or 3, one gets the usual contradiction using Proposition 1.1 or 1.2. If $|H \cap K_2^3| = 9$, then $|H| = 3^5$ and $|H \cap K_1^3| = 3^4$. Suppose H does not contain any Γ_3 or Γ_9. Then H is either a $(2, 3)(I, I)_0$ or one of two types of $(2, 3)(I, I', 1)_0$. An example of the first is given by

$$\{\pm(u + 3(3\xi + z), \xi, 0, u - 3(3\xi + z))\}$$

where ξ describes all values mod 27 and z all values mod 9. Then $W = 3 + 3 + 1 = 7$ and $g(H) = 1$. An example of the second is given by

$$\{\pm(u + 3(3\xi + z), \xi, 9r_0\xi, u - 3(3\xi + z))\}$$

where ξ, z are as above. If $r_0 \equiv 1\ (3)$, $s(1) = 0$; if $r_0 \equiv 2\ (3)$, $s(1) = 6$. In either case, $s(3) = 3$ and $s(9) = 1$. So $W = 4$ or 10 and $g(H) = 2$ or 0 depending on whether $r_0 \equiv 1$ or $2\ (3)$.

Suppose H contains a Γ_3 or Γ_9. Then [2, pp. 364–366] H belongs to one of the following classes: (1) 12 conjugate $\Gamma_{35}''(a)$; (2) 12 conjugate $\Gamma_{35}''(b)$; (3) 12 conjugate $\Gamma_{35}''(c)$. In all three cases, to compute W we need to analyze a $(2, 2)(I', 1)(s_0/3) = -1$ of which

$$\{\pm(u + 3y, 3(y + z), 9z, u - 3y)\}$$

where z and y describe all values mod 9 is an example. So $W = 0 + 0 + 1 = 1$. Also $r = 27$, 0 or 54 in cases (1), (2) or (3) respectively and thus $g(H) = 2$, 3 or 1.

PROPOSITION 3.2. *Suppose F is a subfield of $K(27)$ of level 27. Then F has genus 0 if and only if $G(K(27) \mid F)$ has order 3^5 and is a $(2, 3)(I, I', 1)_0$ of the proper type.*

Proof. If F_1 is a subfield of $K(3)$, F is a subfield of $K(3)$ by the usual arguments using Propositions 1.1–1.3. So we can assume F_1 has level 9 in $K(9)$ and the proposition then follows from Lemmas 3.6–3.8.

LEMMA 3.9. *Suppose F is a subfield of $K(81)$ of genus 0 and $F_1 = F \cap K(27)$ is a subfield of $K(9)$. If $H_1 = G(K(9) \mid F_1)$ has order 9, then F is a subfield of $K(27)$.*

Proof. Since F_1 has genus 0, H_1 is one of the following types: (1) a subgroup of K_1^2, $W = 2$, (2) a conjugate of [S], (3) a $\Gamma_9'(1)$. In any case if

$|H \cap K_3^4| = 1$ or 3 and in case (1) if $|H \cap K_3^4| = 9$, we get the usual contradiction using Propositions 1.1–1.3. In cases (2) and (3) with $|H \cap K_3^4| = 9$, we obtain $|H \cap K_1^4| = 3^6$ and $|H| = 3^7$. In case (2), H is either one of 3 conjugate $(3, 4)(I, I)_0$ such as

$$\{\pm(u + 27\xi + 3z, \xi, 0, u - (27\xi + 3z))\}$$

where ξ describes all values mod 81 and z all values mod 27 or it is one of 2 types of $(3, 4)(I, I', 1)_0$ such as

$$\{\pm(u + 27\xi + 3z, \xi, 27r_0\xi, u-(27\xi + 3z))\}$$

where ξ, z are as above. But on reduction mod 9 both of these groups have order 27 and hence can not be one of the H_1's which have order 9. In case (3), Gierster [2, pp. 364–366] has no groups of order 3^7 of the proper type.

LEMMA 3.10. *Suppose F is a subfield of $K(81)$ of genus 0 and $F_1 = F \cap K(27)$ is a subfield of $K(9)$. If $H_1 = G(K(9) \mid F_1)$ has order 12 or $9 \cdot k$ where $k = 2, 3$ or 4, then F is a subfield of $K(27)$.*

Proof. The only case in which one does not get the usual contradiction to Propositions 1.1–1.3 is the one in which $|H_1| = 12$ and $|H \cap K_3^4| = 9$. But then H is of order $3^6 \cdot 4$ with $H \cap K_1^4$ a (3, 3) and Gierster, pp. 357–360, has no such subgroups.

LEMMA 3.11. *Suppose F is a subfield of $K(81)$ of genus 0 and $F_1 = F \cap K(27)$ is a subfield of $K(27)$ of level 27. Then F is a subfield of $K(27)$.*

Proof. Since F_1 has level 27, H_1 has order 3^5 by proposition 3.2. If $|H \cap K_3^4| = 1$ or 3, we get the usual contradictions to Proposition 1.1 or 1.2. If $|H \cap K_3^4| = 9$, then $|H| = 3^7$ and $|H \cap K_1^4| = 3^6$. Then H is conjugate to one of the two groups given in Lemma 3.9. For the $(3, 4)(I, I)_0$ we have $W = 9 + 3 + 3 + 1 = 16$ and $g(H) = 4$. For the $(3, 4)(I, I', 1)_0$ we have $W = 0 + 3 + 3 + 1 = 7$ and $g(H) = 7$.

PROPOSITION 3.3. *Suppose F is a subfield of $K(3^n)$, $n \geq 4$ and F has genus 0. Then F is a subfield of $K(27)$.*

Proof. The proof is by induction on n. Let $n = 4$ and $F_1 = F \cap K(27)$. If F_1 has level 3, $F \subset K(27)$ follows from the usual argument using Propositions 1.1–1.3. If F_1 has level 9 or 27, $F \subset K(27)$ follows from Lemmas 3.9–3.11. Now let $n \geq 5$ and assume a subfield of $K(3^{n-1})$ of genus 0 is contained in $K(27)$. Then $F_1 = F \cap K(3^{n-1})$ is a subfield of $K(27)$ and supposing F is not a subfield of $K(3^{n-1})$ leads to a contradiction by the usual argument using Propositions 1.1–1.3. So $F \subset K(3^{n-1})$ and, by the induction hypothesis, is a subfield of $K(27)$.

BIBLIOGRAPHY

1. J. GIERSTER, *Die Untergruppen der galois'schen Gruppe der Modulargleichungen fur den Fall eines primzahligen Transformationsgrades*, Math. Ann., vol. 18 (1881), pp. 319-365.

2. ———, *Uber die galois'sche Gruppe der Modulargleichungen, wenn der Transformationsgrad die Potenz einer Primzahl > 2 ist*, Math. Ann., vol. 26 (1886), pp. 309–368.
3. R. C. GUNNING, *Lectures on modular forms*, Princeton University Press, Princeton, 1962.
4. D. L. McQUILLAN, *Some results on the linear fractional group*, Illinois J. Math., vol. 10 (1966), pp. 24–38.
5. ———, *Classification of normal congruence subgroups of the modular groups*, Amer. J. Math. vol. 87 (1965), pp. 285–296.
6. ———, *On the genus of fields of elliptic modular functions*, Illinois J. Math., vol. 10 (1966), pp. 479–487.

UNIVERSITY OF CONNECTICUT
STORRS, CONNECTICUT