2007

Torsion-Free Groups and Modules with the Involution Property

Brendan Goldsmith
Technological University Dublin, brendan.goldsmith@tudublin.ie

C. Meehan
Technological University Dublin

S.L. Wallutis
Fachbereich 6, Mathematik und Informatik, Universitat Essen, 45118 Essen, Germany

Recommended Citation

Goldsmith, B., Meehan, C. & Wallutis, S.L. (2007). Torsion-free groups and modules with the involution property. *Journal of Pure and Applied Algebra*, vol. 208, no. 1, pg. 127-134. 10.1016/j.jpaa.2005.11.006

Available online at www.sciencedirect.com
ScienceDirect
Journal of Pure and Applied Algebra 208 (2007) 127–134
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

Torsion-free groups and modules with the involution property

B. Goldsmith[a,*], C. Meehan[a], S.L. Wallutis[b]

[a] *School of Mathematical Sciences, Dublin Institute of Technology, Kevin Street, Dublin 8, Ireland*
[b] *Fachbereich 6, Mathematik und Informatik, Universität Essen, 45117 Essen, Germany*

Received 2 August 2005
Available online 13 December 2005
Communicated by C.A. Weibel

Abstract

An Abelian group or module is said to have the involution property if every endomorphism is the sum of two automorphisms, one of which is an involution. We investigate this property for completely decomposable torsion-free Abelian groups and modules over the ring of p-adic integers.

MSC: 20K30; 16A65

0. Introduction

The circumstances under which the automorphism group of an Abelian group or module additively generates the full endomorphism ring has long been of interest to algebraists [8]. Of more specific interest has been the determination for a given module, M, of the least positive integer n (if such exists), such that every endomorphism of M is a sum of exactly n automorphisms of M; this n is called the *unit sum number* of M, $\mathrm{usn}(M)$: where no such n exists, we say $\mathrm{usn}(M) = \omega$ if every endomorphism of M is a sum of a finite number of automorphisms and $\mathrm{usn}(M) = \infty$ if not. There is a considerable body of literature on this topic including [2,9,11–13,15,18–20].

In 1954 Zelinsky showed for a vector space V over a field F that $\mathrm{usn}(V) = 2$ unless V is one-dimensional and F is the field of two elements, in which case $\mathrm{usn}(V) = \omega$: see [24]. In 1985 the first author [11] considered unit sum numbers for reduced torsion-free modules over a complete discrete valuation ring. This approach was further developed and formalized by Goldsmith, Pabst and Scott in [13]. Recently the second author has shown that for a large class of rings R, including PIDs, a free R-module M of any rank greater than 2 has $\mathrm{usn}(M) = 2$ — see [19, 20]. Surprisingly, certain rational groups have been shown to have a *finite* unit sum number greater than 2 (see [12] and [18]).

It is, however, possible in certain circumstances to obtain stronger results: an Abelian group, or more generally an R-module M, is said to have the *involution property* if every endomorphism of M can be expressed as the sum of two

* Corresponding author.
E-mail addresses: brendan.goldsmith@dit.ie (B. Goldsmith), mcandt@gofree.indigo.ie (C. Meehan), simone.wallutis@uni-essen.de (S.L. Wallutis).

0022-4049/$ - see front matter
doi:10.1016/j.jpaa.2005.11.006

automorphisms, one of which is an involution; this concept has been investigated in [18]. The involution property is closely related to a property first introduced by Nicholson [21] in connection with exchange rings: a ring E is said to be *clean* if every element can be expressed as the sum of a unit and an idempotent. The notion can be extended to modules in a natural way: an R-module M is said to be clean if its endomorphism ring $\mathrm{End}_R(M)$ is clean. A significant, and rather surprising result in this area is Ó Searcóid's theorem [23]: every vector space over a field is clean. There is an extensive and growing literature on this topic including [1,21,22] and [23].

The present work focuses on two broad areas: an investigation of completely decomposable Abelian groups and consideration of modules over the ring of p-adic integers. In this final section we shall show that a free p-adic module of infinite rank does not have the involution property (and is not clean, thereby answering a query of Nicholson) but that modules with the involution property exist in such abundance that there is no hope of classifying them.

All groups other than automorphism groups are assumed to be Abelian and our terminology and notation are standard and may be found in [6,7,16]; an exception is that we write maps on the right. Throughout the paper all rings will be associative unital rings. The set of rational primes is denoted by $\mathbb{P}$ and where there is no danger of misinterpretation we refer to rational primes as primes.

1. Preliminaries

In this section we derive some elementary properties of modules with the involution property and make precise the connection with clean modules. Throughout this section the ring R is arbitrary, not necessarily commutative.

Proposition 1.1. *If G is an R-module which has the involution property, then 2 is an automorphism of G.*

Proof. Let 1 be the identity in $\mathrm{End}_R(G)$ so that $1 = \alpha + v$, where $\alpha, v \in \mathrm{Aut}(G)$ and $v^2 = 1$. Then pre-multiplying by v and substituting for v in the resulting equation we get $0 = (1 + v)\alpha$. However, since $\alpha \in \mathrm{Aut}(G)$ this forces $v = -1$ and so $\alpha = 2$. □

Now we can state clearly the connection between the involution property and the property of being clean.

Proposition 1.2. *Let G be an R-module. Then:*

(i) *if G has the involution property then G is clean;*
(ii) *if G is clean, then G has the involution property if and only if 2 is an automorphism of G.*

Proof. If G has the involution property then 2 is an automorphism of G by Proposition 1.1. Then for any $\phi \in \mathrm{End}_R(G)$, we have $2\phi - 1 = \alpha + v$, where $\alpha, v \in \mathrm{Aut}(G)$ and $v^2 = 1$. Therefore, $\phi = 2^{-1}\alpha + 2^{-1}(v + 1)$. Clearly, $2^{-1}\alpha$ is an automorphism of G and a straightforward calculation shows that $2^{-1}(v + 1)$ is an idempotent. This proves (i).

The proof of (ii) is similarly direct: if G is clean and 2 is a unit then, for any endomorphism ϕ, we have $2^{-1}(\phi + 1) = u + e$ where u is an automorphism and e is an idempotent. Then since $\phi = 2u + (2e - 1)$, it is clear that ϕ is a sum of two automorphisms of M, one of which is an involution. The converse follows immediately from the previous proposition. □

If a ring R has the involution property, it is easy to see that a free R-module of finite rank also has the property.

Proposition 1.3. *Suppose that R is a ring with the involution property; then, for each positive integer n, the free R-module of rank n has the same property.*

Proof. Note firstly that the endomorphism ring may be identified as the ring of $n \times n$ matrices over the opposite ring R^{op}. Since it is clear that a ring R has the involution property if and only if its opposite ring, R^{op}, has it, it will suffice to consider matrices over R itself. Our proof is by induction on n. In fact we show somewhat more: every $n \times n$ matrix is the sum of a diagonal involution and a unit. If $n = 1$, the result is true by hypothesis. Suppose now the result is true for n and consider a matrix of size $(n + 1) \times (n + 1)$: say,

$$M = \begin{pmatrix} A & B \\ C & d \end{pmatrix}$$

where A is $n \times n$, B is $n \times 1$, C is $1 \times n$ and $d \in R$. By the induction hypothesis, $A = D + U$ where D is a diagonal involution and U is a unit.

Now $CU^{-1}B \in R = \alpha$, say. Then $d - \alpha = \nu + \iota$, where ν is a unit and ι is an involution. So we may write

$$M = \begin{pmatrix} U & B \\ C & \nu + \alpha \end{pmatrix} + \begin{pmatrix} D & 0 \\ 0 & \iota \end{pmatrix}.$$

Clearly the second term is a diagonal involution, so it remains to show that the first term is a unit. If

$$P = \begin{pmatrix} I & 0 \\ -CU^{-1} & 1 \end{pmatrix} \quad \text{and} \quad Q = \begin{pmatrix} U^{-1} & -U^{-1}B\nu^{-1} \\ 0 & \nu^{-1} \end{pmatrix}$$

then P, Q are both invertible. Moreover a straightforward check shows that

$$PMQ = \begin{pmatrix} I & 0 \\ 0 & 1 \end{pmatrix}$$

and hence M is a unit as required. □

Our next result is well known and its proof is elementary.

Lemma 1.4. *Let M be an R-module where $2 \in \mathrm{Aut}(M)$. If v is any involutary automorphism of M and 1_M denotes the identity in $\mathrm{End}_R(M)$, then $M = \mathrm{Ker}(1_M - v) \oplus \mathrm{Ker}(1_M + v)$.*

Proof. Let $m \in \ker(1_M - v) \cap \ker(1_M + v)$. Since $m(1_M - v) = 0$, we have $m = mv$. Therefore $m(1_M + v) = m + mv = 2m$. Since $m \in \ker(1_M + v)$, it follows that $m = 0$. Therefore $\ker(1_M - v) \cap \ker(1_M + v) = 0$.

Now let x be an arbitrary element of M. If $x(1_M - v) \neq 0$ then $(x - xv)(1_M + v) = x - xv + xv - x = 0$. Therefore, $x - xv \in \ker(1_M + v)$. Similarly, if $x(1_M + v) \neq 0$ then $(x + xv)(1_M - v) = x + xv - xv + x = 0$. So $x + xv \in \ker(1_M - v)$. Therefore we may write x in the form $x = \frac{1}{2}((x - xv) + (x + xv))$ where $(x - xv) \in \ker(1_M + v)$ and $(x + xv) \in \ker(1_M - v)$. □

Recall that an R-module M may have unit sum number 2 even when R itself does not have this property — the free Abelian group of rank 2 provides a simple example. This cannot, however, happen with the stronger involution property.

Theorem 1.5. *Let R be a ring; then a free R-module has the involution property only if R has the property.*

Proof. Suppose that M is a free $\mathbf{R}$-module and assume for a contradiction that $\mathrm{End}_R(M)$ has the involution property but R does not.

Observe firstly that 2 is a unit of R; otherwise 2 is not an automorphism of M, contrary to Proposition 1.1. We show that for any $\lambda \in R$ either $\lambda + 1$ or $\lambda - 1$ is a unit.

Now, $\lambda 1_M \in \mathrm{End}_R(M)$ and so $\lambda 1_M = \alpha + v$ for some $\alpha, v \in \mathrm{Aut}(M)$ and v an involution. By Lemma 1.4, we may write $M = \mathrm{Ker}(1_M + v) \oplus \mathrm{Ker}(1_M - v) = M_1 \oplus M_2$, say; note that one of M_1, M_2 is non-zero. But then α acts diagonally on M as multiplication by $\lambda + 1$ on M_1 and $\lambda - 1$ on M_2. Since α is an automorphism this forces the multiplications to be units and so at least one of $\lambda + 1$, $\lambda - 1$ is a unit.

Now if r is an arbitrary element of R, we may write $r = (r + 1) - 1$ and $r = (r - 1) + 1$. Since both 1 and -1 are involutions of R, it is possible to write r as the sum of a unit and an involution — a contradiction. □

We can immediately deduce:

Corollary 1.6. *Let M be a free R-module of finite rank. Then M has the involution property if and only if R has.*

2. Completely decomposable groups

In this section we consider the involution property for completely decomposable groups. We begin by recalling some definitions and properties of rational groups.

Let G be a torsion-free Abelian group and g any element of G. For a prime $p \in \mathbb{P}$, the p-height of g in G, written $h_p(g)$, is $n \in \mathbb{N}$ if $g \in p^n G$ but $g \notin p^{n+1}G$; we put $h_p(g) = \infty$ if $g \in p^n G$ for all $n \in \mathbb{N}$. If necessary, we write $h_p^G(g)$ or $h^G(g)$ to indicate that we are considering the p-height of g within the group G.

For G a torsion-free Abelian group and x an element of G, the characteristic of x in G, written $\chi_G(x)$, is the sequence of p-heights of x for each $p \in \mathbb{P}$, i.e. $\chi_G(x) = (h_p^G(x))_{p\in\mathbb{P}}$.

Two characteristics $(k_p)_{p\in\mathbb{P}}$ and $(l_p)_{p\in\mathbb{P}}$ are said to be equivalent, written $(k_p)_{p\in\mathbb{P}} \sim (l_p)_{p\in\mathbb{P}}$, if $\{p \in \mathbb{P} \mid k_p \neq l_p\}$ is finite and wherever $k_p \neq l_p$ then both k_p and l_p are finite. An equivalence class of characteristics with respect to this relation is called a type. The type of $x \in G$, written $\text{type}_G(x)$, is the equivalence class of $\chi_G(x)$ with respect to this equivalence relation. A group G is said to be a rational group if G is torsion-free of rank 1 or, equivalently, G is a subgroup of $\mathbb{Q}$; note that all elements of G must be of the same type so we define the type of G as $\text{type}(G) := \text{type}_G(x)$ for any $x \in G$. It is well known that rational groups G and G' are isomorphic if and only if $\text{type}(G) = \text{type}(G')$ — see [7, Theorem 85.1].

Next we describe the endomorphism rings of rational groups; for this purpose it is useful to introduce the following:

Definition 2.1. Let $\tau = (k_p)_{p\in\mathbb{P}}$ be a type. Then the reduced type of τ is $(l_p)_{p\in\mathbb{P}}$ where $l_p = \infty$ for each $p \in \mathbb{P}$ with $k_p = \infty$ and where $l_p = 0$ otherwise.

Lemma 2.2. *Let G be any rational group. Then the endomorphism ring of G is the subring of $\mathbb{Q}$ containing $\mathbb{Z}$ whose type is the reduced type of G.*

Proof. See [1, Theorem 1.5 (b)]. □

For any rational group G define $X_G = \{p \in \mathbb{P} \mid \frac{1}{p} \notin \text{End}_{\mathbb{Z}}(G)\}$. In other words, X_G is the set of primes which have finite entries in the type of G.

At this point we recall some definitions: a group is said to be a completely decomposable group if it is a direct sum of rational groups and it is said to a homogeneous completely decomposable group if it is a direct sum of rational groups each of the same type. The set of critical types, $T_{\text{cr}}(G)$, of a completely decomposable group G is the set of types of the rational groups which occur as summands in the decomposition of G into rational groups.

Decompositions of a completely decomposable group into direct sums of rational groups are unique up to isomorphism — see [7, Proposition 86.1].

Notation 2.3. *Let G be a completely decomposable group. Then, in the decomposition of G into rational groups, given any $t \in T_{\text{cr}}(G)$, we denote by $G_{(t)}$ the direct sum of all rational groups of type t, i.e. the t-homogeneous component of G. In this way we may write $G = \bigoplus_{t\in T_{\text{cr}}(G)} G_{(t)}$ as a decomposition of G into homogeneous summands of distinct types.*

Theorem 2.4. *Let $G = \bigoplus_{i\in I} R_i$ be a homogeneous completely decomposable group of arbitrary rank, where R_i is a rational group of type t for each $i \in I$. Let the reduced type of t be τ and let $R_\tau = \text{End}(R_i)$ be the subring of the rational numbers $\mathbb{Q}$, containing $\mathbb{Z}$, of type τ. Then,* $\text{End}(G)$ *is ring isomorphic to* $\text{End}(\mathcal{R})$*, the endomorphism ring of $\mathcal{R} = \bigoplus_{i\in I} R_\tau$.*

Proof. By Lemma 2.2, it follows that $\text{Hom}(R_i, R_j) \cong R_\tau$, for each $i, j \in I$. Then, it is easily seen that $\text{End}(G) \underset{ring}{\cong} \text{End}(\mathcal{R})$ since both are isomorphic to the ring of row-finite $|I| \times |I|$ matrices over R_τ. □

Theorem 2.5. *A rational group G has the involution property if and only if* 2 *is a unit in* $\text{End}(G)$ *and* $|X_G| \leq 1$.

Proof. Let $R = \text{End}(G)$ and note that the only elements of R which are involutions are 1 and -1.

Let $\frac{1}{2} \in R$ and $|X_G| = 0$. Then, by Lemma 2.2, $R = \mathbb{Q}$ which certainly has the property that every element is a sum of a unit and an involution. Now let $\frac{1}{2} \in R$ and $|X_G| = 1$; in other words, let $X_R = \{q\}$ for some $q \in \mathbb{P} \setminus \{2\}$, i.e. $R = \mathbb{Z}_{(q)}$ the localization of $\mathbb{Z}$ at q. Then let $\frac{a}{b}$ be an arbitrary non-zero element of R with $(a, b) = 1$, so there exist non-zero integers k, l such that $ka + lb = 1$. Now $k(\frac{a}{b}) + l$ is an element of R and $(k(\frac{a}{b}) + l)(b) = 1$. Therefore b is a unit of R.

If $a = \pm b$ then $\frac{a}{b} = 2 - 1$ or $-2 + 1$ expresses $\frac{a}{b}$ as a sum of a unit and an involution.

We now consider when $a \neq \pm b$. Recall that b is a unit, so $q \nmid b$ and thus if $q \mid a + b$ then $q \nmid (a + b) - 2b = a - b$. Similarly, if $q \mid a - b$ then $q \nmid a + b$. In this way there are only two cases:

- If $q \nmid (a + b)$: thus $a + b$ is a unit and we may write $\frac{a}{b} = \frac{a+b}{b} - \frac{b}{b} = \frac{a+b}{b} - 1$, a sum of a unit and an involution.

- If $q \nmid (a-b)$: then $a-b$ is a unit and we may write $\frac{a}{b} = \frac{a-b}{b} + \frac{b}{b} = \frac{a-b}{b} + 1$, a sum of a unit and an involution.

It remains to prove the other direction. By Proposition 1.1, R does not have the involution property unless $\frac{1}{2} \in R$, so we proceed with $\frac{1}{2} \in R$ and $|X_R| > 1$, i.e. let $\{q, r\} \subseteq X_R$ with $q \neq r$.

Choose any $b \in \mathbb{Z} \setminus \{0\}$ such that $b \equiv 2 \bmod q$ and $b \equiv -2 \bmod r$. The Chinese Remainder Theorem — see e.g. [14, II, Theorem 6.2] — guarantees the existence of many such b's. Then $\frac{2}{b}$ is not the sum of an involution and a unit of R since: $\frac{2}{b} - 1 = \frac{2-b}{b}$ is not a unit because q divides $(2-b)$ and $\frac{2}{b} + 1 = \frac{2+b}{b}$ is not a unit because r divides $(2+b)$. □

Note that the only subrings of $\mathbb{Q}$ having the involution property are $\mathbb{Q}$ itself and the localization $\mathbb{Z}_{(p)}$ at a prime $p \neq 2$. Before attempting to derive a corresponding result for certain completely decomposable groups, we note the following general result. In fact it is easy to modify Proposition 1.3 to show that the direct sum of two modules with the involution property again has the involution property, but we are unable to determine in general whether the involution property is inherited by summands.

Lemma 2.6. *Let $G = A \bigoplus B$ be the direct sum of two arbitrary groups with $\mathrm{Hom}(A, B) = 0$. Then G has the involution property if and only if both A and B do.*

Proof. Let ϕ be an arbitrary endomorphism of G written as $\phi = \begin{pmatrix} \phi_{A,A} & 0 \\ \phi_{B,A} & \phi_{B,B} \end{pmatrix}$ where $\phi_{A,A} \in \mathrm{End}(A)$, $\phi_{B,B} \in \mathrm{End}(B)$, $\phi_{B,A} \in \mathrm{Hom}(B, A)$.

Direct calculation shows that ϕ is an automorphism of G if and only if $\phi_{A,A}$ and $\phi_{B,B}$ are automorphisms of A and B respectively; moreover ϕ is an involution if and only if $\phi_{A,A}$ and $\phi_{B,B}$ are involutary automorphisms of A and B respectively.

Now assuming that A does not have the involution property, we may choose some $\psi \in \mathrm{Hom}(A, A)$ such that ψ is not a sum of an automorphism and an involutary automorphism of A. Then any $\phi \in \mathrm{End}(G)$ with $\phi_{A,A} = \psi$ cannot be a sum of two automorphisms, one of which is an involution. Conversely observe that since $\mathrm{Hom}(A, B) = 0$, both $\mathrm{End}(A)$ and $\mathrm{End}(B)$ are ring epimorphic images of $\mathrm{End}(G)$. However, it is immediate that the involution property is preserved under such epimorphic images. □

Before we tackle the general problem of completely decomposable groups, let us consider the somewhat easier problem of determining the homogeneous completely decomposable groups which have the involution property.

Proposition 2.7. *Let $G = \bigoplus_{i \in I} G_i$ be a reduced homogeneous completely decomposable group of type τ. Then G has the involution property if and only if the following hold:*

(i) *the first entry in the type τ is ∞;*
(ii) *the type τ has exactly one finite entry;*
(iii) *the index set I is finite.*

Proof. Note firstly that if R_0 is the subring of $\mathbb{Q}$ with type τ_0 equal to the reduced type of τ, then as noted in Theorem 2.4, the endomorphism ring of G coincides with the endomorphism ring of the free R_0-module of rank $|I|$. Suppose that G has the involution property. Then by Proposition 1.1, 2 is an automorphism of G and hence of G_i. Thus (i) follows. Since the free R_0-module has the involution property, it follows from Theorem 1.5 that R_0 also has it and hence τ_0 has at most one finite entry. Since G is reduced, τ_0 has exactly one finite entry. However a type and its reduced type always have the same number of finite entries, so (ii) now follows. Finally if I is an infinite set, then an easy modification of Lemma 3.6 below — see also Remark 3.7 — leads to a contradiction and so (iii) holds.

Conversely, suppose that (i)–(iii) hold. In this situation G is just a finite direct sum of groups each of which has the involution property by Theorem 2.5. It follows as in Proposition 1.3 that G has the involution property. □

Theorem 2.8. *Let $G = \bigoplus_{t \in T_{\mathrm{cr}}(G)} G_{(t)}$ be a reduced completely decomposable group, where $G_{(t)}$ denotes the t-homogeneous component of G. Then G has the involution property if and only if each homogeneous component has the involution property.*

Proof. Choose an arbitrary $t' \in T_{\mathrm{cr}}(G)$ and set $A = \bigoplus_{\substack{t>t' \\ t\in T_{\mathrm{cr}}(G)}} G_{(t)}$, $B = G_{(t')}$ and $C = \bigoplus_{\substack{t\not\geq t' \\ t\in T_{\mathrm{cr}}(G)}} G_{(t)}$; note that $G = (A \oplus B) \oplus C$. Now, since a homomorphism cannot map an element onto an element of lesser or incomparable type, we know that $\mathrm{Hom}(A, B) = 0 = \mathrm{Hom}((A \bigoplus B), C)$. It follows from two applications of Lemma 2.6 that B, the t'-homogeneous component of G, has the involution property.

Conversely, suppose that each t-homogeneous component $G_{(t)}$ of G has the involution property. Then, by Proposition 2.7, each type in $T_{\mathrm{cr}}(G)$ has exactly one finite entry and so any pair of types in $T_{\mathrm{cr}}(G)$ is incomparable. Hence the endomorphism ring, $\mathrm{End}(G)$, is simply the ring direct product of the corresponding endomorphism rings $\mathrm{End}(G_{(t)})$ and so G has the involution property. □

Corollary 2.9. *A completely decomposable group G has the involution property if and only if it has the form $G = \mathbb{Q}^{(\kappa)} \oplus \bigoplus_{p\in\mathbb{P}'} G_p$, where κ is an arbitrary cardinal, $\mathbb{P}' \subseteq \mathbb{P}$ and each G_p is a finite direct sum of copies of $\mathbb{Z}$ localized at the prime $p \neq 2$.*

Proof. Since there are no non-trivial homomorphisms from a divisible group into a reduced group, it follows from Lemma 2.6 that G has the involution property if and only if both its reduced and divisible components have the property. The divisible part always has the involution property since it is just a vector space. So G has the involution property if and only if its reduced component has and the result follows from Theorem 2.8 and our earlier observation that a rank one group having exactly one finite entry in its type is just a localization of $\mathbb{Z}$ at the prime corresponding to the finite entry. □

3. Complete modules

In this last section we provide some results which will be helpful in considering modules which are complete in their p-adic topologies. The line of approach is similar to that used previously to investigate the n-sum property; see [13]. For simplicity we shall consider torsion-free modules over the ring of p-adic integers, J_p, only; there are clear generalizations to complete discrete valuation rings.

Recall that the Jacobson Radical of a ring R, denoted as $J(R)$, is the intersection of all the maximal right ideals or all the maximal left ideals of R and that for any $x \in R$, $x \in J(R)$ if and only if for all $y, z \in R$, $1 - zxy \in U(R)$, where $U(R)$ denotes the group of units of R.

Our first result is the familiar fact that when a p-adic module is complete, the Jacobson radical of its endomorphism algebra is easy to determine.

Lemma 3.1. *Let M be a torsion-free complete p-adic module. Then $J(\mathrm{End}(M)) = p\mathrm{End}(M)$ and $\mathrm{End}(M)$ is complete in its J-adic topology.*

Proof. See [17, Theorem 2.3]. □

Our next result is the familiar fact that involutions may "be lifted" when the ring is complete in its J-adic topology; the proof is a simple modification of the standard result on lifting idempotents — see e.g. [5, Proposition 18.21].

Lemma 3.2. *Let E be a ring such that E is complete in its J-adic topology and 2 is a unit in E. Let $\bar{E} = E/J(E)$. Then for any $\mu \in \bar{E}$ with $\mu^2 = 1_{\bar{E}}$, where $1_{\bar{E}}$ is the identity in $\bar{E}$, there exists $i \in E$ such that $\bar{i} = \mu$ and $i^2 = 1_E$ where 1_E is the identity in E.*

With these preliminaries, it is easy to determine whether a ring R has the involution property by considering its quotient $R/J(R)$.

Theorem 3.3. *Let E be a ring such that E is complete in its J-adic topology, with 2 a unit of E. If $E/J(E)$ has the involution property then E also has this property.*

Proof. Take an arbitrary $\theta \in E$. We are given $(\theta + pE) = (\alpha + J(E)) + (\beta + J(E))$ where $(\alpha + J(E))$ is a unit of $E/J(E)$, and $(\beta + J(E))$ is an involution of $E/J(E)$. By Lemma 3.2 there exists i, an involution in E, such that $(i + J(E)) = (\beta + J(E))$. Therefore we can write $\theta = (\alpha + \gamma + i)$ for some $\gamma \in J(E)$. Now we show that $(\alpha + \gamma)$ is a unit of E: $(\alpha + J(E)) = ((\alpha + \gamma) + J(E))$ is a unit of $E/J(E)$. Therefore there exists $\phi \in E$ such that $(\phi + J(E))$ is a right inverse of $((\alpha + \gamma) + J(E))$.

It follows that $(\alpha+\gamma)\phi - 1_E \in J(E)$, where 1_E is the identity in E and so, by the properties of the Jacobson Radical, $(\alpha + p\gamma)\phi$ is a unit in E. Writing $(\alpha+\gamma)(\phi((\alpha+\gamma)\phi)^{-1}) = 1_E$ we see that $(\alpha+\gamma)$ has a right inverse. A similar argument shows that $(\alpha+\gamma)$ also has a left inverse. Therefore $(\alpha+\gamma)$ is a unit in E. □

Lemma 3.4. *Let $M = \bigoplus_{i\in I} J_p e_i$ be a reduced torsion-free p-adic module of non-trivial rank. Let $\widehat{M}$ be the p-adic completion of M. Then*

$$\mathrm{End}_{J_p}(\widehat{M})/p\mathrm{End}_{J_p}(\widehat{M}) \underset{ring}{\cong} \mathrm{End}_{J_p}(M)/p\mathrm{End}_{J_p}(M) \underset{ring}{\cong} \mathrm{End}_{\mathbb{Z}/p\mathbb{Z}}(M/pM).$$

Proof. See e.g. [13, Lemma 2.11]. □

It is now easy to derive our desired result that complete torsion-free p-adic modules ($p \neq 2$) have the involution property.

Theorem 3.5. *A torsion-free complete p-adic module has the involution property if and only if $p \neq 2$.*

Proof. If $p \neq 2$ then, modulo its Jacobson radical, the endomorphism algebra of a complete p-adic module is isomorphic to the endomorphism algebra of a vector space. The result then follows from Ó Searcóid's result on vector spaces, Proposition 1.2 and Theorem 3.3. The converse is immediate from Proposition 1.1. □

Although vector spaces of arbitrary dimension have the involution property, this property does not hold for free J_p-modules.

Lemma 3.6. *If the p-adic module G ($p \neq 2$) has a free direct summand of infinite rank, then G does not have the involution property.*

Proof. Suppose that $G = B \oplus H$, where $B = \bigoplus_{i<\omega} J_p e_i$ is a free J_p-adic module of countable rank. Define a mapping $\phi : G \to G$ by

$$x\phi = \begin{cases} e_i + pe_{i+1} : & x = e_i \\ x : & x \in H. \end{cases}$$

Note firstly that $\phi + 1$ is not an automorphism of G: a straightforward calculation shows that e_1 is not in the image of $\phi + 1$. Suppose, for a contradiction, that ϕ can be expressed as $\phi = \nu + \alpha$, where ν is an involution and α is an automorphism of G. Then post-multiplication by $1 + \nu$ yields $(\phi - 1)(1 + \nu) = \alpha(1 + \nu)$ and so $G(\phi - 1)(1 + \nu) = G\alpha(1 + \nu) = G(1 + \nu)$. Hence $G(1 + \nu) = G(\phi - 1)(1 + \nu) \subseteq pG$. But now if $g \in G$, then $g(1 + \nu)^2 = 2g(1 + \nu) \in p^2G$ and so, since $p \neq 2$, $g(1 + \nu) \in p^2G$. Continuing in this way one sees that $G(1 + \nu) \subseteq p^\omega G = 0$. Thus $\nu = -1$ and so $\phi + 1$ is an automorphism — a contradiction. □

Remark 3.7. It is clear that the above argument may be generalized to modules over a much wider class of rings; in particular, it is easy to see that an identical proof holds for proper subrings of the ring of rationals, $\mathbb{Q}$.

Theorem 3.8. *A free p-adic module ($p \neq 2$) has the involution property if and only if it is of finite rank.*

Proof. Since $p \neq 2$, the ring J_p itself has the involution property and hence, by Proposition 1.3, the same is true of any free module of finite rank. The converse follows immediately from Lemma 3.6 since a free module of infinite rank has a summand which is free of countable rank. □

Despite the failure of the involution property for free J_p-modules of infinite rank, torsion-free J_p-modules having the involution property exist in abundance. We shall show below that a p-adic module G with endomorphism algebra $\mathrm{End}_{J_p}(G)$ equal to the split extension of the ideal, $\mathrm{End}_0(G)$, of endomorphisms having finite rank images, by J_p, has the involution property. In fact, such modules of arbitrarily large rank have been constructed previously by Dugas et al. [3] and are easily constructed now with the help of so-called realization theorems based on the combinatorics of Shelah's Black Box — see e.g. [4]. The first author has also constructed "small" modules which can be shown to have the involution property [10]; interestingly these modules are of corank one in their p-adic completion. The existence in such abundance of modules with the involution property suggests that no reasonable classification of J_p-modules with the property exists.

Proposition 3.9. *If G is a torsion-free J_p-module ($p \neq 2$) with $\mathrm{End}_{J_p}(G) = J_p \oplus \mathrm{End}_0(G)$, then every endomorphism of G is the sum of a unit and an involution.*

Proof. Let ψ be an arbitrary endomorphism of G having finite rank image. Thus the image of G under ψ is free and so G splits as $G = K_1 \oplus F_1$ where K_1 is the kernel of ψ and F_1 is free of finite rank. If $S = F_1 + F_1\psi$ then S is finitely generated and so is again free of finite rank. Hence $K_1 \cap S$ can be embedded in a finite rank summand N of K_1; say $G = K \oplus N \oplus F_1 = K \oplus F$. Thus K is a summand of Ker ψ and F is free of finite rank. Moreover $F\psi \subseteq F$; this follows since if $x \in F$ then $x\psi = (n + f_1)\psi = f_1\psi$, where $n_1 \in N$, $f_1 \in F$. But $f_1\psi = k_1 + f_2$ with $k_1 \in K_1$, $f_2 \in F_1$ and so $k_1 = f_1\psi - f_2 \in K_1 \cap S \subseteq N$. Hence $x\psi = f_1\psi = k_1 + f_2 \in N + F_1 = F$.

Now consider an arbitrary endomorphism ϕ of G; this has the form $\phi = r + \psi$, where $r \in J_p$ and ψ has an image of finite rank. Since F is free of *finite* rank and $r + \psi \restriction F$ is an endomorphism of F, it is possible to write, by Proposition 1.3, $r + \psi \restriction F = \nu + \alpha$ where ν is an involution and α is an automorphism of F. Moreover, the p-adic integer r can be expressed, since $p \neq 2$, as $r = s + t$ where $s \in \{1, -1\}$ and t is a unit.

Now define endomorphisms γ, δ of $G = K \oplus F$ as follows:

$$k\gamma = sk, \qquad f\gamma = f\nu \qquad \text{and} \qquad k\delta = tk, \qquad f\delta = f\alpha.$$

Clearly γ is an involution and δ is a unit. Moreover, the sum $\gamma + \delta = r + \psi = \phi$ since $K \subseteq$ Ker ψ. This completes the proof. □

References

[1] V.P. Camillo, H.-P. Yu, Exchange rings, units and idempotents, Comm. Algebra 22 (1994) 4737–4749.
[2] F. Castagna, Sums of automorphisms of a primary abelian group, Pacific J. Math. 27 (3) (1968) 463–473.
[3] M. Dugas, R. Göbel, B. Goldsmith, Representation of algebras over a complete discrete valuation ring, Q. J. Math. 35 (1984) 131–146.
[4] P. Eklof, A. Mekler, Almost Free Modules, Set-theoretic Methods, revised edition, North-Holland, 2002.
[5] C. Faith, Algebra II, Ring Theory, in: Grundlehren der mathematischen Wissenschaften, vol. 191, Springer-Verlag, Berlin, Heidelberg, New York, 1976.
[6] L. Fuchs, Infinite Abelian Groups I, Academic Press, New York, 1970.
[7] L. Fuchs, Infinite Abelian Groups II, Academic Press, New York, 1973.
[8] L. Fuchs, Recent results and problems on abelian groups, in: Topics in Abelian Groups, Chicago, 1963, pp. 9–40.
[9] R. Göbel, A. Opdenhövel, Every endomorphism of a local Warfield module of finite torsion-free rank is the sum of two automorphisms, J. Algebra 233 (2000) 758–771.
[10] B. Goldsmith, Essentially indecomposable modules over a complete discrete valuation ring, Rend. Sem. Mat. Univ. Padova 70 (1983) 21–29.
[11] B. Goldsmith, On endomorphisms and automorphisms of some torsion-free modules, in: Abelian Group Theory, Gordon and Breach, New York, 1987, pp. 417–423.
[12] B. Goldsmith, C. Meehan, S. Wallutis, Sums of automorphisms of rational Groups, Rocky Mountain J. 32 (2002) 1431–1439.
[13] B. Goldsmith, S. Pabst, A. Scott, Unit sum numbers of rings and modules, Q. J. Math. 49 (1998) 331–344.
[14] L.C. Grove, Algebra, Academic Press, San Diego, 1983.
[15] P. Hill, Endomorphism rings generated by units, Trans. Amer. Math. Soc. 141 (1969) 99–105.
[16] I. Kaplansky, Infinite Abelian Groups, The University of Michigan Press, 1962.
[17] W. Liebert, Endomorphism rings of reduced torsion-free modules over complete discrete valuation rings, Trans. Amer. Math. Soc. 169 (1972) 347–363.
[18] C. Meehan, Unit sum numbers of abelian groups and modules, Ph.D. Thesis, Dublin Institute of Technology, 2001.
[19] C. Meehan, Sums of automorphisms of free abelian groups and modules, Math. Proc. R. Ir. Acad. 104A (1) (2004) 59–66.
[20] C. Meehan, Sums of automorphisms of free modules and completely decomposable groups, J. Algebra (in press).
[21] W.K. Nicholson, Lifting idempotents and exchange rings, Trans. Amer. Math. Soc. 229 (1977) 269–278.
[22] W.K. Nicholson, Strongly clean rings and Fitting's Lemma, Comm. Algebra 27 (1999) 3583–3592.
[23] M. Ó Searcóid, Perturbation of linear operators by idempotents, Bull. Irish Math. Soc. 39 (1997) 10–13.
[24] D. Zelinsky, Every linear transformation is a sum of nonsingular ones, Proc. Amer. Math. Soc. 5 (1954) 627–630.