Acta Mathematica et Informatica Universitatis Ostraviensis

Erich Lamprecht

Existence of and computation of integral bases

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 6 (1998), No. 1, 121--128

Persistent URL: http://dml.cz/dmlcz/120523

Acta Mathematica et Informatica Universitatis Ostraviensis 6 (1998) 121–128

Existence and computation of integral bases

Erich Lamprecht

Abstract: The existence of an integral basis of the integral closure $\mathfrak{O}$ of an integral domain $\mathfrak{o}$ in a finite extension of the field of quotients can be proved either by general algebraic considerations or by computation of an $\mathfrak{o}$-module basis of $\mathfrak{O}$ satisfying the conditions of an integral basis. In **2.** we give new results for the first method, in **3.** we illustrate the second method for some types of separable extensions of interest.

Key Words: Integral bases, free modules, algebraic function fields.

Mathematics Subject Classification: 11R33, 11R58, 11S23, 13F++, 16D40.

1. Introduction

Let $\mathfrak{o}$ be an integrally closed integral domain with the quotient field K and $\mathfrak{O}$ be its integral closure in a finite field extension L of K and $\{\omega\} = \{\omega_1, ..., \omega_n\}$ a K-basis of L of integral elements such that $\mathfrak{O}$ is a free $\mathfrak{o}$-module with basis $\{\omega\}$ then this basis is called an *$\mathfrak{o}$-integral basis* of $\mathfrak{O}$. If $\mathfrak{o}$ is a principal ideal domain, then there exist integral bases for all finite separable extensions. We will give some results concerning the question of existence and of computation of integral bases in the case of *Krull* domains $\mathfrak{o}$, i.e.

$$\mathfrak{o} = \bigcap_{\mathfrak{p}} \mathfrak{o}_{\mathfrak{p}} \tag{1.1}$$

is the intersection of discrete valuation rings $\mathfrak{o}_{\mathfrak{p}}$ with the additional finiteness condition ([2],§1 and [8], §2):

$$x \in K, x \neq 0 \quad \Rightarrow \quad x \in \mathfrak{o}_{\mathfrak{p}} \text{ for almost all } \mathfrak{p}. \tag{1.2}$$

Dedekind domains or polynomial rings over principal ideal rings are examples of Krull domains.

The following two criteria can be used:

a. If $\mathfrak{o}$ is a Dedekind domain and L a separable extension of K then a K-basis $\{\omega\}$ of $\mathfrak{o}$-integral elements is an integral basis exactly when for the discriminant of the basis holds

$$d(\{\omega\}) = \mathfrak{d}_{\mathfrak{o}}(L/K) = \prod_{\mathfrak{p}} \mathfrak{d}_{\mathfrak{p}}(L/K), \tag{1.3}$$

if $\mathfrak{d}_\mathfrak{p}(L/K)$ denotes the local discriminant at $\mathfrak{p}$. -

b. A K-basis $\{\omega\}$ of $\mathfrak{o}$-integral elements of the field L is an integral basis over the Krull domain $\mathfrak{o}$ if and only if it is an integral basis for all localizations $\mathfrak{o}_\mathfrak{p}$ (see [5], Proposition 1a and [11], Korollar 2.1). -

By use of these two criteria we reduce the investigation to local considerations. In **2.** the existence of an integral basis for separable extensions of polynomial rings can be shown by theoretical considerations without any algorithm for the computation: this implies several applications. In **3.** for special types of extensions the existence of an integral basis can be shown in the following way: we construct special bases and use the above mentioned rules for the proof of existence.

2. Existence of integral bases

Let $\mathfrak{o}_0$ denote a principial ideal domain; this includes the cases (i) $\mathfrak{o}_0 = \mathbb{Z}$ or (ii) $\mathfrak{o}_0 = k[x]$ (a polynomial ring over a field) or (iii) $\mathfrak{o}_0 = \mathfrak{o}_\mathfrak{p}$ (a discrete valuation ring). Now we consider rings of polynomials in $x_1, ..., x_n$

$$R = \mathfrak{o}_0[x_1, ..., x_n], \tag{2.1}$$

over $\mathfrak{o}_0$ and their normal closures $\mathfrak{O}_L$ in finite separable extensions L of the field of quotients of R. R is noetherian, integrally closed and $\mathfrak{O}_L$ is a finitely generated R-module. We want to apply the following result of Suslin which proves a conjecture of J.P.Serre:

Theorem of Suslin-Serre([10], page 243).*Every finitely generated projective R-Module $\mathcal{M}$ is free.*

If we know that $\mathfrak{O}_L$ is a projective R-module then by use of the result of Serre-Suslin $\mathfrak{O}_L$ is R-free and consequently there must exist an integral basis. In the case $n = 1$ R.Krämer [3] shows the following

Theorem 2.1. *Every finite separable extension of R has an integral basis if $n = 1$, i.e.*

$$R = \mathfrak{o}_0[x_1]. \tag{2.2}$$

Proof of the Theorem. 1. According to [1] (Chap.I. 2, no.8, Lemme 8 (ii)) a finitely generated R-module $\mathcal{M}$ has a finite presentation. If $\mathfrak{m}$ is a maximal ideal of R then the corresponding local ring $R_\mathfrak{m}$ is also noetherian and $\mathcal{M}_\mathfrak{m} = R_\mathfrak{m} \otimes_R \mathcal{M}$ is also a finitely generated $R_\mathfrak{m}$-module; consequently $\mathcal{M}_\mathfrak{m}$ has a finite presentation. According to [1] (Chap.II, Ý3, no.2 and Corollaire 2 of Prop.5) the homomorphism

$$\iota_\mathfrak{m} : (\mathfrak{m}R_\mathfrak{m}) \otimes \mathcal{M}_\mathfrak{m} \to \mathcal{M}_\mathfrak{m}, \quad \sum_i m_i \otimes a_i \mapsto \sum_i m_i \cdot a_i \tag{2.3}$$

is injective iff $\mathcal{M}_\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module. $\mathcal{M}$ is flat iff $\mathcal{M}_\mathfrak{m}$ is flat for all maximal ideals $\mathfrak{m}$ of R ([1], Chap.II. Ý3, no.4, Corollaire of Prop.15). If (2.2) holds for all maximal ideals of R then according to [1], (Chap.II, Ý5, no.2, Cor.2) $\mathcal{M}$ is a projective R-module (these conclusions also hold in the case (2.1)).

2. Now we consider the special case $R = \mathfrak{o}_0[x_1]$ of (2.2) and $\mathcal{M} = \mathfrak{O}_L$ and demonstrate for all maximal ideals $\mathfrak{m}$ of R that the homomorphism $\iota_\mathfrak{m}$ into $\mathcal{M}_\mathfrak{m} = \mathfrak{O}_{L,\mathfrak{m}} = R_\mathfrak{m} \otimes \mathfrak{O}_L$ in (2.3) will be injective. Then the Suslin-Serre theorem shows the freeness of the R-module $\mathfrak{O}_L$ and the existence of a relative integral basis. - A slight modification of the proof of [8] (Theorem 19.5, p. 157) gives the following structure of $\mathfrak{m}$

$$\mathfrak{m}R_\mathfrak{m} = (q, p(x_1)), \tag{2.4}$$

where $p(x_1) \in R[x_1]$ are prime and irreducible polynomials and $q \in R$ either a prime element of R or zero. The set $\mathcal{V}$ of all the prime elements $p(x_1)$ and q - unique up to units of $\mathfrak{o}_0$ - determines the system of the discrete valuations of the Krull domain R. For every $\mathfrak{m}$ we have to evaluate the kernel of $\iota_\mathfrak{m}$, i.e.

$$\iota_\mathfrak{m}(y) = q \cdot a_1 + p \cdot a_2 = 0 \quad \text{for } y = q \otimes a_1 + p \otimes a_2, \quad a_1, a_2 \in \mathfrak{O}_{L,\mathfrak{m}}. \tag{2.5}$$

If $q \neq 0$ then $\iota_\mathfrak{m}(y) = 0$ iff $a_2 = \frac{-q \cdot a_1}{p}$. - Otherwise for $q = 0$ the injectivity of $\iota_\mathfrak{m}$ is obvious. - If we can show

$$\frac{a_1}{p} \in \mathfrak{O}_{L,\mathfrak{m}} \tag{2.6}$$

then $y = q \otimes a_1 - (q \cdot p) \otimes \frac{a_1}{p} = q \otimes a_1 - q \otimes \frac{p a_1}{p} = q \otimes a_1 - q \otimes a_1 = 0$ demonstrates the injectivity of $\iota_\mathfrak{m}$.
Let v_p and v_q be the normalized discrete valuations of R corresponding to the prime elements p, q and let $v_\mathfrak{P}$ and v_Ω respectively be corresponding extensions in L then $v_\mathfrak{P}(q) = 0$ for all extensions. This implies $0 \leq v_\mathfrak{P}(a_2) = v_\mathfrak{P}(q) - v_\mathfrak{P}(p) + v_\mathfrak{P}(a - 1)$ and $v_\mathfrak{P}(p) \leq v_\mathfrak{P}(a_1)$. This holds for all such $\mathfrak{P}$ and we obtain (2.6) and the theorem. □

Remark 1. Let $\mathfrak{o}$ be an arbitrary noetherian Krull domain with quotient field K and $L = K[\alpha]$ a finite separable extension where α satisfies the monic irreducible polynomial $f[T] \in [T]$ with the discriminant $d = d(f)$ and let $\mathfrak{O}_L$ be the integral closure of $\mathfrak{o}$ in L. Then we only have to check the maximal ideals $\mathfrak{m} \ni d$ for the projectivity of the $\mathfrak{o}$-module $\mathfrak{O}_L$. But this does not yet show the freeness. - According to examples of Kaplansky, Ojanguren and others the above method of proof can not work for $n > 1$; and this method gives no computation of a base.

The above mentioned cases (i), (ii) and (iii) correspond to the following essential special cases of this theorem, namely (i') $R = \mathbb{Z}[x_1]$, (ii') $R = k[x, x_1]$ and (iii') $R = \mathfrak{o}_\mathfrak{p}[x_1]$. - (iii') can be applied for reducing mod $\mathfrak{p}$ and lifting respectively of integral bases of function fields.

Let L be an algebraic function field of one variable over the exact field of constants k and $x \in L$ be transcendental over k such that L is finite and separable over $k(x)$. A discrete valuation $v_\mathfrak{P}$ of L with non-trivial restriction $v_{\mathfrak{p}_0}$ in k is called a functional extension of $v_{\mathfrak{p}_0}$ to L if the reduction of L with respect to $\mathfrak{P}$ - i.e. the residue field $\overline{L}$ - is also a function field over $\overline{k}$, the reduction of k mod $\mathfrak{p}_0$. $\mathfrak{p}$ denotes the restriction of $\mathfrak{P}$ in K.

Definition. $\mathfrak{P}$ and $v_\mathfrak{P}$ respectively are called *x-regular-inert* or *x-good* if the following holds: (α) $\mathfrak{p}$ of $k(x)$ has only one extension $\mathfrak{P}$ in L and $\mathfrak{P}$ is inert over $K = k(x)$;

(β) $\overline{k}$ is the exact field of constants of $\overline{L}$; (γ) L and $\overline{L}$ have the same genus $g(L/k) = g(\overline{L}/\overline{k})$.

In this situation we have the following rings

$$\mathfrak{o}_{\mathfrak{p}_0}[x] \subset \mathfrak{o}_{\mathfrak{p}} \subset k[x], \quad \mathfrak{o}_{\mathfrak{p}},\ \mathfrak{O}_{\mathfrak{P}} \text{ valuation rings of } K \text{ and } L \text{ respectively,}$$
$$\mathfrak{O}_{\mathfrak{P},x} = \mathfrak{O}_L \cap \mathfrak{O}_{\mathfrak{P}}, \quad \mathfrak{O}_L \text{ integral closure of } k[x] \text{ in } L. \tag{2.7}$$

$\mathfrak{O}_{\mathfrak{P},x}$ is also a Krull domain and the integral closure of $\mathfrak{o}_{\mathfrak{p}_0}[x]$ in L. - If $\mathfrak{P}$ is x-regular-inert then by use of reduction theory of divisors (see [3], p.8) and differentials [4] and the Hurwitz-formula for differents $\mathfrak{D}(L/K) = \mathfrak{D}_x \cdot \mathfrak{D}_\infty$ and discriminants $\mathfrak{d}(L/K) = \mathfrak{d}_x \cdot \mathfrak{d}_\infty$ of L over K and $\overline{L}$ over $\overline{K}$ and the corresponding reduced terms we have

$$\overline{\mathfrak{D}(L/K)} = \overline{\mathfrak{D}_x} \cdot \overline{\mathfrak{D}_\infty} = \mathfrak{D}(\overline{L}/\overline{K}) = \mathfrak{D}_{\overline{x}} \cdot \mathfrak{D}_{\overline{\infty}}, \tag{2.8}$$
$$\overline{\mathfrak{d}(L/K)} = \overline{\mathfrak{d}_x} \cdot \overline{\mathfrak{d}_\infty} = \mathfrak{d}(\overline{L}/\overline{K}) = \mathfrak{d}_{\overline{x}} \cdot \mathfrak{d}_{\overline{\infty}}.$$

$\mathfrak{D}_\infty$ denotes the $\mathfrak{p}_\infty$-part of the different and $\mathfrak{D}_x$ the part of the x-integral places in the different and analogously for the discriminant $\mathfrak{d}_x, \mathfrak{d}_\infty$ and the reduced divisors $\overline{\mathfrak{D}_x}, \ldots$ and terms in the reduced fields $\mathfrak{D}_{\overline{x}}, \ldots$. - In the following we use the *assumption*

$$\overline{\mathfrak{D}_x} = \mathfrak{D}_{\overline{x}}, \quad \overline{\mathfrak{d}_x} = \mathfrak{d}_{\overline{x}}. \tag{2.9}$$

Almost all x-regular-inert $\mathfrak{P}$ satisfy the condition (2.9); by discriminant conditions the exceptions can be described. - By use of Theorem 2.1 in the case (iii') we obtain

Theorem 2.2. *Let the extension L over $k(x)$ satisfy the condition* (2.9) *for an x-regular-inert $\mathfrak{P}$ and $\{\omega\} = \{\omega_1, \ldots, \omega_n\}$ an integral basis of $\mathfrak{O}_{\mathfrak{P},x}$ over $\mathfrak{o}_{\mathfrak{p}_0}[x]$ - and also of $\mathfrak{O}_L$ over $k[x]$ - then the residues $\{\overline{\omega}\} = \{\overline{\omega_1}, \ldots, \overline{\omega_n}\}$ yield an integral basis of $\mathfrak{O}_{\overline{L}}$ over $\overline{k}[x]$. - If on the other hand an integral basis $\{\overline{\omega}\}$ of $\mathfrak{O}_L$ over $\overline{k[x]}$ is given, then there always exists an integral basis $\{\bar{\omega}_1, \ldots, \bar{\omega}_n\}$ of $\mathfrak{O}_L$ over $k[x]$ such that $\overline{\bar{\omega}}_\nu = \overline{\omega}_\nu$ for $\nu = 1, \ldots, n$.* This result can be used for the computation of an integral basis of $\mathfrak{O}_L$ over $k[x]$ if we know an integral basis of $\mathfrak{O}_{\overline{L}}$ over $\overline{k}[x]$. - We mention some further applications.

Remark 2. Let $\mathfrak{P}$ be an x-regular-inert functional extension of $\mathfrak{p}_0$ of k in L and let the field F be given according to

$$k \subset K = k(x) \subseteq F \subseteq L, \quad L \text{ separable over } K, \tag{2.10}$$

and let the restriction $\mathfrak{P}'$ of $\mathfrak{P}$ in F also be x-regular-inert. Then similar conditions for the reduction of integral bases $\{\omega\}$ of L over F and for the lifting of integral bases of $\overline{L}$ over $\overline{F}$ can be given.

The following theorem shows an improvement of the criteria **b.** in section **1.**

Theorem 2.3. *Let $\mathfrak{o}_0$ be a Krull domain with the field of quotients k and L a finite separable extension of rank n of the rational function field $K = k(x)$ and let $\mathfrak{O}$ be the integral closure of $\mathfrak{o}_0[x]$ in L. Then the field basis $\{\omega\} = \{\omega_1, \ldots, \omega_n\}$ of L over $k(x)$ is an integral basis for $\mathfrak{O}$ over $\mathfrak{o} = \mathfrak{o}_0[x]$ iff $\{\omega\}$ is an integral basis for $\mathfrak{O}_{\mathfrak{P},x}$ over $\mathfrak{o}_{\mathfrak{p}_0}[x]$ for all primes $\mathfrak{p}_0$ of $\mathfrak{o}_0$.* According to [3] (Satz II.5) it is sufficient to consider only the primes $\mathfrak{P}|\mathfrak{p}_0$ dividing the basis discriminant of $\{\omega\}$.

3. Computation of integral bases

On the other hand we have the following situation: If $\mathfrak{o}$ is a noetherian Krull domain of higher dimension, i.e. a polynomial ring (2.1), then there exist several types of field extensions with integral bases. In these cases explicite formulas of computation for the bases can be given. We prove the local integral bases property and apply the localization method mentioned in criteria **b** of section **1** and in [5]; this shows the property of a global integral basis and gives formulas for its computation.

We consider algebraic extensions of the field of quotients K of $\mathfrak{o}$ of the kind:

$$L = K(y_1, y_2, ..., y_m), \tag{3.1}$$
$$y_\mu^{n_\mu} = B_\mu \in K,\ n = \operatorname{lcm}(n_1, ..., n_m) \quad (\mu = 1, ..., m), \quad \operatorname{char}(K) \nmid n.$$

Let ϵ_n be a primitive n-th root of unity. If $\epsilon_n \in K$ then L is called a *Kummer*-extension of exponent n. We may assume that $n_\mu | n_{\mu-1}$, $n = n_m$, $n_0 = 1$ and that all the B_μ are integral elements of a Krull domain $\mathfrak{o}$ of K. According to [5], Theorem IVa we have

Theorem 3.4. *Let $K = k(x_1, ..., x_m)$ be a rational function field, k the field of quotients of the principal ideal domain $\mathfrak{o}_0$ containing the n-th root of unity and L be a Kummer-extension of exponent n then the integral closure $\mathfrak{O}_L$ of $\mathfrak{o}$ always has an integral basis.- More general if $\mathfrak{o}$ is a Krull domain of a separable extension F of K and if n is a unit in $\mathfrak{o}$ and if the Kummer-extension L of F has a distinguished generation, then also an integral basis of $\mathfrak{O}_L$ over $\mathfrak{o}$ can be calculated.*

Remark 3. The integral basis consists of products of powers of the elements y_μ modified by factors of the elements B_μ, i.e. it has the form

$$\{..., \prod_{\mu=1}^{m} y_\mu^{i_\mu} \cdot \tilde{b}^{-1}_{i_1,...,i_m}, ...\} \text{ for } 1 \le i_\mu \le n_\mu,\ \mu = 1, ..., m; \tag{3.2}$$

the elements $\tilde{b}_{i_1,...,i_m} \in K$ are suitable factors of B_μ in (3.1). If these elements can be constructed in K the generation is called *distinguished.*

If $\epsilon_n \notin K$ an extension (3.1) is called a *radical*-extension (*multi-radical*-extension) of K. Applying the theory of local fields the existence of integral bases can be proved in a similar way for $m = 1$, i.e. for a single equation. This is shown in [6]. The following theorem contains the results for a radical equation of prime degree p, i.e. $y^p = B \in \mathfrak{o}$, also if p is not a unit in $\mathfrak{o}$. This gives an improvement of theorem 3.1 for this case.

Theorem 3.5. *Let $K = k(x_1, ..., x_m)$ be a rational function field, k the field of quotients of the principal ideal domain $\mathfrak{o}_0$ and L a radical extension of prime degree p, then the integral closure $\mathfrak{O}_L$ of $\mathfrak{o} = \mathfrak{o}_0[x_1, ..., x_n]$ always has an integral basis. - More general if $\mathfrak{o}$ is a Krull domain of a separable extension F of K and if L is a radical-extension of F of prime degree p with a distinguished generation, then also an integral basis of $\mathfrak{O}_L$ over $\mathfrak{o}$ can be calculated.*

Remark 4- In the rational čase we may assume that $0 < v_p(B) < p$ for all p of o. We háve to consider two subcases:
(a) If $v_v(B) > 0$ for all $p|p$ then we obtain a modified power basis of the form

$$\{u\} = \{1,\ldots, if \cdot g;|\ldots\}, \quad (i/ = 1, \ldots,p - 1), \tag{3.3}$$

with suitable factors g_v G o of J3. - If char(i^) = p or if Oo D Q all p are of this kind.
(b) If $Vp(B) = 0$ for some p|p we need the following corresponding numbers

$$e_p = u_p(p), \quad ej = e_p - — - , \tag{3.4}$$

$$/3_p = \max(/J \text{ G No} \mid 3a_p \text{ G o such that } v_p(a£ - B) = /?).$$

Then there exists an integrál basis ([6],II, Satz 5.4, 5.6 and III, Satz 3.5) of the form

$$\{u\} = \{1,\ldots, (y - a)'' \cdot g\sim| -..\} \quad (i/ = 1, \ldots,P - 1) \tag{3.5}$$

with suitable factors g_u G o determined by B where a G o is determined with the aid of approximation by the a_p. In the speciál čase $K = Q$ this result is mentioned in [9],(Kap.III).- The extension L over F is distinguished if the corresponding factors g_v can be calculated in F.

Let the íield K of quotients of the Krull domain o be of prime characteristic, i.e. char(it') = p. Then a separable and cyclic extension L of the form

$$L — K(y), \quad p(y) = y^p - y = BeK(\text{ and } G \text{ o respectively }) \tag{3.6}$$

is called an ^rčm-^c/ireier-extension. This is of speciál interest for function fields of several variables in prime characteristic p.

Theorem 3.6. *Let $K = k(x|_1,\ldots, x_m)$ be a rational function field over a field k with* char(fc) = p *and L an Artin-Schreier-extension of prime degree p, then the integrál closure OL of o — k[xi,..., x_n] has an integrál basis.- If K is the field of quotients of a generál Krull domain and L is a distinguished extension then there exists again an integrál basis.*

Remark 5. In the čase of a factorial ring o the constant term of the equation (3.6) can be transformed to

$$^B = \sim x7 \text{———} X''' \quad G, \ TT_P €O \quad (p=1,\ldots,r), \quad X_p > 0, \tag{3.7}$$

where the $7T_P$ are prime elements of o corresponding to ramified or inseparable primes. Then according to [6], III, Satz 4.3 we obtain again a modified power integrál basis

$$\{1,2/t/i,\ldots,2/^{P''}\sim^{1}0P\text{-}I\}, \quad g_P \text{ G o}, \tag{3.8}$$

where the g_p are suitable power products of the TX_P. - If in the generál čase a representation (3.6) can be found the extension is called distinguished and we háve the samé result.

If $\epsilon_n \notin K$ the investigation of *abelian* extensions of exponent n of the field K of quotients of a Krull domain can be reduced to Kummer or radical extensions by a method sketched in [7], section 5. We illustrate this method for $n = p$ and consider the fields

$$K_p = K(\epsilon_p) \text{ and } L_p = L(\epsilon_p),\ \epsilon_p = p\text{-th root of unity },\ [L_p : K_p] = g, \tag{3.9}$$

and special radical extensions of K_p (for more general cases see [3]).

Theorem 3.7. *Let $K = k(x_1, ..., x_m)$ be a rational function field, $\epsilon_p \notin k$, $\mathrm{char}(k) \neq p$ and L a cyclic extension of prime degree p. Then the integral closure $\mathfrak{O}_L$ of $\mathfrak{o} = k[x_1, ..., x_n]$ always has an integral basis.- If in a more general case of K and $\mathfrak{o}$ there is a distinguished cyclic extension L then there exists again an integral basis.*

Remark 6. Let $L_p = K_p(y)$ have the special generation $y^p = B \in \mathfrak{o}$ and let $g = p-1$ then there exists the modified normal basis of L over K

$$\{\omega\} = \{1, u, \sigma(u), ..., \sigma^{p-2}(u)\}, \quad \mathrm{Gal}(L/K) = \langle\sigma\rangle, \tag{3.10}$$
$$u = \sum_{i=0,...,p-2} \tau^i(y), \quad \mathrm{Gal}(K_p/K) = \langle\tau\rangle.$$

If $g < p-1$ then a more complicated formula for u has to be used; modified versions of the integral basis also can be given (see [3], Satz III.5 and Satz III.3). - If K is the field of quotients of a Krull domain $\mathfrak{o}$ where p is a unit of $\mathfrak{o}$ and if in K_p the special form of B can be constructed then the extension is called distinguished and an integral basis can be constructed.

According to these theorems the radical extensions or cyclic extensions of degree p of factorial Krull domains $\mathfrak{o} = k[x_1, ..., x_n]$ always have an integral basis. This can be generalized for single radical extensions of arbitrary degree ([6]) and Kummer extensions ([5]).

If $m > 1$ multi-radical extensions (3.1) over Dedekind domains in $\mathbb{Q}$ or in number fields or in other fields can be described as in [9] and in [12] by composition of the results of theorem 3.2. Especially in the case of arithmetic function fields over a number field the condition that p is a unit of $\mathfrak{o}$ has to be considered separately. A quite similar method gives explicit integral bases for multi-radical extensions of exponent p of Krull domains $\mathfrak{o} = k[x_1, ..., x_n]$.

For special abelian extensions of the above mentioned fields the existence can also be proved by explicitly given bases. - The same method works for multi-Artin-Schreier extensions of exponent p because these extensions are distinguished. In this case and for abelian extensions we obtain also modified power bases or normal integral bases.

These results suggest the *conjecture* that for all solvable extensions of quotient fields of rings of type (2.1) an integral basis is existing and can be computed by explicit formulas.

References

[1] Nicolas Bourbaki, Algèbre Commutative, Chapitre 1+2. Herrmann, Paris 1961.

[2] Nicolas Bourbaki, Algèbre Commutative, Chapitre 7. Herrmann, Paris 1965.

[3] Rudi Kraemer, Existenz und Konstruktion von Ganzheitsbasen bei Erweiterungen von Krullringen in algebraischen Funktionenkörpern. Diss. Saarbrücken (1996), 1-138.

[4] Erich Lamprecht, Zur Klassifikation von Differentialen in Körpern von Primzahlcharakteristik. Math.Nachr.**19**, 353-374 (1958).

[5] Erich Lamprecht, Integral bases in Function and Number Fields. Colloq. Math. Soc. János Bolyai, Number Theory, Budapest, 795-825 (1987).

[6] Erich Lamprecht, Verzweigungsordnungen, Differenten und Ganzheitsbasen bei Radikalerweiterungen I, II, III. Arch.Math.**56**, 569-581 (1991); Arch.Math.**57**, 254-266 (1991); Ann.Univ.Saraviensis **8**, No.4, 395-415 (1997).

[7] Erich Lamprecht, Über zyklische Erweiterungen p-ten Grades von Körpern, die die p-ten Einheitswurzeln nicht enthalten. Ann. Univ.Saraviensis **7**, No.3, 51-74 (1996).

[8] Hideyuki Matsumura, Commutative ring theory. Cambridge studies in advanced mathematics 8 (1994).

[9] Bernhard Schmal, Diskriminanten, $\mathbb{Z}$-Ganzheitsbasen und relative Ganzheitsbasen bei Komposita von Radikalerweiterungen vom Grad p über $\mathbb{Q}$. Diss. Saarbrücken 1991.

[10] A.A. Suslin, Projective Modules over a Polynomial Ring are free. Dokl.Akad. Nauk. SSSR, Tom 229, No.5 (1976).

[11] August Thomé, Zur Existenz von Ganzheitsbasen bei endlichen separablen Erweiterungen von Dedekindringen. Diss. Saarbrücken 1986.

[12] August Thomé, Existenz von Ganzheitsbasen bei Kummererweiterungen und Komposita. Arch.Math.**51**, 523-531 (1988).

Author's address: Fachbereich 9 Mathematik, Universität des Saarlandes, Postfach 15 11 50, D-66041 Saarbrücken

Received: January 27, 1998