ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 2, Number 2, Spring 1972

SEPARABLE POLYNOMIALS OVER A COMMUTATIVE RING

FRANK DEMEYER

If R is a commutative ring with no idempotents other than 0 and 1 then G. J. Janusz in [2] called a polynomial $p(X) \in R[X]$ separable in case $p(X)$ is monic and $R[X]/(p(X))$ is a separable R-algebra. Janusz shows that to each separable polynomial $p(X) \in R[X]$ there is a (unique up to isomorphism) extension N of R so that $p(X)$ factors into linear factors in $N[X]$, N is generated from R by the roots of $p(X)$, the only idempotents in N are 0 and 1, and N is a Galois (in the sense of [1]) extension of R with finite Galois group G.

Such an extension N of R is called a splitting ring for $p(X)$, and the full group of automorphisms of N fixing R elementwise is called the Galois group of $p(X)$. Our first objective is to elaborate on some of Janusz' results. To each commutative ring R with no idempotents other than 0 and 1 we associate a locally strongly separable R-algebra Γ with no idempotents other than 0 and 1 (unique up to isomorphism) so that any finite subset of Γ is contained in an extension $R(\alpha_1, \cdots, \alpha_n)$ of R in Γ with α_i the root of a separable polynomial over $R(\alpha_1, \cdots, \alpha_{i-1})$ and so that any separable polynomial over Γ factors into linear factors in Γ. The full group of R-algebra automophisms of Γ is a compact Hausdorff topological group $G(R)$. This process describes a contravariant functor from the category of commutative rings with no idempotents other than 0 and 1 (and ring homomorphisms) to the category of compact Hausdorff topological groups (with morphisms certain equivalence classes of continuous homomorphisms). The rest of this paper studies the situation when no restriction is placed on idempotents in R. The fundamental tool in this study is the representation of R as a global cross section of a sheaf of commutative rings with no idempotents other than 0 and 1 as elaborated by O. Villamayor and D. Zelinsky in [5]. In order to carry out results analogous to those in [2] it is necessary to consider monic polynomials $p(X) \in R[X]$ so that $R[X]/(p(X))$ is a separable R-algebra and the representation of $p(X)$ in the stalks of the sheaf described above is "uniform" in the sense that the Galois groups of the polynomials at the stalks are isomorphic in a neighborhood of each point in the base space. This is made precise in §2. A Galois theory is developed for these polynomials

Received by the editors May 18, 1970 and, in revised form, October 26, 1970.

AMS 1970 *subject classifications.* Primary 13B05, 13B10, 13B25; Secondary 13C05, 13J99.

which generalizes the situation where R has no idempotents other than 0 and 1. We conclude with a number of examples which show the importance of some restriction on the idempotents in R, or the nature of the polynomial $p(X)$.

Throughout this paper all rings and algebras will be commutative rings and algebras with identity (denoted 1). All ring and algebra homomorphisms carry identity to identity, and by the statement "S is an extension of R" we mean "S is a faithful R-algebra".

We assume throughout a familiarity with [2] and all undefined terminology is as in [2].

1. In this section R will denote a commutative ring whose only idempotents are 0 and 1.

A locally strongly separable R-algebra Γ with no idempotents other than 0 and 1 will be called a polynomial closure of R in case

1. Any finite subset of Γ is contained in an extension $R(\alpha_1, \cdots, \alpha_n)$ of R in Γ with α_i a root of a separable polynomial over $R(\alpha_1, \cdots, \alpha_{i-1})$.
2. Any separable polynomial over Γ factors into linear factors in Γ.

If Γ is a locally strongly separable R-algebra with no proper idempotents then Lemma 2.7 of [2] implies that $R(\alpha)$ is strongly separable over R if and only if α is the root of a separable polynomial over R.

THEOREM 1.1. *Any commutative ring R with no idempotents other than 0 and 1 has a polynomial closure Γ which is unique up to isomorphism. Moreover, Γ is a normal extension of R and the group of R-automorphisms of Γ is a compact Hausdorff topological group.*

PROOF. *Existence*: Let Ω be the separable closure of R. Consider the set $\mathcal{S}$ of all extensions of R in Ω of the form $R(\alpha_1, \cdots, \alpha_n)$ with α_i the root of a separable polynomial in $R(\alpha_1, \cdots, \alpha_{i-1})$. The transitivity properties of separability (Proposition 1.5 of [2]) and the remark preceding Theorem 1.1 imply that $R(\alpha_1, \cdots, \alpha_n)$ is strongly separable over R. If $R(\beta_1, \cdots, \beta_m)$ is another element in $\mathcal{S}$, then observe that β_1 satisfies a separable polynomial in R, and therefore one in $R(\alpha_1, \cdots, \alpha_n)$. Thus $R(\alpha_1, \cdots, \alpha_n, \beta_1)$ is in $\mathcal{S}$ and by a finite induction $R(\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m)$ is an element of $\mathcal{S}$.

Thus $\mathcal{S}$ is a directed set and the union of all the elements of $\mathcal{S}$ provides a locally separable subextension Γ of Ω. Let $p(X)$ be a separable polynomial in $\Gamma[X]$. Let t denote the trace of the free Γ-module $\Gamma[X]/(p(X))$, and let y denote the coset of X modulo $(p(X))$. Find an element $S \in \mathcal{S}$ containing the coefficients of $p(X)$, the elements $t(y^i y^j)$ $(0 \leqq i, j < \deg(p(X)))$, and $\det(t(y^i y^j))^{\pm 1}$. The invertibility of $\det(t(y^i y^j))$ is equivalent to the separability of $p(X)$

(Theorem 2.2 of [2]). Thus $p(X)$ is a separable polynomial over S. If $\beta_1, \cdots, \beta_m$ are the roots of $p(X)$ in Ω and $S = R(\alpha_1, \cdots, \alpha_n)$ then $R(\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m) \in \mathcal{S}$ so all the roots of $p(X)$ are in Γ.

Uniqueness: We show first that the algebra Γ constructed above is a locally strongly separable normal extension of R in Ω.

Now Γ is locally strongly separable by property 1 of the definition of a polynomial closure. If σ is any R-automorphism of Ω and $R(\alpha_1, \cdots, \alpha_n)$ is an extension of R in Ω with α_i the root of a separable polynomial in $R(\alpha_1, \cdots, \alpha_{i-1})$ then $\sigma(R(\alpha_1, \cdots, \alpha_n)) = R(\sigma(\alpha_1), \cdots, \sigma(\alpha_n))$ and $\sigma(\alpha_i)$ is the root of a separable polynomial in $\sigma(R(\alpha_1, \cdots, \alpha_{i-1})) = R(\sigma(\alpha_1), \cdots, \sigma(\alpha_{i-1}))$. Thus $\sigma(\Gamma) \subseteq \Gamma$ for all R-automorphisms σ of Ω which is equivalent to the statement that Γ is a normal extension of R. If G is the group of all R-automorphisms of Ω and H is the closed subgroup fixing Γ then by Theorem 3 of [3] the compact Hausdorff topological group G/H is the full group of R-algebra automorphisms of Γ.

Let Γ' be another polynomial closure of R. The proof of Proposition 1.7 of [2] shows that Γ' is isomorphic to an R-subalgebra of Ω. The construction of Γ insures that the isomorphic copy Γ'' of Γ' in Ω is an R-subalgebra of Γ. Let $\beta \in \Gamma$. Then there exist $\alpha_1, \cdots, \alpha_n$ with $\beta \in R(\alpha_1, \cdots, \alpha_n)$ and α_i the root of a separable polynomial in $R(\alpha_1, \cdots, \alpha_{i-1})$. Thus $\beta \in \Gamma''(\alpha_1, \cdots, \alpha_n)$ and by property 2 of the polynomial closure $\Gamma''(\alpha_1) = \Gamma''$, by induction $\beta \in \Gamma''$ so $\Gamma = \Gamma''$.

Let $p(X)$ be a separable polynomial in $R[X]$ and let $\alpha_1, \cdots, \alpha_n$ be the roots of $p(X)$ in Γ. Then by Proposition 2.6 of [2], $R(\alpha_1, \cdots, \alpha_n)$ is a Galois extension of R with a finite group $G(p(X))$ of R-automorphisms. $G(p(X))$ is a group of permutations on the roots $\alpha_1, \cdots, \alpha_n$ of $p(X)$ and will be called the group of $p(X)$.

We will call the compact Hausdorff group $G(R)$ of R-automorphisms of the polynomial closure Γ of R the Galois group of R. For each commutative ring R with no idempotents other than 0 and 1 we have associated a unique compact Hausdorff group $G(R)$. If G and H are two compact Hausdorff groups and g, h are continuous homomorphisms from G to H say g is equivalent to h if there is a $y \in H$ with $g(x) = yh(x)y^{-1}$ for all $x \in G$. The class of all compact Hausdorff groups with morphisms equivalence classes of continuous homomorphisms is a category.

Let K be another commutative ring with no idempotents other than 0 and 1 and let ϕ be a ring homomorphism from R to K. Let Γ be the polynomial closure of R and let Λ be the polynomial closure of K. The homomorphism ϕ makes K into an R-algebra. Any finite subset of $K \otimes_R \Gamma$ is contained in $K \otimes_R S$ where S is a strongly separable

R-subalgebra of Γ. Thus $K \otimes_R \Gamma$ is a locally strongly separable K-algebra.

Any polynomial $p(X) \in R[X]$ which is separable over R must be separable over K. By Proposition 1.7 of [2] there is a K-homomorphism from $K \otimes_R \Gamma$ into Ω (the separable closure of K). The restriction of this homomorphism is a ring homomorphism $\bar{\phi}$ from Γ to Ω extending ϕ. Let F be a finite subset of image $(\bar{\phi})$ and let F' be a set of representatives for the preimage of F in Γ. There is an extension $R(\alpha_1, \cdots, \alpha_n)$ of R in Γ containing F' with α_i the root of a separable polynomial in $R(\alpha_1, \cdots, \alpha_{i-1})$. By construction, $F \subseteq K(\bar{\phi}(\alpha_1), \cdots, \bar{\phi}(\alpha_n))$, and it is easy to check that $\bar{\phi}(\alpha_i)$ is the root of the separable polynomial over $K(\bar{\phi}(\alpha_1), \cdots, \bar{\phi}(\alpha_{i-1}))$ obtained via $\bar{\phi}$ from the corresponding polynomial over $R(\alpha_1, \cdots, \alpha_{i-1})$. Thus, image $\bar{\phi} \subseteq \Lambda$. If $\bar{\tau} \in G(K)$ then $\bar{\tau}\bar{\phi}$ is another extension of ϕ. For each Galois extension N of R in Γ, $\bar{\tau}\bar{\phi}|_N$ is an isomorphism from N into Λ. By Lemma 1.3 of [2] we conclude that there is an automorphism σ of N so that $\bar{\tau}\bar{\phi}|_N = \bar{\phi}\sigma|_N$. Define $\bar{\sigma}$ on all of Γ by using the fact that Γ is the union of its R-subalgebras which are Galois extensions of R. Then one can check that $\bar{\sigma} \in G(R)$. Thus using the extension $\bar{\phi}$ of ϕ we are able to associate to each element $\bar{\tau} \in G(K)$ a unique element $\bar{\sigma} \in G(R)$. The different extensions of ϕ to Γ yield different (but equivalent) homomorphisms from $G(K)$ to $G(R)$. Thus we have associated to the ring homomorphism ϕ from R to K a morphism $G(\phi)$ from $G(K)$ to $G(R)$. It is now routine to verify the following theorem.

THEOREM 1.2. *The association $R \to G(R)$ defines a contravariant functor from the category of commutative rings with no idempotents other than 0 and 1 to the category of compact Hausdorff topological groups with morphisms equivalence classes of homomorphisms.*

2. Throughout this section we will be employing freely the ideas and results of [5]. We begin by introducing the terminology we will need.

Let R be any commutative ring, and let $B(R)$ be the collection of idempotents in R. Then $B(R)$ is a Boolean algebra with operations $e * f = ef$ and $e \oplus f = e + f - ef$ for all $e, f \in B(R)$. Let spec $B(R)$ be the set of maximal ideals in $B(R)$. As a base for a topology on spec $B(R)$ call a subset U_e of spec $B(R)$ a basic open set in case $U_e = \{x \in \text{spec } B(R) \mid e \in x, e \text{ fixed in } B(R)\}$. This base defines a compact, totally disconnected, Hausdorff topology on spec $B(R)$. If $U_{e_1}, \cdots, U_{e_n}$ are basic open sets which cover spec $B(R)$ then observe that there are idempotents $f_1, \cdots, f_n$ contained in $(1 - e_1), \cdots, (1 - e_n)$ so that

$R = Rf_1 \oplus Rf_2 \oplus \cdots \oplus Rf_n$. We will use this fact several times in what follows. For each $x \in \operatorname{spec} B(R)$ let $R_x = R/Rx$. Then R_x is a commutative ring whose only idempotents are 0 and 1.

This process defines a sheaf whose base space is spec $B(R)$, and whose stalks are the rings R_x. In this case R is represented in a natural way as a global cross section of this sheaf. The basic sheaf property that if two cross sections agree at a point then they agree in a neighborhood of the point can be used to lift information true at R_x for all x to information about R. If M is an R-module let $M_x = R_x \otimes_R M$. If M and N are R-modules and $g \in \operatorname{Hom}_R(M\ N)$, let g_x be the corresponding homomorphism induced in $\operatorname{Hom}_{R_x}(M_x, N_x)$.

We call a polynomial $p(X) \in R[X]$ separable in case it is monic and $R[X]/(p(X))$ is separable over R. If $y \in \operatorname{spec} B(R)$ then the natural homomorphism from R onto R_y induces a homomorphism from $R[X]$ to $R_y[X]$. If $p(X) \in R[X]$ we denote the corresponding polynomial in $R_y[X]$ by $p_y(X)$.

A separable polynomial $p(X) \in R[X]$ is called uniform in case for each $x \in \operatorname{spec} B(R)$ there exists a neighborhood U of x in spec $B(R)$ such that for all $y \in U$, $G(p_y(X)) \simeq G(p_x(X))$.

THEOREM 2.1. *Let $p(X)$ be a uniform separable polynomial in $R[X]$. Then there exists a finite projective separable extension N of R and elements $\alpha_1, \cdots, \alpha_n$ in N so that*

1. $p(X) = \prod_{i=1}^{n}(X - \alpha_i)$ *in* $N[X]$,
2. $N = R(\alpha_1, \cdots, \alpha_n)$,
3. $B(N) = B(R)$.

PROOF. Let $S = R[X]/p(X)$, then S is a strongly separable extension of R containing a root α_1 of $p(X)$. In $S[X]$, $p(X) = (X - \alpha_1)p_1(X)$ where $p_1(X)$ is a monic polynomial in $S[X]$. Now $S[X]/(p_1(X))$ is a homomorphic image of $S \otimes R[X]/(p(X))$ so $p_1(X)$ is a separable polynomial in S. The property of being strongly separable is transitive so by a finite induction we come to a strongly separable extension T of R in which $p(X)$ factors completely.

Let $x \in \operatorname{spec} B(R)$, and write T_x as a finite direct sum of strongly separable R_x-algebras. In each of those algebras $p_x(X)$ factors completely so T_x contains an algebra $R_x(\alpha_{1x}, \cdots, \alpha_{nx})$ which is a splitting ring for $p_x(X)$ over R_x. Lift the elements $\alpha_{1x}, \cdots, \alpha_{nx}$ to elements $\alpha_1, \cdots, \alpha_n$ in T and let $N = R(\alpha_1, \cdots, \alpha_n)$. Find a neighborhood U of x so that for all $y \in U$

1. N_y is separable over R_y,
2. $p_y(X) = \prod_{i=1}^{n}(X - (\alpha_i)_y)$ in $N_y[X]$,
3. $G(p_y(X)) \simeq G(p_x(X))$.

Such a neighborhood can be found using the hypothesis and (2.9) of [5]. This neighborhood U defines an idempotent e of R so that Ne is a separable Re-algebra so by Proposition 1.5 of [2], Ne is projective over Re. We can therefore further restrict U so that $\text{Rank}_{R_y}(N_y) = \text{Rank}_{R_x}(N_x)$ for all $y \in U$. Since $\text{Rank}_{R_y}(N_y) = [G(p_y(X)) : 1]$ it follows that the only idempotents in N_y are 0_y and 1_y. If f is an idempotent in Ne then either $f_y = 0_y$ or $f_y = 1_y$ for all $y \in U$. Thus $(Re + Rf)_y = (Re)_y$ for all $y \in U$ which implies that $f \in Re$ by (2.11) of [4]. Thus Ne satisfies the conclusion of the theorem for $p(X)e$ over Re. Now employ the compactness of spec $B(R)$ to find a finite collection $e_1, \cdots, e_m$ of orthogonal idempotents in R summing to 1 so that an extension N_i of Re_i satisfies the theorem for $p(X)e_i$. Then let $N = N_1 \oplus \cdots \oplus N_m$.

Let $p(X)$ be a uniform separable polynomial in $R[X]$. An extension N of R satisfying the conditions of Theorem 2.1 will be called a splitting ring for $p(X)$.

Let N be a splitting ring for $p(X)$ and let $x \in \text{spec } B(R)$. By 2.14 of [5] one can extend the R_x-automorphisms in $G(p_x(X))$ to a set G of R-automorphisms of N where the identity is extended to the identity on N. By Theorem 1.3 of [1] there are elements $a_{1x}, \cdots, a_{nx}$, $b_{1x}, \cdots, b_{nx}$ in N_x so that

$$\sum_{i=1}^{n} a_{ix}\sigma_x(b_{ix}) = 1_x, \qquad \sigma_x = 1 \text{ in } G_x,$$
$$= 0, \qquad \sigma_x \neq 1 \text{ in } G_x.$$

Let $a_1, \cdots, a_n, b_1, \cdots, b_n$ be elements of N with $(a_i)_x = a_{ix}$, $(b_i)_x = b_{ix}$ for $i = 1, \cdots, n$. By 2.9 of [5] there is a basic open set V in spec $B(R)$ defining an idempotent $e \in R$ so that

$$\sum_{i=1}^{n} (a_ie)\sigma(y_ie) = e, \qquad \sigma = 1 \text{ in } G,$$
$$= 0, \qquad \sigma \neq 1 \text{ in } G.$$

By Theorem 1.3 of [1], Ne is a Galois extension of $(Ne)^G$ with group G and $\text{Rank}_{(Ne)^G}(Ne) = [G : 1] = \text{Rank}_{Re}(Ne)$. This implies that $(Ne)^G = Re$ and applying compactness of spec $B(R)$ we have that N is a weakly Galois extension of R [5]. We can now prove

THEOREM 2.2. *Any two splitting rings for a uniform separable polynomial are isomorphic.*

PROOF. Let S and T be splitting rings for the separable polynomial $p(X)$ in $R[X]$. By decomposing R by a finite number of idempotents

we can assume by Theorem 3.15 of [5] that S and T are Galois extensions of R with Galois group G. For each $x \in \operatorname{spec} B(R)$ there is a G_x-isomorphism g_x from S_x to T_x over R_x. Lift g_x to an R-module isomorphism g from S to T using (2.7) of [4].

Let $a_1, \cdots, a_n; b_1, \cdots, b_n$ be in S with

$$\sum_{i=1}^{n} a_i\sigma(b_i) = 1, \qquad \sigma = \text{identity in } G,$$
$$= 0, \qquad \sigma \neq \text{identity in } G.$$

In a basic neighborhood U of x the following are satisfied for each $y \in U$.

1. $[g(\sigma(a_i))]_y = [\sigma(g(a_i))]_y$, $i = 1, \cdots, n$,
2. $g(a_ia_j)_y = g(a_i)_y g(a_j)_y$, $1 \leqq i, j \leqq n$.

Thus g is a G-homomorphism from Se to Te where e is the idempotent defining U. Since Se and Te are Galois extensions of Re Theorem 3.4 [1] implies that g is an isomorphism. Applying the usual compactness argument completes the proof.

Call a ring R uniform if for each $x \in \operatorname{spec} B(R)$ there is a collection of isomorphisms $\phi_y : R_y \to R_x$ ($y \in \operatorname{spec} B(R)$) such that if F is a finite subset of R there is a neighborhood V of x with $\phi_y(a_y) = a_x$ for all $a \in F$, $y \in V$.

Call a ring R weakly uniform if it is a finite direct sum of uniform rings. For example, if R is any ring whose only idempotents are 0 and 1 then the subring of the direct product of any number of copies of R generated by the direct sum together with the R-multiples of the identity is a uniform ring.

If R is a commutative ring and $\mathcal{X}$ is a topological space we let $\mathcal{C}(\mathcal{X}, R)$ be the ring of continuous functions from $\mathcal{X}$ to R where R is given the topology where point sets are open.

THEOREM 2.3. *The following conditions on a commutative ring R are equivalent.*

1. *R is a weakly uniform ring.*
2. *There is a finite collection $R_1, \cdots, R_n$ of commutative rings with no idempotents other than 0 and 1 and orthogonal idempotents $e_1, \cdots, e_n$ in R which sum to 1 so that $Re_i \simeq \mathcal{C}(\operatorname{spec} B(Re_i), R_i)$, $i = 1, \cdots, n$.*
3. *There is a finite collection of totally disconnected compact Hausdorff spaces $\{\mathcal{X}_i\}_{i=1}^n$ and commutative rings $\{R_i\}_{i=1}^n$ with no idempotents other than 0 and 1 so that $R \simeq \bigoplus \sum_{i=1}^n \mathcal{C}(\mathcal{X}_i, R_i)$.*

PROOF. (1 implies 2).

We can assume without loss of generality that R is uniform. Let $x \in \operatorname{spec} B(R)$ and define a homomorphism $\phi : R \to \mathcal{C}(\operatorname{spec} B(R), R_x)$ by letting the image of $\phi(a)$ at y be $\phi_y(a_y)$ where $a \in R$ and the ϕ_y are given in the definition of uniformity. Notice that the last condition in the definition of uniformity implies that $\phi(a)$ is continuous so ϕ is well defined. A consequence of (2.9) of [5] is that ϕ is one-to-one. Let $\Psi \in \mathcal{C}(\operatorname{spec} B(R), R_x)$ and let $a \in R$ with $a_x = \Psi(x)$. Since Ψ is continuous there is a neighborhood U of x with $\Psi(y) = a_x$ for all $y \in U$. Thus $\phi(a)$ agrees with Ψ on U. Let e be the idempotent defined by U, then $\phi(ae) = \Psi$ on U.

By compactness one can find $x_1, \cdots, x_n$ in spec $B(R)$ and orthogonal idempotents $e_1, \cdots, e_n$ which sum to 1 and elements a_i in Re_i so that $\Psi(ae_i) = \phi_{x_i}^{-1}(a_x)$ where $\phi_{x_i} : R_{x_i} \to R_x$ is an isomorphism given in the definition of uniformity. Observe that if $a = ae_1 + \cdots + ae_n$, then $\phi(a) = \Psi$.

Once one identifies spec $B(\mathcal{C}(\mathcal{X}_i, R_i))$ with $\mathcal{X}_i$ the rest of the theorem is easy to check.

COROLLARY 2.4. *If R is a weakly uniform ring then any separable polynomial over R is uniform.*

PROOF. Let $p(X)$ be a separable polynomial in $R[X]$ and let $x \in \operatorname{spec} B(R)$. Let U be a neighborhood of x satisfying the condition given in the definition of uniform ring where F consists of the coefficients of $p(X)$. It is clear that for each $y \in U$ that $G(p_y(X)) \simeq G(p_x(X))$ so $p(X)$ is uniform.

PROPOSITION 2.5. *Let R be a weakly uniform ring and N the splitting ring of a separable polynomial $p(X)$ over R. Then N is weakly uniform.*

PROOF. Decomposing by a finite number of idempotents in R reduces to the situation where R is uniform. In this case by Theorem 2.3, $R = \mathcal{C}(\mathcal{X}, S)$ where S is a commutative ring whose only idempotents are 0 and 1 and $\mathcal{X}$ is a totally disconnected compact Hausdorff space. Let $p(X) = a_0 + a_1X + \cdots + X^n$ and for $x \in \mathcal{X}$ let U be a basic neighborhood of x with $a_i(y) = a_i(x)$ for all $y \in U$, $i = 0, 1, \cdots, n-1$. Let e be the idempotent in R defined by

$$\begin{aligned} e(y) &= 0, \qquad y \notin U, \\ &= 1, \qquad y \in U. \end{aligned}$$

Then $Re = \mathcal{C}(U, S)$. View $p_x(X)$ as a polynomial in $S[X]$ and let T be its splitting ring over S. Then one can check that $Ne = \mathcal{C}(U, T)$ is a splitting ring for $p(X)e$ over Re. The splitting ring for $p(X)$ over

R is a finite direct sum of such uniform rings and thus is weakly uniform.

A polynomial closure of a uniform ring R is a locally strongly separable extension Γ of R such that

1. Γ is uniform and $B(\Gamma) = B(R)$.
2. Any finite subset of Γ is contained in an extension $R(\alpha_1, \cdots, \alpha_n)$ of R in Γ with α_i the root of a separable polynomial in $R(\alpha_1, \cdots, \alpha_{i-1})$.
3. Any separable polynomial in Γ factors into linear factors in Γ.

Generalizing the results in §1 we have

THEOREM 2.6. *Let R be a uniform ring, then a polynomial closure Γ of R exists and is unique up to isomorphism.*

PROOF. Since R is uniform we can let $R = \mathcal{C}(\text{spec } B(R), S)$ where S is a fixed commutative ring with no idempotents other than 0 and 1 with the discrete topology. Let T be the polynomial closure of S, given by Theorem 1.3. Let $\Gamma = \mathcal{C}(\text{spec } B(R), T)$, then Γ clearly satisfies the first condition for the polynomial closure of R. Using the usual compactness argument on spec $B(R)$ and the previous proposition, it is not hard to check condition 2 of the definition. A separable polynomial over Γ factors into linear factors at each point in spec $B(\Gamma)$ = spec $B(R)$ so again condition 3 follows from the compactness of spec $B(R)$. Thus the polynomial closure of a uniform ring exists.

To prove uniqueness, let Λ be another polynomial closure of R. Condition 1 implies $\Lambda = \mathcal{C}(\text{spec } B(R), T')$ for some extension T' of S with no idempotents other than 0 and 1. Condition 2 of the definition of Λ implies that T' is a locally separable extension of S such that any finite subset of T' is contained in an extension $S(\alpha_1, \cdots, \alpha_n)$ of S in T' with α_i the root of a separable polynomial over $S(\alpha_1, \cdots, \alpha_{i-1})$. Any separable polynomial in T' can be lifted to a separable polynomial in Λ so by condition 3 of the definition any separable polynomial in T' must factor into linear factors in T'. Thus $T' = T$ by Theorem 1.1 and $\Lambda = \Gamma$ which completes the proof.

Let R be a uniform ring and let $G(R)$ be the group of all R-algebra automorphisms of the polynomial closure Γ of R. Then $G(R)$ is naturally a subgroup of the direct product of $G(S)$ where S has no idempotents other than 0 and 1 and $R = \mathcal{C}(\text{spec } B(R), S)$. While the direct product of $G(S)$ is a compact group, $G(R)$ is not necessarily a closed subgroup in the relative topology so there seems to be no convenient way to make $G(R)$ into a compact group.

There is a broad class of rings for which our results are relevant.

A ring R is regular if and only if R_x is a field for each $x \in \operatorname{spec} B(R)$ (see [4]).

THEOREM 2.7. *Let R be a regular ring and let S be a finite projective separable extension of R with $B(S) = B(R)$. Then there is an element $\alpha \in S$ and a separable polynomial $p(X) \in R[X]$ so that $S = R(\alpha)$ and α is a root of $p(X)$. Moreover, if S is a weakly Galois extension of R then the polynomial $p(X)$ can be chosen to be uniform.*

PROOF. Let $x \in \operatorname{spec} B(R)$. Then S_x is a separable projective extension of R_x whose only idempotents are 0 and 1. Since R_x is a field, S_x is a field. By the "primitive element theorem" there is an element $\alpha_x \in S_x$ which is the root of the separable polynomial $p_x(X)$ over $R_x[X]$ and so that $S_x = R_x(\alpha_x)$. Lift $p_x(X)$ and α_x to a monic polynomial $p(X) \in R[X]$ and $\alpha \in S$. If $y_1, \cdots, y_n$ generate S as an R-module then

$$y_{ix} = \sum r_{ijx}\alpha_x^j, \qquad i = 1, \cdots, n.$$

These equations will hold in a neighborhood of x by (2.9) of [5]. As in Theorem 2.2 (5) of [2], in the R-algebra $R[X]/(p(X))$ form the matrix $[t(X^iX^j)]$, $0 \leqq i, j <$ degree (p), where t is the trace map of the free R-module $R[X]/(p(X))$. By Theorem 2.2 (5) of [2] there is an element $u_x \in R_x$ so that

$$\det [t(X^iX^j)]_x u_x = 1_x.$$

By lifting u_x to an element u in R this equation will also hold in a neighborhood of x. Therefore, there is an idempotent $e \in R$ so that $Se = Re(\alpha)$ and $\alpha \cdot e$ satisfies the monic polynomial $p(X) \cdot e$. Now $p(X)e$ is separable at each $y \in \operatorname{spec} B(Re)$, therefore $p(X)e$ is separable over Re. Applying the usual compactness argument and decomposing R by a finite number of orthogonal idempotents e as above gives the first assertion of the theorem.

If S is weakly Galois over R then by decomposing R by a finite number of idempotents we can assume S is Galois over R with Galois group G in the sense of [1] (3.15 of [5]). In this case if $x \in \operatorname{spec} B(R)$, S_x will be a Galois extension of R_x so we can choose the polynomial $p_x(X)$ in the first paragraph of the proof so that S_x is a splitting field for $p_x(X)$. In addition to the equations developed there we know $p_x(X) = \prod_{i=1}^n (X - \alpha_{ix})$ in $S_x[X]$. Lift the α_{ix} to α_i in S where $\alpha_x = \alpha_{1x}$ and α_{1x} is lifted to α. Then in a neighborhood U of x, $p_y(X) = \prod_{i=1}^n (X - \alpha_{iy})$ for all $y \in U$. Intersect U with the neighborhood of x constructed in the first paragraph. For all y in this neighborhood

$$\text{degree } p_y(X) = \text{Rank}_{R_y}(R_y(\alpha_y)) = [G:1].$$

Thus $G_y = G(p_y(X)) = G$ for all y in a neighborhood of x which proves $p(X)$ is uniform.

At this point there are several things one would like to do, and we present a series of examples which show the difficulties involved.

Let $\mathcal{X} = \{1, 1/2, 1/3, \cdots, 1/n, \cdots, 0\}$ with the relative topology of the real line. Then $\mathcal{X}$ is a compact totally disconnected Hausdorff space and 0 is the only point in $\mathcal{X}$ which is not both open and closed. Let R be the ring of continuous complex functions f on $\mathcal{X}$ such that $f(0)$ is real. Algebraically, R is the subring of the direct product of countably many copies of the complex numbers generated by the direct sum and real multiples of the identity. Then spec $B(R)$ is just $\mathcal{X}$, and it is clear that R is not a uniform ring because of the situation at 0. The polynomial $X^2 + 1$ is separable over R but not uniform, again because of the situation at 0. There is no splitting ring N for $X^2 + 1$ over R, the only candidate is the continuous functions from $\mathcal{X}$ to the complex numbers and this ring is not projective over R.

Let $\mathcal{X}$ be as before and let S be the ring of real valued continuous functions on $\mathcal{X}$. Let $e_n \in S$ be defined by $e_n(1/m) = \delta_{m,n}$. Let $p_n(X) \in S[X]$ be defined by $p_n(X) = X^2 + e_n$. Then each $p_n(X)$ is a uniform separable polynomial over the uniform ring S. The ring T_n of continuous functions f from $\mathcal{X}$ to the complex numbers so that $f(1/m)$ is real for $m > n$ is a uniform, locally strongly separable extension of S which is a splitting ring for $\prod_{i=1}^{n} p_i(X)$. However, $\bigcup_{n=1}^{\infty} T_n$ is the ring R we discussed before. Observe that R is a locally separable S-algebra and is a subalgebra of the polynomial closure of S. The polynomial $X^2 + 1$ is uniform over S but not R.

The separable polynomial closure Γ of S is the ring of continuous functions from $\mathcal{X}$ to the complex numbers. The full group $G(S)$ of S-automorphisms of Γ is contained in the countable direct product $\prod C_2$ of copies of the cyclic group C_2 of order = 2, one copy of C_2 for each element of $\mathcal{X}$. However, $G(S) \neq \prod C_2$ since an automorphism in $G(S)$ is determined in a neighborhood of $0 \in \mathcal{X}$ by its action at $f(0)$ where $f \in \Gamma$. Moreover, $G(S)$ is not closed in the relative topology of $\prod C_2$.

In [2], G. J. Janusz defines a separable closure Ω for any commutative ring R with no idempotents other than 0 and 1 and associates to R the group of algebra automorphisms of Ω. As Janusz points out (p. 471 of [2]), this group may be different from the group of the polynomial closure, even if R is a local ring. The two groups coincide if R is a field.

REFERENCES

1a. D. K. Harrison, *Abelian extensions of commutative rings,* Mem. Amer. Math. Soc. No. 52 (1965), 1-14. MR 33 #4117.

1b. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings,* Mem. Amer. Math. Soc. No. 52 (1965), 15-33. MR 33 #4118.

1c. S. U. Chase and A. Rosenberg, *Amitsur cohomology and the Brauer group,* Mem. Amer. Math. Soc. No. 52 (1965), 34-79. MR 33 #4119.

2. G. J. Janusz, *Separable algebras over commutative rings,* Trans. Amer. Math. Soc. **122** (1966), 461-479. MR 35 #1585.

3. T. Nagahara, *A note on Galois theory of commutative rings,* Proc. Amer. Math. Soc. **18** (1967), 334-340. MR 34 #7580.

4. R. S. Pierce, *Modules over commutative regular rings,* Mem. Amer. Math. Soc. No. 70 (1967). MR 36 #151.

5. O. E. Villamayor and D. Zelinsky, *Galois theory with infinitely many idempotents,* Nagoya Math. J. **35** (1969), 83-98. MR 39 #5555.

COLORADO STATE UNIVERSITY, FORT COLLINS, COLORADO 80521