Publl. Math. Debrecen
89/1-2 (2016), 97–104
DOI: 10.5486/PMD.2016.7344

The ordering of idempotents in a finite ring

By DAVID DOLŽAN (Ljubljana)

Abstract. In this paper we study the ordering of idempotents in a finite ring. We prove that the relation, defined by $e \leq f$ if and only if $ef = fe = e$, is well behaved whilst moving to the factor ring modulo the Jacobson radical. We then proceed to explicitly find all idempotents of a semisimple ring that are in a relation with each other and observe some special cases when the infimum of two idempotents is equal to zero.

1. Introduction

Idempotents in a ring play a very important role in determining its structure. In a commutative ring, one can define operations $\cup$ and $\cap$ with $e \cup f = e + f - ef$ and $e \cap f = ef$, and then the set $E(R)$ of all idempotents in a ring R together with those two operations becomes a Boolean algebra. The same can be done if all idempotents in a non-commutative ring are central. There exist many conditions that guarantee that $E(R)$ lies in the centre of R. For example, it is well known (see [5]) that if all the idempotents commute with one another, then all the idempotents are central.

However, in a general non-commutative case, the product of two idempotents is not necessarily idempotent. See, for example [2], [3], for some results on the conditions of multiplicativity of the set of idempotents.

Lately, there has been a lot of research on ordering of idempotents in non-commutative rings. For $e, f \in E(R)$, we define $e \leq f$ if and only if $ef = fe = e$. Clearly, $e \leq f$ if and only if $e \in fRf$. Define $e < f$ if $e \leq f$ and $e \neq f$. Now,

Mathematics Subject Classification: 16P10, 16U99.
Key words and phrases: idempotent, ordering, finite ring.

let $e \cap f$ and $e \cup f$ denote the infimum and supremum of e and f (if they exist). Then $(E(R), \leq)$ forms a partially ordered set.

Following [1], we say that idempotents e, f are generalized commuting if there exists a positive integer n such that $(ef)^n = (fe)^n$ or $(ef)^n e = (fe)^n f$. Let $\langle e, f \rangle$ denote the subsemigroup of the multiplicative monoid of R, generated by e and f. In [1], the author proves that for $e, f \in E(R)$ both $e \cap f$ and $e \cup f$ exist and $e \cap f \in \langle e, f \rangle$ if and only if the idempotents e and f are generalized commuting.

In [4], the authors prove that for an algebra R over a field K, for any $e, f \in E(R)$ such that there exists a polynomial $q(\lambda) \in K[\lambda]$ with zero constant term, $q(1) \neq 0$ and $q(ef) = 0$, we have $e \cap f = 0$ and $e \cup f = 1 - q(1)^{-1}(1-e)(1-f)q((1-e)(1-f))$.

However, there exist examples of idempotents which are not generalized commuting, but $e \cap f$ and $e \cup f$ exist nevertheless (see, for example [4, Example 1.2]). This can only happen if $e \cap f \notin \langle e, f \rangle$.

In this paper, we examine the ordering defined above in the set of idempotents of a finite ring. The organization of the paper is as follows: in the next section, we first look at the connection between the idempotents in a ring and those in the factor ring modulo the Jacobson radical. The main result is the following theorem. Here, $\overline{x}$ denotes the image of x under the canonical projection onto the factor ring modulo the Jacobson radical.

Theorem. (1) *If $e \leq f$ in $E(R)$, then $\overline{e} \leq \overline{f}$ in $E(R/J)$.*

(2) *Let $f \in E(R)$. Suppose that there exists $\overline{g} \in E(R/J)$ such that $\overline{g} \leq \overline{f}$. Then there exists an idempotent $e \in E(R)$ such that $e \leq f$ and $\overline{e} = \overline{g}$.*

We further investigate the connection between $e \cap f$ and $\overline{e} \cap \overline{f}$. We prove that $\overline{e} \cap \overline{f} = \overline{0}$ implies $e \cap f = 0$ and give an example that in general the converse does not hold. However, in the special case of generalized commuting idempotents we prove that $\overline{e \cap f} = \overline{e} \cap \overline{f}$.

Thus, the ordering of idempotents in a finite ring is in a strong relationship with their corresponding images modulo the Jacobson radical. In the third section, we therefore examine the idempotents in a semisimple ring and prove that we can study the ordering of idempotents separately in each simple direct summand.

In the last section, we turn our attention to the case of idempotents in a simple finite ring, and for an arbitrary idempotent e we explicitly find all idempotents that are in a relation with e. We also observe some special cases when the infimum of two idempotents is equal to zero.

Throughout this paper, R will denote an arbitrary finite ring with identity.

2. Idempotents modulo Jacobson radical

Let J denote the Jacobson radical of R and let $\pi : R \longrightarrow R/J$ be the canonical projection. For $x \in R$, we shall write $\overline{x}$ for $\pi(x)$.

Let us examine the connection between $E(R)$ and $E(R/J)$. We know that idempotents in a finite ring can be lifted modulo the Jacobson radical (the explicit algorithm for this can be found in [6]). However, we shall need more than this, we have to lift idempotents in such a way that the partial ordering is also preserved.

The first lemma is a technical one.

Lemma 2.1. *Let $x, y \in R$ such that $xy = yx = x$. Then the following statements hold.*

(1) *If $j = y^2 - y$ and $y' = y + j - 2yj$, then $xy' = y'x = x$.*

(2) *If $j = x^2 - x$ and $x' = x + j - 2xj$, then $x'y = y'x' = x'$.*

Proof. In case (1), we can easily see that $jx = xj = 0$. In case (2), we have $jy = yj = j$. The rest is a straightforward calculation. □

The next theorem is crucial in describing the procedure of lifting idempotents in a way that preserves the partial ordering.

Theorem 2.2. *Let R be a finite ring.*

(1) *If $e \leq f$ in $E(R)$, then $\overline{e} \leq \overline{f}$ in $E(R/J)$.*

(2) *Let $f \in E(R)$. Suppose that there exists $\overline{g} \in E(R/J)$ such that $\overline{g} \leq \overline{f}$. Then there exists an idempotent $e \in E(R)$ such that $e \leq f$ and $\overline{e} = \overline{g}$.*

Proof. The first part is straightforward. Let's prove the second part. There exists $t \in R$ (not necessarily idempotent) such that $\overline{t} = \overline{g}$. Then $tf = t + j$ for some $j \in J$. Multiplying this with f from the right, we get $tf = tf + jf$, so $jf = 0$ and thus $(t + j)f = tf = t + j$. Now,

$$f(t + j) = t + j + k \tag{1}$$

for some $k \in J$. Multiplying (1) with f from the left, we get $fk = 0$. This implies $f(t + j + k) = f(t + j) = t + j + k$. However, multiplying (1) with f from the right, we get $f(t + j)f = f(t + j) = t + j + k = (t + j)f + kf = t + j + kf$, so $kf = k$. Therefore, $(t + j + k)f = t + j + kf = t + j + k$.

Denote $x_1 = t + j + k$ and observe that $\overline{x_1} = \overline{g}$ and also $x_1 f = f x_1 = x_1$. If x_1 is not an idempotent, then let $j_1 = x_1^2 - x_1 \in J$ and $x_2 = x_1 + j_1 - 2x_1 j_1$. Observe that $\overline{x_2} = \overline{g}$ and $x_2^2 - x_2 = 4x_1^6 - 12x_1^5 + 9x_1^4 + 2x_1^3 - 3x_1^2 = j_1^2(4j_1 - 3)$. If x_2 is not an idempotent, we can repeat this step with $j_2 = x_2^2 - x_2 \in J^2$ and

$x_3 = x_2 + j_2 - 2x_2j_2$, arriving at $x_3^2 - x_3 = j_2^2(4j_2 - 3) \in J^4$ with $\overline{x_3} = \overline{g}$, etc. Since J is nilpotent, by successively applying the above, we eventually arrive at an idempotent x_n in finitely many steps. By Lemma 2.1, this procedure preserves products, so $x_if = fx_i = x_i$ for $i = 1, 2, \dots, n$, thus $x_nf = fx_n = x_n$ and $\overline{x_n} = \overline{g}$. Therefore, $e = x_n$ is the desired idempotent. □

Immediately, we have a corollary.

Corollary 2.3. *Let $e, f \in E(R)$. If $\overline{e} \cap \overline{f} = \overline{0}$, then $e \cap f = 0$.*

Proof. If $\overline{e} \cap \overline{f} = \overline{0}$, then we have to prove that there exists no idempotent $h \in R$ such that $0 \neq h \leq e, f$. We can assume that $\overline{e}, \overline{f} \neq \overline{0}$, because $\overline{e} = \overline{0}$ implies $e = 0$ (since J is nilpotent) and the statement clearly follows if either $e = 0$ or $f = 0$. Now, suppose such an h exists. Then by Theorem 2.2, $\overline{h} \leq \overline{e}, \overline{f}$. This implies that $\overline{h} = \overline{0}$, $\overline{h} = \overline{e}$ or $\overline{h} = \overline{f}$. But J is a nilpotent ideal and h is an idempotent, so $\overline{h} \neq \overline{0}$. Say, $\overline{h} = \overline{e}$. Then $h \leq f$ implies $\overline{h} \leq \overline{f}$ by Theorem 2.2, which yields $\overline{e} = \overline{e} \cap \overline{f}$, a contradiction. We treat the case $\overline{h} = \overline{f}$ similarly. □

The next example shows that the converse does not generally hold.

Example 2.4. Let R be a ring of upper triangular 2×2 matrices over a field F and let $e = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $f = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in E(R)$. One can easily check that $e \cap f = 0$. However, $R/J \simeq F \times F$ and $\overline{e} = \overline{f} = (1, 0)$, so $\overline{e} \cap \overline{f} \neq \overline{0}$.

We can, however, say something more about the connection between idempotents and their images modulo the Jacobson radical when the idempotents in question are generalized commuting.

Corollary 2.5. *Let $e, f \in E(R)$ be generalized commuting idempotents. Then $e \cap f \in E(R), \overline{e} \cap \overline{f} \in E(R/J)$ and $\overline{e \cap f} = \overline{e} \cap \overline{f}$.*

Proof. By [1, Proposition 6], we know that $e \cap f \in E(R)$ exists and either $e \cap f = (ef)^n$ or $e \cap f = (ef)^n e$ for some integer n. Obviously, $\overline{e}$ and $\overline{f}$ are also generalized commuting idempotents in R/J, so $\overline{e} \cap \overline{f}$ exists again by [1, Proposition 6]. Denote $g = e \cap f$ and $\overline{h} = \overline{e} \cap \overline{f}$. We know that $\overline{g}$ and $\overline{h}$ are both elements of $\langle \overline{e}, \overline{f} \rangle$. By Theorem 2.2, $\overline{g} \leq \overline{e}, \overline{f}$ and by definition, $\overline{h} \leq \overline{e}, \overline{f}$. We can therefore conclude that $\overline{g} = \overline{g}\overline{h} = \overline{h}$. □

3. Semisimple and simple rings

By the previous section, to understand the partial ordering of idempotents, we can examine the factor ring modulo the Jacobson radical. However, since our ring in question is finite, the factor ring is a semisimple ring. In this section, we therefore first examine the set of idempotents of a finite direct sum of (simple) rings.

Proposition 3.1. *Let $R = R_1 \oplus R_2 \oplus \cdots \oplus R_n$ and $e = (e_1, e_2, \dots, e_n), f = (f_1, f_2, \dots, f_n) \in E(R)$. Then $e \leq f$ if and only if $e_i \leq f_i$ for all $i = 1, 2, \dots, n$.*

Proof. The proposition is clear, since $ef = e$ if and only if $e_i f_i = e_i$ for all i. □

Proposition 3.1 together with Theorem 2.2 now implies that in order to study the ordering of idempotents in a finite ring, it pays to examine the idempotents in a simple ring in more detail.

Suppose R is a simple finite ring. So, since R is finite, we can assume that $R = M_n(F)$ for an integer n and a field F. We can always assume that $n \geq 2$ since a field contains no non-trivial idempotents.

First, we need the following technical lemma.

Lemma 3.2. *Let $x, y, z, w \in F^n$ be nonzero (column) vectors such that $xy^T = zw^T$. Then there exist $\alpha, \beta \in F$ such that $x = \alpha z$ and $y = \beta w$.*

Proof. We have $x_i y_j = z_i w_j$ for all i and j. Since x is nonzero, there exists some $1 \leq i \leq n$ such that $x_i \neq 0$. But F is a field, so we have $y_j = \frac{z_i}{x_i} w_j$ for all j, thus $\beta = \frac{z_i}{x_i}$. Similarly, we see that $\alpha = \frac{w_j}{y_j}$ for some nonzero $y_j \in F$. □

Next, we shall examine the ordering of matrix idempotents. Let $e \in E(R)$. We say that e is a minimal idempotent if $0 \leq f \leq e$ for an idempotent f implies that either $f = 0$ or $f = e$. We say that e decomposes as an orthogonal sum of minimal idempotents if $e = e_1 + e_2 + \ldots + e_n$ for some minimal idempotents $e_i \in E(R)$ with $e_i e_j = e_j e_i = 0$ for all $i \neq j$. It follows from [6, Theorem VII.13] that every idempotent in $M_n(F)$ decomposes (not necessarily uniquely) as an orthogonal sum of minimal idempotents and that all minimal idempotents in $M_n(F)$ are rank one matrices.

Lemma 3.3. *Let $n \geq 2$ and F a field. Choose $e \in E(M_n(F))$ and let $e = e_1 + e_2 + \ldots + e_k$ be an orthogonal decomposition of e into the sum of* *minimal idempotents with $e_i = a_i b_i^T$, $a_i, b_i \in F^n$ for all $i = 1, 2, \dots, k$. Suppose h is an idempotent matrix of rank one. Then $h \leq e$ if and only if $h = \left(\sum_{i=1}^{k} \alpha_i a_i\right)\left(\sum_{j=1}^{k} \beta_j b_j^T\right)$ for some $\alpha_i, \beta_j \in F$ $(i, j = 1, \dots, k)$ with $\sum_{i=1}^{k} \alpha_i \beta_i = 1$.*

Proof. One implication is a straightforward calculation: if

$$h = \left(\sum_{i=1}^{k} \alpha_i a_i\right)\left(\sum_{j=1}^{k} \beta_j b_j^T\right)$$

then h is an idempotent since $\sum_{i=1}^{k} \alpha_i \beta_i = 1$ and $b_j^T a_i = \delta_{ij}$.

Furthermore,

$$he = \left(\sum_{i=1}^{k} \alpha_i a_i\right)\left(\sum_{j=1}^{k} \beta_j b_j^T\right)\left(\sum_{\ell=1}^{k} a_\ell b_\ell^T\right) = \left(\sum_{i=1}^{k} \alpha_i a_i\right)\left(\sum_{\ell=1}^{k} \beta_\ell b_\ell^T\right) = h$$

and similarly we check that $eh = h$.

Let us now prove the other implication. Suppose $h = xy^T$ is an arbitrary idempotent of rank one with $h \leq e$. Now, $xy^T = h = he = x\left(\sum_{i=1}^{k} (y^T a_i) b_i^T\right)$ and by Lemma 3.2 we have $y = \sum_{j=1}^{k} \beta_j b_j$ for some $\beta_1, \dots, \beta_k \in F$. Similarly, $h = eh$ gives us $x = \sum_{i=1}^{k} \alpha_i a_i$ for some $\alpha_1, \dots, \alpha_k \in F$. The condition $h^2 = h$ now also yields $\sum_{i=1}^{k} \alpha_i \beta_i = 1$. □

As a consequence, we now have the following theorem.

Theorem 3.4. *Let $n \geq 2$ and F a field. Choose $e \in E(M_n(F))$ and let $e = e_1 + e_2 + \cdots + e_k$ be an orthogonal decomposition of e into the sum of minimal idempotents with $e_i = a_i b_i^T$, $a_i, b_i \in F^n$ for all $i = 1, 2, \dots, k$. Suppose h is an idempotent matrix. Then $h \leq e$ if and only if $h = \sum_{i,j=1}^{k} \gamma_{i,j} a_i b_j^T$ for some $\gamma_{i,j} \in F$ $(i, j = 1, \dots, k)$ satisfying the equations $\sum_{\ell=1}^{k} \gamma_{i,\ell}\gamma_{\ell,j} = \gamma_{i,j}$ for all i and j.*

Proof. Suppose $h = \sum_{i,j=1}^{k} \gamma_{i,j} a_i b_j^T$ for some $\gamma_{i,j} \in F$ with $\sum_{\ell=1}^{k} \gamma_{i,\ell}\gamma_{\ell,j} = \gamma_{i,j}$ for all i and j. Observe that $he = eh = h$. Also, $h^2 = \sum_{i,j=1}^{k} \left(\sum_{\ell=1}^{k} \gamma_{i,\ell}\gamma_{\ell,j}\right) a_i b_j^T = h$.

Conversely, let $h \leq e$ and suppose $h = h_1 + h_2 + \ldots + h_r$ is an orthogonal sum of minimal idempotents. Then $h_t \leq h \leq e$ for each t, so by Lemma 3.3, $h_t = \left(\sum\limits_{i=1}^{k} \alpha_{t,i} a_i\right)\left(\sum\limits_{j=1}^{k} \beta_{t,j} b_j^T\right)$ for some $\alpha_{t,i}, \beta_{t,j} \in F$ $(i, j = 1, \ldots, k)$, which implies $h_t = \sum\limits_{i,j=1}^{k} \gamma_{t,i,j} a_i b_j^T$ for some $\gamma_{t,i,j} \in F$. Thus, $h = \sum\limits_{i,j=1}^{k} \gamma_{i,j} a_i b_j^T$ for some $\gamma_{i,j} \in F$ $(i, j = 1, \ldots, k)$. Since $h^2 = h$, we also have $\sum\limits_{i,j=1}^{k} \left(\sum\limits_{\ell=1}^{k} \gamma_{i,\ell}\gamma_{\ell,j}\right) a_i b_j^T = \sum\limits_{i,j=1}^{k} \gamma_{i,j} a_i b_j^T$ and by multiplying this with $a_j b_i^T$ we get $\sum\limits_{\ell=1}^{k} \gamma_{i,\ell}\gamma_{\ell,j} = \gamma_{i,j}$ for all i and j. □

In some special cases, we can now immediately conclude that the infimum of two idempotents is equal to zero.

Corollary 3.5. *Let $n \geq 2$ and F a field. Let $e = e_1 + e_2 + \cdots + e_k, f = f_1 + f_2 + \cdots + f_l \in E(M_n(F))$ be the orthogonal decompositions of idempotents e and f into the sum of minimal idempotents with $e_i = a_i b_i^T$, $a_i, b_i \in F^n$ for $i = 1, 2, \ldots, k$ and $f_j = c_j d_j^T$, $c_j, d_j \in F^n$ for $j = 1, 2, \ldots, l$. Denote the following linear spans in F^n: $\mathcal{A} = \mathcal{L}\{a_1, \ldots, a_k\}$, $\mathcal{B} = \mathcal{L}\{b_1, \ldots, b_k\}$, $\mathcal{C} = \mathcal{L}\{c_1, \ldots, c_l\}$ and $\mathcal{D} = \mathcal{L}\{d_1, \ldots, d_l\}$. If $\mathcal{A} \cap \mathcal{C} = \{0\}$ or $\mathcal{B} \cap \mathcal{D} = \{0\}$ then $e \cap f = 0$.*

Proof. Suppose we have an idempotent h such that $h \leq e, f$. Decompose $h = h_1 + h_2 + \cdots + h_r$ as an orthogonal sum of minimal idempotents. Then $h_t \leq h \leq e, f$ for each t, so by Lemma 3.3, $h_t = \left(\sum\limits_{i=1}^{k} \alpha_{t,i} a_i\right)\left(\sum\limits_{j=1}^{k} \beta_{t,j} b_j^T\right) = \left(\sum\limits_{i=1}^{k} \gamma_{t,i} c_i\right)\left(\sum\limits_{j=1}^{k} \delta_{t,j} d_j^T\right)$ for some $\alpha_{t,i}, \beta_{t,j}, \gamma_{t,i}, \delta_{t,j} \in F$. Lemma 3.2 now implies that $h_t = 0$. □

Example 3.6. Let R be a ring of 4×4 matrices over a field F and let

$$e = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad f = \begin{bmatrix} 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & -1 & 1 & 1 \end{bmatrix} \in E(R).$$

One can easily check that for $a_1 = b_1 = (1, 0, 0, 0)^T$, $a_2 = b_2 = (0, 0, 1, 0)^T$, $c_1 = (0, 1, 1, 0)^T, d_1 = (0, 1, -1, 0)^T$, $c_2 = (0, -1, -1, 1)^T$ and $d_2 = (1, -1, 1, 1)^T$ we have orthogonal decompositions to the sum of minimal idempotents, $e =$

$a_1b_1^T + a_2b_2^T$ and $f = c_1d_1^T + c_2d_2^T$. By Corollary 3.5, we have $e \cap f = 0$. Note that in this case e and f are generalized commuting, so $e \cap f \in \langle e, f \rangle$.

Now, let also

$$g = \begin{bmatrix} 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \in E(R).$$

We have $g = c_1'd_1'^T + c_2'd_2'^T$ for $c_1' = (0,1,1,0)^T$, $d_1' = (0,1,-1,0)^T$, $c_2' = (0,1,1,0)^T$ and $d_2' = (0,0,1,1)^T$. Again, by Corollary 3.5, we have $e \cap g = 0$. In this case, however, e and g are not generalized commuting, so $e \cap g \notin \langle e, g \rangle$.

References

[1] G. Calugareanu, Rings with lattices of idempotents, *Comm. Algebra* **38** (2010), 1050–1056.

[2] K. Cvetko-Vah and J. Leech, Rings whose idempotents form a multiplicative set, *Comm. Algebra* **40** (2012), 3288–3307.

[3] D. Dolžan, Multiplicative sets of idempotents in a finite ring, *J. Algebra* **304** (2006), 271–277.

[4] J. Han, T.-K. Lee, S. Park and T.-L. Wong, A note on lattices of idempotents in algebras, *Publ. Math. Debrecen* **86** (2015), 183–186.

[5] T. Y. Lam, Exercises in Classical Ring Theory, Problem Books in Mathematics, *Springer-Verlag*, *New York*, 1995.

[6] B. R. McDonald, Finite Rings with Identity, Pure and Applied Mathematics, Vol. **28**, *Marcel Dekker, Inc.*, *New York*, 1974.

DAVID DOLŽAN
DEPARTMENT OF MATHEMATICS
FACULTY OF MATHEMATICS AND PHYSICS
UNIVERSITY OF LJUBLJANA
JADRANSKA 21
SI-1000 LJUBLJANA
SLOVENIA

E-mail: david.dolzan@fmf.uni-lj.si

(Received April 7, 2015; revised January 26, 2016)