UNIQUE FACTORIZATION IN ALGEBRAIC FUNCTION FIELDS[1]

BY
WILLIAM M. CUNNEA

Introduction

Let K be a field of algebraic functions of one variable over a field k. Only those subdomains R of K which properly contain k are considered.

A preliminary result on quotient rings with respect to a multiplicative system is applied to the particular case that K is of genus zero to determine the conditions under which a given integrally closed subdomain of K is a quotient ring of a selected ring of a particularly simple type. This, in connection with a criterion that R be a unique factorization domain, yields a description of all subdomains of K which are unique factorization domains. The restriction on the genus of K removed, it is shown that under suitable conditions if R is a unique factorization domain or possesses certain kinds of prime elements, then K is of genus zero.

The author wishes to express his appreciation to Professor Abraham Seidenberg for his guidance in the preparation of this work and to the referee for several helpful suggestions.

1. Preliminaries

If K is a field of algebraic functions of one variable over a field k, it shall always be assumed that k is algebraically closed in K.

The definitions of place, valuation, zero, pole, divisor, and related terms are those of Chevalley [1]. Note, in particular, that a place is the ideal of non-units of a valuation ring.

A *Krull domain* is an integral domain R with unity such that there exists a family V of valuations of the quotient field F of R which are discrete and of rank 1, and such that R is the intersection of all valuation rings of valuations of V, and every nonzero element of F has zero value in all but a finite number of valuations of V. V is called a *definition family* of R. A valuation v in V is *essential* if there is an element x in F such that $v(x)$ is negative, but x has nonnegative value in every other valuation of V. The basic facts about Krull domains are to be found in Samuel [2], where they are called "normal" rings.

A *Dedekind domain* is a Krull domain in which every nontrivial prime ideal is minimal. Occasionally, for expository purposes, a domain, instead of being called simply a Dedekind domain, will be referred to as both a Krull and Dedekind domain.

Received March 21, 1963.

[1] This paper contains part of a doctoral dissertation written under the direction of Professor Abraham Seidenberg at the University of California, Berkeley.

2. Krull domains and quotient rings

LEMMA 2.1. *Let K be a field of algebraic functions of one variable over a field k, and R any intersection of valuation rings of K/k not equal to k. Then R has the following properties:*

(a) *K is the quotient field of R.*

(b) *R is a Krull domain.*

(c) *R is a Dedekind domain.*

Proof. (a) Since R contains but is not equal to k and k is algebraically closed in K, there exists an x in R which is transcendental over k. K is a finite algebraic extension of $k(x)$ and hence also of the quotient field of R.

R is an intersection of valuation rings of K and so is integrally closed in K.

Let y be an element of K. Then

$$y^n + (a_{n-1}/b_{n-1})y^{n-1} + \cdots + (a_0/b_0) = 0,$$

where a_i, b_i are in R for all i, since y is algebraic over the quotient field of R. If $s = b_0 \cdots b_{n-1}$, then

$$(sy)^n + a'_{n-1}(sy)^{n-1} + \cdots + a'_0 = 0,$$

where a'_i is in R for all i.

Thus sy is integral over R and so is in R. Say $sy = r$. Then $y = r/s$; r, s in R.

Thus K is the quotient field of R.

(b) Since K is a field of algebraic functions of one variable over k, every valuation of K/k has rank one and is discrete, and every element of the field has nonzero value for only a finite number of valuations. Thus, since R is an intersection of valuation rings of K, R is a Krull domain.

(c) Let F be the set of all valuations of K which are nonnegative on R. R is the intersection of all valuation rings of valuations in F, and every valuation of F is a valuation of K/k, so it follows from the proof of (b) that F is a definition family of R. But the Riemann theorem implies that for every valuation v of K/k there is an x in K which has negative value for v and nonnegative value in every other valuation. Thus, every valuation in F is essential, and so R is a Dedekind domain since a Krull domain, S, is a Dedekind domain if and only if every valuation of the quotient field of S nonnegative on S is essential. This completes the proof.

If R is a subdomain containing a field k of a field, K, of algebraic functions of one variable over k, every valuation of K nonnegative on R is a valuation of K/k. The integral closure of R in K is the intersection of all valuation rings of valuations of K/k nonnegative on R. Every Krull, and hence every Dedekind, domain is integrally closed. If R is integrally closed, so is every quotient ring with respect to a multiplicative system of R. Thus if K is a field of algebraic functions of one variable over a field k, and R a subdomain of K with quotient field K containing k, then the following properties hold:

(a) R is a Krull domain if and only if R is integrally closed.
(b) R is a Dedekind domain if and only if R is a Krull domain.
(c) If R is a Krull domain and M is a multiplicative system in R, then the quotient ring of R with respect to M is a Krull domain.

LEMMA 2.2. *Let R and S be integral domains, R contained in S, and S^* the integral closure of S.*

If M is a multiplicative system in R, and S^* is the quotient ring, R_M, of R with respect to M, then S is equal to S^* and so is integrally closed.

Proof. Assume that a is a non-unit in S but is a unit in S^*. Then there exists a b in S^* such that $ab = 1$. Now b satisfies an equation of integral dependence

$$b^n + c_1 b^{n-1} + \cdots + c_n = 0$$

where the c_i are in S. Then

$$(ab)^n + ac_1(ab)^{n-1} + \cdots + a^n c_n = 0,$$

and so

$$1 + ac_1 + \cdots + a^n c_n = 0.$$

But there is a nontrivial ideal in S which contains a and thus also contains 1. This is a contradiction, and so a is a non-unit in S.

Now every element of M is a unit in S^* and hence a unit of S. Thus, R_M is contained in S. Clearly S is contained in R_M, and so R_M is equal to S. This completes the proof.

THEOREM 2.1. *Let K be a field of algebraic functions of one variable over a field k, and R a subdomain of K containing k and with quotient field K.*

Every overdomain of R in K is a quotient ring with respect to a multiplicative system of R if and only if every minimal prime ideal of R contains a primary principal ideal and R is integrally closed.

Proof. Assume that every minimal prime ideal in R contains a principal primary ideal and that R is integrally closed. Let S be an overring of R in K. Since R is integrally closed, so is every quotient ring of R, and thus, by Lemma 2.2, S is a quotient ring of R if and only if the integral closure of S is a quotient ring of R. Thus, we may assume that S is integrally closed.

Since R and S are integrally closed and contain k, they are both Krull and Dedekind domains. In particular, every valuation essential for S is essential for R.

Let the prime ideals $P_1, \cdots, P_n, \cdots$ be the centers in R of the valuations, v_i, of K/k essential for R but not essential for S. For all i, let (a_i) be a principal P_i-primary ideal in R, and let M be the multiplicative system generated in R by the set of all a_i.

For all i, $v_i(a_i)$ is positive, but $v(a_i) = 0$ for every essential valuation of R distinct from v_i. In particular, a_i has value zero in every valuation essential for S. Thus, for all i, a_i is a unit in S, and R_M, the quotient ring of R with respect to M, is contained in S.

R_M is a Krull domain. So to show that S is contained in R_M it suffices to show that every valuation essential for R_M is essential for S, or equivalently that every valuation of K/k negative for some element of S is negative for some element of R_M.

So let v be a valuation of K/k not essential for S. If v is not essential for R, it is not essential for R_M. Assume v is essential for R.

There exists an element a/b in S such that a and b are in R and $v(a/b)$ is negative. Thus, $v(b)$ is positive, and so if P is the center of v in R, b is in P.

There exists a c in M such that (c) is a principal P-primary ideal, and there exists an n greater than zero such that $v(b)$ is less than $nv(c)$. Now b/c^n is in R_M, and $v(b/c^n)$ is negative, so v is not essential for R_M.

Thus, R_M is equal to S.

Assume now that every overdomain of R is a quotient ring of R. In particular, the integral closure of R is a quotient ring of R, and thus R is integrally closed and a Krull domain.

Let P be a minimal prime ideal of R, and v the corresponding essential valuation of R; let S be the intersection of all rings of valuations, v_i, essential for R and distinct from v.

S is a quotient ring of R. Let M be the maximal multiplicative system in R such that R_M is equal to S. Every element of M is a unit in S, and so $v_i(m) = 0$ for all m in M and all v_i essential for S, hence for all v_i.

If $v(m) = 0$ for all m in M, then every element of M is a unit in R, and so R_M is equal to R. Thus, there is an m in M such that $v(m)$ is positive and $v_i(m) = 0$ for all i, that is, for every essential valuation of R distinct from v. Therefore (m) is a P-primary ideal of R. This completes the proof.

Every unique factorization domain is integrally closed. A Krull domain is a unique factorization domain if and only if every minimal prime ideal is principal. A quotient ring with respect to a multiplicative system of a unique factorization domain is a unique factorization domain. Thus, we have

COROLLARY 2.1. *Let K be a field of algebraic functions of one variable over a field k, R a unique factorization domain containing k and with quotient field K.*

Every overdomain of R in K is a quotient ring with respect to a multiplicative system of R and is a unique factorization domain.

3. Quotient rings and fields of genus zero

THEOREM 3.1. *Let K be a field of algebraic functions of one variable over a field k, and R a domain containing k and with quotient field K.*

If K is of genus zero and R is integrally closed, then every minimal prime ideal P of R contains a principal P-primary ideal.

Proof. R is a Krull domain, and so there is a unique place, M_1, and a unique valuation v_1 of K/k with center P on R. Let M_2 be a place corresponding to a valuation, v_2, nonessential for R. Let d_1 be the degree of M_1, d_2 the degree of M_2, and A the divisor $M_1^{-d_2}M_2^{d_1}$.

Then, since K is of genus zero, Riemann's theorem implies that there exists an a in K whose divisor is equal to A.

Thus, there exists an a in K such that $v_1(a)$ is greater than or equal to $-d_2$, $v_2(a)$ is greater than or equal to d_1, and a has nonnegative value in every other valuation of K/k. The multiplicative inverse, b, of a in R then has a zero of order d_2 at M_1, a pole of order d_1 at M_2, and has value zero at every other place.

Therefore b has nonnegative value for every valuation essential for R, and so is in R, and has nonzero value for only one essential valuation, v_1. Thus (b) is contained in only one prime ideal, P, of R, and so is a P-primary ideal in R. This completes the proof.

COROLLARY 3.1. *Let K be a field of algebraic functions of one variable over a field k, and R a domain containing k and with quotient field K.*

If K is of genus zero and R is integrally closed, then every overring of R in K is a quotient ring with respect to a multiplicative system of R.

If a field K of algebraic functions of one variable over a field k has a place of degree one, then K is of genus zero if and only if K is a simple transcendental extension of k. The next theorem gives some information on the Krull domains in fields of rational functions of one variable.

THEOREM 3.2. *Assume that R is an integral domain containing a field k whose quotient field is a simple transcendental extension, $k(t)$, of k.*

The integral closure of R is a quotient ring with respect to a multiplicative system of a polynomial ring in one variable over k if and only if there exists a valuation ring of $k(t)/k$ of degree one not containing R.

Proof. Since the integral closure of R is the intersection of all valuation rings of $k(t)/k$ containing R, it suffices to prove the result for an integrally closed ring. We will assume R is integrally closed.

If s is transcendental over k and R is a quotient ring of $k[s]$, then $k(s)$ is equal to $k(t)$, and the ring of that valuation in which s is negative has degree one and does not contain R.

Assume there exists a valuation v of $k(t)/k$ with valuation ring O which is of degree one and does not contain R. v is not essential for R.

As is well known, the valuations of $k(t)/k$ are precisely the p-adic valuations of $k(t)$, so since O is of degree one, it is generated either by $t - a$ for some a in k or by $1/t$. Assume O is generated by $t - a$. If $1/(t - a)$ is not in R, there must be an essential valuation of R which is negative at $1/(t - a)$. But v is the only valuation of $k(t)/k$ negative at $1/(t - a)$, so v is essential for R. Thus, $1/(t - a)$ is in R, the polynomial domain $k[1/(t - a)]$ is contained in R, and R is a quotient ring of $k[1/(t - a)]$ since $k(t)$ is of genus zero. Similarly, if O is generated by $1/t$, R is a quotient ring of $k[t]$. This completes the proof.

Combining this last result with the remarks preceding the theorem, we obtain the following corollary.

COROLLARY 3.2. *Let K be a field of algebraic functions of one variable over a field k, R a subdomain of K containing k and with quotient field K.*

If there exists a valuation ring of K/k of degree one which does not contain R, then K is of genus zero if and only if the integral closure of R is a quotient ring with respect to a multiplicative system of a polynomial ring in one variable.

If K is a field of algebraic functions of one variable over a field k and is of genus zero, then K has either a place of degree one or a place of degree two. We consider next the case in which K has no place of degree one.

THEOREM 3.3. *Let R be an integral domain containing a field k of characteristic different from two whose quotient field is a field K of algebraic functions of one variable over k which is of genus zero and contains no valuation rings of K/k of degree one.*

The integral closure of R is a quotient ring with respect to a multiplicative system of a ring $k[x, y]$ where $y^2 + C(x) = 0$, $C(X)$ a polynomial of degree two with distinct factors and $Y^2 + C(X)$ irreducible in the polynomial domain $k[X, Y]$ if and only if there exists a valuation ring of K/k of degree two not containing R.

Proof. As before we may assume without loss of generality that R is integrally closed.

If R is a quotient ring of $k[x, y]$ where $y^2 + C(x) = 0$ with $C(X)$ a polynomial of degree two with distinct factors, then that valuation ring of $k(x, y)/k$ in which both x and y have negative value is of degree two and does not contain R.

Now assume that there exists a valuation ring, O, of K/k of degree two which does not contain R, and let M be the place, and v the valuation, associated with O. By Riemann's theorem the length of M^{-1} is at least equal to three. Thus, there exist elements x, y not in k such that the degree of the divisor of zeros of x and the degree of the divisor of zeros of y is equal to two and 1, x, y are linearly independent over k. Then, the degree of K over $k(x)$ is equal to the degree of K over $k(y)$ is equal to two.

Let S be the integral closure of $k[x]$ in K. y has negative value only at M, so y is in S.

Assume y is in $k[x]$. Then, for some n there exist elements $a_0, \cdots, a_n$ in k such that

$$y = a_0 + a_1 x + \cdots + a_n x^n$$

and

$$-1 = v(y) = nv(x) = -n.$$

Thus, $y = a_0 + a_1 x$; but this implies $1, x, y$ linearly dependent over k. Thus, y is not in $k[x]$, and so K is equal to $k(x, y)$.

Now y in S implies $y^2 + A(x)y + B(x) = 0$ where $A(x)$, $B(x)$ are in $k[x]$ and $Y^2 + A(x)Y + B(x)$ is irreducible over $k(x)$. Since 1, $A(x), B(x)$ have no common factor, $Y^2 + A(X)Y + B(X)$ is irreducible in $k[X, Y]$, and so $y^2 + A(X)y + B(X)$ is irreducible as a polynomial in X over $k(y)$. But the degree of K over $k(y)$ is equal to two, so $A(X)$ and $B(X)$ have degree less than or equal to two, and one of them has degree equal to two.

Let $y' = y + A(x)/2$.

$$k[x, y] = k[x, y + A(x)/2] = k[x, y'], \quad \text{and}$$

$$\begin{aligned}(y' - A(x)/2)^2 + A(x)(y' - A(x)/2) + B(x) \\ &= y'^2 - A(x)y' + A(x)^2/4 + A(x)y' - A(x)^2/2 + B(x) \\ &= y'^2 + (B(x) - A(x)^2/4) = 0.\end{aligned}$$

Set y' equal to y, $B(x) - A(x)^2/4$ equal to $C(x)$.

Now since x and y have negative value only at M, x is integral over $k[y]$, and since $k[y]$ is integrally closed, the monic defining equation for x over $k[y]$ is an equation of integral dependence. Thus, the degree of $A(X)$ is less than or equal to one, and the degree of $B(X)$ is equal to two. Therefore, the degree of $C(X)$ is equal to two.

Suppose $C(X)$ has multiple factors. Then

$$C(X) = eC_1(X)^2; \qquad y^2 + eC_1(x)^2 = 0$$

where e is in k. But then, $(y/C_1(x))^2 + e = 0$, $y/C_1(x)$ is algebraic over k and, since k is algebraically closed in K, is in k. Then $y = dC_1(x)$ where d is in k, and so y is in $k[x]$. But this is a contradiction.

Now let z in K be integral over $k[x]$. Then $z = a(x) + b(x)y$; $a(x)$, $b(x)$ in $k(x)$. The norm and trace of z over $k(x)$ belong to $k[x]$, so

$$2a(x) + b(x)(y - y) = 2a(x)$$

is in $k[x]$, and

$$a(x)^2 - b(x)^2y^2 = a(x)^2 + b(x)^2C(x)$$

is in $k[x]$. Then $a(x)$ is in $k[x]$, and hence also $b(x)$ is in $k[x]$ since otherwise $C(X)$ is divisible by the square of the denominator of $b(X)$; but $C(X)$ has no nontrivial multiple factors. Thus z is in $k[x, y]$.

Thus, the integral closure S of $k[x]$ in K is of the form $k[x, y]$ where $y^2 + C(x) = 0$ and $C(X)$ is of degree two with distinct factors. Also, since y is not in $k(x)$, $Y^2 + C(X)$ is irreducible in $k[X, Y]$.

Now x has nonnegative value in every valuation nonnegative on R, and so x is in R. Then, since R is integrally closed, $k[x, y]$ is contained in R, and since K is of genus zero, R is a quotient ring of $k[x, y]$. This completes the proof.

It is easily verified that the quotient field of the domain $k[x, y]$ described in the preceding theorem is of genus zero. We then obtain the following result.

COROLLARY 3.3. *Let K be a field of algebraic functions of one variable over a field k of characteristic different from two, R a subdomain of K containing k and with quotient field K.*

If there are no valuation rings of K/k of degree one and there exists a valuation ring of K/k of degree two which does not contain R, then K is of genus zero if and only if the integral closure of R is a quotient ring with respect to a multiplicative system of a ring $k[x, y]$ where $y^2 + C(x) = 0$, $C(X)$ a polynomial of degree two with distinct factors, and $Y^2 + C(X) = 0$ is irreducible in the polynomial domain $k[X, Y]$.

4. Unique factorization domains and fields of genus zero

THEOREM 4.1. *Let K be a field of algebraic functions of one variable over a field k, K of genus zero, and R an integrally closed domain containing k and with quotient field K.*

R is a unique factorization domain if and only if the degree of every place of K/k with finite center on R is a finite linear combination with integer coefficients of the degrees of places of K/k that do not have finite center on R.

Proof. Assume that R is a unique factorization domain and that M is a place with finite center P in R. P is a minimal prime ideal of R, there exists an a in R which generates P, and the only places of K/k other than M which contain a are places that do not have finite center on R. Thus, the divisor of a is of the form $MM_1^{e_1} \cdots M_n^{e_n}$ where only M has finite center. But the degree of the divisor of an element of K is always equal to zero, and so if $d, d_1, \cdots, d_n$ are the degrees of $M, M_1, \cdots, M_n$ respectively,

$$d + e_1 d_1 + \cdots + e_n d_n = 0.$$

Now let P be a minimal prime ideal of R; M the unique place of K/k with center P in R; $M_1, \cdots, M_n$ places of K/k which do not have finite center on R. Let $d, d_1, \cdots, d_n$ be the degrees of $M, M_1, \cdots, M_n$ respectively, and assume that there exist integers $a_1, \cdots, a_n$ such that

$$d = a_1 d_1 + \cdots + a_n d_n .$$

The divisor $A = M^{-1}M_1^{a_1} \cdots M_n^{a_n}$ has degree zero, and hence Riemann's theorem implies that there is an element a in K with value one at M, value $-a_i$ at M_i for $i = 1, \cdots, n$ and value zero elsewhere. Then a is a member of R, and P is generated by a. This completes the proof.

COROLLARY 4.1. *Let K be a field of algebraic functions of one variable over a field k, K of genus zero, R an integrally closed domain containing k and with quotient field K.*

If M is a place of K/k of degree one and with finite center P on R, then R is a unique factorization domain if and only if P is a principal ideal in R.

We give some elementary examples of the application of the theorem.

Example 4.1. Let k be the field of real numbers, K the field $k(x, y)$ where x is transcendental over k and $x^2 + y^2 + 1 = 0$.

k is algebraically closed in K, K is of genus zero, every place of K/k is of degree two, and $k[x, y]$ is integrally closed.

Thus, $k[x, y]$ is a unique factorization domain.

Example 4.2. Let k be the field of real numbers, K the field $k(x, y)$ where x is transcendental over k and $x^2 + y^2 - 1 = 0$.

k is algebraically closed in K and K is of genus zero. There is only one place of K/k which does not have finite center on $k[x, y]$, and that place has degree two. There exist places with finite center on $k[x, y]$ which are of degree one.

Therefore, $k[x, y]$ is not a unique factorization domain. Note, however, that $k[x, y]$ is integrally closed.

THEOREM 4.2. *Let K be a field of algebraic functions of one variable over a field k, K of genus zero, R a subdomain of K containing k and with quotient field K.*

If there exists a valuation ring of K/k of degree one which does not contain R, then the integral closure of R is a unique factorization domain.

If k is of characteristic different from two, if there are no valuation rings of K/k of degree one, and if there exists a valuation ring of K/k of degree two not containing R, then the integral closure of R is a unique factorization domain.

Proof. Since every quotient ring with respect to a multiplicative system of a unique factorization domain is a unique factorization domain, it suffices to show that in both cases the integral closure of R is a quotient ring of a unique factorization domain.

If there exists a valuation ring of K/k of degree one which does not contain R, then the integral closure of R is a quotient ring of a polynomial ring in one variable, and the desired result is established.

In the remaining case, the integral closure of R is a quotient ring of a ring $k[x, y]$ such that $k(x, y)$ is of genus zero, there are no valuation rings of $k(x, y)/k$ of degree one, and the only valuation ring of $k(x, y)/k$ which does not contain $k[x, y]$ is of degree two.

In every field, K, of algebraic functions of one variable over a field k which is of genus zero there is either a valuation ring of K/k of degree one, or there is a valuation ring of K/k of degree two, and every other valuation ring of K/k has even degree (see [1, page 33]). Thus, by an earlier theorem, $k[x, y]$ is a unique factorization domain. This completes the proof.

THEOREM 4.3. *Let R be a unique factorization domain containing a field k whose quotient field is a simple transcendental extension, $k(t)$, of k and such that every valuation ring of $k(t)/k$ of degree one contains R.*

If v is a valuation of $k(t)/k$ with valuation ring O of degree one, then there *exists a quotient ring, S, with respect to a multiplicative system of a polynomial ring in one variable such that R is equal to the intersection of O and S.*

Proof. R is integrally closed, hence a Dedekind domain, and so the center of v on R is a minimal prime ideal, P. Since R is a unique factorization domain, there exists a prime element p in R such that P is equal to (p). Let M be the multiplicative system generated in R by p, and let S be the quotient ring of R with respect to M.

S is a Dedekind domain, and, clearly, R is contained in $S \cap O$. Thus, to show that R is equal to $S \cap O$ it suffices to show that every valuation of $k(t)/k$ not essential for $S \cap O$ is not essential for R.

Let v' be a valuation of $k(t)/k$ not essential for $S \cap O$ but essential for R. Then v' is distinct from v, and v' must be positive at p.

Let O' be the valuation ring of v'. The center of O' on R contains and hence is generated by p, and so O and O' have the same center on R. But the valuation ring of an essential valuation of a Krull domain is determined by its center; the valuation ring is the quotient ring of the domain with respect to the multiplicative system of elements not contained in the center. Thus, O is equal to O', which is a contradiction. This completes the proof.

We thus have a description of all unique factorization domains containing k and with quotient field K in the case that K is a simple transcendental extension of k; if R is a unique factorization domain, then R is either a quotient ring of a polynomial ring in one variable or is the intersection of such a quotient ring with a valuation ring of degree one.

The next theorem completes these results to the general case that K is of genus zero and k of characteristic different from two.

THEOREM 4.4. *Let R be a unique factorization domain properly containing a field k of characteristic different from two whose quotient field is a field K of algebraic functions of one variable over k which is of genus zero and contains no valuation rings of degree one.*

If v is a valuation of K/k with valuation ring O of degree two containing R, then there exists a quotient ring, S, with respect to a multiplicative system of a ring of the form $k[x, y]$ where $y^2 + C(x) = 0$ and $C(X)$ is of degree two with distinct factors such that R is equal to the intersection of O and S.

The proof is almost exactly the same as the proof of the analogous result for the case in which K is a pure transcendental extension of k.

THEOREM 4.5. *Let K be a field of algebraic functions of one variable over an algebraically closed field k, $K = k(x_1, \cdots, x_n)$, $R = k[x_1, \cdots, x_n]$ integrally closed.*

R is a unique factorization domain if and only if K is of genus zero.

Proof. Since k is algebraically closed, every place of K/k is of degree one. Thus, if K is of genus zero, it follows from an earlier theorem that R is a unique factorization domain.

Assume now that R is a unique factorization domain.

Since k is algebraically closed and hence infinite, we may assume without loss of generality that $x_2, \cdots, x_n$ are integral over $k[x_1]$, and thus that x_1 has negative value at all places of K/k not at finite distance. Thus x_1 has positive value at one or more places at finite distance.

If a valuation v of K/k is nonnegative on $x_1, \cdots, x_n$, then v is nonnegative for every polynomial in $x_1, \cdots, x_n$ with coefficients in k and hence is nonnegative on every element of R. Thus, if v is negative at some element of R, it is negative at x_i, for some i. But every element of K has nonzero value for only a finite number of valuations. Thus there exist only a finite number of valuation rings of K/k not containing R and so only a finite number of places of K/k which do not have finite center on R.

Let $M_1, \cdots, M_n$ be those places of K/k which do not have finite center on R, and let $t_1, \cdots, t_n$ be such that t_i is in the ring O_i of M_i and M_i is equal to $t_i O_i$ for all i. For each i, there are only a finite number of places of K/k containing t_i. Let s_i be an element of K having value one at M_i and value zero at all other places containing t_i.

Let R be equal to the residue-class ring of the polynomial ring $k[X_1, \cdots, X_n]$ modulo the prime ideal $(f_1(X_1, \cdots, X_n), \cdots, f_d(X_1, \cdots, X_n))$. Adjoin to the prime field π of k the coefficients of $f_j(X_1, \cdots, X_n)$ for all j, plus, for all i, the coefficients of t_i and s_i occurring in some representation of t_i and s_i as quotients of polynomials in $x_1, \cdots, x_n$. The subfield, L, of k so obtained is thus a finite extension of π.

Since L is a finite extension of π, there exists a nontrivial normal extension N of L in k, the splitting field of some polynomial separable over L. N possesses a nontrivial automorphism over L which can be extended to a nontrivial automorphism F of k over L. F can be extended to an automorphism F' of R such that

$$F'(\sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}) = \sum F(a_{i_1 \cdots i_n}) x_1^{i_1} \cdots x_n^{i_n}$$

which in turn induces an automorphism G of K such that for a and b in R, b not equal to zero, $G(a/b) = F'(a)/F'(b)$.

If M is a place of K/k with valuation ring O, then $G(M)$ is a place with valuation ring $G(O)$. Since $G(t_i) = t_i$, $G(s_i) = s_i$ where s_i, t_i are in $G(M_i)$, and since O_i is the only valuation ring containing t_i in which s_i is a non-unit, $G(M_i) = M_i$ and $G(O_i) = O_i$. Moreover, $G(t_i^n O_i) = t_i^n O_i$, and so the values of an arbitrary element of K at $M_1, \cdots, M_n$ are unchanged by G.

Choose an element a in k such that the image b of a under F is distinct from a. Since R is a unique factorization domain, both $x_1 - a$ and $x_1 - b$, the image of $x_1 - a$ under G, are uniquely expressible as a product of prime elements of R. Also, since x_1 has negative value at every place of K/k not at finite distance, so does $x_1 - a$, and hence $x_1 - a$ has positive value at at least one place at finite distance. Let, then, $x_1 - a$ be equal to $p_1^{k_1} \cdots p_n^{k_n}$ where the p_i are prime elements in R. $x_1 - b$ is thus equal to $G(p_1)^{k_1} \cdots G(p_n)^{k_n}$, and the $G(p_i)$ are prime elements of R.

If for all i, $G(p_i)$ is associate to p_i in R, then $x_1 - a$ is associate to $x_1 - b$, and they have the same value at every place at finite distance. But $x_1 - a$ and $x_1 - b$ have no common zeros. Thus, there exists a prime element p of R such that $G(p)$ is a prime element of R not associate to p.

Now $G(p)$ and p have equal value at every place not at finite distance, and hence $G(p)/p$ has exactly one zero.

Thus, K is of genus zero. This completes the proof.

COROLLARY 4.2. *Let K be a field of algebraic functions of one variable over an algebraically closed field k, and R an integrally closed subdomain of K properly containing k which is contained in all but a finite number of valuation rings of K/k.*

R is a unique factorization domain if and only if K is of genus zero.

Proof. Riemann's theorem implies that there is an element x in K which has negative value in every valuation whose ring does not contain R and nonnegative value elsewhere. Thus R is the integral closure of $k[x]$ in K and is a finite integral domain $k[x_1, \cdots, x_n]$ over k.

Thus R is a unique factorization domain if and only if K is of genus zero. This completes the proof.

If the field k is uncountable, then the proof of the preceding theorem can be greatly simplified. In that case, R contains uncountably many prime elements, and since there is only a finite number of places of K/k not at finite distance with respect to R, there are at least two prime elements of R whose values coincide at every place not at finite distance. The quotient of these elements has exactly one zero and one pole. The theorem follows immediately.

That the assumption that R is contained in all but a finite number of valuation rings of K/k, and hence is a finite integral domain over k, is essential to Theorem 4.5 is shown by the next example.

Example 4.3. Let k be an algebraically closed field of characteristic zero, and let K be equal to $k(x, y)$ where x is transcendental over k and $y^2 = x(x - 1)(x - 2)$.

K is of genus one.

Let F be the family of ideals generated in $k[x, y]$ by the elements $x - a$, where a is in k and is distinct from zero, one, and two. The ring $k[x, y]$ is integrally closed, and every ideal in F is the intersection of two prime ideals of $k[x, y]$. Hence, if P is a place at finite distance whose center on $k[x, y]$ contains an ideal $(x - a)$ of F, then P is generated by $x - a$.

For every element of F choose one of the prime ideals of $k[x, y]$ containing it, and let G be the family of valuations of K/k determined by these prime ideals. Denote by R the Krull domain with G as a definition family.

For every valuation v in G there is an element of the form $x - a$ in R which has value equal to one for v and value zero for every other valuation in G. Thus R is a unique factorization domain.

The following example shows that the preceding theorem is not true for an arbitrary field k and also that a unique factorization domain $k[x_1, \cdots, x_n]$, where k is arbitrary, need not remain so if k is extended to its algebraic closure.

Example 4.4. Let h be a field of characteristic zero, t transcendental over h, and k the field $h(t)$. Let K be equal to $k(x, y)$ where x is transcendental over k and $y^2 + x^3 - t = 0$.

k is algebraically closed in K, and K is of genus one.

Since $t = y^2 + x^3$, $h[x, y, t] = h[x, y]$ is a polynomial ring over h and hence is a unique factorization domain. Thus, since $k[x, y]$ is a quotient ring of $h[x, y, t]$, $k[x, y]$ is a unique factorization domain.

If k is extended to its algebraic closure $\bar{k}$, then $\bar{k}[x, y]$ is still integrally closed, but as the genus is unchanged by separable extensions of the base field, $\bar{k}[x, y]$ is not a unique factorization domain.

It is worth remarking here that P. Samuel [3] has given examples which, while unrelated to the previous theorem, show that unique factorization need not be preserved either under extension or restriction of the base field k.

The next theorem does not deal directly with the question of unique factorization, but is concerned with the existence of certain kinds of prime elements.

DEFINITION 4.1. Let K be a field of algebraic functions of one variable over a field k, R an integrally closed domain containing k and with quotient field K.

A prime element p of R has degree n if and only if the place of K/k with center on R equal to the prime ideal in R generated by p has degree n.

THEOREM 4.6. *Let K be a field of algebraic functions of one variable over an infinite field k, $K = k(x_1, \cdots, x_n)$, and $R = k[x_1, \cdots, x_n]$ integrally closed. Let there be n places of K/k not having finite center on R, at least one of which has degree one.*

K is of genus zero if and only if there exist at least n prime elements of R of degree one which differ only by an element of k.

Proof. If K is of genus zero, then R is a quotient ring with respect to a multiplicative system M of a polynomial ring $k[t]$. Every element of M is a unit in R and hence has value zero in every valuation nonnegative on R. Thus, there are at most a finite number of valuations of K/k positive on some element of M, and since every prime ideal of $k[t]$ is the center of a valuation of K/k, there are at most a finite number of prime ideals of $k[t]$ which contain an element of M. Thus there are infinitely many elements of the form $t + a_i$ with a_i in k which are prime elements in R.

Assume now that there exist n prime elements of R of degree one and of the form $p + a_i$ where a_i is in k for $i = 1, \cdots, n$. The poles of the $p + a_i$ coincide, the zeros of the $p + a_i$ occur at distinct places, and the degree of the divisor of zeros of $p + a_i$ is equal to the degree of the divisor of zeros of $p + a_j$ for all i, j from 1 to n.

Let A_i be the divisor of zeros of $p + a_i$, d the common degree of the A_i, and assume that d is greater than one. Let M_i be that place of K/k with center the minimal prime ideal of R generated by $p + a_i$. By assumption, the degree of M_i is equal to one. Thus, the degree of $B_i = A_i M_i^{-1}$ is greater than or equal to one. Moreover, no place of B_i is at finite distance.

Now the $p + a_i$ have the same poles, and so there are at most $n - 1$ distinct places involved in all of the B_i. But there are n of the B_i, and no two can have a common place. This is a contradiction.

Thus, for $i = 1, \cdots, n$ the degree of the divisor of zeros of $p + a_i$ is equal to one, K contains an element with only one zero and one pole, and so is of genus zero. This completes the proof.

References

1. C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Amer. Math. Soc. Mathematical Surveys, no. 6, 1951.
2. P. Samuel, *Commutative algebra*, mimeographed notes, Cornell University, 1953.
3. P. Samuel, *On unique factorization domains*, Illinois J. Math., vol. 5 (1961), pp. 1–17.

Washington State University
Pullman, Washington