

Note on complete local integrity domains

By

Masayoshi NAGATA

(Received Dec. 1, 1953)

Previously some interesting results concerning prime ideals in rings of formal power series were proved by C. Chevalley [1]. In the present paper, we want to offer a new treatment on the similar assertions. We see on the way a new result that when \mathfrak{o} is a complete (Noetherian) local integrity domain with a basic field k , \mathfrak{o} is separably generated¹⁾ over k if and only if there exists a system of parameters x_1, \dots, x_n of \mathfrak{o} such that \mathfrak{o} is separable over the ring $k\{x_1, \dots, x_n\}$ (formal power series).

Throughout the present paper, a local ring means a Noetherian local ring which contains a field.

§1. Kroneckerian products.

Let \mathfrak{o}_1 and \mathfrak{o}_2 be complete local rings with basic fields k_1 and k_2 respectively. If K is a field containing both k_1 and k_2 , we can define the Kroneckerian product of (k_1 -algebra) \mathfrak{o}_1 and (k_2 -algebra) \mathfrak{o}_2 over K , as was defined by C. Chevalley [2]. We denote this Kroneckerian product by $\mathfrak{o}_1/k_1 \times_K \mathfrak{o}_2/k_2$ ²⁾. (For the detail, see Chevalley [2]). When $k_1 = k_2 = K$, we denote this by $\mathfrak{o}_1 \times_K \mathfrak{o}_2$.

We define further Kroneckerian products of complete local rings with discrete rings:

Let \mathfrak{o}_1 be a complete local ring with basic field k_1 , and let \mathfrak{o}_2 be a discrete ring³⁾ which contains a field k_2 . Assume that K is a field which contains both k_1 and k_2 . We define the Kroneckerian product of k_1 -algebra \mathfrak{o}_1 and discrete k_2 -algebra \mathfrak{o}_2 over K as follows:

1) For the definition, see Chevalley [1] or §2 in the present paper.

2) Though Chevalley [2] denotes this ring by $\mathfrak{o}_1 \times_{K'} \mathfrak{o}_2$, we dare use a more complicated notation because the product depends on the choice of basic fields.

3) \mathfrak{o}_2 may be a topological ring which is not discrete; we only regard it as an abstract ring (or a discrete topological ring).

Let B_1 be a strong base of \mathfrak{o}_1 over k_1 and let B' be a linearly independent base of \mathfrak{o}_2 over k_2 . We set $\mathfrak{o} = \{ \sum (\sum a_{\lambda n} v_\lambda) u_n ; a_{\lambda n} \in K, v_\lambda \in B', u_n \in B_1, \sum a_{\lambda n} v_\lambda \text{ is a finite sum} \}$. We introduce in \mathfrak{o} operations of sum and product by the followings;

$$(\sum (\sum a_{\lambda n} v_\lambda) u_n) + (\sum (\sum b_{\lambda n} v_\lambda) u_n) = \sum (\sum (a_{\lambda n} + b_{\lambda n}) v_\lambda) u_n,$$

$$(\sum (\sum a_{\lambda n} v_\lambda) u_n) (\sum (\sum b_{\lambda n} v_\lambda) u_n) = \sum (\sum (\sum a_{\lambda n} b_{\lambda' n'} c_{\lambda \lambda'} d_{nn'}) v_\lambda) u_m,$$

where $v_\lambda v_{\lambda'} = \sum c_{\lambda \lambda'} v_\kappa$ ($c_{\lambda \lambda'} \in k_2$) and $u_n u_{n'} = \sum d_{nn'} u_m$ ($d_{nn'} \in k_1$). (Observe that $\sum a_{\lambda n} b_{\lambda' n'} c_{\lambda \lambda'} d_{nn'}$ is a finite sum).

It is easy to see that though this depends on the choice of strong base B_1 and linearly independent base B' of \mathfrak{o}_1 and \mathfrak{o}_2 respectively, the structure of \mathfrak{o} does not depend on the choice of them. This ring \mathfrak{o} is called the Kroneckerian product of (complete local) k_1 -algebra \mathfrak{o}_1 and (discrete) k_2 -algebra \mathfrak{o}_2 over K and we denote this by $\mathfrak{o}_1/k_1 \times_K (\mathfrak{o}_2/k_2)_d$. When $k_1 = k_2 = K$, we denote this by $\mathfrak{o}_1 \times_K (\mathfrak{o}_2)_d$. If $\mathfrak{o}_2 = k$ is a field, we denote this by $\mathfrak{o}_1 \times_K k$.

Next we explain an easy, but, important lemma:

Lemma 1. Let \mathfrak{o}_1 and \mathfrak{o}_2 be complete local rings with the same basic field K . Then $\mathfrak{o}_1 \times_K \mathfrak{o}_2 = \mathfrak{o}_1 \times_K (\mathfrak{o}_2)_d$.

Proof. Let B_1 and B_2 be strong bases of \mathfrak{o}_1 and \mathfrak{o}_2 over K respectively and let B' be a linearly independent base of \mathfrak{o}_2 over K . Set $\mathfrak{o}' = \mathfrak{o}_1 \times_K (\mathfrak{o}_2)_d$ and $\mathfrak{o} = \mathfrak{o}_1 \times_K \mathfrak{o}_2$. Then

$$\mathfrak{o}' = \{ \sum (\sum a_{\lambda n} v_\lambda) u_n ; a_{\lambda n} \in K, v_\lambda \in B', u_n \in B_1, \sum a_{\lambda n} v_\lambda \text{ is a finite sum} \},$$

$$\mathfrak{o} = \{ \sum b_{\mu n} w_\mu u_n ; b_{\mu n} \in K, w_\mu \in B_2, u_n \in B_1 \}.$$

Let ϕ be a mapping from \mathfrak{o}' into \mathfrak{o} as follows:

$$\phi(\sum (\sum a_{\lambda n} v_\lambda) u_n) = \sum b_{\mu n} w_\mu u_n,$$

where $\sum a_{\lambda n} v_\lambda = \sum b_{\mu n} w_\mu$ ($\sum b_{\mu n} w_\mu$ may be infinite sum).

Similarly, let ϕ^* be a mapping from \mathfrak{o} into \mathfrak{o}' as follows:

$$\phi^*(\sum b_{\mu n} w_\mu u_n) = \sum (\sum a_{\lambda n} v_\lambda) u_n,$$

where $\sum b_{\mu n} w_\mu = \sum a_{\lambda n} v_\lambda$ ($\sum a_{\lambda n} v_\lambda$ must be a finite sum).

Then we see easily that ϕ and ϕ^* are homomorphisms and that $\phi \circ \phi^*$ is the identity mapping. Therefore ϕ is an isomorphism.

§2. Separably generated extensions.

We denote hereafter by p the characteristic of the field of reference when it is not zero or the number 1 for the other case.

Definition. We say that a complete local integrity domain \mathfrak{o}

is separably generated over its basic field k if $\mathfrak{o} \times_k k^{p^{-1}}$ is an integrity domain.

Theorem 1. *Let \mathfrak{o} be a complete local integrity domain with a basic field k . Then the following three conditions are equivalent to each other:*

- (1) \mathfrak{o} is separably generated over k .
- (2) For any strongly linearly independent subset B of \mathfrak{o} over k , $B_p = \{u^p; u \in B\}$ is also strongly linearly independent over k .
- (3) For any integer m , $\mathfrak{o} \times_k k^{p^{-m}}$ is an integrity domain.

Proof. Assume that B is a strongly linearly independent set of \mathfrak{o} over k and assume that B^p is not strongly linearly independent over k : There exist $u_n \in B$ such that $\sum a_n u_n^p = 0$ ($u_i \neq u_j$ if $i \neq j$, $a_n \in k$), and therefore in $\mathfrak{o} \times_k k^{p^{-1}}$, $(\sum a_n^{-1} u_n)^p = 0$ and $\sum a_n^{-1} u_n \neq 0$. Therefore $\mathfrak{o} \times_k k^{p^{-1}}$ is not an integrity domain. This proves that (2) follows from (1). Next we prove the converse: Assume that $\mathfrak{o} \times_k k^{p^{-1}}$ contains a divisor c of zero ($c \neq 0$). Since $c^p \in \mathfrak{o}$, we see that $c^p = 0$. We write $c = \sum a_n u_n$ ($\{u_n\}$ is strongly linearly independent over k ($u_n \in \mathfrak{o}$, $a_n \in k^{p^{-1}}$)). Then $\{u_n^p\}$ is not strongly linearly independent over k . These being settled, the equivalence with (3) is evident.

Corollary. If a complete local integrity domain \mathfrak{o} is separably generated over its basic field k , then for any integer m , $\mathfrak{o} \times_k k^{p^{-m}}$ is separably generated over $k^{p^{-m}}$.

Remark 1. It is evident that if \mathfrak{o} is a complete local ring with a basic field k and if K is a field which contains k , then $\mathfrak{o} \times_k K$ is a complete semi-local ring; we have the identity

$$\mathfrak{o} \times_k K = \mathfrak{o}/k \times_k k/k = \mathfrak{o}/k \times_k K/K.$$

Remark 2. By Lemma 1, we see that when $[k:k^p] < \infty$, a complete local integrity domain \mathfrak{o} with a basic field k is separably generated over k if and only if the quotient field of \mathfrak{o} is separably generated over k .⁴⁾ In general case, we see easily that the tensor product $\mathfrak{o} \otimes_k k^{p^{-1}}$ is a subring $\mathfrak{o} \times_k k^{p^{-1}}$ and therefore we see that if \mathfrak{o} is separably generated over k , then the quotient field of \mathfrak{o} is

4) We say, according to C. Chevalley [1], that a field K is separably generated over its subfield k if the tensor product $K \otimes_k k^{p^{-1}}$ is an integrity domain. This is equivalent to that every finitely generated extension field of k contained in K has a separating transcendence base over k .

separably generated over k . The converse is not true as is easily seen.

§3. Derivations.

Definition. Let \mathfrak{o} be a complete local integrity domain. A derivation D of \mathfrak{o} is a linear operator to the quotient field L of \mathfrak{o} which satisfies the following conditions:

- i) $D(xy) = xDy + yDx$ (for any $x, y \in L$),
- ii) There exists an element $d (\neq 0)$ of \mathfrak{o} such that $dDx \in \mathfrak{o}$ for any $x \in \mathfrak{o}$ and if $\sum u_n$ is a convergent series in \mathfrak{o} then $\sum dDu_n$ is also convergent (therefore $\sum Du_n$ has a meaning in L) and $D(\sum u_n) = \sum Du_n$.

A derivation D , for which it holds that $Da=0$ if a is in a subring \mathfrak{o}' of \mathfrak{o} , is called a derivation of \mathfrak{o} over \mathfrak{o}' .

It is evident that the totality of derivations of \mathfrak{o} (over a subring) form an \mathfrak{o} -module. Linear dependency of derivations is defined in this sense.

Lemma 2. Let \mathfrak{o} be the ring of formal power series in x_1, \dots, x_n over a field k . Then the partial derivations $D_i = \partial/\partial x_i$ ($i=1, \dots, n$) form a maximal linearly independent set of derivations of \mathfrak{o} over k .

Proof is easy.

Lemma 3. Let \mathfrak{o} be a complete local integrity domain with a basic field k . Let L be the quotient field of \mathfrak{o} . Assume that the characteristic p of \mathfrak{o} is not zero. Let M be the subfield of L generated by L^p and k . Take an integer r such that $[L:M] = p^r$. Then any maximal set of linearly independent derivations of \mathfrak{o} over k consists of r derivations.

Proof. If a is in L^p , $Da=0$ for any derivation D of \mathfrak{o} . Therefore, for any derivation D of \mathfrak{o} over k and for any element a of M , we have $Da=0$. We take elements, a_1, \dots, a_r of L such that $L = M(a_1, \dots, a_r)$. Then we can find derivations D_1, \dots, D_r of \mathfrak{o} over k such that $D_i a_j = \delta_{ij}$ (Kroneckerian δ). That this is a maximal set of linearly independent derivations can be proved easily.

Theorem 2. *Let \mathfrak{o} be a complete local integrity domain of dimension n and with a basic field k . Then the number of members of a maximal set of linearly independent derivations of \mathfrak{o} over k is at least n . It is n if and only if \mathfrak{o} is separably generated over k .*

Proof. Let x_1, \dots, x_n be a system of parameters of \mathfrak{o} and set $\mathfrak{r} = k\{x_1, \dots, x_n\}$. Let \mathfrak{o}' be the totality of separably algebraic (integral) elements of \mathfrak{o} over \mathfrak{r} .

1) We first show that a maximal set of linearly independent derivations of v' over k consists of just n numbers: It is true for r by Lemma 2; since v' is separable over r , we see that this is also true for v' (similarly to the case of the theory of fields).

2) Next we show that v' is separably generated over k : Let c be an element of v' such that v' is contained in the quotient field of $v[c]$ and let $f(x)$ be the irreducible monic polynomial over v satisfied by c . If $v' \times_r k^{p-1}$ is not an integrity domain, we see that $f(x)$ is reducible over $k^{p-1}\{x_1, \dots, x_n\}$, which is impossible because $f(x)$ is separable and $k^{p-1}\{x_1, \dots, x_n\}$ is purely inseparable over $k\{x_1, \dots, x_n\}$.

3) We prove the general case by induction on $[v : v']^{(p)}$ ($p \geq 2$): Let c_1, \dots, c_r be elements of v such that $c_i^p \in v'[c_1, \dots, c_{i-1}]$, and $[v'[c_1, \dots, c_r] : v'] = p^r$ ($[v : v'] = p^r$). We set $\mathfrak{s} = k\{x_1^p, \dots, x_n^p\}[v'^p][c_1^p, \dots, c_r^p]$, $v'' = v'[c_1, \dots, c_{r-1}]$, $\mathfrak{s}'' = k\{x_1^p, \dots, x_n^p\}[v''^p][c_1^p, \dots, c_{r-1}^p]$. Then $[\mathfrak{s} : \mathfrak{s}''] \leq p$, $[v : v''] = p$ and $[v'' : \mathfrak{s}''] \geq p^n$ (by induction assumption), which shows $[v : \mathfrak{s}] = [v : \mathfrak{s}''] / [\mathfrak{s} : \mathfrak{s}''] = [v : v''] [v'' : \mathfrak{s}''] / [\mathfrak{s} : \mathfrak{s}''] \geq p^n$. Thus we see that there exists a system of n linearly independent derivations of v over k .

4) We assume that v is separably generated over k . We use the same notations as in 3). Since our assertion is true for v' , we prove our assertion by induction on $[v : v']$. Since v'' is a subspace of v , we see that v'' is also separably generated. Therefore by our induction assumption we see that $[v'' : \mathfrak{s}''] = p^n$. Therefore we have only to show that $[\mathfrak{s} : \mathfrak{s}''] = p$. Let B be a strong base of v'' over k . Then $\{B, Bc_r, \dots, Bc_r^{p-1}\}$ form a strong base of $v''[c]$ over k . If $[\mathfrak{s} : \mathfrak{s}''] = 1$, we must have a relation $\sum_{i=0}^{p-1} b_i c_i^p = 0$ ($b_i \in \mathfrak{s}'', b_0 \neq 0$). Then we must have a relation $\sum_{\lambda} a_{\lambda} u_{\lambda}^p c_r^p = 0$ ($a_{\lambda} \in k, u_{\lambda} \in B, 0 \leq i \leq p-1, \sum a_{\lambda} u_{\lambda}^p = b_i$), which is a contradiction to our assumption that v is separably generated over k (because $v''[c]$ is a subspace of v).

5) Conversely, we assume that a maximal set of linearly independent derivations over k consists of just n members. We can take a set of linearly independent derivations D_1, \dots, D_n over k and a system of elements c_1, \dots, c_n of v such that $D_i c_j = \delta_{ij}$ (Kroneckerian δ). We may assume that these c_i are unit in v , because if c_i is not a unit, we may take $1+c_i$ instead of c_i . It is evident that x_1^p, \dots, x_n^p is a system of parameters of v . We set $y_i = c_i x_i^p$.

5) $[v : v']$ means the index of the quotient field of v over that of v' .

Then y_1, \dots, y_n form a system of parameters of \mathfrak{o} . Then by our construction, we see easily that every derivations of $k\{y_1, \dots, y_n\}$ over k can be uniquely extended to a derivation of \mathfrak{o} over k . This shows that \mathfrak{o} is separable over $k\{y_1, \dots, y_n\}$. Now we see that \mathfrak{o} is separably generated over k by virtue of 2) above.

We have proved in the same time (in 2) and 5)) the following

Theorem 3. *Let \mathfrak{o} be a complete local integrity domain with a basic field k . Then \mathfrak{o} is separably generated over k if and only if there exists a system of parameters x_1, \dots, x_n of \mathfrak{o} such that \mathfrak{o} is separable over $k\{x_1, \dots, x_n\}$.*

Now we prove

Theorem 4. *Assume that a complete local integrity domain \mathfrak{o} is separably generably generated over its basic field k . If K is an extension field of k such that k is separably algebraically closed in K , then $\mathfrak{o} \times_k K$ is an integrity domain.*

Proof. By virtue of Theorem 3, we can choose a system of parameters x_1, \dots, x_n of \mathfrak{o} so that \mathfrak{o} is separable over $k\{x_1, \dots, x_n\}$. We choose an element c of \mathfrak{o} so that $[\mathfrak{o} : k\{x_1, \dots, x_n\}[c]] = 1$ and let $f(x)$ be the irreducible monic polynomial over $k\{x_1, \dots, x_n\}$ satisfied by c . If $\mathfrak{o} \times_k K$ is not an integrity domain, we have that $f(x)$ is reducible over $K\{x_1, \dots, x_n\}$: $f(x) = g(x)h(x)$, where g and h are monic polynomials over $K\{x_1, \dots, x_n\}$. Then every coefficients of g and h are integral over $k\{x_1, \dots, x_n\}$, therefore they are in $k^{p^{-m}}\{x_1, \dots, x_n\}$ for some integer m , which shows that $\mathfrak{o} \times_k k^{p^{-m}}$ is not an integrity domain and this is a contradiction to that \mathfrak{o} is separably generated over k .

§4. Regular extensions.

Definition. A complete local integrity domain \mathfrak{o} with a basic field k is said to be a regular extension of k if 1) k is algebraically closed in the quotient field of \mathfrak{o} and 2) \mathfrak{o} is separably generated over k .

Theorem 5. *Let \mathfrak{o} be a complete local integrity domain with a basic field k . Then the following three conditions are equivalent to each other:*

- (1) \mathfrak{o} is a regular extension of k .
- (2) \mathfrak{o} is separably generated over k and for any finite separable extension k' of k , $\mathfrak{o} \times_k k'$ is an integrity domain.
- (3) For any finite separable extension k'' of $k^{p^{-1}}$, $\mathfrak{o} \times_k k''$ is an integrity domain.

Proof is easy.

Remark. We see easily that if a complete local integrity domain \mathfrak{o} with a basic field k is a regular extension of k , then the quotient field of \mathfrak{o} is regular extension of k .⁶⁾ The converse is true if $[k:k^n] < \infty$. (See the remark at the end of §2.)

Theorem 6. *Let \mathfrak{o} be a complete local integrity domain with a basic field k . Assume that \mathfrak{o} is a regular extension of k .⁶⁾ Then for any field K containing k , $\mathfrak{o} \times_k K$ is an integrity domain. Further $\mathfrak{o} \times_k K$ is a regular extension of K .*

Proof. That $\mathfrak{o} \times_k K$ is an integrity domain can be proved by a similar way as in the proof of Theorem 4. Let K' be an arbitrary field containing K . Then $(\mathfrak{o} \times_k K) \times_{K'} K' = \mathfrak{o} \times_k K$ is an integrity domain, which shows that $\mathfrak{o} \times_k K$ is a regular extension of K .

§5. An application.

Theorem 7. *Let \mathfrak{o}_1 and \mathfrak{o}_2 be complete local integrity domains with the same basic field k . Assume that \mathfrak{o}_1 is a regular extension of k . Then $\mathfrak{o}_1 \times_k \mathfrak{o}_2$ is an integrity domain. In this case, if \mathfrak{o}_2 is also a regular extension of k , then $\mathfrak{o}_1 \times_k \mathfrak{o}_2$ is a regular extension of k .*

Proof. Let L be the quotient field of \mathfrak{o}_2 . Then $\mathfrak{o}_1 \times_k L$ is an integrity domain. By Lemma 1, $\mathfrak{o}_1 \times_k \mathfrak{o}_2$ is a subring of $\mathfrak{o} \times_k L$, which shows that $\mathfrak{o}_1 \times_k \mathfrak{o}_2$ is an integrity domain. Now we assume that \mathfrak{o}_2 is also a regular extension of k . Let K be an arbitrary field containing k . Then $(\mathfrak{o}_1 \times_k \mathfrak{o}_2) \times_k K = (\mathfrak{o}_1 \times_k K) \times_{K'} (\mathfrak{o}_2 \times_k K)$. Since $\mathfrak{o}_1 \times_k K$ is a regular extension of K and since $\mathfrak{o}_2 \times_k K$ is an integrity domain, we see that $(\mathfrak{o}_1 \times_k \mathfrak{o}_2) \times_k K$ is an integrity domain. This shows that $\mathfrak{o}_1 \times_k \mathfrak{o}_2$ is a regular extension of k .

Corollary 1. Let \mathfrak{o}_1 and \mathfrak{o}_2 be complete local integrity domains with basic fields k_1 and k_2 respectively. Assume that K is a field containing both k_1 and k_2 . Then $\mathfrak{o}_1/k_1 \times_k \mathfrak{o}_2/k_2$ is a regular extension of K if \mathfrak{o}_1 and \mathfrak{o}_2 are regular extensions of k_1 and k_2 respectively.

Corollary 2. Let $x_1, \dots, x_n, y_1, \dots, y_m$ be analytically independent elements over a field k and let \mathfrak{p}_1 and \mathfrak{p}_2 be prime ideals of $\mathfrak{o}_1 = k\{x_1, \dots, x_n\}$ and $\mathfrak{o}_2 = k\{y_1, \dots, y_m\}$ respectively. Then $(\mathfrak{p}_1, \mathfrak{p}_2)k\{x_1, \dots, x_n, y_1, \dots, y_m\}$ is prime if $\mathfrak{o}_1/\mathfrak{p}_1$ is a regular extension

6) We say that a field K is a regular extension of its subfield k if the tensor product $K \otimes_k \bar{k}$ of K and the algebraic closure \bar{k} of k over k is an integrity domain, or equivalently, if K is separably generated over k and if k is algebraically closed in K .

of k . If furthermore, $\mathfrak{o}_2/\mathfrak{p}_2$ is also a regular extension of k , then $k\{x_1, \dots, x_n, y_1, \dots, y_m\}/(\mathfrak{p}_1, \mathfrak{p}_2)k\{x_1, \dots, x_n, y_1, \dots, y_m\}$ is a regular extension of k .

BIBLIOGRAPHY

1. C. Chevalley, Some properties of ideals in rings of power series, Trans. Amer. Math. Soc. 55 (1944), pp. 68-84.
2. C. Chevalley, Intersections of algebraic and algebroid varieties, Trans. Amer. Math. Soc. 57 (1945), pp. 1-85.