PACIFIC JOURNAL OF MATHEMATICS
Vol. 35, No. 2, 1970

GENERIC SPLITTING ALGEBRAS FOR PIC

GERALD GARFINKEL

Our purpose is to develop a splitting theory for the functor Pic. For each rank one projective module P, we exhibit a generic splitting algebra $T_\infty(P/R)$. Whenever n is a multiple of the order of P in Pic(R), it has a splitting algebra which is a rank n projective module. We then show the relationship of the latter algebra to the usual splitting ring of an ideal in a Dedekind domain.

Throughout this paper all rings and algebras are commutative and associative and have identities. The symbol "R" will always denote a fixed but arbitrary ring and all modules and algebras are over R. An unadorned tensor product sign "$\otimes$" is to be interpreted as "$\otimes_R$". If M is an R-module we let M^n be $M \otimes \cdots \otimes M$ (n times), M^* be Hom (M, R) and $e: M \otimes M^* \longrightarrow R$ be the evaluation map (i.e., $e(x \otimes f) = f(x)$ for all $x \in M$ and $f \in M^*$).

An R-module P is a rank n projective if it is finitely generated and if for each prime ideal $\mathfrak{m}$ of R, $P_\mathfrak{m}$ is a free $R_\mathfrak{m}$ module of rank n. If P is a rank one projective, so is P^* and $e: P \otimes P^* \longrightarrow R$ is an isomorphism. Thus Pic (R), the set of isomorphism classes (P) of rank one projectives P, is a group under the multiplication rule: $(P)(Q) = (P \otimes Q)$. If P is a rank one projective we write P^{-n} for P^{*n} ($\cong P^{n*}$). An R-algebra S splits (P) in Pic (R) if $P \otimes S \cong S$ as S-modules. See [3] for more details.

A final note on general notation: If $\{A_i\}$ is a collection of R-modules, by $\sum \oplus A_i U^i$ is meant the R-module whose elements are all finite sums $\sum a_i U^i$ where $a_i \in A_i$. Addition and scalar multiplication are defined as for polynomials in the indeterminant U. Sometimes the U may be in lower case and it may or may not have a subscript. Clearly the notation is such that $\sum \oplus RU^i$ is the module of ordinary polynomials over R in the indeterminant U.

In § 2 we define for each rank one projective P an algebra $T_\infty(P/R)$ which by Theorem 1 is a generic splitting algebra for the module Q in the same sense that $F_m(A)$ is a generic splitting algebra for the central simple algebra A in the works of Amitsur [1] and Roquette [8]. If $T'(P/R)$ is the tensor algebra of P, Theorem 2 characterizes the splitting algebras of P as those commutative algebras S such that $S \otimes T'(P/R)$ is isomorphic to $S[X]$.

In § 3 it is shown that for every isomorphism $f: P^n \longrightarrow R$, P has a splitting algebra $T_n(P/R, f)$ which is a rank n projective module. This algebra is separable if and only if n is a unit of R. We close

the section with some information about when two of the generic or finite splitting algebras are isomorphic (as graded algebras).

We define Picard ideals as those which are rank one projective modules. Our last section is concerned with the case in which I is a Picard ideal with $I^n = Rw$ and $T = T_n(I/R, w^{-1})$. We give some information about when T is a domain and in Theorem 4 show that if R is Dedekind and n is both the order of (I) in Pic (R) and is a unit of R, then T is the usual splitting algebra for I. We give two examples illustrating what may happen to T when R is Dedekind but n fails to satisfy the hypotheses of Theorem 4.

2. **Generic splitting algebras.** Throughout this section P is a rank one projective. Before we can define the generic splitting algebra we need the following rather technical lemma.

LEMMA 1. (i) *Suppose α is any permutation of the first n integers and let $\theta: P^n \longrightarrow P^n$ be the unique homomorphism with $\theta(x_1 \otimes \cdots \otimes x_n) = x_{\alpha 1} \otimes \cdots \otimes x_{\alpha n}$. Then θ is the identity map.*

(ii) *If m and n are any two integers, the various maps from $P^n \otimes P^m$ to P^{n+m} induced by interchanging factors and applying the evaluation map e and the identity map are all the same. We denote this map by $t_{n,m}: P^n \otimes P^m \longrightarrow P^{n+m}$.*

(iii) *If $\sigma: P^n \otimes P^m \longrightarrow P^m \otimes P^n$ is the "switch" map, then $t_{m,n} \cdot \sigma = t_{n,m}$.*

(iv) *If q is also an integer, the following diagram commutes:*

$$\begin{array}{ccc} P^n \otimes P^m \otimes P^q & \xrightarrow{t_{n,m} \otimes 1} & P^{n+m} \otimes P^q \\ \downarrow 1 \otimes t_{m,q} & & \downarrow t_{n+m,q} \\ P^n \otimes P^{m+q} & \xrightarrow{t_{n,m+q}} & P^{n+m+q} . \end{array}$$

Proof. For (i) we need only show that for each maximal ideal $\mathfrak{m}$, the map $\theta_m: P^n_{\mathfrak{m}} \longrightarrow P^n_{\mathfrak{m}}$ is the identity. Since $R_{\mathfrak{m}}$ is local, $P_{\mathfrak{m}} = R_{\mathfrak{m}}x$ for some x in $P_{\mathfrak{m}}$. Thus $P^n_{\mathfrak{m}} = R_{\mathfrak{m}}y$ where $y = x \otimes \cdots \otimes x$ and clearly $\theta_{\mathfrak{m}}(y) = y$. The proofs of the other parts of the lemma are clear from the statement and proof of (i).

We can now make the following definition.

DEFINITION. Suppose (P) is in Pic (R), let $T_\infty(P/R) = \sum_{i=-\infty}^{+\infty} \oplus P^i U^i$ as an R-module, and define a multiplication by:

$$(\sum a_i U^i) \cdot (\sum b_j U^j) = \sum_{i,j} t_{i,j}(a_i \otimes b_j) U^{i+j} .$$

Lemma 1 shows that $T_\infty(P/R)$ is a commutative, associative R-algebra. Let $T'(P/R) = \sum_{i=0}^{\infty} P^i U^i$. Clearly $T'(P/R)$ is an R-subalgebra of $T_\infty(P/R)$ which is isomorphic to the tensor algebra of the R-module P.

REMARK. It is clear that up to isomorphism $T_\infty(P/R)$ depends only on the isomorphism class of the R-module P and if S is any commutative R-algebra, then $S \otimes T_\infty(P/R) \cong T_\infty(S \otimes P/S)$. Similar facts hold for T'. In fact $T_\infty(P/R)$ and $T'(P/R)$ are both natural in the following sense. For any commutative ring R, let $PCA(R)$ be the set of isomorphism classes of commutative R-algebras which are projective and countably generated as R-modules. If $\mathscr{K}$ is the category of commutative rings with identity and $\mathscr{S}$ the category of Sets, then Pic and PCA can be considered functors from $\mathscr{K}$ to $\mathscr{S}$ and T and T' then induce natural transformations from Pic to PCA.

PROPOSITION 1. *If S is any commutative R-algebra splitting P, then $S \otimes T_\infty(P/R) \cong S[\boldsymbol{Z}]$ (the group ring over S of the additive group of integers $\boldsymbol{Z}$) $\cong S[X, X^{-1}]$ the polynomial ring over S in the indeterminants X and X^{-1}). Also $S \otimes T'(P/R) \cong S[X]$.*

Proof. By the above remark,

$$S \otimes T_\infty(P/R) \cong T_\infty(S/S) = \sum_{i=-\infty}^{\infty} SU^i .$$

Multiplication in the latter is defined by

$$(\sum a_i U^i)(\sum b_j U^j) = \sum a_i b_j U^{i+j} ,$$

and thus it is clearly isomorphic to $S[\boldsymbol{Z}]$ and to $S[X, X^{-1}]$. A similar calculation shows $S \otimes T'(P/R) \cong S[X]$.

PROPOSITION 2. *$T = T_\infty(P/R)$ splits P; in fact if we let $\theta: T \otimes P \to T$ be the map induced by the maps*

$$t_{n,1}: P^n U^n \otimes P \longrightarrow P^{n+1} U^{n+1} ,$$

then θ is a T-isomorphism.

Proof. Clear.

In fact not only does T split P, but T is a "generic" splitting algebra for P in the sense of the following theorem.

THEOREM 1. *Let (P) be in* Pic (R) *and $T = T_\infty(P/R)$. Then for*

any commutative R-algebra S, the following are equivalent:

(i) *S splits P,*

(ii) $S \otimes T \cong S[Z] \cong S[X, X^{-1}]$ *as S-algebras,*

(iii) *there is an R-algebra homomorphism from T to S.*

Proof. (i) $\Rightarrow$ (ii) by Proposition 1. If (ii) holds, then the composition $T \longrightarrow S \otimes T \cong S[Z] \longrightarrow S$ is an R-algebra map where the last factor in the composition is induced by the group homomorphism from Z to the one element group. Thus (ii) $\Rightarrow$ (iii). If (iii) holds we can view S as a T-algebra. Then since by Proposition 2, T splits P, we have

$$S \otimes P \cong S \otimes_T T \otimes P \cong S \otimes_T T \cong S$$

as S-modules. Hence (iii) $\Rightarrow$ (i).

Using the map θ of Proposition 2 it is easy to see that $P' = \sum_{i=1}^{\infty} P^i U^i$ is a T' ideal isomorphic to $T' \otimes P$. Thus T' splits P if and only if P' is T'-free. The following theorem shows that T' does not split P (except when P is itself trivial) and that moreover the "splitting" algebras for P, T' and P' are the same.

THEOREM 2. *For each commutative algebra S the following are equivalent:*

(i) *S splits P,*

(ii) $S \otimes T'(P/R) \cong S[X]$ *as S-algebras,*

(iii) $S \otimes P'$ *is a free* $S \otimes T'(P/R)$ *module.*

Proof. By the naturality of $T' = T'(P/R)$ we can assume $S = R$. (i) $\Rightarrow$ (ii): By Proposition 1. (ii) $\Rightarrow$ (iii): Let $\varphi: T' \to R$ be defined by $\varphi(\sum a_i U^i) = a_0$. Clearly φ is an R-algebra map with kernel P'. Suppose $\alpha: R[X] \longrightarrow T'$ is any R-isomorphism. Then since the kernel of $\varphi\alpha$ is generated by $y = X - \varphi\alpha X$, it is easy to see that P' is generated by αy and thus is a free T' module. (iii) $\Rightarrow$ (i): If inc: $R \longrightarrow T'$ is the inclusion map, then since φ inc is the identity map of R, Pic (inc) is a split monomorphism. Since (P') is Pic (inc) of (P), we see that P' is T'-free if and only if P is R-free.

3. Finite splitting algebras. Throughout this section, P is a rank one projective module.

DEFINITION. If $f: P^n \longrightarrow R$ is an isomorphism, we let $T_n(P/R, f)$ be the R-module $\sum_{i=0}^{n-1} \oplus P^i u_f^i$. We define a multiplication on $T_n(P/R, f)$ by the formula:

$$(a\,u_f^i)(b\,u_f^j) = \begin{cases} ab\,u_f^{i+j} & \text{when } i+j < n \\ fab\,u_f^{i+j-n} & \text{when } i+j \geqq n \end{cases}$$

and the distributive law: $(\sum_i a_i u_f^i)(\sum_j b^j u_f^j) = \sum_{i,j}(a_i u_f^i)(b_j u_f^j)$. We will often write "$T_n$" for "$T_n(P/R, f)$" and "$u^i$" for "$u_f^i$".

Note that an isomorphism $f\colon P^n \longrightarrow R$ is an element of $P^{n*} = P^{-n}$. Suppose $f(w) = 1$. If for each $k \geqq 0$, we let w^{-k} be the element f^k in P^{-nk}, then for each integer k, P^{nk} is the free R-module with generator w^k. Thus each element Y of $T = T_\infty(P/R)$ is uniquely expressible as

$$(*) \qquad Y = \sum_{j=0}^{n-1} \sum_{k=-\infty}^{+\infty} a_{k,j} w^k U^{kn+j} \text{ with } a_{k,j} \in P^j .$$

PROPOSITION 3. *Suppose f, w, T and T_n are as above. Then there is an R-module map $\pi\colon T \longrightarrow T_n$ such that*

(i) *π is an R-module epimorphism*

(ii) *π is multiplicative*

(iii) *kernel $\pi = T(wU^n - 1) = T(fU^{-n} - 1)$*

(iv) *if π' is π restricted to $T' = T'(P/R)$ then π' is an R-module epimorphism with kernel $T'(wU^n - 1)$.*

In particular if $I = T(wU^n - 1)$ and $I' = T'(wU^n - 1)$, then T_n is an R-algebra which is isomorphic to T/I and to T'/I'.

Proof. If Y is a nonzero element of T of the form (*), we define $\pi(Y) = \sum_{j,k} a_{k,j} u_f^j$. From this definition it is clear that π is a well defined R-module epimorphism. The fact that when $j + j' \geqq n$ then $a_{k,j}a_{k',j'} = f(a_{k,j}a_{k',j'})w$, shows that π is multiplicative. Thus conditions (i) and (ii) hold.

Now let $I = T(wU^n - 1)$. Since $-fU^{-n}(wU^n - 1) = fU^{-n} - 1$ and $(-wU^n)(fU^{-n} - 1) = wU^n - 1$, we see that $I = T(fU^{-n} - 1)$ also. Since $\pi(wU^n - 1) = 0$, it is clear that I is contained in kernel π. Now suppose Y is an element of form (*). Then it is easy to see that $\pi(Y) = 0$ if and only if for each $0 \leqq j < n$, we have $\sum_k a_{k,j} = 0$. Thus if $\pi(Y) = 0$, then $Y = \sum_{j,k} a_{k,j} U^j (w^k U^{nk} - 1)$. However, if $k > 0$, then $(wU^n)^k - 1 = (wU^n - 1)(1 + wU^n + \cdots + (wU^n)^{k-1})$ and hence is in I. A similar equation shows that if $k < 0$, then

$$(wU^n)^k - 1 = (fU^{-n})^{-k} - 1$$

is also in I. Hence condition (iii) has been verified.

Clearly π' is an epimorphism with kernel $I \cap T'$. To prove (iv) we must show that $I \cap T'$ is contained in $T'(wU^n - 1)$. An element

Y of $I \cap T'$ is of the form $Y = \sum_M^N a_i U^i(U^0 - wU^n)$ where $M \leqq N$ and each $a_i \in P^i$. However, since $a_M U^M$ is the homogeneous component of Y of lowest degree and Y is in T', we see that $M \geqq 0$ and hence Y is in $T'(wU^n - 1)$.

The last statement in the proposition is clear.

NOTATION. If M is any R-module, let $E^0(M/R) = R$, and if $n > 0$ let $E^n(M/R) = M \wedge \cdots \wedge M$ (the n-th exterior product of M with itself).

LEMMA 2. *Suppose M is any R-module, (P) is in* Pic (R) *and $n > 0$ is an integer. Then there is an R-module isomorphism*

$$\theta\colon P^n \otimes E^n(M/R) \longrightarrow E^n(P \otimes M/R)$$

such that if $a_i \in P$, $x_i \in M$ for $i \leqq n$,

$$\theta((a_1 \otimes \cdots \otimes a_n) \otimes (x_1 \wedge \cdots \wedge x_n)) = (a_1 \otimes x_1) \wedge \cdots \wedge (a_n \otimes x_n) .$$

Proof. Let $M' = M \times \cdots \times M$ (cartesian product of M with itself n times) and $P' = P \times \cdots \times P$ and define

$$\theta\colon P' \times M' \longrightarrow E^n(P \otimes M/R)$$

by $\theta'(a, x) = (a_1 \otimes x_1) \wedge \cdots \wedge (a_n \otimes x_n)$ when $a = (a_1, \cdots, a_n) \in P'$ and $x = (x_1, \cdots, x_n) \in M'$. Clearly θ' is multilinear in the variables $a_1, \cdots, x_n$. For each maximal ideal $\mathfrak{m}$ of R, let $f_{\mathfrak{m}}$ be the map

$$E^n(P \otimes M/R) \longrightarrow R_{\mathfrak{m}} \otimes E^n(P \otimes M/R) \longrightarrow E^n(P_{\mathfrak{m}} \otimes M_{\mathfrak{m}}/R_{\mathfrak{m}})$$

induced by localization. It is easy to check that each $f_{\mathfrak{m}}\theta'$ is alternating in the x_i's and thus θ' is alternating in those variables. Hence there is a well defined homomorphism θ satisfying the given property. Since each $\theta_{\mathfrak{m}}$ is an isomorphism, θ itself is an isomorphism.

THEOREM 3. *Suppose (P) is in* Pic (R) *and $n > 0$. Then the following are equivalent:*

(i) $(P)^n = 1$,

(ii) *there is a commutative R-algebra T which is a rank n projective R-module with $T \otimes P \cong T$ as T-modules,*

(iii) *there is a rank n projective R-module M with $M \otimes P \cong M$.*

Proof. (A slightly weaker form of (i) $\Leftrightarrow$ (iii) is shown by Bass [2].)

(i) $\Rightarrow$ (ii): By Propositions 2 and 3, we can take $T = T_n(P/R, f)$ where $f\colon P^n \longrightarrow R$ is any isomorphism.

(ii) $\Rightarrow$ (iii): Let $M = T$ and forget the T-structure.

(iii) $\Rightarrow$ (i): By [3, p. 142], $E^n(M/R) = E^n(P \otimes M/R) = N$ is a rank one projective R-module. However, by Lemma 2, $P^n \otimes N \cong N$. Thus $(P)^n(N) = (N)$ in Pic (R) and since Pic (R) is a group, $(P)^n = 1$.

PROPOSITION 4. *Suppose* (P) *is in* Pic (R). *Then* $T'(P/R)$ *and* $T_\infty(P/R)$ *are not separable* R*-algebras. If* $f: p^n \longrightarrow R$ *is an isomorphism, then* $T_n(P/R, f)$ *is a separable* R*-algebra if and only if* n *is a unit in* R.

Proof. The first statement follows from Villameyer's Theorem [7] which states that a separable, projective algebra is also finitely generated as an R-module and clearly T' and T_∞ are not finitely generated. By Bass [2; pp. 94, 96] $T_n = T_n(P/R, f)$ is separable if and only if for all maximal ideals $\mathfrak{m}$ of R, $(R/\mathfrak{m}) \otimes T_n$ is a separable $R/\mathfrak{m}$-algebra. By the naturality of T_∞ and Proposition 3, it is clear that if $\bar{R} = R/\mathfrak{m}$, then $\bar{R} \otimes T_n = \bar{R}[X]/(1 - wX^n)$ for some element w in $\bar{R}$. Thus $\bar{R} \otimes T_n$ is separable if and only if $X^n - w^{-1}$ is a separable polynomial in $\bar{R}[X]$; however this is true if and only if n is a unit (i.e., nonzero) in $\bar{R}$. But clearly n is nonzero in each $R/\mathfrak{m}$ if and only if n is not in any maximal ideal $\mathfrak{m}$; which is to say that n is a unit in R.

We consider an isomorphism between two graded algebras A and B to be graded (and write $A \cong_g B$) if it preserves homogeneous components. Noting that $T_\infty(P/R)$, $T'(P/R)$ and $T_n(P/R, f)$ are graded algebras with grading respectively $\boldsymbol{Z}$, $\boldsymbol{Z}^+$ and $\boldsymbol{Z}/n\boldsymbol{Z}$, we can now state:

PROPOSITION 5. *Suppose* (P) *and* (Q) *are in* Pic (R).

(i) $T'(Q/R) \cong_g T'(P/R)$ *if and only if* $(Q) = (P)$.

(ii) *The mapping* $xU^m \longrightarrow xU^{-m}$ *defines a graded isomorphism* $h: T_\infty(P^*/R) \longrightarrow T_\infty(P/R)$.

(iii) $T_\infty(Q/R) \cong_g T_\infty(P/R)$ *if and only if* $(Q) = (P)^e$ *where* $e = \pm 1$.

(iv) *There is a graded isomorphism* $h: T_m(Q/R, g) \longrightarrow T_n(P/R, f)$ *if and only if* $m = n$ *and there are an integer* $k > 0$ *and an isomorphism* $h': Q \longrightarrow P^k$ *with* $(k, m) = 1$ *and* $g = f^k h'^n$.

Proof. (i), (ii) and (iii) are clear, so we only give the proof of (iv).

($\Leftarrow$): The correspondence $xU^r \longrightarrow h'^r(x)U^{kr}$ induces an algebra map $h'': T'(Q/R) \longrightarrow T'(P/R)$. Since $h''(1 - g^{-1}U^n) = 1 - (f^{-1}U^n)^k$, an element of $T'(P/R)(1 - f^{-1}U^n)$, by Proposition 3 we see that h'' induces a graded algebra homomorphism $h: T_n(Q/R, g) \longrightarrow T_n(P/R, f)$. Since (k, n) = 1, h is onto and thus is an isomorphism since its domain

and range are rank n projectives. Clearly h is graded.

($\Rightarrow$): Clearly $m = n$ and since h is a graded isomorphism there is an integer k and a map $h'\colon Q \longrightarrow P^k$ with $h(xU) = h'(x)U^k$. Thus $h((QU)^r) \subseteq (PU)^{r'}$ where $kr \equiv r' (\mathrm{mod}\, n)$. Since h is onto, the equation $kr \equiv 1$ is solvable and thus $(k, n) = 1$. Also $kr \equiv k$ if and only if $r \equiv 1$ and so $h(QU) = P^kU^k$. Therefore h' is onto and hence is an isomorphism.

4. **Picard ideals.** In this section we are interested in the case where the rank one projective module is actually an ideal of R-which we call a Picard ideal. In many rings (e.g., domains and Noetherian rings) this is always the case—i.e., $\mathrm{Pic}\,(R) = C(R)$—the isomorphism classes of Picard ideals. See [3] or [9]. However by an exercise in Bourbaki [3, p. 179] it can be seen that $C(R)$ is not functoral, is not always a group and may be a proper subset of $\mathrm{Pic}\,(R)$. Since $C(R)$ is not well behaved, one often gets information about it by studying the functor $\mathrm{Pic}\,(R)$.

We introduce the following special notation for this section: "I" will always denote an ideal of R and "K" is always the total quotient ring of R. I^n is the ideal product of I with itself n times and $I^{(n)} = I \otimes \cdots \otimes I$. It is easy to see that if I is flat then $I^n \cong I^{(n)}$. Finally we let $I^{-1} = \{x \in K\colon xI \subseteq R\}$.

LEMMA 3. *I is a Picard ideal with finite order in* $\mathrm{Pic}(R)$ *if and only if some power of I is generated by a non zero divisor. If either condition holds then the map $\theta\colon I^{-1} \longrightarrow I^*$ defined by $\theta(x)(a) = xa$ is an isomorphism.*

Proof. The necessity condition is clear. Now suppose $I^n = Rw$ where w is a non zero divisor. First note that $\varphi\colon I^* \longrightarrow I^{-1}$, defined by $\varphi(g) = g(w)w^{-1}$, is an inverse to θ; which is thus an isomorphism. If $w = \sum a_ib_i$ with $a_i \in I$ and $b_i \in I^{n-1}$, it is easy to see that $\{a_i, \theta(b_i)\}$ is a finite projective basis for I in the sense of [4, p. 132] and thus I is finitely generated and projective as a module. Hence I^* is flat and so $I \otimes I^* \cong I \cdot I^* \cong II^{-1}$. Since $I \cdot I^{n-1}w^{-1} = R$, we see that $I \cdot I^{-1} = R$. Then we can conclude that I is rank one from the fact that $I \otimes I^* \cong R$. Clearly $(I)^n = 1$.

PROPOSITION 6. *Let I be an ideal of R with $I^n = Rw$ for some non zero divisor w and let K be the total quotient ring of R.*

(i) *I is a Picard ideal and if we identify w and w^{-1} with multiplication by that element in K, then $w^{-1}\colon I^n \longrightarrow R$ and $w\colon I^{-n} \longrightarrow R$ are isomorphisms.*

(ii) *The inclusions $R \subseteq I^{-1} \subseteq K$ induce inclusion maps*

$$R[U]/(U^n - w) \longrightarrow T_n(I^{-1}/R, w) \longrightarrow K[U]/(U^n - w) .$$

(iii) *If R is an integral domain, then $T_n(I/R, w^{-1})$ is an integral domain if and only if $U^n - w$ is an irreducible polynomial over K.*

Proof. (i) Clear from Lemma 3.

(ii) Clearly the inclusions $R \subseteqq I^{-1} \subseteqq K$ induce inclusions

$$T'(R/R) \subseteqq T'(I^{-1}/R) \subseteqq T'(K/K) .$$

Thus if we define

$$J_0 = T'(K/K)(w^{-1}U^n - 1)$$
$$J_1 = T'(I^{-1}/R) \cap J_0$$
$$J_2 = T'(R/R) \cap J_0$$

then there is a sequence of inclusions:

$$R[U]/J_2 \longrightarrow T'(I^{-1}/R)/J_1 \longrightarrow K[U]/(U^n - w) .$$

Thus to prove (ii) we need only show that

$$J_1 = J_1' = T'(I^{-1}/R)(w^{-1}U^n - 1)$$

and $J_2 = J_2' = R[U](U^n - w)$. Also it is clear that $J_1' \subseteqq J_1$ and since $U^n - w = w(w^{-1}U^n - 1) \in J_2$, $J_2' \subseteqq J_2$. Thus we need only show the opposite inclusions.

Suppose $y = (\sum y_i U^i)(w^{-1}U^n - 1) = \sum a_i U^i$ is in J_0. Note that $y_i = w(a_{i+n} + y_{i+n})$. Now assume y is in J_1, i.e., each $a_i \in I^{-i}$. If y is not in J_1', let N be the largest integer with y_N not in I^{-N}. Then $y_N = w(a_{N+n} + y_{N+n}) \in I^n \cdot I^{-N-n} = I^{-N}$, a contradiction. Thus $J_1 = J_1'$. Now assume y is in J_2. We claim that for each i, y_i is in Rw. If not, letting N be a maximal counter-example, the above expression for y_N show it is in $w(R + Rw) = Rw$, a contradiction. Thus

$$y = w(\sum w^{-1}y_i U^i)w^{-1}(U^n - w)$$

is an element of J_2' and so $J_2' = J_2$.

(iii) It is easy to see that $K' = K[U]/(U^n - w)$ is the total quotient ring of $R[U]/(U^n - w)$ and thus K' is also the total quotient ring of $T_n' = T_n(I^{-1}/R, w)$. By Proposition 5 we see that T_n' is isomorphic to $T_n = T_n(I/R, w^{-1})$. Thus T_n is a domain if and only if K' is a field and it is well known that K' is a field if and only if $U^n - w$ is irreducible.

LEMMA 4. *Suppose n_1 and n_2 are relatively prime positive integers and w is an element of the field K. Then $X^{n_1 n_2} - w$ is*

irreducible if and only if both $x^{n_1} - w$ *and* $x^{n_2} - w$ *are irreducible.*

Proof. Let $n = n_1 n_2$. Clearly if $x^n - w$ is irreducible so is each $x^{n_i} - w$. Now suppose each $x^{n_i} - w$ is irreducible. Thus for each i, there is a field $L_i = K[u_i]$ where $x^{n_i} - w$ is the minimal polynomial of u_i. Since $(n_1, n_2) = 1$, it is easy to see that any field compositum $L = L_1 L_2$ is unique up to isomorphism and is of dimension n over K. Suppose s_1 and s_2 are integers with $n_1 s_2 + n_2 s_1 = 1$. Let v be the element $u_1^{s_1} \cdot u_2^{s_2}$ in L. A simple calculation then shows that $v^{n_1} = u_2$ and $v^{n_2} = u_1$. Thus v generates the field L of dimension n and satisfies the polynomial $v^n - w$. Hence $x^n - w$ is the minimal polynomial of v and so is irreducible.

THEOREM 4. *Suppose* R *is a Dedekind domain with quotient field* K *and* I *is an ideal of* R *with* $I^n = Rw$, *and* n *is the order of* (I) *in* Pic (R). *Then* $T = T_n(I/R, w^{-1})$ *is a domain. If* n *is also a unit of* R, *then* T *is a Dedekind domain and is isomorphic to the integral closure of* R *in* $K[X]/(X^n - w)$.

Proof. We first prove the theorem in the case where n is non-zero in R. By Proposition 6, we need to show $f(X) = X^n - w$ is an irreducible K polynomial. Let $g(X)$ be any irreducible factor of $f(X)$ of degree say d. We must show $d = n$.

Let S be the integral closure of R in $L = K[X]/(g(X))$. Since n is a unit of K, $f(X)$ is a separable polynomial and hence so is $g(X)$. Since L is a separable extension of K, S is finitely generated as an R-module [6, p. 70]. Since S is torsion free, it is also a projective R module. Since L is isomorphic to $K \otimes S$, the rank of S as a projective R module is d, the dimension of L. If we knew that S splits I, then by Theorem 3 we would know $(I)^d = 1$ in Pic (R) and thus $d \geqq n$, the order of (I). Hence we would have $d = n$, which is what we wanted.

Since S is a projective R-module, $S \otimes I$ is S-isomorphic to $J = SI$. Let v be any root of $g(X)$ in L. Then $J^n = Sw = (Sv)^n$ and thus since S is Dedekind [10, p. 281], $J = Sv$ and so S splits I.

Now suppose n is a unit of R. By Propositions 6 and 4, we know T is isomorphic to a separable R-order T' of L. Since T' is separable, it is maximal, i.e., $T' = S$, the integral closure of R in L and thus is Dedekind.

Now let us do the case in which n is the zero element of R. All we have to show is that T is a domain since clearly n is not a unit. By Proposition 6 we need to show that $X^n - w$ is irreducible over K. Suppose p is the characteristic of K and $n_1 = p^e$ is the highest power of p dividing n. Let $n_2 = n/n_1$. By Lemma 4, we

need to show that both $X^{n_2} - w$ and $X^{n_2} - w$ are irreducible. Let $I' = I^{n_1}$. Then clearly $I'^{n_2} = Rw$, n_2 is the order of (I') in Pic (R) and n_2 is nonzero in R. Hence by the proof of the theorem in the special case, $X^{n_2} - w$ is irreducible. Now we note that w cannot be a p-th power in K. Otherwise if $w = v^p$ for some v in K, and if $n' = n/p$, then $I^{n'p} = (Rv)^p$ indicates $I^{n'} = Rv$ and so n would not be the order of (I). Since w is not a p-th power, $X - w$ is irreducible [10, p. 65].

Suppose I is a nonzero ideal of the Dedekind domain R with $I^n = Rw$, and let $T = T_n(I^{-1}/R, w)$ and let S be the integral closure of R in $L = K[X]/(X^n - w)$. Then Theorem 4 gives sufficient conditions to ensure that T is a domain or is equal to S. We conclude with two examples illustrating then if the hypotheses of Theorem 4 do not hold, the conclusion may or may not still hold.

EXAMPLE 1. n is neither a unit of R nor the order of I, but $T = S$ and is a Dedekind domain.

Proof. Let $R = I = \boldsymbol{Z}$—the rational integers. Let $n = 2$ and $w = -1$. Clearly $T = \boldsymbol{Z}[i]$—the Gaussian integers in $L = Q[i]$.

EXAMPLE 2. n is the order of (I) in Pic (R), is a non zero divisor but is not a unit of R and $T \neq S$.

Proof. Let p and q be distinct rational primes with $p \equiv q \equiv 1 \pmod 4$. Let $R = \boldsymbol{Z}[\sqrt{-pq}]$ and $I = Rp + R\sqrt{-pq}$. One can check that R is the integral closure of $\boldsymbol{Z}$ in $Q(\sqrt{-pq})$ and is thus Dedekind and that I is nonprincipal with $I^2 = Rp$. Let $n = 2$ and let $w = \pm p$. It is not too difficult to show that L is an unramified field extension of K and thus T is a domain and S is separable [5, p. 21]. Since 2 is not a unit of R, by Proposition 4 we know that T is not separable; hence $T \neq S$.

REFERENCES

1. S. A. Amitsur, *Generic splitting fields of central simple algebras*, Ann. of Math. **62** (1955), 8-43.
2. H. Bass, *Lectures in Algebraic K-theory*, Tata Institute of Fundamental Research, Bombay, 1967.
3. N. Bourbaki, *Algebre Commutative*, Chapter 1, Hermann, Paris, 1961.
4. H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton Univ. Press, Princeton, 1956.
5. S. Chase and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Amer. Math. Soc. Memoirs, No. 52, 1965.
6. M. Deuring, *Algebren* (Zweite Auflage), Springer-Verlag, New York, 1968.

7. T. Nagahara, *A note on Galois theory of commutative rings*, Proc. Amer. Math. Soc. **18** (1967), 334-340.
8. P. Roquette, *On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras*, Math. Ann. **150** (1963), 411-439.
9. A. Rosenberg and D. Zelinsky, *Automorphisms of separable algebras*, Pacific J. Math. **11** (1961), 1109-17.
10. O. Zariski and P. Samuel, *Commutative Algebra*, Volume 1, D. Von Nostrand, Princeton, 1958.

Received March 10, 1970.

UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS