Units generated by idempotents

Grigore Călugăreanu

October 18, 2025

1 Introduction

In this note we consider only nonzero unital rings and for a ring R, $Id(R)$ denotes the set of all the idempotents of R.

It is easy to check that if e is an idempotent in a unital ring R then $2e-1$ is an order two unit, i.e., $u^2=1$, or equivalently, $u^{-1}=u$.

Observe that, to simplify the wording, the previous definition does not assume $u\neq 1$, so the identity is also an order two unit.

We can call an order two unit $u\in U(R)$ an *id-unit* if there exists an idempotent e such that $u=2e-1$. We denote by $IU(R)$ the set of all id-units of a ring R.

In any unital ring R, $\{\pm 1\}$ are id-units, corresponding to the trivial idempotents $e\in\{1,0\}$. We shall call these, *trivial* id-units.

Obviously, if a ring has only the trivial idempotents, it also has only the trivial id-units. Examples include the domains, or the local rings and in particular the division rings.

Therefore, **a natural problem** consists in *characterizing the nontrivial id-units in some given rings.*

Clearly this can be done in any ring for which all idempotents are known, i.e. with the above notations, $IU(R)=2Id(R)-1$.

After some elementary remarks in section 2, in section 3 we characterize the id-units in $\mathbb{Z}_n$, integers modulo n, for some positive integer n, and, in section 4, the id-units in 2×2 matrix rings over commutative domains.

2 Elementary

Lemma 1 *If $2\in U(R)$ then every order two unit is an id-unit.*

Proof. If $2\in U(R)$, the definition is equivalent to $e=2^{-1}(1+u)$. Indeed, the RSH is an idempotent (i.e. $(2^{-1}(1+u))^2=2^{-1}(1+u)$) if $u^2=1$). ■

Obviously, the trivial id-units belong here.

Example. Take $U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ for which $U^2 = I_2$. Over $\mathbb{Z}$, this is not an id-unit: there is no integral matrix E such that $2E = I_2 + U = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$.

However, it is a nontrivial id-unit over $\mathbb{Z}_3$: indeed, $E = \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$ is an idempotent and $2E - I_2 = U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. This follows also from the previous lemma, as $2I_2$ is a unit in $\mathbb{M}_2(\mathbb{Z}_3)$.

As examples (and the study) below show, there are (nontrivial) id-units also when 2 is not cancellable.

It is easy to show that the *uniqueness* of the idempotent, for a given id-unit, generally fails.

Example: in $\mathbb{M}(\mathbb{Z}_2)$ (where $2I_2 = 0_2$ is not cancellable), we have 6 nontrivial idempotents:

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$. For all 6, the corresponding id-unit is I_2.

Of course $2e-1 = 2e'-1$ iff $2e = 2e'$, so we have uniqueness if 2 is cancelable (such a ring is called 2-*torsionfree*). In particular, $2 \in U(R)$. That is

Lemma 2 *If a ring R is 2-torsionfree, the function $f : Id(R) \longrightarrow IU(R)$, $f(x) = 2x - 1$, $x \in Id(R)$ is bijective and so $|Id(R)| = |IU(R)|$.*

For an arbitrary ring R, the function f is surjective (by construction) and so $|IU(R)| \leq |Id(R)|$.

The converse fails, that is, there are id-units *generated by only one* idempotent (that is, f is injective) also in rings which are not 2-torsionfree.

Example. Clearly $\overline{2} \notin U(\mathbb{Z}_{12})$ and is not cancellable. Then $Id(\mathbb{Z}_{12}) = \{\overline{0}, \overline{1}, \overline{4}, \overline{9}\}$ and $U(\mathbb{Z}_{12}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$, all are order two units. In this case, $\overline{1}$ and $\overline{11} = -\overline{1}$ are the trivial id-units, and we have *nontrivial id-units*: $\overline{7} = 2 \cdot \overline{4} - \overline{1}$ which is generated *only* by the idempotent $\overline{4}$. So is $\overline{5} = 2 \cdot \overline{9} - \overline{1}$.

In what follows, we omit the superscript for classes modulo n, for any n.

Remarks. 1) If $f(e) = u$ then $f(1-e) = 2(1-e) - 1 = 1 - 2e = -u$, that is, $f(1-e) = -f(e)$.

2) In what follows, we assume the *rings have not characteristics 2*. Otherwise, the only order two id-unit is -1.

3 Id-units in $\mathbb{Z}_n$

We first recall some well-known characterizations.

It is well-known that u is a unit in $\mathbb{Z}_n$ iff $\gcd(u,n) = 1$. Suppose $n = p_1^{\alpha_1}...p_k^{\alpha_k}$.The number of units of $\mathbb{Z}_n$ is given by Euler's totient function $\phi(n) = (p_1-1)p_1^{\alpha_1-1}...(p_k-1)p_k^{\alpha_k-1} = |U(\mathbb{Z}_n)|$.

The number of idempotents of $\mathbb{Z}_n$ is $2^k = |Id(\mathbb{Z}_n)|$ (including the two trivial idempotents).

Also notice that u is a unit in $\mathbb{Z}_n$ iff $n-u$ is a unit in $\mathbb{Z}_n$ (indeed, $uv \equiv 1(\text{mod } n) \Longleftrightarrow (n-u)(n-v) \equiv 1(\text{mod } n)$).

Remarks. 1) For any unit u in $\mathbb{Z}_n$, we can always consider $\dfrac{1+u}{2}$.

Indeed, $2 \notin U(\mathbb{Z}_n)$ iff n is even, case in which the units are odd, so $\dfrac{1+u}{2}$ exists. If $2 \in U(\mathbb{Z}_n)$ then clearly $\dfrac{1+u}{2} = 2^{-1}(1+u)$.

2) $\dfrac{1+u}{2}$ is 'of interest' because it is a possible idempotent solution of $u = 2e-1$, in the definition of id-units.

Now we are ready to prove the following

Proposition 3 *Assume* $\gcd(u,n) = 1$. *Then* u *is an id-unit in* $\mathbb{Z}_n$ *iff* $u^2 \equiv 1(\text{mod } n)$.

Proof. Indeed, by the previous remarks, u is an id-unit iff $\left(\dfrac{1+u}{2}\right)^2 \equiv \dfrac{1+u}{2}(\text{mod } n)$. Equivalently, $(1+u)^2 \equiv 2+2u$ and also $u^2 \equiv 1(\text{mod } n)$. ■

Examples. 1) For $n = 12$, $\phi(12) = 4$ and $U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$. Then 1 and $11 = -1$ are the trivial id-units, and since $7 = 12 - 5$ it suffices to check 5. Indeed, $5^2 = 25 \equiv 1(\text{mod } 12)$ so 5 is an id-unit. Hence, so is 7.

2) For $n = 60$, $\phi(60) = 16$ and $2^3 = 8$, that is, at most 8 units are id-units and the other 8 units are not id-units.

We indeed have 8 id-units: the trivial id-units $\{1, 59\}$ and $\{11 = 2\cdot 36 - 1, 19 = 2\cdot 40 - 1, 29 = 2\cdot 45 - 1, 31 = 2\cdot 16 - 1, 41 = 2\cdot 21 - 1, 49 = 2\cdot 25 - 1\}$. The other units, namely $\{7, 13, 17, 23, 37, 43, 47, 53\}$ are not id-units.

In this special case, since the last digit of $n = 60$ is 0, for $u^2 \equiv 1$ we need the last digit of u to be 1 or 9. This way we can immediately isolate the id-units.

4 Id-units in 2×2 matrix rings

We proceed with matrix 2×2 rings.

As already mentioned, in order to determine the nontrivial id-units, we assume $2 \notin U(R)$.

Lemma 4 *For an arbitrary unital ring* R, $2I_2$ *is a unit in* $\mathbb{M}_2(R)$ *iff* $2 \in U(R)$.

Proof. If $2I_2$ is a unit, there exists a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, such that $2I_2 \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = 2\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot 2I_2 = I_2$ implies $2a = a \cdot 2 = 1$ so $2 \in U(R)$.

Conversely, if $2 \in U(R)$, $2^{-1}I_2$ is the inverse of $2I_2$. ■

Therefore $2I_2$ is *not* a unit in $\mathbb{M}_2(\mathbb{Z})$ and $2I_2$ is a unit in $\mathbb{M}_2(\mathbb{Z}_n)$ iff n is odd. Combining with Lemma 1 gives

Proposition 5 *If 2 is a unit in a ring R then the id-units U of $\mathbb{M}_2(R)$ are the matrices with $U^2 = I_2$.*

For commutative rings we can prove the following

Proposition 6 *For a commutative domain R, a unit $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $\det U = ad - bc = -1$ is a nontrivial id-unit in the matrix ring $\mathbb{M}_2(R)$ iff $d = -a$, $a \in 2R + 1$ and $b, c \in 2R$.*

Proof. Since Cayley-Hamilton theorem is valid for matrices over commutative rings, for any idempotent 2×2 matrix E, we get $(Tr(E) - 1)E = \det(E)I_2$.The nontrivial 2×2 idempotents are characterized by trace $= 1$ and determinant $= 0$, i.e. are of form $E = \begin{bmatrix} x+1 & y \\ z & -x \end{bmatrix}$ with $x(x+1) + yz = 0$. The conditions follow from the equality $2E = U + I_2$, i.e. $2\begin{bmatrix} x+1 & y \\ z & -x \end{bmatrix} = \begin{bmatrix} a+1 & b \\ c & d+1 \end{bmatrix}$.

The condition $\det U = ad - bc = -1$, follows from $\det(2E - I_2) = -(2x + 1)^2 - 4yz = -1$ since $x(x+1) + yz = 0$. ■

Corollary 7 *A 2×2 matrix over a commutative domain R is a nontrivial id-unit iff it is of form $\begin{bmatrix} a & b \\ \frac{1-a^2}{b} & -a \end{bmatrix}$ for $a \in 2R + 1$ and b a divisor of $1 - a^2$.*

We just revisit the example in the introduction, $U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ over $\mathbb{Z}_3$.

Since $2 \in U(\mathbb{Z}_3)$, we must have $U^2 = I_2$, so Lemma 1 is verified. As for the previous corollary, notice that $a = 0 = 2 \cdot 1 + 1 \in 2\mathbb{Z}_3 + 1$ and $b = 1$ divides $1 = 1 - 0^2$.

Corollary 8 *The nontrivial id-units in $\mathcal{M}_2(\mathbb{Z})$ are the matrices $U = \begin{bmatrix} a & b \\ c & -a \end{bmatrix}$ with odd a, even b, c and $a^2 + bc = 1$ (i.e. $\det U = -1$ and $\{\begin{bmatrix} a & b \\ \frac{1-a^2}{b} & -a \end{bmatrix} : a \in 2\mathbb{Z} + 1, b \in 2\mathbb{Z}, b | a^2 - 1\}$).*

Examples. $\begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} = 2\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} - I_2$, $\begin{bmatrix} 3 & 2 \\ -4 & -3 \end{bmatrix} = 2\begin{bmatrix} 2 & 1 \\ -2 & -1 \end{bmatrix} - I_2$ and so on.

Remark. Over commutative rings which are not domains, we still have $(Tr(E) - 1)E = \det(E)I_2$, but $Tr(E) = 1$, and then $\det(E) = 0$, are not necessary conditions.

For an example, take $E = 4I_2$ over $\mathbb{Z}_6$. Then $E^2 = E$ is a nontrivial idempotent with $Tr(E) = 2$ and $\det(E) = 4$ (an idempotent in $\mathbb{Z}_6$).

Consequently, the characterization of 2×2 id-units over commutative rings requires more detailed analysis.