ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 5, Number 4, Fall 1975

ON A PAPER OF RICHMAN AND WALKER

ROBIN KUEBLER AND J. D. REID*

This note was inspired by a paper of F. Richman and E. A. Walker [5] in which, among other results, is the theorem that an abelian p-group with an unbounded basic subgroup is determined by its endomorphism ring. In fact these authors do more than give a new proof of this well-known theorem. They construct the group as a module over its endormorphism ring, not merely as Z-module. They also point out that if the group is bounded, then it is isomorphic to the left ideal of the endomorphism ring generated by any primitive idempotent of maximal additive order; thus in this case, too, constructing the group, as module, from the ring. This leaves the problem of determining the group as module over its endomorphism ring, in the case of a bounded basic subgroup but non-zero divisible subgroup. We give a solution to this problem for divisible groups in § 1, and show there too that if $G = D \oplus H$ with D divisible and H reduced, then the modules D and $R = G/D$ over $E = \mathrm{Hom}_Z(G, G)$ are determined from E. Thus, knowing E, we then know the E-modules D and R and will know the E-module G once we know the element of $\mathrm{Ext}_E{}^1(R, D)$ determined by the exact sequence $0 \to D \to G \to R \to 0$.

It turns out (§ 2) that $\mathrm{Ext}_E{}^1(R, D)$ is a cyclic module over a certain ring Γ with the class of the sequence above as a generator. Moreover two exact sequences $0 \to D \to X_i \to R \to 0$ of E-modules have isomorphic modules X_i if and only if their classes are multiples of each other by p-adic units. Finally, in § 3 it is shown that Γ is the ring of p-adic integers. In this way G is determined, as E-module, by E. Thus, in case R is bounded, we have answered the question which motivated us but no restriction on R is necessary (thanks partly to the referee — cf. § 3) so that we obtain a much more general result than we sought. Clearly, however, we require $D \neq 0$.

1. **The Modules D and R.** The object of this section is to show how the modules D and $R = G/D$ can be constructed from $E = \mathrm{Hom}_Z(G, G)$ when D is the maximal divisible subgroup of G. These results, taken

Received by the Editors February 12, 1974 and in revised form November 11, 1974.

*The work of the second author was supported in part by the National Science Foundation (NSF Grant GP 19351). The first author is not at the University of Texas of the Permian Basin, Odessa, Texas.

with our structure theorem for $\mathrm{Ext}_E{}^1(R, D)$ will yield the determination of G as E-module. Here, as Z-module, $G \cong D \oplus R$. We have at our disposal, not this splitting, but rather the exact sequence $0 \to D \to G \to R \to 0$ of E-modules; for D is clearly an E-submodule of G so that R, by definition the quotient G/D, is too. As indicated in the introduction, our interest is in the case $D \neq 0$, so this will be our assumption henceforth.

In case $G = D$, write D_n for the p^n layer of D,

$$D_n = \{x \in D \mid p^n x = 0\},$$

and E_n for the endomorphism ring of D_n. Then D_n is an E-submodule of D and, since D is injective, restriction is a homomorphism of the ring E onto E_n. Since D is divisible the kernel of this restriction map is $p^n E$. Write J_n for the restriction map, P_n for multiplication by p^n and view E_n as an E module via J_n to obtain the exact sequence of E-modules

$$0 \to E \xrightarrow{P_n} E \xrightarrow{J_n} E_n \to 0.$$

If $n = m + k, k \geqq 0$, then there is a unique map $\varphi_m{}^n \in \mathrm{Hom}_E(E_m, E_n)$ making

$$\begin{tikzcd}
0 \arrow[r] & E \arrow[r, "P_m"] \arrow[d] & E \arrow[r] \arrow[d, "P_k"] & E_m \arrow[r] \arrow[d, "\varphi_m{}^n"] & 0 \\
0 \arrow[r] & E \arrow[r, "P_n"] & E \arrow[r] & E_n \arrow[r] & 0
\end{tikzcd}$$

commutative. We then have a direct system $\{E_m, \varphi_m{}^n\}$ of E-modules, uniquely determined by E.

Now if e is a primitive idempotent in E, then $e_n = J_n(e)$ is a primitive idempotent in E_n of maximal additive order. We have

$$\varphi_m{}^n(e_m) = \varphi_m{}^n J_m(e) = J_n P_{n-m}(e) = p^{n-m} e_n, \qquad n \geqq m.$$

Thus if $\eta = J_m(\rho) \in E_m$, then

$$\varphi_m{}^n(\eta e_m) = \varphi_m{}^n J_m(\rho e) = p^{n-m} J_n(\rho e) = p^{n-m} J_n(\rho) e_n.$$

Since the inclusion $D_m \to D_n$ had image $p^{n-m} D_n$, this yields the commutative diagram of E-modules

$$\begin{tikzcd}
E_m e_m \arrow[r, "\varphi_m{}^n"] \arrow[d, phantom, "\wr\wr"] & E_n e_n \arrow[d, phantom, "\wr\wr"] \\
D_m \arrow[r] & D_m
\end{tikzcd},$$

so that $D = \varinjlim E_m e_m$. In this way D is determined as an E-module by its endomorphism ring E.

Now consider the case in which $G \neq D \neq 0$. From the remarks above it is clear that, if we can construct the endomorphism rings $E(D)$ and $E(R)$ of D and R as homomorphic images of $E = E(G)$, then we can construct the E-modules D and R. Restriction takes E onto $E(D)$ with kernel $\Sigma = \{\alpha \in E \mid \alpha D = 0\}$, and it is equally clear that every endormorphism of R is induced by one of G, the kernel of this representation being $\Delta = \{\alpha \in E \mid \alpha G \subseteq D\}$. Thus it suffices to determine the ideals Δ and Σ of E. Moreover, if δ is a projection of G onto D, then Σ is simply the left annihilator of δ in E while $\Delta = \delta E$. This shows also that Σ is the left annihilator of Δ as well, and Δ is the right annihilator of Σ in E.

Our problem then is to characterize, in ring theoretic terms, the projections of G onto its maximal divisible subgroup D. Two such characterizations are contained in the simple result below, for whose statement, however, we need a bit of notation. We denote by $I(E)$ the set of idempotents in E and recall that $I(E)$ is a partially ordered set under the relation defined by writing $u \leqq v$, for $u, v \in I(E)$, provided $uv = vu = u$. For $v \in I(E)$, we put $L(v) = \{u \in I(E) \mid u \leqq v\}$.

Proposition 1.1. *Let G be a p-group with endomorphism ring E and maximal divisible subgroup D, and let T be the torsion ideal of E. Then the following are equivalent:*

(i) *δ is a projection of G onto D;*

(ii) *δ is a maximal element of the set $\{v \in I(\mathrm{E}) \mid L(v) \cap T = 0\}$ ordered by $\leqq$;*

(iii) *δ is a maximal element of the set $\{v \in I(E) \mid vEv \cap T = 0\}$ ordered by $\leqq$.*

Proof. It is clear that the relation $u \leqq v$ on $I(E)$ is equivalent to the inclusions im $u \subseteq$ im v, ker $u \supseteq$ ker v. Thus if δ is a projection of G onto D and if $u \leqq \delta$, $u \neq 0$, then $u(G)$ is a summand of D, hence unbounded, so $u \notin T$. Hence $L(\delta) \cap T = 0$. If $\delta < v$ for some $v \in I(E)$, then $v - \delta$ is a projection of G onto a reduced subgroup which in turn has finite summands. Such a finite summand of $(v - \delta)G$ is a summand of G as well, providing therefore an idempotent u of finite order with $u \leqq v$. We conclude that (i) implies (ii). On the other hand, if δ satisfies (ii), then from $L(\delta) \cap T = 0$ it is clear that $\delta(G)$ has no bounded summands, so is divisible. The maximality of δ now forces $\delta(G) = D$. Hence (i) and (ii) are equivalent.

The equivalence of (ii) and (iii) follows from the easily-established fact that the conditions $L(v) \cap T = 0$ and $vEv \cap T = 0$ are equivalent.

We note in passing that the ideals Σ and Δ admit neater descriptions in special cases. For example, it is easy to show, for any p-group

G with first Ulm subgroup G^1, that $\mathrm{Hom}(G, G^1)$ (viewed as subset of E) is the right annihilator of the torsion ideal of E. Therefore if R has no elements of infinite height, so $G^1 = D$, then Δ is the right annihilator of the torsion ideal of E and of course Σ is the left annihilator of Δ. If R is bounded, then Σ is the torsion ideal.

To summarize, given E we can construct the E-modules R and D. We note too that the Z-module G can now be recaptured from E; $G \cong R \oplus D$.

2. $\mathbf{Ext}_E{}^1(R, D)$. In this section we establish the basic structure theorem for $\mathrm{Ext}_E{}^1(R, D)$. From above we have the ideals $\Delta = \{\alpha \in E \mid \alpha G \subset D\}$ and $\Sigma = \{\alpha \in E \mid \alpha D = 0\}$ given, once E is given, in ring theoretic terms. The fundamental object from our point of view, however, is the ideal $L = \Delta \cap \Sigma$, which, of course, is now also determined from E ring theoretically. On the other hand, in terms of R and D, L may be viewed as $\mathrm{Hom}_Z(R, D)$ made into an E-bimodule in the usual way. It is our assumption here that $D \neq 0$, so the center of E is the ring J of p-adic integers. We view E as J-algebra and now adopt the standard convention of viewing E-bimodules as modules over the enveloping algebra E^e of E. Recall that $E^e = E \otimes_J E^*$, where E^* is the opposite ring to E, and the action of E^e on, for example L, is given by $\alpha \otimes \beta^* : \lambda \to \alpha\lambda\beta$, $\quad \alpha, \beta \in E$, $\quad \lambda \in L$. Recall also the definition of the cohomology groups $H^n(E, L) \equiv \mathrm{Ext}^n_{E^e}(E, L)$.

Because $\mathrm{Ext}_J{}^n(R, D) = \mathrm{Ext}_Z{}^n(R, D) = 0$ for all n, it follows that $H^n(E, \mathrm{Hom}_J(R, D)) \approx \mathrm{Ext}_E{}^n(R, D)$ for all n. This is known ([1], ch. IX (4.4)), but since it seems to arise in the literature immersed in contexts of one sort or another, we give a proof for the case $n = 1$, which is all we need, later. In any case, we have $\mathrm{Hom}_J(R, D) = \mathrm{Hom}_Z(R, D) \approx L$, so that $\mathrm{Ext}_E{}^1(R, D) \approx H^1(E, L)$.

The augmentation map $\epsilon : E^e \to E$ given by $\epsilon : \alpha \otimes \beta^* \to \alpha\beta$ yields the exact sequence of E^e modules $0 \to I \to E^e \xrightarrow{\epsilon} E \to 0$ from which we obtain

$$0 \to \mathrm{Hom}_{E^e}(E, L) \to \mathrm{Hom}_{E^e}(E^e, L) \to \mathrm{Hom}_{E^e}(I, L) \to \mathrm{Ext}^1_{E^e}(E, L) \to 0$$

since E^e is projective over itself. Since $\mathrm{Hom}_{E^e}(E, L) \subseteq \mathrm{Hom}_e(E, E) = J$, $\mathrm{Hom}_{E^e}(E^e, L) \approx L$, and no element of J annihilates D, it follows that $\mathrm{Hom}_{E^e}(E, L) = 0$. It is well known that in the sequence above, $\mathrm{Hom}_{E^e}(I, L)$ is isomorphic to the group $\mathrm{Der}(E, L)$ of derivations of E into L and the image of $\mathrm{Hom}_{E^e}(E^e, L)$ is the subgroup of inner derivations. These remarks admittedly assume a little diagram chasing, but given such, and the isomorphism $\mathrm{Ext}_E{}^1(R, D) \approx \mathrm{Ext}^1_{E^e}(E, L)$, we arrive at the exact sequence

$$0 \to L \to \mathrm{Der}(E, L) \to \mathrm{Ext}_E{}^1(R, D) \to 0.$$

Put $\Gamma = \mathrm{Hom}_{E^e}(L, L)$. We can now prove that $\mathrm{Ext}_E{}^1(R, D)$ is a cyclic Γ-module.

PROPOSITION 2.1. *$\mathrm{Ext}_E{}^1(R, D)$ is a cyclic Γ-module. Explicitly, if δ is a projection of G onto D and $\beta = 1 - \delta$,* then the *map $\mathfrak{D} : \alpha \to \delta\alpha\beta$ is a derivation of E into L, and every derivation of E into L is congruent to a multiple of $\mathfrak{D}$ by an element of Γ, modulo the inner derivations.*

PROOF. From the facts that $\Sigma = E\beta$, $\Delta = \delta E$ and $\Sigma\Delta = 0$, it follows that $L = \Sigma \cap \Delta = \Delta\Sigma = \delta E\beta$. Thus the function $\mathfrak{D}$ defined by $\mathfrak{D}(\alpha) = \delta\alpha\beta$ maps E into L, and it is easy to verify that $\mathfrak{D}$ is a derivation. Moreover, since $\beta \in \Sigma$ and $\delta \in \Delta$, we have $\beta E\delta \subseteq \Sigma\Delta = 0$. Thus the two-sided Peirce decomposition of E relative to the idempotents δ and β is $E = \delta E\delta \oplus \delta E\beta \oplus \beta E\beta$.

Now let $d \in \mathrm{Der}(E, L)$. Then for $\alpha \in E$,

$$\begin{aligned} d(\delta\alpha\delta) &= \delta d(\alpha\delta) + d(\delta)\alpha\delta \\ &= d(\alpha\delta) \\ &= \alpha d(\delta) + d(\alpha)\delta \\ &= \alpha d(\delta) \end{aligned}$$

since $d(E) \subseteq L = \delta E\beta$, $\delta \in \Delta$ and $L\Delta = 0$. A similar argument gives $d(\beta\alpha\beta) = d(\beta)\alpha$. But $\beta = 1 - \delta$ so that $d(\beta\alpha\beta) = -d(\delta)\alpha$. Hence for any $\alpha \in E$,

$$\begin{aligned} d(\alpha) &= d(\delta\alpha\delta + \delta\alpha\beta + \beta\alpha\beta) \\ &= \alpha d(\delta) + d(\delta\alpha\beta) - d(\delta)\alpha \\ &= \alpha d(\delta) - d(\delta)\alpha + d(\delta\alpha\beta). \end{aligned}$$

Writing $\zeta = d(\delta) \in L$ and denoting the restriction of d to L by γ, we have

$$d(\alpha) = \alpha\zeta - \zeta\alpha + \gamma \circ \mathfrak{D}(\alpha),$$

and it remains only to show that $\gamma \in \Gamma$. For this, let $\alpha \in E$, $\lambda \in L$. Then

$$\begin{aligned} \gamma(\alpha\lambda) &= d(\alpha\lambda) = \alpha d(\lambda) + d(\alpha)\lambda = \alpha d(\lambda) = \alpha\gamma(\lambda) \\ \gamma(\lambda\alpha) &= d(\lambda\alpha) = \lambda d(\alpha) + d(\lambda)\alpha = d(\lambda)\alpha = \gamma(\lambda)\alpha \end{aligned}$$

since $L^2 = 0$.

Thus every derivation of E into L is, up to an inner derivation, a multiple of $\mathfrak{D}$ by an element of Γ. Clearly $\mathrm{Der}(E, L)$ is a Γ-module and the set of inner derivations forms a submodule. The exact sequence preceding the statement of the proposition now shows that $\mathrm{Ext}_E{}^1(R, D)$ is generated by the image of $\mathfrak{D}$ as Γ-module.

In order to add a few details to Proposition 2.1, we give one indication of how the isomorphism $\mathrm{Ext}_E{}^1(R, D) \approx H^1(E, L)$ might be obtained. We assume given the E-modules D and R and construct first canonical representatives for the elements of $\mathrm{Ext}_E{}^1(R, D)$.

Let $0 \to D \to X \to R \to 0$ be any short exact sequence of E-modules. Then since $\mathrm{Ext}_Z{}^1(R, D) = 0$, there is a Z-isomorphism $\rho : X \to G$ such that the diagram

$$\begin{array}{ccccccccc} 0 & \to & D & \to & X & \to & R & \to & 0 \\ & & \| & & \downarrow{\scriptstyle\rho} & & \| & & \\ 0 & \to & D & \to & G & \to & R & \to & 0 \end{array}$$

is commutative. Here the bottom row is the Z-split sequence of § 1. By definition of $E = \mathrm{Hom}_Z(G, G)$, G is an E-module, but we can now give G a different E-module structure, via ρ, by defining

$$\alpha * g = \rho\alpha\rho^{-1}g, \qquad \alpha \in E, g \in G.$$

Since the map $g \mapsto \alpha * g$ is an endomorphism of G, it is given by some element $\varphi(\alpha)$ of E. Clearly the map $\alpha \mapsto \varphi(\alpha)$ is a homomorphism of the ring E into itself, and it is easily checked that $\varphi(\alpha)$ and α induce the same maps on D and on R. We denote the module so obtained by (G, φ) and observe that ρ is an E-isomorphism from X to (G, φ), so that the sequence given is equivalent to $0 \to D \to (G, \varphi) \to R \to 0$.

Since α and $\varphi(\alpha)$ induce the same maps on D and R, the map $d : \alpha \to \varphi(\alpha) - \alpha$ has range contained in L. Using the facts that φ is a homomorphism and $L^2 = 0$, it is easy to see that d is a derivation of E into L. One can check too that two sequences $0 \to D \to (G, \varphi_i) \to R \to 0$ $(i = 1, 2)$ are E-equivalent if and only if the corresponding derivations differ by an inner derivation. This gives the correspondence between $\mathrm{Ext}_E{}^1(R, D)$ and $H^1(E, L)$. We omit further details because this is more or less known.

However, we do wish to make two observations. The first is that, if φ is the homomorphism of E into itself corresponding to the derivation $\mathfrak{D}$ of Proposition 2.1, then the sequence $0 \to D \to (G, \varphi) \to R \to 0$ is equivalent to our original sequence $0 \to D \to G \to R \to 0$ of E-modules. Thus our original sequence determines a generator of the Γ-module $\mathrm{Ext}_E{}^1(R, D)$. On the other hand, there are many generators, and until we know more about Γ we have not determined our sequence as precisely as we would like. We consider this in the next section.

The second observation is that two modules (G, φ) and (G, φ') might be isomorphic, yet determine distinct elements of $\mathrm{Ext}_E{}^1(R, D)$. To clarify this situation one notes that if $\theta : (G, \varphi) \to (G, \varphi')$ is an E-isomorphism, then the restriction of θ to D is an E-automorphism of D since D is the maximal divisible subgroup of G. Thus θ induces an E-automorphism $\bar{\theta}$ of R as well. Since, however, every endomorphism of the groups D and R is induced by some element of E, the maps $\theta|_D$ and $\bar{\theta}$ are in fact central automorphisms. These are simply multiplications by suitable p-adic units, say u and v respectively. Now it is easy to check that the element of $\mathrm{Ext}_E{}^1(R, D)$ corresponding to (G, φ) is the multiple by $u^{-1}v$ of that determined by (G, φ'). The converse is even more immediate. We summarize these remarks in

PROPOSITION 2.2 *The sequence* $0 \to D \to G \to R \to 0$ *yields a generator of the cyclic* Γ*-module* $\mathrm{Ext}_E{}^1(R, D)$. *Two sequences* $0 \to D \to (G, \varphi_i) \to R \to 0$ $(i = 1, 2)$ *have isomorphic middle modules* (G, φ_i) *if and only if the elements of* $\mathrm{Ext}_E{}^1(R, D)$ *they determine are multiples of each other by p-adic units.*

3. **Identifying** Γ. In order to identify the E-module G in a more explicit way, we must know more about the ring $\Gamma = \mathrm{Hom}_{E^e}(L, L)$. The following Proposition settles the issue. In our original statement of this result, R was a direct sum of cyclic groups, which would cover comfortably the case of bounded R which motivated us. This was subsequently generalized to totally projective R. However, we wish to thank the referee for a suggestion which simultaneously simplified our proof and extended its applicability to the general case.

PROPOSITION 3.1. *If* γ *is any bimodule homomorphism of L into itself, then there exists a p-adic integer* α *such that* $\gamma(\varphi) = \alpha\varphi$ *for all* $\varphi \in L$.

PROOF. We consider projections π of G onto summands with rank 1 complements, and let $A(\pi) = \{\alpha \in E \mid \alpha\pi = 0\}$ be the left annihilator of π in E. Let K be the union of all these left annihilators. If $0 \neq \varphi \in A(\pi) \cap L$, then, since φ annihilates D, the image of π actually has a cyclic complement and it is clear that the kernel of φ has the form $\pi G \oplus p^m(1 - \pi)G$ for some m. Thus there are endomorphisms $\alpha \in E$, for example $\alpha = \pi + p^m(1 - \pi)$, such that $\ker \varphi = \mathrm{im}\,\alpha$. On the other hand, the image of φ is cyclic, say $[d]$ with $d \in D$, and there is an epimorphism $\theta : D \to D$ with kernel $[d]$. We may define $\beta = \theta\delta + (1 - \delta)$, with δ a projection of G onto D, and obtain $\mathrm{im}\,\varphi = \ker\beta$.

From these two remarks, we conclude that, for all $\gamma \in \Gamma$ and $\varphi \in K \cap L$, the inclusions $\ker \varphi \subseteq \ker \gamma(\varphi)$, $\mathrm{im}\ \gamma(\varphi) \subseteq \mathrm{im}\ \varphi$ hold.

They in turn imply that the map $\varphi(g) \to [\gamma(\varphi)](g)$ is a (well-defined) endomorphism of the cyclic group $\varphi(G)$, so that $\gamma(\varphi) = n\varphi$ for some integer n. Moreover, if $\varphi_1, \varphi_2 \in K \cap L$, it is easy to find $\varphi \in K \cap L$ and $\alpha_i, \beta_i \in E$ such that $\beta_i\varphi\alpha_i = \varphi_i$, $i = 1, 2$, so that, if $\gamma(Y) = n\varphi$, then $\gamma(\varphi_i) = n\varphi_i$ as well.

It follows from the paragraph above that there exists a p-adic integer α such that $\gamma(\varphi) = \alpha\varphi$, at least for all $\varphi \in K \cap L$. But if $\varphi \in L$ and $\kappa \in K$ are arbitrary, then $\varphi\kappa \in K \cap L$ so $\gamma(\varphi)\kappa = \alpha\varphi\kappa$. Thus $[\gamma(\varphi) - \alpha\varphi]\kappa = 0$ for all $\kappa \in K$, which clearly yields $\gamma(\varphi) = \alpha\varphi$ as required.

COROLLARY. *If R is unbounded, then Γ is the ring J of p-adic integers. If R is bounded with exponent k then Γ is the ring $J/(p^k)$.*

Our main result now follows from the result of Richman and Walker mentioned in the introduction (indeed only the reduced case is needed) along with Propositions 2.1, 2.2 and 3.1.

THEOREM. *Let G be a p-group with endomorphism ring E. Then G can be constructed, as E-module, from E. If G has divisible subgroup D satisfying $0 \neq D \neq G$, then the E-modules D and R in $0 \to D \to G \to R \to 0$ are determined by E. The group $\mathrm{Ext}_E{}^1(R, D)$ is a cyclic p-adic module—free of rank 1 if R is unbounded, of order p^k if R has exponent k—with generator determined by the above sequence. Two E-exact sequences $0 \to D \to X_i \to R \to 0$ have isomorphic modules X_i if and only if the corresponding elements of $\mathrm{Ext}_E{}^1(R, D)$ generate the same p-adic submodule.*

REFERENCES

1. H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton, 1956.

2. F. Richman and E. A. Walker, *Primary abelian groups as modules over their endomorphism rings*, Math. Zeitschr. 89(1965), 77-81.

WESLEYAN UNIVERSITY, MIDDLETOWN, CONNECTICUT 06457