Proceedings of the Royal Society of Edinburgh, **139A**, 1275–1287, *2009*

Decompositions of groups of invertible elements in a ring

Petar Pavešić
Fakulteta za Matematiko in Fiziko, Univerza v Ljubljani,
Jadranska 19, 1111 Ljubljana, Slovenia
(petar.pavesic@fmf.uni-lj.si)

(MS received 12 November 2008; accepted 11 March 2009)

We describe decompositions of the group of units of a ring and of its subgroups, induced by idempotents with certain properties. The results apply to several classes of rings, most notably to semi-perfect rings.

1. Introduction

The main aim of this paper is to explain how idempotent elements in a ring induce decompositions of the group of invertible elements and of its subgroups. The role of idempotents in the decomposition of individual invertible elements is well established in the literature, whereas simultaneous decompositions of entire groups of invertible elements are less frequent. We are going to extend the line of thought developed by Putcha [8, 9] and by Cohen and Koh [2] and improve some of their results.

Our approach is somewhat different from the works mentioned as we use the adjoint group induced by the circle product in a ring. This method turns out to be surprisingly effective as it allows short and elegant proofs of results which are general enough to include the group of units of a semi-perfect ring, the congruence groups and other important examples (see also [7] for an application to stable homotopy theory).

Let R be a ring. If R is unital, we denote by r^* the inverse, when it exists, of an element $r \in R$, and by R^* the group of all invertible elements of the monoid $(R, \cdot)$. It turns out that, for the purposes we have in mind, the study of R^* and its subgroups assumes a much simpler and more natural form when expressed in terms of the circle product on R. This product is defined by $x \circ y := x + y + xy$, it is associative with 0 as its neutral element, and hence $(R, \circ)$ is a monoid. If r is invertible with respect to the circle product, then we denote its inverse by r°: it is uniquely determined by the equations $r + r^\circ + rr^\circ = r + r^\circ + r^\circ r = 0$. A subset $M \subseteq R$, which is a group with respect to the circle product, is denoted for emphasis by M°. A partial exception to this is R°, which denotes the group of all invertible elements of $(R, \circ)$. When R is unital, the map $r \mapsto r - 1$ defines an isomorphism of monoids $(R, \cdot)$ and $(R, \circ)$ and hence a bijective correspondence between subgroups of R^* and R°.

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

We will determine when a group of invertible elements in R can be written as a product of its subgroups. This is to say, given a group G and subgroups A, B we will write $G = A \cdot B$ if every $g \in G$ can be uniquely factorized as $g = ab$, where $a \in A$ and $b \in B$. Equivalently, $G = A \cdot B$ if $G = \{ab \mid a \in A,\ b \in B\}$ and the intersection of A and B is trivial. If B is a normal subgroup of G, then $A \cdot B$ is simply the semi-direct product $A \ltimes B$. Note that, in general, the product $A \cdot B$ of two subgroups A, B of G is a subgroup of G if and only if $A \cdot B = B \cdot A$ as sets [1, theorem 3.1.1]. In particular, $G = A \cdot B$ is equivalent to $G = B \cdot A$.

The paper is organized as follows. In § 2 we study subsets $M \subseteq R$, which are groups with respect to the circle product. The main results are theorems 2.4 and 2.7. The first of these says that if some complete set of orthogonal idempotents $e_1, \dots, e_n$ (i.e. $e_1 + \cdots + e_n = 1$) preserves M (in the sense that $e_i M \subseteq M$ for all i), then M° is the product of its subgroups $(e_i M)^\circ$. Moreover, if $Me_i \subseteq M$ for all i, then the second theorem describes another decomposition of M°, which recalls the factorization of matrices into a product of lower- and upper-triangular matrices. In § 3 we present applications of these results to the group of all invertible elements, to groups associated with quasi-invertible ideals, to congruence groups of matrices and to semi-perfect rings.

One final remark: an important goal of the paper is to demonstrate that the most natural approach to the decomposition problem is through the circle product and the adjoint group. Indeed, in this context the computations are considerably streamlined (so as to become almost trivial) and the results assume a very elegant form. The price for such a simplification is also evident: the reader may find it difficult to follow the guesswork hidden behind the proofs. We hope that the final result is worth the trouble.

2. Decompositions of circle groups

Throughout this section, let M be a subset of a ring R such that M° is a group. Given an idempotent $e \in R$ we say that e *preserves* M if $eM \subseteq M$. See § 3.1 for some typical examples of such M. We shall consider two types of decomposition: the symmetric and the LDU.

2.1. Symmetric decomposition

Proposition 2.1. *If an idempotent, e, preserves M, then eM is a group with respect to the $\circ$-product.*

Proof. It suffices to prove that eM is closed for $\circ$-products and $\circ$-inverses. Given $em, em' \in eM$, we have

$$(em) \circ (em') = em + em' + emem' = e(m \circ (em')) \in eM.$$

Moreover,

$$(e(em)^\circ) \circ (em) = e(em)^\circ + em + e(em)^\circ(em) = e((em)^\circ \circ (em)) = 0$$

implies that the inverse of em is of the form $e(em)^\circ$, which is in eM. □

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

Let u, v be orthogonal idempotents which preserve M. The formula

$$(u+v)m = (u(m \circ (vm)^\circ)) \circ (vm)$$

follows by direct computation. It shows that $u+v$ also preserves M and that $((u+v)M)^\circ$ is a group which is contained in the product $(uM)^\circ \cdot (vM)^\circ$. Moreover, since the groups $(uM)^\circ$ and $(vM)^\circ$ have trivial intersection, we have the following proposition.

Proposition 2.2. *If u, v are orthogonal idempotents which preserve M, then*

$$((u+v)M)^\circ = (uM)^\circ \cdot (vM)^\circ.$$

Remark 2.3. If R is unital, and if u is an idempotent which preserves M, then its complement $v = 1 - u$ also preserves M, since

$$(um^\circ) \circ m = um^\circ + (u+v)m + um^\circ m = u(m^\circ \circ m) + vm = vm.$$

It follows that every $m \in M$ admits a canonical decomposition $m = (um^\circ)^\circ \circ (vm)$, and that $M^\circ = (uM)^\circ \cdot (vM)^\circ$.

The inductive application of proposition 2.2 yields the *symmetric decomposition* of the group M°.

Theorem 2.4. *If $e_1, \dots, e_n$ is a set of orthogonal idempotents which preserve M, then*

$$(e_1 + \cdots + e_n)M^\circ = (e_1M)^\circ \cdot \cdots \cdot (e_nM)^\circ.$$

In particular, if $e_1, \dots, e_n$ is a complete set of orthogonal idempotents, then we obtain the product decomposition $M^\circ = (e_1M)^\circ \cdot \cdots \cdot (e_nM)^\circ$.

The factors of the symmetric decomposition can be further analysed by means of the map

$$\varphi \colon (eM)^\circ \to (eMe)^\circ, \quad x \mapsto xe.$$

First observe that

$$((em)^\circ e) \circ (eme) = (em)^\circ e + (em)e + (em)^\circ eme = ((em)^\circ \circ (em))e = 0$$

and hence $(eme)^\circ = (em)^\circ e$. It follows that $(eMe)^\circ$ is a group. Moreover, we prove by routine computation that φ is an epimorphism. Its kernel is $\{em \in M \mid eme = 0\}$, which, in unital rings, equals $(eM) \cap (eM(1-e))$. This yields a description of $(eM)^\circ$ as a group extension, which can be improved if we assume that $eMe \subseteq M$.

Proposition 2.5. *In a unital ring, if e preserves M and if $eMe \subseteq M$, then $(eM)^\circ$ is isomorphic to $(eMe) \ltimes (eM(1-e))$, the semi-direct product of $(eMe)^\circ$ and the abelian group $eM(1-e)$, where the action of eme on $eM(1-e)$ is induced by the multiplication by $e + eme$ from the left.*

Proof. Clearly $(eMe)^\circ$ is a group and the inclusion of eMe into eM determines the splitting of φ. From $em(1-e) = (em) \circ ((em)^\circ e)$ it follows that $eM(1-e) \subseteq eM$ and hence $\ker \varphi = eM(1-e)$. Commutativity of $eM(1-e)$ follows from the fact

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

that the circle product coincides with the ring addition. The conjugation action of eme on $ex(1-e)$ is computed as

$$(eme) \circ (ex(1-e)) \circ (eme)^{\circ} = ex(1-e) + emex(1-e) = (e + eme)(ex(1-e)).$$

□

Let us say that an idempotent e *strongly preserves* M if $eM \subseteq M$ and $Me \subseteq M$. Clearly, if e strongly preserves M, then the assumptions of the above proposition are satisfied. However, the full strength of this condition will be used in the following section.

2.2. *LDU* decomposition

As we have proved above, if $e_1, \dots, e_n$ is a set of orthogonal idempotents that strongly preserve M, then their sum also strongly preserves M. Based on this fact, we can further decompose the factors of the symmetric decomposition and then rearrange the newly obtained factors to obtain another decomposition of the group M°. This new decomposition is related to the usual triangular (or flag) decomposition of matrices, and it depends on the chosen ordering of the basic idempotents.

For an ordered n-tuple of orthogonal idempotents $(e_1, \dots, e_n)$, let $e = e_1 + \cdots + e_n$ and let

$$\underline{e}_i := e_1 + \cdots + e_{i-1} \quad \text{and} \quad \bar{e}_i := e_{i+1} + \cdots + e_n$$

be the lower and the upper complement of e_i (in particular $\underline{e}_1 = \bar{e}_n = 0$).

As $eMe \in eM$, we can apply theorem 2.4 to decompose eme, so there are elements $m_1, \dots, m_n \in M$ such that $eme = (e_1 m_1 e) \circ \cdots \circ (e_n m_n e)$. The factors can be further decomposed as

$$\begin{aligned} e_i me &= (e_i m \bar{e}_i) \circ (e_i m \underline{e}_i) \circ (e_i m e_i) \\ &= (e_i m \bar{e}_i) \circ (e_i m e_i) \circ ((e_i m e_i)^{\circ} \circ (e_i m \underline{e}_i) \circ (e_i m e_i)). \end{aligned}$$

Since

$$\begin{aligned} (e_i m e_i)^{\circ} \circ (e_i m \underline{e}_i) \circ (e_i m e_i) &= (e_i m \underline{e}_i) + (e_i m e_i)^{\circ} (e_i m \underline{e}_i) \\ &= e_i ((e_i m \underline{e}_i) + (e_i m e_i)^{\circ} (e_i m \underline{e}_i)) \underline{e}_i, \end{aligned}$$

if we define $m' := (e_i m e_i)^{\circ} \circ (e_i m \underline{e}_i) \circ (e_i m e_i)$, then the above factorization becomes

$$e_i me = (e_i m \bar{e}_i) \circ (e_i m e_i) \circ (e_i m' \underline{e}_i).$$

By combining the above we obtain

$$eme = (e_1 m_1 \bar{e}_1) \circ (e_1 m_1 e_1) \circ (e_1 m_1' \underline{e}_1) \circ \cdots \circ (e_n m_n \bar{e}_n) \circ (e_n m_n e_n) \circ (e_n m_n' \underline{e}_n).$$

For $j > i$, every factor of the form $e_i m_i \underline{e}_i$ commutes with factors of the form $e_j m_j e_j$ and $e_j m_j' \bar{e}_j$. Similarly, for $j < i$, every factor of the form $e_i m_i' \bar{e}_i$ commutes with factors of the form $e_j m_j e_j$ and $e_j m_j \underline{e}_j$. Thus, we can rearrange the above factorization to obtain

$$\begin{aligned} eme = ((e_1 m_1 \bar{e}_1) \circ \cdots \circ (e_n m_n \bar{e}_n)) \circ ((e_1 m_1 e_1) \circ \cdots \\ \circ (e_n m_n e_n)) \circ ((e_1 m_1' \underline{e}_1) \circ \cdots \circ (e_n m_n' \underline{e}_n)). \end{aligned}$$

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

Thus, we have a factorization of eme into a product of three elements of the form $eme = l \circ d \circ u$, where

$$\begin{aligned} l &= (e_1 m_1 \bar{e}_1) \circ \cdots \circ (e_n m_n \bar{e}_n), \\ d &= (e_1 m_1 e_1) \circ \cdots \circ (e_n m_n e_n), \\ u &= (e_1 m_1' \underline{e}_1) \circ \cdots \circ (e_n m_n' \underline{e}_n). \end{aligned}$$

Being canonical, this factorization induces a decomposition of $(eMe)^\circ$. In order to describe its factors we introduce the following subsets of M:

$$\begin{aligned} L &:= \{m \in eMe \mid (\forall i) e_i m = e_i m \bar{e}_i\}, \\ U &:= \{m \in eMe \mid (\forall i) e_i m = e_i m \underline{e}_i\}, \\ D &:= \{m \in eMe \mid (\forall i) e_i m = e_i m e_i\}. \end{aligned}$$

Their main properties are collected in the following proposition.

Proposition 2.6. *Let $(e_1, \dots, e_n)$ be any ordered n-tuple of orthogonal idempotents in R. Then L° and U° are nilpotent subgroups of $(eMe)^\circ$, with order of nilpotency less then n. D° is also a subgroup of $(eMe)^\circ$ and is isomorphic to the direct product $\prod_i (e_i M e_i)^\circ$. Moreover, D° normalizes L° and U°.*

Proof. Let $m, m' \in L$. Since L is additively closed, $m \circ m'$ is in L if and only if $e_i mm' = e_i mm' \bar{e}_i$. Bearing in mind the relations $e_i m = e_i m \bar{e}_i$, $e_i m' = e_i m' \bar{e}_i$ and $\bar{e}_j \bar{e}_i = \bar{e}_j$ for $j > i$, we compute

$$e_i mm' = e_i m \bar{e}_i m' = e_i m \sum_{j>i} e_j m' \bar{e}_j = \left(e_i m \sum_{j>i} e_j m' \bar{e}_j \right) \bar{e}_i = e_i mm' \bar{e}_i.$$

We conclude that L is closed under circle multiplication. As for the inverses, given $m \in L$, we have

$$m = em = \sum_i e_i m = \sum_i e_i m \bar{e}_i = (e_n m \bar{e}_n) \circ \cdots \circ (e_1 m \bar{e}_1).$$

The inverse $(e_i m \bar{e}_i)^\circ$ is in L because $(e_i m \bar{e}_i)(e_i m \bar{e}_i) = 0$ implies $(e_i m \bar{e}_i)^\circ = -e_i m \bar{e}_i$, and $-e_i m \bar{e}_i$ is clearly in L. Since L is $\circ$-multiplicatively closed, we conclude that $m^\circ \in L$.

To prove the nilpotency of L° let $L^{(k)} := \{m \in L \mid \text{for all } i,\ e_i m = e_i m \bar{e}_{i+k-1}\}$. Then

$$L = L^{(1)} \supset L^{(2)} \supset \cdots \supset L^{(n)} = \{0\}.$$

Given $m \in L^{(k)}$ and $m' \in L^{(k')}$, we have

$$e_i mm' = \sum_{j \geqslant i+k} e_i m e_j m = \sum_{\substack{j \geqslant i+k, \\ j' \geqslant j+k'}} e_i m e_j m' e_{j'}$$

and hence $mm' \in L^{(k+k')}$. This implies that the commutator

$$m \circ m' \circ m^\circ \circ m'^\circ = m'm^\circ - mm'^\circ + mm'm^\circ + mm'm^\circ m'^\circ + m'm^\circ m'^\circ$$

is also in $L^{(k+k')}$. Therefore, all n-fold commutators in L are trivial.

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

Given an $m \in D$, we have

$$m = em = \sum_i e_i m = \sum_i e_i m e_i.$$

It follows from

$$\begin{aligned} e_i(m \circ m')e_i &= e_i m e_i + e_i m' e_i + e_i m m' e_i \\ &= e_i m e_i + e_i m' e_i + e_i m e_i m' e_i \\ &= (e_i m e_i) \circ (e_i m' e_i) \end{aligned}$$

that the mapping $m \mapsto (e_1 m e_1, \dots, e_n m e_n)$ defines a homomorphism, which is clearly an isomorphism, between the groups D° and $\prod_i (e_i M e_i)^\circ$.

Finally, to prove that D° normalizes L°, it is sufficient to verify that, for all i, j,

$$(e_i m e_i)^\circ \circ (e_j m' \bar{e}_j) = e_i((e_i m \underline{e}_i) + (e_i m e_i)^\circ (e_i m \underline{e}_i))\underline{e}_i.$$

□

We can now return to the factorization $eme = l \circ d \circ u$. As elements of the form $e_i m \bar{e}_i$ are clearly in L, and since L is closed under circle multiplication, we conclude that $l \in L$ and, similarly, that $d \in D$ and $u \in U$. Moreover, L, U and D have pairwise trivial intersection so the factorization $eme = l \circ d \circ u$ with $l \in L$, $d \in D$ and $u \in U$ is unique. Thus, we obtain our main result, the LDU decomposition of the group M°.

THEOREM 2.7. *If $(e_1, \dots, e_n)$ is an ordered n-tuple of orthogonal idempotents in R which strongly preserve M, then $(eMe)^\circ = L^\circ \cdot D^\circ \cdot U^\circ$. In particular, if the ring R is unital, and if the system of idempotents is complete, then $M^\circ = L^\circ \cdot D^\circ \cdot U^\circ$.*

3. Applications

In this section we first translate the above results into decomposition theorems for groups of invertible elements in a ring, giving special attention to the group of all units and its subgroups, obtained from quasi-invertible ideals. Then we consider the so-called congruence subgroups of matrix groups. Lastly we tackle the issue of the range of applicability. There are certainly many rings in which groups of units are not preserved by idempotents. The main example is the full matrix ring over some ring. Its group of units, the general linear group, is obviously not preserved by matrix idempotents, which are often the only idempotents available. Nevertheless, we show that, for a large class of rings (namely the semi-perfect ones), the general linear group is essentially the only 'bad' case. Other applications can be found in [7], of which this work is a continuation. Most notably, there is an application to the stable homotopy theory, which was in fact the main motivation for this study.

3.1. Groups of units

In a unital ring R, the function $r \mapsto r - 1$ defines an isomorphism between the multiplicative monoid $(R, \cdot)$ and the monoid $(R, \circ)$. Hence, $r \in R$ is invertible with respect to the usual multiplication if and only if $r - 1$ is $\circ$-invertible. It follows

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

that, for every $G \leqslant R^*$, the set $G - 1$ is a group with respect to the circle product, which yields a bijection between subgroups of R^* and subgroups of R°. Using these facts, we can easily translate the results of the previous section into decomposition theorems for subgroups of R^*.

Given an idempotent $e \in R$, let $\bar{e}$ denote its complement $\bar{e} := 1 - e$. For every $G \leqslant R^*$ the idempotent e preserves $G - 1$ if $e(G - 1) \subseteq G - 1$, which is equivalent to $\bar{e} + eG \subseteq G$. Moreover, e strongly preserves $G - 1$ if both $\bar{e} + eG \subseteq G$ and $\bar{e} + Ge \subseteq G$. Then theorem 2.4 translates into the following theorem.

Theorem 3.1. *Let $e_1, \dots, e_n$ be a complete set of idempotents in a ring R, and let G be a subgroup of R^*. If $\bar{e}_i + e_i G \subseteq G$ for all i, then $\bar{e}_i + e_i G$ are subgroups of G, and G admits the symmetric decomposition $G = (\bar{e}_1 + e_1 G) \cdot \dots \cdot (\bar{e}_n + e_n G)$.*

Note that if $e_1, \dots, e_n$ is a set of orthogonal idempotents that preserve $G - 1$, then the same holds for their complement $1 - e_1 - \dots - e_n$, so we may assume, without any loss in generality, that the set of idempotents is complete.

By proposition 2.5, a factor of the symmetric decomposition of the form $\bar{e} + eG$ can be further decomposed if $e(G - 1)e \subseteq (G - 1)$ or, equivalently, if $\bar{e} + eGe \subseteq G$.

Proposition 3.2. *If $\bar{e} + eG$ and $\bar{e} + eGe$ are subsets of G, then eGe is a group and*

$$\bar{e} + eG \cong (eGe) \ltimes (eG\bar{e}),$$

where the semi-direct product is taken with respect to the action given by the left multiplication.

Next we consider the LDU decomposition of a subgroup $G \leqslant R^*$. Let $(e_1, \dots, e_n)$ be an ordered n-tuple of orthogonal idempotents in R that sum up to 1. Then we define the following subsets of G:

$$L := \{g \in G \mid e_i g e_i = e_i \text{ for all } i, \text{ and } e_i g e_j = 0 \text{ for } j < i\},$$
$$U := \{g \in G \mid e_i g e_i = e_i \text{ for all } i, \text{ and } e_i g e_j = 0 \text{ for } j > i\}$$

and

$$D := \{g \in G \mid e_i g e_j = 0 \text{ for } j \neq i\}.$$

Now we can combine proposition 2.6 and theorem 2.7 into the following result.

Theorem 3.3. *Let G be a subgroup of R^* and let $(e_1, \dots, e_n)$ be an ordered n-tuple of orthogonal idempotents in R such that $e_1 + \dots + e_n = 1$. Assume that $\bar{e}_i + e_i G$ and $\bar{e}_i + Ge_i$ are contained in G for all i. Then*

(i) *L and U are nilpotent subgroups of G with order of nilpotency less then n,*

(ii) *D is a subgroup of G whose elements normalize L and U, and which is isomorphic to the direct product of groups $D \cong \prod_i (e_i G e_i)$,*

(iii) *$G = L \cdot D \cdot U$.*

There are two special cases worth mentioning: the entire group R^* and groups of the form $1 + Q$, where Q is a quasi-invertible ideal of R and the entire group R^*.

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

Recall that an ideal $Q \lhd R$ is said to be *quasi-invertible* if $1+Q$ is a group or, equivalently, if Q° is a group. Quasi-invertible ideals (both left and right) are precisely the subideals of the Jacobson radical $\mathrm{Jac}(R) \lhd R$. If Q is a left ideal, then $eQ \subseteq Q$ for every idempotent e. If Q is a two-sided ideal, then also $Qe \subseteq Q$. Thus, we obtain the following.

Corollary 3.4. *Let $Q \lhd R$ be a quasi-invertible left ideal of R. Then*

(i) *The group $1+Q$ admits the symmetric decomposition with respect to every complete set of orthogonal idempotents.*

(ii) *If Q is also a right ideal, then $1+Q$ admits the LDU decomposition with respect to every ordered complete set of orthogonal idempotents.*

Part (ii) of the corollary is a generalization of [2, corollary 2.9].

Example 3.5. Let S be a radical ring (i.e. $\mathrm{Jac}(S)=S$). Then the matrix ring $M_n(S)$ is also a radical ring, so we either directly apply the results of the previous section or adjoin a unit to S and use the results from this section. If $e_1,\dots,e_n$ are the standard matrix units, then the symmetric decomposition of $M_n(S)^\circ$ is

$$M_n(S)^\circ = (e_1 M_n(S))^\circ \cdot (e_1 M_n(S))^\circ.$$

The structure of the factors is given by proposition 3.2:

$$(e_i M_n(S))^\circ = (e_i M_n(S) e_i)^\circ \ltimes \left(\bigoplus_{i\neq j} e_i M_n(S) e_j\right) = S^\circ \ltimes S^{n-1}$$

and hence $M_n(S)^\circ$ is the product of n subgroups, all of which are isomorphic to $S^\circ \ltimes S^{n-1}$.

Clearly, $(M_n(S))^\circ$ also admits the LDU decomposition with respect to the standard matrix idempotents. Factors L° and U° are isomorphic to the groups of unipotent lower-triangular (and, respectively, upper-triangular) matrices with coefficients in S, while D° is isomorphic to $(S^\circ)^n$.

Corollary 3.6. *If S is a radical ring, then every element $m \in M_n(S)$ can be uniquely factorized as $m = l \circ d \circ u$, where $l \in L$, $d \in D$ and $u \in U$.*

We can now apply the results on products of groups to describe the structure of the group $1+Q$. Let us first recall the well-known fact that if the ideal Q is nilpotent, then $1+Q$ is a nilpotent group. The following theorems can be considered as extensions of this result.

Theorem 3.7. *Let $Q \lhd R$ be a quasi-invertible ideal and let $eQe + \bar{e}Q\bar{e} = 0$ for some idempotent $e \in R$. Then the group $1+Q$ is metabelian (i.e. its commutator subgroup is abelian). Moreover, if Q has finite (additive) exponent, then the group $1+Q$ has finite exponent.*

Proof. By corollary 3.4(ii) we have the decomposition $1+Q = L\cdot D\cdot U$, by theorem 3.3(ii) we obtain the group $D \cong (eQe)\oplus(\bar{e}Q\bar{e}) = 0$ and, by theorem 3.3(iii), groups L and U are abelian. By the famous result of Itô [4] the group $1+Q$ is metabelian. Moreover, if Q has finite additive exponent, then both L and U have finite exponent, and, by [3], their product $1+Q$ also has a finite exponent. □

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

A partial generalization of the above result is shown in the following theorem.

Theorem 3.8. *Let $Q \lhd R$ be a finite quasi-invertible ideal and let $e_1, \dots, e_n$ be a complete set of orthogonal idempotents such that $e_1Qe_1 + \dots + e_nQe_n = 0$. Then the group $1 + Q$ is solvable.*

Proof. In a similar way to the proof of the previous theorem we show that $D = 0$ and that L and U are finite nilpotent groups. Then, by the theorem of [6], the product $1 + Q = L \cdot U$ is solvable. □

Next we consider the group R^* of all invertible elements of R. The assumptions of theorems 3.1 and 3.3 can be reformulated and turn out to be equivalent.

Lemma 3.9. *Let $r \in R$ and let $e \in R$ be an idempotent. The following statements are equivalent:*

(i) $\bar{e} + er \in R^*$;

(ii) $\bar{e} + ere \in R^*$;

(iii) $ere \in (eRe)^*$;

(iv) $\bar{e} + re \in R^*$.

Proof. Let $m \in R$. Since $(em) = (em\bar{e}) \circ (eme)$ and since $(em\bar{e})$ is always invertible (as $(em\bar{e})^\circ = -em\bar{e}$), we conclude that em is $\circ$-invertible if and only if eme is $\circ$-invertible.

Now $\bar{e}+er \in R^*$ if and only if $\bar{e}+er-1 = e(r-1) \in R^\circ$, which is in turn equivalent to $e(r-1)e \in R^\circ$. The latter is equivalent to (ii), as $1+e(r-1)e = \bar{e}+ere$. It is also equivalent to (iii), since e is the unit of eRe and $e + e(r-1)e = ere$. Statements (ii) and (iii) are symmetric and hence are clearly equivalent to (iv). □

We can now formulate several equivalent forms of our main assumption on R^*.

Proposition 3.10. *Let $e \in R$ be an idempotent. The following statements are equivalent:*

(i) $\bar{e} + eR^* \subseteq R^*$;

(ii) $\bar{e} + R^*e \subseteq R^*$;

(iii) $eR^*e \subseteq (eRe)^*$;

(iv) $eR^*e = (eRe)^*$.

Proof. By the previous lemma, (iii) is equivalent to (i) and (ii). To prove that (iii) implies (iv), observe that if $ere \in (eRe)^*$, then $\bar{e} + ere \in R^*$. Therefore, $ere = e(\bar{e} + ere)e \in eR^*e$. □

Condition (iii) is most easily checked in practice and, by lemma 3.9, it suffices both for the symmetric and for the LDU decomposition.

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

Corollary 3.11. *Let $e_1,\dots,e_n$ be a complete set of idempotents in a ring R such that $e_iR^*e_i \subseteq (e_iRe_i)^*$ for all i. Then the following hold.*

(i) *R^* admits the symmetric decomposition*

$$R^* = ((e_1R^*e_1) \ltimes (e_1R^*\bar{e}_1)) \cdot \cdots \cdot ((e_nR^*e_n) \ltimes (e_nR^*\bar{e}_n)).$$

(ii) *If we choose an order for the idempotents $e_1,\dots,e_n$ and define L, D and U accordingly, then R^* admits the LDU decomposition as well: $R^* = L \cdot D \cdot U$.*

Part (ii) generalizes the result of Putcha and Marquardt as reported in [2, corollary 2.8].

Example 3.12. Let Q be a quasi-invertible ideal in a unital ring S and let R be the subring of all $n \times n$ matrices over S, whose off-diagonal elements are in Q. Then R^* admits both symmetric and LDU decomposition with respect to the standard idempotent matrix units $e_1,\dots,e_n$ of R. As e_i, $i = 1,\dots,n$, form a complete orthogonal system of idempotents then, for $x \in R^*$ we have

$$e_i = e_ixx^*e_i = \sum_j e_ixe_jx^*e_i = e_ixe_ix^*e_i + \sum_{j\neq i} e_ixe_jx^*e_i.$$

If we view the above as an equality in $e_iRe_i = S$ and use the assumption that $e_jxe_i \in Q$ for $j \neq i$, we obtain that $e_ixe_ix^*e_i \in S^*$ and hence that e_ixe_i is right invertible in S. By interchanging the factors we see that e_ixe_i is left invertible as well. Hence, the assumptions of corollary 3.11 are satisfied.

The structure of the factors in the symmetric decomposition of R^* can be described in the following way. By proposition 3.10(iv), $e_iR^*e_i = (e_iRe_i)^* = S^*$ for all i. On the other hand, it is easily seen that $e_iR^*\bar{e}_i$ is isomorphic, as an abelian group, to Q^{n-1}, and that the action of S^* on Q^{n-1} is by direct multiplication. We conclude that R^* is the product of n groups, each of them isomorphic to the semi-direct product $S^* \ltimes Q^{n-1}$.

As for the LDU decomposition, we see that L consists of all unipotent lower-triangular matrices in R (i.e. units on the diagonal and elements of Q under the diagonal), while U consists of all unipotent upper-triangular matrices in R. Therefore, L and U are anti-isomorphic, as the elements of U are precisely the transposes of elements of L. Furthermore, D consists of all diagonal matrices and is isomorphic to $(S^*)^n$.

3.2. Congruence groups

There is another important class of matrix groups that often admit decompositions induced by idempotents. Let I be an ideal in a ring R. For a group G of $n \times n$ matrices over R, let $G_I := (1 + M_n(I)) \cap G$. Clearly, G_I is a normal subgroup of G, as it is precisely the kernel of the componentwise reduction modulo I, and is called the *congruence subgroup* of G modulo I. The most important examples arise when R is the ring of rational, p-adic or p-localized integers. When I is an ideal of finite index in R then G_I is a subgroup of finite index in G. The famous congruence subgroup problem asks if every subgroup of finite index of G contains G_I for some ideal I of finite index.

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

Observe that G_I is, in general, neither the group of units of some ring nor of the form $1+Q$ for some quasi-invertible ideal Q. Clearly, if G is preserved by some idempotent e, then G_I is also preserved by e, but the converse is not true. For example, if $G = Gl_n(R) = (\mathrm{M}_n(R))^*$ and Q is a quasi-invertible ideal of R, then G_Q is preserved by all idempotents of $\mathrm{M}_n(R)$ since $G_Q = 1 + \mathrm{M}_n(Q)$, and $\mathrm{M}_n(Q)$ is a quasi-invertible ideal of $\mathrm{M}_n(R)$. On the other hand, it is obvious that, in many cases, $Gl_n(R)$ is not preserved by any non-trivial idempotent of $\mathrm{M}_n(R)$.

Example 3.13. Consider the ring $M_n(\mathbb{Z}_{(p)})$ of matrices over $\mathbb{Z}_{(p)}$, the integers localized at the prime, p. All ideals of $\mathbb{Z}_{(p)}$ are of the form $p^n\mathbb{Z}_{(p)}$ and are therefore quasi-invertible and of finite index. Moreover, it is known that, for matrices over this ring, the congruence subgroup problem has a positive solution [5, pp. 163–165]. Hence, we conclude that every subgroup of finite index in $GL_n(\mathbb{Z}_{(p)})$ contains a normal subgroup of finite index of the form $1 + M_n(p^n\mathbb{Z}_{(p)})$ whose structure is described in example 3.5 as a product of n subgroups, all of which are isomorphic to the semi-direct product

$$(1 + p^n\mathbb{Z}_{(p)}) \ltimes \mathbb{Z}_{(p)}^{n-1}.$$

3.3. Semi-perfect rings

As mentioned earlier, general linear groups over fields (or division rings) are not decomposable with respect to matrix idempotents, so their structure has to be analysed by different means. This is unsurprising. However, in this section we will show that, for a large class of rings, this is essentially the only indecomposable case.

Recall that a ring, R, is *semi-perfect* if $\mathrm{Jac}(R)$ is idempotent-lifting, and if $R/\mathrm{Jac}(R)$ is semi-simple Artinian. The fundamental structure theorem [10, theorem 2.9.18] states that, in every semi-perfect ring R, there exists a complete set $e_1, \dots, e_n$ of primitive orthogonal idempotents, such that there is a direct sum decomposition $R = \bigoplus_i Re_i$ of left ideals, and all the endomorphism rings $\mathrm{End}_R(Re_i)$ are local rings. Moreover, this decomposition is essentially unique in the sense that any two sets of idempotents with the same properties are conjugated in R.

Lemma 3.14. *Let u, v be primitive idempotents in R. If there are elements $m \in uRv$ and $n \in vRu$ such that mn is invertible in uRu, then Ru and Rv are isomorphic as left R-modules.*

Proof. We may assume that $mn = u$. Otherwise we adjust n by multiplication with the inverse of mn in uRu. Then nm is a non-trivial idempotent in vRv which, by primitivity, implies that $nm = v$. Then, by [10, proposition 2.7.25], $Ru \cong Rv$. □

The idempotents e_i and e_j in R are of the same type if $Re_i \cong Re_j$. Let $e_1, \dots, e_n$ be a complete set of primitive, orthogonal idempotents in a semi-perfect ring R. If all e_i are of the same type, then R is isomorphic to the ring of $n \times n$-matrices over the local ring $R' := \mathrm{End}_R(Re_1)$, and $R^* \cong Gl_n(R')$, which is indecomposable. Otherwise, we can partition $e_1, \dots, e_n$ into subsets by putting together idempotents of the same type. Thus, we obtain a complete set of orthogonal idempotents

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

$u_1, \dots, u_m$, where each u_i is the sum of idempotents of the same type. The idempotents u_i correspond precisely to the central idempotents, which split $R/\operatorname{Jac}(R)$ into a product of matrix rings.

Theorem 3.15. *If R and $u_1, \dots, u_m$ are as above, then $u_i R^* u_i \subseteq (u_i R u_i)^*$ for all i. Therefore, R^* admits the symmetric and the LDU decomposition with respect to $u_1, \dots, u_n$.*

Proof. For $r \in R^*$, we have

$$u_i = u_i r r^* u_i = \sum_j u_i r u_j r^* u_i = u_i r u_i r^* u_i + \sum_{j \neq i} u_i r u_j r^* u_i.$$

For $j \neq i$, each summand $u_i r u_j r^* u_i$ is itself a sum of elements of the form $ere'r^*e$, where e and e' are primitive idempotents of different type. By the previous lemma, $ere'r^*e$ is not invertible eRe and, since $eRe = \operatorname{End}_R(Re)$ is local, we have $ere'r^*e \in \operatorname{Jac}(eRe)$. As $u_i R u_i$ can be identified with matrices over the local ring eRe, the Jacobson radical of $u_i R u_i$ consists of matrices over $\operatorname{Jac}(eRe)$. It follows that

$$u_i r u_j r^* u_i \in \operatorname{Jac}(u_i R u_i) \quad \text{for all } j \neq i.$$

Therefore, $u_i r^* u_i \subseteq (u_i R u_i)^*$.

The second claim follows by corollary 3.11. □

Remark 3.16. A more conceptual proof of the above result would be as follows. Let $\bar{r}$ denote the image of $r \in R$ in $R/\operatorname{Jac}(R)$. Given an $r \in R^*$, its image $\bar{r}$ is invertible in

$$\frac{R}{\operatorname{Jac}(R)} = \prod_i \bar{u}_i \left(\frac{R}{\operatorname{Jac}(R)}\right) \bar{u}_i,$$

which is only possible if $\bar{u}_i \bar{r} \bar{u}_i \in (\bar{u}_i (R/\operatorname{Jac}(R)) \bar{u}_i)^*$. Therefore, $u_i r u_i \in (u_i R u_i)^*$.

An important special case arises when all idempotents e_i are of different type. Semi-perfect rings with this property are called basic rings. Their importance stems from the fact that every semi-perfect ring R has a maximal basic subring R' and R is Morita equivalent to R' [10, theorem 2.7.30].

Corollary 3.17. *Every basic semi-perfect ring admits symmetric and LDU decomposition with respect to a complete set of primitive idempotents.*

Remark 3.18. The methods used in this paper can be employed for yet another description of the group of units of a semi-perfect ring (or, more generally, of a semi-local ring). In fact, if R is semi-local, then $R/\operatorname{Jac}(R)$ is semi-simple Artinian, so there is a short exact sequence of groups $1 \to \operatorname{Jac}(R)^\circ \to R^* \to G \to 1$, where G is a direct product of general linear groups over division rings and $\operatorname{Jac}(R)^\circ$ is a group that can be decomposed with respect to every complete set of orthogonal idempotents in R.

Acknowledgments

This research was supported in part by the Ministry for Education, Science and Sport of the Republic of Slovenia Research Program no. P1-0292-0101-04 and Research Project no. J1-6128-0101-04.

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press

References

1 H. Bechtell. *Theory of groups*, Addison-Wesley Series in Mathematics (Addison-Wesley, 1971).

2 J.-A. Cohen and K. Koh. Idempotents in a compact ring. *Commun. Alg.* **24** (1996), 3653–3679.

3 R. B. Howlett. On the exponent of certain factorizable groups. *J. Lond. Math. Soc.* **31** (1985), 265–271.

4 N. Itô. Über das Produkt von zwei abelschen Gruppen. *Math. Z.* **62** (1955), 400–401.

5 M. I. Kargapolov and J. I. Merzljakov. *Fundamentals of the theory of groups* (Springer, 1979).

6 O. H. Kegel. Produkte nilpotenter Gruppen. *Arch. Math.* **12** (1961), 90–93.

7 P. Pavešić. Factorization of units and groups of stable homotopy equivalences. *J. Pure Appl. Alg.* **182** (2002), 271–284.

8 M. S. Putcha. Semigroup approach to linear algebraic groups. III. Buildings. *Can. J. Math.* **38** (1986), 751–768.

9 M. S. Putcha. Monids on groups with BN-pairs. *J. Alg.* **120** (1989), 139–169.

10 L. H. Rowen. *Ring theory*, vol. 1, Pure and Applied Mathematics, vol. 127 (Boston, MA: Academic Press, 1988).

(*Issued 12 December 2009*)

https://doi.org/10.1017/S0308210508001017 Published online by Cambridge University Press