J. London Math. Soc. (2) 69 (2004) 575–592 © 2004 London Mathematical Society
DOI: 10.1112/S0024610704005290

ON THE NORM EQUATION OVER FUNCTION FIELDS

J. GRÄTER AND M. WEESE

Dedicated to Jochen Wirths on his sixtieth birthday

ABSTRACT

If K is an algebraic function field of one variable over an algebraically closed field k and F is a finite extension of K, then any element a of K can be written as a norm of some b in F by Tsen's theorem. All zeros and poles of a lead to zeros and poles of b, but in general additional zeros and poles occur. The paper shows how this number of additional zeros and poles of b can be restricted in terms of the genus of K, respectively F. If k is the field of all complex numbers, then we use Abel's theorem concerning the existence of meromorphic functions on a compact Riemann surface. From this, the general case of characteristic 0 can be derived by means of principles from model theory, since the theory of algebraically closed fields is model-complete. Some of these results also carry over to the case of characteristic $p > 0$ using standard arguments from valuation theory.

1. *Introduction*

In this paper K always denotes an algebraic function field (of one variable) over an algebraically closed field k, that is, K is a finite extension of the rational function field $k(x)$. A well known theorem due to Tsen states that in an arbitrary finite field extension F/K, any element $a \in K$ can be written as the norm $N_{F/K}(b)$ of some element $b \in F$ (cf. [**17**, **18**]). This remarkable result is interesting in many respects. For example, Tsen used his norm theorem to prove that the Brauer group $B(K)$ of an algebraic function field K of one variable over an algebraically closed field is trivial, that is, if D is a division algebra finite-dimensional over its center K, then $D = K$. This is indeed a significant contribution to the theory of central simple algebras, which is the basis for most work on the Brauer groups of transcendental field extensions leading to the investigation of fields with similar properties (cf. [**14**, **19**]). Using the definition of C_i-fields due to Lang (cf. [**14**]), Tsen basically proved that the Brauer group of any C_1-field is trivial and that a function field K of one variable over an algebraically closed field is C_1, which means that for any positive integer d, any homogeneous polynomial with coefficients from K of degree d in more than d variables has a non-trivial zero over K (Artin called these fields quasi-algebraically closed). The results on C_i-fields proved by Tsen and Lang are not only beautiful and fascinating, but they can also be applied, for instance, to obtain Pfister's theorem on the minimal number of terms needed to represent positive semi-definite rational functions over real closed fields as sums of squares; moreover, they lead to new and interesting problems where algebra, number theory, and model theory meet and interact, for example Artin's conjecture on C_2-fields (cf. [**6**, **11**, **16**]).

Received 30 October 2002; revised 27 August 2003.

2000 *Mathematics Subject Classification* 14H05, 12F10, 12L12 (primary), 12E12, 03C60 (secondary).

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

The usual proof for Tsen's norm theorem is based on a result from basic algebraic geometry about the solution of polynomial equations which states that a proper ideal $(f_1, \ldots, f_s)$ in the polynomial ring $k[x_1, \ldots, x_d]$ over an algebraically closed field k is not maximal (and therefore it has more than one solution by Hilbert's Nullstellensatz) if $s < d$. Thus the existence of $b \in F$ satisfying $a = N_{F/K}(b)$ follows from abstract arguments such as Krull's height theorem for Noetherian rings or by algorithms from elimination theory (cf. [**3**]) which do not shed any light on further algebraic properties of b. The aim of this paper is to provide a totally different approach to the norm theorem, yielding not only a new proof but also additional information about b. To illustrate our results, we describe first the special situation where $K = k(x)$ and $a \in k[x]$ is a polynomial over k. Let $b \in F$ be a solution of the norm equation and let

$$\mathrm{Irr}(b, k(x)) = t^r + b_{r-1}(x)t^{r-1} + \ldots + b_1(x)t + b_0(x)$$

be the minimal polynomial of b over $k(x)$. Clearly, b need not be integral over $k[x]$ and usually an integral solution does not exist. Therefore, we ask for solutions which are at least 'close to integral', that is, we ask for some b solving the norm equation such that the number of poles of $b_1(x), \ldots, b_{r-1}(x)$ is as small as possible (if $a \in k(x)$ is not a polynomial, then we are interested in the poles of $b_1(x), \ldots, b_{r-1}(x)$ which are not poles of a). Of course, any such pole is induced by a pole of b (which does not lie over a pole of a), where b is considered as an algebraic function on the abstract Riemann surface X_F of F, and the aim of this paper is to confine the number of these poles. The main result is Theorem 2, which states the following.

If K is an algebraic function field over an algebraically closed field k of characteristic 0 and F/K is a finite field extension of degree n, then, for any a in K, there exists b in F such that $N_{F/K}(b) = a$, where b has at most $n(g_F - g_K)$ zeros which do not lie over a zero of a and at most $n(g_F - g_K)$ poles which do not lie over a pole of a.

Here, g_K, respectively g_F, denotes the genus of K, respectively F. If in addition $K = k(x)$ and $a \in k[x]$ is a polynomial, then b exists such that the coefficients of $\mathrm{Irr}(b, k(x))$ have at most $2g_F$ poles different from ∞. A slightly weaker version of this even holds in the case of a positive characteristic.

In Section 2, we treat the case $k = \mathbb{C}$ and consider the elements from F as algebraic functions on the corresponding compact Riemann surface X_F. From this point of view we are looking for an algebraic function b on X_F such that a and $N_{F/K}(b)$ have the same zeros and poles where their orders also coincide. Of course, we use Abel's theorem about the existence of meromorphic functions on a compact Riemann surface, and the crucial point is to choose a suitable basis for the $\mathbb{C}$-vector space $\Omega(X_F)$ of all holomorphic 1-forms on X_F in order to obtain b such that a and $N_{F/K}(b)$ have the same divisors. The idea of proving Tsen's result for $k = \mathbb{C}$ via Abel's theorem is not quite new. Witt suggested in [**21**] the derivation of the norm theorem from Abel's and Jacobi's theorems by algebraic arguments, but unfortunately we do not obtain further information about the solutions of the norm equation and their algebraic properties this way (cf. [**4**, 4.13]). The results from Section 2 can be generalized to arbitrary algebraic function fields of one variable over algebraically closed fields of characteristic 0; this is shown in Section 3 using arguments from model theory. Since the theory of algebraically closed fields of a fixed characteristic is complete (in the sense of model theory), any result from Section 2 also holds for arbitrary algebraic function fields of characteristic

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

0 whenever it can be formulated in the first-order language of fields. Basically, this means that we have to formulate the statements from Section 2 in terms of polynomial equations and inequations over the corresponding field of constants, which is not obvious, especially for statements using the genus of a function field and for statements about the existence of algebraic functions having certain properties with respect to their zeros and poles on the abstract Riemann surface. In Section 4 we show how to generalize results from Section 3 to algebraic function fields of positive characteristic. These function fields are considered as residue class fields of certain valued function fields of characteristic 0, and some results from Section 3 carry over to algebraic function fields of positive characteristic in this way. Finally, in Section 5 we apply the theorems of this paper to elliptic function fields and discuss improvements in this special situation.

2. *Function fields over* $\mathbb{C}$

In the following we use the notation introduced in [**5**], and we will fix it up to the end of this section. Let K be an algebraic function field over the field $\mathbb{C}$ of all complex numbers. Then there exists a compact Riemann surface X_K such that K is isomorphic to $\mathcal{M}(X_K)$, the field of meromorphic functions on X_K, and we always assume that both coincide, that is, $K = \mathcal{M}(X_K)$. The genus of X_K is denoted by g_K or just by g, where g is the dimension of the $\mathbb{C}$-vector space $\Omega(X_K)$. Here, $\Omega(X_K)$ is the vector space of holomorphic 1-forms on X_K. Furthermore, if F is a finite field extension of K of degree n, then there exists a compact Riemann surface X_F and a branched holomorphic n-sheeted covering $\pi_{F/K} : X_F \longrightarrow X_K$ such that $F = \mathcal{M}(X_F)$ is the meromorphic function field of X_F. Any meromorphic function, respectively, holomorphic 1-form, on X_K can be considered as a meromorphic function, respectively holomorphic 1-form, on X_F by lifting with respect to $\pi_{F/K}$. In particular, $\Omega(X_K)$ is a subspace of $\Omega(X_F)$. The group $\mathrm{Deck}(X_F/X_K)$ of all deck transformations is canonically isomorphic to $\mathrm{Gal}(F/K)$, where the corresponding isomorphism maps σ from $\mathrm{Deck}(X_F/X_K)$ onto $\mathcal{M}(X_F) \longrightarrow \mathcal{M}(X_F)$, $f \longmapsto f \circ \sigma$ and K is the $\mathrm{Deck}(X_F/X_K)$-fixed subfield of F whenever F is Galois over K. Any $\sigma \in \mathrm{Gal}(F/K)$ also leads to a $\mathbb{C}$-vector space isomorphism $\sigma^* : \Omega(X_F) \longrightarrow \Omega(X_F)$ as defined in [**5**, p. 67], and if F/K is Galois, then $\omega \in \Omega(X_F)$ belongs to $\Omega(X_K)$ if and only if $\sigma^*\omega = \omega$ for all $\sigma \in \mathrm{Gal}(F/K)$.

Before we state the main theorem of this section, we present two results which will be needed later on. We shall skip their proofs, since they are just slightly modified versions of the proofs for [**5**, Lemma 21.3, Theorem 21.7]. The statements are formulated in the way in which they will be used in the proof of Theorem 1.

PROPOSITION 1. *Let E/K be a finite field extension of K and let U be an open subset of X_E. If $\omega_1, \ldots, \omega_\mu$ are linearly independent holomorphic 1-forms on X_E generating the subspace $[\omega_1, \ldots, \omega_\mu]$ in $\Omega(X_E)$, then there exist pairwise distinct $a_1, \ldots, a_\mu$ in U such that any $\omega \in [\omega_1, \ldots, \omega_\mu]$ is zero whenever $\omega(a_1) = \ldots = \omega(a_\mu) = 0$.*

PROPOSITION 2. *Let E/K be a finite field extension of K and let U be an open subset of X_E. Furthermore, let $\omega_1, \ldots, \omega_\mu$ be linearly independent holomorphic 1-forms on X_E generating the subspace $[\omega_1, \ldots, \omega_\mu]$ in $\Omega(X_E)$ and let $a_1, \ldots, a_\mu$ be in U as in Proposition 1. For any $\xi_1, \ldots, \xi_\mu \in \mathbb{C}$, there exist $b_1, \ldots, b_\mu \in U$, $N \in \mathbb{N}$,*

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

and curves γ_i in U from a_i to b_i $(i = 1, \dots, \mu)$ such that

$$\int_{\gamma_1+\ldots+\gamma_\mu} \omega_i = \frac{1}{N}\xi_i, \qquad i = 1, \dots, \mu.$$

THEOREM 1. *Let F/K be a finite field extension of K and let $n = [F : K]$. For any a in K there exists b in F such that $N_{F/K}(b) = a$ and b has at most $n(g_F - g_K)$ zeros which do not lie over a zero of a and at most $n(g_F - g_K)$ poles which do not lie over a pole of a.*

Proof. Let E/F be a finite field extension of F with $[E : F] = m$ that is Galois over K. As mentioned above, we consider $\Omega(X_F)$ as a subspace of $\Omega(X_E)$ and $\Omega(X_K)$ as a subspace of $\Omega(X_F)$. To simplify notation, put $g_K = r$, $g_F = r + s$, and $g_E = r + s + t$. There exists a basis $\{\omega_1, \dots, \omega_{r+s+t}\}$ of $\Omega(X_E)$ such that $\{\omega_1, \dots, \omega_{r+s}\}$ is a basis of $\Omega(X_F)$ and $\{\omega_1, \dots, \omega_r\}$ is a basis of $\Omega(X_K)$. First, we will derive from this a new basis of $\Omega(X_E)$ with special properties which will be needed later on. We define $\omega'_i = \omega_i$ for $i = 1, \dots, r$ as well as

$$\omega'_{r+i} = nm\omega_{r+i} - \sum_{\sigma\in \mathrm{Gal}(E/K)} \sigma^*\omega_{r+i}, \qquad \text{for } i = 1, \dots, s,$$

$$\omega'_{r+s+i} = m\omega_{r+s+i} - \sum_{\sigma\in \mathrm{Gal}(E/F)} \sigma^*\omega_{r+s+i}, \qquad \text{for } i = 1, \dots, t,$$

and show that $\omega'_1, \dots, \omega'_{r+s+t}$ are linearly independent, that is, $\{\omega'_1, \dots, \omega'_{r+s+t}\}$ is a basis of $\Omega(X_E)$. Let $k_1, \dots, k_{r+s+t}$ be in $\mathbb{C}$ such that

$$k_1\omega'_1 + \ldots + k_{r+s+t}\omega'_{r+s+t} = 0.$$

Since $\sum_{\sigma\in \mathrm{Gal}(E/K)} \sigma^*\omega_{r+i}$ is invariant under all $\tau^*, \tau \in \mathrm{Gal}(E/K)$, it belongs to $\Omega(X_K)$, and similarly $\sum_{\sigma\in \mathrm{Gal}(E/F)} \sigma^*\omega_{r+s+i} \in \Omega(X_F)$. This means that $\omega'_1, \dots, \omega'_{r+s} \in \Omega(X_F)$ and

$$mk_{r+s+1}\omega_{r+s+1} + \ldots + mk_{r+s+t}\omega_{r+s+t} \in \Omega(X_F).$$

By choice of $\omega_{r+s+1}, \dots, \omega_{r+s+t}$, we get

$$k_{r+s+1} = \ldots = k_{r+s+t} = 0.$$

Now, we can repeat this argument for

$$k_1\omega'_1 + \ldots + k_{r+s}\omega'_{r+s} = 0$$

and obtain $k_{r+1} = \ldots = k_{r+s} = 0$ as well as $k_1\omega'_1 + \ldots + k_r\omega'_r = 0$, that is, $k_i = 0$ for all i.

We now turn to the proof of the theorem. Assume that a is not 0 having zeros exactly at $x_1, \dots, x_{n_z}$ of orders $\nu_1, \dots, \nu_{n_z}$, respectively, and poles exactly at $x_{n_z+1}, \dots, x_{n_z+n_p}$ of orders $\nu_{n_z+1}, \dots, \nu_{n_z+n_p}$. Then $\nu_1 + \ldots + \nu_{n_z+n_p} = 0$, and by Abel's theorem (cf. [**5**, 20.7]), there exist curves $\tilde\Gamma_1, \dots, \tilde\Gamma_h$ in X_K from x_i $(i > n_z)$ to x_j $(j \leqslant n_z)$ such that any point appears as an initial or end point of some $\tilde\Gamma_l$ as often as its multiplicity demands and

$$\int_{\tilde\Gamma_1+\ldots+\tilde\Gamma_h} \tilde\omega_1 = \ldots = \int_{\tilde\Gamma_1+\ldots+\tilde\Gamma_h} \tilde\omega_r = 0.$$

Here $\{\tilde\omega_1, \dots, \tilde\omega_r\}$ is the basis of $\Omega(X_K)$ obtained from $\{\omega_1, \dots, \omega_r\}$ via $\pi_{E/K}$ (for a moment we have to distinguish precisely between $\Omega(X_K)$ and the subspace of $\Omega(X_E)$

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

which is invariant under all $\sigma^*, \sigma \in \mathrm{Gal}(E/K)$). We choose curves $\Gamma_1, \ldots, \Gamma_h$ in X_E such that $\pi_{E/K}(\Gamma_i) = \tilde{\Gamma}_i$ for $i = 1, \ldots, h$ and

$$\int_{\Gamma_1+\ldots+\Gamma_h} \omega_1 = \ldots = \int_{\Gamma_1+\ldots+\Gamma_h} \omega_r = 0.$$

Furthermore, the end, respectively initial, points of $\Gamma_1, \ldots, \Gamma_h$ lie in the fibers over x_i, where $i \leqslant n_z$, respectively $i > n_z$, such that the number of points lying over x_i corresponds to the order of x_i. To apply Proposition 2, we consider an open subset U in X_E which does not contain any branch point or any point over some x_i and for which no Γ_i starts or ends in U. Then there exist $a_1, \ldots, a_s, b_1, \ldots, b_s \in U$ and curves γ_i in U from a_i to b_i $(i = 1, \ldots, s)$ such that

$$\int_{\gamma_1+\ldots+\gamma_s} \omega_i' = -\frac{1}{N} \int_{\Gamma_1+\ldots+\Gamma_h} \omega_i, \qquad i = r+1, \ldots, r+s,$$

for some $N \in \mathbb{N}$. We put $\Gamma = \Gamma_1 + \ldots + \Gamma_h$ and $\gamma = \gamma_1 + \ldots + \gamma_s$ and define

$$\gamma^F = nm\gamma - \sum_{\sigma \in \mathrm{Gal}(E/K)} \sigma\gamma,$$

where $\sigma \in \mathrm{Gal}(E/K)$ is considered as an element from $\mathrm{Deck}(X_E/X_K)$ as mentioned at the beginning of this section. Then

$$\int_{\gamma^F} \omega_i = -\frac{1}{N} \int_{\Gamma} \omega_i \qquad \text{since } \int_{\gamma} \sigma^*\omega_i = \int_{\sigma\gamma} \omega_i,$$

and therefore

$$\int_{\Gamma+N\gamma^F} \omega_i = 0, \qquad i = r+1, \ldots, r+s.$$

Furthermore,

$$\begin{aligned} \int_{\Gamma+N\gamma^F} \omega_i &= \int_{\Gamma} \omega_i + N\left(nm \int_{\gamma} \omega_i - \sum_{\sigma \in \mathrm{Gal}(E/K)} \int_{\gamma} \sigma^*\omega_i \right) \\ &= \int_{\Gamma} \omega_i = 0, \end{aligned}$$

for $i = 1, \ldots, r$, since $\omega_i = \sigma^*\omega_i$. Now we will apply Proposition 2 again and take an open subset U' of X_E which does not contain any branch point or any point over some x_i and for which no Γ_i or γ_j starts or ends in U'. Then there exist $a_{s+1}, \ldots, a_{s+t}, b_{s+1}, \ldots, b_{s+t} \in U'$ and curves γ_i in U' from a_i to b_i such that

$$\int_{\gamma_{s+1}+\ldots+\gamma_{s+t}} \omega_i' = -\frac{1}{M} \int_{\Gamma+N\gamma^F} \omega_i, \qquad i = r+s+1, \ldots, r+s+t,$$

for some $M \in \mathbb{N}$. We put $\Gamma' = \Gamma + N\gamma^F$ and $\gamma' = \gamma_{s+1} + \ldots + \gamma_{s+t}$ and define

$$\gamma^E = m\gamma' - \sum_{\sigma \in \mathrm{Gal}(E/F)} \sigma\gamma'.$$

Then

$$\int_{\gamma^E} \omega_i = -\frac{1}{M} \int_{\Gamma'} \omega_i, \qquad i = r+s+1, \ldots, r+s+t,$$

and therefore

$$\int_{\Gamma'+M\gamma^E} \omega_i = 0, \qquad i = r+s+1, \ldots, r+s+t.$$

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

Furthermore,

$$\int_{\Gamma'+M\gamma^E} \omega_i = \int_{\Gamma'} \omega_i + M\left(m\int_{\gamma'} \omega_i - \sum_{\sigma\in\mathrm{Gal}(E/F)} \int_{\gamma'} \sigma^*\omega_i\right)$$
$$= \int_{\Gamma'} \omega_i = 0,$$

for $i = 1, \dots, r+s$, since $\omega_i \in \Omega(X_F)$, that is, $\omega_i = \sigma^*\omega_i$ for all $\sigma \in \mathrm{Gal}(E/F)$. Now we can apply Abel's theorem to the 1-chain $\Gamma' + M\gamma^E$, which is

$$\sum_{i=1}^{h} \Gamma_i + N\sum_{i=1}^{s}\left(nm\gamma_i - \sum_{\sigma\in\mathrm{Gal}(E/K)} \sigma\gamma_i\right) + M\sum_{i=s+1}^{s+t}\left(m\gamma_i - \sum_{\sigma\in\mathrm{Gal}(E/F)} \sigma\gamma_i\right).$$

There exists a function $f \in E$ such that the following holds for all x in X_K. If $x \neq x_i$ for all $i = 1, \dots, n_z + n_p$ and no a_i or b_i lies over x, then f has neither zeros nor poles over x. If $x = x_i$ and $i \leqslant n_z$, then f only has zeros over x where the sum of their orders equals ν_i, but if $i > n_z$, then f only has poles over x and the sum of their orders is ν_i. In all other cases f has zeros and poles over x where the sums of the multiplicities equals 0. Using

$$N_{E/K}(f) = \prod_{\sigma\in\mathrm{Gal}(E/K)} \sigma(f) \in K,$$

we see that $N_{E/K}(f)$ and a have the same zeros and poles and that their orders also coincide. Thus $aN_{E/K}(f)^{-1} = c$ is constant and $a = N_{E/K}(c^{1/nm}f)$. To complete the proof, we define

$$b := N_{E/F}\big(c^{1/nm}f\big) = \prod_{\sigma\in\mathrm{Gal}(E/F)} \sigma\big(c^{1/nm}f\big) \in F.$$

Since $N_{F/K}(b) = N_{E/K}(c^{1/nm}f) = a$, it remains to discuss the number of all additional zeros and poles of b. Of course they all come from the additional zeros and poles of f which are initial or end points of the curves $\sigma\gamma_i$, where $i = 1, \dots, s$ and $\sigma \in \mathrm{Gal}(E/K)$, or $i = s+1, \dots, s+t$ and $\sigma \in \mathrm{Gal}(E/F)$. For $i = 1, \dots, s$, we obtain maximal n zeros and n poles, that is, maximal $n(g_F - g_K)$ zeros (poles) which do not lie over a zero (pole) of a. For $i = s+1, \dots, s+t$, we see that the initial (end) points of the 1-chain $m\gamma_i$ and the end (initial) points of the curves $-\sigma\gamma_i$, $\sigma \in \mathrm{Gal}(E/F)$ do not lead to zeros or poles of b, which proves the theorem. □

REMARK 1. The upper bound $n(g_F - g_K)$ for the number of additional zeros and poles is not strict, for different reasons. For instance, [**8**] deals with the special situation where F is a cyclic Galois extension of K. Using arguments similar to those we used in the proof of Theorem 1, it is shown there that under this special assumption there exists a solution of the norm equation in F having at most $2(g_F - g_K)$ additional zeros (poles). Furthermore, in the proof of Theorem 1, the points $a_1, \dots, a_{s+t}$ are all distinct; they do not lie in the fibers over the points x_i and they are different from the branch points of X_E. These restrictions are not necessary; they are just used to simplify the arguments. Therefore, the number of additional zeros and poles can also be reduced by choosing some (or all, if possible) a_i as initial or end points of the curves Γ_i.

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

REMARK 2. Proposition 2 can be viewed as a 'local' solution of the Jacobi inversion problem where no upper bound for N is given. This means that the order of any additional zero or pole may be very high. Using the 'global' solution of the Jacobi inversion problem as given in [**13**, VI.1.12, p. 512], we can always assume that $N = M = 1$ in the proof of Theorem 1, which leads to an upper bound for the multiplicities depending only on the function fields and not on the function a. Furthermore, the points $a_1, \ldots, a_\mu$ need not meet the regularity condition as stated in Proposition 1. We are indebted to C. Adelmann for pointing this out to us.

3. *Function fields of characteristic* 0

In this section we will show that Theorem 1 can be completely generalized to algebraic function fields over arbitrary algebraically closed fields of characteristic 0 by means of a *universal transfer principle* from mathematical model theory which is based on the fact that the theory of algebraically closed fields of a fixed characteristic is complete (cf. [**9**, Theorem 7.3.5, p. 204] or [**6**, Corollary 8.5]). This is a very strong principle and it means for instance that *any sentence of the* (*first-order*) *language of fields* is true for any algebraically closed field of characteristic 0 whenever it is true for at least one such field (model), for example the field $\mathbb{C}$ of all complex numbers. Of course this does not mean that all algebraic theorems about $\mathbb{C}$ also hold for arbitrary algebraically closed fields of characteristic 0; it is true only for results that can be formulated in the *first-order language of fields*, which is indeed a rather serious restriction. Roughly speaking, the principle is reduced to statements that can be formulated in terms of polynomial equations and inequations, and our aim will be to show that this can be done for the statements claimed in Theorem 1. We shall see that it is not too difficult to do for the statement 'any $a \in K$ is a norm of some $b \in F$', but it is not clear at all that this can be done for the statement about the number of additional zeros and poles. For algebraic functions over an arbitrary field of constants, zeros and poles are defined in terms of valuations or valuation rings (places), and therefore statements such as 'for all zeros...' or 'there exist a finite number of zeros...' use quantifiers for functions (valuations) or sets (valuation rings), which is not allowed in any first-order language. An additional problem which occurs is that the genus of a function field also has to be defined in the (first-order) language of fields, which is usually done by means of divisors, that is, valuations or places.

The model-completeness for algebraically closed fields also leads to other important consequences. For instance, if E is any algebraically closed field and E' is a subfield which is also algebraically closed, then E' is an elementary substructure of E (cf. [**9**, p. 195]), which means that any finite system of polynomial equations and inequations with constants from E' is solvable in E' whenever it is solvable in E. This result has been applied by algebraists, particularly in connection with problems from algebraic geometry, where the most prominent example is Hilbert's Nullstellensatz (cf. [**9**, p. 184; **11**, p. 429]). The main arguments come from elimination theory, and they are rather elementary (cf. [**10**, pp. 322–325]), which shows that the generalization of algebraic theorems about $\mathbb{C}$ to arbitrary algebraically closed fields of characteristic 0 can be carried out without mentioning any model theory at all. However, we believe that the model theoretical background is the right setting for understanding the general transfer principle.

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

In order to generalize Theorem 1, we recall some basic facts about algebraic function fields, where we use the notation introduced in [**2**]. Let K be a field; by a valuation on K, we understand a function

$$v : K \longrightarrow \mathbb{R} \cup \{\infty\}, \quad x \longmapsto v(x)$$

with the following properties.

$$v(x) = \infty \iff x = 0, \tag{V.1}$$

$$v(x+y) \geqslant \min\{v(x), v(y)\}, \tag{V.2}$$

$$v(x \cdot y) = v(x) + v(y). \tag{V.3}$$

The values taken from $K^\times := K \setminus \{0\}$ form a subgroup Γ_v (or Γ for short) of the additive group of real numbers, and v is said to be discrete if Γ_v is cyclic. Furthermore, a discrete valuation is called normalized whenever $\Gamma_v = \mathbb{Z}$. The trivial valuation is characterized by $\Gamma = \{0\}$, where nontrivial valuations are said to be proper. Given a valuation v on K, we define

$$V := \{x \in K \mid v(x) \geqslant 0\} \quad \text{and} \quad \mathfrak{p} := \{x \in K \mid v(x) > 0\}.$$

It is easily verified that V is a subring of K, which is the valuation ring of v, and $\mathfrak{p}$ is its unique maximal ideal. Therefore, the residue ring $V/\mathfrak{p}$ is a field, the residue class field of V, and we call

$$^- : V \longrightarrow V/\mathfrak{p}, \quad x \longmapsto \overline{x}$$

the corresponding (canonical) residue class field homomorphism. An element π generating $\mathfrak{p}$ is said to be a prime element or uniformizer of v. A prime element does not exist in general, but if v is discrete, then any nonzero proper ideal of V can be written as $\pi^n V$, $n \in \mathbb{N}$, where $\mathfrak{p} = \pi V$. Given a finite field extension F/K of K, each valuation v on K possesses at least one, but at most $[F : K]$, prolongations to F, and furthermore any extension is discrete if and only if v is. The value group Γ_v is a subgroup of the value group Γ_{v_i} of any extension v_i of v; its index $e(v_i/v) := [\Gamma_{v_i} : \Gamma_v]$ is called the corresponding ramification index. v_i is said to be unramified over v if $e(v_i/v) = 1$.

In this section we will be interested in valuations on function fields only. Thus let $k(x)$ be the rational function field in one indeterminate over the algebraically closed field k, and let K be a finite extension field of $k(x)$. The abstract Riemann surface X_K of K is the set of all proper nonequivalent valuations on K which are trivial on k, where two valuations are said to be equivalent if their valuation rings coincide. Any such valuation extends a valuation on $k(x)$ which is trivial on k, and these correspond to the elements of $k \cup \{\infty\}$ in the following way. If a is in k then there exists a valuation v_a on $k(x)$, the $(x-a)$-adic valuation on $k(x)$, such that

$$v_a\left(\frac{f(x)}{g(x)}(x-a)^n\right) = n \in \mathbb{Z}, \qquad \text{for } f(a), g(a) \neq 0,$$

and if $a = \infty$, then v_∞ is defined by

$$v_\infty\left(\frac{f(x)}{g(x)}\right) = \deg\ g(x) - \deg\ f(x) \in \mathbb{Z}, \qquad \text{for } f(x), g(x) \neq 0.$$

The valuation v_a is discrete and normalized, and it counts the multiplicity of a zero or pole of a rational function at a. We also call v_a the valuation on $k(x)$ at a, where the name for $a = \infty$ is justified by the fact that $v_\infty(f(x)) = v_0(f(x^{-1}))$ for

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

all $f(x)$ in $k(x)$. With this notation any element w of the Riemann surface X_K of K is a discrete valuation on K extending some v_a, and we say that w lies over a. Furthermore, each f in K can be considered as a function on this Riemann surface with values in $k \cup \{\infty\}$. Let w be a valuation on K; if $w(f) < 0$, then $f(w) := \infty$ and f has a pole at w of order $-w(f)$. If $w(f) > 0$, then $f(w) := 0$ and f has a zero at w of order $w(f)$. In all other cases f is a unit in the valuation ring V of w and $f(w) \in k$ is defined as the image $\overline{f} \in V/\mathfrak{p} = \overline{k} \cong k$ of f under the canonical residue class field homomorphism. If w is unramified, then w is normalized; otherwise $e \cdot w$ is normalized, where e denotes the corresponding ramification index. All this coincides with the classical notation in the case of $k = \mathbb{C}$.

Before we state our theorem, we say a few words about the genus g_F of an arbitrary function field F. In this section we do not need the precise definition; we will only use the fact that the genus is invariant under certain field extensions. However, in Section 4 we will need to know some more details. In [**2**], the genus is defined by means of Riemann's theorem [**2**, Theorem 3.1], and it turns out to be the dimension of the space of all first-kind differentials as it is used in Section 2 (cf. [**2**, Corollary 6.3]). However, we will also apply the Hurwitz formula (cf. [**2**, p. 147]), even in case of a positive characteristic $p > 0$, which is helpful in computing the genus in terms of all ramification indices.

THEOREM 2. *Let K be an algebraic function field over an algebraically closed field k of characteristic 0, and let F/K be a finite field extension of degree n. For any a in K, there exists b in F such that $N_{F/K}(b) = a$ and b has at most $n(g_F - g_K)$ zeros which do not lie over a zero of a and at most $n(g_F - g_K)$ poles which do not lie over a pole of a.*

The proof of Theorem 2 will occupy the rest of this section. To avoid the problem of expressing the genus of a field in terms of polynomial equations and inequations, we will show that the theorem has to be proved only for a field k which has finite transcendency degree over the prime field $\mathbb{Q}$. In order to do this, we let α be a primitive element of the field extension $K/k(x)$ and β be a primitive element of the field extension $F/k(x)$. We denote by k' the subfield of k generated by all elements of k appearing in the coefficients of $\mathrm{Irr}(\beta, k(x))$. Moreover, a and α can be written as polynomials in β with coefficients from $k(x)$; let k' also contain all elements from k which occur in these coefficients and let $\tilde{k}$ be the algebraic closure of k' in k. Then $\tilde{k}$ is the algebraic closure of a field that is finitely generated over its prime field $\mathbb{Q}$, that is, $\tilde{k}$ meets the condition about the transcendency degree formulated above. The polynomials $\mathrm{Irr}(\alpha, k(x)), \mathrm{Irr}(\beta, k(x))$ have coefficients in $\tilde{k}(x)$, and they are also irreducible over $\tilde{k}(x)$ since $\tilde{k}$ is a subfield of k. By assumption, Theorem 2 holds for $\tilde{F}/\tilde{K}$, where $\tilde{K} = \tilde{k}(x)(\alpha)$, $\tilde{F} = \tilde{k}(x)(\beta)$, and $[K : k(x)] = [\tilde{K} : \tilde{k}(x)]$ as well as $[F : K] = [\tilde{F} : \tilde{K}]$, that is, there exists $b \in \tilde{F}$ such that $a = N_{\tilde{F}/\tilde{K}}(b)$ and the number of additional zeros, respectively poles, of b which do not lie over a is at most $n(g_{\tilde{F}} - g_{\tilde{K}})$, where b is considered as a function on the Riemann surface $X_{\tilde{F}}$ of $\tilde{F}$. To show $a = N_{F/K}(b)$, we prove that $\mathrm{Irr}(b, \tilde{K}) = \mathrm{Irr}(b, K)$, that is, $[\tilde{K}(b) : \tilde{K}] = [K(b) : K]$. Let γ be a primitive element of the field extension $\tilde{K}(b)/\tilde{k}(x)$. By [**1**, Lemma V.2.1], the polynomial $\mathrm{Irr}(\gamma, \tilde{k}(x))$ is irreducible over $k(x)$ since $\tilde{k}$ is algebraically closed in k and we obtain $\mathrm{Irr}(\gamma, \tilde{k}(x)) = \mathrm{Irr}(\gamma, k(x))$, that is, $[\tilde{k}(x)(\gamma) : \tilde{k}(x)] = [k(x)(\gamma) : k(x)]$. Thus $k(x)(\gamma) = K(b)$, which means that

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

$[\tilde{K}(b) : \tilde{k}(x)] = [K(b) : k(x)]$ and therefore $[\tilde{K}(b) : \tilde{K}] = [K(b) : K]$. It remains to discuss the number of additional zeros and poles of b, where b has to be considered as a function on the Riemann surface X_F of F. We need the following proposition.

PROPOSITION 3. *Let $\tilde{k}$ and k be algebraically closed fields of characteristic 0, where $\tilde{k}$ is a subfield of k, and let $\tilde{F} = \tilde{k}(x)(\beta)$ be a function field over $\tilde{k}$ as well as $F = k(x)(\beta)$. Then $g_{\tilde{F}} = g_F$. Furthermore, if $b \in \tilde{F}$, as a function on the Riemann surface $X_{\tilde{F}}$ of $\tilde{F}$, has exactly n_z zeros of orders $\nu_1, \ldots, \nu_{n_z}$ and exactly n_p poles of orders $\mu_1, \ldots, \mu_{n_p}$, then the same holds for b as a function on the Riemann surface X_F of F.*

Proof. Basically, all this is shown in [**1**]. For instance, the field extension $k/\tilde{k}$ is separable in the sense of [**1**] (cf. [**1**, p. 80]) and $g_{\tilde{F}} = g_F$ follows from [**1**, Theorem V.6.5]. To prove the second statement, we have to discuss the correspondence between the valuations on F which are trivial on k and the valuations on $\tilde{F}$ which are trivial on $\tilde{k}$. Take an arbitrary proper valuation w on F which is trivial on k and which extends the valuation v on $\tilde{F}$. If w is trivial on $\tilde{F}$, then b is a unit in the valuation ring of $\tilde{F}$ belonging to v, that is, w is neither a zero nor a pole of b. If v is nontrivial, then w is the only prolongation of v to F by [**1**, Corollary V.5.1]. Since $\tilde{k}$ is the residue class field of v, we conclude that w is unramified over v by [**1**, Theorem V.5.3]. This proves the statement about the orders of the zeros and poles of b. □

We continue the discussion we interrupted in order to present Proposition 3. Since we know that b, as a function on $X_{\tilde{F}}$, has at most $n(g_{\tilde{F}} - g_{\tilde{K}})$ additional zeros (poles), Proposition 3 shows that b, now as a function on X_F, has at most $n(g_F - g_K)$ additional zeros (poles). Proposition 3 provides even more. The bound for the number of additional zeros and poles may be 'any expression that carries over with passage from $\tilde{F}$ to F', and the same is true for the orders of the zeros and poles. For instance, if we know that b, as a function on $X_{\tilde{F}}$, has at most $2(g_{\tilde{F}} - g_{\tilde{K}})$ additional zeros and poles which are all simple, then the same is true for b as a function on X_F.

So far we have shown that Theorem 2 must be proved only for a field k with finite transcendency degree over $\mathbb{Q}$. Since those fields can be embedded into the field $\mathbb{C}$ of complex numbers, we may assume that k is an algebraically closed subfield of $\mathbb{C}$. Then $\mathrm{Irr}(\alpha, k(x))$ as well as $\mathrm{Irr}(\beta, k(x))$ are irreducible over $\mathbb{C}(x)$ by [**1**, Lemma V.2.1], and we define $\hat{K} := \mathbb{C}(x)(\alpha)$, which is a subfield of $\hat{F} := \mathbb{C}(x)(\beta)$, such that $[\hat{F} : \hat{K}] = [F : K]$. By Proposition 3 we have $g_{\hat{F}} = g_F$ as well as $g_{\hat{K}} = g_K$ and therefore Theorem 2 follows from Theorem 1 using the following lemma.

LEMMA 1. *Let $\hat{k}$ and k be algebraically closed fields of characteristic 0, where k is a subfield of $\hat{k}$, and let $F = k(x)(\beta)$ be a function field over k as well as $\hat{F} = \hat{k}(x)(\beta)$. Furthermore, let $K = k(x)(\alpha)$ be a subfield of F and $\hat{K} = \hat{k}(x)(\alpha)$. For any $a \in K$, the following holds. If there exists $\hat{b} \in \hat{F}$ such that $N_{\hat{F}/\hat{K}}(\hat{b}) = a$ and $\hat{b}$ has exactly n_z zeros of orders $\nu_1, \ldots, \nu_{n_z}$ which do not lie over a zero of a and exactly n_p poles of orders $\mu_1, \ldots, \mu_{n_p}$ which do not lie over a pole of a, then there exists $b \in F$ with $N_{F/K}(b) = a$ and the same property for the zeros and poles.*

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

Proof. The main idea in the proof can roughly be described as follows. We show that the statements about $\hat{b}$ can be formulated in terms of a finite system of polynomial equations and inequations over k. This system has a solution over $\hat{k}$ (which comes from $\hat{b}$) and therefore over k (which provides b) since k is an elementary substructure of $\hat{k}$.

First, we show that such a system exists, which leads to a solution of the norm equation in F. Further equations and inequations will be added to obtain a solution of the norm equation with the supplementary properties. Thus let $m = [K : k(x)] = [\hat{K} : \hat{k}(x)]$ and $n = [F : K] = [\hat{F} : \hat{K}]$, and let $\{a_1, \ldots, a_n\}$ be a basis of F over K which is also a basis of $\hat{F}$ over $\hat{K}$. We can write $\hat{b}$ as

$$\hat{b} = \sum_{\nu=0}^{nm-1} \frac{b_{1\nu}(x)}{b_{2\nu}(x)} \beta^{\nu}, \tag{3.1}$$

where $b_{1\nu}(x), b_{2\nu}(x) \in \hat{k}[x],\ b_{2\nu}(x) \neq 0$. Since $\beta^{\nu} \cdot a_i$ is a linear combination

$$\beta^{\nu} \cdot a_i = \sum_{j=1}^{n} k_{\nu ij} a_j,$$

with $k_{\nu ij} \in K$, we obtain

$$\hat{b} \cdot a_i = \sum_{j=1}^{n} \left(\sum_{\nu=0}^{nm-1} \frac{b_{1\nu}(x)}{b_{2\nu}(x)} k_{\nu ij} \right) a_j.$$

Since $N_{\hat{F}/\hat{K}}(\hat{b}) = a$, we get $\det(A_{ij}) = a$ with

$$A_{ij} = \sum_{\nu=0}^{nm-1} \frac{b_{1\nu}(x)}{b_{2\nu}(x)} k_{\nu ij}.$$

Any $k_{\nu ij}$ and also a can be written as polynomials in α of degree less than m and with coefficients from $k(x)$. Thus $\det(A_{ij}) = a$ leads to a system of polynomial equations and inequations in the coefficients of $b_{1\nu}(x)$ and $b_{2\nu}(x)$ over k. This system has a solution over $\hat{k}$ (the coefficients of $b_{1\nu}(x)$ and $b_{2\nu}(x)$) and therefore over k. We replace the coefficients of $b_{1\nu}(x)$ and $b_{2\nu}(x)$ by the corresponding elements from the solution over k and obtain from equation (3.1) a solution $b \in F$ of the norm equation.

The statements about the additional zeros and poles can be proved in different ways. Here we will follow a suggestion made by the referee of this paper and we will refer to [**7**]. First of all we consider F as the function field on a non-singular projective irreducible curve $\mathcal{C}$ over k, where the elements from F can be viewed as functions $f : \mathcal{C} \longrightarrow k \cup \{\infty\}$ (cf. [**7**, 4.2]). For any point $P \in \mathcal{C}$, let $\mathcal{O}_P$ be the local ring of $\mathcal{C}$ at P which is a nontrivial discrete valuation ring in F containing k such that $f(P) = 0$ if and only if f is a non-unit in $\mathcal{O}_P$ and $f(P) = \infty$ if and only if $f \notin \mathcal{O}_P$; furthermore, any nontrivial valuation ring in F containing k can be obtained in this way. To simplify the arguments, we switch to an affine restriction $\mathcal{C}_*$ of $\mathcal{C}$ as described in [**7**, 4.3]. Then $\mathcal{C}_*$ is a non-singular affine irreducible curve over k where F is the quotient field of the corresponding coordinate ring $R = k[X_1, \ldots, X_m]/P$. Again, the elements of F can be considered as functions $f : \mathcal{C}_* \longrightarrow k \cup \{\infty\}$. Since $\mathcal{C}_*$ is non-singular, R is the intersection of valuation rings in F, that is, R is integrally closed in F. Furthermore, R is a Dedekind domain for R is Noetherian of Krull-dimension 1. Any maximal ideal M of R is generated by

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

elements $X_1 - a_1, \ldots, X_m - a_m \bmod P$, and at least one $\overline{X_i - a_i}$ $(= X_i - a_i + P)$ is a uniformizer of the discrete valuation ring R_M, which can be described by $(j = 1, \ldots, m)$

$$g_j \cdot \overline{X_j - a_j} = h_j \cdot \overline{X_i - a_i}, \qquad \text{where } g_j, h_j \in R,\ g_j(a_1, \ldots, a_m) \neq 0, \quad (3.2)$$

and the fact that $P(a_1, \ldots, a_m)$ is a zero/pole of $f \in F$ of order ν can be stated as

$$g \cdot f = h \cdot \overline{X_i - a_i}^{\,\pm\nu}, \qquad \text{where } g, h \in R,\ g(a_1, \ldots, a_m), h(a_1, \ldots, a_m) \neq 0. \quad (3.3)$$

To complete the proof of Lemma 1, we look at the $\hat{k}$-points of $\mathcal{C}_*$ which form a non-singular affine irreducible curve $\hat{\mathcal{C}}_*$ over $\hat{k}$ with $\hat{F}$ as its function field, and consider $\hat{b}$ as well as a as functions on $\hat{\mathcal{C}}_*$. The desired equations and inequations over k which come from $\hat{b}$ and which will provide b can be obtained in the following way. Let $\hat{P}_1, \ldots, \hat{P}_r \in \hat{\mathcal{C}}_*$ be all zeros and poles of $\hat{b}$. Then we use

$$\hat{b}(P) \neq 0, \infty, \qquad \text{for all } P \in \hat{\mathcal{C}}_* \setminus \{\hat{P}_1, \ldots, \hat{P}_r\}.$$

For any $\hat{P}_i$ we apply (3.2) to define a uniformizer of $\mathcal{O}_{\hat{P}_i}$, and (3.3) leads to the order of the zero or pole, which completes the proof of Lemma 1. □

The following special situation might be the most interesting one. Let $K = k(x)$ and let $a \in k[x]$ be a polynomial over k. Then there exists $b \in F$ such that $N_{F/K}(b) = a$. Furthermore, let

$$t^r + \frac{s_{1(r-1)}(x)}{s_{2(r-1)}(x)} t^{r-1} + \ldots + \frac{s_{11}(x)}{s_{21}(x)} t + \frac{s_{10}(x)}{s_{20}(x)} \in k(x)[t]$$

be the minimal polynomial of b over $k(x)$, where $s_{1i}(x)$ and $s_{2i}(x)$ are relatively prime polynomials over k. By definition, b is integral over $k[x]$ if all $s_{2i}(x)$ are constant. Of course Tsen's theorem does not claim that a is a norm of some integral element, and indeed this is not true in general since the coefficients of $\mathrm{Irr}(b, k(x))$ may have poles (different from ∞). Thus it is interesting to know 'how closely to integral' b can be taken, that is, we are looking for an upper bound (which does not depend on a) for the number of these poles. Clearly, we can take ng_F by Theorem 2, where $n = [F : k(x)]$, but this bound is not strict. To see this, let $k = \mathbb{C}$ be the field of all complex numbers. Then the proof of Theorem 1 shows that the poles of b different from ∞ come from the initial or end points of the curves $\sigma\gamma_i$, where $i = 1, \ldots, s$ and $\sigma \in \mathrm{Gal}(E/K)$. For any $i \in \{1, \ldots, s\}$, the initial and end points of all $\sigma\gamma_i$, $\sigma \in \mathrm{Gal}(E/K)$ lie in the fibers over two points of X_K, which proves that the upper bound ng_F can be sharpened to $2g_F$. It is easily seen by the arguments used in the proof of Lemma 1 that this is true not only for the case $k = \mathbb{C}$, but also for any algebraically closed field k of characteristic 0. Thus we obtain the following theorem.

THEOREM 3. *Let F be an algebraic function field over an algebraically closed field k of characteristic 0. Then any polynomial $a \in k[x]$ can be written as $a = N_{F/k(x)}(b)$ for some $b \in F$ where the coefficients of $\mathrm{Irr}(b, k(x))$ have at most $2g_F$ poles different from ∞.*

If g_F is not known, then the following weaker version of Theorem 3 can be used instead. Let $F = k(x)(\beta)$ be a simple field extension of $k(x)$ and let pol (x, β) be the polynomial relation between x and β. If pol $(X, Y) \in k[X, Y]$ has total degree

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

N, then $g_F \leqslant \frac{1}{2}(N-1)(N-2)$ by [**2**, Theorem 4.4.2], and we obtain the following theorem.

THEOREM 4. *Let $F = k(x)(\beta)$ be an algebraic function field over an algebraically closed field k of characteristic 0 and let N be the total degree of the polynomial relation between x and β. Then any polynomial $a \in k[x]$ can be written as a norm $a = N_{F/k(x)}(b)$ for some $b \in F$ where the coefficients of $\operatorname{Irr}(b, k(x))$ have at most $(N-1)(N-2)$ poles different from ∞.*

4. *Function fields of characteristic $p > 0$*

Unfortunately, it is not clear how to generalize all the theorems from Section 3 to fields with positive characteristic. Of course, some versions of these results also hold if k has characteristic $p > 0$, where p can be any prime number up to a finite number of exceptions by means of the compactness theorem (cf. [**9**]), but we shall not pursue this theme here. Since Tsen's theorem holds for algebraic function fields of arbitrary characteristic, it is worth discussing a method which shows how to derive at least Tsen's theorem for fields of positive characteristic from the case of characteristic 0, that is, from Theorem 2. The main tool that we use is valuation theory, and therefore the reader should be familiar with some standard arguments from valuation theory which can be found in [**11**, **12**]. We show that there exists an algebraic function field K_0 over an algebraically closed field k_0 of characteristic 0 and a finite field extension F_0/K_0 which is endowed with a valuation v, where k, K, respectively E, occur as the residue class fields belonging to the restrictions of v to k_0, K_0, respectively F_0, such that Tsen's theorem for F_0/K_0 carries over to Tsen's theorem for F/K. Under special assumptions, even more can be shown for F/K is this way.

THEOREM 5. *Let K be an algebraic function field (in one variable) over an algebraically closed field k of characteristic $p > 0$. If F/K is a finite field extension, then any $a \in K$ can be written as the norm $N_{F/K}(b)$ of some $b \in F$.*

Proof. Since k has characteristic $p > 0$, we assume that $\mathbb{F}_p$ is a subfield of k. Let T be a transcendence basis of k over $\mathbb{F}_p$, which will be used also as a set of algebraically independent elements over $\mathbb{Q}$, and let k_0 be an algebraic closure of $\mathbb{Q}(T)$. The p-adic valuation v_p of $\mathbb{Q}$ can be extended to a valuation on k_0 (which will be denoted by v_p again) having a residue class field isomorphic to k. To see this, we consider the Gaussian extension v_p of the p-adic valuation to $\mathbb{Q}(T)$, that is, for any $t_1, \ldots, t_\nu \in T$, we have

$$v_p\left(\sum_{\mu_1,\ldots,\mu_\nu} a_{\mu_1\ldots\mu_\nu} t_1^{\mu_1} \cdot \ldots \cdot t_\nu^{\mu_\nu}\right) = \min_{\mu_1,\ldots,\mu_\nu} \{v_p(a_{\mu_1\ldots\mu_\nu})\},$$

where all $a_{\mu_1\ldots\mu_\nu}$ are rational numbers and the sum is taken over a finite number of non-negative μ_i (cf. [**2**]). The corresponding residue class field is canonically isomorphic to $\mathbb{F}_p(T)$, where the isomorphism maps $\bar{t}$ from the residue class field, $t \in T \subseteq \mathbb{Q}(T)$, onto $t \in \mathbb{F}_p(T)$. Now, any valuation on k_0 extending this valuation of $\mathbb{Q}(T)$ has a residue class field which is isomorphic to the algebraic closure of $\mathbb{F}_p(T)$ and therefore isomorphic to k. We choose one extension to k_0 which is fixed

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

now, and let V be the corresponding valuation ring with maximal ideal $\mathfrak{p}$, that is, $V/\mathfrak{p} \cong k$. To obtain a valued field with residue class field isomorphic to $k(x)$, we extend v_p to $k_0(x)$ by the Gaussian extension, which will be denoted by v_p again, and now v_p is a valuation on $k_0(x)$ with residue class field as desired.

There exists a finite field extension $K_0/k_0(x)$ with the following properties.

(i) v_p has a unique extension to K_0 (which will be denoted by v_p).

(ii) $K_0/k_0(x)$ is an inert extension, that is, $[K_0 : k_0(x)] = [V^K/\mathfrak{p}^K : (V/\mathfrak{p})(x)]$, where V^K is the corresponding valuation ring in K_0 and $\mathfrak{p}^K$ is its maximal ideal.

(iii) The isomorphism $V/\mathfrak{p} \longrightarrow k$ extends to an isomorphism $V^K/\mathfrak{p}^K \longrightarrow K$ which maps x onto x.

This is a well known result from valuation theory and we will just sketch the proof. To simplify notation let $k = V/\mathfrak{p}$, and by induction it will be enough to look at simple extensions only. Let $K = k(x)(\overline{\alpha})$, and let m be the degree of the minimal polynomial $\mathrm{Irr}(\overline{\alpha}, k(x))$ which has coefficients $s_{1i}(x)(s_{2i}(x))^{-1}$, where $s_{1i}(x), s_{2i}(x) \in k[x],\ s_{2i}(x) \neq 0$, that is,

$$\frac{s_{10}(x)}{s_{20}(x)} + \frac{s_{11}(x)}{s_{21}(x)}\overline{\alpha} + \ldots + \frac{s_{1(m-1)}(x)}{s_{2(m-1)}(x)}\overline{\alpha}^{m-1} + \overline{\alpha}^m = 0.$$

For any element from k, choose a preimage in V with respect to the residue class field homomorphism. We get polynomials $S_{1i}(x), S_{2i}(x) \in V[x],\ S_{2i}(x) \neq 0$ from $s_{1i}(x), s_{2i}(x)$ by replacing any coefficient by its preimage. The field $K_0 = k_0(x)(\alpha)$ with

$$\frac{S_{10}(x)}{S_{20}(x)} + \frac{S_{11}(x)}{S_{21}(x)}\alpha + \ldots + \frac{S_{1(m-1)}(x)}{S_{2(m-1)}(x)}\alpha^{m-1} + \alpha^m = 0$$

has all the properties described above. By the same arguments, we obtain a finite field extension F_0/K_0 with the following properties.

(i) v_p has a unique extension to F_0 (which will be denoted by v_p).

(ii) F_0/K_0 is an inert extension, that is, $[F_0 : K_0] = [V^F/\mathfrak{p}^F : V^K/\mathfrak{p}^K]$, where V^F is the corresponding valuation ring in F_0 and $\mathfrak{p}^F$ is its maximal ideal.

(iii) The isomorphism $V^K/\mathfrak{p}^K \longrightarrow K$ extends to an isomorphism $V^F/\mathfrak{p}^F \longrightarrow F$.

Since k_0 has characteristic 0, we can apply Theorem 2 to prove Theorem 5. Let $a_0 \in V^K$ be a preimage of $a \in K$ with respect to the residue class field homomorphism. $a \in K \cong V^K/\mathfrak{p}^K$ is a unit and therefore a_0 is a unit V^K. By Theorem 2, there exists $b_0 \in F_0$ such that $N_{F_0/K_0}(b_0) = a_0$. Let r be the degree of the minimal polynomial $\mathrm{Irr}(b_0, K_0)$ and let $u_0, \ldots, u_{r-1}$ be in K_0 satisfying

$$b_0^r + u_{r-1}b_0^{r-1} + \ldots + u_1 b_0 + u_0 = 0.$$

Then u_0 is a unit in the valuation ring V^K for $a_0 = N_{F_0/K_0}(b_0) = ((-1)^r u_0)^{n/r}$, where $n = [F : K] = [F_0 : K_0]$. Since V^F is the only valuation ring in F_0 lying over V^K, this shows that b_0 is integral over V^K, that is, $u_0, \ldots, u_{r-1} \in V^K$. We put $b = \overline{b_0}$ and obtain

$$b^r + \overline{u_{r-1}}b^{r-1} + \ldots + \overline{u_1}b + \overline{u_0} = 0.$$

Again we use the fact that V^F is the only extension of V^K to F_0 and conclude that there exist $d \in \mathbb{N}$ and an irreducible monic polynomial $g(t) \in K[t]$ such that

$$t^r + \overline{u_{r-1}}t^{r-1} + \ldots + \overline{u_1}t + \overline{u_0} = g(t)^d.$$

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

Then $\mathrm{Irr}(b, K) = g(t)$, where $g(t)$ has degree r/d, and

$$\begin{aligned} N_{F/K}(b) &= \big((-1)^{r/d} g(0)\big)^{nd/r} \\ &= ((-1)^r g(0)^d)^{n/r} \\ &= ((-1)^r \overline{u_0})^{n/r} = \overline{a_0} = a, \end{aligned}$$

which proves the theorem. □

In the proof above, the genera of the fields K and K_0, respectively F and F_0, do not coincide in general, and there is no obvious correspondence between the poles of b_0 and $\overline{b_0}$ as well. Therefore, Theorem 2 and Theorem 3 cannot be generalized to function fields of positive characteristic in this way. On the other hand, the arguments used in the proof of Theorem 5 show immediately that in Theorem 4, the field k may be an arbitrary algebraically closed field.

THEOREM 6. *Let $F = k(x)(\beta)$ be an algebraic function field over an algebraically closed field k (of arbitrary characteristic), and let N be the total degree of the polynomial relation between x and β. Then any polynomial $a \in k[x]$ can be written as $a = N_{F/k(x)}(b)$ for some $b \in F$ where the coefficients of* $\mathrm{Irr}(b, k(x))$ *have at most $(N-1)(N-2)$ poles different from ∞.*

Certainly, the results presented in this section are not as sharp as is possible, and they can be improved by using various refinements in the construction which yields F as the residue class field of a valued field F_0, especially if additional assumptions are made. However, it is not our intention to discuss the case of positive characteristic in all details. We just give one example.

In [**2**], the Hurwitz formula is proved for function fields of characteristic 0 expressing the genus g_F of F in terms of the ramification indices

$$g_F = \tfrac{1}{2} \sum (e_{\mathfrak{P}} - 1) - (n-1),$$

where the sum runs over all ramified valuations on F which are trivial on k. If F is a cyclic extension of $k(x)$ such that the characteristic p of k does not divide $n = [F : k(x)]$, then p does not divide any ramification index $e_{\mathfrak{P}}$ and therefore we can adopt the proof of [**2**, Theorem 4.6.6] to obtain the Hurwitz formula also for F under these special assumptions. Thus let $F = k(x)(\overline{\beta})$, where $\mathrm{Irr}(\overline{\beta}, k(x)) = t^n - \overline{f}(x)$ for some polynomial $\overline{f}(x) = \prod(x - \overline{\alpha_i}) \in k[x]$. Using the notation introduced in the proof of Theorem 5, for any $\overline{\alpha_i} \in k$ we choose a preimage $\alpha_i \in V$ with respect to the residue class homomorphism such that $\alpha_i = \alpha_j$ whenever $\overline{\alpha_i} = \overline{\alpha_j}$, and define $f(x) = \prod(x - \alpha_i) \in k_0[x]$ as well as $F_0 = k_0(x)(\beta)$, where $\mathrm{Irr}(\beta, k_0(x)) = t^n - f(x)$. Now we obtain a one-by-one correspondence between the ramified valuations on F which are trivial on k, and the ramified valuations on F_0 which are trivial on k_0, and also their ramification indices are equal, that is, $g_F = g_{F_0}$ by the Hurwitz formula. All this shows that Theorem 3 yields the following theorem.

THEOREM 7. *Let F be a cyclic field extension of $k(x)$ such that the characteristic of k does not divide $[F : k(x)]$, where k is an algebraically closed field. Then any polynomial $a \in k[x]$ can be written as $a = N_{F/k(x)}(b)$ for some $b \in F$ where the coefficients of* $\mathrm{Irr}(b, k(x))$ *have at most $2g_F$ poles different from ∞.*

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

5. *Examples*

We investigate elliptic function fields and treat the case $k = \mathbb{C}$ first. Thus let $K = k(x)$ and $F = K(y)$, where $y^2 = 4x^3 - g_2x - g_3$ and $g_2^3 - 27g_3^2 \neq 0$. Then $g_F = 1$ and $\Omega(X_F)$ is generated by the holomorphic 1-form $\omega = (1/y)\,dx$ having neither zeros nor poles. Therefore, according to Remark 1, any norm equation in F/K can be solved under the supplementary condition that the solution has no additional pole or exactly one by choosing the initial point a_1 of γ_1 in the fiber of ∞. The proof of Theorem 1 does not give any information about the order of this pole, but we will see below that for elliptic function fields, order 1 is always possible. Let $a = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_r) \in k[x]$ with mutually distinct α_i. As usual, we consider the torus as the quotient $\mathbb{C}/L$ of the complex plane by a lattice L, and we use it this way as a ramified cover of the extended complex plane by means of the Weierstrass $\wp$-function (cf. [**15**]). On $\mathbb{C}/L$, we choose the holomorphic 1-form ω which is induced by dx on $\mathbb{C}$, and according to the proof of Theorem 1 we define $\omega' = 2\omega$, since the non-trivial $k(x)$-automorphism of F corresponds to the reflection $z \longmapsto -z$ on $\mathbb{C}$. To satisfy the assumption of Abel's theorem, we take $\beta \in \mathbb{C}$ such that

$$\wp^{-1}(\alpha_1) + \ldots + \wp^{-1}(\alpha_r) + 2\wp^{-1}(\beta) \in L, \tag{5.1}$$

that is,

$$\beta = \wp\big(\tfrac{1}{2}(\wp^{-1}(\alpha_1) + \ldots + \wp^{-1}(\alpha_r))\big),$$

where $\wp^{-1}(\alpha_i)$ is one preimage of α_i. As explained in the proof of Theorem 1, there exists a solution b of the norm equation with a simple pole and a simple zero lying over β, that is,

$$\operatorname{Irr}(b, k(x)) = t^2 + \frac{f(x)}{(x - \beta)}t + a, \qquad f(x) \in k[x].$$

If $\wp^{-1}(\alpha_1) + \ldots + \wp^{-1}(\alpha_r) \in L$, then a solution b exists which is integral over $k[x]$. Using the addition theorem for the Weierstrass $\wp$-function

$$\wp(z_1 + z_2) = \frac{1}{4}\left[\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right]^2 - \wp(z_1) - \wp(z_2),$$

where $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, as well as the duplication formula

$$\wp(2z) = \frac{\big(\wp(z)^2 + \frac{1}{4}g_2\big)^2 + 2g_3\wp(z)}{4\wp(z)^3 - g_2\wp(z) - g_3},$$

we obtain from (5.1) a polynomial equation for β with coefficients from the ring $\mathbb{Z}[\frac{1}{2}][\alpha_1, \ldots, \alpha_r]$. Of course β is not uniquely determined for $\wp^{-1}(\alpha_1), \ldots, \wp^{-1}(\alpha_r)$, and the $\wp^{-1}(\beta)$ are not uniquely determined mod L. As explained in Section 3, all algebraic relations between $\alpha_1, \ldots, \alpha_r$ and β are true not only for $\mathbb{C}$, but also for an arbitrary algebraically closed field of characteristic 0, although they come from identities for the Weierstrass $\wp$-function proved by methods from complex analysis. Moreover, the arguments from Section 4 show that all this is true even if k has positive characteristic $p > 2$.

We discuss two specific examples. If $a = x - \alpha,\ \alpha \in k$, then a is a norm of an element in F having a simple pole and a simple zero over some $\beta \in k$ and we

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

are looking for an equation which provides β. Clearly, $N_{F/k(x)}(b) = a$ leads to the equation

$$(Ax + B)^2 + C(4x^3 - g_2x - g_3) = (x - \alpha)(x - \beta)^2, \tag{5.2}$$

where A, B and C are unknown. Comparing coefficients we get $C = \frac{1}{4}$ as well as

$$A^2 = -2\beta - \alpha, \quad 2AB = \beta^2 + 2\alpha\beta + \frac{g_2}{4}, \quad B^2 = -\alpha\beta^2 + \frac{g_3}{4}.$$

From $(2AB)^2 = 4A^2B^2$, we obtain

$$\beta^4 - 4\alpha\beta^3 + \frac{g_2\beta^2}{2} + (g_2\alpha + 2g_3)\beta + g_3\alpha + \frac{g_2^2}{16} = 0. \tag{5.3}$$

Of course this is the only equation that β must satisfy, since A and B can be computed whenever α and β solve (5.3). On the other hand, $\wp^{-1}(\alpha) + 2\wp^{-1}(\beta) \in L$ (cf. (5.1)) also provides a polynomial condition for β via the duplication formula for the Weierstrass $\wp$-function, and both coincide; moreover, equation (5.3) itself is the duplication formula where $\wp(2z) = \alpha$ and $\wp(z) = \beta$. Finally, let $\alpha_1, \alpha_2, \alpha_3 \in k$ be pairwise distinct and let $a = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \in k[x]$. Now, we are looking for a condition which ensures that a is the norm of an integral $b \in F$, and replace the right-hand side of (5.2) by $(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, leading to

$$4(\alpha_1 + \alpha_2 + \alpha_3)\left(\alpha_1\alpha_2\alpha_3 - \frac{g_3}{4}\right) - \left(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \frac{g_2}{4}\right)^2 = 0. \tag{5.4}$$

As above, this is the only equation that $\alpha_1, \alpha_2, \alpha_3$ must satisfy in order to present a as a norm of some integral b in F. Again, $\wp^{-1}(\alpha_1) + \wp^{-1}(\alpha_2) + \wp^{-1}(\alpha_3) \in L$ also provides a polynomial relation for $\alpha_1, \alpha_2, \alpha_3$ via the addition theorem for the Weierstrass $\wp$-function, which turns out to be equation (5.4) multiplied by $-16(\alpha_1 - \alpha_2)^2$. Moreover, the addition theorem itself can be stated as equation (5.4) multiplied by $-16(\alpha_1 - \alpha_2)^2$, where $\wp(z_1 + z_2) = \alpha_3$, $\wp(z_1) = \alpha_1$, and $\wp(z_2) = \alpha_2$; this can be seen after a little computation.

Acknowledgements. We would like to thank the referees of this paper and E. Becker for helpful suggestions and comments.

References

1. C. Chevalley, 'Introduction to the theory of algebraic functions of one variable', *Math. Surveys Monogr.* VI (1951).
2. P. M. Cohn, *Algebraic numbers and algebraic functions* (Chapman & Hall, 1991).
3. D. Cox, J. Little and D. O'Shea, *Ideals, varieties, and algorithms* (Springer, 1998).
4. S. Ding, M. C. Kang and E. T. Tan, 'Chiungtze C. Tsen (1898–1940) and Tsen's theorems', *Rocky Mountain J. Math.* 29 (1999) 1237–1269.
5. O. Forster, *Lectures on Riemann surfaces*, Graduate Texts in Mathematics 81 (Springer, 1999).
6. M. D. Fried and M. Jarden, *Field arithmetic* (Springer, 1986).
7. W. Fulton, *Algebraic curves* (Benjamin, 1969).
8. J. Gräter and M. Klein, Unpublished notes arising from a lecture on algebraic functions and Riemann surfaces, University of Potsdam, 2000.
9. W. Hodges, *A shorter model theory* (Cambridge University Press, 1997).
10. N. Jacobson, *Basic algebra* I (W. H. Freeman, 1989).
11. N. Jacobson, *Basic algebra* II (W. H. Freeman, 1989).
12. G. J. Janusz, *Algebraic number fields*, Graduate Studies in Mathematics 7 (American Mathematical Society, 1996).
13. F. Klein and R. Fricke, *Vorlesung über die Theorie der elliptischen Modulfunktionen* II (B. G. Teubner, Leipzig, 1892).

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press

14. S. Lang, 'On quasi algebraic closure', *Ann. of Math.* 55 (1952) 373–390.
15. H. McKean and V. Moll, *Elliptic curves* (Cambridge University Press, 1999).
16. A. Pfister, *Quadratic forms with applications to algebraic geometry and topology* (Cambridge University Press, 1995).
17. C. C. Tsen, 'Divisionsalgebren über Funktionenkörpern', *Nachr. Akad. Wiss. Göttingen* (1933).
18. C. C. Tsen, 'Algebren über Funktionenkörpern', Dissertation, Universität Göttingen, 1934.
19. C. C. Tsen, 'Zur Stufentheorie der quasi-algebraisch-Abgeschlossenheit kommutativer Körper', *J. Chinese Math. Soc.* 1 (1936) 81–92.
20. B. L. van der Waerden, *Moderne Algebra* I (Springer, 1930).
21. E. Witt, 'Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkörper über reellem Funktionenkörper', *J. Reine Angew. Math.* 171 (1934) 4–11.

J. Gräter and M. Weese
Institut für Mathematik
Universität Potsdam
Postfach 601553
14469 Potsdam
Germany

graeter@rz.uni-potsdam.de
weese@rz.uni-potsdam.de

https://doi.org/10.1112/S0024610704005290 Published online by Cambridge University Press