DECOMPOSITIONS OF GROUPS OF INVERTIBLE ELEMENTS IN A RING

Petar Pavešić

Fakulteta za Matematiko in Fiziko, Univerza v Ljubljani,
Jadranska 19, 1111 Ljubljana, Slovenija
petar.pavesic@fmf.uni-lj.si

Abstract 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.

Keywords: group of units, circle product, idempotent, semi-perfect ring

MSC 2000 classification: Primary 16U60.

1 Introduction

The main goal 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, while 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 to improve some of their results.

Our approach is somewhat different from the mentioned works, 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 in 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 assume 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, hence $(R, \circ)$ is a monoid. If $r$ is invertible with respect to the circle product...
product then we denote its inverse by \(r^\circ\): it is uniquely determined by the equations \(r + r^\circ + r^\circ r = r + r^\circ + r^\circ r = 0\). A subset \(M \subseteq R\) which is a group with respect to the circle product is denoted for emphasis by \(M^\circ\). A partial exception to this is \(R^\circ\), which denotes the group of all invertible elements of \((R, \circ)\). When \(R\) is unital, then the map \(r \mapsto r - 1\) defines an isomorphism of monoids \((R, \cdot)\) and \((R, \circ)\), and hence a bijective correspondence between subgroups of \(R^\circ\) and \(R^\circ\).

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 (cf. Theorem 3.1.1 of [1]). In particular \(G = A \cdot B\) is equivalent to \(G = B \cdot A\).

Following is the outline of the paper. In Section 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 the two says that if some complete set of orthogonal idempotents \(e_1, \ldots, e_n\) (i.e. \(e_1 + \ldots + e_n = 1\)) preserve \(M\) (in the sense that \(e_i M \subseteq M\) for all \(i\)), then \(M^\circ\) is the product of its subgroups \((e_i M)^\circ\). If moreover \(M e_i \subseteq M\) for all \(i\) then the second theorem describes another decomposition of \(M^\circ\) which reminds the factorization of matrices into a product of lower and upper triangular matrices. In Section 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 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 \(M^\circ\) is a group. Given an idempotent \(e \in R\) we say that \(e\) preserves \(M\) if \(e M \subseteq M\). See Section 3.1 for some typical examples of such \(M\).

### 2.1 Symmetric decomposition

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

**Proof:** It suffices to prove that \(e M\) is closed for \(\circ\)-products and \(\circ\)-inverses. Given \(e m, e m' \in e M\) we have \((e m) \circ (e m') = e m + e m' + e m e m' = e (m \circ (e m')) \in e M\). Moreover \((e (e m)^\circ) \circ (e m) = e (e m)^\circ + e m + e (e m)^\circ (e m) = e ((e m)^\circ \circ (e m)) = 0\) implies that the inverse of \(e m\) is of the form \(e (e m)^\circ\), which is in \(e M\). \(\square\)
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 preserve $M$, 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

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

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

**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 $m = (um^\circ) \circ (vm)$, and that $M^\circ = (uM)^\circ \cdot (vM)^\circ$.

The inductive application of Proposition 2.2 yields the symmetric decomposition of the group $M^\circ$.

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

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

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

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

$$\varphi: (eM)^\circ \rightarrow (eMe)^\circ, \quad x \mapsto xe.$$ 

First observe that $((em)^\circ e) \circ (eme) = (em)^\circ e + (em)e + (em)^\circ eme = ((em)^\circ \circ (em))e = 0$, hence $(eme)^\circ = (em)^\circ e$. It follows that $(eMe)^\circ$ is a group. Moreover we prove by routine computation that $\varphi$ 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 $\varphi(eM(1 - e))$, the semi-direct product of $(eM)^\circ$ 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, $(eM)^\circ$ is a group and the inclusion of $eMe$ into $eM$ determines the splitting of $\varphi$. From $em(1 - e) = (em) \circ ((em)^\circ e)$ it follows that $eM(1 - e) \subseteq eM$, hence $\ker \varphi = eM(1 - e)$. Commutativity of $eM(1 - e)$ follows from the fact 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 in the previous section, if \( e_1, \ldots, e_n \) is a set of orthogonal idempotents which 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 so to obtain another decomposition of the group \( M^2 \). 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 \( (e_1, \ldots, e_n) \) let \( e = e_1 + \ldots + e_n \), and let

\[
\xi_j := e_1 + \ldots + e_{j-1} \quad \text{and} \quad \eta_j := e_{j+1} + \ldots + e_n
\]

be the lower and the upper complement of \( e_j \) (in particular \( \xi_1 = \eta_n = 0 \)).

As \( eMe \in eM \) we can apply Theorem 2.4 to decompose \( eme \), so there are elements \( m_1, \ldots, m_n \in M \) such that

\[
eme = (e_1m_1e) \circ \ldots \circ (e_nm_ne).
\]

The factors can be further decomposed as

\[
e_1me = (e_1m\eta) \circ (e_1m\xi) \circ (e_1m\eta) = (e_1m\eta) \circ (e_1m\xi) \circ (e_1m\eta) \circ (e_1m\eta) \circ (e_1m\xi) \circ (e_1m\eta) .
\]

Since

\[
(e_1m\xi) \circ (e_1m\eta) \circ (e_1m\xi) = (e_1m\eta) + (e_1m\xi) \circ (e_1m\eta) \circ (e_1m\xi) = e_1((e_1m\eta) + (e_1m\xi) \circ (e_1m\eta) \circ (e_1m\xi)) \xi_i
\]

if we define \( m' := (e_1m\xi) \circ (e_1m\eta) \circ (e_1m\xi) \) then the above factorization becomes

\[
e_1me = (e_1m\eta) \circ (e_1m\xi) \circ (e_1m'\xi_j) .
\]

By putting together previous computations we get

\[
eme = (e_1m_1\eta_1) \circ (e_1m_1\xi_1) \circ (e_1m_1'\xi_1) \circ \ldots \circ (e_1m_n\eta_n) \circ (e_1m_n\xi_n) \circ (e_1m_n'\xi_n) .
\]

For \( j > i \) every factor of the form \( e_jm_i\eta_i \) commutes with factors of the form \( e_jm_j\xi_j \) and \( e_jm_j^2\xi_j \). Similarly, for \( j < i \) every factor of the form \( e_jm_i^2\xi_j \) commutes with factors of the form \( e_jm_j\xi_j \) and \( e_jm_j^2\xi_j \). Thus, we can rearrange the above factorization to obtain

\[
eme = (e_1m_1\eta_1) \circ \ldots \circ (e_1m_n\eta_n) \circ ((e_1m_1\xi_1) \circ \ldots \circ (e_1m_n\xi_n)) \circ ((e_1m_1'\xi_1) \circ \ldots \circ (e_1m_n'\xi_n)) .
\]

Thus we have a factorization of \( eme \) into a product of three elements of the form \( eme = l \circ d \circ u \), where \( l = (e_1m_1\eta_1) \circ \ldots \circ (e_1m_n\eta_n) \), \( d = (e_1m_1\xi_1) \circ \ldots \circ (e_1m_n\xi_n) \) and \( u = (e_1m_1'\xi_1) \circ \ldots \circ (e_1m_n'\xi_n) \). Being canonical, this factorization induces a decomposition of \( (eMe)^2 \). In order to describe its factors we introduce the following subsets of \( M \):

\[
L := \{ m \in eMe \mid (\forall i) e_1m = e_1m\eta_i \},
\]

\[
U := \{ m \in eMe \mid (\forall i) e_1m = e_1m\xi_i \}
\]

and

\[
D := \{ m \in eMe \mid (\forall i) e_1m = e_1m\eta_i \} .
\]

Their main properties are collected in
Proposition 2.6 Let \((e_1, \ldots, e_n)\) be any ordered \(n\)-tuple of orthogonal idempotents in \(R\). Then \(L^o\) and \(U^o\) are nilpotent subgroups of \((eMe)^o\), with order of nilpotency less than \(n\). \(D^o\) is also a subgroup of \((eMe)^o\), and is isomorphic to the direct product \(\prod_i(e_iMe_i)^o\). Moreover \(D^o\) normalizes \(L^o\) and \(U^o\).

Proof: Let \(m, m' \in L\). Since \(L\) is additively closed, \(m \circ m'\) is in \(L\) if, and only if \(e_i mm' = e_i mm'\pi_i\). Bearing in mind the relations \(e_i m = e_i m\pi_i\), \(e_i m' = e_i m'\pi_i\) and \(\pi_j\pi_i = \pi_j\) for \(j > i\) we compute

\[
e_i mm' = e_i m\pi_i m' = e_i m \sum_{j>i} e_j m' \pi_j = (e_i m \sum_{j>i} e_j m' \pi_j) \pi_i = e_i mm' \pi_i,
\]

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

\[
m = e_i m = \sum_i e_i m \pi_i = (e_n m \pi_n) \circ \cdots \circ (e_1 m \pi_1).
\]

The inverse \((e_i m \pi_i)^o\) is in \(L\) because \((e_i m \pi_i)(e_i m \pi_i) = 0\) implies \((e_i m \pi_i)^o = -e_i m \pi_i\), and \(-e_i m \pi_i\) is clearly in \(L\). Since \(L\) is \(\circ\)-multiplicatively closed, we conclude that \(m^o \in L\).

To prove the nilpotency of \(L^o\) let \(L^{(k)} := \{m \in L \mid (\forall i) e_i m = e_i m \pi_i + k - 1\}\). 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

\[
e_i mm' = \sum_{j \geq i+k} e_i me_j m = \sum_{j \geq i+k} e_i me_j m' e_j,
\]

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

\[
m \circ m' \circ m^o \circ m'^o = mm' m^o - mm' m^o + mm' m^o m'^o + m'm^o m'^o
\]

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

Given an \(m \in D\) we have \(m = e_m = \sum_i e_i m = \sum_i e_i me_i\). It follows from

\[
e_i(m \circ m')e_i = e_i me_i + e_i m' e_i + e_i mm'e_i = e_i me_i + e_i m' e_i + e_i me_i m' e_i = (e_i me_i) \circ (e_i m' e_i)
\]

that the mapping \(m \mapsto (e_1 me_1, \ldots, e_n me_n)\) defines a homomorphism, which is clearly an isomorphism, between the groups \(D^o\) and \(\prod_i(e_i Me_i)^o\).

Finally, to prove that \(D^o\) normalizes \(L^o\) it is sufficient to verify that for all \(i, j\)

\[
(e_i me_i)^o \circ (e_j m' \pi_j) = e_i ((e_i m \xi_i) + (e_i m e_i)^o (e_j m e_j) \xi_i)
\]

\(\Box\)

We can now return to the factorization \(eMe = l \circ d \circ u\). As elements of the form \(e_i m \pi_i\) 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 \(M^o\).

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

In this section we first translate the above results into decomposition theorems for groups of invertible elements in a ring, with special attention for the group of all units, and for its subgroups, obtained from quasi-invertible ideals. Then we consider the so called congruence subgroups of matrix groups. Thirdly, we tackle the issue of the range of applicability. There are certainly many rings in which group 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 the paper [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 that for every \( G \leq R^\ast \) the set \( G - 1 \) is a group with respect to the circle product, which yields a bijection between subgroups of \( R^\ast \) and subgroups of \( R^\circ \). Using these facts we can easily translate the results of the previous section into decomposition theorems for subgroups of \( R^\ast \).

Given an idempotent \( e \in R \) let \( \bar{e} \) denote its complement \( \bar{e} := 1 - e \). For every \( G \leq R^\ast \) 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

**Theorem 3.1** Let \( e_1, \ldots, e_n \) be a complete set of idempotents in a ring \( R \), and let \( G \) be a subgroup of \( R^\ast \). If \( \bar{e}_i + e_iG \subseteq G \) for all \( i \) then \( \bar{e}_i + e_iG \) are subgroups of \( G \) and \( G \) admits the symmetric decomposition: \( G = (\bar{e}_1 + e_1G) \cdot \ldots \cdot (\bar{e}_n + e_nG) \).

Note that if \( e_1, \ldots, e_n \) is a set of orthogonal idempotents which preserve \( G - 1 \) then the same holds for their complement \( 1 - e_1 - \ldots - e_n \), 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 \( \bar{e} + eG \cong (eGe) \rtimes (eG) \) 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 \( G \leq R^\ast \). Let \( (e_1, \ldots, e_n) \) be an ordered \( n \)-tuple of orthogonal idempotents in \( R \) which sum up to \( 1 \). Then we define the following subsets of \( G \):

\[
L := \{ g \in G \mid e_ige_i = e_i \text{ for all } i, \text{ and } e_ige_j = 0 \text{ for } j < i \},
\]
Theorem 3.3 Let $G$ be a subgroup of $R^*$, and let $(e_1, \ldots, e_n)$ be an ordered $n$-tuple of orthogonal idempotents in $R$ such that $e_1 + \ldots + e_n = 1$. Assume that $e_i + e_i G$ and $e_i + Ge_i$ are contained in $G$ for all $i$. Then

(a) $L$ and $U$ are nilpotent subgroups of $G$ with order of nilpotency less then $n$.

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

(c) $G = L \cdot D \cdot U$.

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 $R^*$.

Recall that an ideal $Q \triangleleft R$ is said to be quasi-invertible if $1 + Q$ is a group, or equivalently if $Q^\circ$ is a group. Quasi-invertible ideals (both left and right) are precisely the sub-ideals of the Jacobson radical $\text{Jac}(R) \triangleleft R$. 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 get the following

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

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

(b) 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 (b) of the corollary is a generalization of Corollary 2.9 in [2].

Example 3.5 Let $S$ be a radical ring (i.e. $\text{Jac}(S) = S$). Then the matrix ring $M_n(S)$ is also a radical ring so we either apply directly the results of the previous section or adjoin a unit to $S$ and use results of this section. If $e_1, \ldots, e_n$ are the standard matrix units, then the symmetric decomposition of $M_n(S)^\circ$ is $M_n(S)^\circ = (e_1 M_n(S))^\circ \cdot \ldots \cdot (e_1 M_n(S))^\circ$. The structure of the factors is given by Proposition 3.2: $(e_i M_n(S))^\circ = (e_i M_n(S) e_i)^\circ \vee (\bigoplus_{j \neq i} e_i M_n(S) e_j) = S^\circ \ltimes S^{n-1}$, 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 $L^\circ$ and $U^\circ$ are isomorphic to the groups of unipotent lower (resp. upper) triangular matrices with coefficients in $S$, while $D^\circ$ 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 $Q \triangleleft R$ 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). If moreover $Q$ has finite (additive) exponent then the group $1 + Q$ has finite exponent.

**Proof:** By Corollary 3.4(b) we have the decomposition $1 + Q = L \cdot D \cdot U$, by Theorem 3.3(b) the group $D \cong (eQe) \oplus (\bar{e}Q\bar{e}) = 0$, and by Theorem 3.3(c) groups $L$ and $U$ are abelian. By the famous result of Itô [4] the group $1 + Q$ is metabelian. If moreover $Q$ has finite additive exponent then both $L$ and $U$ have finite exponent, and by [3] their product $1 + Q$ has also a finite exponent. □

A partial generalization of the above result is

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

**Proof:** Similarly as in 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 Kegel and Wielandt [5] 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:

(a) $\bar{e} + er \in R^*$;
(b) $\bar{e} + ere \in R^*$;
(c) $ere \in (eRe)^*$
(d) $\bar{e} + re \in R^*$;

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

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

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:
Furthemore, $D$ is anti-isomorphic, as the elements of $L$ consists of all unipotent upper-triangular matrices in $L$. 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 $(S^*)^n$.

**Part (b) generalizes the result of Putcha and Marquardt as reported in [2], Corollary 2.8.**
3.2 Congruence groups

There is another important class of matrix groups which 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 component-wise 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.

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 $G = \text{GL}_n(R) = (\text{M}_n(R))^*$, and $Q$ is a quasi-invertible ideal of $R$, then $G_Q$ is preserved by all idempotents of $\text{M}_n(R)$ since $G_Q = 1 + \text{M}_n(Q)$ and $\text{M}_n(Q)$ is a quasi-invertible ideal of $\text{M}_n(R)$. On the other hand it is obvious that in many cases $\text{GL}_n(R)$ is not preserved by any non-trivial idempotent of $\text{M}_n(R)$.

**Example 3.13** Consider the ring $\text{M}_n(\mathbb{Z}_p)$ of matrices over $\mathbb{Z}_p$, the integers localized at the prime $p$. All ideals of $\mathbb{Z}_p$ are of the form $p^n \mathbb{Z}_p$, therefore quasi-invertible and of finite index. Moreover, it is known that for matrices over this ring the congruence subgroup problem has a positive answer (see [6], pp. 163-165). Hence we conclude that every subgroup of finite index in $\text{GL}_n(\mathbb{Z}_p)$ contains a normal subgroup of finite index of the form $1 + \text{M}_n(p^n \mathbb{Z}_p)$ whose structure is described in Example 3.5 as a product of $n$ subgroups, all of which are isomorphic to the semi-direct product $(1 + p^n \mathbb{Z}_p) \rtimes \mathbb{Z}_p^{n-1}$.

3.3 Semi-perfect rings

As we mentioned earlier, general linear groups over fields (or division rings) are not decomposable with respect to matrix idempotents, and so their structure has to be analysed by different means. This is indeed not surprising. 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 $\text{Jac}(R)$ is idempotent-lifting, and if $R/\text{Jac}(R)$ is semi-simple Artinian. The fundamental structure theorem (see [10], Theorem 2.9.18) states that in every semi-perfect ring $R$ there exists a complete set $e_1, \ldots, e_n$ of primitive orthogonal idempotents, such that there is a direct sum decomposition $R = \bigoplus_i R e_i$ of left ideals, and all the endomorphisms rings $\text{End}_R(Re_i)$ 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 $e_1, \ldots, e_n$ 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 $R' := \text{End}_R(Re_1)$, and $R' \cong \text{Gl}_n(R')$, which is indecomposable. Otherwise, we can partition $e_1, \ldots, e_n$ into subsets by putting together idempotents of the same type. Thus we obtain a complete set of orthogonal idempotents $u_1, \ldots, u_m$ 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 $R/Jac(R)$ into a product of matrix rings.

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

**Proof:** For an $r \in R^*$ we have

$$u_i = u_iRu_i^* = \sum_j u_i r_{ij} r_{ij}^* u_i = u_i r_{ii} r_{ii}^* u_i + \sum_{j \neq i} u_i r_{ij} r_{ij}^* u_i.$$  

For $j \neq i$ each summand $u_i r_{ij} r_{ij}^* u_i$ 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 $eRe = \text{End}_R(Re)$ is local we have $ere' r^*e \in Jac(eRe)$. As $u_iRu_i$ can be identified with matrices over the local ring $eRe$, the Jacobson radical of $u_iRu_i$ consists of matrices over $Jac(eRe)$. It follows that $u_i r_{ij} r_{ij}^* u_i \in Jac(u_iRu_i)$ for all $j \neq i$, therefore $u_i r_{ii} r_{ii}^* u_i \subseteq (u_iRu_i)^*$.

The second claim follows by Corollary 3.11. □

**Remark 3.16** A more conceptual proof of the above result would go as follows: let $\overline{r}$ denote the image of $r \in R$ in $R/Jac(R)$. Given an $r \in R^*$, its image $\overline{r}$ is invertible in $R/Jac(R) = \prod \overline{u}_i(R/Jac(R)\overline{u}_i)$, which is possible only if $\overline{r} \overline{u}_i \in (\overline{u}_i(R/Jac(R)\overline{u}_i))^*$, therefore $u_i r u_i \in (u_i Ru_i)^*$.

An important special case arises when all idempotents $e_i$ are of different type. Semiperfect 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 $R'$ (cf. [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** Methods of this paper can be used for still 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 $R/Jac(R)$ is semi-simple Artinian, so there is a short exact sequence of groups $1 \to Jac(R)^\circ \to R^* \to G \to 1$ where $G$ is a direct product of general linear groups over division rings, and $Jac(R)^\circ$ is a group which can be decomposed with respect to every complete set of orthogonal idempotents in $R$.

**References**

REFERENCES


Petar Pavešić
Fakulteta za Matematiko in Fiziko,
Univerza v Ljubljani,
Jadranska 19,
1111 Ljubljana,
Slovenija.

phone: +386-1-4766546
fax: +386-1-2517281 e-mail: petar.pavesic@fmf.uni-lj.si