2001-01-01

Unit Sum Numbers of Abelian Groups and Modules

Christopher Meehan

Technological University Dublin

§2 Definitions and known results

We now present basic definitions and well–known results which will be used in the following chapters. Firstly we recall definitions and results regarding endomorphisms.

Definition 2.1 *Let G be a group and ϕ an endomorphism of G. If, for each $g \in G$, there is some $n \in \mathbb{N}$, n depending on g, such that $g\phi^n = 0$ then ϕ is said to be* locally nilpotent.

There are certain useful kinds of endomorphisms of free modules. Recall that M is a *free module* if M is generated by a linearly independent set of elements, called a *basis* of M; that is $M = \bigoplus\limits_{i \in I} Re_i$ for some index set I where $\mid I \mid$ is the rank of M. Furthermore we define the *support* of elements $m = \sum\limits_{i \in I} r_i e_i$ of M by $[m] = \{i \in I \mid r_i \neq 0\}$ and the support of $0 \in M$ is the empty–set $\emptyset$. Note that the support depends on the choice of basis and that $[m]$ is finite for any $m \in M$.

Definition 2.2 *Let R be a commutative ring and $M = \bigoplus\limits_{i \in I} Re_i$ a free R–module of arbitrary rank with I a linearly ordered set and ϕ an endomorphism of M. We define*

(i) *ϕ is an* α–endomorphism *of M if $[e_i\phi] \subseteq \{j \in I | j > i\}$, for each*

$i \in I$.

(ii) *ϕ is a β* -endomorphism *of M if $[e_i\phi] \subseteq \{j \in I | j < i\}$, for each $i \in I$.*

(iii) *ϕ is an d*-endomorphism *of M if $[e_i\phi] \subseteq \{i\}$, for each $i \in I$.*

Note, if ϕ is represented as a matrix then an α-endomorphism has non-zero entries only in the upper triangle, a β-endomorphism has non-zero entries only in the lower triangle and a d-endomorphism has non-zero entries only on the diagonal.

Lemma 2.3 *Let R be a commutative ring and $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ a free R-module. If ϕ is a β-endomorphism of M then ϕ is locally nilpotent.*

Proof: Consider any arbitrary basis element e_k, $k < n$. Since ϕ is a β-endomorphism of M we have $[e_k\phi] \subseteq \{0, \ldots, k-1\}$, $[e_k\phi^2] \subseteq \{0, \ldots, k-2\}$, $\ldots$, $[e_k\phi^k] \subseteq \{0\}$, and so it is clear that $e_k\phi^{k+1} = 0$. Therefore ϕ is locally nilpotent. □

Theorem 2.4 (*Wans* [29]) *If R is a PID and F is a free R-module of finite rank $n > 1$, then* $\mathrm{usn}(F) = 2$.

Proof: As above let F be a free module with rk$(F)= n > 1$, say $F = \bigoplus_{i<n} Re_i$. Further, let ϕ be an arbitrary endomorphism of F. Then there are two automorphisms $\eta, \zeta \in Aut(F)$ such that $\phi' = \eta\phi\zeta$ acts 'diagonally', that is $e_i\phi' = s_ie_i$ for some $s_i \in R$, for each $i < n$.

(This is the so-called Smith Normal Form, see [4, page 279]).

Next decompose F as $F = \bigoplus_j F_j$ where each F_j is generated by a distinct pair e_{j_1}, e_{j_2} of the original generators except, where n is odd, for F_0; in which case F_0 is generated by the triple e_0, e_1, e_2.

Clearly $F_j\phi' \subseteq F_j$ and ϕ' decomposes into a direct sum $\phi' = \sum_j \phi'_j$ where $\phi'_j = \phi' \restriction_{F_j}$, for each j.

Now, if rk $(F_j) = 2$, write $\phi'_j = \alpha_{j.1} + \alpha_{j.2}$ with

$$e_{j_1}\alpha_{j.1} = s_{j_1}e_{j_1} + e_{j_2}, \quad e_{j_2}\alpha_{j.1} = -e_{j_1}$$

$$\text{and } e_{j_1}\alpha_{j.2} = -e_{j_2}, \quad e_{j_2}\alpha_{j.2} = e_{j_1} + s_{j_2}e_{j_2}$$

We show that $\alpha_{j.1}$ and $\alpha_{j.2} \in Aut(F_j)$: Since $e_{j_1} = (-e_{j_2}\alpha_{j.1})$ and $e_{j_2} = (e_{j_1} + s_{j_1}e_{j_2})\alpha_{j.1}$ we have that $\alpha_{j.1}$ is onto F_j. Let $(ae_{j_1} + be_{j_2})\alpha_{j.1} = 0$, for some $a, b \in R$. Then $-be_{j_1} + as_{j_1}e_{j_1} + ae_{j_2} = 0$ which, of course, implies $a = 0$, $b = 0$. So $\alpha_{j.1}$ is injective. Therefore $\alpha_{j.1} \in Aut(F_j)$. A similar argument applies for $\alpha_{j.2}$.

If rk$(F_0) = 3$, then write $\phi'_0 = \alpha_{0.1} + \alpha_{0,2}$ where $e_{0_1}\alpha_{0.1} = s_{0_1}e_{0_1} + e_{0_3}$,

$$e_{0_2}\alpha_{0,1} = e_{0_1}, \quad e_{0_3}\alpha_{0,1} = s_{0_3}e_{0_3} - e_{0_2}, \text{ and } e_{0_1}\alpha_{0,2} = -e_{0_3},$$
$$e_{0_2}\alpha_{0,2} = -e_{0_1} + s_{0_2}e_{0_2}, \quad e_{0_3}\alpha_{0,2} = e_{0_2}.$$

We show $\alpha_{0,1}$ and $\alpha_{0,2} \in Aut(F_0)$: Since we may write $e_{0_1} = e_{0_2}\alpha_{0,1}$ and $e_{0_2} = (-e_{0_3} + s_{0_3}e_{0_1} - s_{0_3}s_{0_1}e_{0_2})\alpha_{0,1}$ and $e_{0_3} = (e_{0_1} - s_{0_1}e_{0_2})\alpha_{0,1}$ we have that $\alpha_{0,1}$ is onto. Let $0 = ae_{0_1} + be_{0_2} + ce_{0_3}$, where $a, b, c \in R$. Then $0 = a(s_{0_1}e_{0_1} + e_{0_3}) + b(e_{0_1}) + c(e_{0_2}) = (as_{0_1} + b)e_{0_1} + ce_{0_2} + ae_{0_3}$. It is easily seen that $a = b = c = 0$. So $\alpha_{0,1}$ is injective and $\alpha_{0,1} \in Aut(F_0)$. A similar argument applies for $\alpha_{0,2}$.

Clearly, $\alpha_1 = \sum_j \alpha_{j,1}$ and $\alpha_2 = \sum_j \alpha_{j,2}$ are automorphisms of F with $\phi' = \alpha_1 + \alpha_2$ and so $\phi = \eta^{-1}\alpha_1\zeta^{-1} + \eta^{-1}\alpha_2\zeta^{-1}$, a sum of two automorphisms. □

For a free module of countably infinite rank the following has been shown by Wans[29].

Theorem 2.5 *Let R be a PID and let M be a free R-module of countably infinite rank. Then every endomorphism of M can be written as a sum of three automorphisms of M.*

Proof: See Wans [29, Theorem 3.4]. □

Note that one of the important results of this thesis is an improvement of the above Theorem: we will prove that usn(M)= 2 for any free R-module

M of countably infinite rank over any PID, R.

We proceed with some definitions and results from abelian group theory. We refer to the standard text books by Fuchs [7, 8].

Definitions 2.6

(i) *Let G be an abelian group and g any element of G. The p-*height *of g in G, written $h_p(g)$, is $n \in \mathbb{N}$ if $g \in p^nG$ but $g \notin p^{n+1}G$; we put $h_p(g)= \infty$ if $g \in p^nG$ for all $n \in \mathbb{N}$.*

Where we are refering to a p-group we talk of this as the height *of the element in the group and we write this as $h(g)$. 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.*

(ii) *Let G be a torsion-free abelian group and x an element of G. Then the* characteristic *of x in G, written $\chi_G(x)$, is the sequence of p-heights of x for each $p \in \Pi$, i.e. $\chi_G(x) = (h_p^G(x))_{p\in\Pi}$.*

(iii) *Every sequence $(k_p)_{p\in\Pi}$, where $k_p \in \mathbb{N}\cup\{\infty\}$, is a characteristic for some torsion-free abelian group. Let $(k_p)_{p\in\Pi}$ and $(l_p)_{p\in\Pi}$ be characteristics. These characteristics are said to be* equivalent, *written $(k_p)_{p\in\Pi} \sim (l_p)_{p\in\Pi}$, if $\{p \in \Pi \mid k_p \neq l_p\}$ 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.

(iv) *Let G be a torsion-free group and x an element of G. The* type *of $x \in G$, a torsion-free group, written* $\text{type}_G(x)$, *is the equivalence class of $\chi_G(x)$ with respect to the relation defined in* (iii).

(v) *A* rational group *G is a torsion-free abelian group of rank* 1.

(vi) *If G is a rational group then all elements of G must be of the same type (i.e. let $0 \neq x$, $y \in G$, then $mx = ny$ for some $0 \neq m, n \in \mathbb{Z}$; it is easily seen that $\chi(x) \sim \chi(mx) = \chi(ny) \sim \chi(y)$). So, we define the* type of G *as* $\text{type}(G) := \text{type}_G(x)$ *for any $x \in G$.*

Note that $\text{type}_G(x)$ (or $\text{type}(G)$) may be represented by any characteristic within $\text{type}_G(x)$ (or $\text{type}(G)$).

Remark 2.7 *Let G and G'' be rational groups, and x and y arbitrary non-zero elements of G and G', respectively. For any $k \in \mathbb{Z}$,*

if $\chi_G(kx)$= $\chi_{G'}(y)$, then k divides y in G'' uniquely. Moreover, for any elements $x, x' \in G$ if $\chi(x)$= $\chi(x')$ then $x = x'$ or $x = -x'$.

The next result is due to Baer [1].

Lemma 2.8 *Let G and G' be rational groups.*

Then G is isomorphic to G' if and only if type(G) = type(G').

Proof: Let ϕ be an isomorphism from G onto G' and let $0 \neq x \in G$ then $h_p^G(x)= h_p^{G'}(x\phi)$ for each $p \in \Pi$ since heights must be preserved under isomorphisms. Thus $\chi_G(x)= \chi_{G'}(x\phi)$ and therefore type(G)= type(G'). Conversely, let type(G)= type(G'). Firstly, fix non-zero elements $a \in G$, $b \in G'$ such that $\chi_G(a)= \chi_{G'}(b)$. This is possible since for any $a' \in G$, $b' \in G'$ we can find positive integers m, n with $\chi_G(ma')= \chi_{G'}(nb')$. Now, let x be any non-zero element of G. Since rk(G)= 1 there are non-zero integers r, s such that $rx = sa$ and thus $\chi_G(rx)= \chi_G(sa)= \chi_{G'}(sb)$. By Remark 2.7 there is $b_x \in G'$ such that $sb = rb_x$. Now we can define a mapping $\psi : G \longrightarrow G'$ by $x\psi = b_x$ and $0\psi = 0$. The mapping is well defined since, if $r'x = s'a$ and $s'b = r'b'_x$, then we have $rs' = r's$ and thus $r(s'b) = r'(sb) = rr'b'_x = r'rb_x$, i.e. $b_x = b'_x$.

Clearly, b_x is non-zero for any $0 \neq x \in G$ as b is non-zero and hence ψ is injective.

Moreover, for $0 \neq y \in G'$ we can find non-zero integers r, s with $ry = sb$. Using the same arguments as above we obtain $0 \neq x \in G$ such that

$sa = rx$ and so $x\psi = b_x$ with $sb = rb_x = ry$, i.e. $b_x = y$. Therefore ψ is a bijective mapping.

Finally it remains to show that ψ is a homomorphism. Let $0 \neq x_1, x_2 \in G$ with $r_1x_1 = s_1a$ and $r_2x_2 = s_2a$. Then $r_1r_2(x_1 + x_2) = (s_1r_2 + s_2r_1)a$ and therefore $r_1r_2b_{x_1+x_2} = (s_1r_2 + s_2r_1)b = r_2(s_1b) + r_1(s_2b) = r_1r_2(b_{x_1} + b_{x_2})$, i.e. $(x_1 + x_2)\psi = b_{x_1+x_2} = b_{x_1} + b_{x_2} = x_1\psi + x_2\psi$. □

The following lemma gives us an easy representative for each type.

Lemma 2.9 *Every rational group is isomorphic to a subgroup of the rational numbers, $\mathbb{Q}$, containing $\mathbb{Z}$.*

Proof: Let G be an arbitrary rational group. Let x be any non-zero element of G and let $\chi_G(x)=(k_p)_{p\in\Pi}$. Choose that subgroup S of $\mathbb{Q}$ containing $\mathbb{Z}$ where $\chi_S(1)=(k_p)_{p\in\Pi}$, i.e. $S = \left\langle \frac{1}{p^{k_p}} \mid p \in \Pi \right\rangle$ where we mean by "$\frac{1}{p^\infty}$" the set $\{\frac{1}{p^n} \mid n \in \omega\}$. Since $\chi_S(1)= \chi_G(x)$, and so type(G)= type(S) it follows from Lemma 2.8 that $S \cong G$. □

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

Definition 2.10 *Let $\tau = (k_p)_{p\in\Pi}$ be a type. Then the* reduced type *of τ is $(l_p)_{p\in\Pi}$ where $l_p = \infty$ for each $p \in \Pi$ with $k_p = \infty$ and where $l_p = 0$ otherwise.*

Lemma 2.11 *Let G be any rational group.*

Then the endomorphism ring of G is that subring of $\mathbb{Q}$ containing $\mathbb{Z}$ whose type is the reduced type of G.

Proof: Using Lemma 2.9, we may consider G to be a subgroup of $\mathbb{Q}$ containing $\mathbb{Z}$ without loss of generality. Let $0 \neq \phi \in E(G)$ and let $0 \neq x \in G$. Since G is a rational group there are non-zero integers m, n such that $mx = n(x\phi)$ and choosing (m,n)= 1 we can write $x\phi = \frac{m}{n}x$. In fact, take any $0 \neq y \in G$. We can write $y = \frac{a}{b}x$ for some a, $b \in \mathbb{Z}$, $b \neq 0$ where $(a,b) = 1$, and so $y\phi = (\frac{a}{b}x)\phi = \frac{m}{n}\frac{a}{b}x = \frac{m}{n}y$. In this way each endomorphism of G is a multiplication by a rational so $E(G) \leq \mathbb{Q}$. Since $E(G)$ certainly contains an identity then $\mathbb{Z} \subseteq E(G)$.

Now, letting $\chi_G(1)$=$(k_p)_{p\in\Pi}$ consider $\chi_{E(G)}(1)$. Assume $\frac{1}{p} \in E(G)$ for some arbitrary $p \in \Pi$, then $\frac{1}{p^2} \in E(G)$ and so $\frac{1}{p^n} \in E(G)$ for each $n \in \mathbb{N}$, i.e. so $h_p^{E(G)}(1)$= ∞. However, if $h_p^G(1)$= k_p is finite then $1(\frac{1}{p^{k_p+1}}) \notin G$ and so $\frac{1}{p} \notin E(G)$, i.e. $h_p^{E(G)}(1)$= 0. If $h_p^G(1)$= ∞ then $\frac{1}{p}$ is an allowable endomorphism of G and so $h_p^{E(G)}(1)$= ∞ in this case. Therefore $\chi_{E(G)}(1)$ is equivalent to the reduced type of G. □

Now we can introduce the following definition:

Definition 2.12 *Let G be any rational group. Then define*

$X_G = \{p \in \Pi \mid \frac{1}{p} \notin E_{\mathbb{Z}}(G)\}.$

X_G is the set of primes which have finite entries in type(G). A special role is played by direct sums of rational groups. Hence we introduce:

Definitions 2.13

(i) *A* completely decomposable group *is a direct sum of rational groups.*

(ii) *A* homogeneous *completely decomposable group is a direct sum of rational groups each of the same type.*

(iii) *The* type of a homogeneous completely decomposable group *is that of the rational groups which are its summands in its decomposition into rational groups.*

(iv) *The* set of critical types, *$T_{cr}(G)$, of a completely decomposable group G is the set of types of the rational groups which are its summands in its decomposition into rational groups.*

Decompositions of a completely decomposable group into direct sums of rational groups are unique up to isomorphism — see [8, Proposition 86.1].

Notation 2.14 *Let G be a completely decomposable group. Then, in the decomposition of G into rational groups, given any $t \in T_{cr}(G)$, 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 $G = \bigoplus_{t \in T_{cr}(G)} G_{(t)}$ as a decomposition of G into homogeneous summands of distinct types.*

Theorem 2.15 *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. Let $R_{(\tau)} = E(R)$ be that subring of the rational numbers $\mathbb{Q}$, containing $\mathbb{Z}$, of type τ.*

Then, $E(G)$, the endomorphism ring of G, is ring isomorphic to $E(\mathcal{R})$, the endomorphism ring of $\mathcal{R} = \bigoplus_{i \in I} R_\tau a_i$.

Proof: Since $G = \bigoplus_{i \in I} R_i$ we may write ϕ, any arbitrary endomorphism of G, as $\phi = \sum_{i,j \in I} \phi_{i,j}$ where $\phi_{i,j} \in Hom(R_i, R_j)$ for each $i, j \in I$. By Lemma 2.11, it follows that $Hom(R_i, R_j) \cong R_\tau$, that subring of $\mathbb{Q}$ containing $\mathbb{Z}$ with type τ, the reduced type of t. Since each R_i $(i \in I)$ is isomorphic to a subgroup of $\mathbb{Q}$ containing $\mathbb{Z}$, then any $\phi_{i,j} \in Hom(R_i, R_j)$ may be considered to be defined by its action on $1 \in R_i$, i.e. say $(1)\phi_{i,j} = r_{\phi_{i,j}}$ for some $r_{\phi_{i,j}} \in R_\tau$. Let $\mathcal{R} = \bigoplus_{i \in I} R_\tau a_i$. Then, $Hom(R_\tau a_i, R_\tau a_j) \cong R_\tau$ for each $i, j \in I$ in the same way we showed for $Hom(R_i, R_j)$. Now, define

$\Theta : E(\bigoplus_{i\in I} R_i)\longrightarrow E(\bigoplus_{i\in I} R_\tau a_i)$ by $\phi_{i,j} \longmapsto r_{\phi_{i,j}}$ where $r_{\phi_{i,j}} :(1a_i)\longmapsto r_{\phi_{i,j}}a_j$ for each $i,j \in I$. Since $\ker\Theta = \{\phi \in E(G); r_{\phi_{i,j}} = 0$ for each $i,j \in I\} = \{\phi \in E(G); \phi_{i,j} = 0$ for each $i,j \in I\} = \{\phi \in E(G); \phi = 0\} = 0$ and since by definition Θ is clearly surjective we have that θ is bijective. Now, given $\phi_{i,j}$, $\psi_{i,j}$, arbitrary elements of $Hom(R_i, R_j)$ for any arbitrary $i,j \in I$ then $(\phi_{i,j})\Theta+(\psi_{i,j})\Theta = r_{\phi_{i,j}} + r_{\psi_{i,j}} =(\phi_{i,j} + \psi_{i,j})\Theta$ for any $i,j \in I$; and given arbitrary $\phi_{i,k} \in Hom(R_i, R_k)$, $\psi_{k,j} \in Hom(R_k, R_j)$ for any arbitrary $i,j,k \in I$ then $(\phi_{i,k})\Theta(\psi_{k,j})\Theta = r_{\phi_{i,k}}r_{\psi_{k,j}} =(\phi_{i,k}\psi_{k,j})\Theta$. Therefore $E(G) \underset{ring}{\cong} E(\mathcal{R})$. □

We continue now considering some useful properties of rings.

Definition 2.16 *The* Jacobson Radical *of a ring R, denoted $J(R)$ is the intersection of all the maximal right ideals and all the maximal left ideals of R.*

Lemma 2.17 *Let R be a unital ring and $x \in R$. Then the following are equivalent.*

(i) *$x \in \mathcal{M}_r$, the intersection of all maximal right ideals of R.*

(ii) *$1 - xy$ is right invertible for any $y \in R$.*

(iii) *$Nx = 0$ for any simple right R–module N.*

Proof:

(i)$\Rightarrow$(ii): Let $x \in \mathcal{M}_r$ and assume $1 - xy$ has no right inverse for some $y \in R$. Then there exists a maximal right ideal I of R such that $1 - xy \in I$. But $x \in I$, so $1 - xy + xy \in I$. Therefore, since $1 \in I$, $I = R$, contradicting I being a maximal right ideal.

(ii)$\Rightarrow$(iii): Recall that a module with no non-trivial submodules is called simple. Let $1 - xy$ be right invertible for all $y \in R$ and suppose that $nx \neq 0$ for some $n \in N$. Then $(nx)R$ is a right R-submodule of N and is not zero, so $(nx)R = N$. In particular, $n = nxy$ for some $y \in R$ and so $n(1 - xy)= 0$. Now, since $1 - xy$ is right invertible then $n = 0$ contradicting our assumption.

(iii)$\Rightarrow$(i): If I is a maximal right ideal of R then R/I is a simple right R-module and so by (iii) $(R/I)x \equiv 0$. Thus $(1 + I)x = I$ so $x \in I$. Since I is an arbitrary maximal right ideal of R then $x \in \mathcal{M}_r$. □

Lemma 2.18 *For $x \in R$, a unital ring, the following are equivalent.*

(i) *$x \in \mathcal{M}_l$, the intersection of all maximal left ideals of R.*

(ii) *$1 - yx$ is left invertible for any $y \in R$.*

(iii) *$xN = 0$ for any simple left R-module N.*

Proof: Similar to the proof of Lemma 2.17. □

Proposition 2.19 *For $x \in R$, a unital ring, the following are equivalent*

(i) $x \in J(R)$

(ii) $1 - zxy \in U(R)$, *where $U(R)$ denotes the group of units of R, for any y, $z \in R$.*

Proof:

(i)⇒(ii): Let $x \in J(R)$ ($J(R)= \mathcal{M}_r \cap \mathcal{M}_l$). Then, by Lemma 2.17 , $1-xr$ is right invertible for all $r \in R$. Let $y, z \in R$ be arbitrary. Therefore, there exists $v \in R$ such that $(1 - x(yz))v = 1$, so v has a left inverse. Now, $v = 1+(xyzv)$ is right invertible, again by hypothesis. Thus, v and so also $1 - xyz$ are units since if $vw = 1$, then $(1 - xyz)vw = w = (1 - xyz)1$.

Finally, since $(1 - zxy)(1 + zvxy) = 1 - zxy + zvxy - zxyzvxy =$
$1 - zxy + z(v - xyzv)xy = 1 - zxy + z(1)xy = 1$ and, similarly, $(1 + zvxy)(1 - zxy) = 1$, we have that $1 - zxy$ is a unit as required.

(ii)⇒(i): If $1 - zxy \in U(R)$ for all $y, z \in R$ then, by (ii) of Lemma 2.17 and (ii) of Lemma 2.18, $x \in J(R)$. □

We often use this last result in the form; given $x \in J(R)$ then $1 - xy$ and

$1 - yx$ are units for all $y \in R$ (i.e. in fact $\mathcal{M}_r = \mathcal{M}_l = J(R)$).

Later we will discuss reduced modules over the ring of p-adic integers ($p \in \Pi$). We will be particularly concerned with such p-adic modules when they are complete in the so-called p-adic topology, i.e. a linear topology having the subgroups $p^n M$ ($n \geq 0$) as a basis of neighbourhoods of zero. Since the p-adic topology is metrizable in this case, completeness is equivalent to the convergence of all cauchy sequences. At this point we include this result:

Lemma 2.20 *Let M be a torsion-free complete p-adic module.*
Then $J(E(M)) = pE(M)$.

Proof: If $\phi \in pE(M)$ then $\phi = p\theta$ for some $\theta \in E(M)$. For α an arbitrary element of $E(M)$ we will consider the endomorphism
$1 - \phi\alpha = 1 - p(\theta\alpha)$. Firstly consider the formal binomial expansion

$$1 + p(\theta\alpha) + p^2(\theta\alpha)^2 + \ldots$$

This is an endomorphism of M since, given any $x \in M$, the expression $x(1 + p(\theta\alpha) + p^2(\theta\alpha)^2 + \ldots)$ is the sum of a cauchy sequence of elements of M and hence converges to an element of M.

Moreover,

$$1 = (1 - p(\theta\alpha))(1 + p(\theta\alpha) + p^2(\theta\alpha)^2 + \ldots)$$

$$=(1+p(\theta\alpha)+p^2(\theta\alpha)^2+\ldots)(1-p(\theta\alpha))$$

since p is a central element of M.

Thus, $1-\phi\alpha$ is a unit of $E(M)$ and so it follows from Proposition 2.19 that $\phi\in J(E(M))$. So $pE(M)\subseteq J(E(M))$.

Conversely, suppose $J(E(M))\not\subseteq pE(M)$. Then there exists $0\neq x\in M$ and $\alpha\in J(E(M))$ such that $x\alpha\notin pM$.

However, consider the cyclic submodule generated by $x\alpha$, $\langle x\alpha\rangle$. This is pure in M and complete since it is isomorphic to $\widehat{\mathbb{Z}}_p$. Hence, by

[14, Theorem 23], it is a direct summand of M. Therefore there exists some $\eta\in E(M)$ such that $(x\alpha)\eta=x$. Since $\alpha\eta\in J(E(M))$ then, by Lemma 2.17, it follows that $1-\alpha\eta$ is a unit of $E(M)$.

However, $x(1-\alpha\eta)=x-x(\alpha\eta)=x-x=0$ which contradicts $1-\alpha\eta$ being a unit of $E(M)$. Hence $J(E(M))$ must be contained in $pE(M)$. Therefore $J(E(M))=pE(M)$.

□

We finish this section with some important statements from arithmetic number theory.

Lemma 2.21 (*Dirichlet's Theorem*)

For each integer $k\geq 1$ and each integer l where $0\leq l<k$ and $(l,k)=1$

there is an infinite number of rational primes p of the form $p = l + nk$ where $n \in \mathbb{Z}^+$.

Proof: See [23, IV, Theorem 4.3] for details. □

Lemma 2.22 (*Cauchy-Schwarz Inequality*)

Let $a_1, \ldots, a_n$, $b_1, \ldots, b_n$ be real numbers where $n \in \mathbb{Z}^+$. Then $\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \left(\sum_{i=1}^{n} a_i^2\right) \left(\sum_{i=1}^{n} b_i^2\right)$.

Proof: See [18, Lemma 7.1]. □

Lemma 2.23 (*Chinese Remainder Theorem*)

Given positive integers $m_1, \ldots, m_r$ which are pairwise relatively prime and given any set of integers $n_1, \ldots, n_r$ ($r \in \mathbb{Z}^+$). Then, there exists an integer n such that $n \equiv n_i \bmod m_i$ for all $i \in 1, \ldots, r$.

This solution is not unique.

Proof: Follows from [12, II, Theorem 6.2] with $R = \mathbb{Z}$. □

The following historic theorem is credited to Hadamard and, independently, de la Vallée Poussin. The Prime Number Theorem for Arithmetic Progressions followed from this.

Theorem 2.24 (*Prime Number Theorem*)

$$\lim_{x\to\infty}\left(\frac{\pi(x)}{\frac{x}{\ln x}}\right)=1 \qquad (x\in\mathbb{R}),$$

Proof: See [23, III, Theorem 2.4]. □

Note that the Euler function is defined by $\varphi(k)=k\prod_{p|k}(1-\frac{1}{p})$ $(k\in\mathbb{Z})$. Recall $\pi(x,k,l)$ denotes the number of primes which are congruent to l mod k but do not exceed x.

Theorem 2.25 (*Prime Number Theorem for Arithmetic Progressions*)

Let $k,\ l\in\mathbb{N}$ *with* $(k,l)=1$, *then*

$$\lim_{x\to\infty}\left(\frac{\pi(x,k,l)}{\frac{x}{\ln x}}\right)=\frac{1}{\varphi(k)} \qquad (x\in\mathbb{R}),$$

Proof: See [23, IV, Theorem 7.5]. □

§2 The involution property for vector spaces

In this section we introduce the notion of involution property firstly by definition and then through a corollary to a result of Ó Searcóid [21] concerning vector spaces. Ó Searcóid shows that every linear transformation of a vector space X is a sum of a unit and an idempotent of $E(X)$ the endomorphism ring of X. This, along with Corollary 3.3, provide the motivation for Chapter IV. In Chapter IV we provide an alternative proof to that of Corollary 3.3 (see IV, Theorem 2.1).

Definition 3.1 *A unital ring E has the involution property if every element of E is a sum of a unit and an involution of E.*

An R–module M over a commutative ring R has the involution property if every endomorphism of M is a sum of an automorphism of M and an involutary automorphism of M.

The next result is due to Ó Searcóid [21]

Theorem 3.2 *Let X be a vector space over a field F. Let T be an arbitrary element of $E(X)$, the ring of linear transformations of X. Then there exists $P \in E(X)$ with $P^2 = P$ such that $T - P$ is invertible in $E(X)$.*

Proof: Let

$S = \{(M.Q)| \ M \subseteq X, (M)T \subseteq M, Q^2 = Q \in E(M), (M)(T-Q) = M,$

$(T \restriction_M) - Q$ is injective$\}$

We note that

- $S \neq \emptyset$, since $(\{0\}, 0) \in S$.

- S is a partially ordered set with $(M, Q) \leq (M', Q')$ if $M \subseteq M'$ and $Q' \restriction_M = Q$.

- If $\{(M_i, Q_i) | i \in I\}$ is a chain in S, then $(\bigcup\limits_{i \in I} M_i, \bigcup\limits_{i \in I} Q_i)$ is an upper bound which is also an element of S.

We may therefore invoke Zorn's Lemma. Therefore there exists a maximal element (Y, P) in S. We will show that $Y = X$.

Assume there exists $x \in X \setminus Y$.

Case 1:

Suppose there exists a polynomial $p = \sum\limits_{j=0}^{m} p_j U^j$ of minimal degree such that $x(p(T)) \in Y$.

- Certainly $m \neq 0$, since if so $xp_0 \in Y$ contradicting $x \in X \setminus Y$.

- We show that we cannot have $m = 1$ with $p_0 = 0$. If so then $p_1 xT \in Y$ and so $xT \in Y$. Define $Y' = Y \bigoplus Fx$, and $P' : Y' \longrightarrow Y'$ where $(y + \alpha x)P' = yP + \alpha x$; $y \in Y$, $\alpha \in F$.

  It is clear that $Y' \subseteq X$ and $(Y')T \subseteq Y'$. Also $P'^2 = P'$, since $(y + \alpha x)P'^2 = (yP + \alpha x)P' = yP^2 + \alpha x = yP + \alpha x = (y + \alpha x)P'$. Since $y + \alpha x T \in Y$, for each $y \in Y$ and each $\alpha \in F$, then $y + \alpha x T = w(T - P)$, for some $w \in Y$. Hence $y + \alpha x = w(T - P) - \alpha x T + \alpha x = (w - \alpha x)(T - P')$ so $Y'(T - P') = Y'$.

  Moreover $(T\,|_{Y'}) - P'$ is injective: Let $(y + \alpha x)(T - P') = 0$ for some $y \in Y$, $\alpha \in F$; then $y(T - P) + \alpha x T - \alpha x = 0$, which, looking at the summand Fx, implies that $\alpha x = 0$, so that $\alpha = 0$, and looking at the summand Y, implies that $y(T - P) = 0$ so by injectivity of $T - P$ we get $y = 0$.

Therefore $(Y', P') \in S$, contradicting maximality of (Y, P).

- If $m \geq 1$. Assume that $p_0 = 0$. Since $x \sum_{j=1}^{m} p_j T^j = (x \sum_{j=1}^{m} p_j T^{j-1})T$ then by minimality of m we have an $x' = (x \sum_{j=1}^{m} p_j T^{j-1}) \in X \setminus Y$ such that $x'T \in Y$. This corresponds to $m = 1$ and $p_0 = 0$, a case already considered. Therefore from now on we assume $p_0 \neq 0$.

Now

(i) $\{xT^k | 0 \leq k < m\}$ is a linearly independent set:
Let $\sum_{k=0}^{m-1} \alpha_k x T^k = x \sum_{k=0}^{m-1} \alpha_k T^k = 0 \in Y$, $\alpha_k \in F$ for each $k \in 0, 1, \ldots, m-1$. Then, by minimality of m, $\alpha_0 = \alpha_1 = \ldots = \alpha_{m-1} = 0$.

(ii) Let $W = \langle xT^k | 0 \leq k < m \rangle$. Then,$W \bigcap Y = \{0\}$, by minimality of m.

(iii) Define $Y' = Y \bigoplus W$, and $P' : Y' \longrightarrow Y'$, by $(y + w)P' = yP$, for any $y \in Y$, $w \in W$.

We must show that $(Y', P') \in S$.

Certainly $Y' \subseteq X$.

$\underline{Y'T \subseteq Y'}$: $YT \subseteq Y$; $(xT^k)T = xT^{k+1} \in W$ for $k = 0, \ldots, m-2$, and for $k = m-1$ we have $(xT^{m-1})T = xT^m = y_T - \frac{1}{p_m} \sum_{j=0}^{m-1} p_j xT$, for some $y_T \in Y$, $p_m \neq 0$, so $xT^m \in Y \bigoplus W = Y'$.

$\underline{(P')^2 = P'}$: Since, given any arbitrary element $y + w$ of Y', where $y \in Y$ and $w \in W$, then $(y+w)(P')^2 = (yP)P' = yP^2 = yP = (y+w)P'$.

$\underline{Y'(T - P') = Y'}$: Consider an arbitrary element $y + \sum_{k=0}^{m-1} \alpha_k xT^k$ of Y', where $y \in Y$, $\alpha_k \in F$, $k = 0, \ldots, m-1$. Then

$$y + \sum_{k=0}^{m-1} \alpha_k xT^k = (y' + \sum_{k=0}^{m-1} \beta_k xT^k)(T - P'), \quad \text{for some } y' \in Y,$$

$\beta_k \in F$, $k = 0, \ldots, m-1$,

$$\iff \quad y + \sum_{k=0}^{m-1} \alpha_k xT^k = y'(T - P') + \sum_{k=0}^{m-1} \beta_k xT^{k+1}$$

$$\iff \quad y + \sum_{k=0}^{m-1} \alpha_k xT^k = y'(T - P) + \sum_{k=1}^{m-1} \beta_{k-1} xT^k + \beta_{m-1} xT^m$$

$$\iff \quad y + \sum_{k=0}^{m-1} \alpha_k xT^k = y'(T - P) + \sum_{k=1}^{m-1} \beta_{k-1} xT^k + \beta_{m-1}(y_T - \frac{1}{p_m} \sum_{k=0}^{m-1} p_k xT^k),$$

for some $y_T \in Y$. This is so if and only if the following conditions are fulfilled,

$$y = y'(T - P) + \beta_{m-1} y_T \quad , \alpha_0 = -\frac{\beta_{m-1}}{p_m} p_0$$

$$\text{and } \alpha_k = \beta_{k-1} - \frac{\beta_{m-1}}{p_m} p_k \quad , \text{for } k = 1, \ldots, m-1.$$

Since $p_0 \neq 0$ then we can always find a solution for $\beta_0, \ldots, \beta_{m-1}$ for any given $\alpha_0, \ldots, \alpha_{m-1}$. Furthermore, since $Y(T-P) = Y$ then we may always find some $y' \in Y$ such that $y'(T-P) = y - \beta_{m-1}y_T$.

<u>$T\lceil_Y - P'$ is injective:</u> Consider an arbitrary element $y + \sum\limits_{k=0}^{m-1} \alpha_k x T^k$ of Y', where $y \in Y$, $\alpha_k \in F$, $k = 0, \ldots, m-1$, such that

$$(y + \sum_{k=0}^{m-1} \alpha_k x T^k)(T - P') = 0.$$

This can be true if and only if $\quad y(T-P) + \sum\limits_{k=0}^{m-1} \alpha_k x T^{k+1} = 0.$

The last statement is true if and only if $\alpha_0 = \ldots = \alpha_{m-2} = 0$ and $y(T-P) + \alpha_{m-1}(y_T - \frac{1}{p_m}\sum\limits_{k=0}^{m-1} p_k x T^k) = 0$, some $y_T \in Y$, and this is so if and only if $\alpha_0 = \ldots = \alpha_{m-2} = 0$ and $\alpha_{m-1}p_k = 0$, for all $0 \leq k \leq m-1$ and $y(T-P) + \alpha_{m-1}y_T = 0$; which is true if and only if $\alpha_0 = \ldots = \alpha_{m-1} = 0$ and $y(T-P) = 0$; which in turn is true if and only if $\alpha_0 = \ldots = \alpha_{m-1} = 0$ and $y = 0$. Therefore $\ker(T\lceil_Y - P') = 0$.

So $(Y', P') \in S$. This contradicts the maximality of (Y, P).

Case (2):

Suppose $xp(T) \notin Y$, for all polynomials p.

(i) $\{xT^k | 0 \leq k \in \mathbb{N}\}$ is a linearly independent set:

Let $\sum\limits_{k=0}^{m} \alpha_k x T^k = x\sum\limits_{k=0}^{m} \alpha_k T^k = 0 \in Y$ for some $m \in \mathbb{N}$. This contradicts the supposition unless $\alpha_0 = \alpha_1 = \ldots = \alpha_m = 0$.

(ii) Let $V = \langle xT^k | k \in \mathbb{N} \rangle$. Then $V \bigcap Y = \{0\}$.

(iii) Define $Y' = Y \bigoplus V$, and define $P' : Y' \longrightarrow Y'$ by $P' \restriction_Y = P$, and $P' \restriction_V = Q$ where $xT^{2n}Q = xT^{2n}$ and $xT^{2n+1}Q = xT^{2n+2} - xT^{2n}$, for all $n \geq 0$.

We must show that $(Y', P') \in S$. Clearly $Y' \subseteq X$ and $(Y')T \subseteq Y'$

$(P')^2 = P'$: It is enough to show that $Q^2 = Q$ since $P^2 = P$ by assumption. Let $n \in \mathbb{N}$, arbitrary, then $(xT^{2n})Q^2 = (xT^{2n})Q$ and $(xT^{2n+1})Q^2 = (xT^{2n+2} - xT^{2n})Q = xT^{2n+2} - xT^{2n} = (xT^{2n+1})Q$. Therefore $Q^2 = Q$.
$Y'(T - P') = Y'$: It is enough to show that $V(T - Q) = V$ since $Y = Y(T-P) = Y(T-P')$ and $V(T-Q) = V(T-Q) \subseteq V$. Furthermore, it is enough to show $xT^k = v(T-P)$ for some $v \in V$ and for all $k \in \mathbb{N}$; we show this as $xT^{2n} = xT^{2n+1}(T - Q)$ and $xT^{2n+1} = (xT^{2n} + xT^{2n+1})(T - Q)$. Therefore $T - P'$ is onto Y'. $T \restriction_{Y'} - P'$ is injective: Again it suffices to show that $T \restriction_V - Q$ is injective. We show that $T \restriction_V + 1_V - Q$ is a right inverse of $T \restriction_V - Q$: For any $n \in \mathbb{N}$, $xT^{2n}(T \restriction_V - Q)(T \restriction_V + 1_V - Q) = (xT^{2n+1} - xT^{2n})(T \restriction_V + 1_V - Q)$
$= xT^{2n+2} - xT^{2n+1} + xT^{2n+1} - xT^{2n} - xT^{2n+2} + 2xT^{2n} = xT^{2n}$, and
$xT^{2n+1}(T \restriction_V - Q)(T \restriction_V + 1_V - Q) = (xT^{2n+2} - xT^{2n+2} + xT^{2n})(T \restriction_V + 1_V - Q)$
$= xT^{2n+1} + xT^{2n} - xT^{2n} = xT^{2n+1}$. So, $(T \restriction_V - Q)(T \restriction_V + 1_V - Q) = 1_V$.

Similarly, $(T\restriction_V + 1_V - Q)(T\restriction_V - Q) = 1_V$ so $T\restriction_V - Q$ is injective.

Therefore, $(Y', P') \in S$, contradicting the maximality of (Y, P) and so eliminating Case 2.

Hence there can be no $x \in X$ such that $x \notin Y$, therefore $X = Y$. Therefore $(X, P) \in S$, and so P is an idempotent of $E(X)$; we also have $T - P$ is injective; further, since $X(T - P) = X$ therefore $T - P$ is onto. Therefore $T - P$ is an automorphism of X.

□

Next we relate Ó Searcóid's result to the involution property. Notice the role of 2 being an element of the field.

Corollary 3.3 *Let F be any field containing 2. Let X be a vector space over F and T an arbitrary element of $E(X)$. Then there exists $I \in E(X)$ with $I^2 = 1_X$, where 1_X is the identity on X, such that $T - I$ is invertible in $E(X)$.*

Proof: By Theorem 3.2, $\frac{1}{2}(T + 1_X) = P + V$ where $P, V \in E(X)$ with P an idempotent and V an automorphism of X.

Then $T = (2P - 1_X) + 2V$. Certainly $2V$ is an automorphism of X, and since $(2P - 1_X)^2 = 4P^2 - 4P + 1_X = 1_X$ we see that $(2P - 1_X)$ is an involutary automorphism of X. □

II Free modules and completely decomposable groups

In the first two sections of this chapter unit sum numbers for a free R–module, M, over a commutative ring R are investigated. Wans has shown, for R a PID, where the rank of M is finite, but greater than 1, then usn(M)$=2$ and if the rank of M is infinite then usn(M)≤ 3 (see I, Theorems 2.4 and 2.5). We concentrate therefore on cases of infinite rank and attempt to determine precise unit sum numbers for these modules. We begin in the first section of this chapter by considering the easier case of a free R–module M where R has unit sum number of 2; we show that usn(M)$=2$. In this case R is an arbitrary commutative ring not necessarily a PID.

§1 Free modules over rings with the 2–sum property

In this section we will show that for M a free R–module of arbitrary rank, where R is a commutative ring then usn(M)$=2$ if usn(R)$=2$. Although we will improve on this result in Section 2 where R is a PID, the method in this section is easier. We begin by developing some results regarding certain types of endomorphisms. The first proposition is due to Freedman [6]; it provides useful sequences for "breaking" endomorphisms into pieces.

Proposition 1.1 *Let* $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ *be a free R-module of countable rank and let ϕ be an endomorphism of M.*

Then there exists a strictly increasing sequence of natural numbers

$0 = r_0 < r_1 < \ldots < r_s \ldots$ $(s \in \omega)$ *such that*

if $i < n$ *and* $r_s \leq i < r_{s+1}$ *then* $[e_i\phi] \subseteq \{0, 1, \ldots, r_{s+2} - 1\}$.

$$(*)$$

Proof: Firstly, if $n < \omega$, set $r_0 = 0$ and choose some $1 \leq r_1 \leq n$ which satisfies $[e_0\phi] \subseteq \{0, 1, \ldots, r_1 - 1\}$, i.e. trivially we can choose $r_1 = n$. For $r_k > n$ $(k > 1)$, set $r_k = n + k$. In this way a sequence $(r_s)_{s\in\omega}$ can be chosen fulfilling condition (*).

Now we turn our attention to the infinite case $n = \omega$. Choose r_1 to be any positive integer greater than 0. Clearly $[e_i\phi]$ is finite for any $i \leq r_1$ and so we may choose $r_2 \in \mathbb{N}$ to be bigger than the maximum of the finite set $\{r_1\} \cup \bigcup_{i=r_0}^{r_1-1} [e_i\phi]$. Therefore the property (*) is satisified for $s = 0$.

We continue inductively in the same way. Suppose r_{s+1} is given for some $s \geq 1$, then we obtain r_{s+2} as an integer bigger than the maximum of the finite set $\{r_{s+1}\} \cup \bigcup_{i=r_s}^{r_{s+1}-1} [e_i\phi]$. Then $[e_i\phi] \subseteq \{1, \ldots, r_{s+2} - 1\}$ for each $r_s \leq i < r_{s+1}$.

Henceforth $0 = r_0 < r_1 < \ldots$ is a strictly ascending sequence with the desired property (*) □

Applying the above proposition to an α-endomorphism we obtain:

Corollary 1.2 *Let $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ be a free R-module of countable rank and let ϕ be an α-endomorphism of M.*

Then there exists a strictly increasing sequence of natural numbers $0 = r_0 < r_1 < \ldots < r_s \ldots$ $(s \in \omega)$, such that if $i < n$ and $r_s \leq i < r_{s+1}$ then $[e_i\phi] \subseteq \{i+1, \ldots, r_{s+2} - 1\}$.

Proof: The proof follows directly from Proposition 1.1 and the definition of an α-endomorphism (see I, Definition 2.2). □

The next lemmas concern locally nilpotent endomorphisms.

Lemma 1.3 *Let M be a free R-module of arbitrary rank over a commutative ring R and let η be any locally nilpotent endomorphism of M. Then $(\eta + 1)$ is an automorphism of M.*

Proof: Obviously, $\eta + 1$ is also an endomorphism of M. To show that $\eta + 1$ is bijective let $m \neq 0$ be an arbitrary element of M. Since η is locally nilpotent there exists an integer $n \geq 1$ such that $m\eta^n = 0$ and $m\eta^{n-1} \neq 0$ where we agree that $\eta^0 = 1$.

Since $m(\eta + 1)\eta^{n-1} = m\eta^{n-1} \neq 0$ it follows that $\ker(\eta + 1) = 0$ and so $(\eta + 1)$ is injective. Also, $(m(1 - \eta + \eta^2 - \eta^3 + \ldots \eta^{n-1}))(\eta + 1) = m$ which shows that $(\eta + 1)$ is surjective. □

Lemma 1.4 *Let M be a free R–module of arbitrary rank over a commutative ring R. Moreover, let ϕ, ψ be locally nilpotent endomorphisms of M satisfying $\phi\psi = 0$.*

Then the endomorphism $\phi + \psi$ is locally nilpotent.

Proof: Firstly we show, by induction on n, that the following holds for any $n \in \mathbb{N}$:

$$(\phi + \psi)^n = \sum_{i=0}^{n} \psi^i \phi^{n-i} \qquad (*)$$

The statement (*) is certainly true for $n = 1$, i.e. $(\phi + \psi)^1 = \phi^1 + \psi^1$. Therefore we assume that (*) is true for all $1 \leq n \leq k$ for some $k \in \mathbb{N}$. Then:

$$\begin{aligned}(\phi + \psi)^{k+1} &= (\sum_{i=0}^{k} \psi^i \phi^{k-i})(\phi + \psi) \\ &= (\phi^k + \sum_{i=1}^{k} \psi^i \phi^{k-i})(\phi + \psi) \\ &= \phi^{k+1} + \sum_{i=1}^{k} \psi^i \phi^{(k+1)-i} + \phi^k \psi + \sum_{i=1}^{k} \psi^i \phi^{k-i} \psi.\end{aligned}$$

However, since $\phi\psi = 0$ the last two summands reduce to ψ^{k+1} and thus we deduce $(\phi + \psi)^{k+1} = \phi^{k+1} + \sum_{i=1}^{k} \psi^i \phi^{(k+1)-i} + \psi^{k+1} = \sum_{i=0}^{k+1} \psi^i \phi^{(k+1)-i}$, as required.

Using (*), now it can be shown that $\phi + \psi$ is locally nilpotent. Let $m \neq 0$ be an arbitrary element of M. Since ψ is locally nilpotent there exists $u \in \mathbb{N}$ such that $m\psi^u = 0$. Since ϕ is also locally nilpotent we can find $v \in \mathbb{N}$ so that $(m\psi^i)\phi^v = 0$ for all $0 \leq i \leq u$. Therefore, letting $n = u + v$, it follows that $m\psi^i\phi^{n-i} = 0$ for all $0 \leq i \leq n = u + v$, and thus $m(\phi + \psi)^n = m \sum_{i=0}^{n} \psi^i \phi^{n-i} = 0$.

As this is true for all elements $m \in M$ we can conclude that $\phi + \psi$ is locally nilpotent. □

Lemma 1.5 *Let $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ be a free R–module of countable rank over a commutative ring R and let η be an α–endomorphism of M. Then η is a sum of two locally nilpotent α–endomorphisms.*

Proof: By Corollary 1.2 there is a strictly ascending sequence of integers

$0 = r_0 < r_1 < r_2 \ldots$ such that $[e_i\eta] \subseteq \{i + 1, \ldots, r_{s+2} - 1\}$, for each $r_s \leq i < r_{s+1}$ $(s \in \omega)$.

Using this sequence we now define endomorphisms η_1, η_2 of M as follows (for $t = 0, 1, \ldots$):

$$e_i\eta_1 = \begin{cases} e_i\eta & for \quad r_{2t} \leq i < r_{2t+1} \\ 0 & for \quad r_{2t+1} \leq i < r_{2t+2} \end{cases}$$

and

$$e_i\eta_2 = \begin{cases} 0 & for \quad r_{2t} \leq i < r_{2t+1} \\ e_i\eta & for \quad r_{2t+1} \leq i < r_{2t+2} \end{cases}$$

Clearly, η_1 and η_2 are α–endomorphisms of M with $\eta = \eta_1 + \eta_2$. Thus it remains to show that η_1 and η_2 are locally nilpotent. Obviously, it is enough to consider η_1 (or η_2) because of their similarity. Moreover, we only need to consider the base elements e_i ($i < n$). If $r_{2t+1} \leq i < r_{2t+2}$ for some $t \in \omega$ then $e_i\eta_1^1 = e_i\eta_1 = 0$ by the above definition.

So, let $r_{2t} \leq i < r_{2t+1}$. for some $t \in \omega$. Then also by definition, $e_i\eta_1 = e_i\eta$ and therefore we have: $[e_i\eta_1] \subseteq \{i + 1, \ldots, r_{2t+2} - 1\}$. Now, since $e_j\eta_1 \subseteq \{j + 1, \ldots, r_{2t+1} - 1\}$ or $e_j\eta_1 = 0$ for all $j = r_{2t}, \ldots, r_{2t+2} - 1$ then $[e_i{\eta_1}^2] \subseteq \{i + 2, \ldots, r_{2t+2} - 1\}$ or $e_i{\eta_1}^2 = 0$, and $[e_i{\eta_1}^3] \subseteq \{i + 3, \ldots, r_{2t+2} - 1\}$ or $e_i{\eta_1}^3 = 0$, and continuing in this way we have $[e_i{\eta_1}^m] \subseteq \{r_{2t+1} + 1, \ldots, r_{2t+2} - 1\}$ or $e_i{\eta_1}^m = 0$, for some $m \in \omega$. Hence $e_i{\eta_1}^{m+1} = 0$ and so η_1 is locally nilpotent as required.

□

Now we are ready to prove the main theorem of this section.

Theorem 1.6 *Let $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ be a free R-module of countable rank over a commutative ring R. If* $\operatorname{usn}(R) = 2$ *then* $\operatorname{usn}(M) = 2$.

Proof: Let M be as above and assume $\operatorname{usn}(R)= 2$. Moreover, let ϕ be an arbitrary endomorphism of M. Then ϕ can obviously be expressed as

$$\phi = \eta + \rho + \delta \tag{1}$$

where η is an α–endomorphism, ρ is a β– endomorphism and δ is a d–endomorphism. By Corollary 1.2 there is a strictly ascending sequence of integers $0 = r_0 < r_1 < r_2 \ldots$ such that $[e_i\eta] \subseteq \{i+1, \ldots, r_{s+2} - 1\}$ or $e_i\eta = 0$, for all $r_s \leq i < r_{s+1}$ $(s \in \omega)$.

Now, by Lemma 1.5 there are locally nilpotent α–endomorphisms η_1 and η_2 such that $\eta_1 + \eta_2 = \eta$.

Recall that $e_i\eta_1 = 0 = e_j\eta_2$ for $j \in I_1 := \bigcup_{t\in\omega}\{k \in \omega \mid r_{2t} \leq k < r_{2t+1}\}$ and $i \in I_2 := \bigcup_{t\in\omega}\{k \in \omega \mid r_{2t+1} \leq k < r_{2t+2}\}$ while $e_i\eta_1 = e_i\eta$ for $i \in I_1$ and $e_j\eta_2 = e_j\eta$ for $j \in I_2$.

Therefore we have, in fact, obtained that $\gamma\eta_1$ and $\gamma\eta_2$ are locally nilpotent α–endomorphisms for any d–endomorphism γ of M (see proof of Lemma 1.5).

Next we decompose the β–endomorphism ρ. For each $i < n$ we write $e_i\rho$ as

$$e_i\rho = \sum_{j<i} e_j b_{ij} = \sum_{\substack{j<i\\ j\in I_1}} e_j b_{ij} + \sum_{\substack{j<i\\ j\in I_2}} e_j b_{ij}$$

and we define ρ_1, ρ_2 correspondingly, i.e.

$$e_i\rho_1 = \sum_{\substack{j<i\\ j\in I_1}} e_j b_{ij} \quad e_i\rho_2 = \sum_{\substack{j<i\\ j\in I_2}} e_j b_{ij}.$$

Clearly, $\rho_1 + \rho_2 = \rho$ and $\gamma\rho_1$ and $\gamma\rho_2$ are also β–endomorphisms of M for any d–endomorphism of M. Note that any β–endomorphism is locally nilpotent by I, Lemma 2.3 . Moreover, the definitions of η_1, η_2, ρ_1, ρ_2 imply immediately that $\rho_1\eta_2 = 0 = \rho_2\eta_1$. In fact, given any d–endomorphism γ of M we have $\gamma\rho_1\gamma\eta_2 = 0 = \gamma\rho_2\gamma\eta_1$.

Now we consider the d–endomorphism δ. For each $i < n$ there is an element a_i of R such that $e_i\delta = a_ie_i$. Since usn(R)= 2, there are units u_{i1}, u_{i2} of R ($i < n$), such that $a_i = u_{i1} + u_{i2}$. Putting

$$e_i\delta_1 = u_{i1}e_i \quad \text{and} \quad e_i\delta_2 = u_{i2}e_i \quad \text{for each } 0 \leq i < \omega$$

we obtain d–endomorphisms δ_1 and δ_2 of M which are, in fact, automorphisms of M and satisfy $\delta = \delta_1 + \delta_2$.

Finally, we rewrite equation (1) as follows:

$$\phi = \eta+\rho+\delta = \eta_1+\eta_2+\rho_1+\rho_2+\delta_1+\delta_2 = (\eta_1+\rho_2+\delta_1)+(\eta_2+\rho_1+\delta_2)$$

$$= \delta_1(\delta_1^{-1}(\eta_1 + \rho_2) + 1) + \delta_2(\delta_2^{-1}(\eta_2 + \rho_1) + 1) \tag{2}$$

By Lemma 1.4, $\delta_1^{-1}(\eta_1 + \rho_2)$ is locally nilpotent since $\delta_1^{-1}\eta_1$ and $\delta_1^{-1}\rho_2$ are locally nilpotent and satisfy $\delta_1^{-1}\rho_2\delta_1^{-1}\eta_1 = 0$. Therefore, by Lemma 1.3, $\delta_1^{-1}(\eta_1 + \rho_2) + 1$ is an automorphism of M and so $\delta_1(\delta_1^{-1}(\eta_1 + \rho_2) + 1)$ is also an automorphism.

Moreover using the same argument, we deduce that $\delta_2(\delta_2^{-1}(\eta_2 + \rho_1) + 1)$ is an automorphism.

Therefore ϕ is a sum of two automorphisms of M as required. $\square$

Applying a method due to Castagna (see [3]), we can extend the above result to free modules of uncountable rank.

Let $M = \bigoplus_{i \in I} Re_i$ be a free module of rank I, then for any $X \subseteq M$ we define the *support of* X as $[X] = \bigcup_{m \in X} [m]$.

Definition 1.7 *Let $M = \bigoplus_{i \in I} Re_i$ be a free module of arbitrary rank and ϕ be an endomorphism of M. For any subset S of M the ϕ*–closure *of S, $\langle S \rangle_\phi$, is defined as $\langle S \rangle_\phi = \bigcup_{n < \omega} S_n$, with $S_0 = \langle e_i \mid i \in [S] \rangle$ and $S_{n+1} = \langle e_i \mid i \in [S_n] \cup [S_n\phi] \rangle$.*

Note that $\langle S \rangle_\phi$ is invariant under ϕ and $\langle S \rangle_\phi$ is countable whenever S is.

Now we adjust Castagna's lemma to our situation.

Lemma 1.8 *Let $M = \bigoplus_{\alpha<\kappa} Re_\alpha$ be a free R-module of uncountable rank κ, ϕ any endomorphism of M and $m \in \mathbb{Z}^+$. Then M can be written as the union of a smooth ascending chain $\{H_\beta \mid \beta < \kappa\}$ of submodules H_β of M of rank less than κ such that*

(i) $(H_\beta)\phi \subseteq H_\beta$ *for all* $\beta < \kappa$.

(ii) $H_{\beta+1} = H_\beta \oplus C_\beta$ *where* $m \leq rk(C_\beta) \leq \aleph_0$, *for all* $\beta < \kappa$.

(iii) $[H_\beta] \subseteq H_\beta$ *for all* $\beta < \kappa$.

Proof: We inductively define the H_β ($\beta < \kappa$).

Put $H_0 = 0$ and let $H_\beta = \bigcup_{\alpha<\beta} H_\alpha$ if β is a limit ordinal.

Clearly, $H_0\phi = 0 \subseteq H_0$ and, if $H_\alpha\phi \subseteq H_\alpha$ for all $\alpha < \beta$, then $H_\beta\phi \subseteq H_\beta$. Now, suppose H_β is given for some $\beta < \kappa$. We choose distinct basis elements $e_{\alpha_1}, e_{\alpha_2}, \dots e_{\alpha_m}$ which do not belong to $[H_\beta]$ and we put $X = [\langle e_{\alpha_1}, e_{\alpha_2}, \dots, e_{\alpha_m}\rangle_\phi] \setminus [H_\beta]$. Clearly, $m \leq \mid X \mid \leq \aleph_0$. We define C_β and hence $H_{\beta+1}$ by $C_\beta = \bigoplus_{\alpha\in X} Re_\alpha$ and $H_{\beta+1} = H_\beta \oplus C_\beta$.

Obviously, $m \leq \mathrm{rk}(C_\beta) \leq \aleph_0$. It remains to show that $H_{\beta+1}$ is invariant under ϕ and contains its support. The latter is obvious. Now, $H_\beta\phi \subseteq H_\beta$ by assumption and $C_\beta\phi \subseteq H_{\beta+1}$ by our definition of X and C_β. Therefore property (i) also holds. □

Theorem 1.9 *Let $M = \bigoplus_{\beta<\kappa} Re_\beta$ be a free module of uncountable rank and $m \in \mathbb{N}$ $(0 \neq m \in \mathbb{N})$. If every free module over R of countable rank greater than $m-1$ has unit sum number equal to $n \in \mathbb{N}$, then* $\mathrm{usn}(M) \leq n$.

Proof: Let $\phi \in E(M)$ and write $M = \bigcup_{\beta<\kappa} H_\beta$ as in Lemma 1.8.

Inductively we define automorphisms $\theta_{i,\beta}$ for each $\beta < \kappa$ and for each $i = 1, 2, \ldots, n$ such that $\phi\restriction_{H_\beta} = \sum_{i=1}^{n} \theta_{i,\beta}$ and if $\alpha < \beta$ then $\theta_{i,\beta}\restriction_{H_\alpha} = \theta_{i,\alpha}$ for each $i = 1, 2, \ldots, n$.

For $\beta = 0$, $H_0 = 0$ and therefore $\phi\restriction_{H_0} = 0 = \sum_{i=1}^{n} 0$. Since $H_0 = 0$ the endomorphism 0 is injective and surjective and so is an automorphism of H_0.

For $\alpha < \beta$ assume that $\{\theta_{i,\alpha} \mid i = 1, 2, \ldots, n\}$ has been suitably defined.

Let β be a limit ordinal. For any $i \in \{1, 2, \ldots, n\}$ define $\theta_{i,\beta} = \bigcup_{\alpha<\beta} \theta_{i,\alpha}$, which is well defined since each $\theta_{i,\alpha}$, for each $\alpha < \beta$, is an extension of $\theta_{i,\delta}$, for each $\delta < \alpha$.

Moreover, $\mathrm{dom}\theta_{i,\beta} = \mathrm{dom} \bigcup_{\alpha<\beta} \theta_{i,\alpha} = \bigcup_{\alpha<\beta} \mathrm{dom}\theta_{i,\alpha} = \bigcup_{\alpha<\beta} H_\alpha = H_\beta$, i.e. $\theta_{i,\beta}$ has the correct domain.

Also, $\mathrm{Im}\theta_{i,\beta} = \mathrm{Im} \bigcup_{\alpha<\beta} \theta_{i,\alpha} = H_\beta$ as above and thus $\theta_{i,\beta}$ is surjective.

Clearly, $\theta_{i,\beta}$ is injective as all the $\theta_{i,\alpha}$'s are. Similarly it is clear that $\theta_{i,\beta}$ is a homomorphism of H_β. Henceforth, $\theta_{i,\beta}$ is an automorphism of H_β $(1 \leq i \leq n)$.

Now, let $h \in H_\beta$, then $h \in H_\alpha$ for some $\alpha < \beta$. By the induction hypothesis and the definition of the $\theta_{i,\beta}$'s we have $h\phi = h \sum\limits_{i=1}^{n} \theta_{i,\alpha} = h \sum\limits_{i=1}^{n} \theta_{i,\beta}$. Therefore $\phi \restriction_{H_\beta} = \sum\limits_{i=1}^{n} \theta_{i,\beta}$ as required.

Now assume β is not a limit ordinal.

Let $\beta = \alpha + 1$. By Lemma 1.8 we have $H_{\alpha+1} = H_\alpha \oplus C_\alpha$ where $m \leq$ rk$(C_\alpha) \leq \aleph_0$.

Define π_1 and π_2 as the projections of $H_{\alpha+1}$ onto H_α and C_α respectively. Then $(\phi \restriction_{C_\alpha})\pi_2$ is a mapping from C_α to C_α, in other words an endomorphism of C_α. Since $m \leq rk(C_\alpha) \leq \aleph_0$ there exist $\{\psi_i\}_{i=1,2,\ldots,n}$ such that $\psi_i \in Aut(C_\alpha)$ for each $i \in 1, 2, \ldots, n$ and such that $(\phi \restriction_{C_\alpha})\pi_2 = \sum\limits_{i=1}^{n} \psi_i$.

For each $c \in C_\alpha$ define $v_c \in H_\alpha$ as $v_c = (c\phi)\pi_1$. Note that $\phi\pi_1$ is a mapping from C_α to H_α.

For each $i \in 1, 2, \ldots, n$ define $\theta_{i,\alpha+1}$ on $H_{\alpha+1}$ by

$$(x + c)\theta_{1,\alpha+1} = x\theta_{1,\alpha} + c\psi_1 + v_c,$$

$$(x + c)\theta_{i,\alpha+1} = x\theta_{i,\alpha} + c\psi_i \quad , \text{ for } i = 2, \ldots, n$$

where $x \in H_\alpha$ and $c \in C_\alpha$.

For each $i = 1, 2, \dots, n$ it is clear that $\theta_{i,\alpha+1}$ is a homomorphism; $\theta_{i,\alpha+1}$ is an extension of $\theta_{i,\alpha}$ because, for any $x \in H_\alpha$, $x\theta_{i,\alpha+1} = x\theta_{i,\alpha} + 0\psi_i + v_0 = x\theta_{i,\alpha}$since $v_0 = (0\phi)\pi_1 = 0$.

Next we show that $\theta_{i,\alpha+1}$ is an automorphism of $H_{\alpha+1}$ for each $i = 1, 2, \dots, n$. Consider the kernel of $\theta_{1,\alpha+1}$. For $x \in H_\alpha$, $c \in C_\alpha$ with $x + c \in \ker\theta_{1,\alpha+1}$ we have $0 = (x+c)\theta_{1,\alpha+1} = x\theta_{1,\alpha} + c\psi_1 + v_c = (x\theta_{1,\alpha} + v_c) + c\psi_1$. Now, $(x\theta_{1,\alpha} + v_c) \in H_\alpha$ and $c\psi_1 \in C_\alpha$. Since ψ_1 is an automorphism of C_α then $c\psi_1 = 0$ implies that $c = 0$ and so $v_c = 0$. Therefore we are left with $x\theta_{1,\alpha} = 0$. By assumption, $\theta_{1,\alpha}$ is an automorphism of H_α so that $x = 0$. Therefore $\ker\theta_{1,\alpha+1} = 0$.

For $i = 2, \dots, n$ it is just as easy to show that $\ker\theta_{i,\alpha+1} = 0$. Suppose $(x+c)\theta_{i,\alpha+1} = 0$. Then $x\theta_{i,\alpha} + c\psi_1 = 0$ and it follows again that $x = 0 = c$ since ψ_i is an automorphism of C_α and, by assumption, $\theta_{i,\alpha}$ is an automorphism of H_α.

Next we show that $\theta_{1,\alpha+1}$ is surjective.

Let $a + b$ be an arbitrary element of $H_{\alpha+1} = H_\alpha \oplus C_\alpha$ where $a \in H_\alpha$ and $b \in C_\alpha$. Then $a + b = ((a - v_c)\theta_{1,\alpha}^{-1})\theta_{1,\alpha} + (b\psi_1^{-1})\psi_1 + v_c$ where $c = b\psi_1^{-1} \in C_\alpha$ and $v_c = (c\phi)\pi_1$. Therefore, letting $x = (a - v_c)\theta_{1,\alpha}^{-1} \in H_\alpha$, we have $a + b = (x + c)\theta_{1,\alpha+1}$.

Now we show that $\theta_{i,\alpha+1}$ is surjective for all $i = 2, \ldots, n$. Take an arbitrary $i \in \{2, \ldots, n\}$ and let $a + b$ be an arbitrary element of $H_{\alpha+1} = H_\alpha \oplus C_\alpha$ where $a \in H_\alpha$ and $b \in C_\alpha$. Define $c = b(\psi_i)^{-1} \in C_\alpha$ and $x = a(\theta_{i,\alpha})^{-1} \in H_\alpha$. Then $a + b = (x\theta_{i,\alpha} + c\psi_i)\theta_{i,\alpha+1}$, i.e. $\theta_{i,\alpha+1}$ is surjective.

Therefore $\theta_{i,\alpha+1} \in Aut(H_{\alpha+1})$ for all $i = 1, \ldots, n$. It remains to show that $\phi \restriction_{H_{\alpha+1}} = \sum\limits_{i=1}^{n} \theta_{i,\alpha+1}$. Let $(x + c) \in H_{\alpha+1}$ $(x \in H_\alpha,\ c \in C_\alpha)$. Then

$$(x+c)(\sum_{i=1}^{n} \theta_{i,\alpha+1}) = x(\sum_{i=1}^{n} \theta_{i,\alpha}) + c(\sum_{i=1}^{n} \psi_i) + v_c = x(\phi \restriction_{H_\alpha}) + (c\phi)\pi_2 + (c\phi)\pi_1$$
$$= x\phi + (c\phi)(\pi_2 + \pi_1) = x\phi + c\phi = (x + c)\phi.$$

Finally we conclude that $\phi = \sum\limits_{i=1}^{n} \theta_i$ where $\theta_i = \bigcup\limits_{\beta<\kappa} \theta_{i,\beta}$ is an automorphism for each $i = 1, \ldots, n$. □

Corollary 1.10 *Let M be a free R -module of arbitrary rank over a commutative ring R. If* $\text{usn}(R) = 2$ *then* $\text{usn}(M) = 2$.

Proof: The proof follows from Theorem 1.6 followed by Theorem 1.9 (taking $m = 1$ and $n = 2$) . □

It has been shown here that, for example, free modules of countably infinite rank over $R = J_p$ $(p \neq 2)$ or $R = \mathbb{Z}_{(p)}$ $(p \neq 2)$ have unit sum number 2. This improves the result of [11] for p-adic modules.

§2 Free modules – extending finite rank results

Next we use known results for free modules of finite rank over commutative rings to consider free R–modules, $M = \bigoplus_{i<\omega} Re_i$, of countably infinite rank over a commutative ring R where usn(R) may not equal 2; e.g. $R = \mathbb{Z}$, $R = \mathbb{Z}_{(2)}$, $R = J_2$. Many free modules of finite rank over commutative rings have been shown to have unit sum numbers of 2. In particular, Wans [29] (see I, Theorem 2.4 of this text) has shown that free modules of finite rank greater than 1 over a PID have unit sum number of 2. We develop a method which extends the finite rank result to the countably infinite case. Then we can extend to the uncountable case using the approach of Castagna.

The method used is one of matrix decomposition. It relies again on Freedman's Proposition 1.1 but noting that every endomorphism of M is the sum of an α–endomorphism, a β–endomorphism and a d–endomorphism the proposition is reused more generally for any endomorphism of M by way of the following definition.

Definition 2.1 *Let $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ be a free R–module of countable rank and let ϕ be an arbitrary endomorphism of M. We define $\mathcal{W} = (r_s)_{s\in\omega}$ to be a ϕ–*sequence *if it is a strictly increasing sequence of*

integers such that $r_0 = 0$ *and* $[e_i\phi] \subseteq \{0, 1, \dots, r_{s+2} - 1\}$ *or* $e_i\phi = 0$, *for any* $i < n$ *with* $r_s \leq i < r_{s+1}$ $(s \in \omega)$.

Moreover, we define the corresponding $\mathcal{W}$–function, $f_{\mathcal{W}}$, *for* $\mathcal{W}$ *by*

$f_{\mathcal{W}} : \omega \longrightarrow \omega$ *mapping* $i \in \omega$ *onto* $f_{\mathcal{W}}(i) = s \in \omega$ *if* $r_s \leq i < r_{s+1}$.

Note that such a sequence always exists by Proposition 1.1 and that the function $f_{\mathcal{W}}$ is obviously well defined.

Definition 2.2 *Let* $M = \bigoplus\limits_{i<n} Re_i$ $(n \leq \omega)$ *be a free* R*–module and let* $\mathcal{W}$ *be a strictly increasing sequence of integers with* $r_0 = 0$.

We define an endomorphism (automorphism) ϕ *of* M *to be a* $\mathcal{W}$–endomorphism ($\mathcal{W}$–automorphism) *of* M *if* $M_s = \bigoplus\limits_{\substack{i<n \\ r_s \leq i < r_{s+1}}} Re_i$ *is invariant under* ϕ *for any* $s \in \omega$.

The following definition plays a crucial role in tackling the unit sum number problem for modules of countably infinite rank in general.

Definition 2.3 *Let* $M = \bigoplus\limits_{i<n} Re_i$ $(n \leq \omega)$ *be a free* R*–module of countable rank. Moreover, let* ϕ *be an endomorphism of* M *and let* $\mathcal{W} = (r_s)_{s\in\omega}$ *be a* ϕ*–sequence,* $f_{\mathcal{W}}$ *its* $\mathcal{W}$*–function.*

*For any $t \in \omega$ we define the $t^{th}(\phi, \mathcal{W})$-*mapping $\phi_{(\mathcal{W},t)}$ *as follows:*

For any $i < n$ we can express $e_i\phi$ as $e_i\phi = \sum\limits_{j<r_{(f_{\mathcal{W}}(i)+2)}} x_{ij}e_j$, $(x_{ij} \in R)$.

Using these coefficients we put (for $i < n$):

$$e_i\phi_{(\mathcal{W},t)} := \begin{cases} \sum\limits_{r_{s+1-t}\leq j<r_{s+2-t}} x_{ij}e_j & f_{\mathcal{W}}(i) = s \geq t-1 \\ \qquad\qquad 0 & else \end{cases}$$

The following are immediate consequences of the above definition.

Observation 2.4 *Let $M = \bigoplus\limits_{i<n} Re_i$ $(n \leq \omega)$ be a free R-module of countable rank. Moreover, let ϕ be an arbitrary endomorphism of M and let $\mathcal{W} = (r_s)_{s\in\omega}$ be a ϕ-sequence and $f_{\mathcal{W}}$ its $\mathcal{W}$-function.*

(i) *The infinite sum $\sum\limits_{t\in\omega} \phi_{(\mathcal{W},t)}$ has a well-defined meaning as*

$e_i\phi_{(\mathcal{W},t)} = 0$ for all $t > f_{\mathcal{W}}(i) + 1$ with any fixed $i < n$.

Furthermore $\phi = \sum\limits_{t\in\omega} \phi_{(\mathcal{W},t)}$.

(ii) *$\phi_{(\mathcal{W},t)}$ is a β-endomorphism for any $t \geq 2$ and so is $\phi_{(\mathcal{W},\geq 2)} := \sum\limits_{t\geq 2} \phi_{(\mathcal{W},t)}$.*

Recall that all β-endomorphisms are locally nilpotent by I Lemma 2.3.

(iii) *$\phi_{(\mathcal{W},1)}$ is a $\mathcal{W}$-endomorphism.*

Next we have a closer look at the endomorphisms given by (ii) and (iii).

Lemma 2.5 *Let $\mathcal{W} = (r_s)_{s\in\omega}$ be a strictly ascending sequence of integers with $r_0 = 0$. Moreover, let $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ be a free R–module of countable rank and let ϕ be a $\mathcal{W}$–endomorphism of M.*

Then ϕ is an automorphism of M if and only if $\phi \restriction_{M_s}$ is an automorphism of $M_s = \bigoplus_{\substack{i<n \\ r_s \leq i < r_{s+1}}} Re_i$ for each $s \in \omega$.

Proof: Trivially, if $\phi \restriction_{M_s}$ is an automorphism of M_s for all $s \in \omega$ then ϕ is an automorphism of M.

Conversely, if ϕ is an automorphism of M then $M_s\phi^{-1} \subseteq M_s$ $(s \in \omega)$ since for each $j \in [M_s\phi^{-1}]$ we must have $e_j\phi \in M_s$ which is only so if $j \in [M_s]$ by the definition of a $\mathcal{W}$–automorphism. Therefore $\phi \restriction_{M_s}$ is an automorphism of M_s for each $s \in \omega$.

□

Note that, in particular, the above lemma holds for $\phi_{(\mathcal{W},1)}$ for any endomorphism ϕ of M and any ϕ–sequence $\mathcal{W}$.

Lemma 2.6 *Let $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ be a free R–module of countable rank and let ϕ be an endomorphism of M with a given ϕ–sequence $\mathcal{W} = (r_s)_{s\in\omega}$.*

Moreover, let ψ be a $\mathcal{W}$–automorphism.

Then the endomorphism $\psi + \phi_{(\mathcal{W},\geq 2)}$ is also an automorphism of M.

Proof: By Observation 2.4 (ii), $\phi_{(\mathcal{W},\geq 2)} = \sum_{t\geq 2} \phi_{(\mathcal{W},t)}$ is a locally nilpotent β–endomorphism.

We show firstly that $\psi^{-1}\phi_{(\mathcal{W},\geq 2)}$ is also a β–endomorphism of M. We consider an arbitrary $i < n$. Let $s = f_{\mathcal{W}}(i)$. So, by Lemma 2.5, $e_i\psi^{-1} \in M_s$ and so $[e_i\psi^{-1}] \subseteq \{r_s, r_s + 1, \ldots, r_{s+1} - 1\}$. Thus $[e_i\psi^{-1}\phi_{(\mathcal{W},\geq 2)}] \subseteq \{0, 1, \ldots, r_s - 1\}$ since, for any $t \geq 2$, $[e_j\phi_{(\mathcal{W},t)}] \subseteq \{0, 1, \ldots, r_s - 1\}$ for any $j \in \{r_s, \ldots, r_{s+1} - 1\}$ (i.e. $f_{\mathcal{W}}(j)= s$). Therefore $\psi^{-1}\phi_{(\mathcal{W},\geq 2)}$ is a locally nilpotent β– endomorphism of M. Hence $1+\psi^{-1}\phi_{(\mathcal{W},\geq 2)}$ is an automorphism by Lemma 1.3 and thus so is $\psi+\phi_{(\mathcal{W},\geq 2)} = \psi(1+\psi^{-1}\phi_{(\mathcal{W},\geq 2)})$ as required. □

Lemma 2.7 *Let $M = \bigoplus_{i<n} Re_i$ be a free R–module of finite rank $n \geq 2$, let ϕ be an endomorphism of M and let $\mathcal{W} = (r_s)_{s\in\omega}$ be a ϕ–sequence with $r_2 = n$. Moreover let ψ be a $\mathcal{W}$-automorphism of M.*

Then the endomorphism $\psi + \phi_{(\mathcal{W},0)}$ is an automorphism of M.

Proof: Note that we can always choose such a $\mathcal{W}$ by Lemma 1.1. It follows from Lemma 2.5 and the assumption that $[e_i\psi^{-1}] \subseteq \{r_s, \ldots, r_{s+1}-1\}$ for $r_s \leq i < r_{s+1}$, $s = 0, 1$. Now, by definition of $\phi_{(\mathcal{W},0)}$, we have $e_i\psi^{-1}\phi_{(\mathcal{W},0)} = 0$ for $f(i)= 1$ and $[e_i\psi^{-1}\phi_{(\mathcal{W},0)}] \subseteq \{r_1, \ldots, r_2 - 1\}$ for $f(i)=$

0. Therefore $e_i(\psi^{-1}\phi_{(\mathcal{W},0)})^2 = 0$ for any $i < n$ and thus $(\psi^{-1}\phi_{(\mathcal{W},0)})^2 = 0$, i.e. $\psi^{-1}\phi_{(\mathcal{W},0)}$ is nilpotent and so locally nilpotent.

Hence, by Lemma 1.3, $1 + \psi^{-1}\phi_{(\mathcal{W},0)}$ is an automorphism of M and thus so is $\psi(1 + \psi^{-1}\phi_{(\mathcal{W},0)}) = \psi + \phi_{(\mathcal{W},0)}$. □

Next, we decompose the t^{th} $(\phi, \mathcal{W})$–mappings:

Definition 2.8 *Let $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ be a free R–module, let ϕ be an endomorphism of M and let $\mathcal{W} = (r_s)_{s\in\omega}$ be a ϕ–sequence.*

Moreover, let $\phi_{(\mathcal{W},t)}$ be the t^{th} $(\phi, \mathcal{W})$–mapping $(t \in \omega)$.

For any $t \in \omega$ we define mappings ${\phi_{(\mathcal{W},t)}}_0$ and ${\phi_{(\mathcal{W},t)}}_1$ as follows $(i < n)$:

$$e_i {\phi_{(\mathcal{W},t)}}_0 = \begin{cases} e_i\phi_{(\mathcal{W},t)} & f_{\mathcal{W}}(i) \textit{ even} \\ 0 & \textit{otherwise.} \end{cases}$$

$$e_i {\phi_{(\mathcal{W},t)}}_1 = \begin{cases} e_i\phi_{(\mathcal{W},t)} & f_{\mathcal{W}}(i) \textit{ odd} \\ 0 & \textit{otherwise.} \end{cases}$$

Observe that $\phi_{(\mathcal{W},t)} = {\phi_{(\mathcal{W},t)}}_0 + {\phi_{(\mathcal{W},t)}}_1$ for any $t \in \omega$.

Notation 2.9 *Let $(x_i)_{i\in I} = \{x_0, x_1, \ldots, x_i, \ldots\}$ be a sequence with indexing set I and let y be an arbitrary mathematical object. Then $y^\wedge(x_i)_{i\in I}$ denotes the sequence $\{y, x_0, x_1, \ldots, x_i, \ldots\}$.*

Proposition 2.10 *Let $M = \bigoplus_{i<n} Re_i$ $(n \leq \omega)$ be a free R–module, let ϕ be an endomorphism of M and let $\mathcal{W} = (r_s)_{s\in\omega}$ be a ϕ–sequence. Moreover let ψ be a $\mathcal{W}$–automorphism of M.*

Then $\psi + \phi_{(\mathcal{W},0)_0}$ is a $\mathcal{W}^*$–automorphism of M for $\mathcal{W}^* = (r_{2s})_{s\in\omega}$.

Also, $\psi + \phi_{(\mathcal{W},0)_1}$ is a $\mathcal{W}^{**}$–automorphism of M for $\mathcal{W}^{**} = r_0{}^\wedge(r_{2s+1})_{s\in\omega}$.

Proof: As a trivial consequence of Lemma 2.5 notice that since ψ is a $\mathcal{W}$–automorphism of M then so too is ψ^{-1} and furthermore $M_s = \bigoplus_{r_s\leq i<r_{s+1}} Re_i$ is invariant under ϕ^{-1} for any $s \in \omega$. Therefore by the definition of $\phi_{(\mathcal{W},0)_0}$ we have that $(\psi^{-1}\phi_{(\mathcal{W},0)_0})^2 = 0$ since $e_i\psi^{-1}\phi_{(\mathcal{W},0)_0} = 0$ for $f_{\mathcal{W}}(i)$ an odd number and $[e_i\psi^{-1}\phi_{(\mathcal{W},0)_0}] = [e_i\psi^{-1}\phi_{(\mathcal{W},0)}] \subseteq \{r_{f_{\mathcal{W}}(i)+1}, \ldots, r_{f_{\mathcal{W}}(i)+2} - 1\}$ for $f_{\mathcal{W}}(i)$ an even number. Similarly, we have $(\psi^{-1}\phi_{(\mathcal{W},0)_1})^2 = 0$.

Therefore, both $\psi^{-1}\phi_{(\mathcal{W},0)_0}$ and $\psi^{-1}\phi_{(\mathcal{W},0)_1}$ are nilpotent endomorphisms of M.

By applying Corollary 1.2, we obtain that both $1 + \psi^{-1}\phi_{(\mathcal{W},0)_0}$ and $1+\psi^{-1}\phi_{(\mathcal{W},0)_1}$ are automorphisms of M and , recalling that $\psi \in Aut(M)$, we get $\psi + \phi_{(\mathcal{W},0)_0}$ and $\psi + \phi_{(\mathcal{W},0)_1}$ are automorphisms of M.

It remains to show that the condition on the support is satisified.

Let us first consider $\psi + \phi_{(\mathcal{W},0)_0}$. Let $i < n$ and $r_{2s} \leq i < r_{2s+2}$. Then either $e_i\phi_{(\mathcal{W},0)_0} = 0$ (for $f_{\mathcal{W}}(i)= 2s+1$) or $e_i\phi_{(\mathcal{W},0)_0} = e_i\phi_{(\mathcal{W},0)}$ (for $f_{\mathcal{W}}(i)= 2s$). Thus $[e_i\phi_{(\mathcal{W},0)_0}] \subseteq \{r_{2s+1}, \ldots, r_{2(s+1)} - 1\}$. Moreover, $[e_i\psi] \subseteq \{r_{2s}, \ldots, r_{2s+2} - 1\}$ since ψ is a $\mathcal{W}$–automorphism. Hence $[e_i(\psi + \phi_{(\mathcal{W},0)_0})] \subseteq \{r_{2s}, \ldots, r_{2s+2} - 1\}$ for any $i < n$ with $r_{2s} \leq i < r_{2(s+1)}$ $(s \in \omega)$, i.e. $\psi + \phi_{(\mathcal{W},0)_0}$ is a $\mathcal{W}^*$–automorphism of M.

Similarly, consider $\psi + \phi_{(\mathcal{W},0)_1}$. First, let $i < n$ with $r_0 \leq i < r_1$. Then $e_i\phi_{(\mathcal{W},0)_1} = 0$ by definition and thus $[e_i(\psi + \phi_{(\mathcal{W},0)_1})] \subseteq \{0, \ldots, r_1 - 1\}$. Now let $i < n$ with $r_{2s+1} \leq i < r_{2s+3}$. Then $e_i\phi_{(\mathcal{W},0)_1} = 0$ for $f_{\mathcal{W}}(i)= 2s+2$ and $e_i\phi_{(\mathcal{W},0)_1} = e_i\phi_{(\mathcal{W},0)}$ for $f_{\mathcal{W}}(i)= 2s+1$. In the latter case we have $[e_i\phi_{(\mathcal{W},0)_1}] \subseteq \{r_{2s+2}, \ldots, r_{2s+3} - 1\}$. We deduce, therefore, that $[e_i(\psi + \phi_{(\mathcal{W},0)_1})] \subseteq \{r_{2s+1}, \ldots, r_{2s+3} - 1\}$ for any $i < n$ with $r_{2s+1} \leq i < r_{2s+3}$. Therefore $\psi + \phi_{(\mathcal{W},0)_1}$ is a $\mathcal{W}^{**}$–automorphism of M.

□

We are now ready to prove the essential result of this section.

Theorem 2.11 *Let $m \in \mathbb{Z}^+$. Let R be a commutative ring such that any free R–module of finite rank at least m has unit sum number 2. Moreover, let $M = \bigoplus_{i<\omega} Re_i$ be a free R–module of countably infinite rank.*

Then every endomorphism of M is a sum of two automorphisms of M.

Proof: Let M be as in the assumption and let ϕ be any endomorphism of M. We choose a ϕ–sequence $\mathcal{W}$ $=(r_s)_{s\in\omega}$ such that $r_{s+1} - r_s > m$ for all $s \in \omega$. Recall that $\phi = \sum\limits_{t\in\omega} \phi_{(\mathcal{W}.t)}$ where $\phi_{(\mathcal{W}.t)}$ denotes the t^{th} $(\phi, \mathcal{W})$–mapping $(t \in \omega)$.

First we consider $\phi_{(\mathcal{W}.1)}$. By Observation 2.4, $\phi_{(\mathcal{W}.1)}$ is a $\mathcal{W}$–endomorphism, i.e. $M_s = \bigoplus\limits_{r_s\leq i<r_{s+1}} Re_i$ is invariant under $\phi_{(\mathcal{W}.1)}$ for any $s \in \omega$. Thus $\phi_{(\mathcal{W}.1)} \restriction_{M_s}$ is an endomorphism of the finite rank module M_s (with $\mathrm{rk}(M_s) > m$) and hence it can be written as the sum of two automorphisms of M_s, say $\phi_{(\mathcal{W}.1)} \restriction_{M_s}= \alpha_s+\beta_s$ $(\alpha_s, \beta_s \in Aut(M_s))$. Put $\alpha = \sum\limits_{s\in\omega} \alpha_s$ and $\beta = \sum\limits_{s\in\omega} \beta_s$. Clearly, α and β are $\mathcal{W}$–automorphisms (see Lemma 2.5). Now $\phi_{(\mathcal{W}.1)} = \sum\limits_{s\in\omega}(\phi_{(\mathcal{W}.1)} \restriction_{M_s}) = \sum\limits_{s\in\omega}(\alpha_s + \beta_s)= \alpha + \beta$ and therefore

$$\begin{aligned}\phi &= \phi_{(\mathcal{W}.0)} + \alpha + \beta + \phi_{(\mathcal{W}.2)} + \sum_{t\geq 3} \phi_{(\mathcal{W}.t)} \\ &= (\alpha + \phi_{(\mathcal{W}.0)_0} + \phi_{(\mathcal{W}.2)_0} + \phi_{(\mathcal{W}.\geq 3)}) + (\beta + \phi_{(\mathcal{W}.0)_1} + \phi_{(\mathcal{W}.2)_1}) \quad (*)\end{aligned}$$

where $\phi_{(\mathcal{W}.>3)} := \sum\limits_{t>3} \phi_{(\mathcal{W}.t)}$ and $\phi_{(\mathcal{W}.t)} = \phi_{(\mathcal{W}.t)_0} + \phi_{(\mathcal{W}.t)_1}$ $(t \in \omega)$, as given by Definition 2.8.

We now show that (*) is, in fact, a sum of two automorphisms.

First we consider $\gamma = \alpha + \phi_{(\mathcal{W}.0)_0} + \phi_{(\mathcal{W}.2)_0} + \phi_{(\mathcal{W}.\geq 3)}$. By Proposition 2.10 we have that $\alpha + \phi_{(\mathcal{W}.0)_0}$ is a $\mathcal{W}'$– automorphism where $\mathcal{W}'$ $=(r_{2s})_{s\in\omega}$. Now consider $\phi_{(\mathcal{W}.2)_0} + \phi_{(\mathcal{W}.\geq 3)}$; we claim that the sum equals

$\gamma_{(\mathcal{W}^*,\geq 2)} := \sum_{t\geq 2}\gamma_{(\mathcal{W}^*,t)}$. Consider the term $\phi_{(\mathcal{W},2)_0}$. For $0 \leq i < r_1$, since $f_{\mathcal{W}}(i) = 0$ we have $e_i\phi_{(\mathcal{W},2)_0} = 0$ and for $r_1 \leq i < r_2$, since $f_{\mathcal{W}}(i) = 1$, and so is odd, we have $e_i\phi_{(\mathcal{W},2)_0} = 0$. Now let $s > 0$ and $r_{2s} \leq i < r_{2s+2}$. It follows from the definitions that

$$e_i\phi_{(\mathcal{W},2)_0} = \begin{cases} e_i\phi_{(\mathcal{W},2)} & for \quad f_{\mathcal{W}}(i) = 2s \\ 0 & for \quad f_{\mathcal{W}}(i) = 2s+1 \end{cases}$$

Therefore, since $[e_i\phi_{(\mathcal{W},2)}] \subseteq \{r_{2s-1}, \ldots, r_{2s}-1\}$ for $f_{\mathcal{W}}(i)= 2s$, we have, in terms of $\mathcal{W}^*$, that $[e_i\phi_{(\mathcal{W},2)_0}] \subseteq \{r_{2s-2}, \ldots, r_{2s}-1\}$ for any i with $r_{2s} \leq i < r_{2s+2}$ and $e_i\phi_{(\mathcal{W},2)_0} = 0$ otherwise.

Now we consider $\phi_{(\mathcal{W},\geq 3)}$. For $0 \leq i < r_2$, i.e. $0 \leq s < 2$, we have $e_i\phi_{(\mathcal{W},\geq 3)} = 0$ by definition. For $s > 1$ and $r_{2s} \leq i < r_{2s+2}$ we have $[e_i\phi_{(\mathcal{W},\geq 3)}] \subseteq \{0, \ldots, r_{2s}-1\}$.

Now we consider the sum $\phi_{(\mathcal{W},2)_0} + \phi_{(\mathcal{W},\geq 3)}$; it is now clear that $[e_i(\phi_{(\mathcal{W},2)_0} + \phi_{(\mathcal{W},\geq 3)})] \subseteq \{0, \ldots, r_{2s}-1\}$ for any i with $r_{2s} \leq i < r_{2s+2}$ and any $s \in \omega$.

Adjusting these properties to $\mathcal{W}^*$, we have $\phi_{(\mathcal{W},2)_0} + \phi_{(\mathcal{W},\geq 3)} = \gamma_{(\mathcal{W}^*,\geq 2)}$ and also $\alpha + \phi_{(\mathcal{W},0)_0} = \gamma_{(\mathcal{W}^*,1)}$. Since we have already shown that $\gamma_{(\mathcal{W}^*,1)}$ is a $\mathcal{W}^*$-automorphism of M then it follows from Lemma 2.6 that $\gamma = \gamma_{(\mathcal{W}^*,1)} + \gamma_{(\mathcal{W}^*,\geq 2)}$ is an automorphism of M, i.e. $\gamma_{(\mathcal{W}^*,0)} = 0$ by our construction.

Now we let $\delta = \beta + \phi_{(\mathcal{W}.0)_1} + \phi_{(\mathcal{W}.2)_1}$. Using an argument similar to that which we used for γ, we show that δ is an automorphism of M. Using Proposition 2.10, $\beta + \phi_{(\mathcal{W}.0)_1}$ is a $\mathcal{W}^{**}$- automorphism where $\mathcal{W}^{**} = r_0{}^\wedge(r_{2s+1})_{s\in\omega}$. For $0 \leq i < r_1$ we have $e_i\phi_{(\mathcal{W}.2)_1} = 0$. Now let $s \geq 0$ and $r_{2s+1} \leq i < r_{2s+3}$. It follows from the definitions that

$$e_i\phi_{(\mathcal{W}.2)_1} = \begin{cases} 0 & for \quad f_{\mathcal{W}}(i) = 2s \\ e_i\phi_{(\mathcal{W}.2)} & for \quad f_{\mathcal{W}}(i) = 2s+1 \end{cases}$$

Therefore, since $[e_i\phi_{(\mathcal{W}.2)}] \subseteq \{r_{2s},\ldots,r_{2s+1}-1\}$ for $f_{\mathcal{W}}(i)= 2s+1$, we have, in terms of $\mathcal{W}^*$, that $[e_i\phi_{(\mathcal{W}.2)_1}] \subseteq \{r_{2s-1},\ldots,r_{2s+1}-1\}$ for any i with $r_{2s+1} \leq i < r_{2s+3}$ and $e_i\phi_{(\mathcal{W}.2)_1} = 0$ otherwise.

Therefore $[e_i(\phi_{(\mathcal{W}.2)_1})] \subseteq \{0,\ldots,r_{2s+1}-1\}$ for any $r_{2s+1} \leq i < r_{2s+3}$ with $s \geq 0$ and $e_i(\phi_{(\mathcal{W}.2)_1})= 0$ otherwise.

Thus, if we adjust these properties to $\mathcal{W}^{**}$, we have $\phi_{(\mathcal{W}.2)_1} = \delta_{(\mathcal{W}^{**}.\geq 2)}$ and $\beta + \phi_{(\mathcal{W}.0)_1} = \delta_{(\mathcal{W}^{**}.1)}$. Since we have already shown that $\delta_{(\mathcal{W}^{**}.1)}$ is a $\mathcal{W}^{**}$ -automorphism of M then it follows from Lemma 2.6 that $\delta = \delta_{(\mathcal{W}^{**}.1)} + \delta_{(\mathcal{W}^{**}.\geq 2)}$ is an automorphism of M, i.e. note $\delta_{(\mathcal{W}^{**}.0)} = 0$ by construction.

Therefore we have shown $\phi = \gamma + \delta$ is a sum of two automorphisms of

M. □

Applying Theorem 1.9 now to Theorem 2.11 the following result is proven:

Theorem 2.12 *Let* $M = \bigoplus_{i<\kappa} Re_i$ *be a free* R*–module of arbitrary rank* $\kappa > m$ *for some* $m \in \mathbb{Z}^+$*, over a commutative ring* R*. If every free module of finite rank at least* m *over* R *has unit sum number equal to 2, then every endomorphism of* M *is a sum of two automorphisms of* M*.*

We know of no commutative ring R where the unit sum number of a free R-module of rank greater than 2 has a unit sum number differing from that of a free R-module of rank 2. Furthermore, we know of no non-trivial commutative ring, R, where a free R-module of rank not less than 2 has a finite unit sum number differing from 2. However, the following answers finally the question of unit sum number for free R-modules of arbitrary rank greater than 1 over a PID R.

Corollary 2.13 *Let* $M = \bigoplus_{i<\kappa} Re_i$ *be a free* R*–module of arbitrary rank greater than* 1 *over a PID* R*. Then* $\text{usn}(M) = 2$.

Proof: The finite rank case (rank greater than 1) has been shown in I, Theorem 2.4, due to Wans [29]. Then applying Theorem 2.12 with $m = 2$ gives our result. □

In Chapter III we will show that there are a variety of possibilities for the unit sum number of a free R–module of rank 1 over a PID R.

§3 Unit sum numbers of completely decomposable groups

In [20] Opdenhövel has shown that if G is a completely decomposable abelian group of finite rank, then usn$(G) = 2$ if and only if usn$(G(\tau)/G^*(\tau)) = 2$, for all $\tau \in T_{cr}(G)$ with $rk(G(\tau)/G^*(\tau)) = 1$ (see [20, IV Proposition 1.11]). Recall that $G(\tau) = \langle g \in G \mid \text{type}(g) \geq \tau \rangle$ and $G^*(\tau) = \langle g \in G \mid \text{type}(g) > \tau \rangle$ with $T_{cr}(G)$ denoting the set of critical types of G.

Notice that for a homogeneous completely decomposable group G of arbitrary rank greater than 1, it follows from I, Lemma 2.15 that the endomorphism ring of G is ring isomorphic to the endomorphism ring of a free R–module over R where R is that subring of $\mathbb{Q}$, containing $\mathbb{Z}$, with the reduced type of G (i.e. R is a PID) and so, by Corollary 2.13, we can deduce that usn(G)= 2.

We now extend Opdenhövel's result to arbitrary rank and develop it to give a more general result. We begin with two lemmas.

Lemma 3.1 *Let $G = A \bigoplus B$ be the direct sum of two arbitrary groups with $Hom(A, B) = 0$. Let ϕ be an arbitrary endomorphism of G, represented as*

$$\phi = \begin{pmatrix} \phi_{A.A} & 0 \\ \phi_{B.A} & \phi_{B.B} \end{pmatrix}$$

where $\phi_{A.A} \in E(A)$, $\phi_{B.B} \in E(B)$, $\phi_{B.A} \in Hom(B, A)$. Then ϕ is an automorphism of G if and only if both $\phi_{A.A}$ and $\phi_{B.B}$ are automorphisms of A and B, respectively.

Proof: Let α, β be arbitrary endomorphisms of G. Represent the product of α and β as follows

$$\alpha\beta = \begin{pmatrix} \alpha_{A.A} & 0 \\ \alpha_{B.A} & \alpha_{B.B} \end{pmatrix}\begin{pmatrix} \beta_{A.A} & 0 \\ \beta_{B.A} & \beta_{B.B} \end{pmatrix} = \begin{pmatrix} \alpha_{A.A}\beta_{A.A} & 0 \\ \alpha_{B.A}\beta_{A.A} + \alpha_{B.B}\beta_{B.A} & \alpha_{B.B}\beta_{B.B} \end{pmatrix}$$

where $\alpha_{A.A}, \beta_{A.A} \in E(A)$; $\alpha_{B.B}, \beta_{B.B} \in E(B)$; $\alpha_{B.A}, \beta_{B.A} \in Hom(B, A)$. Firstly, if α is an arbitrary automorphism of G, and β the inverse of α then observe that $\alpha_{A.A}\beta_{A.A} = 1_A$, and $\alpha_{B.B}\beta_{B.B} = 1_B$. Similarly, considering the product $\beta\alpha$ we get $\beta_{A.A}\alpha_{A.A} = 1_A$ and $\beta_{B.B}\alpha_{B.B} = 1_B$. Of course, this means that $\alpha_{A,A} \in Aut(A)$ and $\alpha_{B.B} \in Aut(B)$.

Conversely, given δ, any endomorphism of G, such that $\delta_{A,A}$ and $\delta_{B,B}$ are units then δ has the multiplicative inverse

$$\begin{pmatrix} {\delta_{A.A}}^{-1} & 0 \\ -{\delta_{B.B}}^{-1}\delta_{B.A}{\delta_{A.A}}^{-1} & {\delta_{B.B}}^{-1} \end{pmatrix}$$

Therefore an endomorphism of G is an automorphism if and only if the two diagonal entries are units. □

Lemma 3.2 *Let $G = A \bigoplus B$ be the direct sum of two arbitrary groups with $Hom(A,B) = 0$ and $2 \in Aut(G)$. Then $\mathrm{usn}(G) = max\{\mathrm{usn}(A), \mathrm{usn}(B)\}$; using the convention for unit sum numbers $n < \omega < \infty$ for all $n \in \mathbb{N}$.*

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 $\phi_{A.A} \in E(A)$, $\phi_{B.B} \in E(B)$, $\phi_{B.A} \in Hom(B,A)$. Now let $\lambda = \max\{\mathrm{usn}(A), \mathrm{usn}(B)\} = \mathrm{usn}(B)$.

If $\lambda \in \mathbb{N}$ then choose ϕ such that $\phi_{A,A}$ is a sum of usn(A) units of A and no less. Of course, since $\lambda =$ usn(B), then $\phi_{B,B}$ is a sum of λ units of B. Recall that if, say, usn$(A) = k < \lambda$, then we can write $\phi_{A,A} = (\lambda - k)(1_A) + (\phi_{A,A} - (\lambda - k)1_A)$, where 1_A is the identity in $E(A)$, and since $(\phi_{A,A} - (\lambda - k)1_A)$ is a sum of k automorphisms of A then $\phi_{A,A}$ is a sum of λ automorphisms of A. Therefore ϕ is a sum of λ automorphisms of G and so usn$(G)= \lambda$.

If $\lambda = \omega$ then whatever $n \in \mathbb{N}$ there exists some $\phi_{B,B} \in E(B)$ which cannot be expressed as a sum of exactly n automorphisms of B. So, by Lemma 3.1, for each $n \in \mathbb{N}$ there is some $\phi \in E(G)$ which cannot be expressed as a sum of exactly n automorphisms of G so usn$(G)= \omega$.

Similarly, if $\lambda = \infty$ there exists some $\phi_{B,B} \in E(B)$ which is not a sum of automorphisms of B. Then, by Lemma 3.1 there exists some $\phi \in E(G)$ which is not a sum of automorphisms of G. Therefore usn$(G)= \infty$.

A similar argument applies if $\lambda =$ usn(A). We are finished. □

Using the above we finally prove:

Theorem 3.3 *Let* $G = \bigoplus_{t \in T_{cr}(G)} G_{(t)}$ *be a completely decomposable group of arbitrary rank where* $T_{cr}(G)$ *denotes the set of critical types of* G *and* $G_{(t)}$ *denotes the t-homogeneous component of* G. *Let* $2 \in Aut(G)$.

(i) *If* $T_{cr}(G)$ *is finite then* $\text{usn}(G) = max\{\text{usn}(G_{(t)}) \mid t \in T_{cr}(G)\}$.

(ii) *Let* $\mid T_{cr}(G) \mid$ *be infinite then*

(a) *If there exists* $n \in \mathbb{N}$, *such that* $\text{usn}(G_{(t)}) < n$, *for each* $t \in T_{cr}(G)$, *then* $\text{usn}(G) \geq max\{\text{usn}(G_{(t)}) \mid t \in T_{cr}(G)\}$.

(b) *If, for each* $n \in \mathbb{N}$, *there exists* $t \in T_{cr}(G)$ *such that* $\text{usn}(G_{(t)}) > n$ *then* $\text{usn}(G) \geq \omega$.

(*using the convention for unit sum numbers,* $n < \omega < \infty$ *for all* $n \in \mathbb{N}$)

Proof: If $\mid T_{cr}(G) \mid = 1$ then G is homogeneous and by I, Lemma 2.15 and Corollary 2.13 we are finished.

Let $\mid T_{cr}(G) \mid > 1$. Recall that $G = \bigoplus\limits_{t \in T_{cr}(G)} G_{(t)}$ expresses G as a direct sum of its homogeneous summands.

Let $\tau \in T_{cr}(G)$ be arbitrary and set $G' = G_{(\tau)} \bigoplus \bigoplus\limits_{\substack{t > \tau \\ t \in T_{cr}(G)}} G_{(t)}$. Since a homomorphism cannot map an element onto an element of lesser type or even incomparable type, we have that $Hom(\bigoplus\limits_{\substack{t > \tau \\ t \in T_{cr}(G)}} G_{(t)}, G_{(\tau)}) = 0$.

By Lemma 3.2, $\text{usn}(G') = max\{\ \text{usn}(G_{(\tau)}), \text{usn}(\bigoplus\limits_{\substack{t > \tau \\ t \in T_{cr}(G)}} G_{(t)})\}$.

Of course, $G = G' \bigoplus \bigoplus\limits_{\substack{t \not\geq \tau \\ t \in T_{cr}(G)}} G_{(t)}$, and $Hom(G', \bigoplus\limits_{\substack{t \not\geq \tau \\ t \in T_{cr}(G)}} G_{(t)}) = 0$.

So,

$$\mathrm{usn}(G) = max\{\mathrm{usn}(\bigoplus_{\substack{t \ngeq \tau \\ t \in T_{cr}(G)}} G_{(t)}),\ \mathrm{usn}(G')\}.$$

$$\mathrm{usn}(G) = max\{\mathrm{usn}(\bigoplus_{\substack{t \ngeq \tau \\ t \in T_{cr}(G)}} G_{(t)}), \mathrm{usn}(G_{(\tau)}), \mathrm{usn}(\bigoplus_{\substack{t > \tau \\ t \in T_{cr}(G)}} G_{(t)})\}.$$

$$\geq \quad \mathrm{usn}(G_{(\tau)}).$$

Therefore, since τ was arbitrarily chosen: If, for each $n \in \mathbb{N}$, there is some $t \in T_{cr}(G)$ such that $\mathrm{usn}(G_{(t)}) > n$ then $\mathrm{usn}(G) > n$ for each $n \in \mathbb{N}$ and therefore $\mathrm{usn}(G) \geq \omega$. Otherwise there exists some $n \in \mathbb{N}$ such that $\mathrm{usn}(G_{(t)}) \leq n$ for all $t \in T_{cr}(G)$ and so we may write

$$\mathrm{usn}(G) \geq \max\{\mathrm{usn}(G_{(t)}) \mid t \in T_{cr}(G)\}.$$

In this way we have proved (ii).

We now prove (i) using an induction argument. Let $\mid T_{cr}(G) \mid = 1$. Then $\mathrm{usn}(G) = \mathrm{usn}(G_{(t)})$ where $\{t\} = T_{cr}(G)$.

Let $1 < m$ be an arbitrary positive integer and assume for all integers, $1 < k < m$, that if $\mid T_{cr}(G) \mid = k$ then $\mathrm{usn}(G) = \max\{\mathrm{usn}(G_{(t)}) \mid t \in T_{cr}(G)\}$. Now, let $\mid T_{cr}(G) \mid = m$ and choose any $\tau \in T_{cr}(G)$. Then, as we showed above, $\mathrm{usn}(G) = max\{\mathrm{usn}(\bigoplus_{\substack{t \ngeq \tau \\ t \in T_{cr}(G)}} G_{(t)}), \mathrm{usn}(G_{(\tau)}), \mathrm{usn}(\bigoplus_{\substack{t > \tau \\ t \in T_{cr}(G)}} G_{(t)})\}$.

Since, $\{t \mid t \geq \tau, t \in T_{cr}(G)\}$ and $\{t \mid t \ngeq \tau, t \in T_{cr}(G)\}$ are both proper subsets of $T_{cr}(G)$ and so of cardinality less than m, then by our hypothesis $\mathrm{usn}(G) = max\{\max\{\mathrm{usn}(G_{(t)}) \mid t \in T_{cr}(\bigoplus_{\substack{t \ngeq \tau \\ t \in T_{cr}(G)}} G_{(t)})\}, \mathrm{usn}(G_{(\tau)}),$

$$\max\{\mathrm{usn}(G_{(t)}) \mid t \in T_{cr}(\bigoplus_{\substack{t \geq \tau \\ t \in T_{cr}(G)}} G_{(t)})\}\} = \max\{\mathrm{usn}(G_{(t)}) \mid t \in T_{cr}(G)\}$$

and so (i) has been proved. □

We conclude with some examples of unit sum numbers for completely decomposable groups where $\mid T_{cr}(G) \mid$ is countably infinite, including an example of a completely decomposable group with unit sum number ∞. Let $T_{cr}(G) = \{t_i; 1 \leq i < \omega, t_i \neq t_j \text{ for all } i \neq j\}$. Let $\Pi = \{p_i\}_{i=1,2,\ldots}$ be the set of rational primes under the natural ordering. In each case let us assume that $Hom(G_{(t_i)}, G_{(t_j)}) = 0$ for all $i \neq j$, $1 \leq i, j < \omega$, i.e. there are no comparable types within the set of critical types of G, and so $E(G) \underset{ring}{\cong} \prod_{1 \leq i < \omega} E(G_{(t_i)})$. Recalling that sums of units are inherited by ring direct products we begin our examples;

- Choose G and $T_{cr}(G)$ such that $\mathrm{usn}(G_{(t_i)}) = \omega$ for each $1 \leq i < \omega$. Then we may choose some $\phi \in E(G)$ with $\varphi = \prod_{1 \leq i < \omega} \phi_{t_i}$ where $\phi_{t_i} \in E(G_{(t_i)})$ and such that ϕ_{t_i} is not expressible as a sum of i units of $E(G_{(t_i)})$ for each $1 \leq i < \omega$. Then $\phi = (\varphi_{t_1}, \phi_{t_2}, \ldots)$ cannot be written as a sum of n units for any $n \in \mathbb{N}$, and so $\mathrm{usn}(G) = \infty$. Lastly, let us define a group for which this is so. Set $T_{cr}(G) = \{t_i = (k_{p_j})_{j=1,2,\ldots}$ where $k_{p_i} = \infty$, $k_{p_j} = 0$, for all

$j \neq i \quad | \; i \in \mathbb{N}\}$ and set $\mathrm{rk}(G_{(t_i)}) = 1$ for all $1 \leq i < \omega$ (to see $\mathrm{usn}(G_{(t_i)}) = \omega$ for each $0 \leq i < \omega$ refer to III, Theorem 1.2 and III, Proposition 1.1).

- Set $T_{cr}(G) = \{t_i = (k_{p_j})_{j=1,2,\ldots}$ where $k_{p_i} = \infty$ and $k_{p_j} = 0$, for all $j \neq i \quad | \; i \in \mathbb{N}\}$ and set $\mathrm{rk}(G_{(t_i)}) = 2$ for all $i \neq 1$, and set $\mathrm{rk}(G_{(t_1)}) = 1$ (where $t_{p_1} = t_2 = (k_{p_j})_{j=1,2,\ldots}$ with $k_2 = \infty$ and $k_{p_j} = 0$, for all $j \neq 1$). In this case, since $\mathrm{rk}(G(t_i)) = 2$, then $\mathrm{usn}(G_{(t_i)}) = 2$ for each t_i with $i \neq 1$, $1 \leq i < \omega$ and, by III Theorem 1.2, $\mathrm{usn}(G_{(t_1)}) = \omega$. Choose an arbitrary endomorphism ϕ of G, then $\phi = \prod\limits_{1 \leq i < \omega} \phi_{t_i}$, where $\phi_{t_i} \in E(G_{(t_i)})$ for each $1 \leq i < \omega$. Since $\mathrm{usn}(G_{(t_1)}) = \omega$ then ϕ_{t_1} is a sum of m units of $E(G_{(t_1)})$ for some $m(> 0) \in \mathbb{N}$. If $m = 1$ then, since $\frac{1}{2} \in Aut(G_{(t_1)})$, $\phi_{t_1} = \frac{1}{2}\phi_{t_1} + \frac{1}{2}\phi_{t_1}$ is a sum of two units of $E(G_{(t_1)})$. Therefore, ϕ_{t_i} is a sum of two units of $E(G_{(t_i)})$ for each $1 \leq i < \omega$.

  If $m > 2$, then $\phi_{t_i} = (\phi_{t_i} - (m-2)1_{E(G_{(t_i)})}) + (m-2)1_{E(G_{(t_i)})}$ for each $2 \leq i < \omega$, where $1_{E(G_{(t_i)})}$ is the identity in $E(G_{(t_i)})$ for each $1 \leq i < \omega$. Since, for each $2 \leq i < \omega$, $\mathrm{usn}(G_{(t_i)}) = 2$ then $(\phi_{t_i} - (m-2)1_{E(G_{(t_i)})})$ is a sum of 2 units in $E(G_{(t_i)})$ and so ϕ_{t_i} is a sum of m units of $E(G_{(t_i)})$, for each $1 \leq i < \omega$.

If $m = 2$, then ϕ_{t_i} is a sum of two units of $E(G_{(t_i)})$ for each $1 \leq i < \omega$.

In this way it is easily seen that $\phi = (\phi_{t_1}, \phi_{t_2}, \ldots)$ can be expressed as a sum of m units. Therefore $\mathrm{usn}(G) = \omega$.

- Set $T_{cr}(G) = \{t_i = (k_{p_j})_{j=1,2,\ldots}$ where $k_{p_i} = \infty$ and $k_{p_j} = 0$ for all $j \neq i \quad | \ i \in \mathbb{N}\}$ and set $\mathrm{rk}(G_{(t_i)}) = 2$ for all $1 \leq i < \omega$. Using a similar method to that of the last case it can be shown that $\mathrm{usn}(G) = 2$.

III Unit sum numbers of rational groups

In Section 3 of Chapter II we saw in Theorem 3.3 that the unit sum number of a completely decomposable group G is determined by the set of unit sum numbers of the t–homogeneous summands of G which are of rank 1 ($t \in T_{cr}(G)$). Opdenhövel's result [20, IV, Proposition 1.11]) had highlighted this previously for finite rank. In this chapter we show that there are a variety of possibilities for unit sum numbers of rational groups including finite values greater than 2.

§1 General considerations

Every rational group is isomorphic to a subgroup of $\mathbb{Q}$ containing $\mathbb{Z}$. The endomorphism ring of such a group G is easily described: Any endomorphism of G is determined by its action on 1 and hence it corresponds to multiplication by a rational number $\frac{a}{b} \in G$ $((a,b) = 1,\ a, b \in \mathbb{Z})$. Since multiplication by integers is always possible, our only concern is when $\frac{1}{b}$ is an element of $\mathrm{E}_{\mathbb{Z}}(G)$. If $\frac{1}{b} \in \mathrm{E}_{\mathbb{Z}}(G)$ then $\frac{1}{b^2} \in \mathrm{E}_{\mathbb{Z}}(G)$ and so on, and thus it follows that $\frac{1}{b^n} \in \mathrm{E}_{\mathbb{Z}}(G)$ for all $n \in \mathbb{N}$. So, if $p \mid b$ then $h_p^G(1) = \infty$.

Thus $\mathrm{E}_{\mathbb{Z}}(G)$ is that subring of $\mathbb{Q}$ containing $\mathbb{Z}$ with the reduced type of

G.

The first two results reflect the importance of the prime number **2** in determining the unit sum numbers of rational groups .

Proposition 1.1 *Let G be a rational group. If 2 is not an automorphism of G then* usn(G)$=\omega$.

Proof: We need only consider $E_{\mathbb{Z}}(G) = R$, that subring of $\mathbb{Q}$ containing $\mathbb{Z}$ and with the reduced type of G. Consider an element $\frac{a}{b}$ of R where a, b are positive integers. If b is even then $\frac{a}{b} \cdot \frac{b}{2} = \frac{a}{2}$ is an element of R. Therefore a must be even or else $\frac{a-1}{2} \in \mathbb{Z}$ in which case $\frac{a}{2} - \frac{a-1}{2} = \frac{1}{2}$ must be an element of R, contradicting 2 not being a unit of R. Therefore if $\frac{a}{b}$ is a unit of R, expressed in lowest form, then both, a and b, must be odd.

Let n be any even positive integer. Consider any sum of n units of R, $\frac{a_1}{b_1} + \frac{a_2}{b_2} + \ldots + \frac{a_n}{b_n} = \frac{a_1 b_2 \ldots b_n + a_2 b_1 b_3 \ldots b_n + \ldots + a_n b_1 \ldots b_{n-1}}{b_1 \ldots b_n}$, where $\frac{a_i}{b_i}$ is a unit of R expressed in lowest form for each $i \in 1, 2, \ldots, n$. Observe that the denominator is a product of odd numbers and therefore odd and the numerator is an even sum of odd number products and therefore even. A sum of n units can never be a unit in this case. Therefore R has not got the n-sum property for any even integer n.

We know, however, that for any positive integer n a ring which has the n-sum property must also have the $(n+1)$-sum property. It follows that R cannot have the n-sum property for any positive integer n. Every element of R is a sum of units so we conclude that $\text{usn}(R) = \text{usn}(G) = \omega$.

□

Theorem 1.2 *Let G be any rational group such that $E(G) = \mathbb{Q}^{(2)}$. Then* $\text{usn}(G) = \omega$.

Proof: We prove that, for each positive integer n, there is an integer, namely $1 + 2^2 + \ldots + 2^n$, which cannot be expressed as a sum of n units of $\mathbb{Q}^{(2)}$. Now, in $\mathbb{Q}^{(2)}$ each unit is of the form $\pm 2^a$ where a is an integer. The proof is by induction on $n \in \mathbb{Z}^+$ where the induction statement is

$$1 + 2^2 + \ldots + 2^{2n} \neq \sum_{i=1}^{n} \pm 2^{a_i} \quad \text{for whatever } a_i \in \mathbb{Z}. \qquad (*)$$

The statement is true for $n = 1$ since $1 + 2^{2(1)} = 5$ and 5 is not a unit. We assume the statement is true for all positive integers $n < m$. Now, seeking a contradiction, assume

$$1 + 2^2 + \ldots + 2^{2m} = \sum_{i=1}^{m} \pm 2^{a_i}. \qquad (1)$$

for some fixed set of integers $a_1, \ldots, a_m$. The left hand side of this equation is odd and hence the set $\{i \mid a_i < 2\}$ is non-empty. By renumbering we can arrange that there is $l \in \mathbb{Z}^+, l \leq m$ such that $a_i < 2$ for $i = 1, \ldots, l$

and $a_i \geq 2$ for $i = l+1, \ldots, m$. Hence we can rewrite equation (1) as

$$2^2 + \ldots + 2^{2m} = (\sum_{i=1}^{l} \pm 2^{a_i}) - 1 + \sum_{i=l+1}^{m} \pm 2^{a_i}. \tag{2}$$

We claim that the term $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1$ can be written as a sum of less than l units in $\mathbb{Q}^{(2)}$ unless it is zero. Observe from the equation that 4 divides $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1$. So, writing $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1 = 4l'$ for some $l' \in \mathbb{Z}$, we note that this expresses $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1$ as a sum of $\mid l' \mid$ units for $l' \neq 0$. It remains to show that $\mid l' \mid < l$, for $l' \neq 0$.

Since $2^{a_i} \leq 2$ for all $a_i < 2$ it is clear that $\mid (\sum_{i=1}^{l} \pm 2^{a_i}) - 1 \mid = \mid 4l' \mid \leq 2l + 1$.Therefore we have $\mid 2l' \mid + 1 < 2l + 1$ which gives us $\mid l' \mid < l$ as $l' \neq 0$. The claim is proved.

Returning to equation (2), since $(\sum_{i=1}^{l} \pm 2^{a_i}) - 1$ is either zero or can be expressed as a sum of less than l units then $2^2 + \ldots + 2^{2m}$ can be expressed as a sum of less than m units. Thus we may write:

$$2^2 + \ldots + 2^{2m} = \sum_{j=1}^{m'} \pm 2^{b_j} \quad \text{for some } m' < m,\ b_j \in \mathbb{Z}\ .$$

Dividing this equation by 4 we get,

$$1 + \ldots + 2^{2(m-1)} = \sum_{j=1}^{m'} \pm 2^{b_j - 2}.$$

This contradicts the induction statement $(*)$ for $n = m - 1$, since any sum of $m' \leq m - 1$ units can easily be expressed as a sum of $m - 1$ units, i.e. $\sum_{i=1}^{m'} u_i = \sum_{i=1}^{m'-1} u_i + \frac{1}{2} u_{m'} + \frac{1}{2} u_{m'}$ where each u_i is a unit expresses a sum of m' units as a sum of $m'+1$ units. Hence the assumption (1) is false and the proof now follows by induction. Therefore $\text{usn}(G) = \text{usn}(\mathbb{Q}^{(2)}) = \omega$.

□

The following two lemmas will be very useful later on.

Lemma 1.3 *Let G be a rational group with $E_{\Xi}(G) = R$. If $\frac{1}{2} \in R$ then G has the n–sum property if and only if every positive integer is a sum of exactly n units of R.*

Proof: Note that R contains the integers.

In the first direction if R has the n–sum property for some positive integer n then clearly every positive integer is a sum of n units of R.

In the other direction, let every positive integer be expressible as a sum of n units of R. Then every negative integer must also be expressible as a sum of n units of R. For n even, a sum of n units for 0 is $\sum_{i=1}^{\frac{n}{2}} 1 + \sum_{i=1}^{\frac{n}{2}} -1$; for n odd , a sum of n units for 0 is $(\sum_{i=1}^{\frac{n-1}{2}-1} 1)+(\sum_{i=1}^{\frac{n-1}{2}} -1)+\frac{1}{2}+\frac{1}{2}$. Therefore all integers are sums of n units.

Consider an arbitrary non–integer element $\frac{a}{b}$ of R expressed in lowest form, a and b being integers.

If $a = 1$, then $\frac{a}{b}$ is a unit. Since products of units are units and 1 is a sum of n units then $\frac{a}{b} \cdot 1$ is also.

If $b = 1$, then $\frac{a}{b} = a$, an integer, and so is a sum of n units.

In any remaining case a and b must be relatively prime so there exist integers k, l such that $ka + lb = 1$. Now $k \cdot \frac{a}{b} + l$ is an element of R and $(k \cdot \frac{a}{b} + l) \cdot b = 1$. Therefore b is a unit of R and so also $\frac{1}{b}$. Since a, as an integer, is a sum of n units then $\frac{1}{b} \cdot a$ is also. □

Lemma 1.4 *Let G_1, G_2 be rational groups such that $E_{\mathbb{Z}}(G_1) \subseteq E_{\mathbb{Z}}(G_2)$. Then* $\mathrm{usn}(G_1) \geq \mathrm{usn}(G_2)$.

Proof: Since $E_{\mathbb{Z}}(G_1) \leq E_{\mathbb{Z}}(G_2)$ then every unit of $E_{\mathbb{Z}}(G_1)$ is also a unit of $E_{\mathbb{Z}}(G_2)$. So, if a positive integer z is a sum of n units in $E_{\mathbb{Z}}(G_1)$ then the same is true for z as an element of $E_{\mathbb{Z}}(G_2)$. There may, in fact, be more units in $E_{\mathbb{Z}}(G_2)$ than in $E_{\mathbb{Z}}(G_1)$ in which case z may be expressible as a sum of less than n units in $E_{\mathbb{Z}}(G_2)$. Therefore, by Lemma 1.3, $\mathrm{usn}(E_{\mathbb{Z}}(G_2)) \leq \mathrm{usn}(E_{\mathbb{Z}}(G_1))$ and so $\mathrm{usn}(G_2) \leq \mathrm{usn}(G_1)$. □

§2 Approach via elementary number theory

In this section unit sum numbers for various kinds of rational groups are investigated. The unit sum number of a rational group G is that of its endomorphism ring, which has the reduced type of G. The reduced type of a group G can be identified with a sequence of symbols 0 and ∞ corresponding to each of the rational primes. If the symbol ∞ corresponds to a prime p within the reduced type then $\frac{1}{p}$ is an element of the endomorphism ring of G and so p is a unit in the endomorphism ring. If the symbol 0 corresponds to a prime p within the reduced type then $\frac{1}{p}$ is not an element of the endomorphism ring of G. In this way we investigate the unit sum numbers of rational groups relative to the number and positioning of symbols 0 or ∞ within their reduced types.

Recall the definition $X_G := \{p \in \Pi \mid \frac{1}{p} \notin E_{\mathbb{Z}}(G)\}$ for a rational group G.

Theorem 2.1 *Let G be a rational group with $2 \in Aut(G)$. If X_G is finite then* $\mathrm{usn}(G) = 2$.

Proof: Let $R = E_{\mathbb{Z}}(G)$. Let $X_G = \{q_i \mid i = 1, \ldots, k\}$, where $k = \mid X_G \mid$. By Lemma 1.3, we need only prove all positive integers are sums of two units of R. Clearly, if 2 is a unit of R then every unit of R is a sum of two units. Now, by definition of X_G we know that for all $p \in \Pi \backslash X_G$, p is a unit of R and so any products of primes not in X_G are units of R. Let $z = (\prod_{i=1,\ldots,k} q_i^{m_i})(\prod_{p_j \in \Pi \backslash X_G} p_j^{n_j})$ with $m_i, n_j \in \omega$ be an arbitrary positive integer which is not a unit in R, i.e. some $q_i \in X_G$ divides z.

Since $(\prod_{p_j \in \Pi \backslash X_G} p_j^{n_j})$ is a unit we need only show that $z' = (\prod_{i=1,\ldots,k} q_i^{m_i})$ is a sum of two units of R. If every q_i in X_G divides z' then $(z'-1)$ is relatively prime to all $q_i \in X_G$ and therefore a unit, in which case $z' = (z'-1)+1$ is a sum of two units for z'.

If some q_i in X_G do not divide z' then $(z' \pm \prod_{q_i \nmid z'} q_i)$ is a unit since no prime in X_G can divide it. In this way, $z' = \frac{1}{2}(z' + \prod_{q_i \nmid z'} q_i) + \frac{1}{2}(z' - \prod_{q_i \nmid z'} q_i)$ expresses z' as a sum of two units and the result follows. We have shown that every positive integer is a sum of two units of R. □

Theorem 2.1 can be extended to show that there are many rational groups with X_G countably infinite yet with unit sum number of 2. The following result is similar to that of Opdenhövel [16, IV, Theorem 1.20], though it is arrived at in a completely different way. We will illustrate the proposition with an example after the proof. Recall that $\pi(x)$ is defined, for a real number x, as the number of rational primes not exceeding x.

Proposition 2.2 *Let G be a rational group with $E_{\mathbb{Z}}(G) = R$ where $2 \notin X_R$. Moreover, assume that, for any $x \in \mathbb{Z}^+$ with $(x,p) = 1$ for all $p \in \Pi \setminus X_G$ there is some prime $q > x$ so that $q' \notin X_R$ for all $q' \in \Pi$ with $q \leq q' < q^{\pi(q)}$. Then* $\operatorname{usn}(G) = 2$.

Proof: We need only prove that usn(R)= 2. By Lemma 1.3, it is only necessary to show that every positive integer is a sum of two units of R.

Since 2 is a unit of R every unit is a sum of two units. Each $p \in \Pi \setminus X_R$ is a unit of R and since products of units are units it is sufficient show that products of elements of $X_R = \{q_i \mid i \in I\}$ are sums of two units of R.

Let $x \in \mathbb{Z}^+$ such that $(x, p) = 1$ for all $p \in \Pi \setminus X_R$, i.e. x is a product of primes in X_R and $x \geq 3$. By assumption, there is some $q \in \Pi$ with $x < q$ so that $q' \notin X_R$ for all $q' \in \Pi$ with $q \leq q' < q^{\pi(q)}$. Then we claim that the following expresses x as a sum of two primes:

$$x = \frac{1}{2}(x + \prod_{q_i \nmid x; q_i < q} q_i) + \frac{1}{2}(x - \prod_{q_i \nmid x; q_i < q} q_i).$$

To prove this claim we need to show that $(x + \prod_{q_i \nmid x; q_i < q} q_i)$ is a unit of R. Let $p \in \Pi$ be such that p divides $(x + \prod_{q_i \nmid x; q_i < q} q_i)$. We show that $p \notin X_R$. If $p < q$ then since all primes in X_R less than q are accounted for by the prime factors of x and $(\prod_{q_i \nmid x; q_i < q} q_i)$, then p cannot divide both x and $\prod_{q_i \nmid x; q_i < q} q_i$ so $p \notin X_R$.

If $q \leq p < q^{\pi(q)}$ then $p \notin X_R$ by the condition that $q' \notin X_R$ for all $q' \in \Pi$ with $q \leq q' < q^{\pi(q)}$.

Now, we consider $q^{\pi(q)} \leq p$. Note that, by assumption, $x < q$ and $q > 3$ and so $q^{\pi(q)} > q^{\pi(q)-1} + q$. Also notice that $|\{i \in I; q_i < q\}| < \pi(q) - 1$, since $2 \notin X_R$ and thus $(\prod_{q_i \nmid x; q_i < q} q_i) < (\prod_{q_i < q} q) < q^{\pi(q)-1}$.

Therefore $\mid (x + \prod_{q_i \nmid x; q_i < q} q_i) \mid < q + q^{\pi(q)-1} < q^{\pi(q)}$.

So $p \geq q^{\pi(q)}$ cannot divide $(x + \prod_{q_i \nmid x; q_i < q} q_i)$ since it is too big. Therefore the integer $(x + \prod_{q_i \nmid x; q_i < q} q_i)$ must be a product of primes not contained in X_R and therefore a unit of R. By a similar argument $(x - \prod_{q_i \nmid x; q_i < q} q_i)$ is also a unit of R . □

Example 2.3 *Let $\Pi = \{p_i\}_{i=1,2,\ldots}$ denote the set of rational primes under the natural ordering. Denote by $\tau^1[n]$ $(n \in \mathbb{Z}^+)$ the index of the least prime greater than $p_n^{\pi(p_n)}$, i.e. $p_{\tau^1[n]}$ is the least prime greater than ${p_n}^{\pi(p_n)}$. Furthermore, let $\tau^1[\tau^{(m-1)}[n]] = \tau^m[n]$ for all $1 < m \in \mathbb{N}$.*

Let R be that subring of $\mathbb{Q}$ such that type$(R) = (k_{p_i})_{i<\omega}$ *where*

$$k_{p_i} = \begin{cases} \infty & \text{for } i = 1; \\ 0 & \text{for } 1 < i \leq \tau^1[2]; \\ \infty & \text{for } \tau^1[2] < i \leq \tau^2[2]; \\ \ldots & \ldots \\ 0 & \text{for } \tau^j[2] < i \leq \tau^{j+1}[2],\ 1 < j \text{ even}; \\ \infty & \text{for } \tau^j[2] < i \leq \tau^{j+1}[2],\ 1 < j \text{ odd}; \end{cases}$$

Then, by Lemma 1.4, any rational group, G, with $E_{\mathbb{Z}}(G) \geq R$ has unit sum number 2. This is not a unique example. It may be worthwhile, *in this example, to note that given any $x \in \mathbb{Z}^+$ there is always some $x < y, z \in R$ such that $\mid \{p \in X_R; p < y\} \mid > \mid \{p \in \Pi \setminus X_R; p < y\} \mid$ and $\mid \{p \in \Pi \setminus X_R; p < z\} \mid > \mid \{p \in X_R; p < z\} \mid$.*

Next, rational groups are investigated which have only two symbols ∞ within their reduced type or in other words where $\mid \Pi \setminus X_G \mid = 2$. By Proposition 1.1, it is only necessary to consider rational groups G where a symbol ∞ corresponds to the prime 2 within the reduced type of G since otherwise usn(G)$= \omega$. We begin with a technical lemma.

Lemma 2.4 *Let $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ and let $\frac{a}{b}$, $\frac{c}{d}$ be rational numbers expressed in lowest form. If $\frac{a}{b} + \frac{c}{d}$ is an integer then $b = \pm d$.*

Proof: Let $\frac{a}{b}+\frac{c}{d}= z$ for some $z \in \mathbb{Z}$. If $z = 0$ then $\frac{a}{b}= -\frac{c}{d}$ and, $\frac{a}{b}, \frac{c}{d}$ being in lowest form it follows that $b = \pm d$.

If $z \neq 0$ then $\left(\frac{a}{b} + \frac{c}{d}\right) = \frac{ad+cb}{bd} = z$. In this case we consider the two possibilities $b = \pm 1$, or $b \neq \pm 1$.

If $b = \pm 1$ then $d \mid (ad + c)$. Therefore d divides c but $\frac{c}{d}$ being in lowest form it follows that $d = \pm 1$.

If $b \neq \pm 1$ then $b \mid (ad + cb)$. Therefore b divides ad but $\frac{a}{b}$ being in lowest form it follows that b divides d. Of course, by symmetry $d = \pm 1$ only if $b = \pm 1$. Therefore $d \neq \pm 1$ and must divide $(ad + cb)$. Therefore d

divides cb but $\frac{c}{d}$ being in lowest form it follows that d divides b. So b divides d and d divides b so $b = \pm d$. $\square$

Corollary 2.5 *Let $k, l, m, n \in \mathbb{Z}$. Moreover let z be an integer and let $p \neq 2$ be a rational prime such that $z = \pm(2^k p^l \pm 2^m p^n)$. If $k < 0$(or $m < 0$) then $k = m$. If $l < 0$(or $n < 0$) then $l = n$.*

Proof: The proof follows directly from Lemma 2.4. $\square$

The following proposition provides a framework for the discussion of the 2–sum property for all rational groups with only two symbols infinity in their reduced type, one of which corresponds to the rational prime 2.

Proposition 2.6 *Let $p \in \Pi \backslash \{2\}$ and let G be a rational group with $E_{\mathbb{Z}}(G) = R$, where R is that subring of $\mathbb{Q}$ generated by $\frac{1}{2}$ and $\frac{1}{p}$. Then* $\operatorname{usn}(G) = 2$ *if and only if every positive integer z with $(z, 2) = 1 = (z, p)$ can be expressed in one of the following forms:*

(1) $z = \pm(2^k \pm p^l)$ *for some* $k > 0,\ l > 0$.

(2) $z = 2^k p^l \pm 1$ *for some* $k > 0,\ l \geq 0$.

(3) $z = \frac{1}{p^l}(2^k \pm 1)$ *for some* $k > 0,\ l > 0$.

(4) $z = \frac{1}{2^k}(p^l \pm 1)$ *for some* $k > 0,\ l > 0$.

where $k, l \in \mathbb{Z}$.

Proof: In the first direction we assume that usn(G)= 2 and so usn(R)= 2. Every unit of R is of the form $\pm 2^a p^b$ where $a, b \in \mathbb{Z}$. Let z be a positive integer greater than 1 and relatively prime to both 2 and p. Let $z = \pm(2^a p^b \pm 2^c p^d)$ be a sum of two units for z, where $a, b, c, d \in \mathbb{Z}$. Notice that a, b, c, d cannot all be less than or equal to zero since z cannot take the values $\pm 1, \pm 2$, or 0.

By Corollary 2.5 if $a < 0$ then $c = a$ and since z is relatively prime to 2 then if either a or c is greater than 0 then the other must be zero, i.e. if $a > 0$ then $c = 0$. Similarly if $b < 0$ then $d = b$ and since z is relatively prime to p then if either b or d is greater than 0 then the other must be zero, i.e. if $b > 0$ then $d = 0$. In light of this we consider the possible expressions of z as a sum of two units:

If $a > 0$ (forcing $c = 0$) and $d > 0$ (forcing $c = 0$) then $z = \pm(2^a \pm p^d)$. This is of form (1). Similarly, form (1) occurs for $c > 0$ and $b > 0$.

If $a > 0$ (forcing $c = 0$) and $b > 0$ (forcing $d = 0$) then $z = 2^a p^b \pm 1$. Note that only one ± sign occurs in this equation and it must accompany the 1, otherwise a negative integer would result. This equation is of form (2). Similarly form (2) occurs for $c > 0$ and $d > 0$.

If $a = c < 0$ then $b > 0$ and $d = 0$, or $b = 0$ and $d > 0$ resulting in $z = \frac{1}{2^{-a}}(p^b \pm 1)$ or $z = \frac{1}{2^{-a}}(p^d \pm 1)$. Notice, there is only one $\pm$ sign in each equation and it must precede the 1 otherwise a negative integer would result. These equations are of form (4).

If $b = d < 0$ then $a > 0$ and $c = 0$, or $a = 0$ and $c > 0$ resulting in $z = \frac{1}{p^{-b}}(2^a \pm 1)$ or $z = \frac{1}{p^{-b}}(2^c \pm 1)$. Again the only $\pm$ sign accompanies the 1 or a negative integer results. These equations are of form (3).

If $b = d = 0$ then $a > 0$ and $c = 0$, or $a = 0$ and $c > 0$ resulting in $z = 2^a \pm 1$ or $z = 2^c \pm 1$. These equations are of form (2). Since z must be an odd integer both a and c cannot both be zero, i.e. 2 divides $p^b \pm p^d$ for $b, d \geq 0$. We have covered all possible cases.

To prove the other direction let x be a positive integer. We can write $x = 2^a p^b(z)$ with $a, b \in \mathbb{Z}$ where $(z, 2) = 1 = (z, p)$ or $z = 1$. If z $(\neq 1)$ can be expressed in one of the forms (1),(2),(3) or (4) then, also $1 = \frac{1}{2} + \frac{1}{2}$. Therefore every positive integer can be expressed as a sum of two units. Then by Lemma 1.3 usn(G)= 2. □

It is convenient for our purposes to consider the primes modulo 24. Excluding 2 and 3 the primes fall into eight classes modulo 24, these being 1, 5, 7, 11, 13, 17, 19 and 23 mod 24. By Dirichlet's famous theorem (see

I, Theorem 2.21) for primes in an arithmetic progression, we know that in each of these classes there is an infinite number of primes.

Definition 2.7 *Define* $P^* = \{p \in \Pi \mid p \equiv 1, 5, 11, 13, 19$ *or* $23 \bmod 24\}$.

Proposition 2.8 *Let* $P^*_{25} = P^* \backslash \{5, 13, 23, 29, 101\}$ *and* $p \in P^*_{25}$. *Let* R *be that subring of* $\mathbb{Q}$ *generated by* $\frac{1}{2}$ *and* $\frac{1}{p}$. *Then* $\mathrm{usn}(R) > 2$.

Proof: We will show that 25 cannot be expressed as a sum of two units in R and therefore usn(R)> 2. Since $(25, p) = 1$ for all $p \in P^*_{25}$, and $(25, 2) = 1$, then by Proposition 2.6 a sum of two units for 25 in R must be of form (1),(2),(3) or (4). In the following we consider the possible forms separately.

Form (1): We tabulate modulo 24 values of $\pm 2^k \pm p^l$ for $k, l > 0$ and for all possible values of p in P^*.

$\pm p^l$ mod 24

$\pm 2^k$ mod 24

+	1	5	11	13	19	23
2	3	7	13	15	21	1
4	5	9	15	17	23	3
8	9	13	19	21	3	7
16	17	21	3	5	11	15
-4	21	1	7	9	15	19
-2	23	3	9	11	17	21

Table: $\pm 2^k \pm p^l$ mod 24; $k, l > 0$, $p \in P^*$.

On this table 1 mod 24 occurs only for $\pm 2^k \equiv 2$ or -4 mod 24, which correspond to $\pm 2^k = 2$ or -4. However, $25 = 2 \pm p^l$ implies that $p = 23$, which is not contained in P^*_{25}; and $25 = -4 \pm p^l$ implies $p = 29$, which is not contained in P^*_{25}. Therefore 25 does not occur in R as form (1).

Form (2): This time we tabulate values of $2^k p^l$ modulo 24 for $k > 0$, $l \geq 0$ and for all values of p in P^*.

		p^l mod 24					
	×	1	5	11	13	19	23
$\pm 2^k$ mod 24	2	2	10	22	2	14	22
	4	4	20	20	4	4	20
	8	8	16	16	8	8	16
	16	16	8	8	16	16	8

Table: 2^kp^l mod 24; $k > 0$, $l \geq 0$, $p \in P^*$.

From this table we deduce that $2^kp^l \pm 1$ with $k > 0$ and $l \geq 0$ can only be congruent to 1 mod 24 for $k = 1$ (i.e. see values resulting in 0 or 2 in the table above). However $25 = 2p^l \pm 1$ implies $p = 13$ which is not contained in P^*_{25}. Therefore 25 does not occur in R as form (2).

Form (3): The set of congruences modulo 24 for $25p^l$ with $l > 0$ and $p \in P^*$ is $\{1, 5, 11, 13, 19, 23\}$. The set of congruences modulo 24 for $2^k \pm 1$ with $k > 0$ is $\{1, 3, 5, 7, 9, 15, 17\}$. Values common to both sets are 1 and 5 mod 24; these correspond to $k = 1$ and $k = 2$. Since $25 > 2^k \pm 1$ for $k = 1$ or 2, then 25 cannot be expressed as form (3) in R.

Form (4): The set of congruences modulo 24 for $25(2^k)$ with $k > 0$ is $\{2, 4, 8, 16\}$. The set of congruences modulo 24 for $p^l \pm 1$ with $l > 0$ and

$p \in P^*$ is $\{0, 2, 4, 6, 10, 12, 14, 18, 20, 22\}$. Only the congruences 2 and 4 mod 24 occur in both sets. These correspond to $k = 1$ or 2. For $k = 1$ we get $2(25) = p^l \pm 1$ giving $p^l = 49$ or 51 both of which are impossible for $p \in P^*$. For $k = 2$ we get $4(25) = p^l \pm 1$ giving $p^l = 99$ or 101, neither of which is possible for $p \in P^*_{25}$. Therefore 25 cannot be expressed in form (4) in R. □

Proposition 2.9 *Let* $P^*_{73} = P^* \backslash \{37, 71, 293\}$. *Let* $p \in P^*_{73}$. *Let* R *be that subring of* $\mathbb{Q}$ *generated by* $\frac{1}{2}$ *and* $\frac{1}{p}$. *Then* $\mathrm{usn}(R) > 2$.

Proof: We will show that 73 has no two unit sum in R. The proof follows Proposition 2.8 exactly, so we summarise as follows:

Form (1): Let $73 = 2 \pm p^l$ with $l > 0$ and $p \in P^*$. This implies $p = 71$ which is not contained in P^*_{73}.

Let $73 = -4 \pm p^l$ with $l > 0$ and $p \in P^*$. This implies that $77 = p^l$ which is impossible for $p \in P^*$. Therefore 73 cannot be of form (1) in R.

Form (2): Let $73 = 2p^l \pm 1$ with $l > 0$ and $p \in P^*$. This implies $p = 37$ which is not contained in P^*_{73}. Therefore 73 is not of form (2) in R.

Form (3): As in Proposition 2.8.

Form (4): $2(73) = p^l \pm 1$ with $l > 0$ is impossible for $p \in P^*$. Let $4(73) = p^l \pm 1$ with $l > 0$ and $p \in P*$. This implies that $p = 293$ which is not contained in P_{73}^{*}. Therefore 73 is not of form (4) in R. □

Corollary 2.10 *Let $p \in P^{*}$. Let R be that subring of $\mathbb{Q}$ generated by $\frac{1}{2}$ and $\frac{1}{p}$. Let G be a rational group such that $E_{G} = R$. Then* $\operatorname{usn}(G) > 2$.

Proof: Recall from Propositions 2.8 and 2.9 that $P_{25}^{*} = P^{*} \backslash \{5, 13, 23, 29, 101\}$ and $P_{73}^{*} = P^{*} \setminus \{37, 71, 293\}$. Therefore $P^{*} = P_{25}^{*} \cup P_{73}^{*}$. The proof then follows directly from the two propositions. □

Proposition 2.11 *Let $p \in \Pi$ such that $p \equiv 7 \bmod 24$. Let R be that subring of $\mathbb{Q}$ generated by $\frac{1}{2}$ and $\frac{1}{p}$. Then* $\operatorname{usn}(R) > 2$.

Proof: $(p^2 + p + 3) > 1$ is a positive integer relatively prime to p and 2. We will show that $(p^2 + p + 3)$ cannot be expressed in any of forms (1),(2),(3) or (4) and so, by Proposition 2.6, is not a sum of two units of R and therefore $\operatorname{usn}(R) > 2$.

Note that $(p^2 + p + 3) \equiv 11 \bmod 24$.

Form (1): We tabulate values for $\pm(2^k \pm p^l)$ modulo 24, $k, l > 0$.

$\pm p^l$ mod 24

$\pm 2^k$ mod 24

+	1	7	-1	-7
2	3	9	1	19
4	5	**11**	3	21
8	9	15	7	1
16	17	23	15	9
-4	21	3	19	13
-2	23	5	21	15

Table: $\pm(2^k \pm p^l)$ mod 24; $k, l > 0$.

The value 11 occurs only once on this table and as 11 mod 24 $\equiv 4 + p^l$ with $l > 0$. However $p^2+p+3 \neq 4+p^l$ for any $l > 0$. Therefore (p^2+p+3) is not of form (1), i.e. $p^2 + p + 3 \neq \pm(2^k \pm p^l)$ for any $k, l > 0$.

Form(2) and form(3): We consider these two forms together.

The set of possible congruences modulo 24 for $(2^k p^l \pm 1)$, $k > 0$, $l \geq 0$, is $\{1, 3, 5, 7, 9, 13, 15, 17\}$.

The set of possible congruences modulo 24 for $p^m(p^2+p+3)$, $m(\in \mathbb{Z}) \geq 0$, is $\{11, 5\}$.

The only common entry in both sets is 5 mod 24. In the first set, for

$l = 0$, this corresponds to $k = 2$ and so $(2^2p^0 \pm 1) = 2^2 + 1 = 5$ and since $p^m(p^2+p+3) > 5$ for all $p \in \Pi$ with $p \equiv 7 \bmod 24$ then $p^m(p^2+p+3) \neq 2^k \pm 1$ for any $m \geq 0, k > 0$. We are finished for form (3). In the second set the value 5 mod 24 corresponds to m odd and so $m > 0$. Therefore we are finished for form (2).

Form (4): We assume that

$$2^k(p^2+p+3) = p^l \pm 1 \quad \text{for some } k, l > 0 \tag{2}$$

Possible congruences modulo 24 for $2^k(p^2+p+3)$ are $\{22, 20, 16, 8\}$.

Possible congruences modulo 24 for $(p^l \pm 1)$ are $\{0, 2, 6, 8\}$.

The only common value is 8 mod 24 corresponding to $k > 3$ (even), and l odd. This restricts equation (2) to

$$2^k(p^2+p+3) = p^l + 1 \quad , k(\text{even}) > 3,\ l(\text{odd}) > 0 \qquad (2)^+$$

Recall, we are considering $p \equiv 7 \bmod 24$. We may also write this as $p = 8\lambda - 1$, for some $\lambda \in \mathbb{N}$.

First consider $\lambda = 1$, i.e. $p = 7$. The set of possible congruences modulo 48 for $2^k(7^2+7+3)$, $k > 3$ (even), is $\{32\}$. The set of possible congruences modulo 48 for $7^l + 1$, $l > 0$ (odd) is $\{8\}$. Therefore $p = 7$ does not satisfy equations $(2)^+$ or (2).

Next consider equation $(2)^+$ modulo λ to get

$$2^k3 \equiv 0 \bmod \lambda \quad \text{for } (k > 3).$$

This implies that λ divides 2^k3. To satisfy this we must have $\lambda = 3$ or 2^r $(0 < r \leq k)$ or 2^r3 $(0 < r \leq k)$. However, $\lambda = 3$ or 2^r3 are not consistent with $p \equiv 7 \bmod 24$; since $\lambda = 3$ it follows that $p = 23$ and $\lambda = 2^r3$ implies $p = 2^{r+3}3 - 1 \equiv 23 \bmod 24$.

We are left to consider $\lambda = 2^r$ $(0 < r \leq k)$, in which case $p = 2^r8 - 1 = 2^{r+3} - 1$. This time consider equation $(2)^+$ modulo p to get

$$2^k3 \equiv 1 \bmod p \quad (k > 3).$$

This implies that "3 mod p" is a multiplicative inverse of "2^k mod p" for some $k > 3$. However, for $p = 2^{r+3} - 1$, the multiplicative group generated by "2 mod p" is $\{2, 4, \ldots, 2^r, 2^{r+1}, 2^{r+2}, 1 \bmod p\}$. Therefore in this case "3 mod p" is not a multiplicative inverse of (2^k mod p) for any $k > 3$. Therefore

$$2^k(p^2 + p + 3) \neq p^l \pm 1 \quad \text{for any } k > 0,\ l > 0$$

and thus the proof is finished. □

Proposition 2.12 *Let $p \in \Pi$ such that $p \equiv 17 \bmod 24$. Moreover let R be the subring of $\mathbb{Q}$ generated by $\frac{1}{2}$ and $\frac{1}{p}$. Then* $\operatorname{usn}(R) > 2$.

Proof: We will show that $2p + 3$ is not a sum of two units in R, and therefore it follows that usn(R)> 2. Since $(2p+3)$ is a positive integer relatively prime to p and 2 and is greater than 1, then, by showing that $(2p+3)$ cannot be expressed in form (1),(2),(3) or (4), it follows by Proposition 2.6 that usn$(R) > 2$.

Note that $(2p+3) \equiv 13 \bmod 24$.

Form (1): We tabulate values for $\pm(2^k \pm p^l)$ modulo 24, $k, l > 0$.

$\pm p^l$ mod 24

	+	1	17	-1	-17
$\pm 2^k$ mod 24	2	3	19	1	9
	4	5	21	3	11
	8	9	1	7	15
	16	17	9	15	23
	-4	21	**13**	19	3
	-2	23	15	21	5

Table: $\pm(2^k \pm p^l)$ mod 24; $k, l > 0$.

From this table it can be seen that 13 mod 24 occurs only for $\pm 2^k \equiv -4 \bmod 24$, which corresponds to $\pm 2^k = -4$. However $2p+3 \neq -4+p^l$ for any $l > 0$, therefore $2p+3$ does not occur as form (1) in R.

Form(2) and form(3): We consider these two forms together.

The set of possible congruences modulo 24 for $(2^k p^l \pm 1)$, $k > 0$, $l \geq 0$ is $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21\}$.

The set of possible congruences modulo 24 for $p^m(2p+3)$, $m(\in \mathbb{Z}) \geq 0$, is $\{13, 5\}$.

In the first set, for $l = 0$, this corresponds to $k = 2$ so that$(2^2 p^0 + 1) = 5$ and since $p^m(2p+3) > 5$ for all $p \in \Pi$ and $m \geq 0$ then we are finished for form (3). In the second set the value 5 mod 24 corresponds to m odd and so non–zero. Therefore we are finished for form (2).

Form (4): Seeking a contradiction let us assume

$$2^k(2p+3) = p^l \pm 1 \quad \text{for some } k, l > 0 \tag{4}$$

Simple rearrangement gives

$$p^l - 2^{k+1}p = 3.2^k \pm 1 \quad \text{for some } k, l > 0 \tag{5}$$

Since p cannot divide $3.2^k \pm 1$ for $k \leq 3$, we restrict our attention to $k > 3$. The set of possible congruences modulo 24 for $2^k(2p+3)$ with $k > 3$ is $\{8, 16\}$. The set of congruences modulo 24 for $p^l \pm 1$ with $l > 0$ is $\{0, 2, 16, 18\}$. The only common entry in each set is 16 mod 24. This value corresponds to $p^l - 1$ where l is odd, so equation (4) is constrained to

$$2^k(2p+3) = p^l - 1 \quad \text{for some } k > 3, l(odd) > 0 \tag*{$(4)^+$}$$

Since $p = 8\lambda + 1$ for some $\lambda \in \mathbb{Z}^+ \backslash \{1\}$, we consider equation $(4)^+$ modulo λ giving

$$2^k 5 \equiv 0 \bmod \lambda$$

This is only possible if λ divides $2^k.5$. Therefore we consider (i)$\lambda = 5$, (ii)$\lambda = 2^r$ $(0 < r \leq k)$, (iii)$\lambda = 2^r.5$ $(0 < r \leq k)$.

Again refering to equation $(4)^+$ but this time modulo p, we get

$$2^k 3 \equiv -1 \bmod p, \quad (k > 3).$$

Therefore, "$-3 \bmod p$" is the multiplicative inverse of "$2^k \bmod p$" for some $k > 3$.

In case (i) where $p = 8.5 + 1 = 41$ the multiplicative group generated by "2 mod 41" is $\{2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1\}$.

In case (ii) where $p = 8.2^r + 1 = 2^{r+3} + 1$ with $0 < r \leq k$, $k > 3$, the multiplicative group generated by "2 mod p" is $\{2, 4, 8, \ldots, 2^r, 2^{r+1}, 2^{r+2}, 2^{r+3}, -2, -4, \ldots, -2^r, -2^{r+1}, -2^{r+2}, 1\}$.

In neither case (i) nor (ii) is "$-3 \bmod p$" a multiplicative inverse of 2^k for any $k > 3$, so we are left with only case (iii) to consider.

In case (iii) $p = 8.5.2^r + 1 = 5.2^{r+3} + 1$ with $0 < r \leq k$. In this light we consider equation $(4)^+$ modulo 2^{r+3} giving

$$2^k 5 \equiv 0 \bmod 2^{r+3} \quad (k > 3).$$

This implies that $k \geq r+3$. However $k \neq r+3$ since $p = 5.2^{r+3}+1$ cannot divide $3.2^{r+3} \pm 1$, a necessary condition noted after equation (5). So consider

$$2^k(2p+3) = p^l - 1, \quad k > r+3,\ l > 0 \text{ (odd)},\ p = 5.2^{r+3}+1 \qquad (4)^{++}$$

Rewriting this as

$$2^k(2(5.2^{r+3}+1)+3) = (5.2^{r+3}+1)^l - 1 \quad k > r+3,\ l > 0 \text{ (odd)}$$

and then expanding the bracketted term on the right binomially we get

$$2^k(2(5.2^{r+3}+1)+3) = (5.2^{r+3})^l + \ldots + l(5.2^{r+3}) + 1 - 1$$

$$\text{with } k > r+3,\ l(odd) > 0.$$

However this is impossible since modulo 2^{r+4} we get $5l2^{r+3} \equiv 0 \bmod 2^{r+4}$ contradicting l odd. Therefore we are finished for form (4). □

Finally we are left to consider the case for the rational prime 3.

Proposition 2.13 *Let R be that subring of $\mathbb{Q}$ generated by $\frac{1}{2}$ and $\frac{1}{3}$. Then* $\operatorname{usn}(R) > 2$.

Proof: Since 401 is relatively prime to both 2 and 3, by Proposition 2.6, if 401 is shown not to be expressible in any of forms (1), (2), (3) or (4), then $\operatorname{usn}(R) > 2$.

Form (1): That $401 \neq 2^k + 3^l$, for any $k, l \geq 0$ is obvious by merely substituting $3^l = 3, 9, 27, 81, 243$ in the expression. Therefore in the following table we list only values for $\pm(2^k - 3^l)$ with $k, l > 0$ and we do so modulo 48.

$\pm 3^l$ mod 48

	+	3	9	27	33	-3	-9	-27	-33
	2					47	41	23	**17**
	4					1	43	25	19
	8					5	47	29	23
	16					13	7	37	31
	32					29	23	5	47
$\pm 2^k$ mod 48	-2	1	7	25	31				
	-4	47	5	23	29				
	-8	43	1	19	25				
	-16	35	41	11	**17**				
	-32	19	25	43	1				

Table: $\pm(2^k - 3^l)$ mod 48; $k, l > 0$.

Note that $401 \equiv 17$ mod 48 and this value is only listed twice on the table above. It occurs firstly as $2 - 3^l \equiv 17$ mod 48. However, $401 \neq 2 - 3^l$ for any $l > 0$. Secondly, it occurs as $2^k - 3^l \equiv 17$ mod 48, where $k > 3$ and $3^l \equiv 33$ mod 48. Observe that $3^l \equiv 33$ mod 48 is only possible when 4 divides l. To finish for form (1) we consider this modulo 80. The set of congruences for 2^k mod 80 with $k > 3$ is $\{16, 32, 64, 48\}$. When 4 divides $l > 0$ then $3^l \equiv 1$ mod 80. Therefore 401 which is congruent to 1 mod 80 cannot equal $2^k - 3^l$ for any $k > 3$, $l > 0$, l divisible by 4.

Form (2): It is easily checked that $401 \neq 2^k 3^l \pm 1$ for any $k > 0$, $l \geq 0$.

Form (3): The set of congruences modulo 80 for $3^l \cdot 401$ with $l > 0$ is $\{3, 9, 27, 1\}$. The set of congruences modulo 80 for $2^k \pm 1$ with $k > 3$ is $\{15, 17, 31, 33, 63, 65, 47, 49\}$. There are no common values between these sets and certainly $3^l.401 > 2^k \pm 1$ for any $k \leq 3$. Therefore we are finished for form (3).

Form (4): The set of congruences modulo 80 for $2^k.401$ with $k > 0$ is $\{2, 4, 8, 16, 32, 64, 48\}$. The set of congruences modulo 80 for $3^l \pm 1$ with $l > 0$ is $\{2, 4, 8, 10, 26, 28, 0\}$. The only common values for these two sets are $2, 4, 8$ mod 80 which correspond to $k = 1, 2$ and 3, respectively. However, it is easily checked that $2 \cdot 401$, $2^2 \cdot 401$ and $2^3 \cdot 401$ do not equal $3^l \pm 1$ for any $l > 0$. □

We now summarise the above results to obtain:

Theorem 2.14 *Let $p \in \Pi \backslash \{2\}$. Let G be a rational group such that $E_{+}(G)$ is that subring of $\mathbb{Q}$ generated by $\frac{1}{2}$ and $\frac{1}{p}$. Then* $\mathrm{usn}(G) > 2$.

Proof: Since 3 is the only prime p with $p \equiv 3 \bmod 24$, we have that $\Pi \setminus \{2\} = P^{*} \cup \{p \in \Pi | p \equiv 7 \bmod 24\} \cup \{p \in \Pi | p \equiv 17 \bmod 24\} \cup \{3\}$. Then the proof follows as a corollary to Propositions 2.11, 2.12, 2.13 and Corollary 2.10. □

We now extend Proposition 2.6 to rational groups G in which arbitrary numbers of primes have entries ∞ in any characteristic representing type(G).

Proposition 2.15 *Let* $\{2\} \subsetneq \mathcal{P} \subsetneq \Pi$. *Let G be a rational group such that $E_{\mathbb{Z}}(G)$ is that subring of $\mathbb{Q}$ generated by* $\{\frac{1}{p} | \, p \in \mathcal{P}\}$. *Then* $\mathrm{usn}(G) = 2$ *if and only if every positive integer z with* $(z, p) = 1$ *for all* $p \in \mathcal{P}$ *can be expressed in one of the following forms:*

(a) $z = \dfrac{1}{2^m B}(C \pm D)$

(b) $z = \pm\dfrac{1}{B}(2^m C \pm D)$

where $m \in \mathbb{Z}^+$ *and* B, C, D *are products of elements of* $\mathcal{P} \setminus \{2\}$ *such that* $(B, C) = 1 = (C, D) = (B, D)$.

Proof: Let $R = E_{\mathbb{Z}}(G)$. Let us assume that every positive integer z, such that z is relatively prime to every prime integer in $\mathcal{P}$, is expressible in form (a) or (b).

All other positive integers are either units of R, i.e. products of elements of $\mathcal{P}$ and 1, or else products of elements of $\mathcal{P}$ by a product of rational primes relatively prime to $\mathcal{P}$. In the case of a positive integer being a unit we can always express it as a sum of two integers since 2 is also a unit. In the case of a positive integer relatively prime to $\mathcal{P}$, this can, by assumption, be expressed in form (a) or (b), which are sums of two units of R. Finally, any integer which is not a unit yet not relatively prime to $\mathcal{P}$ can always be expressed as unit$\cdot$(unit+unit), using the previous case. Therefore, by Lemma 1.3, usn(R)= 2 =usn(G).

Conversely, let us assume that usn(G)= 2 and so also usn(R)= 2 . Let z be an arbitrary positive integer such that z is relatively prime to $\mathcal{P}$. We can write z as a sum of two units as

$$z = \prod_{p\in\mathcal{P}} p^{l_p} \pm \prod_{p\in\mathcal{P}} p^{k_p} \quad (l_p, k_p \in \mathbb{Z}) \tag{7}$$

We will make some remarks regarding equation (7). Firstly, from Lemma 2.4 we know that $\prod_{\substack{p\in\mathcal{P}\\ l_p<0}} p^{l_p} = \prod_{\substack{p\in\mathcal{P}\\ k_p<0}} p^{k_p}$. So equation (7) may be rewritten as

$$z = \prod_{\substack{p\in\mathcal{P}\\ l_p<0,\in\mathbb{Z}}} p^{l_p}\Big(\prod_{\substack{p\in\mathcal{P}\\ l_p\geq 0,\in\mathbb{Z}}} p^{l_p} \pm \prod_{\substack{p\in\mathcal{P}\\ k_p\geq 0,\in\mathbb{Z}}} p^{k_p}\Big) \tag{8}$$

Secondly, since z is relatively prime to $\mathcal{P}$ then $l_p > 0$ implies $k_p = 0$ and vice versa. Also, both l_2 and k_2, cannot be zero or else the bracketted term in equation (8) will be an even integer which is not possible for z relatively prime to 2.

As a consequence of these remarks we rewrite equation (8) as

$$z = \pm \frac{1}{2^{m_1} B}(2^{m_2} C \pm D) \tag{9}$$

where $B = \prod_{\substack{p \in \mathcal{P}\setminus\{2\} \\ l_p < 0}} p^{-l_p}$, $C = \prod_{\substack{p \in \mathcal{P}\setminus\{2\} \\ l_p \geq 0}} p^{l_p}$, $D = \prod_{\substack{p \in \mathcal{P}\setminus\{2\} \\ k_p \geq 0}} p^{k_p}$,
and where $(B, C) = 1 = (C, D) = (B, D)$, and m_1 or $m_2 = 0$ but not both. The ± sign is unnecessary in form (b) since z is a positive integer and we can always choose C to be the greater product.

Finally, equation (9) is of form (a) when $m_2 = 0$ and is of form (b) when $m_1 = 0$. □

Corollary 2.16 *Let G be a rational group such that $E_{\mathbb{Z}}(G)$ is that subring of $\mathbb{Q}$ generated by $\{\frac{1}{2}\} \cup \{\frac{1}{p} \mid p \in \Pi,\ p \equiv 1 \bmod 24\}$.*

Then $\operatorname{usn}(G) > 2$.

Proof: Consider the set $\mathcal{P} = \{2\} \cup \{p \in \Pi \mid p \equiv 1 \bmod 24\}$ and let $z = 11$. We show that z is not of either form (a) or (b) corresponding to Proposition 2.15. Then z is not of the form (a) since:

$$(C \pm D) \equiv 0 \text{ or } 2 \bmod 24 \qquad \text{and}$$

$$2^m \cdot 11B \equiv 22,\ 20,\ 16 \text{ or } 8 \bmod 24.$$

Moreover, z is not of form (b) either, since:

$$11B \equiv 11 \bmod 24 \quad \text{and}$$

$$\pm(2^m C \pm D) \equiv \pm 1,\ \pm 3,\ \pm 5,\ \pm 7,\ \pm 9,\ \pm 15 \quad \text{or} \quad \pm 17 \bmod 24.$$

Therefore, by Proposition 2.15, usn(R)$\neq$ 2. □

By Dirichlet's Theorem (see I, Theorem 2.21), $\{p \in \Pi \mid p \equiv 1 \bmod 24\}$ is infinitely countable. So R, as defined in the corollary above, is a first example of a subring of $\mathbb{Q}$ where $\Pi \setminus X_R$ is infinitely countable and yet usn(R) $\neq$ 2. This ring becomes of further significance in the next section of this chapter.

§3 Approach via additive number theory

A different line of approach is followed now adapting some results from additive number theory to get some interesting outcomes. First, some definitions are necessary.

Definitions 3.1 *Let A be a set of integers, $x \in \mathbb{Z}$, and $h \in \mathbb{N}$.*

(i) *The* Counting Function *of the set A, defined for $x \in \mathbb{Z}$, is the number of positive elements of A not exceeding x, written $A(x)$,*

$$A(x) = \sum_{\substack{a \in A \\ 1 \leq a \leq x}} 1.$$

(ii) *The* Shnirel'man Density *of the set A, denoted $\sigma(A)$, is*

$\sigma(A) = \inf_{n=1,2,\ldots}\left(\frac{A(n)}{n}\right)$

(iii) *The set A is a* basis of order h *if every non–negative integer can be expressed as a sum of exactly h elements of A.*

We include here some results which will be used later.

Lemma 3.2 *Let x be a positive integer greater than 2. Let $r(N)$ denote the number of representations of the integer N as the sum of two primes. Then* $\sum_{N\leq x} r(N) \geq c_1\frac{x^2}{(\ln x)^2}$, *for some positive constant c_1 .*

Proof: See [18, Lemma 7.6]. □

Lemma 3.3 *Let x be a positive integer greater than 2. Let $r(N)$ denote the number of representations of the integer N as the sum of two primes. Then* $\sum_{N\leq x} (r(N))^2 \leq c_2\frac{x^3}{(\ln x)^4}$, *for some positive constant c_2 .*

Proof: See [18, Lemma 7.7]. □

Let A and B be arbitrary sets of integers. We denote by $A + B$ the set $\{a+b \ \mid a \in A, b \in B\}$.

Lemma 3.4 *Let A and B be sets of integers such that $0 \in A$, $0 \in B$. If $n \in \mathbb{N}$ and $A(n) + B(n) \geq n$, then $n \in A + B$.*

Proof: If $n \in A$, then $n = n + 0 \in A + B$. Similarly if $n \in B$ then $n \in A + B$.

Suppose $n \notin A \cap B$. Define sets A' and B' as $A' = \{n - a : a \in A, 1 \leq a \leq n - 1\}$ and $B' = \{b : b \in B, 1 \leq b \leq n - 1\}$.

Then $|A'| = A(n)$ since $n \notin A$, and $|B'| = B(n)$ since $n \notin B$. Furthermore $A' \cup B' \subseteq \{1, \ldots, n - 1\}$.

Then since $|A'| + |B'| = A(n) + B(n) \geq n$ it follows that $A' \cap B' \neq \emptyset$. Therefore $n - a = b$ for some $a \in A$ and some $b \in B$, and so $n = a + b \in A + B$. □

Lemma 3.5 *Let A and B be sets of integers such that $0 \in A$, $0 \in B$. If $\sigma(A) + \sigma(B) \geq 1$, then $n \in A + B$ for each $n \in \mathbb{N}$.*

Proof: Let $\sigma(A) = \alpha$ and $\sigma(B) = \beta$. Take any arbitrary $n \in \mathbb{N}$, then $A(n) + B(n) \geq (\alpha + \beta)n \geq n$. Therefore, by Lemma 3.4, $n \in A + B$. □

Corollary 3.6 *Let a be a set of integers such that $0 \in A$ and $\sigma(A) \geq \frac{1}{2}$. Then A is a basis of order 2.*

Proof: This follows directly from Lemma 3.5 with $A = B$. □

The next Theorem is due to Shnirel'man; we include the proof.

Theorem 3.7 (*Shnirel'man*) *Let A and B be sets of integers such that $0 \in A$, $0 \in B$. Let $\sigma(A) = \alpha$ and $\sigma(B) = \beta$. Then*

$$\sigma(A+B) \geq \alpha + \beta - \alpha\beta.$$

or, equivalently,

$$1 - \sigma(A+B) \leq (1-\alpha)(1-\beta).$$

Proof: Let $n \geq 1$. Let $a_0 = 0$ and let $1 \leq a_1 < \ldots < a_k \leq n$ be the $k = A(n)$ positive elements of A that do not exceed n. Since $0 \in B$ it follows that $a_i = a_i + 0 \in A + B$ for all $i \in 1, \ldots, k$.

For $i = 0, \ldots, k-1$, let $1 \leq b_1 < \ldots < b_{r_i} \leq a_{i+1} - a_i - 1$ be the $r_i = B(a_{i+1} - a_i - 1)$ positive elements of B less than $a_{i+1} - a_i$.

Then $$a_i < a_i + b_1 < \ldots < a_i + b_{r_i} < a_{i+1}$$

and $a_i + b_j \in A + B$ for $j = 1, \ldots, r_i$.

Now, let $1 \leq b_1 < \ldots < b_{r_k} \leq n - a_k$ be the $r_k = B(n - a_k)$ positive elements of B not exceeding $n - a_k$.

Then $$a_k < a_k + b_1 < \ldots < a_k + b_{r_k} \leq n$$

and $a_k + b_j \in A + B$ for $j = 1, \ldots, r_k$.

It follows that

$$\begin{aligned}
(A+B)(n) &\geq A(n) + \sum_{i=0}^{k-1} B(a_{i+1} - a_i - 1) + B(n - a_k) \\
&\geq A(n) + \beta \sum_{i=0}^{k-1} (a_{i+1} - a_i - 1) + \beta(n - a_k) \\
&= A(n) + \beta \sum_{i=0}^{k-1} (a_{i+1} - a_i) + \beta(n - a_k) - \beta k \\
&= A(n) + \beta n - \beta k \\
&= A(n) + \beta n - \beta A(n) \\
&= (1 - \beta)A(n) + \beta n \\
&\geq (1 - \beta)\alpha n + \beta n \\
&= (\alpha + \beta - \alpha\beta)n,
\end{aligned}$$

and so

$$\frac{(A+B)(n)}{n} \geq \alpha + \beta - \alpha\beta.$$

Therefore

$$\sigma(A + B) = \inf_{n=1,2,\ldots} \frac{(A+B)(n)}{n} \geq \alpha + \beta - \alpha\beta$$

This completes the proof. □

Theorem 3.8 *Let $h \geq 1$, and let $A_1, \ldots, A_h$ be sets of integers such that $0 \in A_i$ for $i \in 1, \ldots, h$. Then*

$$1 - \sigma(A_1 + \ldots + A_h) \leq \prod_{i=1}^{h} (1 - \sigma(A_i)).$$

Proof: The proof is by induction on h. Let $\sigma(A_i) = \alpha_i$ for $i = 1, \ldots, h$. For $h = 1$ there is nothing to prove. For $h = 2$, by Theorem 3.7, our inequality is true.

Let $k \geq 3$, and assume the theorem holds for all $h < k$. Let $B = A_1 + \ldots + A_{k-1}$. It follows from the induction hypothesis that

$$1 - \sigma(B) = 1 - \sigma(A_1 + \ldots + A_{k-1}) \leq \prod_{i=1}^{k-1} (1 - \sigma(A_i)) \quad ,$$

and so

$$\begin{aligned} 1 - \sigma(A_1 + \ldots + A_k) &= 1 - \sigma(B + A_k) \\ &\leq (1 - \sigma(B))(1 - \sigma(A_k)) \quad \text{(by Theorem 3.7)} \\ &\leq (1 - \sigma(A_k)) \prod_{i=1}^{k-1} (1 - \sigma(A_i)) \\ &= \prod_{i=1}^{k} (1 - \sigma(A_i)). \end{aligned}$$

This completes the proof. □

The following theorem due to Shnirel'man is fundamental to our line of approach.

Theorem 3.9 (*Shnirel'man*)

Let A be a set of integers such that $0 \in A$ and $\sigma(A) = \alpha > 0$.

Then A is a basis of finite order.

Further, A is a basis of finite order at most $h = 2l$, $h, l \in \mathbb{N}$ where l is defined by $0 \leq (1 - \alpha)^l \leq \frac{1}{2}$.

Proof: Let $\sigma(A) = \alpha > 0$. Then $0 \leq 1-\alpha < 1$, and so $0 \leq (1-\alpha)^l \leq \frac{1}{2}$, for some integer $l \geq 1$. By Theorem 3.8, $1 - \sigma(lA) \leq (1 - \sigma(A))^l = (1 - \alpha)^l \leq \frac{1}{2}$, and so $\sigma(lA) \geq \frac{1}{2}$. Let $h = 2l$. It follows from Corollary 3.6 that the set lA is a basis of order 2 and so A is a basis of order $2l = h$. This completes the proof. □

Theorem 3.10 (*Shnirel'man-Goldbach*)

The set $A = \{0, 1\} \cup \{p + q \mid p, q \in \Pi\}$ *has positive Shnirel'man density.*

Proof: See [18, Theorem 7.8]. □

Definition 3.11 *Let* S *be a subset of* Π. *Then* S *contains a positive proportion of* Π *if there is a real number* $0 < \theta$ *such that* $S(x) > \theta\pi(x)$ *for all sufficiently large* $x \in \mathbb{Z}^+$.

The following is a well-known result:

Lemma 3.12 *Let* S *be a subset of* Π *which contains a positive proportion of* Π. *Then the set* $S \cup \{0, 1\}$ *is a basis of finite order.*

Proof: We show that the set $A = \{0, 1\} \cup \{p + q; p, q \in S\}$ has positive Shnirel'man density. For any positive integer N let $r(N)$ denote the number of representations of N as a sum of two primes and let $r_{\mathcal{S}}(N)$ denote the number of representations of N as a sum of two primes belonging to $\mathcal{S}$. Then, for all sufficiently large $x \in \mathbb{Z}$,

$$\sum_{N \leq x} r_{\mathcal{S}}(N) \geq \big(\mathcal{S}(\tfrac{x}{2})\big)^2 \geq (\theta\pi(\tfrac{x}{2}))^2,$$

and by the Prime Number Theorem (see I, Theorem 2.24)

$$(\theta\pi(\tfrac{x}{2}))^2 \geq c_1(\frac{\frac{x}{2}}{\ln\frac{x}{2}})^2, \quad \text{for some positive constant } c_1.$$

Also, by Lemma 3.3,

$$\sum_{N \leq x} (r_{\mathcal{S}}(N))^2 \leq c_2\,\frac{x^3}{(\ln x)^4}, \quad \text{for some positive constant } c_2.$$

Now, by the Cauchy-Schwarz inequality (see I, Lemma 2.22),

$$(\sum_{N \leq x} (r_{\mathcal{S}}(N))^2 \leq \sum_{\substack{N \leq x \\ r_{\mathcal{S}}(N) \geq 1}} 1 \sum_{N \leq x} (r_{\mathcal{S}}(N))^2.$$

Of course, $\sum_{\substack{N \leq x \\ r_{\mathcal{S}}(N) \geq 1}} 1 \leq \mathcal{A}(x)$. Therefore we can write,

$$\frac{\mathcal{A}(x)}{x} \geq \frac{1}{x}\frac{(\sum_{N \leq x} r_{\mathcal{S}}(N))^2}{\sum_{N \leq x} (r_{\mathcal{S}}(N))^2}, \text{ and so}$$

$$\frac{\mathcal{A}(x)}{x} \geq \frac{1}{x}\frac{(c_1(\frac{\frac{x}{2}}{\ln\frac{x}{2}})^2)^2}{c_2\frac{x^3}{(\ln x)^4}} = \frac{{c_1}^2(\ln x)^4}{c_2(\ln x - \ln 2)^4} \geq \frac{{c_1}^2(\ln x)^4}{c_2(\ln x)^4}.$$

This means that $\mathcal{A}(x) \geq c_3 x$, for some positive constant c_3 and for all sufficiently large x. Since $1 \in \mathcal{A}$ it follows that $\mathcal{A}$ has positive Shnirel'man density and so is a basis of finite order, say $h \in \mathbb{Z}^+$. Therefore every non-negative integer can be expressed as a sum of exactly h elements of

$\mathcal{A}$. Whenever 0 occurs in such a sum we may write $0+0$ and whenever 1 occurs we may write $1+0$ and so any sum of exactly h elements of $\mathcal{A}$ is a sum of exactly $2h$ elements of $\mathcal{S} \cup \{0,1\}$. Therefore, $\mathcal{S} \cup \{0,1\}$ is a basis of order $2h$. □

Theorem 3.13 *Let S be a subset of Π which contains a positive proportion of Π. If $2 \in S$ then R, the subring of $\mathbb{Q}$ generated by $\{\frac{1}{p} \mid p \in S\}$, has $\operatorname{usn}(R) = n$ for some $n \in \mathbb{N}$.*

Proof: By Lemma 3.12, the set $\mathcal{S} \cup \{0,1\}$ is a basis of finite order, say of order $h \in \mathbb{Z}^+$. By Lemma 1.3, we need only prove that every positive integer is a sum of exactly h units of R to show that R has the h-sum property. For an arbitrary element r of $\mathbb{Z}^+$ we have:

$$r = s_1 + s_2 + \ldots + s_h \qquad (s_i \in S \cup \{0,1\},\ i = 1, \ldots, h).$$

Since $r \in \mathbb{Z}^+$, then $s_i \neq 0$ for all $i = 1, \ldots, h$.

If $s_i \in S \cup \{1\}$ for all $i = 1, \ldots, h$ then r is a sum of h units of R.

If $s_1, \ldots, s_k \neq 0$ for some $1 \leq k < h$ and $s_{k+1}, \ldots, s_h = 0$ then,

$$r = \sum_{i=1}^{k-1} s_i + s_k \left(\frac{1}{2^{h-k}} + \sum_{j=1}^{h-k} \frac{1}{2^j} \right)$$

is a sum of h units of R. By Lemma 1.3, R has the h–sum property. So, certainly $\operatorname{usn}(R) \leq h$. □

This is a significant result. For example, letting $\Pi = \{p_i\}_{i=1,2,\ldots}$ under the natural ordering, the ring generated by $\{\frac{1}{p_1}, \frac{1}{p_n}, \frac{1}{p_{2n}}, \ldots, \frac{1}{p_{in}}, \ldots\}$ has finite unit sum number whatever $n \in \mathbb{Z}^+$. (Note, $R = \mathbb{Q}$ for $n = 1$.)

From the Prime Number Theorem (see I, Theorem 2.24) and the Prime Number Theorem for Arithmetic Progressions (see I, Theorem 2.25) it is seen that;

$$\lim_{x \to \infty} \frac{\pi(x,k,l)}{\pi(x)} = \frac{1}{\varphi(k)}, \quad \text{where } \varphi \text{ is the Euler function.}$$

So, for any $\varepsilon > 0$, we can find $x_0 \in \mathbb{R}$ such that

$$-\varepsilon < \frac{\pi(x,k,l)}{\pi(x)} - \frac{1}{\varphi(k)} < \varepsilon \qquad \text{for all } x > x_0,$$

so that $\quad \pi(x,k,l) > \pi(x)(\frac{1}{\varphi(k)} - \varepsilon) \quad$ for all $x > x_0$.

Now set $k = 24$, $l = 1$ and choose $\varepsilon = \frac{1}{16}$. Then $\quad \pi(x, 24, 1) > \frac{1}{16}\pi(x)$ for all $x > x_0$ and for some $x_0 \in \mathbb{R}$.

Therefore the set of primes congruent to 1 mod 24 is a positive proportion of Π, and by Theorem 3.13 and Corollary 2.8 we have proved:

Corollary 3.14 *Let* $P = \{2\} \cup \{p \in \Pi \mid p \equiv 1 \bmod 24\}$. *Let* G *be a rational group such that* $E_{\mathbb{Z}}(G)$ *is that subring of* $\mathbb{Q}$ *generated by* $\{\frac{1}{p} \mid p \in P\}$. *Then* $\mathrm{usn}(G)$ *is finite but greater than* 2.

Obviously, this result and the results previous to it open the question of what the range of values of unit sum numbers is for rational groups. Do values of unit sum number depend entirely on the proportion or density of primes in X_G (allowing for the special role of 2) or do they depend on other attributes of the particular primes in $\Pi \setminus X_G$? It is interesting to notice that in Example 2.3 a rational group G in which $\Pi \setminus X_G$ does not contain a positive proportion of the primes, by definition, is shown to have usn(G)= 2. We leave the discussion of these questions open.

Our last objective in this chapter is to find an upper bound for usn(R) where R is as described in Corollary 3.14.

Definitions 3.15

- $\theta(x : k, l) = \sum\limits_{\substack{p \equiv k \bmod l \\ p \leq x \\ p \in \Pi}} \ln p \ , \quad x \in \mathbb{R},\ k, l \in \mathbb{N}$ *with* $(k, l) = 1$.
- *A* multiplicative function *is a function defined on the integers such that* $f(m)f(n) = f(mn)$ *whenever* $(m, n) = 1$.

  Note that for any multiplicative function f, *if* $f \neq 0$, *then* $f(1) = 1$.

Proposition 3.16 *Let* $P = \{2\} \cup \{p \in \Pi \mid p \equiv 1 \bmod 24\}$ *and* G *a rational group with* $E_{\mathbb{Z}}(G)$ *that subring of* $\mathbb{Q}$ *generated by* $\{\frac{1}{p} \mid p \in P\}$.

Then $\operatorname{usn}(G) \leq 1208000$.

Proof: In finding the required bound our principal instrument is a cauchy inequality. We set up the cauchy inequality as follows.

First, for each $N \in \mathbb{N}$ set

$$r(N) = \sum_{\substack{p_1+p_2=N \\ p_1,p_2\equiv 1 \bmod 24}} \ln p_1 \ln p_2$$

Let $A = \{p_1 + p_2; p_1, p_2 \in \Pi \text{ and } p_1, p_2 \equiv 1 \bmod 24\}$, so that, recalling the definition of the counting function for A, $A(x) = \sum_{\substack{0<N\leq x \\ N\in A}} 1 = \sum_{\substack{N\leq x \\ r(N)\geq 1}} 1$.

Then the form of the inequality is as usual

$$(\sum_{N\leq x} r(N))^2 \leq A(x) \sum_{N\leq x} (r(N))^2.$$

Next we provide a lower bound for $\sum_{N\leq x} (r(N))$.

Since $\sum_{N\leq x} r(N) \geq (\theta(\frac{x}{2} : 1, 24))^2$, we can refer directly to Ramaré and Rumely [24, Theorem 1] from which we can state

$$\theta(x : 1, 24) \geq (1-\epsilon)\frac{x}{\varphi(24)} \quad \text{for all } x \geq \exp 24$$

where ϵ is calculated to be 0.008173. Therefore

$$\sum_{N\leq x} r(N) \geq 3.84266 \times 10^{-3} x^2 \quad , \text{for all } x \geq 2\exp 24.$$

An upper bound for $r(N)$ is also required.

Let

$$\mathcal{R}(x,a,b)=\sup_{I}\sum_{\substack{p\in\Pi\bigcap I\\ ap+b\in\Pi}}1 \quad , x\in\mathbb{R},\ a,b\in\mathbb{Z}$$

where the supremum is taken over all intervals I of length x.

Then Reisel and Vaughan [26, Lemma 5] give us

$$\mathcal{R}(x,a,b)<\Big(\frac{8cx}{(\ln x)^2}-100x^{\frac{1}{2}}\Big)\prod_{\substack{p|ab\\ p>2}}\Big(\frac{p-1}{p-2}\Big)$$

for all $x\geq \exp 24$ and $ab\neq 0$ and where c is the twin prime constant.

Taking $a=-1$, $b=N$, then

$$\mathcal{R}(x,-1,N)<\Big(\frac{8cx}{(\ln x)^2}\Big)\prod_{\substack{p|N\\ p>2}}\Big(\frac{p-1}{p-2}\Big)\quad \text{for all } x\geq \exp 24 \qquad .$$

Of course, returning to consider $r(N)$,

$$r(N)\leq\Big(\sum_{\substack{p\in\Pi\\ N-p\in\Pi}}1\Big)(\ln x)^2 \quad \text{for all } N\leq x.$$

Therefore, for all $x\geq\exp 24$ and $N\leq x$

$$\begin{aligned}r(N)&\leq\Big(\frac{8cx}{(\ln x)^2}(\ln x)^2\Big)\prod_{\substack{p|N\\ p>2}}\Big(\frac{p-1}{p-2}\Big)\\ &\leq 8cx\prod_{\substack{p|N\\ p>2}}\Big(\frac{p-1}{p-2}\Big).\end{aligned}$$

It is known for c, the twin prime constant, that $1.320323<c<1.320324$ (see [26]). Also notice that 3 cannot divide N where $N\equiv 2 \bmod 24$ so we may write $r(N)\leq 8(1.320324)x\prod_{\substack{p|N\\ p>3}}\Big(\frac{p-1}{p-2}\Big)$ for all $x\geq\exp 24$ and $N\leq x$.

Now we may return to our cauchy inequality and using the bounds described above we write

$$(3.84266 \times 10^{-3}x^2)^2 \leq A(x) \sum_{\substack{N \leq x \\ N \equiv 2 \bmod 24}} (10.5626x \prod_{\substack{p|N \\ p>3}} (\frac{p-1}{p-2}))^2$$

for all $x \geq 2\exp 24$ and therefore

$$\frac{A(x)}{x} \geq \frac{(3.84266 \times 10^{-3})^2 x^4}{x^3 111.57 \sum\limits_{\substack{N \leq x \\ N \equiv 2 \bmod 24}} (\prod\limits_{\substack{p|N \\ p>3}} (\frac{p-1}{p-2})^2)} \quad \text{for all } x \geq \exp 24 \qquad (*)$$

Now we must consider the term $\sum\limits_{\substack{N \leq x \\ N \equiv 2 \bmod 24}} (\prod\limits_{\substack{p|N \\ p>3}} (\frac{p-1}{p-2})^2)$. We begin by defining the multiplicative function f. It is defined over the prime powers, for each $p \in \Pi$, $k \in \mathbb{N}$, as follows

$$f(p^k) = \begin{cases} (\frac{p-1}{p-2})^2 - 1 & for \quad p > 3, k = 1 \\ 0 & for \quad p = 2, p = 3 \\ 0 & for \quad k > 1 \\ 1 & for \quad k = 0 \end{cases}$$

Now we define $f^*(n) = \sum\limits_{\substack{d|n \\ (d.6)=1}} f(d)$ for $n \in \mathbb{Z}^+$, $d \in \mathbb{Z}^+$, and letting $n, m \in \mathbb{Z}^+$ such that $(m, n) = 1$, then

$$\begin{aligned} f^*(m)f^*(n) &= \sum_{\substack{d|m \\ (d.6)=1}} f(d) \sum_{\substack{d|n \\ (d.6)=1}} f(d) \\ &= \sum_{\substack{d|mn \\ (d.6)=1}} f(d) \\ &= f^*(mn) \end{aligned}$$

Therefore f^* is also a multiplicative function. Now let n be any positive integer. Express n uniquely in the usual way $n = \prod\limits_{p \in \Pi} p^{k_p}$ ($k_p \in \mathbb{N}$). Then

$$f^*(n) = \sum_{\substack{d|n \\ (d,6)=1}} f(d) = \prod_{p\in\Pi} \sum_{\substack{d|p^{k_p} \\ (d,6)=1}} f(d) = \prod_{\substack{p\in\Pi \\ p|n \\ p>3}} (f(p) + f(1)) = \prod_{\substack{p\in\Pi \\ p|n \\ p>3}} (f(p) + 1).$$

So we may write

$$\sum_{\substack{d|n \\ (d,6)=1}} f(d) = \prod_{\substack{p|n \\ p>3}} \left(\tfrac{p-1}{p-2}\right)^2.$$

Now, for each $d \le x$, d divides not more than $\dfrac{x}{24d}$ of the set

$\{N \le x; N \equiv 2 \bmod 24\}$. Therefore

$$\sum_{\substack{N\le x \\ N\equiv 2 \bmod 24}} \prod_{\substack{p|N \\ p>3}} \left(\tfrac{p-1}{p-2}\right)^2 = \sum_{\substack{N\le x \\ N\equiv 2 \bmod 24}} \Big(\sum_{\substack{d|N \\ (d,6)=1}} f(d)\Big) \le \frac{x}{24} \sum_{\substack{d|N \\ (d,6)=1}} \frac{f(d)}{d}.$$

We are not yet ready to return to inequality (*). We now show that

$g^*(n) = \displaystyle\sum_{\substack{d|n \\ (d,6)=1}} \frac{f(d)}{d}$ is a multiplicative function.

Let $n, m \in \mathbb{N}$, arbitrary, such that $(m,n) = 1$. Then

$$\begin{aligned} g^*(m)g^*(n) &= \sum_{\substack{d|m \\ (d,6)=1}} \frac{f(d)}{d} \sum_{\substack{d|n \\ (d,6)=1}} \frac{f(d)}{d} \\ &= \sum_{\substack{d|mn \\ (d,6)=1}} \frac{f(d)}{d} \end{aligned}$$

Therefore g^* is a multiplicative function and so, for any $N \in \mathbb{N}$ with

$N = \prod_{p\in\Pi} p^{k_p}$ $(k_p \in \mathbb{N})$, we may write

$$\sum_{\substack{d|N \\ (d,6)=1}} \frac{f(d)}{d} = \prod_{\substack{p\in\Pi \\ p|N \\ p>3}} \sum_{d|p^{k_p}} \frac{f(d)}{d} = \prod_{\substack{p\in\Pi \\ p|N \\ p>3}} \left(\frac{f(p)}{p}+1\right)$$

In fact, changing the conditions under the summation we have

$$\sum_{\substack{d\le x \\ (d,6)=1}} \frac{f(d)}{d} = \prod_{\substack{p\le x \\ p>3}} \left(\frac{f(p)}{p}+1\right)$$

Therefore

$$\lim_{x\to\infty}\sum_{\substack{d\le x\\(d,6)=1}}\frac{f(d)}{d}=\lim_{x\to\infty}\prod_{\substack{p\le x\\p>3}}(\frac{f(p)}{p}+1)$$

We now evaluate a bound for the expression on the right hand side.

By direct computation $\prod_{\substack{p\le100\\p>3}}(\frac{f(p)}{p}+1)=1.31562.$

Now

$$\lim_{x\to\infty}\prod_{\substack{p>3\\p\le x}}(\frac{f(p)}{p}+1)=\prod_{\substack{p\le100\\p>3}}(\frac{f(p)}{p}+1)\lim_{x\to\infty}\prod_{\substack{p>100\\p\le x}}(\frac{f(p)}{p}+1).$$

Since $x+1\le\exp x$ for all $x\ge0$, then $\frac{f(p)}{p}+1\le\exp(\frac{f(p)}{p})$ for all $p\in\Pi$. Therefore

$$\lim_{x\to\infty}\prod_{\substack{p>100\\p\le x}}(\frac{f(p)}{p}+1)\le\lim_{x\to\infty}\exp\sum_{\substack{p>100\\p\le x}}(\frac{f(p)}{p}) \quad .$$

Certainly $\frac{f(p)}{p}=\frac{2p-3}{p(p^2-4p+4)}<\frac{2.06}{p^2}$ for all $p>100, p\in\Pi$. In this way we over-estimate $\lim_{x\to\infty}\prod_{\substack{p>100\\p\le x}}(\frac{f(p)}{p}+1)\le\exp(\int_{100}^{\infty}\frac{2.06}{(n-1)^2}dn)\le$ $\exp(0.020397)=1.0206055.$

So we can drop the terminology of limits and write

$$\prod_{p>3}(\frac{f(p)}{p}+1)\quad\le(1.31562)(1.0206055)\le1.3435.$$

So we have shown that

$$\sum_{\substack{N\le x\\N\equiv2\bmod24}}\prod_{\substack{p|N\\p>3}}(\frac{p-1}{p-2})^2\le\frac{x}{24}(1.3435)\quad\text{for all } x\ge0.$$

Therefore we can rewrite expression (*) as

$$\frac{A(x)}{x}\ge\frac{(3.84266\times10^{-3})^2x^4(24)}{x^4(111.57)(1.3435)}\ge2.3640\times10^{-6}\quad\text{for all } x\ge2\exp24.$$

At this stage recall that the set we are fundamentally interested in is not A but the set $A' = \{a \in \mathbb{Z}^+ \mid a \text{ is a sum or difference of two units of } R\}$. Since $A' \supset A$ then

$$\frac{A'(x)}{x} \geq 2.3640 \times 10^{-6} \qquad \text{for all } x \geq 2\exp 24.$$

We need to show that this inequality is true for all $x \geq 0$. We use a stepwise procedure. For reference purposes, following this proposition there is a list of the first 268 primes congruent to 1 mod 24 (see List 3.17).

Step 1: 1 and 2 are units of R so $1 \in A'$. Therefore $\dfrac{A'(x)}{x} \geq 2.3660 \times 10^{-6}$ for all $x \leq (2.3640 \times 10^{-6})^{-1} = 423011$.

Step 2: The number of primes congruent to 1 mod 24 and not exceeding 17,000 is 268 (see List 3.17). Let p be any one such prime. Then $p+1$, $p+2$, $p+4$, $p+8$, $p+16$, $p-1$, $p-2$, $p-4$, $2p-1$, $2p+2$, $2p+4$, $2p+8$, $2p+16$ and $2p-4$ are all distinct modulo 24. Therefore each prime congruent to 1 mod 24 contributes at least 14 distinct elements to A', which are all positive and less than 423011 , so

$$\frac{A'(x)}{x} \geq \frac{14(268)}{x} \qquad \text{for all } x \geq 423011.$$

Therefore

$$\frac{A'(x)}{x} \geq (2.3640 \times 10^{-6}) \qquad \text{for all } x \leq \frac{14(268)}{2.3640 \times 10^{-6}} = 1.587 \times 10^{9}.$$

Step 3: The number of primes congruent to 1 mod 24 and not exceeding

$10,000$ is 141 (see List 3.17). Then the number of distinct products of pairs of these primes is $\frac{141(141+1)}{2} = 10011$. Each product is congruent to 1 mod 24 and so, in precisely the same way as for the primes congruent to 1 mod 24 in Step 1, each product contributes at least 14 distinct elements to A', all positive and less than 1.587×10^9. Then

$$\frac{A'(x)}{x} \geq \frac{14(10011)}{x} \qquad \text{for all } x \geq 1.587 \times 10^9.$$

Therefore

$$\frac{A'(x)}{x} \geq (2.3640 \times 10^{-6}) \qquad \text{for all } x \leq 5.9286 \times 10^{10}.$$

Step 4: The number of primes congruent to 1 mod 24 and not exceeding $24,000$ is at least 268 (see List 3.17). Then the number of distinct products of pairs of these primes is $\frac{268(268+1)}{2} = 36046$. Each product is congruent to 1 mod 24 and as in Step 3, each product contributes at least 14 distinct elements to A', all positive and less than 5.9286×10^{10}. Then

$$\frac{A'(x)}{x} \geq \frac{14(36046)}{x} \qquad \text{for all } x \geq 5.9286 \times 10^{10}.$$

Therefore

$$\frac{A'(x)}{x} \geq (2.3640 \times 10^{-6}) \qquad \text{for all } x \leq 2.1328 \times 10^{11}.$$

Since $2\exp 24 < 2.1347 \times 10^{11}$ it is evident that we have shown

$$\frac{A'(x)}{x} \geq (2.3640 \times 10^{-6}), \quad \text{for all } x \geq 0.$$

Thus the Shnirel'man density of A' is at least 2.346×10^{-6}. Using Shnirel'man's Theorem 3.9, we calculate an $l \in \mathbb{N}$ such that $(1 - 2.346 \times 10^{-6})^l \leq \frac{1}{2}$ to be 302000. Therefore the set A' is a basis of order at most $2(302000) = 604000$. So, recalling that A' is a set of sums and differences of two units, then $\mathrm{usn}(R)$ is at most $604000 \times 2 = 1208000$. □

The following list was compiled using [15].

List 3.17

List of the first 268 primes congruent to 1 mod 24

73, 97, 193, 241, 313, 337, 409, 433, 457, 577, 601, 673, 769, 937, 1009, 1033, 1129, 1153, 1201,
1249, 1297, 1321, 1489, 1609, 1657, 1753, 1777, 1801, 1873, 1993, 2017, 2089, 2113, 2137, 2161,
2281, 2377, 2473, 2521, 2593, 2617, 2689, 2713, 2833, 2857, 2953, 3001, 3049, 3121, 3169, 3217,
3313, 3361, 3433, 3457, 3529, 3673, 3697, 3769, 3793, 3889, 4057, 4129, 4153, 4177, 4201, 4273,
4297, 4441, 4513, 4561, 4657, 4729, 4801, 4969, 4993, 5113, 5209, 5233, 5281, 5449, 5569, 5641,
5689, 5737, 5857, 5881, 5953, 6073, 6121, 6217, 6337, 6361, 6481, 6529, 6553, 6577, 6673, 6793,
6841, 6961, 7057, 7129, 7177, 7297, 7321, 7369, 7393, 7417, 7489, 7537, 7561, 7681, 7753, 7873,
7993, 8017, 8089, 8161, 8209, 8233, 8329, 8353, 8377, 8521, 8641, 8689, 8713, 8737, 8929, 9001,
9049, 9241, 9337, 9433, 9601, 9649, 9697, 9721, 9769, 9817, 10009, 10177, 10273, 10321, 10369,
10513, 10657, 10729, 10753, 10993, 11113, 11161, 11257, 11329, 11353, 11497, 11593, 11617, 11689,
11833, 11953, 12049, 12073, 12097, 12241, 12289, 1240, 12433, 12457, 12553, 12577, 12601, 12697,
12721, 12841, 12889, 13009, 13033, 13177, 13249, 13297, 13417, 13441, 13513, 13537, 13633, 13681,
13729, 13873, 13921, 14281, 14401, 14449, 14593, 14713, 14737, 14929, 15073, 15121, 15193, 15217,
15241, 15313, 15361, 15601, 15649, 15817, 15889, 15913, 15937, 16033, 16057, 16249, 16273, 16369,
16417, 16561, 16633, 16657, 16729, 16921, 16993, 17041, 17137, 17209, 17257, 17377, 17401, 17449,
17497, 17569, 17713, 17737, 17761, 17881, 17929, 17977, 18049, 18097, 18121, 18913, 19009, 19081,
19249, 19273, 19417, 19441, 19489, 19609, 19681, 19753, 19777, 19801, 19993, 20089, 20113, 20161

IV The involution property

Having considered the unit sum number problem in previous chapters, it is perhaps natural to ask a further question: under what conditions is every element of a ring a sum of two units one of which is an involution? This question is motivated by work of Nicholson [19], Ó Searcóid [21] and others on so called "clean rings", i.e. rings in which every element is the sum of a unit and an idempotent. The latter element can, of course, be converted in suitable circumstances to an involution. In this chapter we have attempted to supply some answers to this question with regard to the rings and the endomorphism rings of modules discussed with regard to unit sum number in previous chapters.

As in previous chapters all rings will be unital associative rings.

§1 General considerations

Recall that a unital ring E has the involution property if every element of E is a sum of a unit and an involution of E and an R-module M over a commutative ring R has the involution property if every endomorphism of M is a sum of an automorphism of M and an involutary automorphism of M.

Proposition 1.1 *If G is a group which has the involution property then 2 is an automorphism of G.*

Proof: Let 1 be the identity in $E(G)$. Certainly $1 \in Aut(G)$. Let $1 = \alpha + v$ where $\alpha, v \in Aut(G)$ and $v^2 = 1$. Then $v = v\alpha + 1$. Therefore $1 = \alpha + v\alpha + 1$ and so we get $0 = (1+v)\alpha$. However, since $\alpha \in Aut(G)$ then $0 = 1 + v$. Thus $v = -1$. Therefore $\alpha + v = 1 = \alpha - 1$ which gives us $\alpha = 2$. □

The following is a well-known result.

Lemma 1.2 *Let M be a R–module where $2 \in Aut(M)$. Let v be any involutary automorphism of M and 1_M the identity in $E(M)$.*

Then $\quad M = \ker(1_M - v) \bigoplus \ker(1_M + v)$.

Proof: Let $m \in \ker(1_M - v) \cap \ker(1_M + v)$. Since $m(1_M - v) = 0$ then $m = mv$. 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 $x = \frac{1}{2}\big((x - xv) + (x + xv)\big)$ where

$(x - xv) \in \ker(1_M + v)$ and $(x + xv) \in \ker(1_M - v)$. □

Unlike the unit sum property, for a PID R, it is necessary for the R to have the involution property in order for any free R-module to have it.

Theorem 1.3 *Let R be a PID. A free R-module has the involution property only if R has the property.*

Proof: Let M be an arbitrary free R-module over R a PID. Let $Inv(E(M))$ be the set of all involutions of $E(M)$. This is a subset of $Aut(M)$. Assume that R does not have the involution property. We show that then M cannot have it.

Let $k \neq 0$ be an arbitrary element of R and assume, for contradiction, $k1_M = \alpha + v$ for some $\alpha \in Aut(M)$ and $v \in Inv(E(M))$ where 1_M is the identity in $E(M)$.

If 2 is not a unit in R then 2 is not an automorphism of M, since for any basis element of M, say e_i, $\frac{1}{2}e_i \notin M$ and so by Proposition 1.1, M has not got the involution property.

If 2 is a unit in R then, by Lemma 1.2, $M = \ker(1_M - v) \oplus \ker(1_M + v)$. So, letting $\{e_i\}_{i \in I}$ be a basis for the summand $\ker(1_M - v)$ and letting $\{e_i\}_{i \in I'}$ be a basis for the other summand $\ker(1_M + v)$ then $e_i v = e_i$ for all $i \in I$ and $e_i v = -e_i$ for all $i \in I'$. Now, letting $J = I \cup I'$, then $\{e_i\}_{i \in J}$

is a basis for M such that $e_i v = \pm e_i$ for each $i \in J$.

Now, for some arbitrary $i \in J$, we may write $e_i \alpha^{-1} = \sum\limits_{j \in J} x_{ij} e_j$ where $x_{ij} \in R$ for each $i, j \in J$, keeping in mind that these are finite sums. By assumption $\alpha = (k1_M - v)$ and so $e_i \alpha^{-1}(k1_M - v) = (\sum\limits_{j \in J} x_{ij} e_j)(k1_M - v) = e_i$. Of course, for each $i \in J$, since $e_i \alpha = e_i(k1_M - v) \neq 0$ then $[e_i(k1_M - v)] = \{i\}$ and consequently $x_{ii} e_i (k1_M - v) = x_{ii}(k \pm 1)e_i = e_i$, where 1 is the identity in R. So $x_{ii}(k \pm 1) = 1$; here, by $k \pm 1$ we mean $k + 1$ or $k - 1$ not both (i.e. $k - 1$ for $i \in I$ and $k + 1$ for $i \in I'$). Therefore, $k + 1$ and or $k - 1$ must be units in R.

Since R does not have the involution property there exists $h \in R$ such that h is not the sum of a unit and an involution of R. Then, since $h = h + 1 - 1$ and both 1 and -1 are involutions of R then neither $h + 1$ nor $h - 1$ are units of R. Therefore $h1_M$ cannot be the sum of an automorphism and an involutary automorphism of M. With this, we are finished. □

At this stage we introduce a technical lemma which we will use later on.

Lemma 1.4 *Let M be a module with a decomposition*

$M = \bigoplus_{i<n} M_i$ $(n \leq \omega)$ and let ϕ be an endomorphism of M. Moreover, let $\pi_j : M \longrightarrow M_j$ denote the canonical projection and assume that

$(\phi \restriction_{M_i})\pi_i \in Aut(M_i)$, $(\phi \restriction_{M_i})\pi_j = 0$ for all $i, j < n$ with $i < j$.

Then ϕ is an automorphism of M.

Proof: First, set $\phi_{i,j} = (\phi \restriction_{M_i})\pi_j$. Clearly, $\phi = \sum_{i,j<n} \phi_{i,j}$ and the assumption now reads as $\phi_{i,i} \in Aut(M_i)$ and $\phi_{i,j} = 0$ for $i < j$.

Consider the set $\mathcal{X}$ of all canonical summands $X_m = \bigoplus_{i<m} M_i$ $(m \leq n)$ with $X_m\phi \subseteq X_m$ and $\phi \restriction_{X_m} \in Aut(X_m)$. Let $\mathcal{X}$ be ordered naturally by inclusion; note that $X \subseteq X'$ is equivalent to $X \sqsubseteq X'$ here for $X, X' \in \mathcal{X}$. Now, $\mathcal{X}$ is non-empty since $X_0 = \{0\}$ is clearly an element of $\mathcal{X}$.

Consider an arbitrary chain in $\mathcal{X}$, say

$\mathcal{M}; = X_{m_0} \sqsubseteq X_{m_1} \sqsubseteq \ldots \sqsubseteq X_{m_j} \sqsubseteq \ldots.$ $(j \in J \subseteq n)$. Then, $L = \bigcup_{j \in J} X_{m_j}$ is a least upper bound for $\mathcal{M}$. We now show that $L \in \mathcal{X}$. For $m = \sup_{j \in J} m_j$, where $X_{m_j} = \bigoplus_{i<m_j} M_i$, we obviously have $L = \bigoplus_{i<m} M_i$. If m is finite then $L = X_{m_j}$ for some $j \in J$ and so $L \in \mathcal{X}$.

Let $m = n = \omega$. Then $L = M$ is obviously invariant under ϕ. Now, for any $h \in L$, there is $j \in J$ such that $h \in X_{m_j}$. Therefore, since $\phi \restriction X_{m_j} \in Aut(X_{m_j})$ we have that $h\phi = 0$ if and only if $h = 0$ and that

$h = x\phi$ for some $x \in X_j$. Thus ϕ is bijective, i.e. $\phi \in Aut(L)$. Therefore $L \in \mathcal{X}$ and we may invoke Zorn's Lemma, i.e. there is a maximal element L of $\mathcal{X}$.

Assume $L = \bigoplus_{j<m} M_j \neq M$. Then there exists an integer i with $m \leq i < n$, such that $M_i \cap L = 0$. Notice that then also $(L\phi) \cap M_i = 0$ by definition of $\mathcal{X}$.

For clarity we now simplify our notation. We write $\phi \restriction_L = \phi_{L.L}$, $(\phi \restriction_{M_i})\pi_L = \phi_{M_i.L}$ and $(\phi \restriction_L)\pi_i = \phi_{L.M_i}$, where π_L and π_i are the canonical projections onto L and M_i respectively. Let 1_L, 1_{M_i} and $1_{L\oplus M_i}$ be the identity mappings for L, M_i and $L \oplus M_i$ respectively.

Now we show that $\phi \restriction_{L\oplus M_i} \in Aut(L \oplus M_i)$. Firstly, since $\phi_{L.M_i} = 0$ we have that $\phi \restriction_{L\oplus M_i} = \phi_{L.L} + \phi_{M_i.L} + \phi_{i.i}$. Since $\phi_{L.L} \in Aut(L)$ and by assumption $\phi_{i.i} \in Aut(M_i)$ then

$$
\begin{aligned}
&\phi \restriction_{L\oplus M_i}(\phi_{L.L}^{-1} - \phi_{i.i}^{-1}\phi_{M_i.L}\phi_{L.L}^{-1} + \phi_{i.i}^{-1}) = \\
&\phi_{L.L}(\phi_{L.L}^{-1} - \phi_{i.i}^{-1}\phi_{M_i.L}\phi_{L.L}^{-1} + \phi_{i.i}^{-1}) + \phi_{M_i.L}(\phi_{L.L}^{-1} - \phi_{i.i}^{-1}\phi_{M_i.L}\phi_{L.L}^{-1} + \phi_{i.i}^{-1}) \\
&\qquad + \phi_{i,i}(\phi_{L.L}^{-1} - \phi_{i.i}^{-1}\phi_{M_i.L}\phi_{L.L}^{-1} + \phi_{i.i}^{-1}) \\
&\qquad\qquad = 1_L + \phi_{M_i.L}\phi_{L.L}^{-1} - \phi_{i.i}\phi_{i.i}^{-1}\phi_{M_i.L}\phi_{L.L}^{-1} + 1_{M_i} \\
&\qquad\qquad = 1_L + 1_{M_i} = 1_{L\oplus M_i}
\end{aligned}
$$

where $\phi_{i,i}^{-1}\phi_{L.L} = 0 = \phi_{i.i}^{-1}\phi_{L.L} = \phi_{M_i.L}\phi_{i,i}^{-1}$. Similarly

$(\phi_{L.L}^{-1}\phi_{i,i}^{-1}\phi_{M_i.L}\phi_{L.L}^{-1} + \phi_{i.i}^{-1})\ \phi \restriction_{L\oplus M_i} =$

$$(\phi_{L.L}^{-1} - \phi_{i,i}^{-1}\phi_{M_i.L}\phi_{L.L}^{-1} + \phi_{i.i}^{-1})\phi_{L.L} + (\phi_{L.L}^{-1} - \phi_{i,i}^{-1}\phi_{M_i.L}\phi_{L.L}^{-1} + \phi_{i.i}^{-1})\phi_{M_i.L}$$

$$+(\phi_{L.L}^{-1} - \phi_{i,i}^{-1}\phi_{M_i.L}\phi_{L.L}^{-1} + \phi_{i.i}^{-1})\phi_{i,i}$$

$$= 1_L - \phi_{i.i}^{-1}\phi_{M_i.L}\phi_{L,L}^{-1}\phi_{L.L} + \phi_{i.i}^{-1}\phi_{M_i.L} + 1_{M_i}$$

$$= 1_L + 1_{M_i}.$$

$$= 1_{L\oplus M_i}.$$

We illustrate this with matrices. Let $\phi \restriction_{L\oplus M_i} = \begin{pmatrix} \phi_{L.L} & 0 \\ \phi_{M_i.L} & \phi_{i.i} \end{pmatrix}$, then

$$1_{L\oplus M_i} = \begin{pmatrix} \phi_{L.L} & 0 \\ \phi_{M_i.L} & \phi_{i.i} \end{pmatrix} \begin{pmatrix} (\phi_{L.L})^{-1} & 0 \\ -(\phi_{i.i})^{-1}\phi_{M_i.L}(\phi_{L.L})^{-1} & (\phi_{i.i})^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} (\phi_{L.L})^{-1} & 0 \\ -(\phi_{i.i})^{-1}\phi_{M_i.L}(\phi_{L.L})^{-1} & (\phi_{i.i})^{-1} \end{pmatrix} \begin{pmatrix} \phi_{L.L} & 0 \\ \phi_{M_i.L} & \phi_{i.i} \end{pmatrix}$$

Thus $\phi \restriction_{L\oplus M_i} \in Aut(L\oplus M_i)$ and $L\oplus M_i \in \mathcal{X}$ contradicting L being maximal and so by Zorn's Lemma we deduce $L = M$.

Therefore $\phi \in Aut(M)$. □

§2 Free modules over a PID

In Chapter I we presented Searcóid's result, (see I, Theorem 3.2) that every vector space is 'clean" and we proved in I, Corollary 3.3, that every vector space over a field F has the involution property if $\frac{1}{2} \in F$. In this section we provide an alternative proof to that of I, Corollary 3.3, with the necessary condition that $\frac{1}{2} \in F$. This proof is of value due to its constructional approach.

Theorem 2.1 *Let F be a field and let $X = \bigoplus_{i<n} Fe_i$ $(n \leq \omega)$ be a vector space of countable rank over F.*

Then X has the involution property if and only if $\frac{1}{2} \in F$.

Proof: If $\frac{1}{2} \notin F$ then F has not got the involution property. Then, by Theorem 1.3, X has not got the property.

We proceed to make a change of basis with respect to ϕ.

Step 1: Set $\epsilon_{0.0} = e_0$.

If $\epsilon_{0.0}\phi \in \langle \epsilon_{0.0} \rangle$ then set $E_0 = \{\epsilon_{0.0}\}$ and go to Step 2.

If not, set $\epsilon_{0,1} = (\epsilon_{0.0}\phi)_r$. Clearly $\epsilon_{0.0}$ and $\epsilon_{0,1}$ are linearly independent.

If $\epsilon_{0.1}\phi \in \langle \epsilon_{0,0}, \epsilon_{0.1} \rangle$ then set $E_0 = \{\epsilon_{0.0}, \epsilon_{0.1}\}$ and go to Step 2.

If not, set $\epsilon_{0,2} = \epsilon_{0,1}\phi$.

Continuing in this way the linearly independent set $E_0 = \{\epsilon_{0.i}; i \in I_0\}$ is formed where the indexing set I_0 is countable.

Clearly, $\langle \epsilon_{0.i}; i \in I_0 \rangle$ is invariant under ϕ.

Step 2: Choose $m_1 \in \mathbb{N}$ minimal such that e_{m_1} is linearly independent of E_0. (If there is no such e_{m_1} then our steps are completed.)

Set $\epsilon_{1.0} = e_{m_1}$.

If $\epsilon_{1.0}\phi \in \langle E_0, \epsilon_{1.0} \rangle$ then set $E_1 = \{\epsilon_{1.0}\}$ and go to Step 3.

If not set $\epsilon_{1.1} = \epsilon_{1.0}\phi$. Clearly, $\epsilon_{0.0}, \epsilon_{0.1}, \ldots, \epsilon_{1.0}$ and $\epsilon_{1.1}$ are linearly independent.

If $\epsilon_{1.1}\phi \in \langle E_0, \epsilon_{1.0}, \epsilon_{1.1} \rangle$ then set $E_1 = \{\epsilon_{1.0}, \epsilon_{1.1}\}$ and go to Step 3.

If not set $\epsilon_{1.2} = \epsilon_{1.1}\phi$.

Continuing in this way we form $E_1 = \{\epsilon_{1.i}; i \in I_1\}$, where I_1 is countable.

Step j($\in \mathbb{N}$): Choose m_j such that e_{m_j} is linearly independent of $E_0 \cup E_1 \cup \ldots \cup E_{j-1}$. (If no such m_j exists then our steps are completed.)

Set $\epsilon_{j.0} = e_{m_j}$.

If $\epsilon_{j.0}\phi \in \langle E_0, \ldots, E_{j-1}, \epsilon_{j.0} \rangle$ then set $E_j = \{\epsilon_{j.0}\}$ and go to Step $j+1$.

If not set $\epsilon_{j,1} = \epsilon_{j,0}\phi$. Clearly $\{E_0, E_1, \ldots, E_{j-1}, \epsilon_{j,1}, \epsilon_{j,1}\}$ is a linearly independent set.

Continuing as before we form $E_j = \{\epsilon_{j,i}; i \in I_j\}$ where I_j is countable.

Continuing on in this manner we form a new basis for X which we may write as $X = \bigoplus_{j\in J} \bigoplus_{i\in I_j} F\epsilon_{j,i} = \bigoplus_{j\in J} X_j$. In the usual way we may write $\phi = \sum_{a,b\in J} \phi_{a,b}$ where $\phi_{a,b} \in Hom(X_a, X_b)$, for all $a, b \in J$, i.e.

$$\phi = \begin{pmatrix} \phi_{0,0} & 0 & 0 & 0 & \ldots & \\ \phi_{1,0} & \phi_{1,1} & 0 & 0 & 0 & \ldots \\ \phi_{2,0} & \phi_{2,1} & \phi_{2,2} & 0 & 0 & \ldots \\ & & & & & \\ \ldots & & & & & \end{pmatrix}$$

We show that indeed $\phi_{a,b} = 0$ for all $a < b \in J$ (i.e. the matrix is zero above the diagonal): Let $x \in X_a$, where x is arbitrary and non-zero, and $a \in J$ arbitrary. Then $x = \sum_{i\in I_a} r_i\epsilon_{a,i}$, a finite sum, where $r_i \in F$ for each $i \in I_a$. Therefore $x\phi = \sum_{i\in I_a} r_i(\epsilon_{a,i}\phi)$. However, by construction, $\epsilon_{a,i}\phi \in \langle E_0, E_1, \ldots, E_a\rangle$, for each $i \in I_a$. Therefore $x\phi \in \bigoplus_{j=0}^{a} X_j$. It follows that $\phi_{a,b} = 0$ for all $b > a$.

Now consider X_a where $a \in J$ is arbitrary. The basis for X_a is $\{\epsilon_{a,i}; i \in I_a\}$. We consider different cases with respect to the cardinality of I_a.

Case (a): $\mid I_a \mid = 1$:

In this case $\phi_{a,a} = c_a$ for some $c_a \in F$. Since F has the involution property $c_a = u_a + v_a$, where u_a is a unit of F and v_a is an involution of F.

Case (b): $\mid I_a \mid$ is countably infinite: In this case $\epsilon_{a,i}\phi_{a,a} = c_{a,i}\epsilon_{a,i+1}$, $0 \neq c_{a,i} \in F$, for each $i \in I_a$. We can represent this in matrix form as

$$\phi_{a,a} = \begin{pmatrix} 0 & c_{a,0} & 0 & \dots & & & \\ 0 & 0 & c_{a,1} & 0 & \dots & & \\ 0 & 0 & 0 & c_{a,2} & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & c_{a,4} & 0 & \dots \\ 0 & 0 & 0 & 0 & \dots & & \\ \dots & & & & & & \\ \dots & & & & & & \end{pmatrix}$$

We define $U_{a,a}$ and $V_{a,a}$, endomorphisms of X_a, as follows;

$$\epsilon_{a,i}U_{a,a} = \begin{cases} \epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1} & for \quad i \text{ even} \\ -\epsilon_{a,i} & for \quad i \text{ odd} \end{cases}$$

$$\epsilon_{a,i}V_{a,a} = \begin{cases} -\epsilon_{a,i} & for \quad i \text{ even} \\ \epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1} & for \quad i \text{ odd} \end{cases}$$

Notice at this point that $\phi_{a,a} = U_{a,a} + V_{a,a}$.

Let x be an arbitrary non-zero element of X_a. We can write $x = \sum_{j=k}^{m} x_j\epsilon_{a,j}$ a finite sum, where each $x_j \in F$ and $x_k \neq 0$ with $m, k \in \mathbb{N}$. Then $xU_{a,a} = \pm x_k\epsilon_{a,k} + \sum_{j=k+1}^{m+1} y_j\epsilon_{a,j}$ where $y_j \in F$ for each $j = k+1, \ldots, m+1$. Since x_k is non-zero then $xU_{a,a}$ is non-zero and therefore $U_{a,a}$ is injective.

Let $\epsilon_{a,i}$ be an arbitrary element of I_a.

When i is even then $\epsilon_{a,i}$ =$(\epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1})U_{a,a}$ and when i is odd then $\epsilon_{a,i} = -\epsilon_{a,i}U_{a,a}$ therefore $U_{a,a}$ is surjective. Therefore, $U_{a,a}$ is an automorphism of X_a.

Notice also that for i even $\epsilon_{a,i}V_{a,a}^2 = -\epsilon_{a,i}V_{a,a} = \epsilon_{a,i}$ and for i odd $\epsilon_{a,i}V_{a,a}^2$ =$(\epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1})V_{a,a} = \epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1} - c_{a,i}\epsilon_{a,i+1} = \epsilon_{a,i}$ which demonstrates that $V_{a,a}^2 = 1_{X_a}$, the identity in $E(X_a)$ and so is an involutary automorphism of X_a. Although unnecessary to the argument, one may note that in this case both $U_{a,a}$ and $V_{a,a}$ are involutary automorphisms of X_a.

Therefore we may write $\phi_{a,a} = U_{a,a} + V_{a,a}$ a sum of two automorphisms of X_a at least one of which is involutary. We represent this in matrix form as follows;

$$\phi_{a,a} = \begin{pmatrix} +1 & c_{a,1} & 0 & \dots & \\ 0 & -1 & 0 & 0\dots & \\ 0 & 0 & +1 & c_{a,3} & \dots \\ 0 & 0 & 0 & -1 & \dots \\ \dots & & & & \end{pmatrix} + \begin{pmatrix} -1 & 0 & 0 & \dots & & \\ 0 & +1 & c_{a,2} & 0 & & \dots \\ 0 & 0 & -1 & 0 & & \dots \\ 0 & 0 & +1 & c_{a,3} & 0\dots & \\ \dots & & & & & \end{pmatrix}$$

Case (c): $\mid I_a \mid = l + 1 > 1$, $l \in \mathbb{N}$: in this case $\phi_{a,a}$ may be described as

$$\epsilon_i \phi_{a,a} = \begin{cases} c_{a,i}\epsilon_{a,i+1} & for \quad i = 0, \dots, l-1 \\ \sum_{j=0}^{l} r_j \epsilon_{a,j} & for \quad i = l \end{cases}$$

where $0 \neq c_{a,i} \in F$, for each $i \in I_a$.

We may represent this in matrix form as follows;

$$\phi_{a,a} = \begin{pmatrix} 0 & c_{a,0} & 0 & \dots & \\ 0 & 0 & c_{a,1} & 0 & \dots \\ \dots & & & & \\ \dots & & & 0 & c_{a,l-1} \\ r_1 & r_2 & \dots & r_{l-1} & r_l \end{pmatrix}$$

Since F has the involution property then $r_l = u + v$; u, v units of F with

$v^2 = 1$.

For l odd, we define endomorphisms $U_{a,a}$ and $V_{a,a}$ of X_a as follows;

$$\epsilon_{a,i}U_{a,a} = \begin{cases} v\epsilon_{a,i} & for \quad i < l \text{ even} \\ -v\epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1} & for \quad i < l \text{ odd} \\ u\epsilon_{a,l} + \sum_{j=0}^{l-1} r_j\epsilon_{a,j} & for \quad i = l \end{cases}$$

$$\epsilon_{a,i}V_{a,a} = \begin{cases} -v\epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1} & for \quad i < l \text{ even} \\ v\epsilon_{a,i} & for \quad i < l \text{ odd} \\ v\epsilon_{a,l} & for \quad i = l \end{cases}$$

Let x be an arbitrary non-zero element of X_a. We can write $x = \sum_{j=k}^{l} x_j\epsilon_{a,j}$ where each $x_j \in F$ and $x_k \neq 0$ for some $k \in 0, 1, \ldots l$. By inspection of the definition for $U_{a,a}$ we can write $xU_{a,a} = \pm x_k v\epsilon_{a,k} + \sum_{j=k+1}^{l-1} y_j\epsilon_{a,j} + (x_l\epsilon_{a,l})U_{a,a}$ where each $y_j \in F$; if $x_l = 0$ then since $(x_l\epsilon_{a,l})U_{a,a} = 0$ and $x_k v \neq 0$ (i.e. $x_k v^2 = x_k$) so the coefficient of $\epsilon_{a,k}$ in $xU_{a,a}$ is non-zero, then $xU_{a,a} \neq 0$; if $x_l \neq 0$ then $xU_{a,a} \neq 0$ since $(x_l\epsilon_{a,l})U_{a,a}$ must have $x_l u \neq 0$ as coefficient for $\epsilon_{a,l}$. Therefore $U_{a,a}$ is injective.

By definition, for each $i < l$, i even, $(v^{-1}\epsilon_{a,i})U_{a,a} = \epsilon_{a,i}$; for $i < l$, i odd, $(-v^{-1}\epsilon_{a,i} + v^{-2}c_{a,i}\epsilon_{a,i+1})U_{a,a} = -v^{-1}(-v\epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1}) + v^{-1}c_{a,i}\epsilon_{a,i+1} = \epsilon_{a,i}$. Thus, for each $\epsilon_{a,i}$ with $i \in \{0, 1, \ldots, l-1\}$, we have shown that there exists some $z_i \in X_a$ such that $z_iU_{a,a} = \epsilon_{a,i}$. Now we can write

$u^{-1}\ (\epsilon_{a.l} - \sum_{j=0}^{l-1} r_j z_j)U_{a.a} = u^{-1}(u\epsilon_{a,l} + \sum_{j=0}^{l-1} r_j \epsilon_{a.j} - \sum_{j=0}^{l-1} r_j \epsilon_{a,j}) = \epsilon_{a.l}$. Hence we have shown $U_{a,a}$ to be surjective since it maps onto all the basis elements. Therefore $U_{a,a}$ is an automorphism of X_a.

Letting $i \in I_a$, arbitrary, and taking $i < l$ with i even, then $\epsilon_{a.i}V_{a.a}^2 = (-v\epsilon_{a.i} + c_{a.i}\epsilon_{a,i+1})V_{a.a} = v^2\epsilon_{a,i} - vc_{a,i}\epsilon_{a,i+1} + c_{a.i+1}v\epsilon_{a,i+1} = \epsilon_{a.i}$ since F is commutative and v is an involution; if $i < l$ with i odd then $\epsilon_{a,i}V_{a.a}^2 = v^2\epsilon_{a.i} = \epsilon_{a.i}$; if $i = l$ then $\epsilon_{a,l}V_{a.a}^2 = v^2\epsilon_{a.l} = \epsilon_{a.l}$. Therefore $V_{a.a}$ is an involutary automorphism of X_a.

By inspection it is also clear that $\phi_{a,a} = U_{a,a} + V_{a,a}$ a sum of two automorphisms of X_a, one of which is involutary. We illustrate this in matrix form as

$\phi_{a.a} =$

$$\begin{pmatrix} v & 0 & 0 & & \dots & \\ 0 & -v & c_{a.1} & \dots & 0 & \dots \\ \dots & \dots & \dots & & & \\ \dots & & & -v & c_{l-2} & 0 \\ \dots & & & 0 & v & 0 \\ r_1 & \dots & \dots & r_{l-2} & r_{l-1} & u \end{pmatrix} + \begin{pmatrix} -v & c_{a.0} & 0 & & \dots & 0 \\ 0 & v & 0 & & \dots & 0 \\ \dots & \dots & \dots & & & \\ \dots & & & v & 0 & 0 \\ 0 & \dots & \dots & 0 & -v & c_{a.l-1} \\ 0 & \dots & \dots & 0 & 0 & v \end{pmatrix}$$

For l even, we define endomorphisms $U_{a,a}$ and $V_{a,a}$ of X_a as follows;

$$\epsilon_{a,i}U_{a,a} = \begin{cases} -v\epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1} & for \quad i < l \text{ even} \\ v\epsilon_{a,i} & for \quad i < l \text{ odd} \\ u\epsilon_{a,l} + \sum_{j=0}^{l-1} r_j\epsilon_{a,j} & for \quad i = l \end{cases}$$

$$\epsilon_{a,i}V_{a,a} = \begin{cases} v\epsilon_{a,i} & for \quad i < l \text{ even} \\ -v\epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1} & for \quad i < l \text{ odd} \\ v\epsilon_{a,l} & for \quad i = l \end{cases}$$

Let x be an arbitrary non-zero element of X_a. We can write $x = \sum_{j=k}^{l} x_j\epsilon_{a,j}$ where each $x_j \in F$ and $x_k \neq 0$, for some $k \in 0, 1, \ldots, l$. By definition of $U_{a,a}$ we can write $xU_{a,a} = \pm x_k v\epsilon_{a,k} + \sum_{j=k+1}^{l-1} y_j\epsilon_{a,j} + (x_l\epsilon_{a,l})U_{a,a}$ where $x_l, y_j \in F$ for each $j \in k+1, \ldots, l-1$; if $x_l = 0$ then $(x_l\epsilon_{a,l})U_{a,a} = 0$ and since $x_k v \neq 0$ (i.e. $x_k v^2 = x_k$) the coefficient of $\epsilon_{a,k}$ in $xU_{a,a}$ is non-zero, so $xU_{a,a} \neq 0$; if $x_l \neq 0$ then $xU_{a,a} \neq 0$ since $(x_l\epsilon_{a,l})U_{a,a}$ must have $x_l u \neq 0$ as coefficient for $\epsilon_{a,l}$. Therefore $U_{a,a}$ is injective.

By definition, for each $i < l$ with i even, $(-v^{-1}\epsilon_{a,i} + v^{-2}c_{a,i}\epsilon_{a,i+1})U_{a,a} = -v^{-1}(-v\epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1}) + v^{-1}c_{a,i}\epsilon_{a,i+1} = \epsilon_{a,i}$; similarly for $i < l$ with i odd, $(v^{-1}\epsilon_{a,i})U_{a,a} = v^{-1}v\epsilon_{a,i} = \epsilon_{a,i}$. So for each $\epsilon_{a,i}$ with $i \in 0, 1, \ldots, l-1$ we have shown there exists some $z_i \in X_a$ such that $z_iU_{a,a} = \epsilon_{a,i}$. We can also write $u^{-1}\ (\epsilon_{a,l} - \sum_{j=0}^{l-1} r_j z_j)U_{a,a} = u^{-1}(u\epsilon_{a,l} + \sum_{j=0}^{l-1} r_j\epsilon_{a,j} - \sum_{j=0}^{l-1} r_j\epsilon_{a,j}) = \epsilon_{a,l}$. In this way, we have shown $U_{a,a}$ to be surjective since it maps onto all the basis elements. Therefore $U_{a,a}$ is an automorphism of X_a.

Let $i \in I_a$ arbitrary; if $i < l$ with i even, then $\epsilon_{a,i}V_{a,a}^2 = v^2\epsilon_{a,i} = \epsilon_{a,i}$; if $i < l$ with i odd, then $\epsilon_{a,i}V_{a,a}^2 = (-v\epsilon_{a,i} + c_{a,i}\epsilon_{a,i+1})V_{a,a} = v^2\epsilon_{a,i} - vc_{a,i}\epsilon_{a,i+1} + c_{a,i+1}v\epsilon_{a,i+1} = \epsilon_{a,i}$ since F is commutative and v is an involution; if $i = l$ then $\epsilon_{a,l}V_{a,a}^2 = v^2\epsilon_{a,l} = \epsilon_{a,l}$. Therefore $V_{a,a}$ is an involutary automorphism of X_a.

By inspection, $\phi_{a,a} = U_{a,a} + V_{a,a}$ and, as we have shown, a sum of two automorphisms of X_a, one of which is involutary. We illustrate this as

$\phi_{a,a} =$

$$\begin{pmatrix} -v & c_{a,1} & 0 & & \dots & 0 \\ 0 & v & 0 & & \dots & \dots \\ \dots & & & & & \\ 0 & \dots & & -v & c_{l-2} & 0 \\ 0 & 0 & & 0 & v & 0 \\ r_1 & \dots & \dots & r_{l-2} & r_{l-1} & u \end{pmatrix} + \begin{pmatrix} v & 0 & 0 & & \dots & 0 \\ 0 & -v & c_{a,2} & & \dots & \\ \dots & & & & & \\ 0 & \dots & & -v & 0 & 0 \\ 0 & \dots & & & -v & c_{a,l-1} \\ 0 & \dots & \dots & 0 & 0 & v \end{pmatrix}$$

So we have shown that, for each $a \in J$, $\phi_{a,a} = U_{a,a} + V_{a,a}$, where

$U_{a.a}, V_{a.a} \in Aut(X_a)$ and $(V_a)^2 = 1_a$ where 1_a is the identity in $E(X_a)$.

Recalling that $\phi = \sum_{\substack{a \geq b \\ a.b \in J}} \phi_{a.b}$ we may write $\phi = (\sum_{a \in J} U_{a.a} + \sum_{\substack{a > b \\ a.b \in J}} \phi_{a.b}) + \sum_{a \in J} V_{a.a}$.

Now, let $U = \sum_{a.b \in J} U_{a.b}$ where we set $U_{a.b} = \phi_{a.b}$ for all $b < a$ and $U_{a.b} = 0$ for all $a < b$, and, moreover, let $V = \sum_{a.b \in J} V_{a.b}$ where we set $V_{a.b} = 0$ for each $a \neq b \in J$. Then we can write $\phi = U + V$. We illustrate this in matrix form as

$\phi =$

$$\begin{pmatrix} V_{0.0} & 0 & 0 & \dots & \\ 0 & V_{1.1} & 0 & 0 & \dots \\ 0 & 0 & V_{2.2} & 0 & \dots \\ & & & & \\ \dots & & & & \end{pmatrix} + \begin{pmatrix} U_{0.0} & 0 & 0 & \dots & \\ U_{1.0} & U_{1.1} & 0 & 0 & \dots \\ U_{2.0} & U_{2.1} & U_{2.2} & 0 & \dots \\ & & & & \\ \dots & & & & \end{pmatrix}$$

Now, since X may be decomposed as $X = \bigoplus_{a \in J \subseteq I} X_a$ where $X_a = \bigoplus_{i \in I_a} Fe_i$ for each $a \in J$ such that $U_{a.a}, V_{a.a} \in Aut(X_a)$ for each a in J and such that $U_{a.b} = V_{a.b} = 0$ for each $a, b \in J$ with $0 \leq a < b$, we deduce by using Lemma 1.4 that both U and V are automorphisms of X.

Finally, V is an involutary automorphism of X since taking any arbitrary

$x \in X$ where $x = \sum_{a \in J} x_a$, a finite sum, where $x_a \in X_a$ for each $a \in J$ then $xV^2 = (\sum_{a \in J} x_a)V^2 = \sum_{a \in J}(x_a V_{a,a}^2) = \sum_{a \in J} x_a = x$ since $V_{a,a}^2 = 1_{X_a}$, where 1_{X_a} is the identity in X_a for each $a \in J$.

Therefore $\phi = U + V$ is a sum of an automorphism and an involutary automorphism of X. □

We extend our result for vector spaces to uncountable rank using the following theorem which we state it in more general form.

Theorem 2.2 *Let $M = \bigoplus_{\beta \in \kappa} Re_\beta$ be a free R-module of uncountable rank over R, a commutative unital ring. If every free R-module of countable rank greater than 1 has the property that every endomorphism is a sum of two automorphisms one being involutary, then M also has this property.*

Proof: We follow the proof of Theorem 1.9 of Chapter II exactly, with $n = 2$ and $m - 1 = 0$.

The only additional condition we impose is that for $\alpha < \beta$ assume $(\theta_{2,\alpha})^2 = 1_{H_\alpha}$ where 1_{H_α} is the identity in $E(H_\alpha)$. For $\beta = 0$, $H_0 = 0$ and therefore $\phi\restriction_{H_0} = 0 = 0 + 0$. Every endomorphism of H_0 is involutary, so this is correct.

In **Case 1** where β is a limit ordinal we need to show that $\bigcup_{\alpha < \beta} \theta_{2,\alpha}$ is involutary.

Let h be an arbitrary element of $H_\beta = \bigcup_{\alpha<\beta} H_\alpha$. Then there exists $\alpha < \beta$ such that $h \in H_\alpha$. Of course by construction $h(\theta_{2,\alpha})^2 = h$. Then since $\theta_{2,\beta} \restriction_{H_\alpha} = \theta_{2,\alpha}$ it follows that $(\theta_{2,\beta})^2 = 1_{H_\beta}$.

In **Case 2** $\beta = \alpha + 1$ is not a limit ordinal.

Since $2 \leq rk(C_\alpha) \leq \aleph_0$ then by assumption we can choose ψ_2 to be an involutary automorphism of C_α. This does not effect the procedure as followed in II, Theorem 1.9 but we do need to show that $\theta_{2,\alpha+1}$ is an involution of $H_{\alpha+1}$. Since $\theta_{2,\alpha+1}$ is defined by $(x+c)\theta_{2,\alpha+1} = x\theta_{2,\alpha} + c\psi_2$, where $x \in H_\alpha$ and $c \in C_\alpha$. Then

$$\begin{aligned}(x+c)(\theta_{2,\alpha+1})^2 &= (x\theta_{2,\alpha} + c\psi_2)(\theta_{2,\alpha+1}) \\ &= x(\theta_{2,\alpha})^2 + c(\psi_2)^2, \quad (\text{since } x\theta_{2,\alpha} \in H_\alpha \text{ and } c\psi_2 \in C_\alpha) \\ &= x + c.\end{aligned}$$

Lastly $\bigcup_{\beta<\kappa} \theta_{2,\beta}$ is an involution: Let h be an arbitrary element of $M = \bigcup_{\beta\in\kappa} H_\beta$. Then there exists $\beta \in \kappa$ such that $h \in H_\beta$. Of course by construction $h(\theta_{2,\beta})^2 = h$. It follows that $\bigcup_{\beta<\kappa} (\theta_{2,\beta})^2 = 1_M$ where 1_M is the identity in $E(M)$. □

Combining Theorem 1.3 and Theorem 2.1, and appealing to Theorem 2.2 we have proved,

Theorem 2.3 *Let F be a vector space. Every vector space over F has the involution property if and only if $\frac{1}{2} \in F$.*

§3 Completely decomposable groups

In this section we consider the involution property for completely decomposable groups. We begin by examining the property for rational groups.

Theorem 3.1 *Let G be a rational group with $E_{\mathbb{Z}}(G) = R$. Then G has the involution property if and only if $\frac{1}{2} \in R$ and $\mid X_R \mid \leq 1$*
(Recall $X_R = \{p \in \Pi \mid \frac{1}{p} \notin R\}$).

Proof: Note that the only elements of R which are involutions are 1 and -1.

Let $\frac{1}{2} \in R$ and $\mid X_R \mid = 0$. Then, by I, Lemma 2.11, $R = \mathbb{Q}$ 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 $\mid X_R \mid = 1$, in other words let $X_R = \{q\}$ for some $q \in \Pi \setminus \{2\}$, i.e. $R = \mathbb{Z}_{(q)}$. 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 $\mid X_R \mid > 1$, 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 I, Theorem 2.23) 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 a result for certain completely decomposable groups we introduce:

Lemma 3.2 *Let $G = A \bigoplus B$ be the direct sum of two arbitrary groups with $Hom(A,B) = 0$. Then G has the involution property if and only if 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 $\phi_{A.A} \in E(A)$, $\phi_{B.B} \in E(B)$, $\phi_{B.A} \in Hom(B,A)$.

By I, Lemma 3.1, ϕ is an automorphism of G if and only if $\phi_{A.A}$ and $\phi_{B.B}$ are automorphisms of A and B respectively. If ϕ is an involutary automorphism of G then by necessity $\phi_{A.A}\phi_{A.A} = 1_A$ where 1_A is the identity in $E(A)$ and $\phi_{B.B}\phi_{B.B} = 1_B$ where 1_B is the identity in $E(B)$. So $\phi_{A.A}$ and $\phi_{B.B}$ must be involutary automorphisms of A and B respectively if ϕ is an involutary automorphism.

Now assume that A does not have the involution property. Then there exists $\psi \in Hom(A, A)$ such that ψ is not a sum of an automorphism and an involutary autormorphism of A. Moreover, let ϕ be an arbitrary endomorphism of G such that $\phi_{A.A} = \psi$ using the same notation as above. This ϕ cannot be a sum of two automorphisms, one being involutary, of G since this would require ψ to be a sum of an automorphism and an involutary automorphism of A. Therefore G does not have the involution property.

The proof is similar if B does not have the involution property.

Conversely, if both A and B have the involution property then given any endomorphism $\theta \in E(G)$,

$$\theta = \begin{pmatrix} \theta_{A.A} & 0 \\ \theta_{B.A} & \theta_{B.B} \end{pmatrix} = \begin{pmatrix} \alpha_{A.A} & 0 \\ \theta_{B.A} & \alpha_{B.B} \end{pmatrix} + \begin{pmatrix} v_{A.A} & 0 \\ 0 & v_{B.B} \end{pmatrix}$$

where $\theta_{A.A} = \alpha_{A.A} + v_{A.A}$ is a sum of two automorphisms of A, $v_{A.A}$ being involutary, and where $\theta_{B.B} = \alpha_{B.B} + v_{B.B}$ is a sum of two automorphisms of B, $v_{B.B}$ being involutary. By I, Lemma 3.1, this is a sum of two automorphisms of G and the second is clearly involutary. □

For any reduced type there may be more than one type for which it is the reduced type, i.e. $(k_p)_{p \in \Pi}$, where $k_p = 0$ for each $p \in \Pi$ is a reduced type which is the reduced type for infinitely many distinct types. In this context the next simple remark is useful in the proof which follows it.

Remark 3.3 *Let G be a rational group with type t. If $\mid X_G \mid$ is finite then the reduced type of t is t itself.*

Theorem 3.4 *Let $G = \bigoplus_{t \in T_{cr}(G)} G_{(t)}$ be a completely decomposable group, where $G_{(t)}$ denotes the t-homogeneous component of G.*

Furthermore, let $\mathrm{rk}(G_{(t)}) = 1$ for each $t \in T_{cr}(G)$.

Then G has the involution property if and only if $\frac{1}{2} \in R^0_{(t)}$ and $\mid X_{R^0_{(t)}} \mid \leq 1$, for each $t \in T_{cr}(G)$, where $R^0_{(t)}$ denotes that subring of $\mathbb{Q}$ containing $\mathbb{Z}$ and having the reduced type of t.

Proof: By Proposition 1.1, G cannot have the involution property unless $2 \in Aut(G)$ and and if $2 \in Aut(G)$ then $2 \in Aut(G_{(t)})$ for each $t \in T_{cr}(G)$. Then, $\frac{1}{2} \in R^0_{(t)}$ for each $t \in T_{cr}(G)$. Therefore, we assume from here on in this proof that $\frac{1}{2} \in R^0_{(t)}$ for each $t \in T_{cr}(G)$.

Assume there exists $t' \in T_{cr}(G)$ such that $\mid X_{R^0_{(t')}} \mid > 1$ so, by Theorem 3.1, $G_{(t')}$ does not have the involution property. Now, let $A = \bigoplus_{\substack{t > t' \\ t \in T_{cr}(G)}} G_{(t)}$, $B = G_{(t')}$ and $C = \bigoplus_{\substack{t \not\geq t' \\ t \in T_{cr}(G)}} G_{(t)}$. Since a homomorphism cannot map an element onto an element of lesser or incomparable type we know that $Hom(A,B) = 0 = Hom((A \bigoplus B), C)$. By Lemma 3.2, since B does not have the involution property and $Hom(A,B) = 0$ then $A \bigoplus B$ does not have the involution property and then since $Hom((A \bigoplus B), C) = 0$, again using Lemma 3.2 , $(A \bigoplus B) \bigoplus C = G$ does not have the involution property.

Conversely, assume that $\mid X_{R^0_{(t)}} \mid \leq 1$, for each $t \in T_{cr}(G)$.

Following Remark 3.3 we note: since $\mid X_{R_{(t)}} \mid \leq 1$ for each distinct $t \in T_{cr}(G)$ then for each $p \in \Pi$ there can be at most one $t \in T_{cr}(G)$ and so $T_{cr}(G)$ is countable: each $t \in T_{cr}(G)$ is of reduced type. Now let $t_{\mathbb{Q}}$ be the type of $\mathbb{Q}$. Since $t_{\mathbb{Q}} > t$ for all $t \in T_{cr}(G) \backslash \{t_{\mathbb{Q}}\}$ then $Hom(G_{(t_{\mathbb{Q}})}, G_{(t)}) = 0$, for all $t \in T_{cr}(G) \setminus \{t_{\mathbb{Q}}\}$, and in fact, letting $G' = \bigoplus\limits_{t \in T_{cr}(G) \backslash \{t_{\mathbb{Q}}\}} G_{(t)}$, then $Hom(G_{(t_{\mathbb{Q}})}, G')= 0$. Since, by Theorem 3.1, each $G_{(t)}$, $t \in T_{cr}(G)$, has the involution property then if $\mid T_{cr}(G) \setminus \{t_{\mathbb{Q}}\} \mid \leq 1$ (i.e. $G' = G_{(t)}$ or 0, for some type t) then by Lemma 3.2 we are finished.

Let $\mid T_{cr}(G) \setminus \{t_{\mathbb{Q}}\} \mid > 1$. Since $\mid X_{R^0_{(t)}} \mid \leq 1$, for each $t \in T_{cr}(G)$, there is at most one symbol 0 within the type t. Then let t_1, t_2 be two arbitrary distinct types within $T_{cr}(G) \backslash \{t_{\mathbb{Q}}\}$. Then the 0 in the type t_1 corresponds to some prime p_1, and the 0 in t_2 to a prime $p_2 \neq p_1$. Since $t_1 \not\leq t_2$ and

$t_2 \not\leq t_1$, then certainly $Hom(G_{(t_1)}, G_{(t_2)}) = 0 = Hom(G_{(t_2)}, G_{(t_1)})$, for all $t_1, \neq t_2 \in T_{cr}(G) \setminus \{t_{\leq}\}$.

We now show that $E(G')$ has the involution property. Let ϕ' be an arbitrary endomorphism of G' then $\phi' = \sum_{t \in T_{cr}(G')} \phi_{t.t}$ where $\phi_{t.t} \in E(G_{(t)})$ for each $t \in T_{cr}(G) \setminus \{t_{\leq}\} = T_{cr}(G')$, since we have shown for all $t_1 \neq t_2 \in T_{cr}(G')$ that $\phi_{t_1.t_2} = 0$.

Since rk$G_{(t)} = 1$ for each $t \in T_{cr}(G')$, then by Theorem 3.1, we know for each $t \in T_{cr}(G')$ that $G_{(t)}$, has the involution property therefore for each $t \in T_{cr}(G')$ we may write $\phi_{t.t} = V_{t.t} + U_{t.t}$ for some $V_{t.t}, U_{t.t} \in Aut(G_{(t)})$ with $(V_{t.t})^2 = 1_{G_{(t)}}$ where $1_{G_{(t)}}$ is the identity in $E(G_{(t)})$. Let $U' = \sum_{t \in T_{cr}(G')} U_{t.t}$ and let $V' = \sum_{t \in T_{cr}(G')} V_{t.t}$. Recalling that $T_{cr}(G')$ is countable, then, by Lemma 1.4, both U' and V' are automorphisms of G'. Let $g = \sum_{t \in T_{cr}(G')} g_t$ be an arbitrary element of G' where $g_t \in G_{(t)}$ for each $t \in T_{cr}(G')$, then $g(V')^2 = (\sum_{t \in T_{cr}(G')} (g_t)V_{t.t})V'$ and since $(g_t)V_{t.t} \in G_{(t)}$ for each $t \in T_{cr}(G')$ we have $g(V')^2 = \sum_{t \in T_{cr}(G')} g_t {V_{t.t}}^2 = g$ thus V' is an involutary automorphism of G'. Therefore $\phi' = U' + V'$ is a sum of two automorphisms, one being involutary.

Now writing $G = G_{(t_{\leq})} \bigoplus G'$ and recalling that $Hom(G_{(t_{\leq})}, G')$= 0 then, by Lemma 3.2, G has the involution property as both G' and $G_{t_{\leq}}$ do. □

§4 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. We also consider torsion-complete p-groups giving a comprehensive result in this case. The line of approach is similar to that followed by researchers of the n–sum property previously (see [11]). We begin with a lemma.

Lemma 4.1 *Let E be a ring such that E is complete in its p-adic topology and where 2 is a unit in E. Let $\bar{E} = E/pE$.*

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.

Proof: Let E and $\bar{E}$ be as above. We prove the conclusion in two steps.

Step 1: For all $n \in \mathbb{Z}^+$ and x an arbitrary ring element we have;

$$1 = (x + (1-x))^{2n} = \sum_{j=0}^{2n} \begin{pmatrix} 2n \\ j \end{pmatrix} x^{2n-j}(1-x)^j, \text{ where as usual } \begin{pmatrix} \\ \end{pmatrix}$$

denotes a binomial coefficient.

So we define, for each $n \in \mathbb{Z}^+$, $f_n(x) = \sum_{j=0}^{n} \begin{pmatrix} 2n \\ j \end{pmatrix} x^{2n-j}(1-x)^j$. In this summation $2n - j \geq n$ for each term, so $f_n(x) \equiv 0 \bmod x^r$ for all $r \leq n$, $r \in \mathbb{Z}^+$. Now, rearranging $f_n(x)$ in the following way $f_n(x) = 1 - \sum_{j=n+1}^{2n} \begin{pmatrix} 2n \\ j \end{pmatrix} x^{2n-j}(1-x)^j$, we note that $j > n$ for each term so $f_n(x) \equiv 1 \bmod (x-1)^r$ for all $0 < r \leq n$, $r \in \mathbb{Z}^+$. Since the same congruences follow for $f_n^2(x)$ we then have:

$$f_n^2(x) \equiv f_n(x) \bmod x^r(x-1)^r \quad \text{for all } r \leq n,\ r \in \mathbb{Z}^+. \qquad (*)$$

Another consequence of these congruences is that we can write

$$f_n(x) \equiv f_r(x) \bmod x^r(x-1)^r \text{ for all } r \leq n-1,\ r \in \mathbb{Z}^+. \qquad (**)$$

Finally $f_1(x) = x^2 + 2(x)(1-x) = 2x - x^2$, so that

$$f_1(x) \equiv x \bmod x^2 - x. \qquad (***)$$

Step 2 We apply the results of Step 1 to E and $\bar{E}$.

We are given that $\mu^2 = 1_{\bar{E}}$ and that 2 is a unit of E(and also of $\bar{E}$). If we let $\epsilon = \frac{1}{2}(\mu + 1_{\bar{E}})$ then ϵ is an idempotent of $\bar{E}$, i.e. $\epsilon^2 = \epsilon$.

Now choose $a \in E$ such that $\bar{a} = \epsilon$. Then $\overline{(a^2 - a)} = \epsilon^2 - \epsilon = 0$, so $(a^2 - a) \in pE$. Therefore $a^{n-1}(a - 1_E)^{n-1} \in p^{n-1}E$ for all $n \in \mathbb{Z}^+$. This along with congruence (**) gives us $f_n(a) - f_{n-1}(a) \in p^{n-1}E$ for all $n \in \mathbb{Z}^+$. Therefore $f_n(a)$ is a cauchy sequence and hence $\lim_{n \to \infty} f_n(a) = e \in E$ since E is complete.

The congruence (*) gives us $f_n^2(a) - f_n(a) \in p^nE$ for all $n \in \mathbb{Z}^+$. so in the limit this implies that $e^2 - e = 0$. Therefore e is an idempotent.

Combining congruences (**) and (***) we get that $f_n(a) \equiv f_1(a) \equiv a \bmod a(a - 1_E)$ which means $f_n(a) - a \equiv 0 \bmod a(a - 1_E)$ and since $a(a - 1_E) \in pE$ then $f_n(a) - a \in pE \quad$ for all $n \in \mathbb{Z}^+$. Since $\{f_n(a) - a\}$ is a cauchy sequence in pE and pE is complete, then in the limit $e - a \in pE$ so $\bar{e} = \bar{a} = \epsilon$.

Choose $i = 2e - 1_E$ an involutary element of E since $i^2 = (2e - 1_E)^2 = 4e^2 - 4e + 1_E = 1_E$.

Then finally $\bar{i} = 2\bar{e} - 1_{\bar{E}} = 2\epsilon - 1_{\bar{E}} = 2((\frac{1}{2})(\mu + \bar{1}_E)) - \bar{1}_E = \mu$. □

Theorem 4.2 *Let E be a ring such that E is complete in its p-adic topology, with 2 a unit of E, and such that $J(E)= pE$.*

If E/pE has the involution property then E also has this property .

Proof:

Take an arbitrary $\theta \in E$. We are given $(\theta + pE) = (\alpha + pE) + (\beta + pE)$ where $(\alpha + pE)$ is a unit of E/pE, and $(\beta + pE)$ is an involution of E/pE.

By Lemma 4.1 there exists i, an involutary element of E, such that $(i + pE) = (\beta + pE)$. Therefore we can write $\theta = (\alpha + p\gamma) + i$ for some $\gamma \in E$.

Now we show that $(\alpha + p\gamma)$ is a unit of E.

$(\alpha + pE) = ((\alpha + p\gamma) + pE)$ is a unit of E/pE. Therefore there exists $\phi \in E$ such that $(\phi + pE)$ is a right inverse of $((\alpha + p\gamma) + pE)$. It follows that $(\alpha + p\gamma)\phi - 1_E \in pE = J(E)$, where 1_E is the identity in E. Then by the properties of the Jacobson Radical (see I, Proposition 2.19) $(\alpha + p\gamma)\phi$ is a unit in E. Writing $(\alpha + p\gamma)(\phi((\alpha + p\gamma)\phi)^{-1}) = 1_E$ we see that $(\alpha + p\gamma)$ has a right inverse. A similar argument shows $(\alpha + p\gamma)$ also has a left inverse . Therefore $(\alpha + p\gamma)$ is a unit in E. □

Lemma 4.3 *Let $M = \bigoplus_{i \in I} J_p e_i$ $(p \in \Pi)$, be a reduced torsion-free p-adic module of non-trivial rank. Let $\widehat{M}$ be the p-adic completion of M. Then*

$$\frac{E(\widehat{M})}{pE(\widehat{M})} \underset{ring}{\cong} \frac{E(M)}{pE(M)}.$$

Proof: Letting $x \in \widehat{M}$ then $x = \sum\limits_{j=0}^{\infty} p^j m_j$, $m_j \in M$.

$\frac{\widehat{M}}{M}$ is divisible since, for any $x \in \frac{\widehat{M}}{M}$, writing $x = \sum\limits_{j=0}^{\infty} p^j m_j + M$, $m_j \in M$, then $x = \sum\limits_{j=0}^{n-1} p^j m_j + \sum\limits_{j=n}^{\infty} p^j m_j + M$ for any arbitrary $n \in \mathbb{N}$, so that $x = \sum\limits_{j=n}^{\infty} p^j m_j + M = p^n \sum\limits_{j=0}^{\infty} p^j m_{n+j} + M = p^n y + M$ for some $y \in \widehat{M}$.

$\frac{\widehat{M}}{M}$ is torsion–free since, for any $x \in \frac{\widehat{M}}{M}$, $x = \sum\limits_{j=0}^{\infty} p^j m_j + M$, $m_j \in M$ with $p^r x \equiv 0 \bmod M$, for some $r \in \mathbb{N}$, then $(p^r \sum\limits_{j=0}^{\infty} p^j m_j + M) = M$, which means that $= \sum\limits_{j=0}^{\infty} p^{r+j} m_j \in M$ but since M contains only finite sums of $p^j m_j$ then $\sum\limits_{j=0}^{\infty} p^{r+j} m_j \in M$ and so $x \in M$.

Now consider the short exact sequence

$$0 \longrightarrow M \longrightarrow \widehat{M} \longrightarrow \frac{\widehat{M}}{M} \longrightarrow 0.$$

By a theorem of Cartan Eilenberg (see [7, Theorem 44.4]), this induces the exact sequence

$$\begin{gathered} 0 \longrightarrow Hom(M, M) \longrightarrow Hom(M, \widehat{M}) \longrightarrow Hom(M, \frac{\widehat{M}}{M}) \longrightarrow \\ Ext(M, M) \longrightarrow Ext(M, \widehat{M}) \longrightarrow Ext\big(M, \frac{\widehat{M}}{M}\big) \longrightarrow 0. \end{gathered}$$

Now, as M is free then, by [7, Theorem 14.4], $Ext(M, M) = 0$ and so we get the short exact sequence

$$0 \longrightarrow Hom(M, M) \longrightarrow Hom(M, \widehat{M}) \longrightarrow Hom(M, \frac{\widehat{M}}{M}) \longrightarrow 0.$$

M is dense in $\widehat{M}$ so every member of $Hom(M, \widehat{M})$can be uniquely extended to an endomorphism of $\widehat{M}$ so we rewrite our short exact sequence as

$$0 \longrightarrow Hom(M,M) \longrightarrow Hom(\widehat{M},\widehat{M}) \longrightarrow Hom\big(M,\frac{\widehat{M}}{M}\big)\longrightarrow 0.$$

Also, by [7, Theorem 43.1], $Hom\big(\bigoplus_{i\in I} J_p,\frac{\widehat{M}}{M}\big) \cong \prod_{i\in I} Hom\big(J_p, \frac{\widehat{M}}{M}\big)$ and so we have $\prod_{i\in I} Hom\big(J_p, \frac{\widehat{M}}{M}\big)\cong \prod_{i\in I}\frac{\widehat{M}}{M}$, since $\sigma : J_p \longrightarrow\frac{\widehat{M}}{M}$ is uniquely determined by $(1)\sigma$. So

$$0 \longrightarrow Hom(M,M) \longrightarrow Hom(\widehat{M},\widehat{M}) \longrightarrow \prod_{i\in I}\frac{\widehat{M}}{M}\longrightarrow 0,$$

where $\mid I \mid$ is the rank of M. From this we get $\prod_{i\in I}\frac{\widehat{M}}{M}\cong\frac{Hom(\widehat{M},\widehat{M})}{Hom(M,M)}$, which makes $\frac{Hom(\widehat{M},\widehat{M})}{Hom(M,M)}$ torsion free and divisible. Since $\frac{Hom(\widehat{M},\widehat{M})}{Hom(M,M)}$ is torsion free then $Hom(M,M)$ is pure in $Hom(\widehat{M},\widehat{M})$.

Given any $\phi \in E(\widehat{M})$, using the divisibility of $\frac{E(\widehat{M})}{E(M)}$, we can write $\phi = \theta + p\phi_1$ for some $\theta \in E(M)$ and some $\phi_1 \in E(\widehat{M})$.

Define $\chi : E(\widehat{M}) \longrightarrow\frac{E(M)}{pE(M)}$ by $\phi\chi = \theta + pE(M)$. Let $\phi = \theta + p\phi_1 = \theta' + p\phi'$. Then $\theta - \theta' \in pE(\widehat{M}) \cap pE(M) = pE(M)$ by purity of $E(M)$ in $E(\widehat{M})$. Therefore $\theta \equiv \theta' \bmod pE(M)$. Therefore χ is well defined.

Now take any ϕ, $\phi' \in E(\widehat{M})$ then $\phi\chi + \phi'\chi = \theta + \theta' + pE(M)$ for suitable θ,$\theta' \in E(M)$ such that $\phi = \theta + p\psi$ and $\phi' = \theta' + p\psi'$, where ψ,$\psi' \in E(\widehat{M})$. Therefore $(\phi + \phi')\chi = (\theta + \theta') + pE(M) = \phi\chi + \phi'\chi$.

Also, using the same arbitrary ϕ,ϕ' as described above

$\phi\phi' = \theta\theta' + \theta p\psi' + p\psi\theta' + p\psi p\psi' \equiv \theta\theta' \bmod pE(\widehat{M})$. Therefore $(\phi\phi')\chi =$

$\theta\theta' + pE(M) = (\theta + pE(M))(\theta' + pE(M)) = (\phi\chi)(\phi'\chi)$. Hence we have shown that χ is a ring homomorphism.

Let $\phi\chi = 0$, for some $\phi \in E(\widehat{M})$, then for any $\theta \in E(M)$, $\psi \in E(\widehat{M})$ such that $\phi = \theta + p\psi$, it follows that $\theta \in pE(M)$. Therefore $\ker(\chi) = pE(\widehat{M})$. χ is surjective since letting $\theta + pE(M)$ be an arbitrary element of $\dfrac{E(M)}{pE(M)}$ and choosing any $\psi \in E(\widehat{M})$ then $(\theta + p\psi)\chi = \theta + pE(M)$.

Now by the First Isomorphism Theorem,

$$\frac{E(\widehat{M})}{pE(\widehat{M})} \underset{ring}{\cong} \frac{E(M)}{pE(M)}.$$

□

The next result is due to Goldsmith, Pabst and Scott [11].

Lemma 4.4 *Let $M = \bigoplus_{i \in I} J_p e_i$, where $p \in \Pi$, be a torsion-free p-adic module. Then $E(M)/pE(M) \underset{ring}{\cong} E(M/pM)$.*

Proof: See [11, Proposition 2.6.] □

Theorem 4.5 *Let $M = \bigoplus_{i \in I} J_p e_i$, where $p \in \Pi$, be a reduced torsion-free p-adic module. Let $\widehat{M}$ be the p-adic completion of M. Then $\widehat{M}$ has the involution property if and only if $p \neq 2$.*

Proof: If $p = 2$ then $2 \notin Aut(\widehat{M})$ so, by Proposition 1.1, $\widehat{M}$ does not have the involution property.

Now assume $p \neq 2$. Since M/pM is a vector space over $\mathbb{Z}_p$, the integers modulo p, then by Theorem 2.3, it is evident that $E(M/pM)$ has the involution property. By Lemma 4.3 and Lemma 4.4, we have $\frac{E(\widehat{M})}{pE(\widehat{M})} \underset{ring}{\cong} \frac{E(M)}{pE(M)} \underset{ring}{\cong} E(M/pM)$. These being ring isomorphisms $\frac{E(\widehat{M})}{pE(\widehat{M})}$ also has the involution property. Since, by I, Lemma 2.20, $J(E(\widehat{M})) = pE(\widehat{M})$, it follows, by Theorem 4.2, that $E(\widehat{M})$ and therefore $\widehat{M}$ has the involution property if and only if $p \neq 2$. $\square$

We now consider the involution property in relation to the torsion completion of a p-group B. Let $B = \bigoplus_{n<\omega} B_n$ be a direct sum of cyclic groups where each B_n is a direct sum of cyclic groups of order p^{n+1}. By the *torsion completion* of B we mean the torsion part, $T(\widehat{B})$, of the p-adic completion, $\widehat{B}$, of B and we denote the torsion completion of B by $\bar{B}$. Then, for any $n \in \mathbb{N}$, $\bar{B} = (\bigoplus_{k<n} B_k) \bigoplus C_n$, where $C_n = \left\langle p^n\bar{B}, \bigoplus_{n\leq k<\omega} B_k \right\rangle$. Let π_n be the canonical projection of $\bar{B}$ onto C_n. Define $\rho_n = \pi_n - \pi_{n+1}$. Then ρ_n is a projection of $\bar{B}$ onto B_n.

Now define the mapping λ_n from $E(\bar{B})$ to $E(B_n[p])$ as $x(\phi\lambda_n) =: (x\phi)\rho_n$ for each $x \in B_n[p]$ and each $\phi \in E(\bar{B})$.

The following two lemmas are due to Castagna [3].

Lemma 4.6 *λ_n is a ring homomorphism of $E(\bar{B})$ onto $E(B_n[p])$.*

Proof: Let $\phi \in E(\bar{B})$ then $\phi\lambda_n$ maps $B_n[p]$ to $B_n[p]$. Note also that $x \in C_n[p]$ implies that $x\phi \in C_n[p]$. Let ψ also be an arbitrary element of $E(\bar{B})$. Then λ_n is a group homomorphism since for any $x \in B_n[p]$, $x((\phi + \psi)\lambda_n) = x(\phi + \psi)\rho_n = (x\phi)\rho_n + (x\psi)\rho_n = x(\phi\lambda_n) + x(\psi\lambda_n)$.

For any $n \in \mathbb{N}$, where $B_n \neq 0$, we may write $B_n = \bigoplus\limits_{i \in I_n} \mathbb{Z}_{p^{n+1}} e_i$. Then for any arbitrary $i \in I_n$, $(p^n e_i)\phi = \sum\limits_{j \in I_n} \alpha_{i,j} p^n e_j + y$, where $y \in C_{n+1}[p]$. Thus $(p^n e_i)(\phi\lambda_n) = \sum\limits_{j \in I_n} \alpha_{i,j} p^n e_j$ and so $(p^n e_i)\phi = (p^n e_i)(\phi\lambda_n) + y$. Therefore $(p^n e_i)(\phi\psi\lambda_n) = (p^n e_i\phi\psi)\rho_n = ((p^n e_i)\phi\lambda_n\psi + y\psi)\rho_n = (p^n e_i)(\phi\lambda_n)(\psi\lambda_n)$.

Thus λ_n is a ring homomorphism. □

Lemma 4.7

Define $\lambda : E(\bar{B}) \longrightarrow \prod\limits_{n<\omega} E(B_n[p])$ by $\lambda : \phi \longmapsto (\phi\lambda_0, \phi\lambda_1, \ldots, \phi\lambda_n, \ldots)$. Then λ is a ring epimorphism.

Proof: Since each λ_n is a ring homomorphism of $E(\bar{B})$ into $E(B_n[p])$, for each $n \in \mathbb{N}$, then by the properties of ring direct products λ is a ring homomorphism also.

Let $(\phi'_0, \phi'_1, \ldots, \phi'_n, \ldots) \in \prod\limits_{n<\omega} E(B_n[p])$, where $\phi'_n \in E(B_n[p])$, for each n. Extend ϕ'_n to $\phi''_n \in E(B_n)$ in the usual way.

If $x \in \bar{B}$ then $x = \lim\limits_{m \longrightarrow \infty} \sum\limits_{k<m} x\rho_k$ the limit being taken in the p-adic

topology. Hence the elements $\sum_{k<m} x\rho_k\phi''_k$, $m = 1, 2, \ldots$ form a cauchy sequence in $\bar{B}$ with bounded order. Now define $x\phi \in E(\bar{B})$ to be the limit of this sequence.

If $x \in B_n[p]$ then $x\phi = x\phi'_n \in B_n[p]$ and hence $(\phi'_0, \phi'_1, \ldots, \phi'_n, \ldots) = \phi\lambda$.

□

We include two results by Pierce [22].

Lemma 4.8 *Let G be a p-group with no non-zero elements of infinite height. Let $H(G) = \{\phi \in E(G) | h(x\phi) > h(x)$ for each $x \in G[p], x \neq 0\}$. Then $H(G) = J(E(G))$ if and only if the following condition is satisified: For each $x \in G[p]$ and each $\phi \in H(G)$, setting $y_n = x + x\phi + \ldots + x\phi^{n-1}$ where $n \in \mathbb{N}$, there exists a $y \in G$ such that $h(y - y_n) \longrightarrow \infty$ as $n \longrightarrow \infty$.*

Proof: See [22, Lemma 14.5]. □

Lemma 4.9 *Let $B = \bigoplus_{n<\omega} B_n$ be a direct sum of cyclic groups where each B_n is a direct sum of cyclic groups of order p^{n+1}. Let $\bar{B}$ denote the torsion completion of B.*

Let $H(G) = \{\phi \in E(G) | h(x\phi) > h(x)$ for each $x \in G[p], x \neq 0\}$. Then $H(G) = J(E(G))$.

Proof: Let x be an arbitrary element of $G[p]$ and ψ an arbitrary element of $H(\bar{B})$ and consider the sequence $(y_n)_{n\in\omega}$ where $y_n = x+x\psi+x\psi^2+\ldots+x\psi^{n-1}$. Since ψ is a height increasing endomorphism then $x\psi^n \in p^nG$ for each $n \in \mathbb{N}$ so for any $n_1 < n_2 \in \mathbb{N}$ it follows that $y_{n_1} - y_{n_2} = -x\psi^{n_1} - \ldots - x\psi^{n_2-1} \in p^{n_1}G$. Therefore $(y_n)_{n\in\omega}$ is a cauchy sequence and so converges to some $y \in \widehat{B}$. Since, for any $n \in \mathbb{N}$, $p(x\psi^n) = (px)\psi^n = 0$ then the sequence $(py_n)_{n\in\omega}$ is cauchy and so converges to $py = 0$ so y is a torsion element of $\widehat{B}$ therefore $y \in \bar{B}$. Since $y - y_n \in p^nG$ for each $n \in \mathbb{N}$ then $h(y-y_n) \longrightarrow \infty$ as $n \longrightarrow \infty$. The result follows directly from Lemma 4.8. □

The above leads us to this useful lemma by Castagna:

Lemma 4.10 *Let $B = \bigoplus_{n<\omega} B_n$ be a direct sum of cyclic groups where each B_n is a direct sum of cyclic groups of order p^{n+1}. Let $\bar{B}$ denote the torsion completion of B. Then*

$$E(\bar{B})/J(E(\bar{B})) \underset{ring}{\cong} \prod_{n<\omega} E(B_n[p]).$$

Proof: Let λ be defined as in Lemma 4.7. We must prove $\ker(\lambda) = J(E(\bar{B}))$.

Suppose $\phi\lambda = 0$ for some $\phi \in E(\bar{B})$. Then, for each $n \in \mathbb{N}$ and each $x \in B_n[p]$, $x\phi \in C_{n+1}[p]$. Hence, if $x \neq 0$, $h(x\phi) > h(x)$. Hence $\phi \in$

$H(\bar{B}) = \{\phi \in E(\bar{B}) | h(x\phi) > h(x)$ for each $x \in \bar{B}[p], x \neq 0\}$.

Conversely if $\phi \in H(\bar{B})$ then $\phi\lambda = 0$, i.e. for $x \in B_n[p]$ then $x\phi \in C_{n+1}$ so $x(\phi\lambda)= 0$. It follows that ker$(\lambda)= H(\bar{B})$ and then, by Corollary 4.9, that $H(E(\bar{B}))= J(E(\bar{B}))$ and the result then follows. □

We are now ready for our final result.

Theorem 4.11 *Let $B = \bigoplus_{n<\omega} B_n$ be a direct sum of cyclic groups where each B_n is a direct sum of cyclic groups of order p^{n+1}. Let $\bar{B}$ denote the torsion completion of B. Then $\bar{B}$ has the involution property if and only if $p \neq 2$.*

Proof: If $p = 2$ then $2 \notin Aut(B)$ so, by Proposition 1.1, B does not have the involution property.

Let $p \neq 2$. In Lemma 4.10 we noted that $E(\bar{B})/J(E(\bar{B})) \underset{ring}{\cong} \prod_{n<\omega} E(B_n[p])$. Each $B_n[p]$ is a vector space . Therefore, by Theorem 2.3, $E(B_n[p])$ ($p \neq 2$) has the involution property. It is clear that the involution property is inherited by ring direct products. Therefore the quotient ring $E(\bar{B})/J(E(\bar{B}))$ has the property. It follows then by Theorem 4.2 that $E(\bar{B})$ has the property and so also $\bar{B}$. □

References

[1] R. Baer, *Abelian groups without elements of finite order*, Duke Math. J. **3** (1937), 68–122.

[2] V. P. Camillo, H. -P. Yu, *Exchange rings ,units and idempotents*, Comm. Alg. **22** (1994), 4737–4749.

[3] F. Castagna, *Sums of automorphisms of a primary abelian group*, Pacific J. Math. (3) **27** (1968), 463–473.

[4] P. M. Cohn, Algebra **I**, John Wiley and Sons, London-New York-Sidney-Toronto (1974).

[5] A. L. S. Corner, B. Goldsmith, *Isomorphic automorphism groups of torsion-free p-adic modules*, Abelian Groups, Module Theory, and Topology, Lecture Notes in Pure and Applied Mathematics **201**, (1998), 125–130.

[6] H. Freedman, *On endomorphisms of primary abelian groups*, J. London Math. Soc. **43** (1968), 305–307.

[7] L. Fuchs, Infinite Abelian Groups **I**, Academic Press, New York (1970).

[8] L. Fuchs, Infinite Abelian Groups **II**, Academic Press, New York (1973).

[9] L. Fuchs, *Recent results and problems on abelian groups*, Topics in Abelian Groups, Chicago (1963), 9–40.

[10] 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.

[11] B. Goldsmith, S. Pabst, A. Scott, *Unit sum numbers of rings and modules*, Quart. J. Math. Oxford **49** (1998), 331–344.

[12] L. C. Grove, Algebra, Academic Press, San Diego (1983).

[13] P. Hill, *Endomorphism rings generated by units*, Trans. Amer. Math. Soc. **141** (1969), 99–105.

[14] I. Kaplansky, Infinite Abelian Groups, The University of Michigan Press (1962).

[15] D. N. Lehmer, List of Prime Numbers from 1 to 10,006,751, Hafner Publishing Co., New York (1956).

[16] H. Leptin, *Abelsche p-Gruppen und ihre Automorphismengruppen*, Math. Z. **73** (1960), 235–253.

[17] W. Liebert, *Isomorphic automorphism groups of primary abelian groups*, in Abelian Group Theory, Proceedings of the 1985 Oberwolfach Conference, New York (1987), 9–31.

[18] M. B. Nathanson, Additive Number Theory: The Classical Bases, Graduate Texts in Mathematics **164** , Springer-Verlag, New York (1996).

[19] W. K. Nicholson, *Strongly clean rings and Fitting's Lemma*, Comm. Algebra **27** (1999), 3583–3592.

[20] A. Opdenhövel, *Über Summen zweier Automorphismen von Moduln*, Ph.D. thesis, Universität Essen (1999).

[21] M. Ó Searcóid, *Perturbation of linear operators by idempotents*, IMS Bulletin **39** (1997), 10–13.

[22] R. S. Pierce, *Homomorphisms of primary abelian groups*, Topics in Abelian Groups, Chicago (1963), 215–310.

[23] K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin (1957).

[24] O. Ramaré, R. Rumely, *Primes in arithmetic progressions*, Math. Comp. **65** (1996), 397–425.

[25] C. E. Rickert, *Isomorphic groups of linear transformations*, Amer. J. Math. **72** (1950), 451–464.

[26] H. Riesel, R. C. Vaughan, *On sums of primes*, Ark. Mat. **21** (1983), 45–74.

[27] A. Scott, *Endomorphisms and automorphisms of abelian groups and modules*, Thesis, Dublin Institute of Technology (1997).

[28] L. Strüngmann, *Does the automorphism group generate the endomorphism ring in Rep*(S, R)*?*, J. Algebra **231** (2000), 163–179.

[29] C. Wans, *Summen von Automorphismen für Moduln*, Thesis, Universität Essen (1995).

[30] D. Zelinsky, *Every linear transformation is a sum of nonsingular ones*, Proc. Amer. Math. Soc. **5** (1954), 627–630.