HOUSTON JOURNAL OF MATHEMATICS, Volume 2, No. 2, 1976.

ON THE DIVISION FIELDS OF AN ALGEBRAIC FUNCTION FIELD OF ONE VARIABLE. AN ESTIMATE FOR THEIR DEGREE OF IRRATIONALITY.

Peter Roquette

To the memory of Abraham Robinson.

Let F|K be an algebraic function field of one variable over an algebraically closed field of constants K. The degree of irrationality d of F is defined to be the minimum of the degrees of F over its rational subfields. We are concerned with the degree of irrationality not of F itself, but of the maximal unramified abelian extension of exponent n over F. (Here, n denotes a natural integer which is not divisible by the characteristic of F.) This extension is the n-th division field over F; let d_n denote its degree of irrationality. We shall prove that $d_n \leq d \cdot g \cdot n^{2g-2}$ where g is the genus of F; it is assumed that $g > 0$. In case of characteristic 0, the above estimate had been obtained by C. L. Siegel using the analytic theory of theta functions. Our proof, valid for arbitrary characteristic, is based on the so-called inequality of Castelnuovo-Severi in the context of Deuring's theory of correspondences. Under certain assumptions, the above estimate for d_n remains valid if the ground field K is not algebraically closed. We had used this estimate in a recent paper, written in collaboration with Abraham Robinson, on the finiteness theorem of Siegel and Mahler concerning diophantine equations.

1.Introduction. Let F|K be an algebraic function field of one variable over an algebraically closed field of constants K. If x is a nonconstant element in F, then the field degree of F over its rational subfield K(x) is finite. Let d denote the smallest of these degrees, i.e.

$$d = \operatorname{Min}_{\substack{x \in F \\ x \notin K}} [F: K(x)].$$

We shall refer to d as the *degree of irrationality* of F|K. It is an immediate consequence of the theorem of Riemann-Roch that $d \leq g+1$, where g denotes the genus of F|K. It is known that this estimate can be improved to be

$$d \leq \frac{g+3}{2}$$

and that this is best possible in general. (I have been informed by G. Martens that this classical estimate holds also in the case of prime characteristic. See [5].) In this paper, we are concerned with a special class of fields, namely the so-called division fields over F. For these fields, the above estimate can be improved in its order of magnitude.

We consider the following situation. n denotes a natural number which is not divisible by the characteristic of F. Let F_n be the maximal unramified abelian extension of exponent n over F. It is well known that

$$[F_n: F] = n^{2g}.$$

Since $F_n|F$ is unramified, the genus g_n of F_n is computed by the formula

$$g_n = 1 + n^{2g}(g-1).$$

We are looking for an estimate of the degree of irrationality d_n of F_n. We may assume that $g > 0$, since otherwise $F_n = F$ and hence $d_n = d = 1$. If $g = 1$, then also $g_n = 1$ and hence $d_n = d = 2$; in this case the following estimate is trivial. We shall prove

THEOREM 1.1. *In the situation as described above, the degree of irrationality d_n of F_n satisfies*

$$d_n \leq d \cdot g \cdot n^{2g-2}.$$

The essential feature is that the power n^{2g-2} which enters into this estimate, is of smaller order of magnitude than the power n^{2g} which determines the genus g_n of F_n.

In case of characteristic zero, an estimate of the above order of magnitude has been obtained by C. L. Siegel, using the analytic theory of theta functions. ([13], page 254, line 6 from below. There, the inequality of Theorem 1.1 is stated for large n only. This is due to the fact that our field F_n corresponds only for large n to the unramified covering surface as constructed in [13]. Also, in [13] the constant factor $d \cdot g^3$ appears whereas in Theorem 1.1 we see that $d \cdot g$ will suffice.) Siegel used this estimate in the proof of his finiteness theorem concerning binary diophantine equations. Recently, in a paper written in collaboration with Abraham Robinson, we have given a nonstandard proof of Siegel's theorem and also of Mahler's generalization. At a certain stage of our proof, we had to use Siegel's estimate of d_n. ([7], Section 7, Lemma 7.5.) At that occasion, there arose the question of whether this estimate is susceptible of an algebraic proof which, hopefully, would extend to arbitrary characteristic. Such a proof will be presented in this paper.

Basically, our proof rests upon the so-called inequality of Castelnuovo-Severi, as we have developed it earlier in the context of Deuring's theory of correspondences [8], [9]. In order to obtain the connection between our problem and the theory of correspondences, we shall show that the field F_n as defined above, admits a representation as field of definition for certain divisors; this then will justify the terminology of F_n to be the *n-th division field over* F. For details, we refer to Theorem 6.1 of Section 6. This theorem is of importance also in its own right, independently of its application to the problem of estimating d_n.

We have said above that Theorem 1.1 is used in [7]. This is not quite correct, however, since in Theorem 1.1 the ground field K is assumed to be algebraically closed, wheras in [7] the field K is an algebraic number field of finite degree. Hence, before being able to apply Theorem 1.1 to the situation as considered in [7], we have first to discuss its generalization to arbitrary ground fields K, not necessarily algebraically closed. In doing so, we assume the function field F|K to be conservative, i.e. its genus g should not change while extending the field of constants. In geometrical terms, this assumption means that F|K admits a model free of singularities. Also, for technical reasons we have to assume that the ground field K is infinite.

Again, the degree d of irrationality of F|K is defined to be the minimum of the degrees $[F: K(x)]$ where $x \in F$, $x \notin K$.

If the ground field K is not algebraically closed, then the definition of the field extension F_n over F has to be modified. This is because the "maximal unramified abelian extension of exponent n" would in general also involve an extension of the field of constants, whereas in the present context we are interested in such extensions only which preserve the field of constants. The correct definition of F_n as a finite extension of F is by means of the following properties (i) - (iv).

(i) F_n *is regular over* K. That is, F_n is separably generated over K, and K is algebraically closed in F_n. It is well known that this is equivalent to saying that F_n is K-linearly disjoint to the algebraic closure K^a of K.

(ii) F_n *is unramified over* F.

(iii) F_n *is semi-abelian of exponent* n *over* F. By this we mean that after suitable extension $K' \supset K$ of the ground field, the field F_nK' will be abelian of exponent n over FK'. Obviously, we can take $K' = K^a$ to be the algebraic closure of K.

(iv) $[F_n: F] = n^{2g}$.

It follows from these conditions that F_nK^a is the *maximal* extension of FK^a which is unramified and abelian of exponent n. In other words, after extending the ground field K to its algebraic closure, we have the situation of Theorem 1.1.

Such a field F_n, if it exists, is not unique in general. That is, for a given number n there may exist several non-isomorphic field extensions of F all of which satisfy (i) - (iv). (The different fields F_n may be characterized by a certain one-dimensional Galois cohomology group. See e.g. [12], §4, Proposition 6.) However, all such fields F_n become equal after suitable extension of the field of constants.

Again, if a field F_n satisfying (i) - (iv) is given, we denote by d_n its degree of irrationality over K. There arises the question of whether the inequality of Theorem 1.1 remains valid in this situation. Now, this is not true in general; there are counterexamples of fields F_n which have no divisor of small degree. On the other hand, if we assume that F_n and F have sufficiently many prime divisors of degree 1 then the above question is answered affirmatively.

THEOREM 1.2. *Let $F|K$ be a conservative function field of genus $g > 0$, its field of constants K being arbitrary infinite, not necessarily algebraically closed. Let F_n denote an extension of F satisfying the conditions (i) - (iv) above.*

If $F|K$ admits at least 2g-1 prime divisors of degree 1, and if $F_n|K$ admits at least one prime divisor of degree 1, then again

$$d_n \leqslant d \cdot g \cdot n^{2g-2}.$$

For the proof see Section 7.

In the situation of our earlier paper [7], the fields F and F_n both are embedded into a nonstandard model *K of K ([7], Theorem 7.4, where we have written E_n instead of F_n) and hence have infinitely many primes of degree 1. ([7], Section 5, Remark 5.6.) Therefore, the inequality of Theorem 1.2 holds in that situation (See [7], Lemma 7.5, where we have cited this result).

2. Symmetric field composita. Until further notice in Section 7, the ground field K is assumed to be algebraically closed.

According to the introduction, we consider a function field F|K of one variable. Let d,g denote the degree of irrationality and the genus of F respectively. If necessary, we assume $g > 0$.

We work in a universal extension field $\tilde{K}$ of K, which we assume to be algebraically closed and of degree of transcendency $\geqslant 1$ over K. The field F admits a K-isomorphic embedding μ: $F \to \tilde{K}$ into $\tilde{K}$. Such an isomorphism is written as right operator, i.e. $x\mu$ denotes the image of $x \in F$ and $\tilde{K} \supset F\mu$ is the image field. If τ is a K-automorphism of $\tilde{K}$ then $\mu\tau$ is another embedding of F into $\tilde{K}$. That is, the embeddings of F into $\tilde{K}$ are permuted by the K-automorphisms of $\tilde{K}$.

Now let $\mu_1,\mu_2,\ldots,\mu_r$ be a system of r embeddings of F into $\tilde{K}$; in this context we tacitly assume that they are mutually different, i.e. $\mu_i \neq \mu_j$ if $i \neq j$. The image fields $\tilde{K} \supset F\mu_i$ generate a subfield of $\tilde{K}$ which is called the *compositum* of $\mu_1,\mu_2,\ldots,\mu_r$ and is denoted by

$$F\mu_1 F\mu_2 \cdots F\mu_r.$$

In addition to this ordinary compositum, we have to consider the symmetric compositum, which is defined as follows.

We consider those K-automorphisms τ of $\tilde{K}$ which permute the embeddings $\mu_1,\mu_2,\ldots,\mu_r$. They form a group, say G. Every $\tau \in G$ induces in the compositum $F\mu_1 \cdots F\mu_r$ a certain automorphism, and this induced automorphism is the identity if and only if $\mu_i\tau = \mu_i$ $(1 \leqslant i \leqslant r)$. Hence, the automorphism group of $F\mu_1 \cdots F\mu_r$ induced by G is finite, being isomorphic to a permutation group of the r objects $\mu_1,\ldots,\mu_r$. The field of fixed elements in $F\mu_1 \cdots F\mu_r$ with respect to this automorphism group is called the *symmetric compositum* of $\mu_1,\ldots,\mu_r$, and it is denoted by

$$F\mu_1 \circ F\mu_2 \circ \cdots \circ F\mu_r.$$

By construction, the ordinary compositum is a finite Galois extension of the symmetric compositum, and its degree k satisfies $k \leqslant r!$.

Let s_i denote the degree of $F\mu_1 \cdots F\mu_r$ over $F\mu_i$. Then the number

$$s = \frac{1}{k} \sum_{1 \leqslant i \leqslant r} s_i$$

is called the co-degree of the symmetric compositum $F\mu_1 \circ \cdots \circ F\mu_r$ (whereas the number r is called its "degree"). The co-degree s is finite if and only if each s_i is finite, which is already the case if at least one of the s_i is finite, i.e. if $F\mu_1 \cdots F\mu_r$ is of degree of transcendency 1 over K. If this is so, then s is easily seen to be an integer; we shall see below that s can be regarded as the degree of a certain divisor.

LEMMA 2.1. *Let $E|K$ be an algebraic function field of one variable, and $E \subset \tilde{K}$.*

We assume that E admits a representation as an r-fold symmetric compositum of F, i.e.

$$E = F\mu_1 \circ F\mu_2 \circ \cdots \circ F\mu_r.$$

Let s denote the co-degree of this symmetric compositum. Then the degree of irrationality d_E of E satisfies

$$d_E \leqslant d \cdot s.$$

Recall that d denotes the degree of irrationality of F.

PROOF. Let $x \in F$ be such that $[F: K(x)] = d$. We put $x_i = x\mu_i$ and

$$y = x_1 x_2 \cdots x_r.$$

Since y is a symmetric function of the x_i, it is clear that y is contained in the symmetric compositum E. Let us first assume that y is nonconstant, i.e. $y \notin K$. We claim that $[E: K(y)] \leqslant s \cdot d$.

For brevity, we put $E' = F\mu_1 \cdots F\mu_r$ and $k = [E': E]$. Then our contention is that

$$[E': K(y)] \leqslant k \cdot s \cdot d = \sum_{1 \leqslant i \leqslant r} s_i \cdot d,$$

in view of the above definition of the co-degree s. We have $s_i = [E': F\mu_i]$ and hence

$$\begin{aligned} s_i \cdot d &= [E': F\mu_i] \cdot [F: K(x)] \\ &= [E': F\mu_i]\,[F\mu_i: K(x_i)] \\ &= [E': K(x_i)] \\ &= \deg(N_i) \end{aligned}$$

where N_i denotes the divisor of poles of x_i in E'.

From the above definition of y, it is clear that every pole of y is also a pole of some x_i, and that the pole divisor N of y satisfies

$$N \leqslant \sum_{1 \leqslant i \leqslant r} N_i.$$

Therefore,

$$[E': K(y)] = \deg(N) \leqslant \sum_1 \deg(N_i) = \sum_1 s_i \cdot d,$$

as contended.

The above argument was based on the assumption that y is nonconstant. If y is constant, then we try to choose a constant $a \in K$ such that the element

$$y_a = (x_1 - a)(x_2 - a) \cdots (x_r - a)$$

is nonconstant, so that the above argument can be applied to x-a and y_a in place of x and y. Let Q be a prime of E' which is a pole of some x_i, say a pole of x_1. Let us

choose $a \in K$ such that

$$x_i(Q) \neq a \qquad (2 \leqslant i \leqslant r).$$

(Notation: If Q is a prime (= place) of a field and if x is an element of that field then x(Q) denotes the image of x with respect to the place Q. We have $x(Q) = \infty$ if and only if Q is a pole of x, which is to say that x is not contained in the valuation ring belonging to Q. Sometimes we shall write xQ instead of x(Q).)These conditions say that Q is not a zero of x_i-a, for every $i \geqslant 2$. In view of the above definition of y_a we see that Q, being a pole of x_1-a, is not cancelled in the product and hence remains to be a pole of y_a. In other words: y_a has at least one pole and is therefore nonconstant.

Now, applying the above arguments to x-a and y_a we conclude that

$$[E: K(y_a)] \leqslant s \cdot d.$$

It follows

$$d_E \leqslant s \cdot d$$

in view of the definition of the degree of irrationality. QED.

Our next aim is to obtain an estimate for the co-degree s of a symmetric compositum. Before doing so, it is convenient to give a description of symmetric composita as defining fields of divisors. This is done as follows.

Let us consider the constant extension $F\tilde{K}$ of F, defined to be the quotient field of the tensor product $F \underset{K}{\otimes} \tilde{K}$. Until further notice, we identify F with the left factor and $\tilde{K}$ with the right factor of that tensor product; thus F and $\tilde{K}$ now appear as K-linear disjoint subfields of $F\tilde{K}$. We regard $F\tilde{K}$ as an algebraic function field of one variable with $\tilde{K}$ as its field of constants. Every prime P of F|K has a unique extension to a prime of $F\tilde{K}|\tilde{K}$; we denote this extension also with the same symbol P. The primes of $F\tilde{K}$ thus obtained are called the *constant primes*; by definition they correspond 1-1 to the primes of F.

In addition, there are the *nonconstant primes* M of $F\tilde{K}$, which are characterized by the fact that they are trivial on F. (Of course, they are also trivial on $\tilde{K}$, since we are considering primes of the function field $F\tilde{K}$ with $\tilde{K}$ as its field of constants.) The map $x \to x(M)$ induces in F a K-isomorphism into $\tilde{K}$, i.e. an embedding μ: $F \to \tilde{K}$. In this way, the nonconstant primes of $F\tilde{K}$ correspond 1-1 to the embeddings μ of F into $\tilde{K}$. This correspondence is given by the formula

$$x(M) = x\mu \qquad (x \in F)$$

if M corresponds to μ.

Every system $\mu_1,\mu_2,\ldots,\mu_r$ of embeddings $F \to \tilde{K}$ yields an integral divisor

$$Z = M_1 + M_2 + \cdots + M_r$$

of $F\tilde{K}$, where the M_i are the primes belonging to the μ_i. Since all components of Z are nonconstant, Z is called totally nonconstant. If $i \neq j$ then $\mu_i \neq \mu_j$ and hence $M_i \neq M_j$; in other words: Z is without multiple components. *In this way, the systems* $\mu_1,\mu_2,\ldots,\mu_r$ *of embeddings* $F \to \tilde{K}$ *correspond 1-1 to the integral, totally nonconstant divisors Z of* $F\tilde{K}$ *without multiple components.*

Let $D(F\tilde{K})$ denote the divisor group of $F\tilde{K}|\tilde{K}$. Similarly, if E is a subfield of $\tilde{K}$ containing K, then $D(FE)$ denotes the divisor group of FE|E. If we regard $F\tilde{K}$ as a constant extension of FE then the inclusion $FE \subset F\tilde{K}$ yields a natural injection $D(FE) \subset D(F\tilde{K})$ of the respective divisor groups, by means of which we regard $D(FE)$ as a subgroup of $D(F\tilde{K})$. This injection preserves the degree and the dimension of divisors. That is, the degree and the dimension of a divisor $Z \in D(FE)$ are independent of whether we regard Z as a divisor of FE or as a divisor of $F\tilde{K}$. The divisors in $D(FE)$ are said to be defined over E. Now let $Z \in D(F\tilde{K})$. Among all subfields $E \subset \tilde{K}$ containing K, over which Z is defined, there is a unique minimal field; this field is denoted by K(Z) and is called *the field of definition of the divisor* Z.

In an earlier paper [11], we have given a construction of these fields of definition as certain generalized symmetric composita. (In [11] we use the name "coordinate field" (Koordinatenkörper) instead of "field of definition". For another treatment of fields of definition, see [1].) Now, if $Z = M_1 + M_2 + \cdots + M_r$ is an integral, totally nonconstant divisor without multiple components, then K(Z) is identical with the symmetric compositum

$$K(Z) = F\mu_1 \circ F\mu_2 \circ \cdots \circ F\mu_r,$$

where μ_i: $F \to \tilde{K}$ is the embedding belonging to M_i as above. This follows directly from our construction as given in [11]. (In particular, if Z = M is a nonconstant prime with its corresponding embedding μ: $F \to \tilde{K}$, then we see that $K(M) = F\mu$. That is, M is defined over a subfield $E \subset \tilde{K}$ if and only if E contains the image field $F\mu$.)

The "degree" r of the symmetric compositum $F\mu_1 \circ \cdots \circ F\mu_r$ can now be interpreted as the degree of the corresponding divisor $Z = M_1 + \cdots + M_r$. Notice that the divisor degree is independent of whether we regard Z as a divisor of $F\tilde{K}$ or as a

divisor of FE, provided Z is defined over $E \subset \tilde{K}$. Thus we may write

$$r = \deg_{FE|E}(Z) \qquad \text{if } K(Z) \subset E \subset \tilde{K}.$$

Here, the notation $\deg_{FE|E}$ is meant to emphasize that the divisor degree is to be understood in the field FE with E as its field of constants.

Now let us assume in addition that E is an algebraic function field of one variable over K. In this case, we may regard FE as an algebraic function field of one variable not only over E but also over F as its field of constants; in the latter case, FE|F is a constant extension of E|K. Since every component of Z is trivial on F, we may now regard Z as a divisor of FE|F. As such a divisor, it also has a degree; we claim that

$$(2.1)\quad [E: K(z)] \cdot s = \deg_{FE|F}(Z) \qquad \text{if } K(Z) \subset E \subset \tilde{K},$$

where s is the co-degree of the symmetric compositum $F\mu_1 \circ \cdots \circ F\mu_r$ as defined above.

In order to verify this formula, let us make the following preliminary remark. Consider an extension E′ of finite degree over E. If in (2.1) we replace E by E′ then clearly the left hand side is multiplied by the field degree $[E': E]$. But the same is also true for the right hand side of (2.1), i.e. we have

$$\deg_{FE'|F}(Z) = [E': E] \cdot \deg_{FE|F}(Z).$$

This is because we have to regard the degrees over F as the field of constants; thus the field of constants does not change if FE is extended to FE′; therefore the divisor degree is multiplied by the field degree $[FE': FE] = [E': E]$.

We have seen that both the left hand side and the right hand side of (2.1) is multiplied by $[E': E]$ if E is replaced by E′. Hence, the validity of (2.1) for E′ implies its validity for E, and conversely. Therefore, in order to prove (2.1) we may extend the field E (by a finite extension) or contract it, as seems suitable.

First, we extend E in such a way that it contains each image field $F\mu_i$, which is to say that each component M_i of Z is defined over E. We then have

$$\deg_{FE|F}(Z) = \sum_{1 \le i \le r} \deg_{FE|F}(M_i).$$

On the other hand, since E contains the compositum $F\mu_1 \cdots F\mu_r$, and since K(Z) equals the symmetric compositum $F\mu_1 \circ \cdots \circ F\mu_r$, we have

$$[E: K(Z)] \cdot s = \sum_{1 \le i \le r} [E: F\mu_i]$$

by the very definition of the co-degree s. Therefore, in order to prove (2.1) we have to verify that

(2.2) $[E: F\mu_i] = \deg_{FE|F}(M_i) \qquad (1 \leqslant i \leqslant r).$

Here, M_i is a prime divisor of the field FE whose residue field is E; the residue homomorphism induces in F the isomorphic embedding $F \to F\mu_i$. Therefore, $[E: F\mu_i]$ is the degree of the residue field of M_i over the isomorphic image of F, which is to say that $[E: F\mu_i]$ is the degree of the prime M_i of FE over F as ground field. Hence (2.2) holds.

Formula (2.1) is now proved. In this formula, we may take E = K(Z); we obtain

(2.3) $s = \deg_{FE|F}(Z) \qquad$ if $E = K(Z)$.

This formula yields an interpretation of the co-degree by means of the degree of a divisor; in particular, we see that s is an integer, as mentioned above already.

The above discussion shows that Lemma 1 may be reformulated in terms of the field of definition of divisors, instead of symmetric composita. We obtain:

LEMMA 2.2. *Let E be an algebraic function field of one variable, and* $E \subset \tilde{K}$. *We assume that there is an integral divisor Z of* $F\tilde{K}$, *totally nonconstant and without multiple components, such that*

$$E = K(Z),$$

i.e. E is the field of definition of Z. Then the degree of irrationality d_E *satisfies*

$$d_E \leqslant d \cdot s,$$

where $s = \deg_{FE|F}(Z)$.

A further estimate for s will be obtained with the help of the inequality of Catelnuovo-Severi, but for "normalized" divisors Z only. In the next section, we shall explain this notion of normalized divisor and develop its relevant properties.

3. **Normalized divisors.** We retain the notations introduced in Section 2. In particular, $\tilde{K}$ is a universal extension of K, and $F\tilde{K}$ is the corresponding constant extension of F.

A divisor Z of $F\tilde{K}$ is called *nonspecial* if it is integral and if dim(Z) = 1. Here, the dimension is to be understood in the sense of the theorem of Riemann-Roch. The condition dim(Z) = 1 is equivalent to saying that Z is the only integral divisor in its class. That is, if $Z \sim Z'$ and $Z' \geqslant 0$ then $Z = Z'$. (The relation $Z \sim Z'$ denotes the ordinary divisor equivalence, modulo principal divisors.) Every nonspecial divisor is of

degree $\leqslant g$.

If a divisor is defined over K then it is called a *constant divisor*; this is the case if and only if each of its components is a constant prime divisor. We write $Z \approx Z'$ if Z and Z' are equivalent up to a constant divisor, i.e. if there exists a constant divisor A such that $Z \sim Z' + A$. The relation $Z \approx Z'$ is called the *coarse equivalence relation*. ("Gröbere Äquivalenz" in the sense of Deuring [3].)

LEMMA 3.1. *Let Z be a nonspecial divisor of $F\tilde{K}$. If Z' is any other divisor of $F\tilde{K}$ such that $Z \approx Z'$, then $K(Z) \subset K(Z')$. If in addition Z' is nonspecial too then $K(Z) = K(Z')$.*

In other words: K(Z) is the unique minimal field among all fields of definition for divisors which are coarse equivalent to Z.

PROOF. For brevity, let us put $E = K(Z')$. We have to show that Z is defined over E. By assumption, there is a constant divisor A such that $Z \sim Z' + A$. Since A is constant, $Z'+A$ is defined over E. We have $\dim(Z'+A) = \dim(Z) = 1$ because Z is nonspecial. Now, the dimension of $Z'+A$ is independent of whether we regard $Z'+A$ as a divisor of $F\tilde{K}$ or as a divisor of FE. In the latter case, the relation $\dim(Z'+A) = 1$ implies that there exists a unique integral divisor X of FE such that $X \sim Z'+A$. By construction, X is defined over E. On the other hand, in $F\tilde{K}$ we have $X \sim Z'+A \sim Z$ and therfore $X = Z$ since Z is nonspecial. We conclude that Z is defined over E. QED.

Our aim in this section is to construct in every coarse equivalence class a unique divisor which is "normalized" in a certain sense. These normalized divisors will be nonspecial; this explains why we are interested in the above lemma concerning nonspecial divisors. But not every nonspecial divisor is normalized. Before stating the definition of "normalized" divisor, let us recall the following facts about specialization of divisors.

We consider a K-place (i.e. a place which is the identity on K)

$$o: \tilde{K} \to K.$$

Since K is algebraically closed, such places do exist; the identity map $K \to K$ can be extended to a place from $\tilde{K}$ to K. By means of o, the constant field $\tilde{K}$ of $F\tilde{K}$ is reduced to the constant field K of F. It is well known that this yields a corresponding homomorphism of the divisor groups

$$o: D(F\tilde{K}) \to D(F)$$

which reduces the divisor group of $F\tilde{K}$ to the divisor group of F. In an earlier paper [10], we have given a construction of this homomorphism and proved its basic properties, namely the following.

If Z is a divisor in $D(F\tilde{K})$ then we write Zo for its image in $D(F)$; in the present context we shall call Zo the *specialization* of Z by means of o. The homomorphism $Z \mapsto Zo$ preserves the divisibility relation:

$$\text{if } Z \leqslant Z' \text{ then } Zo \leqslant Z'o$$

as well as the equivalence relation:

$$\text{if } Z \sim Z' \text{ then } Zo \sim Z'o.$$

Moreover, the degree is preserved:

$$\deg(Zo) = \deg(Z)$$

and constant divisors are unchanged:

$$\text{if } A \in D(F) \text{ then } Ao = A.$$

If M is a nonconstant prime divisor of $F\tilde{K}$ then its specialization Mo can be described as follows. First, the above properties imply that Mo is an integral divisor of degree one, hence a prime divisor (= place) of F|K. Now, *this place* $Mo : F \to K$ *is obtained as the composition of the two maps* $M: F \to \tilde{K}$ and $o: \tilde{K} \to K$. This statement can be expressed by the formula:

$$(3.1)\quad x \cdot Mo = xM \cdot o \qquad (x \in F).$$

As said above, the proofs of the above mentioned properties of specializations can be found in our paper [10].

This being said, we can now state the definition of "normalized" divisor. This concept is not canonical; it refers to two auxiliary data which are assumed to be given in advance, namely:

(i) a K-place $o: \tilde{K} \to K$ as above;

(ii) a nonspecial divisor B of F|K of degree g, without multiple components. (It is well known that there are infinitely many such divisors B if $g > 0$. See e.g. [4], page 470. If $g = 0$ then $B = 0$ is the only nonspecial divisor of F|K.)

Referring to these data, we give the following

DEFINITION. A divisor Z of $F\tilde{K}$ is called normalized if Z is integral, totally nonconstant and if $Zo \leqslant B$.

More precisely, Z should be called o,B - normalized. If o',B' is another datum

satisfying (i) and (ii) then the o,B-normalized divisor need not be o',B'-normalized. We shall call o and B the *normalization parameters* which enter into the definition of "normalized divisor". In the following, we regard o and B as being fixed, and then we omit the reference to o and B. Our results will be independent of the choice of the normalizing parameters (except in Section 7 where the ground field will not be algebraically closed).

If Z is normalized then $\deg(Z) \leq g$. This follows from the fact that the degree is preserved under specialization; we have $\deg(Z) = \deg(Zo) \leq \deg(B) = g$.

Furthermore, a normalized divisor Z has no multiple components. This follows from the fact that the divisorial divisibility relation $\leq$ is preserved under specialization; if M would be a multiple component of Z then $2M \leq Z$, hence $2 \cdot Mo \leq Zo \leq B$, contradicting the fact that B is free from multiple components.

Another property of normalized divisors is that they are *nonspecial*. To show this, we observe that Zo divides the nonspecial divisor B, hence Zo is nonspecial too. From this our contention follows in view of the general

LEMMA 3.2. *Let Z be an integral divisor of $F\tilde{K}$. If Zo is nonspecial, then Z is nonspecial too.* (More generally, for any divisor of $F\tilde{K}$ one can show the inequality $\dim(Z) \leq \dim(Zo)$.)

PROOF. We first assume that, in addition, Z is of degree g. In this case, we conclude from the theorem of Riemann-Roch that

$$\dim(Z) = 1 + \dim(W\text{-}Z)$$

where W is a canonical divisor of F|K. (Observe that W is also canonical divisor of $F\tilde{K}|\tilde{K}$.) If Z were special, then $\dim(Z) > 1$ and hence $\dim(W\text{-}Z) > 0$; this means that there exists an integral divisor X which is equivalent to W-Z:

$$X \geq 0 \text{ and } X \sim W\text{-}Z.$$

Specialization yields:

$$Xo \geq 0 \text{ and } Xo \sim W - Zo.$$

(Observe that W is constant and hence $Wo = W$.) Thus there exists at least one integral divisor which is equivalent to $W - Zo$; this means that $\dim(W - Zo) > 0$. Now, $\deg(Zo) = \deg(Z) = g$; hence we have again by Riemann-Roch:

$$\dim(Zo) = 1 + \dim(W - Zo) > 1,$$

contradicting the fact that Zo is nonspecial.

We have proved Lemma 3.2 in the case where $\deg(Z) = g$. The general case is reduced to this one as follows. Since Zo is nonspecial, it follows from the Riemann-Roch theorem that $\deg(Zo) \leqslant g$; moreover, there is an integral divisor $A \geqslant 0$ of $F|K$ such that $Zo + A$ is of degree g and nonspecial ([4], page 470). Since $Ao = A$ we have

$$(Z + A)o = Zo + A.$$

In particular, $\deg(Z + A) = \deg(Zo + A) = g$. By what we have shown above, $Z + A$ is nonspecial. From this we conclude that Z, which is a divisor of $Z + A$, is nonspecial too. QED

Our next result says that our notion of "normalized" divisor, as defined above, serves to select from every coarse divisor class a unique representative. Moreover, this representative is minimal as regards the field of definition. More precisely, we have

LEMMA 3.4. *Given any divisor Z' of $F\tilde{K}$, there exists one and only one normalized divisor Z such that $Z \approx Z'$. We have $K(Z) \subset K(Z')$, i.e. Z is defined over every field, over which Z' is defined. If Z' is nonspecial then $K(Z) = K(Z')$.*

(i) Existence: Consider the constant divisor $A' = B - Z'o$. We have

$$(Z' + A')o = Z'o + A' = B.$$

In particular, we conclude that $\deg(Z' + A') = \deg(B) = g$. Hence, by the Riemann-Roch theorem, there exists an integral divisor Z'' which is equivalent to $Z' + A'$, i.e.

$$Z'' \geqslant 0 \text{ and } Z'' \sim Z' + A'.$$

From the second of these relations we deduce that $Z''o \sim (Z' + A')o = B$. From the first relation, $Z''o \geqslant 0$. It follows

$$Z''o = B$$

since B is nonspecial. The divisor Z'' may contain constant components; let A denote its constant part and Z its totally nonconstant part, so that

$$Z \geqslant 0,\ A \geqslant 0 \text{ and } Z'' = Z + A.$$

From $Z \leqslant Z''$ we deduce

$$Zo \leqslant Z''o = B,$$

showing that Z is normalized. By construction,

$$Z = Z'' - A \sim Z' + A' - A \approx Z'.$$

(ii) Field of definition: We have seen above that every normalized divisor Z

is nonspecial. Hence, from $Z \approx Z'$ we conclude $K(Z) \subset K(Z')$, in view of Lemma 3.1. If Z' is nonspecial, then again by Lemma 3.1 we have $K(Z) = K(Z')$.

(iii) Uniqueness: We assume that both Z,Z' are normalized divisors, and $Z \approx Z'$. We have to show that $Z = Z'$. Let us define constant divisors A,A' by

$$A = B - Zo, \quad A' = B - Z'o.$$

Since Z and Z' are normalized, we have

$$A \geqslant 0 \text{ and } A' \geqslant 0.$$

Moreover, the definition of A and A' shows that

$$(Z + A)o = B = (Z' + A')o.$$

The assumption $Z \approx Z'$ implies $Z + A \approx Z' + A'$, hence

$$Z + A \sim Z' + A' + C$$

where C is some constant divisor. Specialization by o yields $B \sim B + C$, hence $C \sim 0$ and therefore

$$Z + A \sim Z' + A'.$$

Since $(Z + A)o = B$ is a nonspecial divisor, we conclude from Lemma 3.2 that $Z + A$ is nonspecial too. Hence the above equivalence implies

$$Z + A = Z' + A'.$$

Now, Z is totally nonconstant and A is constant. Thus Z can be characterized as the totally nonconstant part of the divisor $Z + A$. Similarly, Z' is the totally nonconstant part of $Z' + A'$. Hence the relation $Z + A = Z' + A'$ implies $Z = Z'$. QED

4. The inequality of Castelnuovo-Severi. For a normalized divisor Z, we are now going to give an estimate for his co-degree (in the sense of Lemma 2.2). For this we have to use the inequality of Castelnuovo-Severi. Let us first recall the relevant notions and facts about the Weil metric.

Let $E|K$ denote an algebraic function field of one variable, such that $E \subset \tilde{K}$. According to [9], the divisor group $D(FE)$ carries naturally a symmetric bilinear form $\sigma(Z,Z')$ whose values are rational integers. The value $\sigma(Z,Z')$ depends only on the coarse equivalence classes of the divisors Z and Z'. The inequality of Castelnuovo-Severi says that the corresponding quadratic form is positive definite, i.e.

$$\sigma(Z,Z) > 0 \qquad \text{if } Z \not\sim 0.$$

σ is called the *Weil metric* of the field FE.

Our proof of the inequality of Castelnuovo-Severi, as given in [9], yields at the

same time a more detailed result, which can be explained as follows.

Since $\sigma(Z,Z)$ depends on the coarse equivalence class of Z only, we may assume Z to be *normalized*, according to Lemma 3.4. (In [9], page 246 our terminology is "besonderer Divisor" instead of "normalized divisor.") Now we put

$$r = \deg_{FE|E}(Z), \quad s = \deg_{FE|F}(Z).$$

That is, r is the degree and s the "co-degree" of the normalized divisor $Z \in D(FE)$. According to the definition of the Weil metric, we have ([9], page 244, (3) and (4))

$$\sigma(Z,Z) = 2rs - \chi(Z,Z)$$

where $\chi(Z,Z)$ is a certain other quadratic form on the divisor group of FE. We need not go into the details of the definition of $\chi(Z,Z)$, which can be interpreted as a self-intersection number. What we want to point out is that we have proved in [9] the following formula: ([9], page 247, (7))

$$\chi(Z,Z) \leqslant 2(r-1)s.$$

This yields

$$\sigma(Z,Z) \geqslant 2s$$

for every normalized divisor Z. If $Z > 0$ then $s > 0$ and thus the inequality of Castelnuovo-Severi follows.

By what we have said, the following statement holds, the proof of which is contained in [9].

LEMMA 4.1. *Let $E|K$ be an algebraic function field of one variable, and $E \subset \tilde{K}$. Let Z be a normalized divisor, defined over E. Then its co-degree $s = \deg_{FE|F}(Z)$ admits the estimate*

$$s \leqslant 1/2 \cdot \sigma(Z,Z)$$

where σ denotes the Weil metric of the field FE.

Combining this with Lemma 2.2 we obtain as an immediate corollary:

LEMMA 4.2. *In the same situation as in Lemma 4.1 assume in addition that E is the field of definition of Z, i.e. $E = K(Z)$. Then the degree of irrationality d_E of E satisfies*

$$d_E \leqslant d/2 \cdot \sigma(Z,Z).$$

REMARK 4.3. The Weil metric is defined on the divisor group of FE, and thus it depends on the field F as well as on E. In our situation, the field F is to be regarded as given, whereas E may vary inside $\tilde{K}$. If we want to indicate which field E we are

considering then we write $\sigma_E(Z,Z)$. If E′ is a finite algebraic extension of E then we have

$$\sigma_{E'}(Z,Z) = [E': E] \cdot \sigma_E(Z,Z)$$

for every divisor Z of FE. In other words: if we extend the field E to E′ then the Weil metric is multiplied by the field degree [E′: E]. (The reason is that the Weil metric is defined by means of degrees of certain divisors, and that these degrees are multiplied by the field degree if E is extended to E′. See [9], page 244, (4) and page 241, (13).) We shall have to use this remark in the next section.

5. **n-division.** In the following, n denotes a natural number.

LEMMA 5.1. *The group of coarse divisor classes of $F\tilde{K}$ is uniquely divisible by n. That is, for every divisor Z of $F\tilde{K}$ there exists a divisor X, uniquely determined up to coarse equivalence, such that $nX \approx Z$.*

X can be chosen such as to be algebraic over K(Z). If n is not divisible by the characteristic of F, then X can be chosen to be separably algebraic over K(Z).

Here, X is called (separably) algebraic over K(Z) if X is defined over some (separably) algebraic extension of K(Z).

The proof of Lemma 5.1 is based on the following two statements (A) and (B), well known from the theory of algebraic function fields, concerning the divisibility of the group of divisor classes of degree 0. If L is any subfield of $\tilde{K}$ containing K, then $C_0(FL)$ denotes the group of divisor classes (modulo principal divisors) of degree 0 of the function field FL. If $L \subset L'$ then $C_0(FL) \subset C_0(FL')$. That is, the map $L \mapsto C_0(FL)$ determines a functor from fields to abelian groups ($C_0(FL)$ can be interpreted as the group of L-rational points of the Jacobian variety belonging to the function field F.)

(A) *If L is algebraically closed then $C_0(FL)$ is divisible by n. In case n is relatively prime to the characteristic, then it suffices that L is separably algebraically closed.*

The division by n in $C_0(FL)$ is in general not unique. That is, there may be torsion elements in $C_0(FL)$. We denote by $C_n(FL)$ the group of those divisor classes of degree 0 which are annihilated by n. The elements of $C_n(FL)$ are usually referred to as the n-*th division classes* of the function field FL.

(B) *There are only finitely many n-th division classes in $C_0(FL)$, and all of them are defined over K. That is, we have $C_n(FL) = C_n(F)$. The order of $C_n(F)$ is* $\leq$

n^{2g}, and it is $= n^{2g}$ if n is relatively prime to the characteristic.

This being said, we now turn to the

PROOF OF LEMMA 5.1. (i) Let L denote the algebraic closure of K(Z). We know that Z is defined over L, and hence Z determines a certain divisor class of the function field FL. In general Z is not of degree 0 and hence statement (A) cannot be applied directly. Therefore, we first replace Z by a divisor which is of degree 0, e.g. $Z' = Z - A$ where A is some constant divisor which is of the same degree as Z:

$$\deg(A) = \deg(Z).$$

Since A is constant, Z' is defined over K(Z) and hence also over L. Since $\deg(Z') = 0$, we infer from statement (A) that the class of Z' in $C_0(FL)$ is divisible by n. That is, there exists a divisor X of FL such that

$$nX \sim Z' = Z - A \approx Z.$$

By construction, X is defined over L, the algebraic closure of K(Z). This means that X is algebraic over K(Z).

If n is not divisible by the characteristic, then we define L to be the separably-algebraic closure of K(Z); the same proof as above then yields a divisor X, separably-algebraic over K(Z), such that $nX \approx Z$.

(ii) It remains to prove the uniqueness statement of Lemma 5.1. This is equivalent to the statement that the coarse divisor class group of $F\tilde{K}$ has no torsion. Accordingly, we now assume that $nX \approx 0$ for some divisor X of $F\tilde{K}$; we have to show that $X \approx 0$.

After subtracting from X a constant divisor of the same degree, we may assume that $\deg(X) = 0$. Now, the assumption $nX \approx 0$ implies that there is a constant divisor A such that $nX \sim A$; we have

$$\deg(A) = n \cdot \deg(X) = 0.$$

Applying statement (A) to the case L = K, we conclude that the class of A is divisible by n in $C_0(F)$. That is, there exists a constant divisor A' such that

$$nX \sim A \sim nA'.$$

We now have $n(X-A') \sim 0$, which is to say that the class of X-A' is an n-th division class. From statement (B) we infer that this class is defined over K, i.e. it contains a constant divisor, say A". We now have $X - A' \sim A''$, i.e.

$$X \sim A' + A'' \approx 0$$

since both A' and A'' are constant. QED.

As an immediate corollary of our foregoing results we now state

LEMMA 5.2. *Let Z be a normalized divisor of $F\tilde{K}$. There exists one and only one normalized divisor Z_n such that $nZ_n \approx Z$. We have*

$$K(Z) \subset K(Z_n),$$

and this field extension is algebraic of finite degree. If n is not divisible by the characteristic then $K(Z_n)$ is separable over $K(Z)$.

PROOF. According to Lemma 5.1, the relation $nX \approx Z$ can be solved by some divisor X of $F\tilde{K}$. By Lemma 3.4 there is a normalized divisor Z_n of $F\tilde{K}$ such that $Z_n \approx X$. Multiplication by n yields $nZ_n \approx Z$.

If Z_n' is another normalized divisor and $nZ_n' \approx Z$ then, by the uniqueness statement of Lemma 5.1, we have $Z_n' \approx Z_n$. It follows $Z_n' = Z_n$ since every coarse divisor class contains only one normalized divisor by Lemma 3.4.

By assumption, Z is normalized too. Therefore the relation $Z \approx nZ_n$ implies $K(Z) \subset K(nZ_n)$ in view of Lemma 3.4. On the other hand, we have trivially $K(nZ_n) \subset K(Z_n)$. Thus

$$K(Z) \subset K(Z_n).$$

We claim that Z_n is algebraic over $K(Z)$ (resp. separably algebraic if n is not divisible by the characteristic). By Lemma 5.1, we can solve the relation $nX \approx Z$ by some divisor X which is (separably) algebraic over Z. We now have $Z_n \approx X$ and hence, since Z_n is normalized, $K(Z_n) \subset K(X)$ in view of Lemma 3.4. Therefore, Z_n too is (separably) algebraic over $K(Z)$. In other words: $K(Z_n)$ is a (separably) algebraic extension field of $K(Z)$.

Finally, we observe that the field of definition of any divisor is finitely generated over K (since it can be represented as a symmetric compositum of F). We conclude that $K(Z_n)$ is finitely generated over $K(Z)$; since it is also algebraic, the degree $[K(Z_n): K(Z)]$ is finite. QED.

Given a normalized divisor Z of $F\tilde{K}$, Lemma 5.2 shows that there is a series of field extensions $K(Z_n)$ of $K(Z)$, where n ranges over the natural numbers. These extensions are called the *division fields* belonging to the divisor Z; this name reflects the relation $nZ_n \approx Z$, which shows that Z_n can be regarded as obtained from Z through "division" by n. In view of Lemma 3.4 the normalized divisors Z and Z_n are

unique representatives of certain coarse divisor classes; thus the notion of division field is associated, in fact, to coarse divisor classes rather than to divisors.

Our aim is to obtain an estimate for the degree of irrationality of the n-th division field. Before doing so, let us first prove the following result which gives more detailed information about division fields. For reasons of simplicity, *we restrict the following discussion to the case where n is not divisible by the characteristic of F.*

LEMMA 5.3. *Let Z and Z_n be as in Lemma 5.2. The field extension $K(Z_n)$ of $K(Z)$ is Galois, and its Galois group is isomorphic to a subgroup of $C_n(F)$, the group of n-th division classes of F. In particular, $K(Z_n)$ is abelian and of exponent n over $K(Z)$, and $[K(Z_n):K(Z)] \leqslant n^{2g}$.*

Moreover, $K(Z_n)$ is unramified over $K(Z)$ in the following sense: every K-place $K(Z) \to K$ is unramified in $K(Z_n)$.

Let us first state some preliminary remarks concerning automorphisms and their action on divisors.

Let τ be a K-automorphism of $\tilde{K}$. There is a unique extension of τ to an automorphism of the field $F\tilde{K}$, such that the elements of F are left fixed. This extension is again denoted by τ. As an automorphism of the function field $F\tilde{K}$, it is clear that τ acts naturally on the divisor group $D(F\tilde{K})$. We write $Z\tau$ for the image of the divisor Z. The automorphism $Z \to Z\tau$ preserves the divisibility relation and the equivalence relation, as well as the degree and the dimension of divisors. Constant divisors remain fixed under τ; this is so because constant divisors can be regarded as divisors of F|K, and the field F remains elementwise fixed under τ. If M is a nonconstant prime divisor of $F\tilde{K}$ then its image $M\tau$ can be described as follows. First, the above mentioned properties imply that $M\tau$ is an integral divisor of degree one, hence a prime divisor of $F\tilde{K}$; this prime divisor $M\tau$ is necessarily nonconstant. Accordingly, $M\tau$ is uniquely determined by its induced embedding $F \to \tilde{K}$. Now, *this embedding* $M\tau\colon F \to \tilde{K}$ *is obtained as the composition of the two maps* $M\colon F \to \tilde{K}$ *and* $\tau\colon \tilde{K} \to \tilde{K}$. This statement can be expressed by the formula

(5.1) $x \cdot M\tau = xM \cdot \tau \qquad (x \in F)$.

The situation is quite analoguous to the corresponding situation with specializations; compare formula (3.1) in Section 3.

Since τ leaves constant divisors unchanged, it preserves the coarse equivalence.

That is,

$$\text{if } Z \approx Z' \text{ then } Z\tau \approx Z'\tau.$$

If a divisor $Z \in D(F\tilde{K})$ is defined over a subfield $E \subset \tilde{K}$ then its image $Z\tau$ is defined over $E\tau$, and conversely. From this we conclude that

$$K(Z)\tau = K(Z\tau).$$

In this sense, the action of τ on divisors is coherent with its action on the fields of definition of these divisors.

If τ leaves a subfield $E \subset \tilde{K}$ elementwise fixed, then τ leaves FE elementwise fixed; therefore τ acts trivially on the divisor group $D(FE)$. In particular, if τ leaves $K(Z)$ elementwise fixed, then we see that $Z\tau = Z$. *The inverse of this statement does also hold*:

if $Z\tau = Z$ *then* τ *leaves* $K(Z)$ *elementwise fixed.*

This is an immediate consequence of the construction of $K(Z)$ as symmetric compositum [11]. We shall need the above statement in the case of a normalized divisor Z only. In this case, $Z = M_1 + \cdots + M_r$ where the M_i are nonconstant primes and $M_i \neq M_j$ if $i \neq j$. Let $\mu_1,\ldots,\mu_r$ be the embeddings $F \to \tilde{K}$ induced by $M_1,\ldots,M_r$. Now, if $Z\tau = Z$ then τ permutes the M_i; from (5.1) we conclude that the μ_i are permuted under τ in the same way. Hence, it follows from the definition of symmetric composita, that τ leaves the elements of $F\mu_1 \circ \cdots \circ F\mu_r = K(Z)$ fixed.

The K-places q: $\tilde{K} \to K$ are permuted under τ; the image τq of q is defined by the formula

$$(5.2)\quad u \cdot \tau q = u\tau \cdot q \qquad (u \in \tilde{K}).$$

This formula says that the place τq: $\tilde{K} \to K$ is obtained as the composition of the maps τ: $\tilde{K} \to \tilde{K}$ and q: $\tilde{K} \to K$. If Z is any divisor of $F\tilde{K}$, then we have the formula

$$Z \cdot \tau q = Z\tau \cdot q.$$

In other words: the specialization of Z with respect to τq is obtained by first forming the automorphic image $Z\tau$ and then specializing this image with respect to q. In order to prove this formula, one may assume via linearity that Z is a prime divisor, and in fact nonconstant (for constant divisors, the formula is trivial). Now, if $Z = M$ is a nonconstant prime then the formula

$$M \cdot \tau q = M\tau \cdot q$$

is immediately obtained by going back to the definitions, using formulas (3.1), (5.1)

and (5.2).

This being said, we now give the

PROOF OF LEMMA 5.3. (i) Galois property: We know from Lemma 5.2 that $K(Z_n)$ is separable over $K(Z)$. Let τ be an automorphism of $\tilde{K}$ which leaves $K(Z)$ elementwise fixed; then $Z\tau = Z$. We have to show that τ maps $K(Z_n)$ onto itself. Applying τ to the relation $nZ_n \approx Z$ we obtain

$$n \cdot Z_n\tau \approx Z\tau = Z \approx nZ_n$$

and hence

$$Z_n\tau \approx Z_n$$

in view of the uniqueness statement of Lemma 5.1. Now, since Z_n is normalized we know from Lemma 3.2 that Z_n is nonspecial. Since the property of being nonspecial is canonically defined, this property is stable under automorphisms; we conclude that $Z_n\tau$ is nonspecial too (although in general not normalized). Therefore, Lemma 3.1 shows that

$$K(Z_n\tau) = K(Z_n).$$

On the other hand, we have

$$K(Z_n\tau) = K(Z_n)\tau.$$

Hence

$$K(Z_n)\tau = K(Z_n)$$

as contended. Thus $K(Z_n)$ is a Galois extension of $K(Z)$.

(ii) Galois group: Let τ be an automorphism of $\tilde{K}$ over $K(Z)$. We know from (i) that $Z_n\tau \approx Z_n$; hence there is a constant divisor C_τ such that

$$C_\tau \sim Z_n\tau - Z_n.$$

C_τ is uniquely determined up to equivalence. We claim that $nC_\tau \sim 0$. In fact: since $nZ_n \approx Z$ we have $nZ_n \sim Z + A$ with some constant divisor A. Applying τ we obtain $n \cdot Z_n\tau \sim Z\tau + A\tau = Z + A \sim nZ_n$ and therefore $nC_\tau \sim n(Z_n\tau - Z_n) \sim 0$, as contended. Thus the class of C_τ is an n-th division class. The map $\tau \mapsto C_\tau$ induces a homomorphism of the group of $K(Z)$-automorphisms of $\tilde{K}$ into the group $\mathcal{C}_n(F)$. The kernel of this homomorphism consists of those τ for which $Z_n\tau \sim Z_n$; since Z_n is nonspecial this implies $Z_n\tau = Z_n$, and hence that τ leaves the field $K(Z_n)$ elementwise fixed. Using Galois theory, we conclude that $\tau \mapsto C_\tau$ induces an *injection* of the Galois group of $K(Z_n)|K(Z)$ into $\mathcal{C}_n(F)$. In particular, this Galois group is abelian and of

exponent n. Since $|C_n(F)| = n^{2g}$ (see statement (B) above), we conclude $[K(Z_n): K(Z)] \leqslant n^{2g}$.

(iii) Unramifiedness: Let q: $\tilde{K} \to K$ be a K-place from $\tilde{K}$ to K. We denote by $G(q)$ the group of those automorphisms τ of $\tilde{K}$ over K(Z), which leave q fixed, i.e. $\tau q = q$. Then $G(q)$ is the "inertia group" of q over K(Z). This group $G(q)$ induces in $K(Z_n)$ a certain subgroup of its Galois group over K(Z), say $\bar{G}(q)$. It follows from general ramification theory that $\bar{G}(q)$ is the inertia group of q in the extension $K(Z_n)|K(Z)$. Hence, in order to show that q is unramified in the extension $K(Z_n)|K(Z)$, we have to show that $\bar{G}(q) = 1$, which means that every $\tau \in G(q)$ leaves $K(Z_n)$ elementwise fixed. In fact: we have

$$Z_n\tau \cdot q = Z_n \cdot \tau q = Z_n \cdot q$$

and hence

$$C_\tau \cdot q \sim (Z_n\tau - Z_n) \cdot q = 0.$$

Here, C_τ is defined as in (ii). Since C_τ is constant, we have

$$C_\tau \cdot q = C_\tau.$$

We conclude that $C_\tau \sim 0$. By what we have shown in (ii), this implies τ leaves $K(Z_n)$ elementwise fixed. QED.

The following proposition is the main result of this section. Again, *we assume that n is not divisible by the characteristic of F.*

PROPOSITION 5.4. *Let $E|K$ be an algebraic function field of one variable, and $E \subset \tilde{K}$. We assume there is a normalized divisor Z of $F\tilde{K}$ such that $E = K(Z)$.*

Let E_n denote the n-th division field over E with respect to Z. That is, $E_n = K(Z_n)$ where Z_n is normalized and $nZ_n \approx Z$. The degree of irrationality d_n of $E_n|K$ satisfies

$$d_n \leqslant d/2 \cdot \sigma(Z,Z) \cdot n^{2g-2}$$

where σ denotes the Weil metric of the field FE.

Recall that d denotes the degree of irrationality of F|K.

PROOF. E_n is a finite extension of E of degree $\leqslant n^{2g}$ (Lemma 5.3). In particular, E_n is an algebraic function field of one variable over K. Hence Lemma 4.2 is applicable to E_n. We conclude

(5.3) $d_n \leqslant d/2 \cdot \sigma_n(Z_n,Z_n)$

where σ_n denotes the Weil metric of the field FE_n. From $nZ_n \approx Z$ we infer that

$$\sigma_n(Z,Z) = \sigma_n(nZ_n,nZ_n) = n^2\sigma_n(Z_n,Z_n),$$

in view of the bilinear property of σ_n. On the other hand, since Z is defined over E, we have by Remark 4.3:

$$\sigma_n(Z,Z) = [E_n: E]\cdot\sigma(Z,Z) \leqslant n^{2g}\cdot\sigma(Z,Z).$$

Combining these two formulas, we conclude

(5.4) $\sigma_n(Z_n,Z_n) \leqslant n^{2g-2}\cdot\sigma(Z,Z).$

Substitution into (5.3) yields our contention. QED.

6. The n-th division field of an algebraic function field of one variable. We select a subfield $F' \subset \tilde{K}$ which is K-isomorphic to F. Let ι be a K-isomorphism from F to F'. If we regard ι as an embedding

$$\iota: F \to \tilde{K}$$

then it defines a certain nonconstant prime divisor of $F\tilde{K}$, according to Section 2. We denote this prime divisor by I. As said in Section 2, we have

$$K(I) = F\iota = F'.$$

If $I\cdot o \leqslant B$ then I is normalized. In general, however, I will not be normalized. By Lemma 3.4, there is a unique normalized divisor Z of $F\tilde{K}$ such that

$$Z \approx I.$$

Since I is a prime divisor of degree one, we have dim(I) = 1. (From now on we assume that $g > o$. (If $g = 0$ then dim(I) = 2 and Z = 0.)) That is, I is nonspecial. From Lemma 3.4 we conclude that

$$K(Z) = K(I) = F'.$$

In this way we have represented F' as the field of definition of a normalized divisor Z of $F\tilde{K}$.

Let F_n denote the n-th division field over F' with respect to Z. That is, we have

$$F_n = K(Z_n)$$

where Z_n is a normalized divisor satisfying

$$nZ_n \approx Z \approx I.$$

By definition, F_n is a certain field extension of F'. If we identify $F = F'$ by means of the isomorphism ι then F_n becomes a field extension of F itself. However, it is advisable not to make this identification at this stage; until further notice we shall distinguish between F and F' and regard F_n as an extension of F'.

From Lemma 5.3 we know that F_n is unramified over F', and abelian of

exponent n. *Recall that we assume n not to be divisible by the characteristic of F.*

THEOREM 6.1. *The n-th division field F_n over F' can be characterized as the maximal unramified abelian extension of exponent n.*

In particular, we see that F_n is uniquely determined by the field structure of F' (and does not depend on the choice of the normalized divisor Z such that $K(Z) = F'$).

In the proof of Theorem 6.1 we shall need some basic facts from Deuring's theory of correspondences which we first want to recall:

Let $E|K$ be any algebraic function field of one variable, and $E \subset \tilde{K}$. Consider the divisor group $D(FE)$, i.e. the group of those divisors of $F\tilde{K}$ which are defined over E. According to Deuring [3], every divisor $Z \in D(FE)$ defines a homomorphism from the divisor group $D(F)$ to $D(E)$. If $A \in D(F)$, then the image of A under this homomorphism is denoted by $Z(A)$ or, more precisely, $Z_{F\to E}(A)$. In this way, the divisor group $D(FE)$ is represented as a certain group of homomorphisms from $D(F)$ to $D(E)$; these maps are called the *correspondences* from F to E. Any correspondence

$$Z_{F\to E}: D(F) \to D(E)$$

preserves the divisibility relation between divisors, as well as the equivalence relation. It is in general not degree preserving; instead, it multiplies the divisor degree with the number $s = \deg_{FE|F}(Z)$. That is, we have the formula

$$\deg(Z_{F\to E}(A)) = s \cdot \deg(A)$$

for any $A \in D(F)$. In particular, it follows that divisors of degree 0 are mapped onto divisors of degree 0. Hence the correspondence $Z_{F\to E}$ induces a map

$$Z_{F\to E}: C_0(F) \to C_0(E)$$

of the divisor classes of degree 0. This map is called the *multiplier* determined by the divisor Z. It may well be that two different divisors Z and Z' induce the same multiplier; Deuring [3] has shown that this is the case if and only if Z and Z' are coarse equivalent. In particular, we see that the following statement holds:

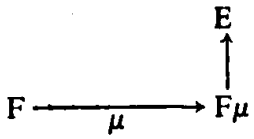
$$\text{If } Z \approx Z' \text{ then } Z_{F\to E}(A) \sim Z'_{F\to E}(A)$$

for every divisor $A \in D(F)$ of degree 0.

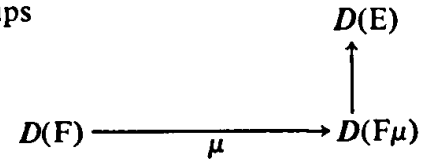
Apart from the above mentioned formal properties of correspondences, we need the following explicit description in case $Z = M$ is a nonconstant prime divisor which is defined over E. As said in Section 2, M is characterized by its induced embedding

$$\mu: F \to \tilde{K}.$$

Since M is defined over E, we have $F\mu \subset E$. Let us regard the following diagram of fields:



where the vertical arrow means the inclusion map. This diagram yields a corresponding diagram for the divisor groups



Here, the horizontal arrow is the natural isomorphism of divisors which results from the field isomorphism from F to $F\mu$. The vertical arrow is the natural injection of divisors which results from the inclusion $F\mu \subset E$. (Observe that E is a finite algebraic extension of $F\mu$.) Sometimes this injection is also called the *conorm* from $F\mu$ to E. In view of this, we shall call the composite map $D(F) \to D(F\mu) \to D(E)$ the *μ-conorm* from F to E. Now, *the correspondence map* $M_{F\to E}$: $D(F) \to D(E)$ *coincides with the μ-conorm map from F to E.*

As said above, the proofs of these facts can be found in Deuring's paper on correspondences [3]. See also [10]. In the following arguments, we shall apply these remarks in the case where $E = F_n$.

PROOF OF THEOREM 6.1. We use the notations I, Z, Z_n in accordance with the definition of F_n as given above, preceding Theorem 6.1. Thus we have $F' = K(I) = K(Z)$ and $F_n = K(Z_n)$. From

$$I \approx Z \approx nZ_n$$

we conclude for the respective multipliers:

$$I_{F\to F_n}(A) \sim Z_{F\to F_n}(A) \sim n\cdot(Z_n)_{F\to F_n}(A) \sim (Z_n)_{F\to F_n}(nA).$$

Here, A denotes an arbitrary divisor of F which is of degree 0. It follows:

$$\text{If } nA \sim 0 \text{ then } I_{F\to F_n}(A) \sim 0.$$

Now, I is the nonconstant prime divisor which belongs to the embedding ι: $F \to F_n$. We conclude:

Every n-th division class vanishes under the ι-conorm map $C_0(F) \to C_0(F_n)$.

At this point it is convenient to identify $F = F'$ by means of the isomorphism ι. Then F_n becomes an extension of F, and the ι-conorm map is the ordinary conorm, resulting from the inclusion $F \subset F_n$. We now have the following situation:

(i) *F_n is an unramified extension of F, abelian and of exponent n.*

(ii) *Every n-th division class of F vanishes in F_n. That is, if A is any divisor of F representing an n-th division class (i.e. $nA \sim 0$) then A becomes principal in F_n.*

From these two statements we have to conclude that F_n is the *maximal* unramified extension of F, which is abelian and of exponent n. This is shown as follows:

Let E|F be any unramified abelian extension of exponent n. As a Kummer extension, E is generated by n-th radicals t, so that $t^n = u \in F$. We have to show that every such radical t is contained in F_n. Now, since E|F is unramified, it is well known that the principal divisor (u) of u is divisible by n. That is, there is a divisor A of F such that $(u) = nA$. Hence $(t) = A$. Now, since $nA \sim 0$ in F, we conclude from (ii) that A becomes principal in F_n. That is, there is an element $t' \in F_n$ such that $(t') = A = (t)$. We conclude that t and t' differ by a constant factor only, i.e. $t = c \cdot t'$ with $c \in K$. Hence $t \in F_n$ as contended. QED.

In order to estimate the degree of irrationality d_n of F_n, we use Proposition 5.4. In this proposition, we have to replace E by F' and E_n by F_n. We obtain

$$d_n \leqslant d/2 \cdot \sigma(Z,Z) \cdot n^{2g-2} = d/2 \cdot \sigma(I,I) \cdot n^{2g-2},$$

the latter equation holding since $Z \approx I$. Recall that σ denotes the Weil metric of FF', and that I is the prime divisor representing the isomorphism ι from F to F'. In this case, the value $\sigma(I,I)$ is easy to compute, namely ([9], page 248, (2))

(6.1) $\sigma(I,I) = 2g$.

Thus we obtain

$$d_n \leqslant d \cdot g \cdot n^{2g-2}.$$

Combining this with Theorem 6.1 we get the following corollary. In this corollary, we again have identified $F = F'$ so that $F_n \supset F$.

COROLLARY 6.2. *Let F_n be the maximal unramified extension of F which is abelian and of exponent n. Then its degree of rationality d_n admits the estimate*

$$d_n \leqslant d \cdot g \cdot n^{2g-2}.$$

This statement is identical with that of Theorem 1.1 of the introduction.

7. **Arbitrary ground fields.** So far we had assumed that the ground field K is algebraically closed. Now let K be an arbitrary infinite field and F|K a function field of one variable, conservative and of genus $g > 0$. We shall try to extend our result to

this more general situation; our aim is to prove Theorem 1.2 stated in the introduction. As said there already, it is necessary to introduce additional assumptions concerning the divisorial structure of F|K. Our standing assumption in this section will be the following:

(A) *The field F|K admits a nonspecial divisor B of degree g which is separable and without multiple components.*

Here, the separability condition means that every prime divisor of F|K which appears in B has a separable residue field over K. This condition guarantees that B remains without multiple components after arbitrary constant field extensions, including inseparable ones.

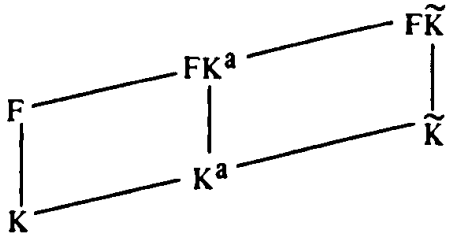
Before starting our discussion, let us briefly explain that assumption (A) is satisfied if F|K admits sufficiently many prime divisors of degree 1.

LEMMA 7.1. *If F|K admits at least 2g-1 prime divisors of degree 1 then there exist g distinct primes $P_1,\dots,P_g$ of degree 1 whose sum $B = P_1 + \cdots + P_g$ is nonspecial.*

PROOF. Starting from an arbitrary prime P_1 of degree 1 we try to select successively $P_2,P_3,\dots,P_g$ such that at each step the sum $B_i = P_1 + \cdots + P_i$ is nonspecial. Also, we have to take care that the P_i are mutually distinct. Assume that $P_1,P_2,\dots,P_i$ have been chosen already according to these specifications, and that $i < g$. The conditions for P_{i+1} are first that $P_{i+1} \neq P_1,\dots,P_i$, and secondly that $\dim(B_i + P_{i+1}) = \dim(B_i) = 1$. By the theorem of Riemann-Roch, this second condition is equivalent to $\dim(W - B_i - P_{i+1}) < \dim(W - B_i)$. (Here, W denotes a canonical divisor of F|K). In other words: there should exist at least one integral divisor $X \sim W - B_i$ which does not contain P_{i+1}. Let $T_i \geq 0$ denote the greatest common divisor of all integral divisors $X \sim W - B_i$. (Observe that B_i is nonspecial, i.e. $\dim(B_i) = 1$. By Riemann-Roch theorem, this implies $\dim(W - B_i) = g - i > 0$. Hence there are integral divisors $X \sim W - B_i$ and therefore T_i is well defined.) Then the condition is that P_{i+1} should not appear in T_i. Since $\deg(T_i) \leq \deg(W - B_i) = 2g - 2 - i$ we see that there are at most $2g - 2 - i$ primes of degree 1 which appear in T_i. These primes, together with the i primes $P_1,\dots,P_i$ should be avoided in choosing P_{i+1}. Thus there are at most $2g - 2$ primes to be avoided; since F|K admits more than $2g - 2$ primes of degree 1, we conclude that P_{i+1} can be chosen appropriately, and that our construction finally yields the nonspecial divisor $B = P_1 + \cdots + P_g$ as required. (The above construction of nonspecial divisors is

well known from the general theory of algebraic function fields; see e.g. [4], page 470. Our aim here was to put into evidence that $2g-1$ primes of degree 1 are already sufficient.) QED.

As in the preceding sections, $\tilde{K}$ denotes a universal field extension of K. We assume $\tilde{K}$ to be algebraically closed and of degree of transcendency ≥ 1 over K. We work in the function field $F\tilde{K}|\tilde{K}$ which arises from $F|K$ by means of the constant field extension $K \subset \tilde{K}$. Accordingly, we regard F and $\tilde{K}$ as K-linearly disjoint subfields of $F\tilde{K}$. Let K^a denote the algebraic closure of K. Then $K^a \subset \tilde{K}$, and we may regard $F\tilde{K}$ as a constant field extension of FK^a. If this is done, then we may apply all the notions and facts of the preceding sections, which refer to algebraically closed ground fields, to this situation.



In particular, the relation of coarse equivalence $Z \approx Z'$ between divisors Z, Z' of $F\tilde{K}$ is now to be understood as referring to K^a. Specifically, this relation means that $Z \sim Z' + A$ where A is some divisor defined over K^a, which is to say that A is algebraic over K.

If Z is any divisor of $F\tilde{K}$ then its field of definition over K is denoted by K(Z); this is the smallest subfield of $\tilde{K}$ containing K over which Z is defined. $K^a(Z)$ denotes the field of definition of Z over K^a. Obviously, $K^a(Z)$ is the field compositum of K^a with K(Z).

Our results of the preceding sections can be regarded as giving some information about the fields $K^a(Z)$, in particular for normalized divisors Z. In the following discussion, our aim is to supplement these results in order to obtain information about the fields K(Z) itself.

Some remarks about the notion of "normalized divisor" are necessary. According to Section 3, this notion refers to certain normalization parameters o and B which are arbitrarily chosen, but are kept fixed throughout the discussion. In our present situation, o is a K^a-place from $\tilde{K}$ to K^a, and B is a nonspecial divisor of degree g of $FK^a|K^a$, free from multiple components. If we change these parameters and consider

another such pair o',B' then to every o,B-normalized divisor Z there belongs exactly one o',B'-normalized divisor Z' such that

$$Z' \approx Z.$$

This follows directly from Lemma 3.4. The same lemma shows that

$$K^a(Z') = K^a(Z)$$

in this situation. In other words: the field $K^a(Z)$ does not depend on the choice of the normalization parameters o,B. However, we shall now be interested in the field K(Z), where K is not necessarily algebraically closed. In this situation, K(Z) may well depend on the choice of the normalization parameters o,B. Therefore, we shall have to be more careful in selecting these parameters in a way which is adapted to our problems.

From now on, we assume that the second normalization parameter B is chosen with the additional specification that B is defined over K already.

In view of our above assumption (A), such a divisor B of F|K does exist. We do not yet impose an additional condition on the first normalization parameter o, which is still at our disposal.

Our first problem is the following. Assume we are given a regular field extension E|K such that $E \subset \tilde{K}$. Assume furthermore that EK^a admits a representation as field of definition

$$EK^a = K^a(Z)$$

where Z is an o,B-normalized divisor of $F\tilde{K}$. The problem is, whether in this situation we can deduce that

$$E = K(Z),$$

possibly after changing the first normaliation parameter o suitably, and changing Z accordingly in its coarse equivalence class. More precisely: Does there exist a divisor $Z' \approx Z$ such that

$$E = K(Z')$$

and that Z' is o',B-normalized for some place o': $\tilde{K} \to K^a$? The following conditions are obviously necessary:

Stability condition: $Z\tau \approx Z$ *for every automorphism* τ *of* $\tilde{K}$ *which leaves E elementwise fixed.*

Separability condition: *There exists a divisor* $X \approx Z$ *which is separably algebraic over E.*

Now we claim: if $E|K$ admits a place of degree 1 then these two conditions are also sufficient for the solvability of the above problem.

The given K-place $E \to K$ of degree 1 extends uniquely to a K^a-place $EK^a \to K^a$, and from there it can be extended (not uniquely) to a K^a-place o: $\tilde{K} \to K^a$. By construction, this place o induces in E the given place of degree 1, i.e. we have $Eo = K$. In other words: if $E|K$ admits a place of degree 1 then there is a K^a-place o: $\tilde{K} \to K^a$ such that $Eo = K$.

This being said, our contention can be stated as follows

LEMMA 7.2 *Let $E|K$ be a regular field extension, and $E \subset \tilde{K}$. It is assumed that there is a normalized divisor Z of $F\tilde{K}$ such that*

$$EK^a = K^a(Z),$$

and that Z satisfies the above stability and separability conditions over E.

If $E|K$ admits a place of degree 1 then there is a K^a-place o: $\tilde{K} \to K^a$ such that $Eo = K$. Let us assume that this place o is chosen to be the first normalization parameter, i.e. that Z is o,B-normalized. Then we have

$$E = K(Z).$$

PROOF. It suffices to show that Z is defined over E. For, if this is shown then we have $K(Z) \subset E$. Since E is K-linearly disjoint to K^a and since $K^a(Z) = EK^a$ by the hypothesis of the lemma, we conclude $K(Z) = E$.

In order to show that Z is defined over E, we first show that

$$Z\tau = Z$$

for every automorphism τ of $\tilde{K}$ over E. Due to the above stability condition, we know that $Z\tau \approx Z$. Thus, in view of Lemma 3.4 it suffices to prove that $Z\tau$ is normalized. According to the definition of normalized divisors in Section 3, we have to verify that

$$Z\tau \cdot o \leqslant B.$$

Since B is defined over K, we have $B\tau = B$. Hence, after applying τ^{-1} our contention now reads as follows:

$$Z \cdot \tau o \tau^{-1} \leqslant B.$$

Observe that $\tau o \tau^{-1}$: $\tilde{K} \to K^a$ is a place which is the identity on K^a (since o is the identity on K^a). That is, $\tau o \tau^{-1}$ is a K^a-place. On the other hand, $\tau o \tau^{-1}$ coincides with o on E (since τ is the identity on E). *It follows that the two K^a-places o and $\tau o \tau^{-1}$ coincide on the field EK^a.*

Now recall that Z is defined over EK^a. *Hence, the specialization* $Z \cdot \tau o \tau^{-1}$ *depends only on the action of* $\tau o \tau^{-1}$ *on* EK^a. By what we have said above, $\tau o \tau^{-1}$ and o have the same action on EK^a. Hence

$$Z \cdot \tau o \tau^{-1} = Zo \leqslant B,$$

as contended.

We have now shown that Z is stable under all E-automorphisms τ of $\tilde{K}$. In order to show that Z is defined over E, it remains to prove Z is *separably algebraic* over E. Due to the above separability condition, we know that there exists a divisor $X \approx Z$ such that X is separably algebraic over E. From this we deduce that Z is separably algebraic over E, as follows.

It is well known that there exists a prime divisor P of $F\tilde{K}$ which is separably algebraic over K (in fact: there are infinitely many such primes). Consider the divisors $X + mP$ where $m = 0, \pm 1, \pm 2, \ldots$. We have $\dim(X+(m+1)P) \leqslant 1+\dim(X+mP)$. If m is large then, by Riemann-Roch theorem, we have $\dim(X+mP) > 0$. On the other hand, if m is small then $\deg(X+mP) < 0$ and hence $\dim(X+mP) = 0$. We conclude that there exists some integer m such that $\dim(X+mP) = 1$. Then there is one and only one integral divisor $Z' \geqslant 0$ such that $Z' \sim X+mP$. Moreover, Z' is defined over every field over which $X+mP$ is defined. Since X and P are both separably algebraic over E, we conclude that Z' too is separably algebraic over E.

By construction, Z' is nonspecial and $Z' \approx X \approx Z$. Now, let us go back to Lemma 3.4 and part (i) of its proof where we have constructed the normalized divisor Z which is coarse equivalent to Z'. Let us check every step in this construction and verify that the divisor constructed in this step is separably algebraic over E. Then after the final step we will conclude that Z is separably algebraic over E.

First, we have to form the constant divisor $A' = B - Z'o$. Recall our general agreement above, that the second normalization parameter B should be chosen such that it is defined over K. As to $Z'o$, we claim that it is separably algebraic over K, i.e. that it is defined over the separably-algebraic closure K^s of K. Note that Z' is nonspecial and $Z' \approx Z$. We conclude from Lemma 3.4 that $K^a(Z') = K^a(Z) = EK^a$. In other words: the two fields $K^s(Z')$ and EK^s become equal if their ground field K^s is extended to K^a. On the other hand, both fields are separably algebraic over E, i.e. they are contained in the separably algebraic closure E^s of E. Since E^s is K^s-linearly disjoint

to K^a, we conclude that $K^s(Z') = EK^s$. From this we see that Z' is defined over EK^s. In particular, its specialization $Z'o$ depends only on the action of o on EK^s, and $Z'o$ is defined over the image field $(EK^s)o$. According to the choice of o as specified in Lemma 7.2, we have $Eo = K$ and hence $(EK^s)o = K^s$. Therefore, $Z'o$ is defined over K^s, as contended.

We have shown that $A' = B - Z'o$ is separably algebraic over K, hence *a fortiori* over E. Since by construction Z' is separably algebraic over E, the same is true for $Z' + A'$. According to part (i) of the proof of Lemma 3.4, we now have to consider the divisor Z'' defined by

$$Z'' \geqslant 0 \text{ and } Z'' \sim Z' + A'.$$

Since $Z''o = B$ is nonspecial, we infer from Lemma 3.2 that Z'' is nonspecial too. Hence, Z'' is uniquely determined by the above conditions, and it is defined over every field over which $Z' + A'$ is defined. It follows: Z'' is separably algebraic over E.

According to part (i) of the proof of Lemma 3.4, the normalized divisor Z is now obtained as the totally nonconstant part of Z''. That is, we have

$$Z'' = Z + A$$

where A is constant and Z is totally nonconstant. Since

$$Z''o = Zo + A = B$$

we see that $A \leqslant B$. By construction, B is composed of primes which are separably algebraic over K. We conclude that the same is true for A; hence A is separably algebraic over K. It follows that $Z = Z'' - A$ is separably algebraic over E. QED.

As in Section 6, we now fix a subfield $F' \subset \tilde{K}$ which is K-isomorphic to F. Let

$$\iota: F \to F'$$

be a fixed K-isomorphism. The embedding $\iota: F \to \tilde{K}$ defines a nonconstant prime divisor of $F\tilde{K}$ which is denoted by I. We have

$$F' = K(I).$$

Let n be a natural number, not divisible by the characteristic. According to Section 5, there is one and only one normalized divisor Z_n of $F\tilde{K}$ such that

$$nZ_n \approx I.$$

We have

$$F'K^a = K^a(I) \subset K^a(Z_n),$$

and $K^a(Z_n)$ is the n-th division field over $F'K^a$ in the terminology of Section 6.

Now assume we are given a regular field extension $F_n|K$ such that $F_n \supset F'$ and

$$F_nK^a = K^a(Z_n).$$

We claim

LEMMA 7.3. *If $F_n|K$ admits a place of degree 1 then, after suitable choice of the normalization parameter and adjusting Z_n accordingly,*

$$F_n = K(Z_n).$$

PROOF. In view of Lemma 7.2 we have to verify that Z_n satisfies the stability and separability conditions over F_n.

Let τ be an automorphism of $\tilde{K}$ which leaves F_n elementwise fixed. Then τ leaves its subfield $F' = K(I)$ elementwise fixed and hence $I\tau = I$. Therefore, applying τ to the relation $nZ_n \approx I$, we obtain $n \cdot Z_n\tau \approx I \approx nZ_n$. Lemma 5.1 now shows that $Z_n\tau \approx Z_n$.

As to the separability condition, let us consider the separably-algebraic closure F'^s of F'; it contains K^s as a subfield. We have said above already that there exists a prime divisor P of FK^s of degree 1, i.e. P is defined over K^s. The divisor I - P is of degree 0 and is defined over F'^s. The divisor class group $C_0(FF'^s)$ is divisible by n (see statement (A) in Section 5). Hence there exists a divisor X of FF'^s such that $nX \approx I - P \approx I$. From Lemma 5.1 we conclude $X \approx Z_n$. By construction, X is defined over F'^s, i.e. X is separably algebraic over F' and hence over F_n. QED.

In the same situation as in Lemma 7.3, let us write

$$Z_n = M_1 + M_2 \cdots + M_r$$

where the M_i are nonconstant prime divisors of $F\tilde{K}$ which are mutually distinct. Let

$$\mu_i: F \to \tilde{K}$$

denote the embedding which is induced by M_i. The relation $F_n = K(Z_n)$ implies that F_n is the symmetric compositum of $\mu_1,\ldots,\mu_r$, i.e.

$$F_n = F\mu_1 \circ F\mu_2 \circ \cdots \circ F\mu_r.$$

Because of this relation, we can obtain an estimate for the degree of irrationality of $F_n|K$, similarly as in Section 2. The argument is as follows.

Let d and d_n denote the degrees of irrationality of the fields $F|K$ and $F_n|K$ respectively. Let $x \in F$ be chosen such that

$$[F: K(x)] = d.$$

Let us put $x_i = x\mu_i$, and

$$y_a = (x_1-a)(x_2-a)\cdots(x_r-a)$$

where $a \in K$. Since y_a is invariant under permutations of the x_i, it is clear that y_a is contained in the symmetric compositum of the μ_i. That is, $y_a \in F_n$. In order to estimate the degree $[F_n: K(y_a)]$, we observe that F_n is regular over K, which is to say that F_n is K-linearly disjoint to the algebraic closure K^a. Hence, we have

$$[F_n: K(y_a)] = [F_nK^a: K^a(y_a)].$$

In other words: we have reduced the computation of $[F_n: K(y_a)]$ to the case where the ground field is algebraically closed; in this case the arguments of Section 2 (proof of Lemma 2.1) apply. (They do not apply directly to the situation over K. For, the ordinary compositum $F\mu_1F\mu_2 \cdots F\mu_r$ need not be a regular extension of K.)

We conclude, first that there is only a finite number of elements $a \in K$ such that y_a is constant. Hence, since K is infinite, we may choose $a \in K$ such that $y_a \notin K$, i.e. that $[F_n: K(y_a)] < \infty$. This being done, we again write x instead of x - a and y instead of y_a; thus we have

$$y = x_1x_2 \cdots x_r$$

and

$$[F_n: K(y)] = [F_nK^a: K^a(y)] < \infty.$$

As in the proof of Lemma 2.1, we obtain

$$[F_nK^a: K^a(y)] \leqslant s \cdot [FK^a: K^a(x)] = s \cdot [F: K(x)] = s \cdot d$$

where s is the co-degree of the symmetric compositum, which is defined over the algebraically closed ground field K^a precisely as in Section 2. Since $d_n \leqslant [F_n: K(y)]$ we obtain:

$$d_n \leqslant d \cdot s.$$

The essential feature of this estimate is the following: whereas d_n and d are defined over K as the ground field, the number s is defined over the algebraic closure K^a and thus may be estimated by the same arguments and methods which are used in the preceding sections. We obtain

$$s \leqslant g \cdot n^{2g-2}.$$

Let us briefly recall the various steps which finally lead to this estimate:

(1) s can be interpreted as the degree of the divisor Z_n, if Z_n is regarded as a divisor of $FK^a \cdot F_nK^a$ over FK^a as field of constants. See formula (2.3) and Lemma 2.2.

(2) Since Z_n is normalized, s can now be estimated with the help of the

inequality of Castelnuovo-Severi. We obtain $s \leqslant 1/2 \cdot \sigma_n(Z_n, Z_n)$, where σ_n denotes the Weil metric of the field $FK^a \cdot F_nK^a$. See Lemma 4.1.

(3) In view of the relation $nZ_n \approx I$, we obtain $1/2 \cdot \sigma_n(Z_n, Z_n) \leqslant 1/2 \cdot \sigma(I,I) \cdot n^{2g-2}$ where σ is the Weil metric of the field $FK^a \cdot F'K^a$. See formula (5.4) in the proof of Proposition 5.4.

(4) Finally, we have $1/2 \cdot \sigma(I,I) \leqslant g$; see formula (6.1).

The steps (1) - (4) lead to the estimate $s \leqslant g \cdot n^{2g-2}$ and this yields

$$d_n \leqslant d \cdot g \cdot n^{2g-2}.$$

In this formula, d_n denotes the degree of irrationality of the field $F_n|K$, the latter being defined as in Lemma 7.3. That is, F_n is an extension of F' such that F_n is regular over K and that $F_nK^a = K^a(Z_n)$. That is, F_nK^a is the n-th division field over $F'K^a$. In view of Theorem 6.1, we conclude that F_nK^a is the maximal extension of $F'K^a$ which is unramified and abelian of exponent n. Hence, $F_n|F'$ *is an extension of maximal degree which is unramified and semi-abelian of exponent n.*

At this stage we identify $F = F'$ by means of the isomorphism ι. We obtain:

COROLLARY 7.4. *Let F_n be an extension of F, regular over K, such that $F_n|F$ is unramified, semi-abelian of exponent n, and of maximal degree $[F_n : F] = n^{2g}$. If $F_n|K$ admits a prime divisor of degree 1 then the degree of irrationality d_n of $F_n|K$ satisfies the estimate $d_n \leqslant d \cdot g \cdot n^{2g-2}$.*

Recall that this result is obtained under the assumption (A), stated at the beginning of this section, about the existence of nonspecial divisors of F|K. We know that this assumption (A) is satisfied if F|K admits at least 2g - 1 primes of degree 1 (Lemma 7.1). Therefore, Theorem 2.1 is contained in Corollary 7.4.

REFERENCES

1. W. L. Chow, *On the defining field for a divisor,* Proc. Amer. Math. Soc., 1(1950), 797-799.
2. M. Deuring, *Zur arithmetischen Theorie der algebraischen Funktionen;* Math. Annalen 106(1932) 77-102.
3. ———, *Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkorper I,* Journ. reine angew. Math., 177(1937), 161-191.
4. H. Hasse, *Zahlentheorie,* 2. Aufl. Akad. Verl. Berlin, 1963.
5. S. L. Kleiman, D. Laksov, *On the existence of special divisors,* Amer. Journ. Math., 94(1972), 431-436.
6. S. Lang, *Abelian Varieties,* Interscience, New York, 1959.
7. A. Robinson, P. Roquette, *On the Finiteness Theorem of Siegel and Mahler concerning Diophantine Equations,* Journ. of Number Theory, 7(1975).

8. P. Roquette, *Riemannsche Vermutung in Funktionenkörpern*, Archiv d. Math., 4(1953), 6-16.
9. ———, *Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunktionenkörpern beliebigen Geschlechts*, Journ. reine angew. Math., 191(1953), 199-252.
10. ——— , *Arithmetische Untersuchung des Abelschen Funktionenkörpers, der einem algebraischen Funktionenkörper höheren Geschlechts zugeordnet ist: Mit einem Anhang über eine neue Begründung der Korrespondenzentheorie algebraischer Funktionenkörper*, Hamburger Abh., 18(1952), 144-178.
11. ——— , *Zur Theorie der Konstantenerweiterungen algebraischer Funktionenkörper: Konstruktion der Koordinatenkörper von Divisoren und Divisorklassen*, Hamburger Abh., 19(1955), 269-276.
12. ——— , *On the Galois Cohomology of the Projective Linear Group and its Applications to the Construction of Generic Splitting Fields of Algebras*, Math. Annalen, 150(1963), 411-439.
13. C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss., 1929, Nr. 1 = Gesammelte Abhandlungen, Band I, 209-266.

Universität Heidelberg
Heidelberg, Germany

Received May 5, 1975