Albu, T.
Osaka J. Math.
16 (1979), 65-69

ON A PAPER OF UCHIDA CONCERING SIMPLE FINITE EXTENSIONS OF DEDEKIND DOMAINS

TOMA ALBU

(Received February 14, 1978)
(Revised May 10, 1978)

In a recent paper, K. Uchida [3] has established by specific methods of algebraic number theory the following nice characterization:

Theorem. Let R be a Dedekind domain, K its quotient field, S an integral domain with $R\subseteq S$, and $\alpha\in S$ an integral element over R. Then $R[\alpha]$ is a Dedekind domain if and only if $\varphi\notin M^2$ for every maximal ideal M of $R[X]$, where φ is the minimal polynomial of α over K.

In the present paper, we show that Uchida's result can be generalized to arbitrary Noetherian regular domains. Our proof is very simple and natural, and is based on standard facts about regular rings which can be found for instance in Kaplansky's book [1]. From our generalization it may be derived immediately a global version of a result of Maury [2] concerning simple finite extensions of regular local rings; this result was established by him in a more complicated manner.

1. Terminology and notations

Throughout this paper, R will denote a commutative ring with unit element, $R[X]$ the polynomial ring in X with coefficients in R, dim (R) the Krull dimension of R, Spec (R) the set of all prime ideals of R, and Max (R) the set of all maximal ideals of R.

Let K be a commutative field and U a K-algebra, not necessarily commutative. If $u\in U$ is an algebraic element (i.e. an integral element) over K, then $\{f\in K[X]\mid f(u)=0\}$ is an ideal of $K[X]$, which is generated by a unique monic polynomial with coefficients in K; this polynomial is called the minimal polynomial of u over K and is denoted by Irr (u, K).

We recall that a Noetherian local ring R with maximal ideal M is regular if M can be generated by n elements, where $n=\dim(R)$, and a Noetherian ring R is regular if for each $M\in\text{Max}(R)$, the local ring R_M is regular. The Noetherian regular domains R with $\dim(R)\leqslant 1$ are exactly the Dedekind domains.

2. Three lemmas

The following three simple facts will be used to prove the main result of this paper:

Lemma 1. *Let R be an integrally closed domain, K its quotient field, U a K-algebra (not necessarily commutative), $u \in U$ an integral element over R, and $f = \mathrm{Irr}\,(u, K)$. Then $f \in R[X]$, and the R-algebras $R[X]/fR[X]$ and $R[u]$ are naturally isomorphic.*

Lemma 2. *Let R be a commutative ring, $P \in \mathrm{Spec}\,(R)$, $P \neq 0$, $x \in P$, $x \neq 0$, $T = R/xR$, and $Q = P/xR$. Then the rings T_Q and R_P/xR_P are naturally isomorphic.*

Lemma 3. *Let R be a regular local ring with maximal ideal M. For a non-zero element x of R, the following two statements are equivalent:*

(1) $x \in M \setminus M^2$,

(2) *R/xR is a regular (non-zero) ring.*

Proof. The lemma follows from [4], Theorem 26, p. 303.

3. The main result

Theorem *Let R be a Noetherian regular domain, K its quotient field, U a K-algebra (not necessarily commutative) $u \in U$ an integral element over R and $f = \mathrm{Irr}\,(u, K)$. The following two statements are equivalent:*

(1) *$R[u]$ is a regular ring,*

(2) *$f \notin M^2$ for every $M \in \mathrm{Max}\,(R[X])$.*

Proof. We abbreviate $R[X]$ to S. Since R is regular, so is S. On the other hand, R is integrally closed, so $R[u] \simeq R[X]/fR[X] = S/fS$ by Lemma 1.

(1) implies (2). Suppose that $f \in M^2$ for some $M \in \mathrm{Max}\,(S)$; then $T_N \simeq S_M/fS_M$, where $T = S/fS$ and $N = M/fS$, by Lemma 2. Since $f \in M^2 S_M$, it follows by Lemma 3 that S_M/fS_M is not a regular ring, i.e. T_M is not a regular ring, contradiction.

(2) implies (1). Let $N \in \mathrm{Max}\,(T)$, where $T = S/fS$; then $N = M/fS$ for some $M \in \mathrm{Max}(S)$ with $f \in M$. We have $f \notin M^2 S_M$, for otherwise $f \in M^2 S_M \cap S = M^2$, M^2 being a M-primary ideal of S. By Lemma 3, S_M/fS_M is a regular ring, hence $T_N \simeq S_M/fS_M$ is regular, i.e. T is regular.

Corollary 1. *Let R be a Noetherian regular domain, K its quotient field, L a finite separable field extension of K, R' the integral closure of R in L, $u \in R'$ an element such that $L = K(u)$, and $f = \mathrm{Irr}\,(u, K)$. If $f \notin M^2$ for all $M \in \mathrm{Max}\,(R[X])$, then $R' = R[u]$.*

Proof. By the previous Theorem, $R[u]$ is a regular ring, hence $R[u]$ is integrally closed, and so $R'=R[u]$.

REMARK. The condition $f\notin M^2$ for all $M\in\mathrm{Max}\,(R[X])$ is sufficient for $R'=R[u]$, but is not necessary; for instance let k be a commutative field, $R=k[Y, Z]$, $K=k(Y, Z)$, $L=K(u)$, where u is a root (in an algebraic closure of K) of the polynomial $X^2-YZ\in K[X]$. Then $R[u]$ is the integral closure of R in L, but $f=\mathrm{Irr}\,(u, K)=X^2-YZ\in(X, Y, Z)^2$ and $(X, Y, Z)\in\mathrm{Max}\,(R[X])$.

The next corollary contains Uchida's result [3]:

Corollary 2. *Let R be a Dedekind ring, K its quotient field, L a field extension of K, $u\in L$ an integral element over R, and $f=\mathrm{Irr}\,(u, K)$. The following statements are equivalent:*

(1) *$R[u]$ is a regular ring,*
(2) *$R[u]$ is a Dedekind ring,*
(3) *$R[u]$ is integrally closed,*
(4) *The integral closure of R in $K(u)$ is $R[u]$,*
(5) *$f\notin M^2$ for all $M\in\mathrm{Max}\,(R[X])$.*

Now we shall give an equivalent form of condition (2) of the previous Theorem, which is sometimes more adequate for applications. The following simple result, which is proved in [3], will be used:

Lemma 4 [3]. *Let R be a commutative ring, and $N\in\mathrm{Max}\,(R[X])$. If N contains a monic polynomial $g\in R[X]$, then N is of the form*

$$N = MR[X]+fR[X]\,,$$

where $M\in\mathrm{Max}\,(R)$ and $f\in R[X]$ is a monic polynomial which is irreducible modulo M.

If R is an arbitrary commutative ring, for each $h\in R[X]$ and $M\in\mathrm{Max}\,(R)$ we denote throughout the remainder of this paper by $\bar{h}_M\in(R/M)[X]$ (or sometimes, more simple by $\bar{h}$, if no confusion can occur) the polynomial obtained from h by reducing the coefficients of h modulo M.

Proposition. *Let R be a commutative ring, and $f\in R[X]$ a monic polynomial. For each $M\in\mathrm{Max}\,(R)$, let*

$$\bar{f}_M = \varphi_{M1}^{e_{M1}}\cdot\varphi_{M2}^{e_{M2}}\cdots\varphi_{Mk_M}^{e_{Mk_M}}$$

be the expression of $\bar{f}_M$ as a product of monic irreducible, mutually distinct polynomials $\varphi_{Mi}\in(R/M)[X]$. For each $M\in\mathrm{Max}\,(R)$ and $1\leqslant i\leqslant k_M$, let $g_{Mi}\in R[X]$ be a monic polynomial with $(\overline{g_{Mi}})_M=\varphi_{Mi}$. Then the following two statements are equivalent:

(1) *$f\notin N^2$ for each $N\in\mathrm{Max}\,(R[X])$,*

(2) *For each $M \in \mathrm{Max}(R)$ and each $1 \leqslant i \leqslant k_M$ with $e_{Mi} \geqslant 2$, the remainder of the euclidean division of f by g_{Mi} has not all its coefficients in M^2.*

Proof. (1) implies (2). Let $M \in \mathrm{Max}(R)$, and $1 \leqslant i \leqslant k_M$ with $e_{Mi} \geqslant 2$. We denote for brevity $g_{Mi}=g$, $e_{Mi}=e$ and $\bar{f}_M=\bar{f}$. Assume that,

$$f = gq+r ,$$

where q, $r \in R[X]$, and $\deg(r)<\deg(g)$ with $r \in M^2R[X]$. By reduction modulo M, we obtain $\bar{f}=\bar{g}\bar{q}+\bar{r}=\bar{g}\bar{q}=\bar{g}^e\bar{h}$, where $h=\prod_{j \neq i} g_{Mj}^{e_{Mj}}$. Hence $g^e h-gq \in MR[X]$, so $(q-gs)g \in MR[X]$, where $s=g^{e-2}h$. Since g is a monic polynomial and $MR[X] \in \mathrm{Spec}\,(R[X])$, it follows $q-gs \in MR[X]$. Hence $q \in MR[X]+gR[X]$, that is

$$f = gq+r \in g^2R[X]+gMR[X]+M^2R[X] = (MR[X]+gR[X])^2 ,$$

and $MR[X]+gR[X] \in \mathrm{Max}(R[X])$, contradiction.

(2) implies (1). Suppose that $f \in N^2$ for some $N \in \mathrm{Max}(R[X])$. By Lemma 4, $N=MR[X]+gR[X]$ for some $M \in \mathrm{Max}(R)$ and $g \in R[X]$ irreducible modulo M, hence $f \in M^2R[X]+gMR[X]+g^2R[X]$. By reduction modulo M, we have $\bar{f}=\bar{g}^2\bar{t}$ for some $t \in R[X]$, hence $\bar{g}=\varphi_{Mi}$ for some i with $1 \leqslant i \leqslant k_M$; it follows that $g-g_{Mi} \in MR[X]$, and so, we can suppose that $g=g_{Mi}$. From $f \in M^2R[X]+gMR[X]+g^2R[X]$, we have $f=gq+r$, for some $q \in R[X]$ and $r \in M^2R[X]$. If $r \neq 0$ and $\deg(r) \geqslant \deg(g)$, we can write $r=gq_1+r_1$, with q_1, $r_1 \in R[X]$, and $r_1=0$ or $\deg(r_1)<\deg(g)$. Let

$$g = X^m+a_{m-1}X^{m-1}+\cdots+a_0$$
$$q_1 = b_kX^k+b_{k-1}X^{k-1}+\cdots+b_0$$

Then

$$r = gq_1+r_1 = b_kX^k \cdot g+(b_{k-1}X^{k-1}+\cdots+b_0)g+r_1 \in M^2R[X] .$$

But $b_k \in M^2$, hence $(b_{k-1}X^{k-1}+\cdots+b_0)g+r_1 \in M^2R[X]$, so $b_{k-1} \in M^2$, etc. Therefore $r_1 \in M^2R[X]$, and then, we have

$$f = (q+q_1)g+r_1$$

with $r_1=0$ or $\deg(r_1)<\deg(r)$, and also $r_1 \in M^2R[X]$, contradiction.

Corollary 3 (Maury [2]). *Let R be a regular local ring with maximal ideal M, K its quotient field, U a K-algebra (not necessarily commutative), $u \in U$ an integral element over R and $f=\mathrm{Irr}\,(u, K)$. The following two statements are equivalent:*

(1) *$R[u]$ is a regular local ring,*

(2) *The reduction $\bar{f}$ of f modulo M has the form $\bar{f}=\varphi^e$ with $\varphi \in (R/M)[X]$ a monic irreducible polynomial, and if $e \geqslant 2$, the remainder of the euclidean division of f by g has not all its coefficients in M^2, $g \in R[X]$ being a monic polynomial with*

$\bar{g}=\varphi$.

Proof. The condition $\bar{f}=\varphi^e$ with $\varphi\in(R/M)[X]$ irreducible is equivalent by [2], Theorem, p. 35, with the condition that $R[u]$ is a local ring.

Corollary 4. *Let R be a Dedekind domain, K its quotient field, L a finite separable field extension of K, R' the integral closure of R in L, $u\in R'$ a primitive element of the extension $L\supseteq K$ (i.e. $L=K(u)$), and $f=\mathrm{Irr}(u, K)$. Let $\delta(f)$ be the discriminant of f and $M_1, M_2, \cdots, M_r$ the distinct non zero prime divisors of $\delta(f)$ in R (possibly $r=0$). For each $1\leqslant i\leqslant r$, let*

$$\bar{f}_{M_i} = \varphi_{i1}^{e_{i1}}\cdot\varphi_{i2}^{e_{i2}}\cdots\varphi_{ik_i}^{e_{ik_i}}$$

be the expression of $\bar{f}_{M_i}$ as a product of monic irreducible, mutually distinct polynomials $\varphi_{ij}\in(R/M_i)[X]$. For each $1\leqslant i\leqslant r$ and $1\leqslant j\leqslant k_i$, let $g_{ij}\in R[X]$ be a monic polynomial with $\overline{(g_{ij})}_{M_i}=\varphi_{ij}$. The following two statements are equivalent:

(1) $R'=R[u]$,

(2) *For each $1\leqslant i\leqslant r$ and $1\leqslant j\leqslant k_i$ uith $e_{ij}\geqslant 2$, the remainder of the euclidean division of f by g_{ij} has not all its coefficients in M_i^2.*

Proof. It suffices to prove only (2) implies (1). If $f\in N^2$ for some $N\in\mathrm{Max}(R[X])$ then we obtain in the same way as in the proof of the previous Proposition that $\bar{f}_M=\bar{g}^2\bar{h}$, for some $M\in\mathrm{Max}(R)$, that is $\bar{f}_M$ has multiple roots. Since the discriminant $\delta(\bar{f}_M)=0$ is the residue class of $\delta(f)$ modulo M, we have $\delta(f)\equiv 0 \pmod{M}$ and therefore $M=M_i$ for some $1\leqslant i\leqslant r$ and $\bar{g}=\varphi_{ij}$ for some $1\leqslant j\leqslant k_i$; by the proof of the previous Proposition, this is a contradiction.

The author is indebted to the referee for some useful suggestions which led to the present version of this paper.

FACULTATEA DE MATEMATICA, BUCHAREST

Bibliography

[1] I. Kaplansky: Commutative rings, Chicago and London, The University of Chicago Press, 1974.

[2] G. Maury: *La condition "integralement clos" dans quelques structures algebriques,* Ann. Sci. Ecole Norm. Sup. **78** (1961), 31–100.

[3] K. Uchida: *When is $Z[\alpha]$ the ring of the integers?,* Osaka J. Math. **14** (1977), 155–157.

[4] O. Zariski and P. Samuel: Commutative algebra, vol. II, Van Nostrand-Reinhold, Princeton, New Jersey, 1960.