IDEMPOTENTS WHICH ARE PRODUCTS OF TWO NILPOTENTS

GRIGORE CĂLUGĂREANU, HORIA F. POP

Abstract. Over any GCD (greatest common divisors exist) commutative domain we show that the nontrivial 2×2 idempotent matrices are products of two nilpotent matrices. In order to find explicitly such decompositions, two procedures are described. Assisted by computer, we were able to find an example of idempotent 2×2 matrix over $\mathbb{Z}[\sqrt{-5}]$ which shows that the GCD condition is (sufficient but) not necessary. Finally, a generalization is discussed and some open questions stated.

1. Introduction

Asking when a product of two nilpotents is an idempotent or else when a product of two idempotents is nilpotent is trivial in commutative rings. Indeed, as products of idempotents are idempotent and products of nilpotents are nilpotent, in both cases 0 is the only answer.

However, in non-commutative rings, and in particular, in matrix rings, examples abound. Using the matrix units notation, $E_{12}E_{21} = E_{11}$ is an example of idempotent which is a product of two nilpotents and $E_{12} = E_{11}(E_{12} + E_{22})$ is an example of nilpotent which is a product of two idempotents.

In [1], a (square) matrix was said to have *property 2I* if it is a product of two idempotents, and *property 2N* if it is a product of two nilpotents.

Recall that a commutative domain R is called *GCD* if for each pair $a, b \in R$, the greatest common divisor $\gcd(a, b)$ exists. Examples of GCD domains include unique factorization domains (UFD), principal ideal domains (PID), Euclidean domains and fields.

Also in [1], it was noticed that (Cor. 3) *nilpotent 2×2 matrices over GCD domains have property 2I.*

In this note (which could be considered as a continuation of [1]), using some known similarities, in Section 2 we show that *the (nontrivial) idempotent 2×2 matrices over GCD commutative domains have property 2N*, that is, are products of two nilpotent 2×2 matrices. Moreover, in Section 3, we develop two procedures, given any nontrivial idempotent 2×2 matrix, to find a 2N decomposition. We can discard the trivial idempotents in any ring from our discussion: 0 obviously has the property 2N and 1 has not property 2N (if $1 = t_1t_2$ and $t_2^n = 0 \neq t_2^{n-1}$, by right multiplication with t_2^{n-1} we get a contradiction). For square matrices over commutative rings this is obvious by determinant comparison.

Additionally, assisted by computer, in Section 4 we produce an example of idempotent matrix over a (not GCD) domain which still has the property 2N. This way,

Keywords: idempotent matrix, nilpotent matrix, quadratic systems of equations, 2×2 matrix, GCD domain, ID ring. MSC 2020 Classification: 15B33, 15B99, 11D09, 11T99.

for the property 2N, the GCD condition is sufficient but turns out to be not necessary. In Section 5, over commutative domains, we provide a criterion for 2×2 nontrivial idempotent matrix which have not a 2N decomposition. In the final section we discuss the generalization of our results to ID rings and state two open questions. All domains we consider are supposed commutative. An Appendix is added giving details on the nonexistence of some gcd's in $\mathbb{Z}[\sqrt{-5}]$.

For additional references related to our subject see [3], [5], [6] and [8].

2. The proof

Over any GCD domain it is easy to see that every nontrivial 2×2 idempotent matrix is similar to E_{11}. Because it will be useful later on, below we provide a proof for a more general statement.

Proposition 2.1. *Over any commutative domain D, a nontrivial 2×2 idempotent matrix $\begin{bmatrix} a & b \\ c & 1-a \end{bmatrix}$ is similar to E_{11}, whenever $\gcd(a, c)$ or $\gcd(a, b)$ exists and for any $u, v, w \in D$, $\gcd(u, v) = 1$ and $u \mid vw$ imply $u \mid w$.*

Proof. Let $E = \begin{bmatrix} a & b \\ c & 1-a \end{bmatrix}$ be a nontrivial idempotent, i.e. $bc = a(1-a)$.

First, for $a = 0$ and arbitrary b, c, over any ring (possible not commutative nor domain) we have the following similarities: $\begin{bmatrix} 0 & b \\ 0 & 1 \end{bmatrix} = PE_{11}P^{-1}$ for $P = \begin{bmatrix} b & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ c & 1 \end{bmatrix} = QE_{11}Q^{-1}$ for $Q = \begin{bmatrix} 0 & 1 \\ 1 & -c \end{bmatrix}$.

Next, assume $a \neq 0$ and let $x = \gcd(a, c)$. If $a = xy$ and $c = xx'$ it follows that $\gcd(y, x') = 1$. By cancellation out x we get $bx' = y(1-a)$, and so, by our last hypothesis, y divides b, say $b = yy'$. We also have $x'y' = 1 - a$. Now take

$$P = \begin{bmatrix} x & y' \\ -x' & y \end{bmatrix}.$$

One can check that $\det(P) = 1$ and $PE = E_{11}P$. Hence E is similar to E_{11}. If $\gcd(a, b)$ exists, we just mention that a matrix is similar to E_{11} iff so is its transpose. □

Corollary 2.2. *Over any GCD (commutative) domain, every nontrivial 2×2 idempotent matrix is similar to E_{11}.*

Remark. The existence of these gcd′s are only sufficient but not necessary conditions. In Section 4 an example is given of a 2×2 nontrivial idempotent which has a 2N decomposition but none of the gcd′s exists.

This enables us to prove the following

Theorem 2.3. *All nontrivial idempotent 2×2 matrices over GCD domains have property 2N.*

Proof. It is easy to see that having property 2N is invariant under conjugations. To be specific, if $e^2 = e = t_1t_2$ and u is a unit, then $u^{-1}eu = (u^{-1}t_1u)(u^{-1}t_2u)$. Thus, if an idempotent has property 2N, every conjugate has property 2N, too.

Therefore, according to the previous proposition, it suffices to show that E_{11} has a 2N decomposition. This was already noticed in the introduction: $E_{11} = E_{12}E_{21}$. □

For $a = 0$ here are some 2N decompositions:

$$\begin{bmatrix} 0 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} b & -b^2 \\ 1 & -b \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & 0 \\ c & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c & 1 \\ -c^2 & -c \end{bmatrix}.$$

3. Finding a 2N decomposition

In this section, for any 2×2 nontrivial idempotent matrix, we provide two algorithms for finding a 2N decomposition.

The first arises from Proposition 2.1.

Theorem 3.1. *Over any GCD domain, let* $E = \begin{bmatrix} a & b \\ c & 1-a \end{bmatrix}$ *be a nontrivial idempotent,* $x = \gcd(a, c)$, $a = xy$, $c = xx'$ *and* $b = yy'$, *as in Proposition 2.1. Then*

$E = \begin{bmatrix} -x'y & y^2 \\ -x'^2 & x'y \end{bmatrix} \begin{bmatrix} -xy' & -y'^2 \\ x^2 & xy' \end{bmatrix}$ *is a 2N decomposition.*

Proof. Indeed, if $E = PE_{11}P^{-1}$ then $E = (P^{-1}E_{12}P)(P^{-1}E_{21}P)$ is a 2N decomposition. We just use $P = \begin{bmatrix} x & y' \\ -x' & y \end{bmatrix}$ and $P^{-1} = \begin{bmatrix} y & -y' \\ x' & x \end{bmatrix}$ since $\det(P) = 1$. By computation, it is easy to check that $\begin{bmatrix} -x'y & y^2 \\ -x'^2 & x'y \end{bmatrix} \begin{bmatrix} -xy' & -y'^2 \\ x^2 & xy' \end{bmatrix} = \begin{bmatrix} a^2+bc & b(xy+x'y') \\ c(xy+x'y') & (1-a)^2+bc \end{bmatrix} = E$ (recall that $x'y' = 1-a$). □

Just to ease the reading of this 2N decomposition, we can (formally) use fractions as follows:

$$\left(\frac{1}{\gcd^2(a,c)} \begin{bmatrix} -ac & a^2 \\ -c^2 & ac \end{bmatrix}\right) \left(\gcd^2(a,c) \begin{bmatrix} -\frac{b}{a} & -(\frac{b}{a})^2 \\ 1 & \frac{b}{a} \end{bmatrix}\right).$$

If $a \mid b$ then $\gcd(a, c)$ can be deleted.

Remark. 1) An analogous formula can be written if $\gcd(a, b)$ exists.

2) From the previously written 2N decomposition it follows that *over any commutative domain* D, a nontrivial idempotent 2×2 matrix $\begin{bmatrix} a & b \\ c & 1-a \end{bmatrix}$ has a 2N decomposition if $\gcd(a, c)$ (or $\gcd(a, b)$ by transpose) exists and for any $u, v, w \in D$, $\gcd(u, v) = 1$ and $u \mid vw$ imply $u \mid w$. In particular, this holds if the entries on the first column (or first row) divide one another.

As for **the second** algorithm, we can start over commutative domains, and we recall from [1] the results concerning the two relevant cases (if a zero determinant 2×2 matrix has a zero entry then it has (at least) another zero entry, on the same row, or on the same column; matrices with three nonzero entries have nonzero determinant).

For matrices with zero second row, we had

Theorem 3.2. *Let* R *be a commutative domain. The matrix* $A = \begin{bmatrix} \alpha & \beta \\ 0 & 0 \end{bmatrix}$ *has property 2N if and only if* $\beta = 0$ *or* $\alpha, \beta \neq 0$ *and* α *divides* β^2.

Since such (nonzero) idempotent 2×2 matrices have trace equal to 1, it is straightforward that

Corollary 3.3. *Over any commutative domain, the idempotent matrix* $E = \begin{bmatrix} \alpha & \beta \\ 0 & 0 \end{bmatrix}$ *has the property 2N iff* $\alpha = 1$.

The 2N decomposition for $\begin{bmatrix} 1 & \beta \\ 0 & 0 \end{bmatrix}$ is $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} -\beta & -\beta^2 \\ 1 & \beta \end{bmatrix}$, 2N decomposition which holds over any (possibly not commutative) ring.

Finally, for matrices with only nonzero entries, we had

Theorem 3.4. *Let* $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ *be a singular matrix with nonzero entries over a commutative domain R, i.e.,* $\alpha\delta = \beta\gamma$. *The matrix A has property 2N if and only if* $\alpha + \delta$ *divides* $\alpha\delta$ *and the equation*

$$(\alpha + \delta)ax = \alpha\delta$$

in the unknowns a, x *has at least one solution* (a, x) *for which* α *divides* βx, β *divides* αx, γ *divides* αa *and* α *divides* γa.

Since for any nontrivial idempotent 2×2 matrix over a commutative domain, the trace $Tr(E) = \alpha + \delta = 1$, the divisibility always holds, we can eliminate $\delta = 1 - \alpha$ and use $\alpha(1 - \alpha) = \beta\gamma$. The equation becomes $ax = \alpha\delta = \alpha(1 - \alpha) = \beta\gamma$.

We successively simplify the conditions in the previous theorem now adding the GCD hypothesis.

First a simple but useful

Lemma 3.5. *Let* $\alpha, \beta, \gamma \in R$, *a GCD domain, and let* $d = \gcd(\alpha, \beta)$ *with* $\alpha = d\alpha'$, $\beta = d\beta'$. *The following conditions are equivalent.*

(i) $\alpha \mid \beta\gamma$ *and* $\beta \mid \alpha\gamma$;

(ii) $\alpha'\beta' \mid \gamma$.

Proof. The case when $\alpha = \beta = 0$ being trivial, in the sequel we assume α, β not both zero. Hence $d \neq 0$ and since R is a domain, we can cancel d when necessary. Also note that $\gcd(\alpha', \beta') = 1$.

(i) $\Leftrightarrow$ (ii) $\alpha \mid \beta\gamma$ is successively equivalent to $d\alpha' \mid d\beta'\gamma$ or $\alpha' \mid \beta'\gamma$ or $\alpha' \mid \gamma$. Similarly, $\beta \mid \alpha\gamma$ is equivalent to $\beta' \mid \gamma$ and so (i) is equivalent to (ii). The last equivalence uses: $\alpha', \beta' \mid \gamma$ and $\gcd(\alpha', \beta') = 1$ imply $\alpha'\beta' \mid \gamma$. □

Recall that if $\gcd(a, b) = 1$ then in any GCD domain $\gcd(a, c)\gcd(b, c) = \gcd(ab, c)$, sometimes called the *multiplicative* property of the gcd. In any ring, $\gcd(ab, c) \mid \gcd(a, c)\gcd(b, c)$, holds whenever these gcd′s exist.

Lemma 3.6. *If* $ab = cdef$, $\gcd(a, b) = 1$, $c, d \mid a$ *and* $e, f \mid b$ *then* $a = cd$, $b = ef$.

Proof. As $c, d \mid a$ and $\gcd(a, b) = 1$ it follows that $\gcd(c, b) = 1 = \gcd(d, b)$ and so $\gcd(cd, b) = 1$. Since $cd \mid ab$ we get $cd \mid a$. The converse is analogous: $\gcd(e, a) = 1 = \gcd(f, a)$ implies $\gcd(ef, a) = 1$ and as $a \mid cdef$, $a \mid cd$ follows. □

Lemma 3.7. *If* $\alpha(1 - \alpha) = \beta\gamma$, $d = \gcd(\alpha, \beta)$ *and* $d_1 = \gcd(\alpha, \gamma)$ *then* $\alpha = dd_1$.

Proof. We also consider $d' = \gcd(1 - \alpha, \beta)$ and $d'_1 = \gcd(1 - \alpha, \gamma)$. Using the multiplicative property, as $\gcd(\alpha, 1 - \alpha) = 1$, we get $\beta = \gcd(\beta, \beta\gamma) = \gcd(\beta, \alpha(1 - \alpha)) = \gcd(\beta, \alpha)\gcd(\beta, 1 - \alpha) = dd'$ and similarly $\gamma = d_1 d'_1$. It remains just to use the previous lemma for $\alpha = dd_1$ (and $1 - \alpha = d'd'_1$). □

Second proof for Theorem 2.3.

Proof. Denote $d = \gcd(\alpha, \beta)$, $d_1 = \gcd(\alpha, \gamma)$. Thus $\alpha = d\alpha'$, $\beta = d\beta'$, $\alpha = d_1\alpha''$ and $\gamma = d_1\gamma''$ and, by the Lemma 3.5, the divisibility conditions in Theorem 3.4, for the solution (a, x), are equivalent to $\alpha'\beta' \mid x$ and $\alpha''\gamma'' \mid a$.

If $x = \alpha'\beta'l$ and $a = \alpha''\gamma''k$ then $ax = \beta\gamma$ can be cancelled to $\alpha'\alpha''kl = dd_1$. Multiplying by dd_1 this gives $\alpha \mid dd_1$. Using the previous lemma, it follows that the solution $(a, x) = (\alpha''\gamma'', \alpha'\beta')$ is suitable ($k = l = 1$). □

Examples. 1) $A = \begin{bmatrix} 3 & 3 \\ -2 & -2 \end{bmatrix}$. Since $a \mid b$, a 2N decomposition (using any of the two procedures) is $\begin{bmatrix} 6 & 9 \\ -4 & -6 \end{bmatrix} \begin{bmatrix} -1 & -1 \\ 1 & 1 \end{bmatrix}$.

2) $A = \begin{bmatrix} 3 & 6 \\ -1 & -2 \end{bmatrix}$. The first procedure gives $\begin{bmatrix} 3 & 9 \\ -1 & -3 \end{bmatrix} \begin{bmatrix} -2 & -4 \\ 1 & 2 \end{bmatrix}$. As for the second, the equation $ax = -6$ has several solutions (a, x):

$(\pm 1, \mp 6), (\pm 2, \mp 3)$ and symmetric. Only $(a, x) = (\pm 3, \mp 2)$ verify the required divisibilities. We get the previous 2N decomposition and the "minus" one: in any ring, if $a = t_1t_2$ is a 2N decomposition then $a = (-t_1)(-t_2)$ is a 2N decomposition too.

3) $A = \begin{bmatrix} 4 & 6 \\ -2 & -3 \end{bmatrix}$. Now a does not divide b (nor c), so for the first procedure, as $\gcd(a, c) = 2$, the 2N decomposition is $\frac{1}{4}\begin{bmatrix} 8 & 16 \\ -4 & -8 \end{bmatrix} \times 4 \begin{bmatrix} -\frac{6}{4} & -(\frac{6}{4})^2 \\ 1 & \frac{6}{4} \end{bmatrix} =$

$\begin{bmatrix} 2 & 4 \\ -1 & -2 \end{bmatrix} \begin{bmatrix} -6 & -9 \\ 4 & 6 \end{bmatrix}$.

As for the second, the equation $ax = -12$ has several solutions (a, x): $(\pm 1, \mp 12)$, $(\pm 2, \mp 6)$, $(\pm 3, \mp 4)$ and symmetric. Only $(a, x) = (\pm 2, \mp 6)$ verify the required divisibilities. We get the previous 2N decomposition and the "minus" one.

4. 2N decompositions over $\mathbb{Z}[\sqrt{-5}]$

We start by discussing the commutative domain $\mathbb{Z}[\sqrt{-5}]$. It is well-known that **this is not UFD** (unique factorization domain) because of

$$3 \cdot 2 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

which are two decompositions not associated in divisibility.

Moreover **this is not GCD** (greatest common divisors exist), the customarily example being the pair $(6, 2(1 + i\sqrt{5}))$ which is proved **not** having a gcd (using the so-called "norm" of elements in $\mathbb{Z}[\sqrt{-5}]$: $N(a + bi\sqrt{5}) = a^2 + 5b^2$).

We also mention that **the "well-known" property**

$$a \mid bc, \gcd(a, b) = 1 \Longrightarrow a \mid c$$

fails.

Indeed, as above, 3 (or 2) divides $(1 + i\sqrt{5})(1 - i\sqrt{5})$, $\gcd(3, 1 \pm i\sqrt{5}) = 1$ but $3 \nmid 1 \pm i\sqrt{5}$.

However, if a domain is GCD then the above property holds.

In fact, $\gcd(a,b)=1$ implies $\gcd(ac,bc)=c\gcd(a,b)=c$. As a is a common divisor of ac and bc, a divides $\gcd(ac,bc)$. That is, a divides c.

Note that here we use the following GCD properties:
(i) $d_1 \mid a,b$ implies $d_1 \mid \gcd(a,b)$ (the definition of the gcd), and
(ii) $r\gcd(a,b)=\gcd(ra,rb)$ if both gcd′s exist.

Remarks. 1) The astute reader will notice which is the obstruction:

$$\gcd(a,b)=1 \text{ implies } \gcd(ac,bc)=c.$$

A counterexample appears already above: $\gcd(3,1\pm i\sqrt{5})=1$ but $\gcd(2\cdot 3, 2(1\pm i\sqrt{5}))$ (not only is not 2 but) **does not exist**.

2) It can be proved (e.g., see [7]) that if D is an integral domain and $a,b\in D$ then the following are equivalent:
(i) a,b have an lcm,
(ii) for any $r\in D$, ra,rb have a gcd.
Therefore, an integral domain has gcd′s iff it has lcm′s. In any GCD domain all these exist and for every a,b,r, $\gcd(ra,rb)=r\gcd(a,b)$.

3) Over integral domains, by cancellation, it is easy to prove the converse: $\gcd(ac,bc)=c$ implies $\gcd(a,b)=1$.

4) There are also well-known examples of GCD domains (even Bézout domains - that is, for every a, b, $\gcd(a,b)$ is a linear combinations of a and b) which are not UFD. The ring of entire functions (functions holomorphic on the whole complex plane) and the ring of all algebraic integers (see [2]).

In the sequel, over $\mathbb{Z}[\sqrt{-5}]$, we are searching for a nontrivial idempotent 2×2 matrix which has a 2N decomposition but the entries on the first row and on the first column have no gcd.

Using the first mentioned above not unique factorization, it follows that

$$E=\begin{bmatrix} 3 & 1+i\sqrt{5} \\ -1+i\sqrt{5} & -2 \end{bmatrix}$$

is a (nontrivial) idempotent (trace = 1, det =0).

However, computer found quickly a 2N decomposition:

$$E=\begin{bmatrix} -1-i\sqrt{5} & 2-i\sqrt{5} \\ 2 & 1+i\sqrt{5} \end{bmatrix}\begin{bmatrix} 1-i\sqrt{5} & 2 \\ 2+i\sqrt{5} & -1+i\sqrt{5} \end{bmatrix}$$

(or the "minus" one). However, at least using entries of form $a+bi\sqrt{5}$ with integers $-4\le a,b\le 4$, no other 2N decomposition was found by computer.

Question. Up to "minus", is this a unique 2N decomposition for E ?

The idempotent above is of form $\begin{bmatrix} n+1 & x+yi\sqrt{5} \\ -x+yi\sqrt{5} & -n \end{bmatrix}$ with $x^2+5y^2=n(n+1)$ and positive integer n. Up to $n=19$ (and up to signs) there are only three more such idempotents: $\begin{bmatrix} 5 & -2i\sqrt{5} \\ -2i\sqrt{5} & -4 \end{bmatrix}$, $\begin{bmatrix} 6 & 5+i\sqrt{5} \\ -5+i\sqrt{5} & -5 \end{bmatrix}$, $\begin{bmatrix} 8 & 6+2i\sqrt{5} \\ -6+2i\sqrt{5} & -7 \end{bmatrix}$ (note that $c=-\overline{b}$ and a is a positive integer). The first two have 2N decompositions.

$$\begin{bmatrix} 5 & -2i\sqrt{5} \\ -2i\sqrt{5} & -4 \end{bmatrix} = \begin{bmatrix} 2i\sqrt{5} & 5 \\ 4 & -2i\sqrt{5} \end{bmatrix} \begin{bmatrix} 2i\sqrt{5} & 4 \\ 5 & -2i\sqrt{5} \end{bmatrix},$$
$$\begin{bmatrix} 6 & 5+i\sqrt{5} \\ -5+i\sqrt{5} & -5 \end{bmatrix} =$$
$$= \begin{bmatrix} -(5+i\sqrt{5}) & -2(2+i\sqrt{5}) \\ 5 & 5+i\sqrt{5} \end{bmatrix} \begin{bmatrix} 5-i\sqrt{5} & 5 \\ -2(2-i\sqrt{5}) & -5+i\sqrt{5} \end{bmatrix}.$$

These two decompositions (and also the initial above with $a = 3$) are of the following form ($a(1-a) = bc$ and $c \mid ab$)

$$\begin{bmatrix} a & b \\ c & 1-a \end{bmatrix} = \begin{bmatrix} -b & \varepsilon \\ a-1 & b \end{bmatrix} \begin{bmatrix} -c & a-1 \\ \overline{\varepsilon} & c \end{bmatrix}$$

with ε being a complex number such that $a = |\varepsilon|$, $b^2 = \varepsilon(1-a)$, $c^2 = \overline{\varepsilon}(1-a)$ and $\varepsilon c = ab$.

However, for the third, that is,

$$F = \begin{bmatrix} 8 & 6+2i\sqrt{5} \\ -6+2i\sqrt{5} & -7 \end{bmatrix},$$

$\varepsilon = \dfrac{ab}{c} = -\dfrac{8}{7}(2+3i\sqrt{5})$, that is $\varepsilon \notin \mathbb{Z}[i\sqrt{5}]$ as $c \nmid ab$.

This is the first example such that $\gcd(a,c) = \gcd(8, -6+2i\sqrt{5})$ does not exist (nor $\gcd(a,b) = \gcd(8, 6+2i\sqrt{5})$) (see Appendix for the details). The computer assistance was essential in order to prove the following

Proposition 4.1. *F has a 2N decomposition.*

Proof. Denoting $F = \begin{bmatrix} x & y \\ z & -x \end{bmatrix} \begin{bmatrix} a & b \\ c & -a \end{bmatrix}$ with $x^2 + yz = 0 = a^2 + bc$, our problem is easy to state in terms of equations. Equivalently

$$\begin{array}{rrcc} (1) & ax + cy & = & 8 \\ (2) & bx - ay & = & 6+2i\sqrt{5} \\ (3) & -cx + az & = & -6+2i\sqrt{5} \\ (4) & ax + bz & = & -7 \\ & x^2 + yz & = & 0 \\ & a^2 + bc & = & 0 \end{array}.$$

Multiplying the equations (1) and (2), first by a resp. c and adding, then by b resp. $-a$ and adding, we can find $8a + (6+2i\sqrt{5})c = 0$ and $-(6+2i\sqrt{5})a + 8b = 0$. Similarly, using (3) and (4), we get $(-6+2i\sqrt{5})a - 7c = 0$ and $7a + (-6+2i\sqrt{5})b = 0$. Together with $a^2 + bc = 0$ this was an easy task for computer, which, for the integer entries bounded by 21 found 6 (nonzero) solutions (actually 12 with the "minus" ones). Here are some of these: $(a,b,c) \in \{(6+2i\sqrt{5}, 2+3i\sqrt{5}, -8), (4-8i\sqrt{5}, 13-5i\sqrt{5}, 8), (10-6i\sqrt{5}, 15-2i\sqrt{5}, 8i\sqrt{5})$.

The second part was equally easy for computer: for each solution (a,b,c), to solve for x, y, z the system (1) to (4) adding $x^2 + yz = 0$. This way, for $(a,b,c) = (-6-2i\sqrt{5}, -2-3i\sqrt{5}, 8)$, computer found the (nonzero) solution $(x,y,z) = (6-2i\sqrt{5}, 8, -2+3i\sqrt{5})$. This finally gave the 2N desired decomposition

$$F = \begin{bmatrix} 6-2i\sqrt{5} & 8 \\ -2+3i\sqrt{5} & -6+2i\sqrt{5} \end{bmatrix} \begin{bmatrix} -6-2i\sqrt{5} & -2-3i\sqrt{5} \\ 8 & 6+2i\sqrt{5} \end{bmatrix}.$$

□

To find a 2N decomposition, one has just to solve this system in the unknowns x, y, z, a, b, c over $\mathbb{Z}[\sqrt{-5}]$. Equivalently, writing every element in $\mathbb{Z}[\sqrt{-5}]$ as $\alpha + \beta i\sqrt{5}$, this is a 12 integer variables quadratic system. As such, we tried to use the computer to solve it, but the computer needs some limitations for the coefficients of the entries of the nilpotent 2×2 matrices. Since the time necessary to cover the possible decompositions only up to $-5 \leq u, y \leq 5$ (for entries of form $u + vi\sqrt{5}$) was one day (and far longer for larger limitations), we had to find a different approach. Actually, as seen in the above proof, we (successfully) divided the computer task into two parts.

Corollary 4.2. *The GCD condition for a commutative domain D is sufficient for idempotent matrices of $\mathbb{M}_2(D)$ to have 2N decompositions, but is not necessary.*

Remark. When the entries (of form $u + vi\sqrt{5}$) are bounded (in absolute value) by small positive integers, as an example, $-1 \leq u, v \leq 1$, the computer produces *temporary* candidates for not having 2N decompositions. Such a candidate was $E = \begin{bmatrix} -i\sqrt{5} & -1 - i\sqrt{5} \\ i\sqrt{5} & 1 + i\sqrt{5} \end{bmatrix}$. However, according to Theorem 3.1, ($\gcd(a, c)$ exists),

$$\begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} 5 - i\sqrt{5} & 4 - 2i\sqrt{5} \\ -5 & -5 + i\sqrt{5} \end{bmatrix}$$

is the corresponding 2N decomposition, which is found for $-5 \leq u, v \leq 5$.

5. 2N decompositions over commutative domains

In an attempt to find a nontrivial idempotent 2×2 matrix over $\mathbb{Z}[\sqrt{-5}]$ with no 2N decomposition, we reconsidered the system used in the previous section, and important simplifications occurred.

Let R be a commutative domain. For 3 given elements $\alpha, \beta, \gamma \in R$ with $\alpha(1-\alpha) = \beta\gamma$, we start with the nontrivial idempotent $E = \begin{bmatrix} \alpha & \beta \\ \gamma & 1 - \alpha \end{bmatrix}$. As already seen, a 2N decomposition exists if the system with unknowns a, b, c, x, y, z

$$\begin{array}{rrcl} (1) & ax + cy & = & \alpha \\ (2) & bx - ay & = & \beta \\ (3) & -cx + az & = & \gamma \\ (4) & ax + bz & = & 1 - \alpha \\ & x^2 + yz & = & 0 \\ & a^2 + bc & = & 0 \end{array} , \qquad \text{(S)}$$

has a solution in $\mathbb{Z}[\sqrt{-5}]$. We use the 2 steps procedure from previous section: first eliminate the unknowns x, y, z and then, for every solution a, b, c we solve the system above. We can suppose $\alpha \neq 0, 1$ and $\beta, \gamma \neq 0$, since otherwise 2N decompositions were already previously mentioned.

Step 1. Multiplying the equations (1) and (2), first by a resp. c and adding, then by b resp. $-a$ and adding, we can find $\alpha a + \beta c = 0$ and $-\beta a + \alpha b = 0$. Similarly, using (3) and (4), we get $\gamma a + (1-\alpha)c = 0$ and $-(1-\alpha)a + \gamma b = 0$. Since $\alpha(1-\alpha) = \beta\gamma$, both homogenous systems $\begin{cases} \alpha a + \beta c & = 0 \\ \gamma a + (1-\alpha)c & = 0 \end{cases}$ and $\begin{cases} -\beta a + \alpha b & = 0 \\ -(1-\alpha)a + \gamma b & = 0 \end{cases}$ have zero determinant. Therefore, the corresponding equations are dependent and

it suffices to retain two of these, say, $\begin{cases} \alpha a &= -\beta c \\ \beta a &= \alpha b \end{cases}$. Moreover, notice that multiplying side by side these equations, we get $\alpha\beta(a^2+bc)=0$, so $a^2+bc=0$ as α, β were supposed nonzero (and the base ring is a domain).

Step 2. For each solution (a,b,c), we solve for x,y,z the system (1) to (4) adding $x^2+yz=0$.

However, an analogous elimination may be performed also in this case.

Multiplying the equations (1) and (3), first by x resp. y and adding, then by z resp. $-x$ and adding, we can find $\alpha x+\gamma y=0$ and $-\gamma x+\alpha z=0$. Similarly, using (2) and (4), we get $\beta x+(1-\alpha)y=0$ and $-(1-\alpha)x+\beta z=0$. Again we associate two by two homogeneous equations, these turn out to be dependent and we can retain only $\alpha x+\gamma y=0$ and$-(1-\alpha)x+\beta z=0$. Writing $\alpha x=-\gamma y$, $(1-\alpha)x=\beta z$ and multiplying side by side we also cover $x^2+yz=0$ (as $\alpha(1-\alpha)=\beta\gamma$). This way we have obtained the following result

Theorem 5.1. *Let* $E=\begin{bmatrix} \alpha & \beta \\ \gamma & 1-\alpha \end{bmatrix}$ *be a nontrivial idempotent matrix (i.e.,* $\alpha(1-\alpha)=\beta\gamma$*) over a commutative domain* R*. Then* E *has* ***no*** *2N decomposition if any of the following conditions holds:*

(i) the system $\begin{cases} \alpha a &= -\beta c \\ \beta a &= \alpha b \end{cases}$ *has no nonzero solutions over* R*;*

(ii) the system $\begin{cases} \alpha x &= -\gamma y \\ (1-\alpha)x &= \beta z \end{cases}$ *has no nonzero solutions over* R*;*

(iii) the system $\begin{cases} \alpha a &= -\beta c \\ \beta a &= \alpha b \end{cases}$ *has nonzero solutions over* R *but for every such solution* (a,b,c)*, the system (S) is not solvable in* (x,y,z) *over* R*;*

(iv) the system $\begin{cases} \alpha x &= -\gamma y \\ (1-\alpha)x &= \beta z \end{cases}$ *has nonzero solutions over* R *but for every such solution* (x,y,z)*, the system (S) is not solvable in* (a,b,c) *over* R*.*

According to Proposition 2.1 and Theorem 2.3, in order to find a nontrivial idempotent 2×2 matrix over $\mathbb{Z}[\sqrt{-5}]$, we have to assume that $\gcd(\alpha,\beta)$ and $\gcd(\alpha,\gamma)$ do **not** exist.

Remarks. 1) A sufficient condition for (i) to have a solution is $\alpha \mid \beta^2$. Indeed, if so, $(a,b,c)=(-\beta,-\dfrac{\beta^2}{\alpha},\alpha)$ is a solution for (i). The condition is fulfilled for the matrix F, the example provided in the previous section.

2) A sufficient condition for (ii) to have a solution is $\beta \mid (1-\alpha)\gamma$. Indeed, if so, $(x,y,z)=(\gamma,-\alpha,\dfrac{(1-\alpha)\gamma}{\beta})$ is a solution for (ii). Also fulfilled for F.

3) Actually (iii) (the positive version) was the combination which provided the (complete) solution for the matrix F, the example provided in the previous section.

From here, *the computer was put into service*.

The code should browse triples (α,β,γ) from $\mathbb{Z}[\sqrt{-5}]$, with not existing $\gcd(\alpha,\beta)$ and $\gcd(\alpha,\gamma)$, nonzero α, β, γ, $\alpha\neq 1$ and $\alpha(1-\alpha)=\beta\gamma$, and search solutions for the systems (i), (iii) with unknowns (a,b,c) or for systems (ii), (iv) with unknowns (x,y,z).

(i) The code should browse pairs (α, β) from $\mathbb{Z}[\sqrt{-5}]$, with not existing $\gcd(\alpha, \beta)$, β divides $\alpha(1-\alpha)$, nonzero α, β, $\alpha \neq 1$ and search solutions for the system (i) with unknowns (a, b, c).

(ii) The code should browse triples (α, β, γ) from $\mathbb{Z}[\sqrt{-5}]$, with $\gcd(\alpha, \beta)$ and $\gcd(\alpha, \gamma)$ do not exist, $\alpha(1-\alpha) = \beta\gamma$, nonzero α, β, γ, $\alpha \neq 1$ and search solutions for the system (ii) with unknowns (x, y, z).

As already mentioned, the problem in this approach is that computer may provide "temporary" candidates, corresponding to entries that are bounded (in absolute value) by small positive integers. Moreover, as reader can see in the Appendix, it is hard to check (by computer) the nonexistence of some gcd's in $\mathbb{Z}[\sqrt{-5}]$.

That's why we tried to check the conditions of the Theorem 5.1, without the nonexistence conditions (but for (i) we added $\beta \nmid \alpha$).

For instance in the (i) case, with (nonzero) a, b, c bounded by 50, after some 24 hours, for all α, β, γ bounded by $z = 9$, the computer found solutions. For the temporary candidates, a separate verification found mostly $\gcd = 1$. Hence by Proposition 2.1 and Theorem 2.3, these have 2N decompositions.

Here are some ($\beta \mid \alpha(1-\alpha)$ and $\beta \nmid \alpha$ included)

Temporary candidates.

1) $z = 4$: $\alpha = 1 + 4i\sqrt{5}$, $\beta = i\sqrt{5}$. As $N(\alpha) = 81$, $N(\beta) = 5$ it follows that $\exists \gcd(\alpha, \beta) = 1$.

2) $z = 5$: $\alpha = 2 + 5i\sqrt{5}$, $\beta = 2 + i\sqrt{5}$. As $N(\alpha) = 129$, $N(\beta) = 9$ it follows that if $d \mid \alpha, \beta$ then $N(d) \in \{1, 3\}$. Since the equation $x^2 + 5y^2 = 3$ has no integer solutions, again $\exists \gcd(\alpha, \beta) = 1$.

3) $z = 6$: $\alpha = 2 + 6i\sqrt{5}$, $\beta = 1 + 6i\sqrt{5}$. As $N(\alpha) = 184$, $N(\beta) = 181$ and 181 is a prime number it follows that $\exists \gcd(\alpha, \beta) = 1$.

4) $z = 7$: $\alpha = -3 + 5i\sqrt{5}$, $\beta = 7 + 3i\sqrt{5}$. As $N(\alpha) = 134 = 2 \times 67$, $N(\beta) = 94 = 2 \times 47$ it follows that if $d \mid \alpha, \beta$ then $N(d) \in \{1, 2\}$. Since the equation $x^2 + 5y^2 = 2$ has no integer solutions, again $\exists \gcd(\alpha, \beta) = 1$.

Hence, in all these cases, there exists a 2N decomposition.

As a result, the following question still has no answer.

Question. Are there nontrivial idempotent 2×2 matrices over $\mathbb{Z}[\sqrt{-5}]$ which do **not** have a 2N decomposition ?

6. Over ID rings

In another direction, we can generalize these results as follows: using Steger's terminology (see [4]), a ring R was called an *ID* ring if every idempotent matrix over R is similar to a diagonal matrix. Examples of ID rings include: division rings, local rings, projective-free rings, principal ideal domains, elementary divisor rings, unit-regular rings and serial rings.

Over any ring, for some special diagonal idempotent 2×2 matrices, we have the following 2N decompositions:

$$\begin{bmatrix} e & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & e \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ e & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 \\ 0 & e \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ e & 0 \end{bmatrix} \begin{bmatrix} 0 & e \\ 0 & 0 \end{bmatrix}.$$

Moreover, for idempotents e, e' in a ring R, the diagonal idempotent $\begin{bmatrix} e & 0 \\ 0 & e' \end{bmatrix} \in \mathbb{M}_2(R)$ has the 2N decomposition $\begin{bmatrix} 0 & e \\ e' & 0 \end{bmatrix} \begin{bmatrix} 0 & e' \\ e & 0 \end{bmatrix}$ iff e and e' are orthogonal.

Recall that a ring is *connected* if it has only the trivial idempotents 0, 1. Note that over any commutative ring R which is **not** connected, $eI_n \in \mathbb{M}_n(R)$, with $e^2 = e \neq 0$ and any positive integer n, is an idempotent matrix which has **no** 2N decomposition: $\det(eI_n) = e \neq 0$ and $\det(N_1N_2) = 0$ for any nilpotent $n \times n$ matrices N_1, N_2. As for *a converse of Theorem* 2.3, namely, for what rings R every nontrivial idempotent in $\mathbb{M}_n(R)$ has a 2N decomposition, this shows that R must be connected.

For ID rings we can prove the following

Proposition 6.1. *Let R be an ID ring. Every nontrivial idempotent $n \times n$ matrix over R has property 2N iff R is connected.*

Proof. If R is ID and connected, by similarity, it suffices to find 2N decompositions for the (nontrivial) diagonal idempotents, having only 0 or 1 on the diagonal. But this is easy to realize as for matrix units $E_{ii} = E_{1i}E_{i1}$. This way, any such diagonal matrix is decomposed into a (product of a) strictly upper triangular matrix and a strictly lower triangular matrix. Conversely, if R is not connected we use the paragraph before the proposition. □

In particular, this holds for local rings.

More generally, we state as open the following

Question. Describe the connected (commutative) rings R such that every nontrivial idempotent in $\mathbb{M}_2(R)$ (or $\mathbb{M}_n(R)$ for some positive integer n) has a 2N decomposition (already partly discussed above).

Even more generally, we can state as open the following

Question. Describe the rings whose all nontrivial idempotents are products of two nilpotents.

7. Appendix

Since the nonexistence of some gcd's is not obvious, for reader's convenience we provide here some necessary details.

First, a simple

Lemma 7.1. *Let $a, b, r \in D$, a commutative domain. Then $r\gcd(a, b) = \gcd(ra, rb)$ for every r, if both $\gcd$'s exist.*

Proof. Let $d = \gcd(a, b)$ and $d_1 = \gcd(ra, rb)$. Then rd divides both ra and rb. So it divides d_1. Write $d_1 = rds$, $a = da_1$, $b = db_1$, and write $ra = d_1x$, $rb = d_1y$. Then $d_1a_1 = rdsa_1 = ras = d_1xs$ and $d_1b_1 = rdsb_1 = rbs = d_1ys$. So $a_1 = xs$, $b_1 = ys$. Since $\gcd(a_1, b_1) = 1$, $s = 1$. So $d_1 = rd$. □

Secondly

Lemma 7.2. $\gcd(4, 3 + i\sqrt{5}) = 1$.

Proof. As customarily, we use the "norm" N of complex numbers in $\mathbb{Z}[i\sqrt{5}]$. As $N(4) = 16$ and $N(3+i\sqrt{5}) = 14$ if d is a common divisor, $N(d) \mid 2$ so $N(d) \in \{1, 2\}$. Since $x^2 + 5y^2 = 2$ has no solutions, $d = 1$ is the only common divisor. □

Finally

Claim 7.3. $\gcd(8, 6+2i\sqrt{5})$ *does not exist.*

Proof. Since $\gcd(4, 3+i\sqrt{5}) = 1$, cancellation by 2 in $8 \cdot (-7) = (6+2i\sqrt{5})(-6+2i\sqrt{5})$ gives $4 \cdot (-7) = (3+i\sqrt{5})(-6+2i\sqrt{5})$.

If the gcd above exists, it should follow that 4 divides $-6+2i\sqrt{5}$. Since $N(4) = 16$, $N(-6+2i\sqrt{5}) = 56$ we derive $16 \mid 56$, a contradiction. □

Acknowledgement 7.4. Thank are due to the referees for careful reading and many suggestions which improved our presentation.

References

[1] G. Călugăreanu *Singular matrices that are products of two idempotents or products of two nilpotents*. Spec. Matrices **10** (2022),47-55.
[2] P. M. Cohn *Bézout rings and their subrings*. Proc. Cambridge Philos. Soc., **64** (1968), 251-264.
[3] T. T. J. Laffey *Factorizations of Integer Matrices as Products of Idempotents and Nilpotents*. Linear Algebra and its Applications **120** (1989), 81-93.
[4] A. Steger *Diagonability of idempotent matrices*. Pacific J. Math. **19** (3) (1966) 535-542.
[5] A. R. Sourour *Nilpotent factorization of matrices*. Linear and Multilinear Algebra **31** (1-4) (1992), 303-308.
[6] P. Sullivan *Products of nilpotent matrices*. Linear Multilinear Algebra **56** (3) (2008), 311-317.
[7] C. Woo https://planetmath.org/anintegraldomainislcmiffitisgcd (2013).
[8] P.Y. Wu *Products of nilpotent matrices*. Linear Algebra and its Applications **96** (1987), 227-232.

Babeş-Bolyai University, Cluj-Napoca, Romania
Email address: calu@math.ubbcluj.ro,horia.pop@ubbcluj.ro