HERMITE SEMIGROUP RINGS

Leo G. Chouinard, II

If S is a commutative, separative semigroup with identity, and R is a commutative ring with unit such that $R[S]$ is arithmetical, then a local-global principle for verifying algebraic equations in $R[S]$ is established. This is then used to show that if S is not a union of torsion groups, then $R[S]$ is an elementary divisor ring.

1. **Introduction and notation.** The arithmetic of commutative semigroup rings has been studied in a number of papers in recent years. Gilmer and Parker [3] were able to determine when such a ring over a torsion-free cancellative semigroup is Prufer, and from their work it is easy to conclude that such a ring is also an elementary divisor ring. Hardy and Shores [4] determined necessary and sufficient conditions for the semigroup ring of a cancellative commutative semigroup to be arithmetical, and in that case if the semigroup is not a torsion group, again the ring is an elementary divisor ring. In a subsequent paper by Hardy, Shores, and this author [1], it was completely determined when the semigroup ring of a commutative separative semigroup is arithmetical.

The purpose of this paper is to show that if S is a commutative, separative semigroup which is not a union of torsion groups, then $R[S]$ is arithmetical iff it is an elementary divisor ring. This also completes the determination of when $R[S]$ is Bezout or Hermite if S is as above. This result substantially generalizes the well-known result that $R[X]$ is an elementary divisor ring if R is a field ([5], §12).

Our notation generally agrees with that in [1]. All rings will be commutative with unit $1 \neq 0$, and regular will mean von Neumann regular. If R is a ring and S is a semigroup, then $R[S]$ is the semigroup ring of S with coefficients in R; however, we reserve $R[X]$ for the ring of polynomials in R. All semigroups will be commutative, separative, and unless noted otherwise, written multiplicatively; furthermore, we shall assume all semigroups have an identity element, although we shall not require this of subsemigroups. All homomorphisms of rings or semigroups are unit preserving. If S is a semigroup, since it is separative it can be written as a semilattice of cancellative archimedean subsemigroups ([2], Theorems 4.13 and 4.16); that is, $S = \bigcup_{\alpha \in Y} S_\alpha$ where Y is a semilattice and the S_α are disjoint cancellative archimedean subsemigroups of S such that $S_\alpha S_\beta \subseteq S_{\alpha \wedge \beta}$. Note each S_α is either a group

or is nonpotent (idempotent free). We call each S_α a component of S, and Y the semilattice of S; we shall say $S = \bigcup_{\alpha \in Y} S_\alpha$ is the decomposition of S. If $\alpha, \beta \in Y$, we write $\alpha\beta$ for $\alpha \wedge \beta$, and we say $\alpha \geq \beta$ if $\alpha\beta = \beta$. We always use 0 for the index of component of the identity element of S, and if S has a zero element distinct from the identity, then by abuse of notation we use z for both that element and for the index of its component.

With S as above, the multiplication on S is determined by the S_α's and suitable group maps $\phi_{\alpha,\beta}: tot(S_\alpha) \to tot(S_\beta)$ defined for all $\alpha \geq \beta$, where $tot(S_\alpha)$ indicates the total quotient group of the cancellative semigroup S_α ([2], Theorems 4.17 and 4.11). We say S is a union of groups if each S_α is a group.

By a filter $\mathscr{F}$ on the semilattice Y we mean a nonempty subsemilattice of Y such that if $\alpha \in \mathscr{F}$, $\beta \in Y$, and $\beta \geq \alpha$, then $\beta \in \mathscr{F}$. If S is a semigroup with decomposition $\bigcup_{\alpha \in Y} S_\alpha$ and each S_α has torsion-free rank ≤ 1, then for any filter $\mathscr{F}$ on Y we can define the local reduction $S_{\mathscr{F}}$ of S at $\mathscr{F}$ as in §3 of [1]. Recall that if $R[S]$ is arithmetical for some ring R, then the rank condition must hold (4.1 and 4.3 of [1]), and the local reductions exist. Our arguments will assume a knowledge of the construction and properties of local reductions given in [1].

If $R[S]$ is a semigroup ring and S has decomposition $\bigcup_{\alpha \in Y} S_\alpha$, then $R[S] \cong \bigoplus_{\alpha \in Y} R[S_\alpha]$ as R-modules. If $\lambda \in R[S]$, then λ can be uniquely written as $\sum_{\alpha \in Y} \lambda_\alpha$ with $\lambda_\alpha \in R[S_\alpha]$ and all but finitely many equal to 0; we then define $\operatorname{supp}(\lambda) = \{\alpha \in Y \mid \lambda_\alpha \neq 0\}$. We also define $\lambda^{(\alpha)} = \sum_{\beta > \alpha} \lambda_\beta$, $\lambda^{[\alpha]} = \sum_{\beta \geq \alpha} \lambda_\beta$, and $S^{[\alpha]} = \bigcup_{\beta \geq \alpha} S_\beta$ for any $\alpha \in Y$; note that the last is a subsemigroup of S. If U is a matrix with entries in $R[S]$, we can likewise write $U = \sum_{\alpha \in Y} U_\alpha$ and speak of $U^{(\alpha)}$, $U^{[\alpha]}$, and $\operatorname{supp}(U)$.

Recall that a ring R is Hermite if for every row vector $[a \quad b]$ of length 2 over R, there exists a 2×2 matrix W over R such that $\det(W) = 1$ and $[a \quad b]W = [d \quad 0]$ for some $d \in R$. Such a ring is automatically Bezout, and thus also arithmetical. R is called an elementary divisor ring (denoted EDR) if it is Hermite and for every 2×2 matrix M over R, there exist 2×2 matrices U, W over R such that $\det(U) = \det(W) = 1$ and UMW is diagonal [5]. Using the Hermite assumption to factor out the gcd of the entries of M, we may assume that these entries generate the unit ideal in R, and that $UMW = \begin{bmatrix} 1 & 0 \\ 0 & \det(M) \end{bmatrix}$.

In §2 we shall develop some further facts about local reductions, and prove a local-global theorem for verifying equations in arithmetical semigroup rings, which reduces the problem to checking a finite number of local reductions. In §3, it is shown that if S is not a

union of torsion groups and $R[S]$ is arithmetical, then it is Hermite. The proof requires a series of technical lemmas, and for most readers only the proof of Proposition 3.1 and the statement of Theorem 3.4 from this section should be read at first. In §4, the much simpler proof that the above implies that $R[S]$ is an EDR is sketched.

The author wishes to thank Thomas Shores for reading a first draft of this paper and recommending certain clarifications.

2. **Local reductions revisited.** Let S be a semigroup with decomposition $\bigcup_{\alpha \in Y} S_\alpha$ such that the torsion-free rank of each S_α is ≤ 1, and let $\mathscr{F}$ be a filter on Y. Let $S_{\mathscr{F}}$ have decomposition $\bigcup_{\alpha \in Y'} \hat{S}_\alpha$, and let $\eta_{\mathscr{F}}: S \to S_{\mathscr{F}}$ be the natural map. Then the following facts can be proved from the construction of local reductions and the results in [1].

(i) If $\beta \in Y$, define $Y^{(\beta)} = \{\alpha \in Y \mid \alpha \geq \beta\}$ if S_β is potent, and $Y^{(\beta)} = \{\alpha \in Y \mid \alpha \geq \beta$ and $\phi_{\alpha,\beta}$ is reduced trivial$\}$ otherwise. Then $Y^{(\beta)}$ is a filter on Y, and is in fact the smallest filter on $\mathscr{G}$ such that $\eta_{\mathscr{F}}(S_\beta) \neq \tilde{S}_z$, with $\tilde{S}_z$ the component of the zero element of $S_{\mathscr{F}}$, if one exists distinct from the identity. Moreover, $\eta_{\mathscr{F}}(S_\beta) \neq \hat{S}_z$ iff for all $\gamma \in \mathscr{F}$, $Y^{(\beta\gamma)} \subseteq \mathscr{F}$. Note also that if $\alpha \geq \beta$ and S_α is potent, then $\alpha \in Y^{(\beta)}$.

(ii) If $R[S]$ is arithmetical and S_β is a nonpotent component of S, then for $\mathscr{F} = Y^{(\beta)}$ we have $S_{\mathscr{F}} \cong \hat{S}_0 \cup S_\beta \cup \hat{S}_z$ with $\hat{S}_0 = \text{inj. lim.}\{S_\alpha \mid \alpha \in Y^{(\beta)}\}$ necessarily a torsion group and $\hat{S}_z$ either ϕ or $\{z\}$, with z a zero element distinct from the identity. Also, if $\gamma \geq \beta$ but $\gamma \notin Y^{(\beta)}$, then for some $\alpha \in Y^{(\beta)}$ we have $\gamma\alpha = \beta$, while if $\gamma \not\geq \beta$, $\eta_{\mathscr{F}}(S_\gamma) = \hat{S}_z$.

(iii) Let $\kappa_{\mathscr{F}}$ be the natural map from $R[S]$ to $R[S_{\mathscr{F}}]/(z)$, where (z) is the ideal of $R[S_{\mathscr{F}}]$ generated by $\hat{S}_z$ (so $(z) = 0$ if $\hat{S}_z = \phi$). Since $S_{\mathscr{F}}$ is of special type (see §5 in [1]), it follows that $\mathscr{H} = \{\alpha \in Y \mid \eta_{\mathscr{F}}(S_\alpha) \neq \hat{S}_z\}$ is also a filter on Y. Let $a \in R[S]$ and let V be a finite subsemilattice of Y containing $\text{supp}(a)$, and suppose β is the minimal element of $\mathscr{H} \cap V$. Suppose $\bar{S} = S^{[\beta]}$, and let $\bar{\eta}_\beta$ by abuse of notation denote both the natural map $\bar{S} \to \bar{S}_{Y^{(\beta)}}$ and the induced map $R[\bar{S}] \to R[\bar{S}_{Y^{(\beta)}}]$. Now $R[\bar{S}_{Y^{(\beta)}}]$ is just the localization of $R[\bar{S}]$ at $\bigcup_{\alpha \in Y^{(\beta)}} S_\alpha$ (note that for this case, step (i) in the definition of the local reduction in [1], §3, is trivial). Since $Y^{(\beta)} \subseteq \mathscr{F}$, we have a natural map $\kappa_{\beta,\mathscr{F}}: R[\bar{S}_{Y^{(\beta)}}] \to R[S_{\mathscr{F}}]/(z)$ such that $\kappa_{\beta,\mathscr{F}} \circ \bar{\eta}_\beta = \kappa_{\mathscr{F}} \circ i$, where $i: R[\bar{S}] \to R[S]$ is the inclusion. But $\kappa_{\mathscr{F}}(a) = \kappa_{\mathscr{F}}(a^{[\beta]})$, so we get the following local-global principle.

PROPOSITION 2.1. *Let S be a separative semigroup with decomposition $\bigcup_{\alpha \in Y} S_\alpha$, and let R be a ring such that $R[S]$ is arithmetical. Suppose $a_1, \cdots, a_n \in R[S]$, and V is a finite subsemilattice of Y con-*

taining $\{0\} \cup \bigcup_{i=1}^{n} \text{supp}(a_i)$. *Let* $P(x_1, \cdots, x_n)$ *be an equation of polynomials in* $x_1, \cdots, x_n$ *with coefficients in* R. *Then* $P(a_1, \cdots, a_n)$ *holds in* $R[S]$ *iff for every* $\beta \in V$, $P(\bar{\eta}_\beta(a_1^{[\beta]}), \cdots, \bar{\eta}_\beta(a_n^{[\beta]}))$ *holds in* $R[S_{Y(\beta)}^{[\beta]}]$.

Proof. Since the inclusion map $R[S^{[\beta]}] \to R[S]$ has a left inverse, namely $a \to a^{[\beta]}$, if $P(a_1, \cdots, a_n)$ holds in $R[S]$, then $P(a_1^{[\beta]}, \cdots, a_n^{[\beta]})$ holds in $R[S^{[\beta]}]$, so $P(\bar{\eta}_\beta(a_1^{[\beta]}), \cdots, \bar{\eta}_\beta(a_n^{[\beta]}))$ holds in $R[S_{Y(\beta)}^{[\beta]}]$ by applying $\bar{\eta}_\beta$. Conversely, since P can be tested locally, to show $P(a_1, \cdots, a_n)$ holds in $R[S]$ it suffices by the proof of Corollary 3.4 of [1] to show that for any filter $\mathscr{F}$ on Y, $P(\kappa_\mathscr{F}(a_1), \cdots, \kappa_\mathscr{F}(a_n))$ holds in $R[S_\mathscr{F}]/(z)$. However, this follows by applying $\kappa_{\beta,\mathscr{F}}$ to $P(\bar{\eta}_\beta(a_1^{[\beta]}), \cdots, \bar{\eta}_\beta(a_n^{[\beta]}))$ for the appropriate $\beta \in V$.

REMARK 2.2. Obviously, the result can be extended to systems of equations, and the assumption that V is finite can be dropped, as long as the number of variables remains finite. Note that the result actually applies to any statement P about a finite set of elements in a commutative R-algebra whose truth is preserved by R-algebra homomorphisms and which can be tested locally.

REMARK 2.3. If $\beta_1, \beta_2 \in Y$, $\beta_1 \geqq \beta_2$ and $\mathscr{F} = Y^{(\beta_2)}$ then we can construct a $\kappa_{\beta_1,\beta_2} : R[S_{Y(\beta_1)}^{[\beta_1]}] \to R[S_{Y(\beta_2)}^{[\beta_1]}]$ such that $\kappa_{\beta_1,\mathscr{F}} = \kappa_{\beta_2,\mathscr{F}} \circ \kappa_{\beta_1,\beta_2}$ and $\kappa_{\beta_1,\beta_2} \circ \bar{\eta}_{\beta_1} = \bar{\eta}_{\beta_2} \circ i'$, where i' is the inclusion from $R[S^{[\beta_1]}]$ to $R[S^{[\beta_2]}]$, further factoring the maps above.

REMARK 2.4. In some respects, the proposition above is reminiscent of a basic result on Pierce sheaves ([6], Proposition 3.4). It would certainly be interesting if there were a sheaf for arithmetical semigroup rings which implied the result above.

3. **Hermite semigroup rings.** Observe that if S is a union of groups S_α, then Proposition 6.7 of [1] implies that $R[S]$ is Hermite (or Bezout, or an EDR) iff each $R[S_\alpha]$ is likewise. In fact, Corollary 6.9 in the same paper implies that if S is a union of groups, at least one of which is not a torsion group, then $R[S]$ is an EDR iff it is arithmetical (so these conditions are also then equivalent to Bezout and to Hermite). If we continue to restrict ourselves to separative semigroups, there are two directions in which to explore: when is $R[G]$ Hermite (or Bezout, or an EDR) for G a torsion group, or when is $R[S]$ Hermite (etc.) for S separative but not a union of groups? We will deal with the latter question. We first show that $R[S]$ is Bezout if it is arithmetical.

PROPOSITION 3.1. *Let* S *be a separative semigroup with decom-*

position $\bigcup_{\alpha \in Y} S_\alpha$ *which is not a union of torsion groups, and let R be a ring such that $R[S]$ is arithmetical, and let $a, b \in R[S]$ not both 0. If V_0 is the subsemilattice of Y generated by* supp $(a) \cup$ supp (b), *then there exists $d \in R[S]$ such that* supp $(d) \subseteq V_0$ *and* $(a, b)R[S] = dR[S]$. *In particular, $R[S]$ is Bezout.*

Proof. We define d_α by induction, for all $\alpha \in V_0$, assuming $d^{(\alpha)}$ has already been defined so that if $\beta > \alpha$, $\beta \in V_0$ then

$$(\bar{\eta}_\beta(a^{[\beta]}), \bar{\eta}_\beta(b^{[\beta]}))R[S_{Y^{(\beta)}}^{[\beta]}] = \bar{\eta}_\beta(d^{[\beta]})R[S_{Y^{(\beta)}}^{[\beta]}] .$$

Consider the composite $R[S_\alpha] \to R[S^{[\alpha]}] \to R[S_{Y^{(\alpha)}}^{[\alpha]}]$, where the first map is the inclusion (and is not in general unit preserving) and the second is $\bar{\eta}_\alpha$. If S_α is a potent component of S, then this composite is an isomorphism of rings, by the construction of $R[S_{Y^{(\alpha)}}^{[\alpha]}]$; if S_α is nonpotent, then by item (ii) in §2, $R[S_{Y^{(\alpha)}}^{[\alpha]}] \cong R[\hat{S}_0 \cup S_\alpha] \cong R[\hat{S}_0] \oplus R[S_\alpha]$ as R-modules, where $\hat{S}_0$ is a torsion group, and the above composite is just the injection of the $R[S_\alpha]$ factor in the coproduct. Now by the proof of Corollary 6.9 in [1], in either case $R[S_{Y^{(\alpha)}}^{[\alpha]}]$ is an EDR, and thus Bezout.

Let $\tilde{d} \in R[S_{Y^{(\alpha)}}^{[\alpha]}]$ be such that

$$\tilde{d}R[S_{Y^{(\alpha)}}^{[\alpha]}] = (\bar{\eta}_\alpha(a^{[\alpha]}), \bar{\eta}_\alpha(b^{[\alpha]}))R[S_{Y^{(\alpha)}}^{[\alpha]}] .$$

If S_α is potent, it follows from the above that there exists a $d_\alpha \in R[S_\alpha]$ such that $\bar{\eta}_\alpha(d_\alpha) = \tilde{d} - \bar{\eta}_\alpha(d^{(\alpha)})$, so that $\bar{\eta}_\alpha(d^{[\alpha]}) = \bar{\eta}_\alpha(d^{(\alpha)} + d_\alpha) = \tilde{d}$. If S_α is nonpotent, let γ be the minimal element of $V_0 \cap Y^{(\alpha)}$ (if this is empty, let $\gamma = 0$). Also, for any $x \in R[S_{Y^{(\alpha)}}^{[\alpha]}]$, let x_0 be the component of x in $R[\hat{S}_0]$ and let x_α be the $R[S_\alpha]$ component of x, so $x = x_0 + x_\alpha$. By Theorems 4.4 and 5.1 of [1], $R[\hat{S}_0]$ is regular, and by projection onto $R[\hat{S}_0]$, $\tilde{d}_0 R[\hat{S}_0] = (\bar{\eta}_\alpha(a^{[\alpha]})_0, \bar{\eta}_\alpha(b^{[\alpha]})_0)R[\hat{S}_0]$. But $\bar{\eta}_\alpha(a^{[\alpha]})_0 = \kappa_{\gamma,\alpha}(\bar{\eta}_\gamma(a^{[\gamma]}))$ and likewise for b and d. Thus $\tilde{d}_0 R[\hat{S}_0] = \kappa_{\gamma,\alpha}(\bar{\eta}_\gamma(d^{[\gamma]}))R[\hat{S}_0]$, so by regularity, $\tilde{d}_0 u = \kappa_{\gamma,\alpha}(\bar{\eta}_\gamma(d^{[\gamma]}))$ for some unit $u \in R[\hat{S}_0]$. Let $\tilde{\tilde{d}} = \tilde{d}u \in R[S_{Y^{(\alpha)}}^{[\alpha]}]$. Then $(\tilde{\tilde{d}} - \bar{\eta}_\alpha(d^{(\alpha)}))_0 = 0$, so there exists a $d_\alpha \in R[S_\alpha]$ such that $\bar{\eta}_\alpha(d_\alpha) = \tilde{\tilde{d}} - \bar{\eta}_\alpha(d^{(\alpha)})$. Now $\bar{\eta}_\alpha(d^{[\alpha]}) = \tilde{\tilde{d}} = \tilde{d}u$, so $\bar{\eta}_\alpha(d^{[\alpha]})R[S_{Y^{(\alpha)}}^{[\alpha]}] = (\bar{\eta}_\alpha(a^{[\alpha]}), \bar{\eta}_\alpha(b^{[\alpha]}))R[S_{Y^{(\alpha)}}^{[\alpha]}]$ as desired. Since V_0 is finite, by induction d is completely defined with supp $(d) \subseteq V_0$. However, since equality of ideals generated by given elements can be tested locally and is preserved by ring homomorphisms, by Remark 2.2, $(a, b)R[S] = dR[S]$. (Note the testing is done on $V_0 \cup \{0\}$.)

Now let a, b, and d be as above, and let $V_1 = V_0 \cup \{0\}$. V_1 is itself a finite subsemilattice of Y. We want next to establish that at each $R[S_{Y^{(\alpha)}}^{[\alpha]}]$, with $\alpha \in V_1$ there are suitable matrices to be the images of a matrix U such that $[a \quad b]U = [d \quad 0]$. Note first that if $\alpha, \beta \in Y$ correspond to distinct nonpotent components of S, then

$Y^{(\alpha)} \neq Y^{(\beta)}$ since otherwise $S_{Y^{(\alpha)}}$ would not be of special type (Theorem 5.1 in [1] and item (i) in §2). Also, by definition if S_α and S_β are distinct potent components then $Y^{(\alpha)} \neq Y^{(\beta)}$. But if S_α is potent and S_β nonpotent, then $Y^{(\alpha)} = Y^{(\beta)}$ iff α is minimal in $Y^{(\beta)}$, so in particular $\alpha > \beta$.

LEMMA 3.2. *Let R, S, a, b, and d be as in Proposition 3.1, and let $V_1 = \{0\} \cup V_0$. Then there exists a set of 2×2 matrices $\{U_{(\alpha)} | \alpha \in V_1\}$, with $U_{(\alpha)}$ defined over $R[S_{Y^{(\alpha)}}^{[\alpha]}]$, such that*

(i) $\det (U_{(\alpha)}) = 1$ *and*

$$[\bar{\eta}_\alpha(a^{[\alpha]}) \ \ \bar{\eta}_\alpha(b^{[\alpha]})] U_{(\alpha)} = [\bar{\eta}_\alpha(d^{[\alpha]}) \ \ 0]$$

for all $\alpha \in V_1$.

(ii)   *If $\alpha < \beta \in V_1$ and $Y^{(\alpha)} = Y^{(\beta)}$, then*

$$\kappa_{\beta,\alpha}(U_{(\beta)}) = (U_{(\alpha)})_0 .$$

Proof. If there does not exist a $\gamma < \alpha$ such that $\gamma \in V_1$ and $Y^{(\gamma)} = Y^{(\alpha)}$, simply choose $U_{(\alpha)}$ over $R[S_{Y^{(\alpha)}}^{[\alpha]}]$ to satisfy (i), using the previously noted fact that $R[S_{Y^{(\alpha)}}^{[\alpha]}]$ is an EDR, and thus Hermite, and the first remark in §4 of [5]. If there is a $\gamma \in V_1$ such that $\gamma < \alpha$ and $Y^{(\alpha)} = Y^{(\gamma)}$, then by the above comments S_α is potent and $R[S_\alpha] \cong R[S_{Y^{(\alpha)}}^{[\alpha]}]$. But by construction of $S_{Y^{(\gamma)}}^{[\gamma]}$, we must have that $\bar{\eta}_\gamma$ restricts to an isomorphism from $R[S_\alpha \cup S_\gamma]$ to $R[S_{Y^{(\gamma)}}^{[\gamma]}]$ (Proposition 6.4 of [1]). Thus, since $U_{(\gamma)}$ is defined so that $[\bar{\eta}_\gamma(a^{[\gamma]}) \ \ \bar{\eta}_\gamma(b^{[\gamma]})] U_{(\gamma)} = [\bar{\eta}_\gamma(d^{[\gamma]}) \ \ 0]$, we have by taking the component of the identity in $R[S_{Y^{(\gamma)}}^{[\gamma]}]$ that $[\bar{\eta}_\gamma(a^{[\gamma]})_0 \ \ \bar{\eta}_\gamma(b^{[\gamma]})_0](U_{(\gamma)})_0 = [\bar{\eta}_\gamma(d^{[\gamma]})_0 \ \ 0]$ and $\det ((U_{(\gamma)})_0) = 1$. By the maps above, however, $\bar{\eta}_\gamma(a^{[\gamma]})_0 = \kappa_{\alpha,\gamma}(\bar{\eta}_\alpha(a^{[\alpha]}))$, with like results for b and d, and for some $U_{(\alpha)}$ defined over $R[S_{Y^{(\alpha)}}^{[\alpha]}]$, $\kappa_{\alpha,\gamma}(U_{(\alpha)}) = (U_{(\gamma)})_0$, satisfying (ii). By the isomorphism of $R[S_{Y^{(\alpha)}}^{[\alpha]}]$ and $R[(S_{Y^{(\gamma)}}^{[\gamma]})_0]$ and the comments preceding the lemma, $U_{(\alpha)}$ satisfies (i) and is uniquely defined.

We next need a strange-looking technical lemma.

LEMMA 3.3. *Let S be a separative semigroup with decomposition $\bigcup_{\alpha \in Y} S_\alpha$, and suppose for some ring R, $R[S]$ is arithmetical. Suppose $\beta_1, \beta_2 \in Y$ with S_{β_1} and S_{β_2} distinct nonpotent components of S. Then there exists an integer $n \geq 2$, and $\gamma_2, \cdots, \gamma_n, \beta_3, \cdots, \beta_n \in Y$ such that*

(a) $\gamma_i \geq \gamma_j$ *if $i \leq j$,*

(b) $\gamma_i \beta_{i-1} = \beta_{i+1}$ *for all $2 \leq i \leq n-1$,*

(c) $\gamma_i \in Y^{(\beta_i)}$ *for all $2 \leq i \leq n$,*

(d)   *either $\gamma_n \beta_{n-1} = \beta_n$, or $\phi_{\beta_{n-1}, \gamma_n \beta_{n-1}}$ is reduced trivial, or $S_{\gamma_n \beta_{n-1}}$ is a group,*

Proof. Define $\mathscr{F}_i$ for all nonnegative integers i by induction as follows:

(1) $\mathscr{F}_0 = \{0\}$,

(2) If i is even, $\mathscr{F}_{i+1} = \bigcup_{\alpha \in \mathscr{F}_i} Y^{(\alpha\beta_2)}$, and if i is odd, $\mathscr{F}_{i+1} = \bigcup_{\alpha \in \mathscr{F}_i} Y^{(\alpha\beta_1)}$.

It is easy to prove by induction that each $\mathscr{F}_i$ is a filter on Y. We wish to show that $\mathscr{F}_i \subseteq \mathscr{F}_{i+1}$ for all $i \geq 0$. Suppose $\alpha_1 \in \mathscr{F}_i$, say for example i is odd and for some $\alpha_1 \in \mathscr{F}_{i-1}$, $\alpha \in Y^{(\alpha_1\beta_2)}$. If $S_{\alpha_1\beta_2}$ is potent, then $\alpha_2 = \alpha_1\beta_2 \in \mathscr{F}_i$ and $\alpha_2 \in Y^{(\alpha_2\beta_1)}$, so since $\alpha \geq \alpha_2$, $\alpha \in Y^{(\alpha_2\beta_1)} \subseteq \mathscr{F}_{i+1}$. So suppose $S_{\alpha_1\beta_2}$ is nonpotent. Then by item (ii) in §2, there must be some $\alpha_3 \in Y^{(\alpha_1\beta_2)}$ such that $\alpha \geq \alpha_3$ and ϕ_{α,α_3} is reduced trivial. Also $\alpha_3 \in \mathscr{F}_i$, so $Y^{(\alpha_3\beta_1)} \subseteq \mathscr{F}_{i+1}$, but $\phi_{\alpha,\alpha_3\beta_1} = \phi_{\alpha_3,\alpha_3\beta_1} \circ \phi_{\alpha,\alpha_3}$ is reduced trivial, so $\alpha \in Y^{(\alpha_3\beta_1)} \subseteq \mathscr{F}_{i+1}$ as desired. Thus $\mathscr{F}_i \subseteq \mathscr{F}_{i+1}$ and $\mathscr{F} = \bigcup_{i=1}^{\infty} \mathscr{F}_i$ is a filter on Y. Note that it also follows above that if $\beta_2 \notin \mathscr{F}_i$, then either $\alpha \in Y^{(\alpha\beta_1)}$ or $\beta_1 \in Y^{(\alpha_3\beta_1)} \subseteq \mathscr{F}_{i+1}$, since either $\phi_{\alpha,\alpha\beta_1}$ or $\phi_{\alpha\beta_1,\alpha_3\beta_1}$ must be reduced trivial. There are now two cases.

Case 1. $\beta_1, \beta_2 \notin \mathscr{F}$. It is clear from the construction that if $\gamma \in \mathscr{F}$, then $Y^{(\gamma\beta_1)}$ and $Y^{(\gamma\beta_2)}$ are subsets of $\mathscr{F}$. It follows by item (i) in §2 that S_{β_1} and S_{β_2} map to nonpotent components of $S_{\mathscr{F}}$; however, $S_{\mathscr{F}}$ has at most one nonpotent component by Theorem 5.1 of [1]. Thus for some $\gamma \in \mathscr{F}$, $\gamma\beta_1 = \gamma\beta_2$. Let us choose i and γ so that $\gamma \in \mathscr{F}_i$ and i is minimal with respect to containing such a γ. Since $\beta_1 \neq \beta_2$, $i \neq 0$; by induction, there exist $\gamma_2', \cdots, \gamma_i', \gamma_{i+1}' = \gamma$ such that $\gamma_j' \in \mathscr{F}_{j-1}$ and if $2 \leq j \leq i$, then $\gamma_{j+1}' \in Y^{(\gamma_j'\beta_{\delta(j)})}$ where $\delta(j) = 1$ if j is even and $\delta(j) = 2$ if j is odd. Now define $\gamma_j = \gamma_2'\gamma_3' \cdots \gamma_j'$ for all $2 \leq j \leq i+1$, and $\beta_{j+1} = \gamma_j\beta_{j-1} = \gamma_j\beta_{\delta(j)}$ for $2 \leq j \leq i$. Then (a)-(d) of the lemma are easily verified with $n = i + 1$.

Case 2. Either β_1 or β_2 is in $\mathscr{F}$. Let i be chosen to be minimal with respect to having β_1 or β_2 in $\mathscr{F}_{i+1}$. Say for instance, $\beta_1 \in \mathscr{F}_{i+1}$. Then there is a $\gamma \in \mathscr{F}_i$ such that $\beta_1 \in Y^{(\gamma\beta_{\delta(i+1)})}$. Now if $i = 0$, there exists $\gamma_2 \in Y^{(\beta_2)}$ such that $\beta_1 > \gamma_2$ and ϕ_{β_1,γ_2} is reduced trivial, and the lemma holds with $n = 2$. If $i \geq 1$, then as before there exist $\gamma_2', \cdots, \gamma_{i+1}' = \gamma$ such that $\gamma_j' \in \mathscr{F}_{j-1}$ and if $2 \leq j \leq i$ then $\gamma_{j+1}' \in Y^{(\gamma_j'\beta_{\delta(j)})}$. Again define $\gamma_j = \gamma_2' \cdots \gamma_j'$ for $2 \leq j \leq i$. If $\beta_{\delta(i+1)}$ or $\gamma_i\gamma_{i+1}'$ is in $Y^{(\gamma_i\gamma_{i+1}'\beta_{\delta(i+1)})}$, choose $\gamma_{i+1} = \gamma_2' \cdots \gamma_{i+1}'$ likewise. For $\beta_{\delta(i+1)} \in Y^{(\gamma_i\gamma_{i+1}'\beta_{\delta(i+1)})}$, let $n = i + 1$ and define $\beta_3, \cdots, \beta_{i+1}$ as before, and it is again easy to see that (a)-(d) hold. If not, then since $\beta_1 \in Y^{(\gamma\beta_{\delta(i+1)})} \subseteq Y^{(\gamma_{i+1}'\beta_{\delta(i+1)})}$, we must have $\delta(i+1) = 2$, and since $\beta_2 \notin Y^{(\gamma_{i+1}\beta_2)}$, $S_{\gamma_{i+1}\beta_2}$ is nonpotent. Thus if $\gamma_{i+1} = \gamma_i\gamma_{i+1}' \in Y^{(\gamma_i\beta_2)}$, so is $\gamma_{i+1}\beta_1$, so there exists a $\gamma_{i+2} \in Y^{(\gamma_i\beta_2)}$ such that $\beta_1\gamma_{i+1} \geq \gamma_{i+2}$ and $\phi_{\beta_1\gamma_{i+1},\gamma_{i+2}}$ is reduced trivial, by item (ii) in §2. Again defining $\beta_j = \gamma_{j-1}\beta_{j-1} = \gamma_{j-1}\beta_{\delta(j)}$ for all $3 \leq j \leq i+2$,

we can verify that $n = i + 2$, $\gamma_2, \cdots, \gamma_{i+2}, \beta_3, \cdots, \beta_{i+2}$ satisfy (a)-(d) of thelemma.

Thus we are reduced to the case where neither $\gamma_i\gamma'_{i+1}$ nor β_2 is in $Y^{(\gamma_i\gamma'_{i+1}\beta_2)}$. But then $\gamma_i\gamma'_{i+1}\beta_2 = \gamma'_{i+1}\beta_i$ by induction, and $\phi_{\gamma_i\gamma'_{i+1},\gamma_{i+1}\beta_i}$ is reduced nontrivial. Also, if $\beta_1 \in Y^{(\gamma_i\beta_1)}$ then $\beta_1 \in \mathscr{F}_i$ contradicting the minimality of i, so $S_{\gamma_i\beta_1}$ is nonpotent, and furthermore $\gamma_i \in Y^{(\gamma_i\beta_1)}$ by our remark after the proof that $\mathscr{F}_i \subseteq \mathscr{F}_{i+1}$. By hypotheis $\gamma'_{i+1} = \gamma \in Y^{(\gamma'_i\beta_1)} \subseteq Y^{(\gamma_i\beta_1)}$ so $\gamma_i\gamma'_{i+1} \in Y^{(\gamma_i\beta_1)}$, and there is some $\gamma_{i+1} \in Y^{(\gamma_i\beta_1)}$ such that $\gamma_i\gamma'_{i+1} \geqq \gamma_{i+1}$ and $\phi_{\gamma_i\gamma'_{i+1},\gamma_{i+1}}$ is reduced trivial. But then $\phi_{\gamma_i\gamma'_{i+1},\gamma_{i+1}\beta_2}$ is reduced trivial, so since $\phi_{\gamma_i\gamma'_{i+1},\gamma_i\gamma'_{i+1}\beta_2}$ is reduced nontrivial, $\phi_{\gamma_i\gamma'_{i+1}\beta_2,\gamma_{i+1}\beta_2}$ and thus $\phi_{\beta_2,\gamma_{i+1}\beta_2}$ are reduced trivial. Now again it is straightforward to show that $n = i + 1$, $\gamma_2, \cdots, \gamma_{i+1}$, $\beta_3, \cdots, \beta_{i+1}$, with the γ's as above and the β's defined by condition (b), satisfy the lemma. Similar arguments for $\beta_2 \in \mathscr{F}_{i+1}$ complete the proof.

THEOREM 3.4. *Let S be a separative semigroup which is not a union of torsion groups, and let R be a ring such that $R[S]$ is arithmetical. Then $R[S]$ is Hermite.*

Proof. Let $a, b \in R[S]$, and adopt the notation of Proposition 3.1 and Lemma 3.2. We wish to find a 2×2 matrix U over $R[S]$ such that $[a\ b]U = [d\ 0]$ and $\det(U) = 1$. Note that if U is defined and V is a subsemilattice of Y containing $\text{supp}(U) \cup V_1$, then it suffices to know that $[\bar{\eta}_\alpha(a^{[\alpha]})\ \bar{\eta}_\alpha(b^{[\alpha]})]\bar{\eta}_\alpha(U^{[\alpha]}) = [\bar{\eta}_\alpha(d^{[\alpha]})\ 0]$ and $\det(\bar{\eta}_\alpha(U^{[\alpha]})) = 1$ for all $\alpha \in V$, by Proposition 2.1 and Remark 2.2.

For each $\beta \in V_1$, we next wish to choose an element $\Delta(\beta) \in Y$ that is in some sense "sufficiently small" among the elements of $Y^{(\beta)}$. If S_β is potent, let $\Delta(\beta) = \beta$, and if S_β is nonpotent but for some $\gamma \in V_1$ with S_γ potent, $Y^{(\beta)} = Y^{(\gamma)}$, let $\Delta(\beta) = \gamma$. Otherwise, let α be the minimal element of $V_1 \cap Y^{(\beta)}$, and recall $R[S_{Y^{(\beta)}}^{[\beta]}] = R[\hat{S}_0 \cup S_\beta] \cong R[\hat{S}_0] \oplus R[S_\beta]$ where $\hat{S}_0$ is a torsion group, as in the proof of Proposition 3.1, and if $x \in R[S_{Y^{(\beta)}}^{[\beta]}]$, let x_0 and x_β be the respective components of x under the direct sum. Now again for any $y \in R[S]$ with $\text{supp}(y) \subseteq V_1$, we must have $(\bar{\eta}_\beta(y^{[\beta]}))_0 = \kappa_{\alpha,\beta}(\bar{\eta}_\alpha(y^{[\alpha]}))$. Thus $\bar{\eta}_\beta([a\ b]^{[\beta]})_0\kappa_{\alpha,\beta}(U_{(\alpha)}) = \kappa_{\alpha,\beta}(\bar{\eta}_\alpha([a\ b]^{[\alpha]})U_{(\alpha)}) = (\bar{\eta}_\beta([d\ 0]^{[\beta]}))_0 = (\bar{\eta}_\beta([a\ b]^{[\beta]})U_{(\beta)})_0 = \bar{\eta}_\beta([a\ b]^{[\beta]})_0(U_{(\beta)})_0$, and $\det((U_{(\beta)})_0) = \det(\kappa_{\alpha,\beta}(U_{(\alpha)})) = 1$, so $\det(\kappa_{\alpha,\beta}(U_\alpha)^{-1}(U_{(\beta)})_0) = 1$ and $\kappa_{\alpha,\beta}(U_\alpha)^{-1}(U_{(\beta)})_0$ acts as the identity on $(\bar{\eta}_\beta([d\ 0]^{[\beta]}))_0 = [\bar{\eta}_\beta(d^{[\beta]})_0\ 0]$. Since $R[\hat{S}_0]$ is regular, $\kappa_{\alpha,\beta}(U_\alpha)^{-1}(U_{(\beta)})_0$ can be written as a product of elementary matrices over $R[\hat{S}_0]$ (triangular matrices with 1's on the diagonal) chosen so that all above diagonal elements annihilate $\bar{\eta}_\beta(d^{[\beta]})_0$. This follows since the standard Pierce sheaf of a regular ring has fields as its stalks, and over a field this can be done while keeping a bound on the number

of elementary matrices needed (using [6], Proposition 3.4 generalized to systems of equations). But $R[\hat{S}_0] = $ inj. lim. $\{R[tot(S_\gamma)] \mid \gamma \in Y^{(\beta)}\}$, so there exists a $\varDelta(\beta) \in Y^{(\beta)}$ such that $\varDelta(\beta) < \alpha$, all the off-diagonal elements of the elementary matrices are in $\bar{\eta}_\beta(R[tot(S_{\varDelta(\beta)})]) = \bar{\eta}_\beta(R[S_{\varDelta(\beta)}])$, and the elements which map to the above-diagonal elements can be chosen so as to annihilate $\kappa_{\alpha,\varDelta(\beta)}(\bar{\eta}_\alpha(d^{[\alpha]}))$.

Next, we choose our finite subsemilattice V of Y by taking the semilattice generated by V_1, for each $\beta \in V_1$ a $\varDelta(\beta)$ as chosen above, and for every pair $\beta_1, \beta_2 \in V_1$ such that S_{β_1} and S_{β_2} are distinct nonpotent components of S, a sequence $\gamma_2, \cdots, \gamma_n$ which (together with the β's defined by condition (b) of the lemma) satisfy Lemma 3.3. If $\beta \in V_1$ such that S_β is nonpotent, let us define the clan of β to be the set of all $\lambda \in V$ such that $\lambda \leqq \beta$, S_λ is nonpotent, $\phi_{\beta,\lambda}$ is reduced nontrivial, and if $\nu \in V_1$ with $\nu \geqq \lambda$, then $\nu \geqq \beta$. Note that not all elements of V belong to clans.

LEMMA 3.5. (a) *If* $\alpha_1, \alpha_2 \in V$ *such that* α_1 *and* α_2 *belong to different clans, then* $Y^{(\alpha_1)} \cap V \neq Y^{(\alpha_2)} \cap V$. (b) *If* $\alpha_1 \in V$ *belongs to a clan, and* α *is the minimal element of* $Y^{(\alpha_1)} \cap V$, *then* α *does not belong to a clan.*

Proof. (a) Suppose $\beta_1, \beta_2 \in V_1$ such that α_1 belongs to the clan of β_1 and α_2 belongs to the clan of β_2. Let $\gamma_2, \cdots, \gamma_n$ be the elements of V chosen to satisfy Lemma 3.3 for this β_1 and β_2. Suppose $Y^{(\alpha_1)} \cap V = Y^{(\alpha_2)} \cap V$. Then $\gamma_2 \in Y^{(\beta_2)} \cap V \subseteq Y^{(\alpha_2)} \cap V$, so let $2 \leqq i \leqq n$ be maximal such that $\gamma_i \in Y^{(\alpha_2)} \cap V$. If $i < n$ and i is odd, then (in the notation of Lemma 3.3), $\gamma_i\beta_2 = \beta_{i+1} \geqq \alpha_2$, and $\gamma_{i+1} \in Y^{(\beta_{i+1})} \cap V \subseteq Y^{(\alpha_2)} \cap V$, a contradiction. Likewise if $i < n$ and i is even. So suppose $i = n$, and say for example that again i is odd. Then $\gamma_n\beta_{n-1} = \gamma_n\beta_2 \geqq \alpha_2$. If $\gamma_n\beta_{n-1} = \beta_n$, then $\beta_1 \geqq \beta_n \geqq \alpha_2$, so $\alpha_2 \leqq \beta_1\beta_2$, and also $\gamma_n\beta_1 = \beta_n \geqq \alpha_1$, so $\alpha_1 \leqq \beta_1\beta_2$. However, β_1 is the minimal element of V_1 over α_1, and likewise for β_2 and α_2, and since $\beta_1 \neq \beta_2$ and $\beta_1\beta_2 \in V_1$, we have a contradiction. If instead, $\phi_{\beta_{n-1},\gamma_n\beta_{n-1}}$ is reduced trivial, then so is ϕ_{β_2,α_2} since it factors through the former map, again a contradiction. If finally $S_{\gamma_n\beta_{n-1}}$ is a groups, then again to avoid a contradiction $\phi_{\gamma_n\beta_{n-1},\alpha_2}$ must be reduced nontrivial, but then S_{α_2} must be a group (since it is closed under multiplication by $\phi_{\gamma_n\beta_{n-1},\alpha_2}(S_{\gamma_n\beta_{n-1}})$), yet another contradiction. Thus all three options in (d) of Lemma 3.3 are impossible.

(b) Suppose α_2 is the minimal element of $V \cap Y^{(\alpha_1)}$ and α_2 belongs to a clan. Let β_1, β_2 be as in part (a). Note $\beta_1 \neq \beta_2$ since ϕ_{β_2,α_1} factors through ϕ_{α_2,α_1} and is thus reduced trivial, while ϕ_{β_1,α_1} is not. Since $\beta_2 \geqq \alpha_1$, and β_1 is minimal in V_1 over α_1, $\beta_2 > \beta_1$. Again let $\gamma_2, \cdots, \gamma_n$ be the elements of V which satisfy 3.3. In this case we

must have $\beta_1 = \beta_3 = \cdots = \beta_{2m+1}$ and since ϕ_{β_2,β_1} must be reduced trivial, $\beta_2, \beta_4, \cdots, \beta_{2m}$ and $\gamma_2, \gamma_3, \cdots, \gamma_n$ are all in $Y^{(\beta_1)}$ (where $n = 2m$ or $2m + 1$). It follows from 3.3 (d) that n is odd and either $\phi_{\beta_2,\gamma_n\beta_2}$ is reduced trivial or $S_{\gamma_n\beta_2}$ is a group (since $\gamma_n\beta_{n-1} = \gamma_n\beta_2$). But $\gamma_n\beta_2 \in Y^{(\alpha_1)} \cap V$, so $\gamma_n\beta_2 \geqq \alpha_2$. This means either ϕ_{β_2,α_2} is reduced trivial or S_{α_2} is a group, both contradicting the assumption that α_2 belongs to the clan of β_2.

Returning to the proof of the theorem, we are now ready to define U so that $\mathrm{supp}\,(U) \subsetneqq V$, $[a\ b]U = [d\ 0]$, and $\det(U) = 1$. In order to state our induction hypotheses, we will divide V into three subclasses: (1) elements minimal in $Y^{(\alpha)} \cap V$ for α an element of some clan; (2) elements which either belong to a clan or correspond to potent components and do not belong to class (1); and (3) all others. We again define U by induction on $\alpha \in V$, assuming $U^{(\alpha)}$ is already defined.

Induction Hypotheses. If $\alpha \in V$ such that $U^{[\alpha]}$ is defined, then
(i) $\det(\bar{\eta}_\alpha(U^{[\alpha]})) = 1$ and

$$\bar{\eta}_\alpha([a\ b]^{[\alpha]})\bar{\eta}_\alpha(U^{[\alpha]}) = [\bar{\eta}_\alpha(d^{[\alpha]})\ 0]\ .$$

(ii) If α is in class (1), γ is in the clan of β and α is minimal in $Y^{(\gamma)} \cap V$, then

$$\bar{\eta}_\gamma(U^{[\alpha]}) = \kappa_{\beta,\gamma}((U_{(\beta)})_0)\ .$$

(iii) If α is in class (2), and β is the minimal element of V_1 which is $\geqq \alpha$, then

$$\bar{\eta}_\alpha(U^{[\alpha]}) = \kappa_{\beta,\alpha}(U_{(\beta)})\ .$$

(iv) If α is in class (3) and β is the minimal element of $Y^{(\alpha)} \cap V$, then $\bar{\eta}_\alpha(U^{[\alpha]}) = \kappa_{\beta,\alpha}(\bar{\eta}_\beta(U^{[\beta]}))$.

So suppose we are trying to define U_α so that $U^{[\alpha]}$ satisfies these hypotheses, assuming that $U^{[\alpha_1]}$ does for all $\alpha_1 > \alpha$. First suppose α is in class (3), and β is as in (iv). Note S_α is nonpotent so $\beta > \alpha$. Let e_α be the identity element of $tot(S_\alpha)$, and recall from [1] that if $\gamma \geqq \alpha$ but $\gamma \notin Y^{(\alpha)}$, then $e_\alpha S_\gamma \subseteq S_\alpha$. Define $U_\alpha = (U^{[\beta]} - U^{(\alpha)})e_\alpha$ and then (iv) clearly holds. But (i) holds since $[a\ b]^{[\alpha]} = [a\ b]^{[\beta]}$ and $d^{[\alpha]} = d^{[\beta]}$, and we may apply $\kappa_{\beta,\alpha}$ to (i) applied to β.

Next suppose α is in class (2), and β is as in (iii). If S_α is potent, then since $\bar{\eta}_\alpha$ induces an isomorphism from $R[S_\alpha]$ to $R[S_{Y^{(\alpha)}}^{[\alpha]}]$, there exists a unique U_α over $R[S_\alpha]$ such that $\bar{\eta}_\alpha(U_\alpha) = \kappa_{\beta,\alpha}(U_{(\beta)}) - \bar{\eta}_\alpha(U^{(\alpha)})$. If instead α belongs to the clan of β, and γ is the minimal element of $Y^{(\alpha)} \cap V$, then it follows from (ii) that $\kappa_{\beta,\alpha}(U_{(\beta)}) - \bar{\eta}_\alpha(U^{(\alpha)})$ sits inside the summand of $R[S_{Y^{(\alpha)}}^{[\alpha]}]$ which is isomorphic

under $\bar{\eta}_\alpha$ to $R[S_\alpha]$. Again there exists a unique matrix U_α over $R[S_\alpha]$ such that $\bar{\eta}_\alpha(U_\alpha) = \kappa_{\beta,\alpha}(U_{(\beta)}) - \bar{\eta}_\alpha(U^{(\alpha)})$, so in either case (iii) holds. However, (i) now follows since $\bar{\eta}_\beta([a\ b]^{[\beta]})U_{(\beta)} = [\bar{\eta}_\beta(d^{[\beta]})\ 0]$ and $\det(U_{(\beta)}) = 1$, and (i) follows by applying $\kappa_{\beta,\alpha}$.

Finally, suppose that α is in class (1). Let $\{\gamma_1, \cdots, \gamma_n\}$ be the set of all elements τ of V which belong to clans and are such that α is the minimal element of $Y^{(\tau)} \cap V$. By Lemma 3.5, $\gamma_1, \cdots, \gamma_n$ all belong to the clan of the same $\beta \in V_1$, and α does not belong to a clan. Let $K = \bigcap_{i=1}^n \ker(\phi_{\alpha,\gamma_i} \colon S_\alpha \to tot(S_{\gamma_i}))$. It follows readily from Theorem 5.1 of [1] and Theorem 3.6 of [4] that S_α/K is a torsion group and $R[S_\alpha/K]$ is regular. Note that if $\Delta(\beta)$ is the element of V chosen earlier, then $\Delta(\beta) \geqq \alpha$. Also if β_1 is the minimal element of $V_1 \cap Y^{(\alpha)}$, then it is also the minimal element of $V_1 \cap Y^{(\Delta(\beta))}$. There are two cases.

Case 1. S_α potent. Our choice of $\Delta(\beta)$ guarantees the existence of a 2×2 matrix M_β over $R[S_{Y(\Delta(\beta))}^{[\Delta(\beta)]}]$ such that $\bar{\eta}_{\Delta(\beta)}([a\ b]^{[\beta_1]})M_\beta = [\bar{\eta}_{\Delta(\beta)}(d^{[\beta_1]})\ 0]$, $\kappa_{\Delta(\beta),\beta}(M_\beta) = (U_{(\beta)},)_0$, and $\det(M_\beta) = 1$. So choose U_α so that $\bar{\eta}_\alpha(U_\alpha) = \kappa_{\Delta(\beta),\alpha}(M_\beta) - \bar{\eta}_\alpha(W^{(\alpha)})$, and thus $\bar{\eta}_\alpha(U^{[\alpha]}) = \kappa_{\Delta(\beta),\alpha}(M_\beta)$. We have (i) by applying $\kappa_{\Delta(\beta),\alpha}$ to the corresponding equations above, and (ii) holds since

$$\bar{\eta}_{\gamma_i}(U^{[\alpha]}) = \kappa_{\alpha,\gamma_i}(\bar{\eta}_\alpha(U^{[\alpha]})) = \kappa_{\Delta(\beta),\gamma_i}(M_\beta)$$
$$= \kappa_{\beta,\gamma_i}((U_{(\beta)})_0) \ .$$

Case 2. S_α nonpotent. Let β_2 be the minimal element of $Y^{(\alpha)} \cap V$ (note $\beta_1 \geqq \beta_2$). Let $S_{Y(\alpha)}^{[\alpha]}$ have decomposition $\tilde{S}_0 \cup S_\alpha$. We wish to show that there exist elementary matrices $E_1, \cdots, E_j$ over $R[S_{Y(\alpha)}^{[\alpha]}]$, with off-diagonal elements from the $R[S_\alpha]$-summand and above-diagonal elements which annihilate $[\bar{\eta}_\alpha(d^{[\beta_2]})\ 0] = \bar{\eta}_\alpha([a\ b]^{[\beta_2]}U^{[\beta_2]})$, such that $\kappa_{\alpha,\gamma_i}(\bar{\eta}_\alpha(U^{[\beta_2]})E_1 \cdots E_j) = \kappa_{\beta,\gamma_i}((U_{(\beta)})_0)$ for all $1 \leqq i \leqq n$. For if so, $\bar{\eta}_\alpha(U^{[\beta_2]})E_1 \cdots E_j - \bar{\eta}_\alpha(U^{(\alpha)})$ is in the $R[S_\alpha]$-summand, so there is a choice of U_α so that $\bar{\eta}_\alpha(U^{[\alpha]}) = \bar{\eta}_\alpha(U^{[\beta_2]})E_1 \cdots E_j$. In that case, by induction on j, $\det \bar{\eta}_\alpha(U^{[\alpha]}) = 1$ and $\bar{\eta}_\alpha([a\ b]^{[\alpha]})\bar{\eta}_\alpha(U^{[\alpha]}) = [\bar{\eta}_\alpha(d^{[\alpha]})\ 0]$, while condition (ii) will hold by definition of the E_i.

Two show $E_1, \cdots, E_j$ exist as desired, we first show that we can find $E_1', \cdots, E_j'$ over $R[S_{Y(\alpha)}^{[\alpha]}]$ satisfying all requirements except that the off-diagonal elements come from the $R[S_\alpha]$-summand. These are defined in two stages. Since $\mathrm{supp}(d) \cup \mathrm{supp}([a\ b]) \subseteqq V_1$,

$$[\bar{\eta}_\alpha(d^{[\beta_2]})\ 0] = [\bar{\eta}_\alpha(d^{[\beta_1]})\ 0] = \bar{\eta}_\alpha([a\ b]^{[\beta_1]}U^{[\beta_1]})$$
$$= \bar{\eta}_\alpha([a\ b]^{[\beta_1]}U^{[\beta_2]}) \ .$$

Thus $\bar{\eta}_\alpha(U^{[\beta_2]})^{-1}\bar{\eta}_\alpha(U^{[\beta_1]})$ acts as the identity on $\bar{\eta}_\alpha([d\ 0]^{[\beta_2]})$, and since these lie in the $R[\tilde{S}_0]$-summand of $R[S_{Y(\alpha)}^{[\alpha]}]$, which is again regular,

there exist $E'_1, \cdots, E'_l$ elementary matrices over $R[\tilde{S}_0]$ whose above-diagonal elements annihilate $\bar{\eta}_\alpha(d^{[\beta_2]})$ such that $\bar{\eta}_\alpha(U^{[\beta_2]})E'_1 \cdots E'_l = \eta_\alpha(U^{[\beta_1]})$. Now by our choice of $\varDelta(\beta)$, there exist $F_1, \cdots, F_m$ elementary matrices over $R[S_{Y(\varDelta(\beta))}^{[\varDelta(\beta)]}]$ whose above-diagonal elements annihilate $\eta_{\varDelta(\beta)}(d^{[\beta_1]})$ such that

$$(U_{(\beta)})_0 = \kappa_{\varDelta(\beta),\beta}(\kappa_{\beta_1,\varDelta(\beta)}(U_{(\beta_1)})F_1 \cdots F_m)$$
$$= \kappa_{\varDelta(\beta),\beta}(\kappa_{\beta_1,\varDelta(\beta)}(\bar{\eta}_{\beta_1}(U^{[\beta_1]}))F_1 \cdots F_m) \ .$$

Let $j = l + m$, and let $E'_{l+i} = \kappa_{\varDelta(\beta),\alpha}(F_i)$ for all $1 \le i \le m$. Then $E'_1, \cdots, E'_j$ behave as desired.

Now let $k \in K = \bigcap_{i=1}^n \ker(\phi_{\alpha,\gamma_i} : S_\alpha \to tot(S_{\gamma_i}))$, and define $E_i = I + (E'_i - I)k$ for all $1 \le i \le j$ (I the identity matrix), i.e., let E_i be obtained by multiplying the off-diagonal element of E'_i by k. Then $E_1, \cdots, E_j$ still have above-diagonal elements which annihilate $\bar{\eta}_\alpha(d^{[\beta_2]})$. However, all off-diagonal elements are in the $R[S_\alpha]$ summand of $R[S_{Y(\alpha)}^{[\alpha]}]$, and for all $1 \le i \le j$, $1 \le l \le n$, $\kappa_{\alpha,\gamma_i}(E_i) = \kappa_{\alpha,\gamma_i}(E'_i)$, so our other conditions are maintained. As stated above, if we now choose U_α so that $\bar{\eta}_\alpha(U_\alpha) = \bar{\eta}_\alpha(U^{[\beta_2]})E_1 \cdots E_j - \bar{\eta}_\alpha(U^{(\alpha)})$, then (i) and (ii) hold and our induction is complete. By Proposition 2.1, the theorem is proved.

4. The elementary divisor ring case.

THEOREM 4.1. *Let S be a separative semigroup which is not a union of torsion groups, and R a ring. The following are equivalent:*
  (1) *$R[S]$ is arithmetical*
  (2) *$R[S]$ is Bezout*
  (3) *$R[S]$ is Hermite*
  (4) *$R[S]$ is an elementary divisor ring.*

Proof. For any ring, $(4) \Rightarrow (3) \Rightarrow (2) \Rightarrow (1)$. In light of Theorem 3.4 and our comments in §1, it suffices to show that if $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is a matrix over $R[S]$ such that $(a, b, c, d)R[S] = R[S]$, then there exist 2×2 matrices U, W over $R[S]$ such that $UMW = \begin{bmatrix} 1 & 0 \\ 0 & ad - bc \end{bmatrix}$ and $\det(U) = \det(W) = 1$. Again let S have decomposition $\bigcup_{\alpha \in Y} S_\alpha$. This time, let V be the finite subsemilattice of Y generated by $\text{supp}(M)$ (note this contains $0 \in Y$). We shall choose U and W to have support in V, again defining them by induction on $\alpha \in V$, assuming $U^{(\alpha)}$ and $W^{(\alpha)}$ are defined. Our induction assumption to be maintained is that $\det(\bar{\eta}_\alpha(U^{[\alpha]})) = \det(\bar{\eta}_\alpha(W^{[\alpha]})) = 1$ and $\bar{\eta}_\alpha(U^{[\alpha]})\bar{\eta}_\alpha(M^{[\alpha]})\bar{\eta}_\alpha(W^{[\alpha]}) = \begin{bmatrix} 1 & 0 \\ 0 & \bar{\eta}_\alpha((ad - bc)^{[\alpha]}) \end{bmatrix}$.

If S_α is potent, we know that $R[S_{Y(\alpha)}^{[\alpha]}] \cong R[S_\alpha]$ is an EDR, so there exist matrices $\tilde{U}_\alpha$, $\tilde{W}_\alpha$ over $R[S_{Y(\alpha)}^{[\alpha]}]$ such that $\det(\tilde{U}_\alpha) =$

$\det(\widetilde{W}_\alpha) = 1$ and $\widetilde{U}_\alpha \bar{\eta}_\alpha(M^{[\alpha]}) \widetilde{W}_\alpha$ has the desired form. Since $\bar{\eta}_\alpha$ restricts to an isomorphism from $R[S_\alpha]$ to $R[S_{\gamma(\alpha)}^{[\alpha]}]$ in this situation, we may choose U_α and W_α so that $\bar{\eta}_\alpha(U_\alpha) = \widetilde{U}_\alpha - \bar{\eta}_\alpha(U^{(\alpha)})$ and $\bar{\eta}_\alpha(W_\alpha) = \widetilde{W}_\alpha - \bar{\eta}_\alpha(W^{(\alpha)})$. The induction hypothesis is then clearly maintained.

To handle the case where S_α is nonpotent, we need the following lemma.

LEMMA 4.2. *Let R_1 be a regular ring, $M(X)$ a 2×2 matrix of elements of the polynomial ring $R_1[X]$ whose elements generate the unit ideal, and U_0, W_0 2×2 matrices over R_1 such that $\det(U_0) = \det(W_0) = 1$ and $U_0 M(0) W_0 = \begin{bmatrix} 1 & 0 \\ 0 & \det(M(0)) \end{bmatrix}$. Then there exist 2×2 matrices $U(X)$, $W(X)$ over $R_1[X]$ such that $U(0) = U_0$, $W(0) = W_0$, $\det(U(X)) = \det(W(X)) = 1$, and $U(X)M(X)W(X) = \begin{bmatrix} 1 & 0 \\ 0 & \det(M(X)) \end{bmatrix}$.*

Proof. An application of the basic theorem on Pierce sheaves ([6], Proposition 3.4) reduces the lemma to the case where R_1 is a field. In that case $R_1[X]$ is an EDR, so there exist matrices $\widetilde{U}(X)$, $\widetilde{W}(X)$ over $R[X]$, with $\det(\widetilde{U}(X)) = \det(\widetilde{W}(X)) = 1$ and $\widetilde{U}(X)M(X)\widetilde{W}(X)$ as desired, so by replacing $M(X)$ by $\begin{bmatrix} 1 & 0 \\ 0 & \det(M(X)) \end{bmatrix}$, U_0 by $U_0\widetilde{U}(0)^{-1}$, and W_0 by $\widetilde{W}(0)^{-1}W_0$ we may assume $M(X)$ already has the desired form, and $U_0 M(0) W_0 = M(0)$. Let $f(X) = \det(M(X))$. Once again, we have two cases.

Case 1. $f(0) \neq 0$. We show that there exist matrices $U(X)$, $\widetilde{W}(X)$ over $R[X]$ such that $U(0) = U_0$, $\det(U(X)) = \det(\widetilde{W}(X)) = 1$ and $U(X)M(X)\widetilde{W}(X) = M(X)$. It then will follow that $\widetilde{W}(0) = W_0 = M(0)^{-1}U(0)^{-1}M(0)$, so we may choose $W(X) = \widetilde{W}(X)$.

To prove this simpler statement, since U_0 can be written as a product of elementary matrices, by induction we may assume U_0 is an elementary matrix. The verification that $U(X)$ and $\widetilde{W}(X)$ can be chosen in this situation is left to the reader.

Case 2. $f(0) = 0$. In this case we must have for some $a, b, c \in R_1$ that $U_0 = \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix}$ and $W_0 = \begin{bmatrix} a^{-1} & 0 \\ c & a \end{bmatrix}$. Then $U(X) = \begin{bmatrix} a & b \\ -cf & a^{-1}(1-bcf) \end{bmatrix}$ and $W(X) = \begin{bmatrix} a^{-1}(1-bcf) & -bf \\ c & a \end{bmatrix}$ satisfy the lemma.

To apply the lemma to the proof of the theorem, let $R[S_{\gamma(\alpha)}^{[\alpha]}] \cong R[\widehat{S}_0] \oplus R[S_\alpha]$ be the usual decomposition and let $K = \ker(\widehat{\phi}_{0,\alpha} \colon \widehat{S}_0 \to tot(S))$, where $\widehat{\phi}_{0,\alpha}$ is the structure map for $S_{\gamma(\alpha)}^{[\alpha]}$. Then as in Theorem 4.4 of [1], we have a semigroup $(\widehat{S}_0/K) \cup S_\alpha$, and a natural surjection $\rho \colon R[S_{\gamma(\alpha)}^{[\alpha]}] \to R[(\widehat{S}_0/K) \cup S_\alpha]$. Observe that $R[(\widehat{S}_0/K) \cup S_\alpha] \cong R[\widehat{S}_0/K] \oplus R[S_\alpha]$ as $R[\widehat{S}_0/K]$-modules, and the induced map on the

$R[S_\alpha]$ summands is the identity. As in the proof of Corollary 4.5 of [1], any finite subset of $(\hat{S}_0/K) \cup S_\alpha$ is contained in a subsemigroup isomorphic to $(\hat{S}_0/K) \times Z^+$, where Z^+ is the nonnegative integers under addition. Pick such a subsemigroup containing all elements which occur in $\rho(\bar{\eta}_\alpha(M^{[\alpha]}))$. Now $R[(\hat{S}_0/K) \times Z^+] \cong (R[\hat{S}_0/K])[X]$ and again $R[\hat{S}_0/K]$ is regular. Apply the lemma to find $\tilde{U}_\alpha$, $\tilde{W}_\alpha$ in $R[(\hat{S}_0/K) \cup S_\alpha]$ such that $\det(\tilde{U}_\alpha) = \det(\tilde{W}_\alpha) = 1$, $\tilde{U}_\alpha \rho(\bar{\eta}_\alpha(M^{[\alpha]}))\tilde{W}_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & \det(\rho(\bar{\eta}_\alpha(M^{[\alpha]}))) \end{bmatrix}$, and $(\tilde{U}_\alpha)_0 = \rho(\bar{\eta}_\alpha(U^{[\beta]}))$, $(\tilde{W}_\alpha)_0 = \rho(\bar{\eta}_\alpha(W^{[\beta]}))$, where of course $(\tilde{U}_\alpha)_0$ and $(\tilde{W}_\alpha)_0$ are the components of $\tilde{U}_\alpha$ and $\tilde{W}_\alpha$ in the $R[S_0/K]$ summand. Thus $\tilde{U}_\alpha - \rho(\bar{\eta}_\alpha(U^{(\alpha)}))$ is in the $R[S_\alpha]$ summand, so there is a (unique) U_α such that $\rho(\bar{\eta}_\alpha(U_\alpha)) = \tilde{U}_\alpha - \rho(\bar{\eta}_\alpha(U^{(\alpha)}))$. Likewise we have W_α such that $\rho(\bar{\eta}_\alpha(W_\alpha)) = \tilde{W}_\alpha - \rho(\bar{\eta}_\alpha(W^{(\alpha)}))$. Now calculating the values in each component of $R[S^{[\alpha]}_{\gamma(\alpha)}]$, one can see that $\det(\bar{\eta}_\alpha(U^{[\alpha]})) = \det(\bar{\eta}_\alpha(W^{[\alpha]})) = 1$, and $\bar{\eta}_\alpha(U^{[\alpha]})\bar{\eta}_\alpha(M^{[\alpha]})\bar{\eta}_\alpha(W^{[\alpha]})$ is also as desired. The theorem is proved.

REMARK 4.3. It can be shown in like manner that in any situation where we have a statement of the form $P(x_1, \cdots, x_m, y_1, \cdots, y_n)$ satisfying the conditions of Remark 2.2 and the analogue of Lemma 4.2, and $R[S]$ is arithmetical with S separative and not a union of torsion groups, then we can prove a theorem analogous to the standard result for Pierce sheaves (Proposition 3.4 of [6]). Specifically, suppose that whenever K is a field and $x_1, \cdots, x_m \in K[X, X^{-1}]$, there exist $y_1, \cdots, y_n \in K[X, X^{-1}]$ such that $P(x_1, \cdots, x_m, y_1, \cdots, y_n)$ is true, and further that if $f_1(X), \cdots, f_m(X) \in K[X]$, $c_1, \cdots, c_n \in K$ with $P(f_1(0), \cdots, f_m(0), c_1, \cdots, c_n)$ true in K, then the c_i's are the constant terms of polynomials $g_i(X) \in K[X]$ such that $P(f_1, \cdots, f_m, g_1, \cdots, g_n)$ is true in $K[X]$. Then for any $x_1, \cdots, x_m \in R[S]$, there exist $y_1, \cdots, y_n \in R[X]$ such that $P(x_1, \cdots, x_m, y_1, \cdots, y_n)$ is true in $R[S]$. Also, the y_i's can be chosen to have support contained in the subsemilattice generated by $\bigcup_{i=1}^{m} \text{supp}(x_i) \cup \{0\}$. The reason for the difficulties encountered in §3 is precisely that the condition about extending solutions from K to $K[X]$ fails for the equations describing the Hermite condition.

REFERENCES

1. L. G. Chouinard, B. R. Hardy, and T. S. Shores, *Arithmetical and semihereditary semigroup rings*, Commun. Alg., (1980), 1593–1652.
2. A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, vol. I. 2nd edition. Amer. Math. Soc., Providence, R. I., 1964.
3. R. Gilmer and T. Parker, *Semigroup rings as Prüfer rings*, Duke Math. J., **41** (1974), 219–230.
4. B. R. Hardy and T. S. Shores, *Arithmetical semigroup rings*, preprint.
5. I. Kaplansky, *Elementary divisors and modules*, Trans. Amer. Math. Soc., **66** (1949),

464-491.

6. R. S. Pierce, *Modules over commutative regular rings*, Memoirs Amer. Math. Soc., **70** (1967).

Received June 5, 1980.

UNIVERSITY OF NEBRASKA-LINCOLN
LINCOLN, NE 68588