SUBFIELDS OF $K(2^n)$ 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 $a \equiv d \equiv 1 \pmod{n}$ and $b \equiv c \equiv 0 \pmod{n}$. 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. The conjecture has been proven if n is prime to $2 \cdot 3 \cdot 5$ or is a power of 3 or 5 [5, 1]. In this paper we show that the conjecture is true if n is a power of 2.

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 H equals 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 $\pm (a, b, c, d)$.

$$I = \pm (1, 0, 0, 1); \qquad T = \pm (0, -1, 1, 0);$$

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

T and S generate $LF(2, 2^n)$ and $R = TS$. H will be a subgroup of $LF(2, 2^n)$; $g(H) =$ 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. φ_r^n will denote the natural homomorphism from $LF(2, 2^n)$ to $LF(2, 2^r)$, $1 \leq r \leq n$,

Received April 29, 1970.