J. Austral. Math. Soc. (*Series A*) 26 (1978), 385–409

ON NORMAL CLOSURES RELATED TO ELLIPTIC CURVES

D. J. LEWIS and PATRICK MORTON

To Kurt Mahler on his 75th birthday

(Received 12 June 1978)

Communicated by J. Coates

Abstract

Let $F(z)$ be a polynomial with coefficients in a perfect field k and let K be the normal closure of $k(z)$ over $k(F)$. All polynomials for which the genus of K over k is one are determined; they depend in part on the characteristic of k. Some results for higher genus are given.

Subject classification (*Amer. Math. Soc.* (*MOS*) *1970*): 12 F 10.

1. Introduction

We are interested in studying the normal closures of a particular class of extensions of function fields. The extensions we consider are of the form $k(z)/k(F(z))$, where k is a perfect field and F is a polynomial in z. The case in which $k(z)$ is normal over $k(F)$ has been discussed in Bremner and Morton (1978). Here we consider those polynomials F for which the normal closure K of $k(z)/k(F)$ is larger than $k(z)$, and we restrict our attention to the situation in which the genus of K is greater than zero.

Since the isomorphism type of the extension $k(z)/k(F)$ is invariant under the substitutions

$$z \to az+b, \quad F \to cF+d, \quad a,b,c,d \text{ in } k, \quad ac \neq 0,$$

The first author is partially supported by a National Science Foundation grant. The second author is a National Science Foundation Predoctoral Fellow.

it follows that for two polynomials E, F related by

$$E(z) = cF(az+b)+d,$$

the corresponding normal closures are isomorphic. We shall say that polynomials E, F satisfying this condition are linearly equivalent. We therefore need consider only one representative of a given equivalence class in order to study K.

The results we prove are as follows. In Section 2 we derive necessary conditions for K to be the normal closure of $k(z)/k(F)$, in terms of the automorphism group of K/k. From these conditions it follows easily that the genus γ of K grows as a power of $f = \deg F$ when $\gamma > 0$ (see Theorem 1).

The rest of the paper is concerned with the case $\gamma = 1$, when K is an elliptic function field. In this case we determine the exact classes of polynomials F which can arise (see Theorems 2, 3). The discussion proceeds differently according to the characteristic p of k. In Section 4 we discuss the case $p \neq 2, 3$; in Section 5 the case $p = 3$; and in Section 6, $p = 2$. In each case we determine the relevant Galois groups completely; the respective expressions for F are then easily determined. The complete list of polynomials is contained in Tables 1 and 3 of Section 7. In particular, the number of classes for which $\gamma = 1$ is always finite when k is algebraically closed.

This raises the following question: if an algebraically closed field k and $\gamma_0 \geq 2$ are given, "how many" classes of polynomials over k are there for which $\gamma = \gamma_0$? Is the number of classes finite? (By the results of Bremner and Morton (1978) this is false for $\gamma_0 = 0$; moreover the degrees of possible F's are unbounded.) The key to this question no doubt lies in the study of the Jacobian of the normal closure K.

2. Preliminary Results

In this and the next four sections we assume that z is an indeterminate over the perfect field k, and that $F(z)$ is a polynomial in z with coefficients from k.

We are interested in the normal closure K of the extension $k(z)/k(F)$. Note first that the irreducible equation over $k(F)$ satisfied by z is

$$F(t)-F(z) = 0. \tag{1}$$

Thus the degree of z over $k(F)$ is equal to $\deg F = f$, and K is the splitting field of (1) over $k(F)$. Since we are primarily interested in K, we shall assume that the extension $k(z)/k(F)$ is separable; by (1) this is the same as requiring that F not be a pth power in $k[z]$, where p is the characteristic of k.

It will also be convenient to assume that k is algebraically closed. If k is not equal to its algebraic closure $\bar{k}$, then by virtue of the fact that (1) is the irreducible equation over $\bar{k}(F)$ satisfied by z, the constants extension $\bar{K} = K\bar{k}$ is the normal

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

closure of $\bar{k}(z)/\bar{k}(F)$. Moreover the genus of $\bar{K}$ equals the genus of K. (For the basic facts concerning algebraic function fields in one variable see Hasse (1963).) From this it is easily seen that the restriction $k = \bar{k}$ does not affect the results of this section. For the case $\gamma = 1$ we shall remove this restriction in Section 7.

We now let G and H be the Galois groups of the extensions $K/k(z)$ and $K/k(F)$. Then $G \subseteq H \subseteq A$, where A is the automorphism group of K/k, and by Galois theory we have

$$h = f \cdot g, \tag{2}$$

where

$$h = |H| = [K: k(F)] \quad \text{and} \quad g = |G| = [K: k(z)]. \tag{3}$$

The following facts are immediate consequences of the assumption that K is the normal closure of $k(z)/k(F)$:

(4) h divides $f!$ and g divides $(f-1)!$;

(5) No non-trivial subgroup of G is normal in H. (In particular, if N is a normal subgroup of H and C is a characteristic subgroup of N, then $C \subseteq G$ implies $C = 1$.)

Now let $\mathfrak{z}$ be the denominator of the divisor (z), and let $\mathfrak{o}$ be a prime divisor of K (automatically of degree 1) dividing $\mathfrak{z}$. Since $\mathfrak{z}$ is a prime divisor of $k(z)$ we have

$$\mathfrak{z} = \prod_{\sigma} \mathfrak{o}^{\sigma}.$$

where σ runs over certain automorphisms in G. Since the degree of $\mathfrak{z}$ as a divisor in K is $[K: k(z)] = g$, and since each $\mathfrak{o}^{\sigma}$ has degree 1, σ must run through all the automorphisms in G. Thus

$$\mathfrak{z} = \prod_{\sigma \in G} \mathfrak{o}^{\sigma}. \tag{6}$$

It follows that the power of $\mathfrak{o}$ dividing $\mathfrak{z}$ is $|G \cap A_{\mathfrak{o}}|$, where $A_{\mathfrak{o}}$ is the subgroup of automorphisms in A which fix $\mathfrak{o}$. We shall denote $G \cap A_{\mathfrak{o}}$ by $G_{\mathfrak{o}}$ and $|G_{\mathfrak{o}}|$ by $g_{\mathfrak{o}}$.

The same argument applied to the denominator $\mathfrak{z}'$ of the divisor $(F(z))$ shows that

$$\mathfrak{z}' = \prod_{\sigma \in H} \mathfrak{o}^{\sigma}, \tag{7}$$

and therefore by (6) that

$$\Big(\prod_{\sigma \in G} \mathfrak{o}^{\sigma}\Big)^{f} = \prod_{\sigma \in H} \mathfrak{o}^{\sigma}.$$

It follows that

$$h_{\mathfrak{o}} = f g_{\mathfrak{o}} \quad \text{where} \quad h_{\mathfrak{o}} = |H \cap A_{\mathfrak{o}}| = |H_{\mathfrak{o}}|. \tag{8}$$

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

If A_0 is a finite group, then by (8) we have that

$$f \text{ is a divisor of } |A_0|. \tag{9}$$

In particular, if $K \neq k(z)$, then (9) implies

$$|A_0| > 2. \tag{10}$$

Otherwise $f \leqslant 2$ and $k(z)/k(F)$ is already normal.

We now draw the following further conclusion from (9).

THEOREM 1. *If the genus γ of the normal closure K of $k(z)/k(F)$ is at least 2, then*

$$\gamma \geqslant \tfrac{1}{84}f + 1 \quad \textit{for } p = 0$$

and

$$\gamma \geqslant (3f/224)^{1/4} \quad \textit{for } p \neq 0,$$

where $f = \deg F$ and p is the characteristic of k.

If $\gamma = 1$, then

$$f \mid 24. \tag{11}$$

PROOF. If $p = 0$ and $\gamma \geqslant 2$, then the Hurwitz estimate (see Roquette (1970b)) for the order of the automorphism group A of K gives

$$|A_0| \leqslant |A| \leqslant 84(\gamma - 1);$$

this implies by (9) that $f \leqslant 84(\gamma - 1)$.

If $p \neq 0$, then it follows from the estimates for $|A|$ given by Stichtenoth (1973) that†

$$|A_0| \leqslant |A| \leqslant \tfrac{1}{3} \cdot 224 \cdot \gamma^4,$$

and therefore $f \leqslant \frac{1}{3} \cdot 224 \cdot \gamma^4$.

If $\gamma = 1$, then by Deuring (1947) the order of A_0 divides 24; this implies (11). (See also the remarks in Section 3 for this case.)

3. Fields of genus one

Henceforth we assume that the genus of K is 1. This together with the equations (2)–(11) will impose such stringent conditions on H and G that we will be able to determine the possible polynomials F exactly. In this section we review the parts of the theory of elliptic function fields we shall need (we refer the reader to Hasse's papers (1936); see also Roquette (1970a) and Cassels (1966)), and we prove some preliminary lemmas.

† Stichtenoth proves $|A| \leqslant 16\gamma^4$, unless $\gamma = \frac{1}{2}p^n(p^n - 1)$ and $|A| = p^{3n}(p^{3n} + 1)(p^{2n} - 1)$ with $p^n \geqslant 3$. The estimate above follows from the fact that $f(x) = 16x^3(x^3 + 1)(x^2 - 1)/x^4(x - 1)^4$ $(= |A|/\gamma^4$ for $x = p^n)$ is decreasing for $x > 1$ and is 224/3 when $x = 3$.

To begin with, the fact $\gamma = 1$ implies by the Riemann–Roch theorem (see Hasse (1963)) that for any integral divisor $\mathfrak{a}$ of K and the associated vector space (over k)

$$L\left(\frac{1}{\mathfrak{a}}\right) = \left\{u \text{ in } K;\ (u) = \frac{\mathfrak{n}}{\mathfrak{a}} \text{ with an integral divisor } \mathfrak{n}\right\},$$

we have

$$\dim L\left(\frac{1}{\mathfrak{a}}\right) = \deg \mathfrak{a}. \tag{12}$$

This implies further that the divisor classes of degree 0 are uniquely represented by the divisors $\mathfrak{p}/\mathfrak{o}$, where $\mathfrak{o}$ is a fixed prime divisor of $\mathfrak{z}$ and $\mathfrak{p}$ runs through all prime divisors of K. The divisor class group of degree zero thus induces an addition on the set of primes, defined by

$$\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 = \mathfrak{o} \quad \text{if} \quad \frac{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}{\mathfrak{o}^3} \sim 1, \tag{13}$$

where $\sim$ denotes linear equivalence (that is, $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\mathfrak{a}\mathfrak{b}^{-1} = (u)$ with u in K).

We denote the group of primes with this addition by D_0; the zero element of D_0 is $\mathfrak{o}$. We shall need the following result of Hasse (1936), Part I, concerning the structure of D_0: the subgroup H_n of primes $\mathfrak{p}$ for which $n\mathfrak{p} = \mathfrak{o}$ is of type

$$H_n \cong C_n \times C_n \quad \text{for } p \nmid n, \tag{14}$$

where C_n denotes a cyclic group of order n; thus $|H_n| = n^2$ for $p \nmid n$.

As is well known, a generating equation for K can be given using the prime $\mathfrak{o}$, as follows. Let x be a non-constant element of $L(1/\mathfrak{o}^2)$ and let $1, x, y$ be a basis for $L(1/\mathfrak{o}^3)$. Then x and y satisfy an equation

$$f(x, y) = 0 \tag{15}$$

which is quadratic in y and cubic in x. Furthermore, the prime divisors $\mathfrak{p} \neq \mathfrak{o}$ of K are in 1–1 correspondence with the solutions $(x_\mathfrak{p}, y_\mathfrak{p})$ in k of (15), where the correspondence is determined by

$$x \equiv x_\mathfrak{p}, \quad y \equiv y_\mathfrak{p} \pmod{\mathfrak{p}}. \tag{16}$$

The point $(x_\mathfrak{p}, y_\mathfrak{p})$ is the so-called "center" of the prime $\mathfrak{p}$. The prime $\mathfrak{o}$ corresponds to the formal solution (∞, ∞) of (15). Moreover the addition in D_0 induces an addition on the solutions $(x_\mathfrak{p}, y_\mathfrak{p})$ of (15), including (∞, ∞), which agrees with the well-known "secant–tangent" construction. In particular (see Hasse (1936), Part II), if $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ are distinct from each other and $\mathfrak{o}$, then (13) is equivalent to

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

the determinant relation

$$\begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} = 0, \quad \text{where } (x_i, y_i) \leftrightarrow \mathfrak{p}_i. \tag{17}$$

We now discuss the automorphism group A of K/k. As Hasse (1936), Part II, shows, A contains an abelian normal subgroup T, which is isomorphic to D_0 by means of the correspondence

$$\tau \leftrightarrow \mathfrak{p} \quad \text{if} \quad \mathfrak{q}^\tau = \mathfrak{q} + \mathfrak{p} \quad (\text{in } D_0) \tag{18}$$

for all prime divisors $\mathfrak{q}$ of K. The group T is independent of the choice of $\mathfrak{o}$, and an element τ in T is determined by its action on $\mathfrak{o}$. It is easy to see using this remark that

$$\tau \leftrightarrow \mathfrak{p} \quad \text{implies} \quad \sigma^{-1}\tau\sigma \leftrightarrow \mathfrak{p}^\sigma \quad \text{for any } \sigma \in A_0, \tag{19}$$

where A_0 is (as in Section 2) the subgroup of A which fixes $\mathfrak{o}$.

The subgroup T_n of T consisting of those τ with $\tau^n = 1$ corresponds to the subgroup H_n of D_0, so that by (14) we have

$$T_n \cong C_n \times C_n \quad \text{for } p \nmid n. \tag{20}$$

In addition, the quotient group A/T is finite, and the cosets are uniquely represented by the elements of A_0; hence

$$A/T \cong A_0. \tag{21}$$

Thus all elements of A are given uniquely in the form $\sigma\tau$ with σ in A_0 and τ in T.

Using these remarks, the action of an automorphism on x and y, and hence on K, can be determined: if τ lies in T and corresponds by (18) to the prime $\mathfrak{p}$, then

$$(x^\tau, y^\tau) = (x, y) - (x_\mathfrak{p}, y_\mathfrak{p}), \tag{22}$$

where (x, y) is treated as a "generic" point on (15), and the addition is performed using (17). (For the reader's convenience a proof of this fact is included in the Appendix.) If σ lies in A_0, then

$$\begin{aligned} x^\sigma &= ax + b, \\ y^\sigma &= cy + dx + e \end{aligned} \tag{23}$$

for some constants $a, \ldots, e$ in k and $ac \neq 0$. Now $(x^{\sigma\tau}, y^{\sigma\tau})$ may be determined by applying first (23) and then (22).

The group A_0 may be worked out in a particular example by solving for all the sets of constants in (23) for which (x^σ, y^σ) satisfies (15). Using this approach one

can verify that A_0 has order dividing 24 (see Deuring (1947)), a fact which we used in Section 2. More precisely, we have by Deuring's results that

$$|A_0| = \begin{cases} 2, 4 \text{ or } 6 & \text{if } p \neq 2,3, \\ 2 \text{ or } 12 & \text{if } p = 3, \\ 2 \text{ or } 24 & \text{if } p = 2. \end{cases} \tag{24}$$

We will also need the following lemmas concerning A_0. For the proofs see the Appendix.

LEMMA 1. *The group A_0 has a unique element ε of order 2. This element lies in the center of A_0 and satisfies*

$$\mathfrak{p} + \mathfrak{p}^{\varepsilon} = \mathfrak{o} \quad \textit{and} \quad \varepsilon^{-1}\tau\varepsilon = \tau^{-1} \tag{25}$$

for all prime divisors $\mathfrak{p}$, and all τ in T.

LEMMA 2. *If $\mathfrak{p} \neq \mathfrak{o}$ is a prime divisor for which*

$$\mathfrak{p}^{\sigma} = \mathfrak{p} \quad \textit{for some } \sigma \neq 1 \textit{ in } A_0,$$

then the order of σ is either a power of 2 or a power of 3, and $2\mathfrak{p} = \mathfrak{o}$ or $3\mathfrak{p} = \mathfrak{o}$ accordingly.

This concludes our review of the theory of elliptic function fields. We now use this theory to prove several lemmas which will be of use in what follows.

LEMMA 3. *Under the assumption that $\gamma = 1$, we have*

$$[K: k(z)] = g > 2 \tag{26}$$

and

$$f > 3. \tag{27}$$

PROOF. Since K has genus 1 and $k(z)$ has genus 0 it is clear that $g \neq 1$. If (26) is false we must have $g = 2$. It follows that the degree of $\mathfrak{z}$, as a divisor of K, is 2; by (12) this gives that $\dim L(1/\mathfrak{z}) = 2$, and that $1, z$ form a basis for $L = L(1/\mathfrak{z})$. Now since F is fixed by the automorphisms in H, its denominator $\mathfrak{z}^f$ is also fixed. Thus $\mathfrak{z}$ is fixed, so that for all σ in H, z^{σ} lies in L. But then each z^{σ} is of the form $cz + d$, with c, d in k, so that $k(z^{\sigma}) = k(z)$. Consequently $k(z)/k(F)$ is normal and $K = k(z)$; hence $g = 1$, contrary to what has been noted. This proves (26).

If $f = 2$, then $K = k(z)$. Hence if (27) is false then $f = 3$, and H is either cyclic or the symmetric group on 3 letters. In either case $g = \frac{1}{3}h \leqslant 2$, which contradicts (26).

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

Before proving the next lemma we make several observations. If I_0 is the set of elements σ in A_0 for which $\sigma\tau_\sigma$ lies in H, for some τ_σ in T, and if I_0' is defined similarly for G, then I_0 and I_0' are subgroups of A_0 containing H_0 and G_0 respectively. Furthermore,

$$H/H\cap T\cong HT/T\cong I_0 \tag{28}$$

and

$$G/G\cap T\cong GT/T\cong I_0'. \tag{29}$$

These equations imply

$$|H|=|I_0|\cdot|H\cap T|,\quad |G|=|I_0'|\cdot|G\cap T|, \tag{30}$$

and division gives

$$f=|H\colon G|=|I_0\colon I_0'|\cdot|H\cap T\colon G\cap T|=j\cdot e, \tag{31}$$

where $j=|I_0\colon I_0'|$, $e=|H\cap T\colon G\cap T|$. It follows that $(H\cap T)^e$, the subgroup of $H\cap T$ of eth powers, lies in $G\cap T\subseteq G$. By (5) and the fact that $(H\cap T)^e$ is a characteristic subgroup of $H\cap T$ we have

$$(H\cap T)^e=1,\quad H\cap T\subseteq T_e. \tag{32}$$

In particular, if $e=1$, then $H\cap T=G\cap T=1$ and H and G are isomorphic to the subgroups I_0 and I_0' of A_0.

We now prove

LEMMA 4. *Let q be a prime number. If $q\mid h$, then q divides $|A_0|$. Hence the only prime divisors of h are 2 and 3.*

PROOF. Suppose $q\nmid|A_0|$, and let S be the q-Sylow subgroup of the abelian group $G\cap T$. By (31) and (9) we have that $q\nmid|H\cap T\colon G\cap T|$, so that S is also the q-Sylow subgroup of $H\cap T$. Thus S is a characteristic subgroup of $H\cap T$, and by (5) it follows that $S=1$. Thus $q\nmid|G\cap T|$. The lemma now follows from (30) and (9).

From Lemma 4 we conclude that

$$|A_0|\neq 4. \tag{33}$$

For otherwise $f=4$ by (9) and (27), so that $g\mid 6$ by (4). Lemma 4 now implies that $3\nmid g$, so $g\leqslant 2$, and this contradicts (26).

Before proceeding to the case $p\neq 2,3$ we make one final observation. Since we are only interested in determining the form of the polynomial F (that is, its coefficients), we may replace the tower $K/k(F(z))$ by any isomorphic tower $K'/k(F(z'))$. In particular, if σ lies in A we may replace $K/k(F(z))$ by $K/k(F(z^\sigma))$; in so doing we have replaced G and H by the conjugate groups $\sigma^{-1}G\sigma$ and $\sigma^{-1}H\sigma$. This allows us to consider any conjugate of H (inside A) in place of H.

4. Characteristic $p \neq 2, 3$

In this section we consider the case in which the characteristic of k is different from 2 and 3. By (10), (24) and (33) we see that $|A_0| = 6$. The generating equation (15) may then be taken to be $y^2 = x^3 + b$ with $b \neq 0$ in k (see Deuring (1947)). Since k is algebraically closed we may take $b = 1$; thus

$$K = k(x, y) \quad \text{with } y^2 = x^3 + 1. \tag{34}$$

The group A_0 is cyclic; a generating element is easily found to be the element ψ defined by

$$(x^\psi, y^\psi) = (\omega x, -y), \tag{35}$$

where ω is a fixed primitive cube root of unity. For the element ε of Lemma 1 we have

$$\varepsilon = \psi^3 \quad \text{and} \quad (x^\varepsilon, y^\varepsilon) = (x, -y). \tag{36}$$

We note that the three primes of order 2 in D_0 are given by

$$\mathfrak{p}_i \leftrightarrow (-\omega^i, 0) \quad \text{for } i = 0, 1, 2, \tag{37}$$

where we use "$\leftrightarrow$" to denote the correspondence given by (16). The $\mathfrak{p}_i$ are exactly the primes $\mathfrak{p}$ for which $\mathfrak{p}^\varepsilon = \mathfrak{p}$. We denote the corresponding translations of T by τ_i. An easy calculation using (16), (35), (37) and (19) shows that

$$\mathfrak{p}_i^\psi = \mathfrak{p}_{i+2} \quad \text{and} \quad \psi^{-1} \tau_i \psi = \tau_{i+2}, \tag{38}$$

where the subscripts are to be read modulo 3. Thus the group A_0 permutes the τ_i transitively.

We also note that the only primes fixed by elements of A_0 are the primes $\mathfrak{p}_i$ (fixed by ε), and the primes

$$\mathfrak{q} \leftrightarrow (0, 1) \quad \text{and} \quad \mathfrak{q}^\varepsilon \leftrightarrow (0, -1). \tag{39}$$

The primes $\mathfrak{q}$ and $\mathfrak{q}^\varepsilon$ are fixed by the subgroup $\langle \psi^2 \rangle$, so by Lemma 2 we see that $\mathfrak{q}$ and $\mathfrak{q}^\varepsilon$ are of order 3 in D_0.

We now determine the groups G and H. We first note that $f = 6$ from (9) and (27). Thus (8) implies $h_0 = 6$ and $g_0 = 1$; hence

$$I_0 = A_0 \subseteq H \quad \text{and} \quad G \cap A_0 = 1.$$

By (30) and (2) we see further that

$$g = |G| = |H \cap T|. \tag{40}$$

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

Now by (32) we have

$$(H \cap T)^e = 1 \quad \text{for some divisor } e \text{ of } 6.$$

We distinguish four cases:

Case (i). If $e = 1$, then by the remark following (32) the group H is cyclic. But then G is normal in H, contrary to our assumption.

Case (ii). If $e = 2$, then by (32) we have $H \cap T \subseteq T_2$. The case $H \cap T = 1$ is impossible as in (i), so by the remark following (38), the normality of $H \cap T$ in H, and the fact $A_0 \subseteq H$, we have

$$H \cap T = T_2. \tag{41}$$

Thus $|H \cap T| = g = 4$ and $e = 2$, so (30) and (31) imply $|G \cap T| = 2$ and $|I_0'| = 2$. Hence $I_0' = \langle \varepsilon \rangle$ and by conjugating by an appropriate power of ψ we may assume $G \cap T = \langle \tau_0 \rangle$. Also, from (2) we have $|H| = 24$, so that

$$H = A_0 T_2. \tag{42}$$

(H contains the right-hand side and both sides have the same order.)

Now by (42), (7) and the fact

$$\mathfrak{o}^{\sigma\tau_i} = \mathfrak{p}_i \quad \text{for } \sigma \text{ in } A_0,$$

we have $\mathfrak{z}^6 = (\mathfrak{o}\mathfrak{p}_0\mathfrak{p}_1\mathfrak{p}_2)^6$, whence

$$\mathfrak{z} = \mathfrak{o}\mathfrak{p}_0\mathfrak{p}_1\mathfrak{p}_2. \tag{43}$$

It now follows easily from (6) that

$$G = \{1, \tau_0, \varepsilon\tau_1, \varepsilon\tau_2\}. \tag{44}$$

Case (iii). If $e = 3$, then by (20) and (32) either $H \cap T = T_3$ or $H \cap T = \langle \tau \rangle$, where $\tau^3 = 1$. In the first case (see (40)) $g = 9$, which is impossible by (4). Thus $|H \cap T| = 3 = g$, and from (2), $h = 18$. Thus

$$H = A_0 \langle \tau \rangle. \tag{45}$$

Moreover, since $\langle \tau \rangle = H \cap T$ is normal in H and $A_0 \subseteq H$ we must have $\psi^{-1}\tau\psi = \tau$ or τ^{-1}, and therefore $\psi^{-2}\tau\psi^2 = \tau$. Hence (19) implies $\mathfrak{p}^{\psi^2} = \mathfrak{p}$ for the prime $\mathfrak{p}$ corresponding to τ. It follows by (39) that $\mathfrak{p} = \mathfrak{q}$ or $\mathfrak{q}^\varepsilon$, and we may assume

$$\tau \leftrightarrow \mathfrak{q}, \quad \tau^2 = \tau^{-1} \leftrightarrow \mathfrak{q}^\varepsilon. \tag{46}$$

As in case (ii) we have $\mathfrak{z}^6 = (\mathfrak{o}\mathfrak{q}\mathfrak{q}^\varepsilon)^6$, so

$$\mathfrak{z} = \mathfrak{o}\mathfrak{q}\mathfrak{q}^\varepsilon. \tag{47}$$

Now by (31) we have $|I_0'| = 3$, whence $I_0' = \langle \psi^2 \rangle$; consequently G must be equal to one of the conjugate subgroups

$$\langle \psi^2 \tau \rangle \quad \text{or} \quad \langle \psi^2 \tau^2 \rangle. \tag{48}$$

Case (*iv*). In the last case $e = 6$. Hence $6 | g$. Now g must divide 5!, so by (40) and $H \cap T \subseteq T_6$ we must have $g = 6$ or 12. But the argument leading to (41) shows that $T_2 \subseteq H \cap T$, so $g = 12$. From (31) it follows that $I_0' = A_0$, and by (30) we have $|G \cap T| = 2$. Thus $G \cap T = \langle \tau_i \rangle$ for some i. Now $G \cap T$ is normal in G. Since $\psi\tau$ lies in G for some τ in T, we have therefore that $(\psi\tau)^{-1} \tau_i (\psi\tau) = \tau_i$. But T is abelian and normal in A, so that

$$\tau_i = (\psi\tau)^{-1} \tau_i (\psi\tau) = \tau^{-1}(\psi^{-1} \tau_i \psi)\tau = \psi^{-1} \tau_i \psi.$$

This contradicts the fact that $\mathfrak{p}_i$ is only fixed by 1 and ε. This case is impossible.

We now work out the polynomial F in case (ii). To do so we first note the following expressions for x^{τ_i} and y^{τ_i}:

$$x^{\tau_i} = -\omega^i \left(\frac{x - 2\omega^i}{x + \omega^i} \right), \qquad \text{for } i = 0, 1, 2. \tag{49}$$

$$y^{\tau_i} = \frac{-3\omega^{2i} y}{(x + \omega^i)^2}$$

These may be verified using (17), (22) and (37), together with the fact that $-(a, b) = (a, -b)$.

We claim that the fixed field of G is $k(u)$, where

$$u = \frac{x^2 + 2x - 2}{2y}. \tag{50}$$

That u is fixed by G is easily computed using (44) and (49). Note further that the divisor of u is

$$(u) = \frac{\mathfrak{a}}{\mathfrak{d}^4} \cdot \frac{\mathfrak{d}^3}{\mathfrak{p}_0 \mathfrak{p}_1 \mathfrak{p}_2} = \frac{\mathfrak{a}}{\mathfrak{d} \mathfrak{p}_0 \mathfrak{p}_1 \mathfrak{p}_2} = \frac{\mathfrak{a}}{\mathfrak{z}},$$

where $\mathfrak{a}$ is prime to $\mathfrak{z}$. (We have used $(y) = \mathfrak{p}_0 \mathfrak{p}_1 \mathfrak{p}_2 / \mathfrak{d}^3$, a fact which is clear from (37).) It follows that

$$[K: k(u)] = \deg \mathfrak{z} = 4.$$

But u lies in $k(z)$ and $[K: k(z)] = 4$. Thus $k(u) = k(z)$. Since the denominators of u and z are equal we have in addition that

$$u = az + b \quad \text{for some } a \neq 0,\ b \text{ in } k. \tag{51}$$

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

To compute the fixed field of H note that

$$u^2-1=\frac{x^4-8x}{4(x^3+1)}=\frac{x^4-8x}{4y^2}$$

is invariant under the group $\langle\varepsilon\rangle G=\langle\varepsilon,\tau_0,\tau_1\rangle$. It follows that

$$E(u)=\prod_{i=0}^{2}(u^2-1)^{\psi^i}=(u^2-1)^3 \tag{52}$$

is invariant under H. Since the denominator of $E(u)$ is $\mathfrak{z}^6$ we have by the same argument which led to (51) that

$$F(z)=cE(u)+d=cE(az+b)+d \quad \text{for some } c\neq 0, d \text{ in } k.$$

Hence F is linearly equivalent to the polynomial $(z^2-1)^3$.

Conversely, our analysis shows that any polynomial equivalent to $(z^2-1)^3$ has a normal closure with $\gamma=1$. For if K is defined by (34) and z is given by (50), then K is the normal closure of $k(z)/k((z^2-1)^3)$. This follows from the fact that the groups G and H defined by (44) and (42) satisfy the condition (5) and are the Galois groups of $K/(k(z))$ and $K/k((z^2-1)^3)$.

In case (iii) we find similarly that $F(z)$ is equivalent to the polynomial $(z^3+1)^2$. We omit the details. For the reader's convenience the information corresponding to the equations (42), (44), (49)–(50) and (52) has been listed in Tables 1 and 2 of Section 7. As the crucial part of the argument is the determination of the fixed field of G, that is, the determination of z in terms of x and y, we indicate briefly how this may be done.

First find a basis $\eta_1,\ldots,\eta_g$ for $L(1/\mathfrak{z})$. Since z lies in $L(1/\mathfrak{z})$ we must have

$$z=\sum_{i=1}^{g}a_i\eta_i \quad \text{for some constants } a_i \text{ in } k.$$

The condition that z be fixed by G gives a set of g^2-g linear conditions on the a_i, which in our case determine a suitable expression for z. The expression will not be unique; this corresponds to the fact that z may be replaced by $az+b$ for any constants $a\neq 0$ and b in k.

5. Characteristic $p=3$

In the case $p=3$ we may take the equation (15) to be of the form

$$y^2=x^3+ax^2+bx \quad \text{where } b\neq 0 \text{ and } a \text{ lie in } k.$$

If $a\neq 0$, a simple computation shows that $|A_0|=2$, which is excluded by (10).

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

Hence $a = 0$. Since k is algebraically closed we may assume $b = -1$, so that (see Deuring (1941a))

$$K = k(x, y) \quad \text{with } y^2 = x^3 - x. \tag{53}$$

From (53) it is easily found that A_0 has order 12 and is generated by the elements ψ and κ defined by

$$(x^\psi, y^\psi) = (x+1, -y), \quad (x^\kappa, y^\kappa) = (-x, iy), \tag{54}$$

where i is a primitive fourth root of unity. We have $\psi^3 = \kappa^2 = \varepsilon$ and $\kappa^{-1}\psi\kappa = \psi^{-1}$. Thus $\langle\psi\rangle$ is normal in A_0, and $\langle\psi^2\rangle$ is the unique 3-Sylow subgroup in A_0. Moreover the elements of the coset $\langle\psi\rangle\kappa$ all have order 4.

The primes of order 2 in D_0 are given by

$$\mathfrak{p}_i \leftrightarrow (i, 0) \quad \text{for } i = 0, 1, 2.$$

As in (38) we find

$$\mathfrak{p}_i^\psi = \mathfrak{p}_{i+2}, \quad \psi^{-1}\tau_i\psi = \tau_{i+2},$$

$$\mathfrak{p}_i^\kappa = \mathfrak{p}_{-i}, \quad \kappa^{-1}\tau_i\kappa = \tau_{-i}, \tag{55}$$

where the subscripts are to be read modulo 3, and τ_i is the element of T corresponding to $\mathfrak{p}_i$ by (18). It follows easily using Lemma 2, (16), (54) and (55) that a prime $\mathfrak{p}$ is fixed by an element σ in A_0 if and only if

$$\text{for some } i, \quad \mathfrak{p} = \mathfrak{p}_i \quad \text{and} \quad \sigma \in \langle\psi^{-i}\kappa\rangle. \tag{56}$$

In fact, there are no primes of order 3 in D_0 since the Hasse invariant is 0 (see Hasse (1934, 1936)), but we shall not use this fact.

The method of determining G and H in the present case differs slightly from the method of Section 4. Here we consider the divisor

$$\mathfrak{z} = \prod_{\sigma \in G} \mathfrak{d}^\sigma = (\mathfrak{d}\mathfrak{q}_1 \dots \mathfrak{q}_r)^{g_0}, \tag{57}$$

where $g_0 = |G \cap A_0|$ and $1 + r = |G : G \cap A_0|$. Since $H_0 = H \cap A_0$ leaves $\mathfrak{z}$ and $\mathfrak{d}$ fixed, the group H_0 permutes the r primes $\mathfrak{q}_j$. In our argument we consider the orbits of the $\mathfrak{q}_j$ under this permutation group. Note that the primes in a single orbit all have the same order in D_0 since elements of H_0 are automorphisms of D_0. Note also that the length of the orbit containing $\mathfrak{q}_j$ is

$$h_0/h_j \quad \text{where } h_j = |H_0 \cap A_{\mathfrak{q}_j}|$$

is the number of elements of H_0 which fix $\mathfrak{q}_j$. By (56) we see that $h_j = 1$ unless $\mathfrak{q}_j = \mathfrak{p}_i$ for some i.

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

We also observe from (8) and (27) that

$$h_0 \geqslant f \geqslant 4; \tag{58}$$

from $f \mid h_0$ and $h_0 \mid 12$ we see that f and h_0 are even.

We now distinguish four cases according to the number of primes $\mathfrak{p}_i$ which divide $\mathfrak{z}$.

Case (i). If no $\mathfrak{p}_i$ divides $\mathfrak{z}$, then each orbit has length $h_0 = fg_0$. If n is the number of orbits we have by (7) and (57) that

$$h = h_0(1+r) = h_0(1+nfg_0).$$

By Lemma 4 and the fact that f is even, this implies that $1+nfg_0$ is a power of 3. But $f \mid 12$ and from (58), $f = 4$, 6 or 12. Thus $f = 4$, Now $(1+4ng_0) \mid g$, and (4) implies that $g \mid 3!$ so that $n = 0$. Thus $\mathfrak{z} = \mathfrak{o}^g$, $G = G_0$ and $H = H_0 \subseteq A_0$. If $3 \mid g$, then G contains the normal subgroup $\langle \psi^2 \rangle$ of A_0, contrary to (5). But otherwise the inequality $g \leqslant 2$ contradicts (26). Case (i) is therefore impossible.

Case (ii). Suppose exactly one of the $\mathfrak{p}_i$ divides $\mathfrak{z}$. By conjugating H by some power of ψ we may assume that $\mathfrak{p}_0 \mid \mathfrak{z}$. Since $\mathfrak{p}_0$ is the only prime of order 2 dividing $\mathfrak{z}$, it must be left fixed by H_0. Thus (56) and (58) imply

$$H_0 = \langle \kappa \rangle, \quad h_0 = f = 4, \quad g_0 = 1.$$

If n represents the number of orbits distinct from the orbit $\{\mathfrak{p}_0\}$, then as in case (i) we have

$$h = h_0(1+r) = 4(2+4n) = 8(1+2n).$$

It follows from (30) and the fact that 4 is the exact power of 2 dividing $|I_0|$ that $|H \cap T| \equiv 2 \pmod 4$. Thus $H \cap T$ contains a unique element τ of order 2; it follows that $\langle \tau \rangle$ is normal in H. From (2) and (26) we have also that $g = 2(1+2n) > 2$. Thus (4) implies that $g = 6$, $h = 24$ and $H \cong S_4$, where S_4 is the symmetric group on 4 letters. But S_4 contains no normal subgroup of order 2. This rules out case (ii).

Case (iii). Suppose exactly two of the primes $\mathfrak{p}_i$ divide $\mathfrak{z}$. By conjugating by appropriate powers of ψ and κ we may assume that $\mathfrak{p}_0$ and $\mathfrak{p}_1$ divide $\mathfrak{z}$. If both $\mathfrak{p}_0$ and $\mathfrak{p}_1$ are fixed by H_0, then by (56) we have $H_0 = \langle \varepsilon \rangle$, which is impossible by (58). Thus $\{\mathfrak{p}_0, \mathfrak{p}_1\}$ forms one of the orbits and $H_0 = \langle \psi^{-2} \kappa \rangle$ (since $\mathfrak{p}_2$ must be fixed by H_0). Thus $f = h_0 = 4$. If n is the number of remaining orbits then we see that $h = 4(3+4n)$ must divide $f! = 24$. This implies that $n = 0$, $h = 12$ and $g = 3$. This gives further that $2 \nmid |I_0'|$, and since 4 divides $|I_0|$ we have by (31) that $e = 1$. Hence $H \cong A_0$. But then G corresponds to the subgroup $\langle \psi^2 \rangle$ of A_0 and is normal in H; contradiction.

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

Case (*iv*). Hence all three of the $\mathfrak{p}_i$ divide $\mathfrak{z}$. As in case (iii) at most one $\mathfrak{p}_i$ can be fixed by H_0. If some $\mathfrak{p}_i$ is fixed, then (56) implies $h_0 = 4$ and $h = 4(4+4n) = 16(1+n)$, where n is the number of orbits not containing any $\mathfrak{p}_i$. But then $f = 4$ and by (4) h is not divisible by 16. Thus no $\mathfrak{p}_i$ is fixed, and $\{\mathfrak{p}_0, \mathfrak{p}_1, \mathfrak{p}_2\}$ is one of the orbits. This implies further that $3 \mid h_0$. Since h_0 is even we have the two possibilities: $h_0 = 6$ or 12.

(**a**). Suppose $h_0 = 6$. Then by (8) and (58) we have $f = 6$ and $g_0 = 1$. Therefore

$$h = 6(4+6n) = 12(2+3n).$$

Since $h \mid 6!$ we see from Lemma 4 that $(2+3n) \mid 2^2 \cdot 3$, whence $n = 0$, $h = 24$ and $g = 4$. By (30) and (31) we have $e \mid 2$, so $H \cap T \subset T_2$. We cannot have $H \cap T = 1$; otherwise H would be isomorphic to a subgroup of A_0, which is contrary to $|H| = 24 > 12 = |A_0|$. Hence $e = 2$, and by the same argument as in Section 4, case (ii) we have $H \cap T = T_2$, $H = \langle \psi \rangle T_2$, $I_0' = \langle \varepsilon \rangle$ and $G = \{1, \tau_0, \varepsilon\tau_1, \varepsilon\tau_2\}$.

(**b**). If $h_0 = 12$, then $A_0 \subseteq H$ and

$$h = 12(4+12n) = 2^4 \cdot 3(1+3n).$$

By (58) and (4) we have that $f = 6$ or 12. In either case g is by Lemma 4 a power of 2, and A_0 is a proper subgroup of H. Thus $H \cap T \neq 1$. Since $I_0 = A_0$ we see that 3 divides $|I_0 : I_0'|$, so (31) implies $e = 2$ or 4. Thus $H \cap T \subseteq T_4$, $H \subseteq A_0 T_4$ and $n = 0$ or 1.

If $n = 1$, then the remaining orbit has length 12; by (7), (20) and $T_2 \subseteq H \cap T \subseteq T_4$ this implies that $H \cap T = T_4$. Hence $e = 4$ and $|G \cap T| = 4$. Since $G \cap T$ is not equal to the characteristic subgroup T_2 of $H \cap T$ we know that $G \cap T$ is cyclic, generated by τ, say; furthermore, $\langle \tau \rangle = G \cap T$ is normal in G. Now by (31), $|I_0'| = 4$, so there is an element σ in A_0 of order 4 and an element τ' in T for which $\sigma\tau'$ lies in G. It follows that

$$(\sigma\tau')^{-1} \tau (\sigma\tau') = \tau \quad \text{or} \quad \tau^{-1};$$

as in Section 4, case (iv) the left-hand side equals $\sigma^{-1}\tau\sigma$. In either case we have $\sigma^{-2}\tau\sigma^2 = \tau$, that is, $\varepsilon^{-1}\tau\varepsilon = \tau$; but this is impossible by (19) and (56), since τ has order 4.

Hence $n = 0$, $H \cap T = T_2$, $h = 48$ and $H = A_0 T_2$. If $f = 6$, then by (8) we have $g_0 = 2$ and $G_0 = \langle \varepsilon \rangle$. But by Lemma 1 and (55) the element ε commutes with all the elements of H; this contradicts (5). Hence $f = 12$, $g_0 = 1$ and $g = 4$. There are two possibilities for G according as $e = 2$ or 4. If $e = 2$ then as in (a) we may take $G = \{1, \tau_0, \varepsilon\tau_1, \varepsilon\tau_2\}$. If $e = 4$ then $G \cap T = 1$ and $|I_0'| = 4$. By considering an appropriate conjugate of G we may assume that $G = \langle \kappa\tau \rangle$ for some τ in T_2. Note that $\tau \neq \tau_0$ since $(\kappa\tau_0)^2 = \varepsilon$ lies in A_0. By conjugating by κ we may also assume that $\tau = \tau_1$, so that finally $G = \langle \kappa\tau_1 \rangle$.

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

This completes the discussion of the four cases. By the method of Section 4 we find for the three pairs of groups (G, H) that F is linearly equivalent respectively to the polynomials

$$z^2(z^4-1), z^4(z^4-1)^2 \quad \text{and} \quad z^2(z^4-1)(z^2+1)^3.$$

6. Characteristic $p = 2$

We turn now to the case $p = 2$. We may take the equation (15) to be

$$y^2+axy+by = x^3+cx^2+dx \quad \text{where one of } a, b \neq 0.$$

If $a \neq 0$ then $|A_0| = 2$. Hence we may take $a = 0$ and $b = 1$. It is now easy to see that we may assume $c = d = 0$, by replacing x and y by

$$x+\alpha \quad \text{and} \quad y+\beta x+\delta$$

for suitable constants α, β and δ. Thus

$$K = k(x, y) \quad \text{with } y^2+y = x^3. \tag{59}$$

(See also Deuring (1941b).)

For the field K given by (59), the group A_0 has order 24 and is generated by the elements ψ, κ_i defined by

$$\begin{aligned} (x^{\psi}, y^{\psi}) &= (\omega x, y+1) \\ (x^{\kappa_i}, y^{\kappa_i}) &= (x+\omega^i, y+\omega^{2i}x+\omega) \quad \text{for } i = 0, 1, 2, \end{aligned} \tag{60}$$

where ω is a primitive cube root of unity. We have

$$\psi^3 = \kappa_i^2 = \varepsilon \quad \text{for } i = 0, 1, 2 \quad \text{and} \quad (x^{\mathfrak{s}}, y^{\mathfrak{s}}) = (x, y+1). \tag{61}$$

The group $B_0 = \langle \kappa_0, \kappa_1, \kappa_2 \rangle$ is isomorphic to the quaternion group, and is normal in A_0 by virtue of the relations

$$\psi^{-1}\kappa_i\psi = \kappa_{i+2} \quad \text{for } i = 0, 1, 2.$$

Moreover A_0 contains four distinct subgroups conjugate to $\langle \psi \rangle$. It is easily seen that A_0 contains no subgroup of order 12.

We note that D_0 contains no primes of order 2. For by Lemma 1 such a prime would satisfy $\mathfrak{p}^{\mathfrak{s}} = \mathfrak{p}$; by (16) and (61) this is equivalent to $y_{\mathfrak{p}}+1 = y_{\mathfrak{p}}$, which is impossible. Hence the group T contains no elements of even order.

The 8 primes of order 3 in D_0 are given by

$$\begin{aligned} &\mathfrak{r} \leftrightarrow (0, 0), \quad \mathfrak{r}^{\mathfrak{s}} \leftrightarrow (0, 1), \\ &\mathfrak{p}_i \leftrightarrow (\omega^i, \omega^2), \quad \mathfrak{p}_i^{\mathfrak{s}} \leftrightarrow (\omega^i, \omega) \quad \text{for } i = 0, 1, 2. \end{aligned} \tag{62}$$

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

From (60) we see that

$$\mathfrak{r}^{\kappa_i} = \mathfrak{p}_i \quad \text{for } i = 0, 1, 2, \tag{63}$$

so the 8 primes are all conjugate under B_0. That they are of order 3 follows from (13), $(y) = \mathfrak{r}^3/\mathfrak{d}^3$, and (63).

By Lemma 2, (60) and (63) it also follows that a prime $\mathfrak{p}$ is fixed by an element σ of A_0 if and only if

$$\mathfrak{p} = \begin{cases} \mathfrak{r}, \mathfrak{r}^\varepsilon \\ \mathfrak{p}_i, \mathfrak{p}_i^\varepsilon \end{cases} \text{ and } \sigma \text{ lies in } \begin{cases} \langle \psi^2 \rangle, \\ \langle \kappa_i^{-1} \psi^2 \kappa_i \rangle. \end{cases} \tag{64}$$

We let ρ and τ_i be the elements of T corresponding to the primes $\mathfrak{r}$ and $\mathfrak{p}_i$.

As in Section 5 we shall consider the action of H_0 on the primes $\mathfrak{q}_j$ dividing $\mathfrak{z}$. Before considering the various cases we make several observations. It follows from (58), as in Section 5, that f and h_0 are even. Lemma 1 implies that H_0 contains ε. Hence if the prime $\mathfrak{q}_j$ divides $\mathfrak{z}$ so does $\mathfrak{q}_j^\varepsilon$ and both belong to the same orbit under H_0. Thus the length of the orbit containing $\mathfrak{q}_j$ is even, and is equal to h_0/h_j, where $h_j = |H_0 \cap A_{\mathfrak{q}_j}|$ as in Section 5.

Since there are no points of order 2 in D_0 we see that $e = |H \cap T : G \cap T|$ is always odd. Since $f \mid 24$ it follows from (31) and (32) that

$$e = 1 \text{ or } 3 \quad \text{and} \quad H \cap T \subseteq T_3. \tag{65}$$

We also claim that

$$H = H_0(H \cap T) \quad \text{and} \quad I_0 = H_0. \tag{66}$$

For, suppose $\sigma\tau$ lies in H, where σ lies in A_0 and τ lies in T. Then the element

$$\varepsilon(\sigma\tau)^{-1}\varepsilon(\sigma\tau) = \varepsilon\tau^{-1}(\sigma^{-1}\varepsilon\sigma)\tau = \varepsilon\tau^{-1}\varepsilon\tau = \tau^2$$

is contained in H. Since the order of τ is odd it follows that τ lies in H, whence σ lies in H. This proves (66).

Now (7), (65) and (66) imply that the only primes $\mathfrak{p} \neq \mathfrak{o}$ dividing $\mathfrak{z}$ are of order 3 in D_0. Moreover by (20) there are 0, 2 or 8 such primes.

Case (*i*). If none of the primes in (62) divide $\mathfrak{z}$, then $\mathfrak{z} = \mathfrak{o}^g$ and $1 \neq G \subseteq H \subset A_0$. The order of G cannot be even, for otherwise G contains the normal subgroup $\langle \varepsilon \rangle$ of H. The only remaining possibility is that $g = 3$ and G is conjugate to $\langle \psi^2 \rangle$; thus we may assume $G = \langle \psi^2 \rangle$. By (2), (58) and the fact that A_0 contains no subgroup of order 12 it follows that $f = 8$ and $H = A_0$.

Case (*ii*). Suppose exactly 2 of the primes in (62) divide $\mathfrak{z}$, which by an appropriate conjugation we may take to be $\mathfrak{r}$ and $\mathfrak{r}^\varepsilon$. Then $\{\mathfrak{r}, \mathfrak{r}^\varepsilon\}$ forms the single orbit

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

distinct from $\{\mathfrak{o}\}$. Thus by (64) we have $H_0 = \langle \psi^2, \varepsilon \rangle = \langle \psi \rangle$; from (7) and (66) we see that $H \cap T = \langle \rho \rangle$ and $H = \langle \psi, \rho \rangle$. Hence $e = 3$. As in Section 4, case (iii) it follows that G is equal to one of the conjugate subgroups $\langle \psi^2 \rho \rangle$ or $\langle \psi^2 \rho^2 \rangle$.

Case (*iii*). Now suppose all the primes in (62) divide $\mathfrak{z}$. Then from (66), $H \cap T = T_3$, $e = 3$ and $|G \cap T| = 3$. From (31) we see that 3 (and therefore 6) divides f and h_0. We distinguish four subcases according to the nature of the orbits of the $\mathfrak{q}_j$ under H_0.

(**a**). If there are at least two orbits of length 2, then H_0 must contain at least two of the four conjugate subgroups of order 3 listed in (64); but in that case neither orbit can have length 2.

(**b**). If there is exactly one orbit of length 2, then the single remaining orbit has length 6, and by (64) and (66) $h_0 = 6$ and $h = 54$. But in this case $f = 6$; since $54 \nmid 6!$ this case is impossible.

(**c**). If there are two orbits of length 4 it is easy to see that $h_0 = 4$. For all the primes in (62) are conjugate under B_0 and A_0, and there is no subgroup of A_0 of order 12. But this contradicts the remark above, according to which $h_0 \geqslant 6$.

(**d**). The remaining possibility is that all the primes are in one orbit; hence $B_0 \subset H_0$. Since $3 | h_0$ we must have $H_0 = A_0$, $h = 9 \cdot 24$ and $H = A_0 T_3$. Also by (4) we have $f = 12$ or 24. If $f = 12$ then $g_0 = 2$ and $G_0 = \langle \varepsilon \rangle$. By the same computation which led to (66) we have that $G = G_0(G \cap T)$, whence $g = 2 \cdot 3 = 6$; but then $fg \neq h$. Hence $f = 24$, $g_0 = 1$ and $g = 9$. From (31) we see that $|I_0'| = 3$, and by an appropriate conjugation we may assume $I_0' = \langle \psi^A \rangle$. Now let $G \cap T = \langle \tau \rangle$, where $\tau = \rho$ or τ_i for some i. Then $G = \langle \tau, \psi^A \tau' \rangle$, where $\tau' \notin \langle \tau \rangle$. Since $g = 9$, G is abelian. Therefore

$$\tau \cdot \psi^A \tau' = \psi^A \tau' \cdot \tau = \psi^A \cdot \tau' \tau = \psi^A \tau \cdot \tau',$$

and it follows that τ and ψ^A commute. By (19) and (64) we see that $\tau = \rho$. By conjugating by some power of ψ we may also assume $\tau' = \tau_0$. Hence $G = \langle \rho, \psi^A \tau_0 \rangle$.

The polynomials corresponding to the three pairs of groups we have found in this section are listed in Section 7, Table 1. Since the last case involves a somewhat more elaborate computation, we sketch the details.

To find the fixed field of G we first find the fixed field of $\langle \rho \rangle$. We note

$$(x^\rho, y^\rho) = \left(\frac{x}{y}, \frac{y+1}{y} \right),$$

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

so that

$$x+x^{\rho}+x^{\rho^2}=x+\frac{1}{x^2}=\xi$$

and

$$y+y^{\rho}+y^{\rho^2}=\frac{y^3+y+1}{y^2+y}=y+1+\frac{1}{x^3}=\eta+\omega^2$$

are fixed by ρ. Since $[K\colon k(\xi)]=6$ and $[K\colon k(\eta)]=9$ it follows that $[K\colon k(\xi,\eta)]=3$, so that $k(\xi,\eta)$ is the fixed field of $\langle\rho\rangle$.

Next we observe that

$$\begin{aligned}\eta^2+\eta &= y^2+y+\frac{1}{x^6}+\frac{1}{x^3}+\omega+\omega^2\\ &= x^3+\frac{1}{x^6}+\frac{1}{x^3}+1\\ &= \left(x+\frac{1}{x^2}\right)^3=\xi^3.\end{aligned}$$

Hence $k(\xi,\eta)$ is isomorphic to $K=k(x,y)$ by means of the meromorphism $\nu\colon (x,y)\to(\xi,\eta)$. (See Deuring (1941a) and Hasse (1936), Part II.) We denote the image of an object a in K by $\nu(a)$.

Now from the factorizations

$$(x)=\frac{\mathfrak{r}\mathfrak{q}}{\mathfrak{o}^2},\quad (y)=\frac{\mathfrak{r}^3}{\mathfrak{o}^3},$$

$$(\xi)=\frac{\mathfrak{p}_0\mathfrak{q}_0\mathfrak{p}_1\mathfrak{q}_1\mathfrak{p}_2\mathfrak{q}_2}{(\mathfrak{o}\mathfrak{r}\mathfrak{q})^2},\quad (\eta)=\left(\frac{(y+\omega^2)^3}{y^2+y}\right)=\frac{(\mathfrak{p}_0\mathfrak{p}_1\mathfrak{p}_2)^3}{(\mathfrak{o}\mathfrak{r}\mathfrak{q})^3}$$

(we have set $\mathfrak{q}=\mathfrak{r}^e$ and $\mathfrak{q}_i=\mathfrak{p}_i^e$ for short), it follows that

$$\begin{aligned}\nu(\mathfrak{o}) &= \mathfrak{o}\mathfrak{r}\mathfrak{q}=\mathfrak{o}\mathfrak{o}^{\rho}\mathfrak{o}^{\rho^2}=N\mathfrak{o},\\ \nu(\mathfrak{r}) &= \mathfrak{p}_0\mathfrak{p}_1\mathfrak{p}_2=\mathfrak{p}_0\mathfrak{p}_0^{\rho^2}\mathfrak{p}_0^{\rho}=N\mathfrak{p}_0,\end{aligned}\tag{67}$$

where N denotes the norm from K to $k(\xi,\eta)$. Furthermore, $(\xi^{\psi},\eta^{\psi})=(\omega\xi,\eta+1)$ shows that ψ induces the automorphism $\nu(\psi)$ on $k(\xi,\eta)$.

Next we determine the automorphism of $k(\xi,\eta)$ induced by τ_0: since

$$\mathfrak{x}^{\tau_0}=\mathfrak{x}+\mathfrak{p}_0\quad\text{in } D_0$$

for all primes $\mathfrak{x}$ of K, we have by (13) that

$$\frac{\mathfrak{x}^{\tau_0}}{\mathfrak{o}}\sim\frac{\mathfrak{x}\mathfrak{p}_0}{\mathfrak{o}^2},$$

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

whence (noting that ρ and τ_0 commute)

$$\frac{(N\mathfrak{x})^{\tau_0}}{N\mathfrak{D}} \sim \frac{N\mathfrak{x}\cdot N\mathfrak{p}_0}{(N\mathfrak{D})^2}.$$

Thus from (13) and (67)

$$(N\mathfrak{x})^{\tau_0} = N\mathfrak{x} + \nu(\mathfrak{x}) \quad \text{in } D_{\nu(\mathfrak{o})}.$$

Since $N\mathfrak{x}$ runs through all the primes of $k(\xi,\eta)$ as $\mathfrak{x}$ runs through primes of K, this shows that τ_0 induces the automorphism $\nu(\rho) \leftrightarrow \nu(\mathfrak{x})$ on $k(\xi,\eta)$.

Now let K' be the fixed field of G. By Galois theory the Galois group of $k(\xi,\eta)$ over K' is isomorphic to

$$G/\langle\rho\rangle \cong \langle\psi^4\tau_0\rangle.$$

By the above remarks it follows that K' is the fixed field of the automorphism group $\langle\nu(\psi)^4\cdot\nu(\rho)\rangle = \langle\nu(\psi)^2\cdot\nu(\rho)^2\rangle$. But this is one of the conjugate groups which appears in case (ii). From Table 1 (or an easy computation) we see that the fixed field of $\langle\psi^2\rho^2\rangle$ is $k(u)$, where

$$u = \frac{y+\omega^2}{x}.$$

TABLE 1

k algebraically closed

	$K = k(x,y)$	H	G	z	$F(z)$
$p \neq 2, 3$	$y^2 = x^3+1$	$A_0\, T_2$	$\langle\tau_0, \varepsilon\tau_1\rangle$	$\dfrac{x^2+2x-2}{2y}$	$(z^2-1)^3$
		$A_0\langle\tau\rangle$	$\langle\psi^2\tau^2\rangle$	$\dfrac{y+\sqrt{-3}}{\sqrt{(-3)}.x}$	$(z^3+1)^2$
$p = 3$	$y^2 = x^3-x$	$\langle\psi\rangle\, T_2$	$\langle\tau_0, \varepsilon\tau_1\rangle$	$\dfrac{x^2+1}{y}$	$z^2(z^4-1)$
		$A_0\, T_2$	$\langle\tau_0, \varepsilon\tau_1\rangle$	$\dfrac{x^2+1}{y}$	$z^4(z^4-1)^2$
		$A_0\, T_2$	$\langle\kappa\tau_1\rangle$	$\zeta\left(\dfrac{x^2-ix-1}{y}\right)$	$z^2(z^4-1)\,(z^2+1)^3$
$p = 2$	$y^2+y = x^3$	A_0	$\langle\psi^2\rangle$	y	$z(z^3+1)\,(z^2+z+1)^2$
		$\langle\psi\rangle\,\langle\rho\rangle$	$\langle\psi^2\rho^2\rangle$	$\dfrac{y+\omega^2}{x}$	$z^3(z^3+1)$
		$A_0\, T_3$	$\langle\rho, \psi^4\tau_0\rangle$	$\dfrac{x^3y+x^3+1}{x^4+x}$	$z^3(z^3+1)\,(z^6+z^3+1)^3$

$(\omega^3 = 1, \sqrt{-3} = \omega-\omega^2, i^4 = 1, \zeta^2 = i)$.

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

Thus $K' = k(v(u)) = k(u')$, where

$$u' = \frac{\eta+\omega^2}{\xi} = \frac{x^3y+x^3+1}{x^4+x}.$$

As in Section 4 we have

$$(u') = \frac{\mathfrak{a}}{\mathfrak{z}} \quad \text{where } (\mathfrak{a}, \mathfrak{z}) = 1,$$

so we may assume without loss of generality that $u' = z$; it now follows after some calculation that $F(z)$ is equivalent to

$$E(z) = \prod_{\sigma \in A_0} z^\sigma = z^3(z^3+1)(z^6+z^3+1)^3.$$

7. Summary

We sum up the results of Section 4–6 in

THEOREM 2. *If k is an algebraically closed field, and γ is the genus of the normal closure K of the separable extension $k(z)/k(F(z))$, then $\gamma = 1$ if and only if F is linearly equivalent to one of the polynomials listed in Table* 1.

We note that the 'if' part of the theorem follows in each case just as in the example worked out in Section 4. With each of the polynomials in Table 1 are listed the particular generating equation for K, the Galois groups G and H, and the element z in terms of x and y. The expressions for the automorphisms occurring in the groups G and H are listed in Table 2. For convenience in working out the expressions for F we note that in the last six cases

$$F(z) = \pm N(z) = \pm \prod_\sigma z^\sigma,$$

where N denotes the norm form $k(z)$ to $k(F)$, and σ runs through a set of coset representatives of G in H. In case 6 we may take the representatives to lie in B_0; in the other cases we may take A_0 as a set of coset representatives. Note that F is always defined over the prime field of k.

If k is not algebraically closed, we have

THEOREM 3. *If k is a perfect field, and γ is the genus of the normal closure K of the separable extension $k(z)/k(F(z))$, then $\gamma = 1$ if and only if F is linearly equivalent over k to one of the polynomials listed in Table* 3.

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

TABLE 2

$p \neq 2, 3$	$p = 3$	$p = 2$
$A_0 = \langle \psi \rangle$	$A_0 = \langle \psi, \kappa \rangle$	$A_0 = \langle \psi, \kappa_0 \rangle$
$(x^\psi, y^\psi) = (\omega x, -y)$	$(x^\psi, y^\psi) = (x+1, -y)$, $\psi^3 = \varepsilon$	$(x^\psi, y^\psi) = (\omega x, y+1)$
$\varepsilon = \psi^3$	$(x^\kappa, y^\kappa) = (-x, iy)$	$(x^{\kappa_0}, y^{\kappa_0}) = (x+1, y+x+\omega)$
$T_2 = \langle \tau_0, \tau_1 \rangle$	$T_2 = \langle \tau_0, \tau_1 \rangle$	$T_3 = \langle \rho, \tau_0 \rangle$
$x^{\tau_i} = -\omega^i\left(\frac{x-2\omega^i}{x+\omega^i}\right)$	$(x^{\tau_0}, y^{\tau_0}) = \left(\frac{-1}{x}, \frac{y}{x^2}\right)$	$(x^\rho, y^\rho) = \left(\frac{x}{y}, \frac{y+1}{y}\right)$
$y^{\tau_i} = \frac{-3\omega^{2i} y}{(x+\omega^i)^2}$	$(x^{\tau_1}, y^{\tau_1}) = \left(\frac{x+1}{x-1}, \frac{y}{(x-1)^2}\right)$	$x^{\tau_0} = \frac{x^2+x+y+\omega}{(x+1)^2}$
$x^\tau = 2\frac{y+1}{x^2}$		
$y^\tau = -\frac{y+3}{y+1}$		$y^{\tau_0} = \frac{xy+\omega(x+\omega)^3}{(x+1)^3}$

($\omega^3 = 1$, $i^4 = 1$.)

TABLE 3
k perfect

	$p \neq 2, 3$	$p = 3$	$p = 2$
$F(z)$	$(z^2+a)^3$	$z^2(z^4+a)$	$(z^4+z+b^2+b)(z^2+z+b)^2$
	$(z^3+a)^2$	$z^4(z^4+a)^2$	$z^3(z^3+a)$
		$z^2(z^4-a^2)(z^2+a)^3$	$(z^6+az^3)(z^6+az^3+a^2)^3$

($a \neq 0$, b lie in k.)

PROOF. Let $\bar{k}$ be the algebraic closure of k. Then the genus of the field $\bar{K} = K\bar{k}$ equals γ. By Theorem 2 and the remarks at the beginning of Section 2 it follows that $\gamma = 1$ if and only if F is linearly equivalent over $\bar{k}$ to one of the eight polynomials listed in Table 1.

Suppose that F is linearly equivalent to the third polynomial of Table 1, so that the characteristic of k is 3, and

$$F(z) = c(az+b)^2((az+b)^4-1)+d$$

for some constants a, b, c, d in $\bar{k}$ with $ac \neq 0$. Then setting $a_1 = -1/a^4$, $u = ca^6$ and $v = b/a$ we see that

$$F(z) = u(z+v)^2((z+v)^4+a_1)+d.$$

https://doi.org/10.1017/S1446788700011939 Published online by Cambridge University Press

Since the left-hand side has coefficients in k we see that u lies in k. Moreover the coefficients of z^3 and z^2 on the right-hand side are $-uv^3$ and ua_1. Hence v^3 and a_1 lie in k. But k is perfect, so that v lies in k. Finally it is clear that d lies in k. Hence F is equivalent over k to the polynomial $z^2(z^4+a_1)$, where $a_1 \neq 0$ lies in k. This is the third case listed in Table 3.

Similar arguments hold for the other cases.

8. Appendix

We now give the proofs of (22) and Lemmas 1 and 2. In doing so we avail ourselves freely of the concepts, notation and results of Hasse's papers (Hasse (1936), Parts II and III). We shall refer to these papers simply by II and III.

(a). We begin by proving Lemma 2. Let $\mathfrak{p} \neq \mathfrak{o}$ be some prime divisor for which $\mathfrak{p}^\sigma = \mathfrak{p}$, for some $\sigma \neq 1$ in A_0, and let n be the order of σ. We first show that $n\mathfrak{p} = \mathfrak{o}$ in D_0.

Let K_σ be the fixed field of $\langle\sigma\rangle$. Then

$$N_{K/K_\sigma}\mathfrak{p} = \mathfrak{p}^{1+\sigma+\ldots+\sigma^{n-1}} = \mathfrak{p}^n.$$

It follows that K/K_σ is a ramified extension. By the relative genus formula

$$1 = ng_\sigma + \tfrac{1}{2}\cdot d_\sigma - (n-1), \tag{68}$$

where g_σ is the genus of K_σ and d_σ is the degree of the different of K/K_σ. By the ramification of $\mathfrak{p}$ we have $d_\sigma \geqslant 1$, and by (68) this implies that $g_\sigma = 0$. Now $N_{K/K_\sigma}(\mathfrak{p}/\mathfrak{o}) = \mathfrak{p}^n/\mathfrak{o}^n$, so $\mathfrak{p}^n/\mathfrak{o}^n$ is a divisor of degree zero of the field K_σ, whence $\mathfrak{p}^n/\mathfrak{o}^n \sim 1$ in K_σ and therefore in K. Thus $n\mathfrak{p} = \mathfrak{o}$ in D_0.

Now let m be any divisor of n. If we apply what we have just proved to $\mathfrak{p}$ and the automorphism $\sigma^{n/m}$, we see that $m\mathfrak{p} = \mathfrak{o}$. If n is composite this implies $\mathfrak{p} = \mathfrak{o}$. If $n = q^\alpha$ is a prime power, then letting $m = q$ shows that $q\mathfrak{p} = \mathfrak{o}$. Since the order of A_0 divides 24 we can only have $q = 2$ or 3, and this proves Lemma 2.

(b). We now prove Lemma 1. The existence of an element ε (σ_0 in Hasse's notation) with the properties stated in Lemma 1 is proved in II. The uniqueness follows easily from the theory of the ring M of meromorphisms of K. The following proof is independent of this theory. Suppose σ is an element of A_0 of order 2. For each prime $\mathfrak{p}$ let $\mathfrak{a}_\mathfrak{p} = \mathfrak{p} + \mathfrak{p}^\sigma$. Note that $\mathfrak{a}_\mathfrak{p}^\sigma = \mathfrak{a}_\mathfrak{p}$, so that Lemma 2 implies $2\mathfrak{a}_\mathfrak{p} = \mathfrak{o}$. Since H_2 (see (14)) has order 4, this implies that $\mathfrak{a}_\mathfrak{p}$ takes on some value (in H_2) infinitely often: hence for some fixed prime $\mathfrak{q}$ and infinitely many primes $\mathfrak{p}$

we have

$$\mathfrak{p}+\mathfrak{p}^{\sigma}=\mathfrak{q}+\mathfrak{q}^{\sigma},$$

$$(\mathfrak{p}-\mathfrak{q})+(\mathfrak{p}-\mathfrak{q})^{\sigma}=\mathfrak{o}.$$

Since $\mathfrak{p}-\mathfrak{q}$ takes on infinitely many values in D_0 this implies by (25) that $\mathfrak{p}^{\sigma}=\mathfrak{p}^{\varepsilon}$ for infinitely many primes $\mathfrak{p}$. By II, p. 75, this gives that $\sigma=\varepsilon$.

(c). We turn now to the proof of (22). Let $\tau_{\mathfrak{p}}$ be the automorphism in T corresponding to the prime $\mathfrak{p}$ by means of (18). Let ι and λ be the meromorphisms of K defined by

$$(x^{\iota}, y^{\iota})=(x, y), \quad (x^{\lambda}, y^{\lambda})=(x_{\mathfrak{p}}, y_{\mathfrak{p}}), \tag{69}$$

and let τ and ρ be the meromorphisms

$$\tau=\iota-\lambda \quad \text{and} \quad \rho=\iota+\lambda.$$

(For the definition of the addition of meromorphisms see II.) If N denotes the norm of a meromorphism as defined in II, then $N(\iota)=1$ and $N(\lambda)=0$ and so by III, equation (1) we have

$$N(\tau)+N(\rho)=2N(\iota)+2N(\lambda)=2. \tag{70}$$

If $N(\tau)=0$, then τ is 'uneigentlich' (see II), so the meromorphism $\tau+2\lambda=\rho$ is also 'uneigentlich', whence $N(\rho)=0$. But this contradicts (70). It follows from (70) that $N(\tau)=N(\rho)=1$ and so τ and ρ are automorphisms of K.

We claim that $\tau=\tau_{\mathfrak{p}}$. For by II, p. 73 and the Addition theorem (II, p. 79) we have

$$\mathfrak{q}^{\tau^{-1}}=\tau\mathfrak{q}=(\iota-\lambda)\mathfrak{q}=\iota\mathfrak{q}-\lambda\mathfrak{q}=\mathfrak{q}-\mathfrak{p}$$

for all primes $\mathfrak{q}$. It follows that $\tau^{-1}=\tau_{\mathfrak{p}}^{-1}$ and so $\tau=\tau_{\mathfrak{p}}$. Finally, by (69), the definition of $\iota-\lambda$ and the fact that $\tau\neq-\iota=\varepsilon$ we have (see II, p. 79)

$$(x^{\tau}, y^{\tau})=(x^{\iota-\lambda}, y^{\iota-\lambda})=(x^{\iota}, y^{\iota})-(x^{\lambda}, y^{\lambda})$$

$$=(x, y)-(x_{\mathfrak{p}}, y_{\mathfrak{p}}),$$

where the addition is performed using (17). This completes the proof of (22).

References

A. Bremner and P. Morton (1978), 'Polynomial relations in characteristic p', *Quart. J. Math. Oxford* (2), **29**, 335–347.

J. W. S. Cassels (1966), 'Diophantine equations with special reference to elliptic curves', *J. London Math. Soc.* **41**, 193–291.

M. Deuring (1941a), 'Die Typen der Multiplikatorenringe elliptischer Funktionenkörper', *Abh. Math. Sem. Hans. Univ.* **14**, 197–272.
M. Deuring (1941b), 'Invarianten und Normalform elliptischer Funktionenkörper', *Math. Z.* **47**, 47–56.
M. Deuring (1947), 'Zur Theorie der elliptischen Funktionenkörper', *Abh. Math. Sem. Univ. Hamburg* **15**, 211–261.
H. Hasse (1934), 'Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrad p über elliptischen Funktionenkörpern der Charakteristik p', *J. Reine angew. Math.* **172**, 77–85.
H. Hasse (1936), 'Zur Theorie der abstrakten elliptischen Funktionenkörper I, II, III', *J. Reine angew. Math.* **175**, 55–62, 69–88, 193–208.
H. Hasse (1963), *Zahlentheorie* (Akademie Verlag, Berlin).
P. Roquette (1970a), *Analytic theory of elliptic functions over local fields* (Hamburger Math. Einzelschriften, Neue Folge, Heft 1).
P. Roquette (1970b), 'Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik', *Math. Z.* **117**, 157–163.
H. Stichtenoth (1973), 'Über die Automorphismengruppe eines algebraischen Funktionenkorpers von Primzahlcharakteristik I', *Arch. Math. Oberwohlfach*, **24**, 527–544.

University of Michigan
Ann Arbor, Michigan 48109