RAMIFICATION IN ELLIPTIC MODULAR FUNCTION FIELDS

DONALD L. McQUILLAN

1. The field of elliptic modular functions of level n is a finite galois extension K of the field $\mathbf{C}(j)$ generated over $\mathbf{C}$ by the Weierstrass absolute invariant j. Furthermore, the galois group is $\mathrm{LF}(2, n) = \mathrm{SL}(2, Z/nZ)/\pm I_2$ and the genus g of K is given by

$$2g - 2 = 1/12\cdot(n-6)n^2 \prod_{q|n} (1 - 1/q^2)$$

for $n>2$ ($g=0$ for $n=1, 2$). If p is a prime number not dividing n and if k is an algebraic closure of $\mathrm{GF}(p) = Z/pZ$ (k can also be an algebraic closure of $\mathbf{Q}$), Igusa [**4**] constructed a galois extension of $k(j)$ with the same galois group and the same genus. On the other hand, if the level n is a prime number q, Hecke [**3**] proved that $K/\mathbf{C}(j)$ is uniquely determined by the two properties. The purpose of this short note is to extend this theorem of Hecke in the following way:

THEOREM. *Let $K/k(j)$ be a galois extension of genus g ($n=q$) with* $\mathrm{LF}(2, q)$ *as galois group. Then, the ramification of $K/k(j)$ is uniquely determined. Hence, (as in Igusa's extension) $K/k(j)$ is ramified over one point with index q and over two other points with indices* 2, 3 *for $p\neq 2, 3$, over one other point with the tetrahedral group as inertia group (second ramification group = trivial) for $p=2$ and with the dihedral group of order* 6 *as inertia group (second ramification group = trivial) for $p=3$. Moreover, in the case $p\neq 2, 3$, (if we fix three points with ramification indices* 2, 3, *q) the extension $K/k(j)$ is uniquely determined.*

2. We shall start proving the theorem. Since the case $q=2$ can be treated separately (and rather easily), we shall assume that q is an odd prime. Suppose that K is ramified over $k(j)$ at $j=a_1, a_2, \cdots, a_w$ and that

$$T(a_i) \supset V_1(a_i) \supset V_2(a_i) \supset \cdots$$

is a sequence of the inertia group and the first, second, $\cdots$ ramification groups at a place of K lying over a_i. Then, it is a normal sequence (unique up to an inner automorphism of $\mathrm{LF}(2, q)$) such that $V_1(a_i)$ is the unique p-Sylow group of $T(a_i)$ with cyclic factor group. In particular, the commutator group of $T(a_i)$ has to be a p-group. Now, thanks to Gierster [**1**], we know all subgroups of $\mathrm{LF}(2, q)$: A subgroup of $\mathrm{LF}(2, q)$ is

Received by the editors March 26, 1962.

(i) a cyclic group C_m of order m where $m=q$, $m|(q-1)/2$ or $m|(q+1)/2$,

(ii) a dihedral group D_{2n} of order $2n$ where $n|q-1$ or $n|q+1$,

(iii) a metacyclic group of order qt where $t|(q-1)/2$ with C_q as commutator group, or

(iv) a tetrahedral, octahedral or icosahedral group. Because of the property of $T(a_i)$ mentioned above, candidates for $T(a_i)$ are limited. In fact, they are C_m in (i), D_{2n} in (ii) with $n=p^r$ (p odd) and the tetrahedral group. This being remarked, the "relative genus formula" applied to $K/k(j)$ gives

$$\sum_i (E_i - 1)/e_i = (2 - w) + 1/6 - 1/q$$

where

$$e_i = \text{ord. } T(a_i),$$

$$E_i = (\text{ord. } V_1(a_i) - 1) + (\text{ord. } V_2(a_i) - 1) + \cdots .$$

Since the right side of the genus formula is not integral at q, at least one e_i, say e_1, is a multiple of q. Then $T(a_1)$ is either C_q or the tetrahedral group (with $q=3$, $p=2$). In the second case, K contains a cyclic subextension of $k(j)$ of degree 3, hence e_2, say, is also a multiple of $q=3$. If $T(a_2)$ is again the tetrahedral group, we get $e_1=e_2=12$, $E_1, E_2 \geqq 3$, and this will bring a contradiction. Hence, we can always assume that $T(a_1)$ is C_q. This implies

$$\sum_{i>1} (E_i - 1)/e_i = (2 - w) + 1/6.$$

Since $e_i \geqq 2$ and $E_i \geqq 0$, therefore, we have $w \leqq 3$ and certainly $w \geqq 2$. Suppose, first, that $w=3$. Then, we see immediately that $e_2=2$. $e_3=3$ with $E_2=E_3=0$, hence $p\neq 2, 3$. Suppose, next, that $w=2$, Then, we have $e_2=6(E_2-1)$ and this is a multiple of p. Consequently, $T(a_2)$ is C_m in (i), D_{2n} in (ii) with $n=3^r$ or the tetrahedral group (with $V_2(a_2)=1$). In the second case, we see that $T(a_2)=D_6$ (with $V_2(a_2)=1$). We shall show that the first possibility has to be rejected entirely.

3. We recall [1] that subgroups in (i), (iii) are unique up to inner automorphisms of LF$(2, q)$. We denote by Σ the subextension of $k(j)$ which corresponds (by the theory of Galois) to the group of linear transformations $x \rightarrow a^2x+b$ with a in GF$(q)^*$ (=multiplicative group of GF(q)) and b in GF(q). Using Hilbert's galois theory, we shall calculate the relative genus formulas for K/Σ and for $\Sigma/k(j)$ (cf. [**4**, pp. 473–474]). In doing this, we can assume that $T(a_1)$ is the group of

linear transformations $x \to x+b$ with b in GF(q). Suppose, first, that $T(a_2)=C_{e_2}$ with $e_2 \mid (q-1)/2$. Then, we can assume that $T(a_2)$ is the subgroup of order e_2 of the group of linear transformations $x \to a^2 x$ with a in $GF(q)^*$. Thus, if g_0 is the genus of Σ, we get

$$2g-2=(q-1)^2/2+q(q-1)/e_2\cdot((e_2-1)+E_2)+q(q-1)/2\cdot(2g_0-2),$$
$$2g_0-2=(q-1)+(q-1)/e_2\cdot((e_2-1)+E_2)-2(q+1).$$

By eliminating g_0, we get $q(q+1)(q-1)=0$. This is a contradiction. Suppose, next, that $T(a_2)=C_{e_2}$ with $e_2 \mid (q+1)/2$. Then, in the same way we get

$$2g-2=(q-1)^2/2+q(q-1)/2\cdot(2g_0-2),$$
$$2g_0-2=(q-1)+(q+1)/e_2\cdot((e_2-1)+E_2)-2(q+1),$$

and hence $q(q+1)(q-1)=0$. This is a contradiction.

4. Finally, we shall indicate how the uniqueness of $K/k(j)$ follows from the information about ramifications in the case $p\neq 2$, 3. Suppose that $K_1/k(j)$, $K_2/k(j)$ are two such extensions, i.e. with the same genus g and with $LF(2, q)$ as galois group. By an automorphism of $k(j)$, we can make an adjustment so that $K_1/k(j)$, $K_2/k(j)$ are ramified over the same three points a_1, a_2, a_3 with the same indices. Consider their compositum $\Omega/k(j)$ (in some algebraic closure of $k(j)$). Then $\Omega/k(j)$ is ramified only over a_1, a_2, a_3 and, in fact, tamely. Let G be the galois group of $\Omega/k(j)$ and let H_1, H_2 be the normal subgroups of G which correspond to K_1, K_2. Then, by a general result of Grothendieck [2], we can pick σ_1, σ_2, σ_3 from inertia groups over a_1, a_2, a_3 which generate G and which satisfy $\sigma_1\sigma_2\sigma_3=1$. Let σ_i', σ_i'' be the images of σ_i in G/H_1, G/H_2. Then, by a lemma of Hecke [3, p. 574], there exists an isomorphism $G/H_1 \simeq G/H_2$ in which σ_i' and σ_i'' correspond to each other. This is possible (if and) only if $H_1=H_2$ completing the proof.

References

1. J. Gierster, *Die Untergruppen der Galois'schen Gruppe der Modulargleichungen für den Fall eines primzahligen Transformation-grades*, Math. Ann. **18** (1881), 319–360.

2. A. Grothendieck, *Géométrie formelle et géométrie algébrique*, Seminaire Bourbaki, May, Secrétariat Mathématique, Paris, Exposé 182, 1959.

3. E. Hecke, *Die eindeutige Bestimmung der Modulfunktionen q-ter Stufe durch algebraische Eigenschaften*, Collected Works, Vandenhoeck and Ruprecht, Göttingen, 1959, pp. 568–576.

4. J. Igusa, *Fibre systems of Jacobian varieties*. III, *Fibre systems of elliptic curves*, Amer. J. Math. **81** (1959), 453–476.

University College Galway, Ireland