Zero-Dimensional Commutative Rings
ed. D.F. Anderson, D.E. Dobbs
Lecture Notes in Pure and Applied Mathematics
Volume 171, Marcel Dekker
p. 223 - 239, 1995

18 Splitting Rings for *p*-Local Torsion-Free Groups

Sarah Glaz University of Connecticut, Storrs, Connecticut

Charles Vinsonhaler University of Connecticut, Storrs, Connecticut

William Wickless University of Connecticut, Storrs, Connecticut

0 INTRODUCTION

The concept of a splitting ring dates back to Szekeres (1948). The motivation for his work was the fact that the ring of p-adic integers, $\hat{Z}_p$, "splits" any torsion-free finite rank abelian group G in the sense that $\hat{Z}_p \otimes_Z G$ is isomorphic to the direct sum of a free and a divisible $\hat{Z}_p$-module. Here, a torsion-free abelian group G is an additive subgroup of a vector space over the field of rational numbers Q; and the rank of G is the dimension of the subspace spanned by G. If Δ is any subfield of the field of p-adic numbers, $\hat{Q}_p$, and $R = \Delta \cap \hat{Z}_p$, then Szekeres called Δ a splitting field for G if $R \otimes_Z G$ is isomorphic to the direct sum of a free and a divisible R-module. For our purposes, an R-module M is divisible if $nM = M$ for all nonzero integers n; every R-module M contains a unique maximal divisible submodule div(M); and M is reduced if $\text{div}(M) = 0$. The main result in (Szekeres 1948) is that each G has a unique minimal splitting field.

In a series of papers, Lady made an extensive study of splitting fields and splitting rings. In Lady (1977, 1980a, 1980b) he works with torsion-free modules over a discrete valuation domain V. In this context a splitting ring R for a V-module G is a pure subring of the completion of V such that the reduced tensor product $R * G = (R \otimes_V G)/\mathrm{div}(R \otimes_V G)$ is a finitely generated R-module. In Lady (1983) he obtains global results, working with modules over a Dedekind domain W with quotient field Q(W). Here a splitting ring is a reduced torsion-free commutative W-algebra I such that p-rank $I = \dim_{W/p}(I/pI) = 1$ for all prime ideals p of W; and I is quasi-isomorphic (defined below) to the product of W-algebras $W_1 \times \ldots \times W_t$, where each W_i is a Dedekind domain such that $Q(W)W_i$ is a field. Lady's general approach is to consider the W-modules split by a fixed splitting ring I.

In this paper we follow a different path by fixing a torsion-free reduced Z_p-module G of finite p-rank and considering splitting rings for G. Here Z_p denotes the localization of the ring of integers at a fixed prime p; and the p-rank of G is the Z/pZ-dimension of G/pG. For us a splitting ring for G is a commutative Z_p-algebra R whose additive group is torsion-free reduced of finite p-rank. We say that such an R splits G if the reduced tensor product $R * G$ is quasi-isomorphic to a free R-module, that is, $R * G$ contains a free R-module F such that $(R * G)/F$ is finite. We have chosen to work with Z_p-modules for the sake of simplicity. Our results extend immediately to modules over a discrete valuation ring.

Every torsion-free Z_p-module G contains a p-basic submodule, that is, a free Z_p-submodule B such that G/B is torsion-free divisible. We call a submodule B of G **pure** whenever G/B is torsion-free. To each p-basic submodule B of G we associate a "canonical splitting ring" R_B which is a pure subring of $\hat{Z}_p$. While R_B depends on B as well as G, we show that all the R_B's have a common field of quotients Δ (Corollary 2.5). This Δ is just the splitting field of Szekeres -- seen from a different point of view. We show that there exist minimal canonical splitting rings if G has finite rank (Theorem 3,6). On the other hand, not every splitting ring will contain a canonical one (Example 4.1). However, if R is a splitting ring for G such that the additive group R+ of R has finite rank, then R contains a unique minimal canonical splitting ring S, and $S \simeq R_B$ for each p-basic submodule B of G (Theorem 4.5).

Throughout, we work in the category of reduced torsion-free Z_p-modules of finite p-rank and quasi-homomorphisms. The objects of this category are called simply p-local groups. Let G and H be p-local groups. The group of quasi-homomorphisms from G to H is QHom(G,H). Two subgroups G and H of a group K are quasi-equal ($G \doteq H$) provided $nG \subseteq H$ and $nH \subseteq G$ for some non-zero integer n. If G and H are p-local groups, then we can assume $n = p^r$ for some $r \geq 0$. In this case, G/nH and H/nG are finite p-groups. Quasi-isomorphism ($\dot{\cong}$) and quasi-containment ($\dot{\subset}$) are defined similarly. If X is a subset of a group G, we use $\langle X\rangle_*$ for the pure subgroup generated by X and write A is quasi-pure in B to mean that $A \doteq \langle A \cap B\rangle_*$, the purification being taken in B. The Q-subspace generated by a torsion-free group G is written QG. If R is a torsion-free ring then QR is endowed with the natural ring structure.

All rings are commutative with identity and subrings are assumed to contain the identity. If R is a ring, a divisible R-module is an R-module M such that M+ is a divisible group. A ring R is called a p-local ring if R+ is a p-local group. For a p-local ring R, $\hat{R}$ denotes the p-adic completion of R and R is regarded as a subring of $\hat{R}$. All unadorned tensor products are taken over Z and, if G is a group and R is a ring, then $R \otimes G$ is endowed with the natural R-module structure.

1 SPLITTING RINGS FOR p-LOCAL GROUPS

Throughout, G is a reduced p-local torsion-free abelian group of finite p-rank $r = r(G)$. As previously noted, we will refer to G simply as a "p-local group." For such a G, it is well known that the ring $\hat{Z}_p$ splits G in the sense that $\hat{Z}_p \otimes G \cong \hat{Z}_p^r \oplus D$, where D is a divisible $\hat{Z}_p$-module. This fact motivates our first definition.

DEFINITION 1.1 Let G be a p-local group and let R be a p-local ring. We say that R **splits** G if, as an R-module, $R \otimes G \doteq R^t \oplus D$, where t is a positive integer and D is a divisible R-module. We also call such an R a **splitting ring** for G.

In this section we present some simple facts, most of them easy generalizations of results contained in Lady (1977-83), on splitting rings.

LEMMA 1.2 Let G be a p-local group and let R and S be p-local rings.
(a) If R is quasi-isomorphic to a subring of S and R splits G then so does S.
(b) If R splits G then so does R/I where I is any ideal of R.
(c) If $R \otimes G \doteq R^t \oplus D$, then $t = r = $ p-rank G.

Proof: (a) Wolog, assume $R \subseteq S$. If $R \otimes G \doteq R^t \oplus D$, where D is a divisible R-module, then apply $S \otimes_R \_\_$ to obtain $S \otimes G \doteq S^t \oplus (S \otimes_R D)$.

(b) If $R \otimes G \dot{\simeq} R^t \oplus D$ then apply $R/I \otimes_R$ — .

(c) Let $R \otimes G \dot{\simeq} R^t \oplus D$. Then there is an exact sequence of R-modules $0 \to R^t \oplus D \to R \otimes G \to A \to 0$, where A is finite. Since $R^t \oplus D$ and $R \otimes G$ are torsion-free of finite p-rank it follows that p-rank$(R^t \oplus D)$ = p-rank$(R \otimes G)$. But p-rank$(R^t \oplus D)$ = t(p-rank R) and p-rank$(R \otimes G)$ = (p-rank R)(p-rank G) = r(p-rank R). Since p-rank $R < \infty$ we have $t = r$.

Note that if R is any ring such that R splits G then R must automatically be p-local because G is. Further, Lemma 1.2(b) allows us to add the standing assumption that all "p-local rings" are torsion-free and reduced.

THEOREM 1.3 (Lady 1977, Theorem 4.1) Let R be a p-local ring and let G be a p-local group of p-rank r. Then R splits G if and only if G is isomorphic to a subgroup G' of R^r such that G' is quasi-pure in R^r and $RG' \doteq R^r$.

Proof: The proof, identical to that in Lady (1977), is included for the reader's convenience. Suppose $\phi : R \otimes G \to R^t \oplus D$ is an R-quasi-isomorphism. By Lemma 1.2(c), $t = r =$ p-rank G. Let $\pi : \phi(R \otimes G) \to R^r$ be quasi-projection and let $G' = \pi\phi(1 \otimes G)$. We have $G' \dot{\subseteq} R^r$ and, since $\pi\phi$ is an R-map, $RG' \doteq R^r$. Additionally, $1 \otimes G$ is pure in $R \otimes G$ since $pR \neq R$. Hence $\phi(1 \otimes G)$ is quasi-pure in $R^r \oplus D$ and, since $\phi(1 \otimes G)$ is reduced, $\phi(1 \otimes G) \cap D = (0)$. It follows that $G' \cong G$ and that G' is quasi-pure in R^r.

Conversely, let G be quasi-pure in R^r with $RG \doteq R^r$. Define $\theta : R \otimes G \to R^r$ by $\theta(r \otimes g) \to rg$. Then θ is an R-quasi-epimorphism, hence quasi-splits. That is $R \otimes G \doteq F \oplus K$, where $F \cong R^r$ and $K = \mathrm{Ker}\, \theta$. But, since p-rank $R < \infty$, we must have p-rank $K = 0$, i.e., K is divisible.

COROLLARY 1.4 (Lady 1977, Corollary 2.2) Let R be a pure subring of $\hat{Z}_p$. Then R splits R+.

Proof: In this case p-rank R+ = 1 and R is pure in R, so Theorem 1.3 applies.

2 CANONICAL SPLITTING RINGS

Let G be a p-local group. In this section, for each p-basic submodule $B \subseteq G$, we construct a canonical splitting ring R_B. These rings R_B, in general, will depend on B, but all of them will have a common field of quotients Δ. The field Δ will be the p-local splitting field for G as defined in Szekeres (1948). See also Turgi (1977) and Lady (1977). Our original motivation was to investigate the connection between p-basic submodules and splitting rings. The main result, Theorem 2.2, is a key to the results in Sections 3 and 4. A byproduct is a simple proof of Szekeres' original theorem.

To each p-basic submodule B of G, we associate a unique splitting ring R_B as follows. The exact sequence

$$0 \to B \to G \to D \to 0$$

where D is p-torsion-free and divisible, induces a split exact sequence of $\hat{Z}_p$-modules

$$0 \to \hat{Z}_p \otimes B \overset{f}{\leftrightarrows} \hat{Z}_p \otimes G \to \hat{Z}_p \otimes D \to 0.$$

Note that since $\hat{Z}_p \otimes B$ is p-reduced, the splitting map $f : \hat{Z}_p \otimes G \to \hat{Z}_p \otimes B$ is uniquely determined by the fact that the restriction of f to $\hat{Z}_p \otimes B$ is the identity. Define R_B to be the smallest pure subring of $\hat{Z}_p$ such that $f(1 \otimes G) \subseteq R_B \otimes B$. If R and S are two pure subrings of $\hat{Z}_p$, then $(R \cap S) \otimes B = (R \otimes B) \cap (S \otimes B)$, so that $R_B = \cap\{R \mid R$ is a pure subring of $\hat{Z}_p$ and $f(1 \otimes G) \subseteq R \otimes B\}$. This equality demonstrates both the existence and the uniqueness of R_B.

We now have an induced exact sequence

$$(*) \qquad 0 \to R_B \otimes B \to R_B \otimes G \to R_B \otimes D \to 0.$$

Moreover, the restriction of the map f to $R_B \otimes G$ provides an R_B-module splitting of (*), since $f(R_B \otimes G) = R_B f(1 \otimes G) \subseteq R_B(R_B \otimes B) = R_B \otimes B$. Clearly, $R_B \otimes B$ is a free R_B-module, while $R_B \otimes D$ is a torsion-free divisible R_B-module. It follows that R_B is a splitting ring for G.

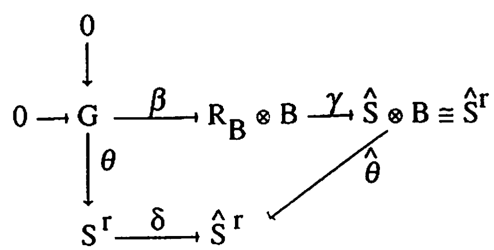
Note that if X is a maximal Z-independent subset of G then R_B is the smallest pure subring of $\hat{Z}_p$ such that $f(1 \otimes X) \subseteq R_B \otimes B$. In particular, this implies the following result which also appears in Szekeres (1948), Turgi (1977) and Lady (1977).

PROPOSITION 2.1 Let G be a p-local group of finite rank. Then, for each p-basic submodule $B \subseteq G$, R_B is purely finitely generated as a subring of $\hat{Z}_p$.

Our next theorem allows us to derive the main result of Szekeres (1948).

THEOREM 2.2 Let B be a p-basic submodule of a p-local group G and let S be a splitting ring for G. Then there is an element $u \in S$ such that u is a unit in $Q\hat{S}$ and such that R_B is isomorphic to a subring of $S[u^{-1}]$.

Proof: Let $r = \text{p-rank } G$ and consider the diagram,



The pure embedding β is the composition of the natural embedding $G \to 1 \otimes G$ and the splitting map f from the definition of R_B. The pure embedding γ comes from the natural inclusion of $\hat{Z}_p$ in $\hat{S}$. The embedding θ is derived as in Theorem 1.3 from the fact that S is a splitting ring for G, and δ is the canonical embedding. We will use also that $S\theta(G) \doteq S^r$. The lifting $\hat{\theta}$, of θ, is the unique $\hat{S}$-map which makes the diagram commute. That is, $\hat{\theta}$ is the $\hat{S}$-map satisfying $\hat{\theta}\gamma\beta = \delta\theta$.

The homomorphism $\hat{\theta}$ can be represented as a matrix $A \in \mathrm{Mat}_r(\hat{S})$ with respect to a basis for $1 \otimes B$ in $\hat{S} \otimes B$ and the canonical basis for $\hat{S}^r$. Indeed, since $\hat{\theta}(1 \otimes B) = \theta(B) \subseteq S^r$, $A \in \mathrm{Mat}_r(S)$. As noted above, $S\theta(G) \doteq S^r$, so that $\hat{S}\hat{\theta}(1 \otimes B) \doteq \hat{S}^r$. It follows that the map $\hat{\theta}$ is a quasi-isomorphism. Let A^{-1} be the matrix for the quasi-isomorphism $\hat{\theta}^{-1}$ with respect to the same bases used for A. Then $A^{-1} \in \mathrm{Mat}_r(Q\hat{S})$, and $u = \det A \in S$ is a unit in $Q\hat{S}$. However, $A^{-1} = u^{-1}(\mathrm{adj}\, A)$, so $A^{-1} \in \mathrm{Mat}_r(S[u^{-1}])$. The latter implies that $\gamma\beta(G) \subseteq \gamma(R_B \otimes B) \cap A^{-1}(S^r) \subseteq S[u^{-1}] \otimes B$. Since B is free and $\gamma: R_B \otimes B \to \hat{S} \otimes B$ is the natural inclusion map, it follows that R_B is isomorphic to a subring of $S[u^{-1}]$ and the proof is complete.

COROLLARY 2.3 Let B be a p-basic submodule of a p-local group G and let S

be a pure subring of $\hat{Z}_p$ which splits G. Then $R_B \subseteq \Omega(S)$, where $\Omega(S)$ is the quotient field of S taken in the field $\hat{Q}_p$.

Proof: Applying Theorem 2.2, $R_B \subseteq S[u^{-1}] \subseteq \Omega(S) \subseteq \hat{Q}_p$.

The equivalence of (a) and (b) in the next corollary appears as Proposition 1.21 in Lady (1983).

COROLLARY 2.4 Let G be a p-local group of p-rank r and R a p-local ring such that QR is a field. The following are equivalent.

(a) R splits G.

(b) G is quasi-isomorphic to a pure subgroup of R^r.

(c) For every basic submodule B of G, $R_B \subset R$.

Proof: The statement (a) implies (b) is Theorem 1.3; and (c) implies (a) is Lemma 1.2(a). For (b) implies (c), let B be a p-basic submodule of G and suppose G is quasi-equal to a pure subgroup of R^r. Then RB is a free R-submodule of R^r of rank r. Since QR is a field, it follows that $RB \doteq R^r$. Thus, $RG \doteq R^r$ and R is a splitting ring for G by Theorem 1.3. Therefore, by Corollary 2.3, $R_B \subset \Omega(R) = QR$. Also, $R_B \subset \hat{Z}_p \subset \hat{R}$. Since $\hat{R} \cap QR = R$, $R_B \subset R$.

Following Szekeres (1948), a subfield $\Delta \subseteq \hat{Q}_p$ is called a splitting field for G if $\Delta \cap \hat{Z}_p$ is a splitting ring for G. Szekeres originally defined Δ to be a splitting field for G if $R * G$ is a finite rank free R-module where $R = \Delta \cap \hat{Z}_p$. Our definition of a splitting ring R for G only requires that $R * G$ be quasi-equal to a finite rank free R-module. However, if $R = \Delta \cap \hat{Z}_p$ for some subfield $\Delta \subseteq \hat{Q}_p$, then $R+$ has p-rank one, so any R-module quasi-equal to R is isomorphic to R. It follows that any R-module quasi-equal to a free R-module is free. Thus, our definition of splitting field, restricted to his context, coincides with that of Szekeres.

COROLLARY 2.5 (Szekeres 1948, Theorem 3). Let G be a p-local group with p-basic submodule B and let $\Delta = \Omega(R_B) \subset \hat{Q}_p$. Then Δ is a unique minimal splitting field for G (and, thus, is an invariant of G).

Proof: Let $\Delta = \Omega(R_B)$ and let $K \subseteq \hat{Q}_p$ be a splitting field for G. Then $K \cap \hat{Z}_p$ is a splitting ring so, by Corollary 2.3, $R_B \subseteq \Omega(K \cap \hat{Z}_p)$. Hence $\Delta \subseteq K$.

In particular, Corollary 2.5 implies that $\Omega(R_B) = \Omega(R_{B'})$ for any p-basic submodules $B, B' \subseteq G$. If Δ is algebraic over the rational number field Q we can conclude $R_B = R_{B'}$.

COROLLARY 2.6 Let G be a p-local group and suppose that $\Delta = \Delta(G)$ is algebraic over Q. Then $R_B = R_{B'}$ for all p-basic submodules $B, B' \subseteq G$.

Proof: Since $R_B, R_{B'} \subseteq \Delta \subseteq \hat{Q}_p$ and Δ/Q is algebraic, then $\Omega(R_B) = QR_B$, $\Omega(R_{B'}) = QR_{B'}$, where QR_B, $QR_{B'}$ are the divisible hulls of R_B, $R_{B'}$ in $\hat{Q}_p$. Furthermore, R_B and $R_{B'}$ are pure in $\hat{Z}_p$. Thus, $R_B = QR_B \cap \hat{Z}_p = \Omega(R_B) \cap \hat{Z}_p = \Omega(R_{B'}) \cap \hat{Z}_p = QR_{B'} \cap \hat{Z}_p = R_{B'}$.

EXAMPLE 2.7 Let G be the pure subgroup of $\hat{Z}_p$ generated by $1, \alpha$ and α^2, where α is a transcendental p-adic unit. Let $B = \langle 1 \rangle$ and $B' = \langle \alpha \rangle$. Plainly, B and B' are p-basic submodules of G. It is easy to see that R_B is the pure subring of $\hat{Z}_p$ generated by 1 and α, while $R_{B'}$ is purely generated by $1, \alpha$ and α^{-1}. Thus, R_B is properly contained in $R_{B'}$. Note, however, that the quotient fields of R_B and $R_{B'}$ coincide.

3 MINIMAL CANONICAL SPLITTING RINGS

In this section we investigate the existence of minimal canonical splitting rings for a group G. A canonical splitting ring R_B is called **minimal** if no canonical splitting ring is properly contained in R_B. Example 2.7 shows that not all canonical splitting rings are minimal. However, there are useful criteria for determining containment relationships between canonical splitting rings.

Let B and B' be p-basic submodules of the p-local group G and denote $R = R_B$, $R' = R_{B'}$. We will employ the following diagram:

$$\begin{array}{ccc} \hat{Z}_p \otimes B & \underset{e}{\overset{f}{\leftrightarrows}} & \hat{Z}_p \otimes G \\ \uparrow \gamma & & \uparrow 1 \\ \hat{Z}_p \otimes B' & \underset{e'}{\overset{f'}{\leftrightarrows}} & \hat{Z}_p \otimes G \end{array}$$

Here f, f' are the unique splitting maps for the natural inclusion maps e, e' and the isomorphism γ makes the diagram commute.

By choosing bases for $1 \otimes B \subseteq \hat{Z}_p \otimes B$ and $1 \otimes B' \subseteq \hat{Z}_p \otimes B'$, we can represent the isomorphism γ by a matrix $C \in \mathrm{Mat}_r(R)$ as in the proof of Theorem 2.2. Similarly γ^{-1} can be represented by $C^{-1} \in \mathrm{Mat}_r(R')$. Moreover, if $u = \det C^{-1}$, then $R \subseteq R'[u^{-1}] = R'[\det C]$. The next lemma follows directly.

LEMMA 3.1 The following are equivalent:

(a) $R \subseteq R'$

(b) $C \in \mathrm{Mat}_r(R')$

(c) $\det C \in R'$

LEMMA 3.2 Continuing with the same notation, let $d = \det C$. Then R is properly contained in R' if and only if $d \in (R')^* \backslash R^*$, where * denotes the multiplicative group of units in a ring.

Proof: We have $d \in R$, $d^{-1} = \det C^{-1} \in R'$. In view of Lemma 3.1, $R \subsetneqq R'$ (proper containment) if and only if $d \in R'$ and $d^{-1} \notin R$. Thus, $R \subsetneqq R'$ if and only if $d \in (R')^* \backslash R^*$.

LEMMA 3.3 Suppose $R \subsetneqq R'$. Then $(R')^*/R^*$ is infinite.

Proof: By Lemma 3.2, if $R \subsetneqq R'$ then $d \in (R')^* \backslash R^*$. Since $d \in R$, we must have $\{d^j \mid j \in Z\} \cap R^* = \{1\}$. Otherwise $d^j \in R$ for some $j > 0$, whence $d^{-1} = d^j d^{(-1-j)} \in R$ and $d \in R^*$, a contradiction.

Let QR, QR' be the divisible hulls of R, R' taken in $\hat{Q}_p$. Then QR, QR'

are subrings of $\hat{Q}_p$ and we have:

LEMMA 3.4 Suppose $R \subsetneq R'$. Then $(QR')^*/(QR)^*$ is infinite.

Proof: By Lemma 3.3, $(R')^*/R^*$ is infinite. Moreover, $(QR)^* = QR^*$ and since R is pure in R' , $R' \cap QR = R$. Thus, $(R')^*/R^*$ embeds into $(QR')^*/(QR)^*$ via $x + R^* \longrightarrow x + (QR)^*$ and $(QR')^*/(QR)^*$ is infinite.

To prove our main theorem, we employ Lemma 3.4 together with a result on the multiplicative group of units of a ring. For the reader's convenience we give a complete statement of this latter result.

LEMMA 3.5 (Krempa 1985, Theorem 1.4). Let $A \subseteq B$ be domains such that A is integrally closed in B and B is finitely generated as an A-algebra. If A is a Krull domain, then B^*/A^* is a free abelian group of finite rank.

THEOREM 3.6 Let G be a reduced p-local group of finite rank. Then there exists a p-basic submodule B of G such that the corresponding canonical splitting ring R_B is minimal in the set of canonical splitting rings.

Proof: Plainly, it is enough to show that under the assumptions of Theorem 3.6 there exists no sequence of p-basic submodules $B_1, B_2, B_3, \ldots$ for G such that the corresponding sequence $R_1, R_2, R_3, \ldots$, where $R_i = R_{B_i}$, forms a properly descending chain of canonical splitting rings.

Assume the contrary. Then, since each R_i is pure in $\hat{Z}_p$, we have a properly decending chain: $QR_1 \supset QR_2 \supset QR_3 \supset \cdots$. Since G is of finite rank, each R_i is purely finitely generated as a ring by Proposition 2.1. Hence each QR_i is a finitely generated Q-algebra.

Let F_i be the algebraic closure of Q in QR_i . Then $F_1 \supseteq F_2 \supseteq F_3 \supseteq \cdots$ is a descending chain of algebraic number fields. Choose t such that $F_t = F_{t+j}$ for all $j \geq 0$. For $i \geq t$ each QR_i is an algebra over $F = F_t$. Apply Lemma 3.5 with $A = F$, $B = QR_i$, $i \geq t$, to conclude that, for each $i \geq t$, $(QR_i)^*/F^*$ is a free abelian group of finite rank. But, for $i \geq t$, $[(QR_i)^*/F^*]/[(QR_{i+1})^*/F^*] \cong (QR_i)^*/(QR_{i+1})^*$ is infinite by Lemma 3.4. This implies that, for all $i \geq t$, $\mathrm{rank}(QR_{i+1})^*/F^* <$

$\text{rank}(QR_i)^*/F^*$, an impossibility. Thus, no infinite proper descending chain of canonical splitting rings exists and the proof is complete.

4 FINITE RANK SPLITTING RINGS

The following example shows that Theorem 2.2 cannot be strengthened: not every splitting ring contains a canonical splitting ring.

EXAMPLE 4.1 Let $G = \langle\alpha, 1-\alpha^2\rangle_* \subset \hat{Z}_p$, where α is a transcendental p-adic unit, and let S be the pure subring of $\hat{Z}_p$ generated by 1 and α. Let $\theta : S \otimes G \to S$ be given by $\theta(\Sigma s_i \otimes g_i) = \Sigma s_i g_i$. Then θ is an S-map which is epic since

$$\theta[(\alpha \otimes \alpha) + (1 \otimes (1-\alpha^2))] = 1 .$$

Hence, $S \otimes G \cong S \oplus \text{Ker}\theta$. But p-rank$(S \otimes G)$ = (p-rank S)(p-rank G) = 1, so p-rank $\text{Ker}\theta = 0$, i.e., $\text{Ker}\theta$ is divisible. Thus, S is a splitting ring for G.

We claim that S contains no canonical splitting ring. To see this, consider the possibilities for p-basic submodules B of G. First suppose $B = \langle\alpha\rangle$. If f is the splitting map for $\hat{Z}_p \otimes \langle\alpha\rangle \longrightarrow \hat{Z}_p \otimes G$, then $f(1 \otimes \alpha) = 1 \otimes \alpha$. Therefore, by p-adic continuity, $f[1 \otimes (1-\alpha^2)] = \frac{1-\alpha^2}{\alpha} \otimes \alpha$. Thus, in this case, R_B is the pure subring of $\hat{Z}_p$ generated by 1 and $\frac{1-\alpha^2}{\alpha}$. Next suppose $B = \langle\beta\rangle$, $\beta = u\alpha + v(1-\alpha^2)$, $u,v \in Q$, $v \neq 0$. Then $\{\beta, \alpha\}$ is a maximal linearly independent set in G and, if f is the splitting map for $\hat{Z}_p \otimes \langle\beta\rangle \longrightarrow \hat{Z}_p \otimes G$, then $f(1 \otimes \beta) = 1 \otimes \beta$, $f(1 \otimes \alpha) = \frac{\alpha}{\beta} \otimes \beta$. In this case R_B is the pure subring of $\hat{Z}_p$ generated by 1 and α/β. In neither case is R_B contained in S.

In view of Example 4.1, the best we could hope for is to show that each splitting ring R contains a subring of p-rank one which is a splitting ring. The logical candidate for such a subring is the ring $R_0 = \hat{Z}_p \cap R$. More precisely, if R is any p-local ring, then $Z_p \cdot 1$ is the pure subring generated by $1 \in R$. Write $R/(Z_p \cdot 1) = D \oplus C$ where D is divisible and C is reduced. It is easy to see that if R_0 is the subgroup of R such that $R_0/(Z_p \cdot 1) = D$, then R_0 is a subring of R of p-rank one. It is possible to regard $R_0 = \hat{Z}_p \cap R$ by identifying R and $\hat{Z}_p = \hat{Z}_p \cdot 1$ as subrings of the completion $\hat{R}$ of R.

If R is a splitting ring for G, when does R_0 split G? We begin our discussion of this question by providing two examples where this is not the case. Example 4.2 shows that R_0 does not have to split G even if R_0 is a discrete valuation domain (equivalently, since R_0 is a pure subring of $\hat{Z}_p$, QR_0 is a field). In this example, G cannot be embedded in R_0^r, where r = p-rank(G). In contrast, Example 4.3 provides a ring R_0 for which G can be purely embedded in R_0^r, but still R_0 does not split G. By (Lady 1977, Proposition 1.2), such an R_0 cannot be a discrete valuation ring.

EXAMPLE 4.2 Suppose S is a pure subring of $\hat{Z}_p$ properly containing Z_p and that α and β are units of $\hat{Z}_p$ which are algebraically independent over S. Further suppose that the polynomial $f(x) = \alpha\beta x^2 + x + 1$ is irreducible over S. This will be the case, for example, if p = 2. Let d be a root of f(x), let R be the pure subring of the ring $\hat{Z}_p[d]$ generated by $\{S, \alpha d, \beta d, d\}$ and let G be the pure subgroup of $R \oplus R$ generated by $\{(0,1), (d,0), (\alpha d,\gamma)\}$, where γ is some element of $S \backslash Z_p$. The construction guarantees that G is a strongly indecomposable group of rank three and p-rank two. Moreover, $RG = R \oplus R$, since $(0,1) \in G$ and $(1,0) = -\beta d[(\alpha d,\gamma) - \gamma(0,1)] - (d,0) \in RG$. Thus, R is a splitting ring for G by Theorem 1.3.

The next step is to show that $R_0 = R \cap \hat{Z}_p = S$. For this it suffices to show $Q(R \cap \hat{Z}_p) = QS$, since S is pure in R and $\hat{Z}_p$. Clearly, $Q(R \cap \hat{Z}_p) \subset QS[\alpha,\beta] \subset \hat{Q}_p$. Furthermore, QR is isomorphic to the quotient ring $QS[\alpha x, \beta x, x]/(f(x))$, where α,β and x are considered as indeterminates over QS. Note that all these rings may be regarded as subrings of $\hat{Q}_p[x]/(f(x))$. Thus, an element $\phi(\alpha,\beta)$ of $Q(R \cap \hat{Z}_p)$ gives rise to an equation $\phi(\alpha,\beta) - \psi(\alpha x,\beta x,x) = mf(x)$, where ϕ and ψ are polynomials with coefficients in QS, and $m \in \hat{Q}_p[x]$. Moreover, for a given ϕ, we may choose ψ, regarded as a polynomial in $\hat{Q}_p[x]$, to be of minimal degree in x. In this case, it must be that m = 0 and $\psi \in QS$. If $m \neq 0$, then the term of mf(x) of highest degree in x has the highest term in f(x), $\alpha\beta x^2$, as a factor. This term must also be the term of highest degree in x in $\psi(\alpha x,\beta x,x)$. Then employing the substitution $\alpha\beta x^2 = f(x) - (x + 1)$ and transposing the ensuing multiple of f(x), we obtain an equation $\phi(\alpha,\beta) - \psi'(\alpha x,\beta x,x) = m'f(x)$ with ψ' of lower degree in x than ψ. This completes the proof that $R \cap \hat{Z}_p = S$.

Finally, we show that $R_0 = S$ is not a splitting ring for G. To see this, let

$\theta \in \text{Hom}(G,S)$. Write $\theta(d,0) = s \in S$ and $\theta(0,1) = t \in S$. Then, by continuity, $\theta(\alpha d,\gamma) = \alpha s + \gamma t$ is an element of S. However, $\gamma \in S$, whence $\gamma t \in S$; and α is transcendental over S, so $s = 0$. This shows that (d,0) is in the kernel of every map in Hom(G,S). In particular, G cannot be embedded into a direct sum of copies of S. By Theorem 1.3, S does not split G.

Our next example is constructed in a similar fashion.

EXAMPLE 4.3 Let α,β,γ be units of $\hat{Z}_p$ which are algebraically independent over Q. Further assume that $f(x) = \alpha\beta x^2 + \alpha x + 1$ is irreducible over $\hat{Z}_p$, and let d be a root of f(x). Let R be the pure subring of $\hat{Z}_p[d]$ generated by $\{1,\alpha,\alpha\beta,\gamma,d\}$, and let G be the pure subgroup of $R \oplus R$ generated by $\{(0,1), (\alpha,0), (\alpha\beta,\gamma)\}$. As in 4.2, G is strongly indecomposable of rank three and p-rank two and $RG = R \oplus R$. Also, R_0 is the pure subring of $\hat{Z}_p$ generated by $\{1,\alpha,\alpha\beta,\gamma\}$. In particular, G is a pure subgroup of $R_0 \oplus R_0$. Suppose θ is an element of $\text{Hom}(G,R_0)$. Denote $\theta(\alpha,0) = r$ and $\theta(0,1) = s$. Thus, $\theta(\alpha\beta,\gamma) = \beta r + \gamma s$ by continuity. Since γ and s are in R_0, we must have βr in R_0. Then consideration of the generating set for R_0 shows that $r \in \alpha R_0$. It follows that for any embedding $\varepsilon : G \to R_0 \oplus R_0$, we have $\varepsilon(\alpha,0) = (\alpha r_1,\alpha r_2)$ for some $r_1,r_2 \in R_0$. If $\varepsilon(0,1) = (s_1,s_2) \in R_0 \oplus R_0$, then $R_0\varepsilon(G) \doteq R_0 \oplus R_0$ implies that the matrix $M = \begin{bmatrix} \alpha r_1 & \alpha r_2 \\ s_1 & s_2 \end{bmatrix}$ is invertible in the two by two matrix ring over QR_0. But $\det M \in \alpha R_0$ and α is not a unit in QR_0. Thus, by Theorem 1.3, R_0 is not a splitting ring for G.

The next theorem shows that the class of rings R such that $R_0 = R \cap \hat{Z}_p$ is a discrete valuation ring is quite large. Recall that a ring R is called a local ring provided it has a unique maximal ideal. A ring R is called a Zariski ring if R is Noetherian and the integral prime p is contained in the Jacobson radical of R. The Zariski rings are precisely those rings R such that the p-adic completion $\hat{R}_p$ of R is a faithfully flat R-module. For a more detailed discussion of Zariski rings, see Matsumura (1986).

THEOREM 4.4 Let R be a p-local ring and let $R_0 = R \cap \hat{Z}_p$. Then R_0 is a discrete valuation ring in either of the following cases :

(a) R is a Zariski ring, or

(b) R is a local ring of Krull dimension one.

Proof: (a) Since in this case $\hat{R}_p$ is a faithfully flat R module, it follows from (Glaz 1989, Theorem 1.2), that R is an R-pure R-submodule of $\hat{R}_p$. Let $\alpha \in F \cap \hat{Z}_p$, where F is the quotient field of R_0 taken in $\hat{Q}_p$. There exists $\beta \in R_0$ with $\beta\alpha \in R_0$, so, by R-purity, there exists $r \in R$ with $\beta r = \beta\alpha$. Since $\beta \in R_0 \subset \hat{Z}_p \subset \hat{R}_p$ and $\hat{R}_p$ is a free $\hat{Z}_p$-module, β is not a zero-divisor in $\hat{R}_p$. It follows that $\alpha = r \in \hat{Z}_p \cap R = R_0$. We have shown that $R_0 = F \cap \hat{Z}_p$. Thus, the only ideals of R_0 are of the form p^nR_0 and R_0 is a discrete valuation ring.

(b) Let M be the unique maximal ideal of R. Since p is not invertible and is not a zero-divisor in R, M is the unique prime ideal over pR and is therefore the radical of pR. Thus, if $x \in M$, then $x^n \in pR$ for some positive integer n. Now let $x \in R_0 \backslash pR_0$. If $x \in M$ then $x^n \in pR \cap R_0 = pR_0$. It follows that $x \notin M$ and x is invertible in R. Since x is also invertible in $\hat{Z}_p$, x is invertible in R_0. We have shown that pR_0 is the unique maximal ideal of R_0. A similar argument shows that the only ideals of R_0 are of the form p^nR_0. Hence, R_0 is a discrete valuation ring

Our final result stands in contrast to Examples 4.1. 4.2, and 4.3.

THEOREM 4.5 Let G be a p-local group and suppose R is a p-local ring of finite rank such that R is a splitting ring for G. Then all canonical splitting rings R_B are equal and isomorphic to a subring of R. In particular, each R_B is a minimal splitting ring in R.

Proof: The finite rank hypothesis on R implies, by the Beaumont-Pierce Principal Theorem (Beaumont and Pierce 1961), that $R \doteq S \oplus N$, where N is the nil radical of R and S is a subring of R such that QS is semi-simple. By Lemma 1.2, $S \doteq R/N$ is a splitting ring for G.

Since QS is semi-simple, there are central idempotents $e_1,\ldots,e_n \in QS$ such that $QS = e_1QS \times \cdots \times e_nQS$ and each e_iQS is simple. It follows that $S \doteq e_1S \times \cdots \times e_nS$, so that each e_iS is a splitting ring for G, again by Lemma 1.2.

For the moment, assume $S = e_1S$. In this case QS is simple so there is a field of definition, F, for S. That is, there exists a subfield F of center QS such that S is quasi-equal to a free module over $E = F \cap S$. Additionally, the ring E is an E-ring and is strongly indecomposable as an additive group. See Pierce (1960) or Vinsonhaler and Wickless (1985) for details. Since S is a splitting ring, $S \otimes G \doteq S^r \oplus D$, where r = p-rank G and D is divisible. If $S \doteq E^m$ as E-modules, then as E-modules, $(E \otimes G)^m \simeq E^m \otimes G \doteq S \otimes G \doteq S^r \oplus D \doteq E^{mr} \oplus D$. Knowing E is strongly indecomposable we can use the uniqueness of quasi-decompositions to conclude that $E \otimes G \doteq E^r \oplus D_0$ for some divisible E-module D_0. Furthermore, this last quasi-isomorphism can be taken to preserve E-module structure since E is an E-ring. In fact, if M is any E-module, then $f \in \mathrm{Hom}(M,E)$ implies $f \in \mathrm{Hom}_E(M,E)$. Indeed, for each $m \in M$, the map given by $\theta(x) = f(xm)$ defines a Z-endomorphism of E. Since E is an E-ring, θ is left multiplication by $\theta(1)$. It follows that $f(xm) = xf(m)$ for all $x \in E$ and $m \in M$. Thus, the quasi-projection of $E \otimes G$ onto E^r is a quasi-split E-map whose kernel is a divisible E-module. That is, E is a splitting ring for G.

Because E is p-local and reduced, we may identify Z_p with the pure subring of E generated by 1. Define E_0 to be the inverse image in E of the maximal divisible subgroup of E/Z_p. As previously noted, $E_0 = \hat{Z}_p \cap E$ if we regard $\hat{Z}_p$ and E as subrings of $\hat{E}$, the p-adic completion of E. In particular, E_0 is a pure subring of E having p-rank one. We will show E_0 is a splitting ring for G.

Let $\pi : E \otimes G \longrightarrow E^r$ be the quasi-epimorphism obtained from $E \otimes G \doteq E^r \oplus D$ via quasi-isomorphism and projection. Then π is an E-map. Moreover, since QE is a field, $\pi(1 \otimes G)$ contains a QE-basis for QE^r, say $\{x_i = \pi(1 \otimes g_i) \mid 1 \le i \le r\}$, chosen so that $g_1, \dots, g_r$ is a p-basis for G. We may assume that $\pi(1 \otimes G) \subseteq \oplus Ex_i$, so that for each $g \in G$, $\pi(1 \otimes g) = \oplus \alpha_i x_i$ for a unique r-tuple $(\alpha_1, \dots, \alpha_r) \in E^r$. Consider the map $\varphi_j : G \longrightarrow E$ by $\varphi_j(g) = \alpha_j$ where $\pi(1 \otimes g) = \oplus \alpha_i x_i$. Note that $Z_p \subseteq \mathrm{Im}\ \varphi_j \subseteq E$. Moreover, $\oplus_{i \ne j} Z_p g_i \subseteq \mathrm{Ker}\ \varphi_j$. The last inclusion implies p-rank(Ker φ_j) $\ge r - 1$. Thus, p-rank(Im φ_j) ≤ 1 because p-rank G = r. The condition $Z_p \subseteq \mathrm{Im}\ \varphi_j \subseteq R$ then implies that $\mathrm{Im}\ \varphi_j \subseteq E_0$. In particular, if $G' = \pi(1 \otimes G)$ then $\oplus_{i=1}^r Z_p x_i \subseteq G' \subseteq \oplus_{i=1}^r E_0 x_i$. Clearly $E_0 G' = \oplus E_0 x_i$. Moreover, since Z_p is pure in E then $1 \otimes G = Z_p \otimes G$ is pure in $E \otimes G$. Since D is divisible it follows that G' is quasi-pure in $\oplus_{i=1}^r Ex_i$ and, hence, that G' is quasi-pure in $\oplus_{i=1}^r E_0 x_i$. Additionally, since p-rank G' = r = p-rank G and $Z_p \otimes G$ is reduced, it follows that π is monic on $Z_p \otimes G$, i.e. $G' \cong G$. Thus, we can apply Theorem 1.3 to conclude that E_0 splits G.

Next observe that QE_0 is the quotient field of E_0 since E_0 is a subring of an algebraic number field. If B is any p-basic submodule of G, by Corollary 2.4, $R_B \subseteq E_0$. Furthermore, R_B is independent of B by Corollary 2.6.

Finally, returning to our original $S \doteq e_1S \times \cdots \times e_nS$, we can employ the mapping $r \longrightarrow (re_1,\ldots, re_n)$ to conclude that R_B is quasi-isomorphic to a subring of S, thus quasi-isomorphic to a subring of $R \doteq S \oplus N$. But quasi-isomorphic p-local rings of p-rank one are isomorphic. This completes the proof of the theorem.

5 OPEN QUESTIONS

The following questions, which we are unable to answer at present, seem worthy of further attention.

1. For a given G of finite rank is there a uniform bound, expressed in terms of G, on the lengths of chains of canonical splitting rings?

2. Does every splitting ring contain a minimal one?

Theorem 4.5 shows that every finite rank splitting ring contains a unique minimal splitting ring which is, in addition, canonical. A minimal splitting ring is defined as a splitting ring R with no proper pure splitting subrings.

3. When is a p-local group G determined by the collection of its splitting rings? When is a p-local ring R determined by the collection of splittings rings for R+?

If R is a pure subring of $\hat{Z}_p$ then R is a splitting ring for R+ by Corollary 1.4. Moreover, if S is a pure subring of $\hat{Z}_p$ such that S splits R+ then by Theorem 1.3, R+ is isomorphic to a pure subgroup R' of S such that $SR' \doteq S$. Since R, R' are pure in $\hat{Z}_p$ we have $R' = Rx$ for some $x \in \hat{Z}_p$. Thus, $SRx \doteq S$. But then $RS \doteq RSRx = RSx \doteq S$, so $S \dot{\supseteq} R$. By purity, $S \supseteq R$. Therefore, R can be identified as the minimal pure subring of $\hat{Z}_p$ which splits R+.

ACKNOWLEDGEMENT

We would like to thank Professor Kevin O'Meara for providing a reference for, and Professor Roger Wiegand for providing an independent proof of, the result stated in Lemma 3.5.

REFERENCES

[B-P] Beaumont, R. and Pierce, R. (1961) Torsion Free Rings, Ill. J. Math 5, pp 61-98.

[G] Glaz, S. (1989) Commutative Coherent Rings, Springer-Verlag Lecture Notes 1371.

[K] Krempa, J. (1985) Finitely Generated Groups of Units in Group Rings, preprint, Universytet Warszawski Instytut Mathematyki.

[L-1] Lady, L. (1977) Splitting fields for torsion-free modules over discrete valuation rings I, J. Algebra 49, pp 261-275.

[L-2] _____, (1980a) Splitting fields for torsion-free modules over discrete valuation rings II, J. Algebra 66, pp 281-306.

[L-3] _____, (1980b) Splitting rings for torsion-free modules over discrete valuation rings III, J. Algebra 66, pp 307-320.

[L-4] _____, (1983) A Seminar on Splitting Rings for Torsion Free Modules over Dedekind Domains, Lecture Notes in Math 1006, Springer-Verlag, pp 1-48.

[M] Matsumura, H. (1986) Commutative Ring Theory Cambridge studies in advanced mathematics 8, Cambridge University Press, Cambridge.

[P] Pierce, R. (1960) Subrings of Simple Algebras, Mich. Math. J. 7, pp 241-243.

[S] Szekeres, G. (1948) Countable abelian groups without torsion, Duke Math. J. 15, pp 293-306.

[T] Turgi, M. (1977) Sheaves and Torsion Free Modules, Thesis, Univ. of Illinois.

[V-W] Vinsonhaler, C. and Wickless, W. (1985) Locally irreducible rings, Bull. Aust. Math. Soc. 32, pp 129-145.