RINGS WITH LATTICES OF IDEMPOTENTS

Grigore Călugăreanu

Department of Mathematics and Informatics, “Babeș-Bolyai” University, Cluj-Napoca, Romania

The central idempotents of any ring with identity form a Boolean algebra. This result is largely extended for rings with generalized commuting idempotents.

Key Words: Boolean algebra; Generalized commuting idempotents; Principal ideals generated by idempotents.

2000 Mathematics Subject Classification: 16U80; 06E20; 06B99.

1. INTRODUCTION

In associating lattices to rings with identity, attention was mainly paid to right (or left) principal ideals, that is, the set \( \{aR : a \in R\} \) naturally ordered by inclusion. A celebrated class of rings, the regular rings, was defined by John von Neumann. For such rings, every right principal ideal is (also) generated by an idempotent, and \( \{aR : a \in R\} = \{eR : e \in \text{Id}(R)\} \) forms a complemented distributive lattice (i.e., a Boolean algebra and/or a Boolean ring) with respect to addition and intersection of such ideals. Therefore, this is a sublattice of the (complete) lattice \( I_R(R) \) of all the right ideals of \( R \).

Since right annihilators in any ring always form a (complete) lattice, which is not generally a sublattice of \( I_R(R) \), conditions were imposed in order to connect this lattice to the principal ideals: a ring is right Rickart if every right annihilator of any element is (a principal right ideal) generated by an idempotent, and right Baer, if all the right annihilators are principal right ideals generated by idempotents.

Even more special conditions can be found in the literature: a ring is an ISS-ring (see [3]) if for any idempotents \( e, f \in R \) there exists an idempotent \( g \in R \) with \( eR + fR = gR \). It is proven that \( R \) has ISS and the ACC on idempotent generated right ideals if and only if the idempotent generated right ideals form a ACC lattice under addition and intersection. Or, a ring \( R \) has \( AC1 \) (see [1]) if the set of all the right annihilators forms a sublattice of \( I_R(R) \), and has \( AC3 \) if this is a complete sublattice of \( I_R(R) \). Of course, left versions of all these are available.

Received August 11, 2008; Revised January 15, 2009. Communicated by T. Albu.

Address correspondence to Dr. Grigore Călugăreanu, Facultatea de Matematică, Informatică, Universitatea “Babeș-Bolyai”, Str. M. Kogălniceanu nr. 1, Cluj-Napoca 400084, Romania; E-mail: calug2001@yahoo.com
However, when it comes to \((\text{Id}(R), \leq)\) (the poset of all the idempotents), there seems to be no progress from another celebrated result: \(B(R) = Z(R) \cap \text{Id}(R)\), that is, the set of all the central idempotents, forms a Boolean algebra (and so a Boolean ring and/or a distributive complemented lattice) with respect to inf \([e, f] = ef\) and sup \([e, f] = e + f - ef \) (together with ring multiplication and the special addition \(e \boxplus f = e + f - 2ef = (e - f)^2\)).

The aim of this note is to extend this result.

In the sequel, \(\text{Id}(R)\) denotes the set of all the idempotent elements in a ring with identity \(R\), and, for \(a, b \in R\) we use the notation \(a \leq b\) if \(a = ab = ba\). It is readily checked that this (binary) relation is transitive and antisymmetric on \(R\). However, it is reflexive (and so, a partial order) only when restricted to the set \(\text{Id}(R)\). Two idempotents \(e, f\) are orthogonal if \(ef = fe = 0\), and isomorphic if \(e = ab\) and \(f = ba\) for suitable elements \(a, b \in R\). Zero and 1 are the trivial (orthogonal) idempotents of any ring. For an idempotent \(e\), \(e' = 1 - e\) is the complementary idempotent. For two idempotents \(e, f\), we denote by \(\langle e, f \rangle\), the subsemigroup of the multiplicative monoid of the ring, generated by \(e\) and \(f\).

The main results we obtain are the following ones.

**Theorem.** In the poset \((\text{Id}(R), \leq)\), two idempotents \(e, f\) have a greatest lower bound and a least upper bound with \(\inf\{e, f\} \in \langle e, f \rangle\), if and only if \(e\) and \(f\) are generalized commuting idempotents.

**Proposition.** The poset \((\text{Id}(R), \leq)\) has only generalized commuting idempotents if and only if all idempotents are central (i.e., \(\text{Id}(R) = B(R)\)).

### 2. GENERALIZED COMMUTING IDEMPOTENTS

For the first part of this section, suppose \(R\) is a (multiplicatively written) semigroup. Two idempotents \(e, f\) are called generalized commuting idempotents if there exists a positive integer \(n\) such that \((ef)^n = (fe)^n\) or, \((ef)^n e = (fe)^n f\). It is easy to prove that there is a strict hierarchy for these conditions, namely,

\[
ef = fe \implies efe = fef \implies \cdots \implies (ef)^n = (fe)^n \implies (ef)^n e = (fe)^n f \implies \cdots.
\]

For instance, \((\ast)\) is proved as follows: by left multiplication with \(e\), we first obtain \((ef)^n = e(fe)^n\); then by left multiplication with \(f\), we obtain \(f(ef)^n = (fe)^n\). Hence also \((ef)^n e = e(fe)^n = (fe)^n f\).

These implications cannot be reversed. As an example, for the first implication: in the \(2 \times 2\) matrix ring over \(\mathbb{Z}\), take \(e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\) and \(f = \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix}\). Then \(efe = fef = 0\), the zero matrix (and so \(e, f\) are generalized commuting idempotents), but \(ef = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = fe\).

If \(f' = I_2 - f = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}\) is the complementary idempotent, then \(e = ef' = ef' e = (ef')^2 = \cdots\) and \(f' = f + e\). In this case, \(f' = (f e)^2 = \cdots\). Hence \(e\) and \(f'\) are not generalized commuting idempotents.
Remarks. 1) More can be proved: if for instance \((ef)^n = (fe)^n\), then not only (as we already saw) \((ef)^ne = (fe)^nf\), but \((ef)^n = (ef)^ne = (fe)^nf = (fe)^n\), and all elements “to the right” are equal.

2) Therefore, using the above sequence, a commuting index can be introduced for any two idempotents: the least positive integer \(n\), if any, such that \((ef)^n = (fe)^n\) or, \((ef)^n e = (fe)^n f\).

3) Clearly, all elements above are contained in the subsemigroup of \(R\) generated by \(e\) and \(f\), denoted \(\langle e, f\rangle\). Actually, since we only consider idempotents, elements in \(\langle e, f\rangle\), are of four possible forms: \((ef)^n\), \((ef)^ne\), \((fe)^n\), and \((fe)^nf\), for some positive integer \(n\).

**Proposition 1.** Two idempotents \(e, f\) are generalized commuting if and only if \(\langle e\rangle \cap \langle f\rangle = \emptyset\).

**Proof.** The condition is clearly necessary. To check that it is also sufficient, suppose \((ef)^n = (fe)^m\) for positive integers \(n\) and \(m\). If \(k = \max(n, m)\), we show that \((ef)^k = (fe)^k\), and so these are generalized commuting idempotents. Indeed, if \((ef)^n = (fe)^m\), then checking \((ef)^1 = (ef)^{n+1} = (ef)^{n+2} = \cdots\) and \((fe)^m = (fe)^{m+1} = (fe)^{m+2} = \cdots\) will do. Here is a sample: \((ef)^{n+1} = (ef)^ne = (fe)^mef = (fe)^nf = (ef)^nf = (ef)^n\).

Once again, more can be shown about the intermediate products: \((ef)^ne = (fe)^m = (ef)^n\).

Further, idempotents in a ring \(R\) (with identity) are called generalized commuting whenever they are generalized commuting in the multiplicative monoid of the ring.

We first prove some technical equalities gathered in the following lemma.

**Lemma 2.** For any two idempotents \(e, f\) in a ring \(R\), the following hold:

a) If \(s = e + f - ef - fe + efe + fef - \cdots + e(fe)^{n-1} + f(ef)^{n-1} - (ef)^n\) then \(es = s\) and \(sf = f\); but

b) \(se = e + (fe)^n \text{ and } fs = f + (fe)^n - f(ef)^n\);  

c) \((\text{de Morgan})\) \(s = 1 - [(1 - e)(1 - f)]^n\), and similarly;  

d) \(e + f - ef - fe + efe + fef - \cdots - (ef)^n - (fe)^n + (ef)^ne = 1 - [(1 - e)(1 - f)]^n\) \( (1 - e)\).

**Proof.** We will just mention the induction step \((n \rightarrow n + 1)\) in the proof of an equality which is equivalent to (c), that is,

\[ a = [(1 - e)(1 - f)]^n = 1 - e - f + ef + fe - \cdots + (ef)^n \]

(clearly true for \(n = 1\) or 2).

\[ [(1 - e)(1 - f)]^{n+1} = (1 - e)[1 - f][1 - e](1 - f)\]

\[ = a - (1 - e)fa = a - (1 - e)f(1 - s) \]
as desired. \qed

**Theorem 3.** In \((\text{Id}(R), \subseteq)\), generalized commuting pairs of idempotents have a greatest lower bound and a least upper bound.

**Proof.** Case 1. We show that if \((ef)^n = (fe)^n\), then for the idempotents \(e, f\), the greatest lower bound exists and

\[
\inf\{e, f\} = (ef)^n = (fe)^n,
\]

respectively, the least upper bound exists and

\[
\sup\{e, f\} = e + f - ef - fe + efe + fef - \cdots + e(fe)^{n-1} + f(ef)^{n-1} - (ef)^n.
\]

First note that \((ef)^n \leq e\) holds since \(e(ef)^n = (ef)^n\) is true for any idempotents and \((ef)^n e = e(ef)^n = (ef)^n = (ef)^n\), using the hypothesis. Similarly, \((fe)^n \leq f\) and so, \((ef)^n = (fe)^n\) is a lower bound for \(e, f\). If \(a \in \text{Id}(R)\) and \(a \leq e\) and \(a \leq f\), any product of \(a\) with any product of \(e\) and \(f\) equals \(a\). Hence also \(a = a(ef)^n = (ef)^n a\) and so \(a \leq (ef)^n\), which solves the \(\inf\) part.

Notice that \((ef)^n = (fe)^n\) is an idempotent: indeed,

\[
(ef)^n(ef)^n = e(ef)^n f(ef)^n = e(ef)^n f(ef)^n = (ef)^n (ef)^n = \cdots = (ef)^n.
\]

As for the \(\sup\), one first verifies \(e \leq e + f - ef - fe + \cdots + e(fe)^{n-1} + f(ef)^{n-1} - (ef)^n\) (half is \((a)\) in the previous lemma, the other half needs—see \((b)\)—the hypothesis \((ef)^n = (fe)^n\), respectively, \(f \leq e + f - ef - fe + \cdots + e(fe)^{n-1} + f(ef)^{n-1} - (ef)^n\) (similar). Therefore, (by hypothesis) the common element is an upper bound for \(e, f\). Finally, if \(a \in \text{Id}(R)\) and \(e \leq a\) and \(f \leq a\), multiplication of any sum of products of \(e, f\) by \(a\) does not change this sum of products. Hence \(e + f - ef - fe + \cdots + e(fe)^{n-1} + f(ef)^{n-1} - (ef)^n \leq a\). Thus

\[
\sup\{e, f\} = e + f - ef - fe + \cdots + e(fe)^{n-1} + f(ef)^{n-1} - (ef)^n.
\]

Denote by \(s = \sup\{e, f\}\). Since \(e, f \leq s\), taking \(a = s\) above, multiplication of any sum of products of \(e, f\) by \(s\) does not change this sum of products. Therefore, \(s^2 = s\) and so \(s\) is an idempotent.

Case 2. We show that if \((ef)^n e = (fe)^n f\), then for the idempotents \(e, f\), the greatest lower bound exists and

\[
\inf\{e, f\} = (ef)^n e = (fe)^n f,
\]

respectively, the least upper bound exists and

\[
\sup\{e, f\} = e + f - ef - fe + efe + fef - \cdots - (ef)^n - (fe)^n + (ef)^n e.
\]
The verifications are analogous. However, now the hypothesis is not necessary in order to check \( e(f)e^n \leq e \), or \( (fe)^n f \leq f \), respectively, \( e \leq e + f - ef + efe + ef - \cdots - (ef)^n - (fe)^n + (ef)^ne \), or \( f \leq e + f - ef + efe + ef - \cdots - (ef)^n - (fe)^n + (fe)^nf \).

A converse of the previous theorem also holds.

Indeed, in a similar vein, some arguments in its proof may be refined and give the following proposition (we skip the details).

**Proposition 4.** Let \( e, f \in \text{Id}(R) \). (a) There exists \( \inf\{e, f\} = (ef)^n \) if and only if \( (ef)^n = (ef)^ne = (fe)^nf \). (b) There exists \( \sup\{e, f\} = e + f - \cdots - (ef)^n \) if and only if \( (fe)^n = (ef)^ne = (fe)^nf \). A similar statement holds for \( \inf\{e, f\} = (ef)^ne \) and \( \sup\{e, f\} = e + f - \cdots - (ef)^n - (fe)^n + (ef)^ne \).

**Corollary 5.** Let \( e, f \in \text{Id}(R) \). Then \( \inf\{e, f\} \) exists and equals \( (ef)^n \), and \( \sup\{e, f\} \) exists and equals \( e + f - \cdots - (ef)^n \) if and only if \( (ef)^n = (fe)^n \). A similar statement holds for \( \inf\{e, f\} = (ef)^ne \) and \( \sup\{e, f\} = e + f - \cdots - (ef)^n - (fe)^n + (ef)^ne \).

**Proposition 6.** In the poset \( (\text{Id}(R), \leq) \), for two idempotents \( e, f, \inf\{e, f\} = (ef)^n \) (or \( (ef)^ne \)) and \( \sup\{e, f\} = e + f - \cdots - (ef)^n \) (respectively, \( e + f - \cdots - (ef)^n - (fe)^n + (ef)^ne \)), with suitable positive integers \( n \) depending on the idempotents \( e, f \) if and only if \( e \) and \( f \) are generalized commuting idempotents.

We can finally give the following characterization.

**Theorem 7.** In the poset \( (\text{Id}(R), \leq) \), two idempotents \( e, f \) have a greatest lower bound and a least upper bound with \( \inf\{e, f\} \in \langle e, f \rangle \), if and only if the idempotents \( e \) and \( f \) are generalized commuting.

**Proof.** By the previous proposition, the condition is sufficient. To prove it is also necessary, suppose (we have listed above the only four possibilities), say, \( i = \inf\{e, f\} = (ef)^n \). By the inf definition (and partial order \( \leq \)), if \( i = fi = ie = ei = i \). Therefore, \( (ef)^ne = ie = i = fi = f(ef)^n \), and we have generalized commutativity. The other three cases are analogous. \( \square \)

**Corollary 8.** If idempotents in a ring \( R \) commute, then \( (\text{Id}(R), \leq) \) forms a lattice with respect to \( \inf\{e, f\} = ef \) and \( \sup\{e, f\} = e + f - ef \). More, this is a Boolean algebra.

**Corollary 9.** Let \( e \) and \( f \) be orthogonal idempotents in an arbitrary ring. Then there is \( \inf\{e, f\} = 0 \), and there is \( \sup\{e, f\} = e + f \).

Actually, a direct proof of this last corollary is an easy exercise.

**Corollary 10.** \( B(R) = Z(R) \cap \text{Id}(R) \) forms a Boolean algebra.

It should be also noticed that generalized commutativity of idempotents is not sufficient for

\[ \inf\{e, f'\} = 0 \iff \inf\{e, f\} = e, \]

equivalence which holds in Boolean algebras.
Passage to the complementary idempotent does not even preserve the "commuting index" (i.e., \((ef)^n = (fe)^n\) does not imply \((ef')^n = (f'e')^n\)).

To check these two last claims, the example already given beginning of this section can be used.

3. RINGS WITH ONLY GENERALIZED IDEMPOTENTS ARE ABELIAN

It is well-known (and somehow surprising) that if (and only if) idempotents in a ring \(R\) commute, then the ring is Abelian (i.e., all idempotents are central). As we will see below, even less is sufficient in order to have \(B(R) = \text{Id}(R)\).

Now, since generally

\[ e, f \in Z(R) \Rightarrow e, f \text{ commute} \Rightarrow e, f \text{ generalized commute}, \]

but examples (e.g., our example in the previous section) show that none of these implications can be reversed, one would expect a ring having only generalized idempotents to have a lattice of idempotents which should be a genuine generalization of the Boolean algebra \(B(R)\).

In the next result we show that (unfortunately) it is not.

**Proposition 11.** For a ring \(R\) the following conditions are equivalent:

(a) \(R\) is Abelian (i.e., all idempotents are central, or equivalently, \(B(R) = \text{Id}(R)\));
(b) in \(R\) idempotent and nilpotent elements commute;
(c) in \(R\) idempotents commute;
(d) every idempotent \(e\) commutes with all the idempotents which are isomorphic to \(e\);
(e) \(R\) has only generalized commuting idempotents;
(f) every idempotent \(e\) generalized commutes with all the idempotents which are isomorphic to \(e\).

**Proof.** Since most of these results are known (see Exercises 12.7 and 22.3A [2]), we prove only the generalized commuting statement \((f) \implies (a)\).

Suppose the idempotent \(e\) is not central. Then there is \(r \in R\) such that \(er \neq re\), or equivalently, \(er \neq 0\) or \(\bar{r}e \neq 0\). In the first case, consider the idempotent \(f = e + er\), which is different from \(e\). It can be checked that \(ef = f\) and \(fe = e\) (see also Exercise 21.4 [2]), so these are isomorphic idempotents. Therefore, \(e = fe = efe = (fe)^2 = \cdots\) and \(f = ef = fef = (ef)^2 = \cdots\), and \(e\) is not generalized commuting with \(f\).

In the second case, if \(\bar{r}e \neq 0\), one deals similarly with the idempotent \(g = e + \bar{r}e\).

**Remark.** For the proof of \((c) \implies (a)\), the nilpotent elements \(er\bar{e}\) respectively \(\bar{e}r\) (indeed, \((er\bar{e})^2 = (\bar{e}r)^2 = 0\) are used. Even extending the definition of generalized commutativity to arbitrary elements in a ring (including the nilpotent ones), \(n = er\bar{e}\) (or \(\bar{e}r\)) is no more suitable for a "generalized" statement like \((c)\): indeed, \(0 = ne = ene = nen = \cdots\), so now \(e\) and \(n\) are generalized commuting.
ACKNOWLEDGMENT

The author is grateful for the referee’s comments which led to the addition of the last section, this way improving the research.

REFERENCES