EXCEPTIONAL AND COMPLEMENTABLE UNITS IN RINGS

GRIGORE CĂLUGĂREANU

Abstract. A unit u in a ring R is called exceptional if $1-u$ is also a unit. Such units have been previously studied from a Number Theory perspective. In this paper, we investigate exceptional units from the standpoint of Ring Theory, with particular emphasis on matrix rings, where several characterizations are provided. We define and explore a special subclass of exceptional units, termed complementable units. An exceptional unit u is called complementable if $u(1-u)=1$. We determine the residue class rings that contain complementable units and identify such units in certain matrix rings.

1. Introduction

There are three particularly important subsets of a ring R: $Idem(R)$, the set of idempotents, $N(R)$, the set of nilpotents, and $U(R)$, the set of units in the ring R.

Given an element a from any of these sets, one may ask whether $1-a$ also belongs to the same set. For idempotents, the answer is affirmative: $1-a$ is the *complementary* idempotent. For nilpotents, the answer is negative, as $1-a$ is always a unit. For units, this question gives rise to the following definition.

A unit $u \in U(R)$ is called *exceptional* (or *exunit*, for short) if $1-u \in U(R)$. We denote the set of all exceptional units in R by $U_e(R)$. Equivalently, $u \in U_e(R)$ if there exists a unit $v \in U(R)$ such that $u+v=1$.

Similar questions have been addressed in Ring Theory for other classes of elements. For instance, the property that $1-a$ shares the same structure as a holds for nil-clean, clean, or exchange elements, but fails in general for (unit-)regular or weakly clean elements (see [12]).

The study of unit pairs u, v such that $u+v=1$ (or equivalently $1+u+v=0$) is not new. This equation was considered by Nagell in a series of papers ([6] 1959, [7] 1960, [8] 1964, [9] 1968, [10] 1969), where he investigated its solvability over algebraic extensions of the rationals. For example, solvability was established in quadratic extensions, in cubic extensions with negative discriminant, and in certain quartic extensions. Moreover, Nagell (1964), and independently S. Chowla (1961), proved that over an arbitrary algebraic extension, this equation admits only finitely many solutions in units u, v. Thus, exceptional units were originally studied from a Number Theoretic perspective.

After a hiatus of approximately 45 years, exceptional units have re-emerged in recent research, specifically within $\mathbb{Z}_n$ and, more broadly, in finite commutative rings (see [11], [14], [5]), again primarily from a Number Theoretic viewpoint. For example, Sander ([11]) determines the number of ways an element in $\mathbb{Z}_n$ can be expressed as a sum of two exceptional units - that is, the sumset $U_e(\mathbb{Z}_n)+U_e(\mathbb{Z}_n)$ is characterized.

MSC2010: 15B36, 16U99, 11D09 Keywords: exceptional unit, complementable unit, matrix, quadratic Diophantine equation. Orcid: 0000-0002-3353-6958.

In this paper, we shift focus to a Ring Theoretic investigation of exceptional units, with special emphasis on matrix rings. In Section 2, we present general results about exceptional units in arbitrary unital rings. In Section 3, we provide several characterizations of exceptional units specifically in matrix rings. In Section 4, we define and examine a special subclass of exceptional units, termed complementable. An exunit u is called *complementable* if $u(1-u)=1$. We determine the complementable units in residue class rings and in certain matrix rings.

Throughout this paper, all rings considered are associative and unital. By a triangular matrix, we always mean an upper triangular matrix. A unit of the form $1+t$, where $t\in N(R)$, is called *unipotent*. When convenient, we use the standard abbreviation "iff" for "if and only if."

2. General facts

As mentioned in the introduction, $u\in U(R)$ is exceptional iff there exists $v\in U(R)$ such that $u+v=1$. Clearly, this implies that v is also exceptional. Thus, the definition naturally gives rise to pairs of exunits. In what follows, we use the term pair of exunits exclusively in this sense.

In general, the set $U(R)$ is not closed under addition. However, exunits arise precisely in those cases where a sum of units is again a unit. Indeed, if $u+v=w$ with $u,v,w\in U(R)$ then $uw^{-1}+vw^{-1}=1$, showing that uw^{-1}, vw^{-1} form a pair of exunits.

A ring R is called *2-good* (see [13]) if every element of R can be written as the sum of two units. In such rings, every unit gives rise to (at least) one pair of exunits.

In any nonzero ring, the identity element $1\in U(R)$ is not exceptional. More generally, *unipotent units are not exceptional.*

A ring was termed *UU* in [3] if $U(R)=1+N(R)$, that is, all units are unipotent. Consequently, *UU rings contain no exunits.* Notably, *Boolean rings* or the field $\mathbb{F}_2$ are UU rings and hence *have no exunits.* In fact, $\mathbb{F}_2$ is the only field without exunits.

In any division ring D, every unit except 1 is clearly exceptional. Therefore, $U_e(D)=D-\{0,1\}$.

The property of being exceptional is invariant under conjugation: for $u\in U_e(R)$ and $v\in U(R)$, the conjugate $v^{-1}uv\in U_e(R)$, since $1-v^{-1}uv=v^{-1}(1-u)v\in U(R)$.

However, the set $U_e(R)$ is not closed under negation or multiplication. That is, even if $u,v\in U_e(R)$, it is not necessarily the case that $-u\in U_e(R)$ or $uv\in U_e(R)$, as concrete examples will demonstrate.

We collect several elementary properties in the next proposition, with examples provided thereafter.

Proposition 2.1. *(a) In any ring R, the only possible order 2 exunit is -1. This is the case iff $2\in U(R)$.*

(b) All possible (order n) exunits are roots of the polynomial $1+X+...+X^{n-1}$, that is, are roots of unity $\neq 1$.

(c) The number of exunits in $\mathbb{Z}_n$ is $n\prod\limits_{p|n}(1-\frac{2}{p})$ with prime p.

(d) Any pair of exunits $u,v\in R$ determines another two pairs of exunits: u^{-1}, $-vu^{-1}$ and v^{-1}, $-v^{-1}u$. These three pairs are different *iff u,v are not roots of the polynomial $X^2-X+1\in R[X]$.*

(e) For any pair of exunits, $u^{-1}v = vu^{-1}$ resp. (equivalently) $uv^{-1} = v^{-1}u$ (each exunit commutes with the inverse of its pair). More, exunits in a pair are mutually conjugate.

(f) Inverses of exunits are also exunits.

Proof. (a) Suppose $u^2 = 1$ is an exunit. Then by left multiplying $(1-u)(1+u) = 1-u^2 = 0$ with $(1-u)^{-1}$ we get $1+u = 0$, i.e. $u = -1$. However, -1 is exceptional iff $1-(-1) = 2$ is a unit. Actually whenever 2 is a unit, it is also an exunit.

(b) If $a^n = 1$ in any (unital) ring R, then $a \in U(R)$ and if $a \in U_e(R)$, by left multiplying $(1-a)(1+a+a^2+...+a^{n-1}) = 1-a^n = 0$ with $(1-a)^{-1}$ we obtain $1+a+a^2+...+a^{n-1} = 0$.

(c) See [11]. Nevertheless, the topic may have been addressed in earlier sources.

(d) Multiplying $u+v = 1$, both sides with u^{-1} and v^{-1}, respectively, gives $1 = u^{-1} + (-u^{-1}v) = u^{-1} + (-vu^{-1})$ and $1 = v^{-1} + (-uv^{-1}) = v^{-1} + (-v^{-1}u)$.

For the second statement, suppose $u+v = 1$, $1-u+u^2 = 0 = 1+v+v^2$. Then $v = -u^2$, $u = -v^2$ and since $u^3 = v^3 = -1$ (by multiplying with $1+u$ resp. $1+v$), $u^{-1} = -u^2 = v$ (and $v^{-1} = -v^2 = u$), so $1 = u^{-1} + (-u^{-1}v) = v^{-1} + (-uv^{-1})$ are the same pair.

(e) Follows from the proof of (d). It is easy to check $v = uvu^{-1}$ and $u = v^{-1}uv$.

(f) If $u, 1-u \in U(R)$ then $1-u^{-1} = -(1-u)u^{-1} \in U(R)$. □

Remarks. 1) 4 and 11 are order 2 units in $\mathbb{Z}_{15}$, but none is exceptional. The exunits in $\mathbb{Z}_{15}$ are $2, 8, 14$.

Negatives of exunits may not be exunit: indeed, $-2 = 13$ is not an exunit

Products of exunits may not be exunits. Even $u(1-u) \notin U(R)$ is possible: $2+14 = 1$ but $2 \cdot 14 = 13$ is not an exunit.

2) For each idempotent $e \in R$, $2e-1$ is an order 2 unit. By the above proposition, it is an exunit iff $2e-1 = -1$, i.e. iff $2e = 0$ (e.g. 3 in $\mathbb{Z}_6$).

3) Among other characterizations, a ring R is *local* iff for any $a \in R$, $a \in U(R)$ or $1-a \in U(R)$. Since the disjunction "or" has *not* an exclusive meaning, *local rings may have exunits.* Indeed, 2 is a unit (so forms a pair of exunits with -1) in the ring of integers localized at the prime ideal $p\mathbb{Z}$: $\mathbb{Z}_{(p)} = \{\frac{m}{n} \in \mathbb{Q} : \gcd(p,n) = 1\}$, for any odd prime p. Clearly $2 \cdot \frac{1}{2} = 1$, with p not dividing 2.

Other properties are given in the next list.

Theorem 2.2. *(a) An element is an exunit in a direct product (sum) of rings iff all its components are exunits.*

(b) Let u be an exunit in R, $e^2 = e \in R$ and $\overline{e} + u \in eRe$. Then eue is an exunit in eRe. However, corners of rings with exunits may not have exunits.

(c) Let A be a proper ideal in R. If u is an exunit in R then $u+A$ is an exunit in R/A. However, exunits may not lift in a factor ring R modulo a proper ideal.

Proof. (a) Obvious.

(b) Recall that the units in a corner ring are given by the equality $U(eRe) = (eRe) \cap (\overline{e} + U(R))$. Equivalently, $a = \overline{e} + u$ is a unit in eRe iff $a \in eRe$. Also note that in this case, $a = eae = eue$, and so $eu^{-1}e$ is the inverse of $a = eue$ (both in eRe).

So every unit a of eRe is determined by a unit u of R. If u is an exunit, we just multiply $u+v = 1$ both sides with e: $eue + eve = e$.

For the last claim: $\mathbb{Z}$ is a corner for $\mathbb{M}_2(\mathbb{Z})$, which has plenty of exunits (see Proposition 3.9, next section).

(c) The first part is obvious. As seen above $2, 8, 14$ are exunits in $\mathbb{Z}/15\mathbb{Z}$, but do not lift since $\mathbb{Z}$ has no exunits. □

3. Exunits in matrix rings

We primarily consider the problem over commutative rings, in order to take advantage of tools such as the determinant, the Cayley–Hamilton theorem, and related techniques.

We note that a matrix $U \in \mathbb{M}_n(R)$ is an exceptional unit if and only if its transpose U^T is also an exceptional unit.

Furthermore, exceptional invertible matrices can be characterized in terms of their characteristic polynomials, a connection that will be explored in detail.

Proposition 3.1. *Let R be a commutative ring, $U \in GL_n(R)$ and let $p_U(X) = \det(XI_n - U)$ be the characteristic polynomial of U. Then U is exceptional iff $p_U(1) \in U(R)$.*

Proof. Obvious: $p_U(1) = \det(I_n - U)$. □

Corollary 3.2. *(i) A 2×2 matrix U over a commutative ring R is an exunit iff $\det(U) \in U(R)$ and $1 - \mathrm{Tr}(U) + \det(U) \in U(R)$.*

(ii) A 3×3 matrix U over a commutative ring R is an exunit iff $\det(U) \in U(R)$ and $1 - \mathrm{Tr}(U) + \frac{1}{2}(\mathrm{Tr}(U)^2 - \mathrm{Tr}(U^2)) - \det(U) \in U(R)$.

Proof. (i) Indeed, $\det(I_2 - U) = 1 - \mathrm{Tr}(U) + \det(U)$.

(ii) Indeed, $p_U(X) = X^3 - \mathrm{Tr}(U)X^2 + \frac{1}{2}[\mathrm{Tr}(U)^2 - \mathrm{Tr}(U^2)]X - \det(U)$ and so $\det(I_3 - U) = 1 - \mathrm{Tr}(U) + \frac{1}{2}[\mathrm{Tr}(U)^2 - \mathrm{Tr}(U^2)] - \det(U)$. □

Remarks. 1) In the general case, if the ring R has zero characteristic, a characterization in terms of traces of powers of U holds. Indeed, $p_U(X) = \det(XI_n - U) =$

$$\sum_{k=0}^{n} X^{n-k}(-1)^k \tfrac{1}{k!}T_k, \text{ with } T_k = \det \begin{bmatrix} \mathrm{Tr}(U) & k-1 & 0 & ... & 0 \\ \mathrm{Tr}(U^2) & \mathrm{Tr}(U) & k-2 & ... & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ \mathrm{Tr}(U^{k-1}) & \mathrm{Tr}(U^{k-2}) & & ... & 1 \\ \mathrm{Tr}(U^k) & \mathrm{Tr}(U^{k-1}) & & ... & \mathrm{Tr}(U) \end{bmatrix}.$$

Therefore $U \in GL_n(R)$ is exceptional iff $\det(I_n - U) = \sum_{k=0}^{n} (-1)^k \frac{1}{k!}T_k \in U(R)$.

2) Clearly, all invertible 2×2 matrices with $\mathrm{Tr}(U) = 1$ (over any commutative ring) are exceptional, since in that case $\det(I_2 - U) = \det(U)$.

The *triangular* case can be easily ruled out over any ring, not necessarily commutative.

Proposition 3.3. *Let U be a triangular invertible $n \times n$ matrix over any ring R. Then U is exceptional iff the diagonal entries are exceptional units. If $2 \in U(R)$ then $2I_n$ is an exceptional unit.*

Proof. A triangular matrix $U = [u_{ij}]$ is invertible iff its diagonal entries are units, that is $u_{11}, ..., u_{nn} \in U(R)$. Same for $I_n - U$, i.e. $1 - u_{11}, ..., 1 - u_{nn} \in U(R)$. So all diagonal entries must be exunits. □

Since $U(\mathbb{Z}) = \{\pm 1\}$ and none is exceptional we obtain at once

Corollary 3.4. *There are no triangular integral exceptional invertible matrices.*

However, there exist 2×2 and 3×3 triangular exunits. Moreover, these can be diagonal.

Example. Over $\mathbb{Z}_3$, for any a, the matrices $\begin{bmatrix} 2 & a \\ 0 & 2 \end{bmatrix}$ are exunits (in particular $U = 2I_2$ is diagonal). Similarly $U = 2I_3$ is a diagonal 3×3 exunit.

Proposition 3.5. *A triangular matrix U over any division ring D is an exunit iff no diagonal entry is* 0 *or* 1.

Proof. In any division ring D, $U_e(D) = D - \{0, 1\}$. □

Having settled the case of 2×2 matrices with at least one zero off-diagonal entry (i.e., triangular matrices), we now turn our attention to matrices with at least one zero on the diagonal.

Proposition 3.6. *Let* $A = \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \in \mathbb{M}_2(R)$ *with* $b, c \in U(R)$*. Then*

(i) A is invertible.

(ii) A is an exunit iff $a - 1 + bc \in U(R)$.

(iii) Same conclusions for matrices of form $\begin{bmatrix} 0 & b \\ c & d \end{bmatrix}$ *(here $cb + d - 1 \in U(R)$ gives the exunits).*

Proof. (i) It is readily checked that $A^{-1} = \begin{bmatrix} 0 & c^{-1} \\ b^{-1} & -b^{-1}ac^{-1} \end{bmatrix}$.

(ii) By writing $(A - I_2)W = I_2$ with $W = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$ we get

$$\begin{bmatrix} (a-1)x + bz = 1 \\ (a-1)y + bt = 0 \\ cx - z = 0 \\ cy - t = 1 \end{bmatrix},$$

a solvable linear system iff $a - 1 + bc \in U(R)$ (we replace $z = cx$ in the first equation and $t = cy - 1$ in the second equation). If so, we get

$$(A - I_2)^{-1} = \begin{bmatrix} (a-1+bc)^{-1} & (a-1+bc)^{-1}b \\ c(a-1+bc)^{-1} & c(a-1+bc)^{-1}b - 1 \end{bmatrix},$$

since the right inverse W turns out to be also a left inverse.

(iii) These matrices are obtained from the ones in the statement, by conjugation with $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. □

Remark. If R is a division ring, the conditions are simply $b \neq 0 \neq c$ and $a - 1 + bc \neq 0$, respectively.

A 3×3 version also holds.

Proposition 3.7. *Let* $A = \begin{bmatrix} a & b & c \\ d & e & 0 \\ f & 0 & 0 \end{bmatrix} \in \mathbb{M}_3(R)$ *with* $c, e, f \in U(R)$*. Then*

(i) A is invertible.
(ii) A is an exunit iff d is a unit and $b-(a+cf-1)d^{-1}(e-1)\in U(R)$.

Proof. (i) As in the previous proposition, we search for a 3×3 matrix W such that $AW=I_3$ and check that also $WA=I_3$ holds. The suitable (unique) matrix is $A^{-1}=\begin{bmatrix} 0 & 0 & f^{-1} \\ 0 & e^{-1} & -e^{-1}df^{-1} \\ c^{-1} & -c^{-1}be^{-1} & -c^{-1}af^{-1}+c^{-1}be^{-1}df^{-1}\end{bmatrix}$.

(ii) Analogously, for $(A-I_3)V=I_3$, we replace a and d by $a-1$, $d-1$, respectively and the SE corner by -1. The system is solvable iff d is a unit and $b-(a-1+cf)d^{-1}(e-1)$ has a right inverse. However, since we have to check also $V(A-I_3)=I_3$, we need this to be a (two-sided) unit. If we denote $\alpha=[b-(a-1+cf)d^{-1}(e-1)]^{-1}$ and $\beta=(a-1+cf)d^{-1}$ we get

$$(A-I_3)^{-1}=\begin{bmatrix} -d^{-1}(e-1)\alpha & d^{-1}[1+(e-1)\alpha\beta] & -d^{-1}(e-1)\alpha c \\ \alpha & -\alpha\beta & \alpha c \\ -fd^{-1}(e-1)\alpha & fd^{-1}[1+(e-1)\alpha\beta] & -fd^{-1}(e-1)\alpha c-1\end{bmatrix}$$

(note that $b-\beta(e-1)=\alpha^{-1}$). □

Recall that a ring R is called *Dedekind finite* if $ab=1$ for $a,b\in R$ implies $ba=1$ (i.e., one-sided invertible elements are two-sided). Matrix rings over commutative rings are Dedekind finite.

In the general 2×2 case, *if* $\mathbb{M}_2(R)$ *is Dedekind finite* (in particular, if R is commutative), we have the following result.

Proposition 3.8. *Let $U=\begin{bmatrix} a & b \\ c & d\end{bmatrix}$ be a matrix, $a,d\in U(R)$ and suppose $\mathbb{M}_2(R)$ is Dedekind finite. Then U is an unit iff $a-bd^{-1}c, d-ca^{-1}b\in U(R)$ and an exunit iff also $a-1-bd^{-1}c, d-1-ca^{-1}b\in U(R)$.*

Proof. Let $W=\begin{bmatrix} x & y \\ z & t\end{bmatrix}$ be such that $UW=I_2$. This amounts to the system

$$\begin{aligned} ax+bz&=1\\ ay+bt&=0\\ cx+dz&=0\\ cy+dt&=1\end{aligned}$$

and the middle equations can be solved as $y=-a^{-1}bt$ and $z=-d^{-1}cx$.

By replacement we get $(a-bd^{-1}c)x=1$ and $(d-ca^{-1}b)t=1$ so W exists iff $a-bd^{-1}c, d-ca^{-1}b\in U(R)$. In order to have an exunit, we also need a matrix P such that $(U-I_2)P=I_2$, that is, the same as above, replacing a by $a-1$ and d by $d-1$ (this explains why we prefer $U-I_2$ instead of I_2-U). So $a-1-bd^{-1}c, d-1-ca^{-1}b\in U(R)$. □

Remarks. 1) Over any division ring, the conditions become $a-bd^{-1}c\neq 0, 1\neq d-ca^{-1}b$.

2) There are *another three similar characterizations* for exunits $U=\begin{bmatrix} a & b \\ c & d\end{bmatrix}$ with Dedekind finite $\mathbb{M}_2(R)$:

(i) $a, a-1, c\in U(R)$ (so a is exunit) together with $b-ac^{-1}d$, $d-ca^{-1}b\in U(R)$ and $b-(a-1)c^{-1}(d-1)$, $(d-1)-c(a-1)^{-1}b\in U(R)$,

(ii) $b, c \in U(R)$ together with $b - ac^{-1}d$, $c - db^{-1}a \in U(R)$ and $b - (a-1)c^{-1}(d-1)$, $c - (d-1)b^{-1}(a-1) \in U(R)$,

(iii) $b, d, d-1 \in U(R)$ (so d is exunit) together with $a - bd^{-1}c$, $c - db^{-1}a \in U(R)$ and $a - 1 - b(d-1)^{-1}c$, $c - (d-1)b^{-1}(a-1) \in U(R)$.

The remaining possibilities $a, b \in U(R)$ or $c, d \in U(R)$ are also covered by transpose.

3) For $b, c \in U(R)$ and $d = 0$, the conditions are $b + (a-1)c^{-1}$, $c + b^{-1}(a-1) \in U(R)$, both equivalent to $bc + a - 1 \in U(R)$, as in the previous proposition.

The following characterization, which follows from Corollary 3.2, provides a more detailed description of 2×2 *integral* exunits.

Proposition 3.9. *A 2×2 integral matrix U is an exunit iff* $\det(U) = 1$ *and* $\mathrm{Tr}(U) \in \{1, 3\}$*, or else* $\det(U) = -1$ *and* $\mathrm{Tr}(U) \in \{-1, 1\}$*.*

Recall that $\mathbb{Z}$ does not contain exunits, while $\mathbb{M}_2(\mathbb{Z})$ does.

Corollary 3.10. *Even if a ring lacks exunits, its matrix ring may contain exunits.*

Corollary 3.11. *For a 2×2 integral exunit U, $-U$ is also an exunit iff* $\det(U) = -1$*.*

Proof. Just note that $\mathrm{Tr}(-U) = -\mathrm{Tr}(U)$ and $\det(-U) = \det(U)$. □

Example. In the previous section, examples were given in residue class rings, in order to show that negatives or products of exunits may not be exunits. Here are some examples in matrix rings.

$U = \begin{bmatrix} -1 & 5 \\ -1 & 4 \end{bmatrix}$ is an integral exunit, but $-U = \begin{bmatrix} 1 & -5 \\ 1 & -4 \end{bmatrix}$ is not (its trace is -3).

Moreover, U and $I_2 - U$ are exunits but $U(I_2 - U) = \begin{bmatrix} 3 & -10 \\ 2 & -7 \end{bmatrix}$ is not: the trace is -4 (alternatively: $I_2 - \begin{bmatrix} 3 & -10 \\ 2 & -7 \end{bmatrix} = \begin{bmatrix} -2 & 10 \\ -2 & 8 \end{bmatrix}$ is not invertible).

Determining the 3×3 integral exceptional invertible matrices is considerably more challenging. To approach this problem, we examine several special cases.

An integral matrix is invertible iff its determinant equals ±1. This condition implies that the entries in any row or column must be coprime - that is, their greatest common divisor must be 1. More precisely, we have the following result.

Proposition 3.12. *Let a, b, c be entries in any row (or any column) of an integral invertible 3×3 matrix U and let a be the diagonal entry. Two necessary conditions for U to be an exunit are: a, b, c are coprime and so are $1 - a, b, c$.*

So if a, b, c are entries in a row (or column) and a is the diagonal entry, we should have $\gcd(a; \gcd(b; c)) = 1 = \gcd(1 - a; \gcd(b; c))$.

In a special case, we have the following result.

Proposition 3.13. *Let U be a 3×3 integral invertible matrix.*

(i) If U has two even, non-diagonal entries, in the same row or column, then U is not exceptional.

(ii) There exist infinitely many integral exceptional invertible matrices with two even entries in the same row or column, provided that one of these lies on the diagonal.

Proof. (i) If two not diagonal entries in the same row (or column) of U are even, since U is invertible, the corresponding diagonal entry must be odd. Then in $I_3 - U$, the entries in the same row (or column) are even and so $\det(I_3 - U) \in 2\mathbb{Z}$. Hence U is not an exunit.

(ii) We discuss the case $u_{11} = u_{31} = 0$ and, since $\det(U) = \pm 1$, accordingly $u_{21} = \pm 1$.

If $\det(U) = 1$ and $u_{21} = 1$, then for $u_{33} = u_{13} = u_{32} = 1$, $u_{12} = 0$ and $u_{23} = -2$, we have infinitely many exunits: $U = \begin{bmatrix} 0 & 0 & 1 \\ 1 & a & -2 \\ 0 & 1 & 1 \end{bmatrix}$. The case $u_{21} = -1$ is analogous.

If $\det(U) = -1$ and $u_{21} = 1$, then for $u_{33} = u_{13} = 1$, $u_{32} = -1$, $u_{12} = 0$ and $u_{23} = -2$, we have infinitely many exunits: $U = \begin{bmatrix} 0 & 0 & 1 \\ 1 & a & -2 \\ 0 & -1 & 1 \end{bmatrix}$. The case $u_{21} = -1$ is analogous. □

4. Complementable (ex)units

The starting point of this section is the observation that the equation $x(1-x) = 0$ defines precisely the idempotent elements in any unital ring. This naturally leads to the question: what kind of elements are defined by the equation $x(1-x) = 1$?

Since x and $1 - x$ commute in any ring, it follows that *both must be units*, and more precisely, that $1 - x = x^{-1}$.

Thus, this equation defines a special class of (ex)units $u \in U(R)$, for which $1 - u$ is the inverse of u. To simplify terminology, we call such elements *complementable* units and suggestively, we refer to the inverse $u^{-1} = 1 - u$ as the *complementary* unit to u. Clearly, if u is complementable, then so is $1 - u$.

It is well-known that such units do not exist in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, but they do exist in the field of complex numbers. Specifically, there are exactly two such units in $\mathbb{C}$, complementary to each other: $u_{1,2} = \frac{1}{2}(1 \pm i\sqrt{3})$.

As a positive example in finite rings, the element 2 is *self-complementable* (i.e., $1 - u = u$) in $\mathbb{Z}_3$, since $2(1-2) = 2 \cdot 2 = 1$. On the other hand, the element 1 is never complementable in any unital ring.

The central problem in this line of study is *the existence problem* - determining when such complementable units exist - both in division rings (or fields) and in arbitrary rings, whether commutative or not. In what follows, we address this problem for residue class rings $\mathbb{Z}_n$ and for $\mathbb{M}_n(R)$, the ring of $n \times n$ matrices over commutative rings R, with special emphasis to the $n = 2$ case.

4.1. In residue class rings $\mathbb{Z}_n$.

For easy reference we mention the equivalent definitions of complementable units.

Lemma 4.1. *Let a be an element of a ring R. The following conditions are equivalent.*

(i) $a^2 - a + 1 = 0$,

(ii) $a(1 - a) = 1$,

(iii) a is a unit and $1 - a = a^{-1}$,

(iv) a is a unit and $a + a^{-1} = 1$.

First we discuss the case when the unit u is self-complementable.

Proposition 4.2. *In a ring R there exist self-complementable units iff $3 = 0$ iff $char(R) = 3$. In this case, 2 is the only self-complementable unit.*

Proof. Equivalently, we are searching for units u such that $2u = 1$ and $u^2 = 1$.

It follows that $u = 2^{-1}$ and so $2^{-2} = 1$. Hence $4 = 1$ and this holds if $3 = 0$. Conversely, if $3 = 0$ then $2 \cdot 2 = 1$ and $1 - 2 = -1 = -1 + 0 = -1 + 3 = 2$. □

Corollary 4.3. *$\mathbb{Z}_3$ is the only residue class ring which has self-complementable units. In $\mathbb{Z}_3$, 2 is the only self-complementable unit.*

Except for self-complementable units, all complementable units must occur in pairs. Therefore, if any such units exist, their total number must be even.

In both $\mathbb{Z}$ and $\mathbb{Z}_n$ (for some positive integer n), the elements u and $1 - u$ have opposite parity. As a result, the product $u(1 - u)$ is even. This implies that a necessary condition for the existence of complementable units is that 2 must be a unit. Consequently, there are no complementable units in $\mathbb{Z}$ and such units may exist in $\mathbb{Z}_n$ only when n is odd, that is, when 2 is a unit in $\mathbb{Z}_n$.

However, this condition is not sufficient. For example, in $\mathbb{Z}_5$, which is a field, so all nonzero elements are units, none are complementable. The relevant pairs $(u, 1 - u)$ are: $(2, 4), (3, 3), (4, 2)$ but none of these satisfies $u(1 - u) = 1$. On the other hand, in $\mathbb{Z}_7$, there are two complementable (and complementary) units: 3 and 5. These correspond to the pairs $(3, 5)$ where $5 = 1 - 3 \bmod 7$ and $(5, 3)$ where $3 = 1 - 5 \bmod 7$.

In order to characterize the complementable units in residue class rings, we need some prerequisites.

We first recall some well-known (or easy to prove) facts.

Lemma 4.4. *1. Every prime number, excepting 2 and 3, is of form $6n + 1$ or $6n - 1$.*

2. Products of integers of the form $6n + 1$ are also of the form $6n + 1$. In particular, this holds for products of powers of prime numbers that are themselves of the form $6n + 1$.

3. Let d be an odd positive integer. Then $d \equiv 1$ (mod 3) iff $d \equiv 1$ (mod 6).

4. 9 does not divide $n^2 - n + 1$, for any positive integer n.

Proof. **3**. One way is obvious. Conversely, suppose $d = 3k + 1$ for some k. As d is odd, it follows that $2 \mid k$ and so $d = 6h + 1$ for some h.

4. Denote $\sigma := n^2 - n + 1$. For $n = 3m$, $\sigma = 3m(3m - 1) + 1$, for $n = 3m + 1$, $\sigma = 3m(3m + 1) + 1$ and for $n = 3m + 2$, $\sigma = 9m(m + 1) + 3$. □

We also need the classical Hensel's Lemma.

Lemma 4.5. *Let $f(x)$ be a polynomial with integer coefficients, and let p be a prime. Suppose $f(a) \equiv 0 \bmod p$, and $f'(a) \not\equiv 0 \bmod p$. Then, $\bmod p^2$, there exists a unique integer b such that $b \equiv a \bmod p$ and $f(b) \equiv 0 \bmod p^2$.*

One can also keep repeating this process to find roots modulo p^3, p^4,...

A special case will be useful.

Corollary 4.6. *Let p be a prime number greater than 3. If $x^2 \equiv -3 \bmod p$ is solvable over the integers then also $x^2 \equiv -3 \bmod p^k$ is solvable over the integers, for every $k \geq 2$.*

Proof. Define the polynomial $f(x) = x^2+3$. Then by hypothesis $f(-3) \equiv 0 \bmod p$. Next, we show that $f'(x) \not\equiv 0 \bmod p$.

Since $x^2 \equiv -3 \bmod p$ and $p > 3$, we have $x \not\equiv 0 \pmod p$, hence $f'(x) = 2x \not\equiv 0 \pmod p$.

So Hensel's Lemma applies and we can lift the solution $x \equiv -3 \bmod p$ to a unique solution modulo p^2, i.e., there exists a unique nonnegative $b < p^2$ such that $b \equiv -3 \bmod p$ such that $b^2 \equiv -3 \bmod p^2$. This process extends uniquely to higher powers p^k. □

To solve the congruence $x^2 - x + 1 \equiv 0 \pmod{2k+1}$, we equivalently seek the solutions of the associated quadratic Diophantine equation

$$x^2 - x + 1 = (2k+1)y.$$

Theorem 4.7. *Let k be a positive integer. The quadratic Diophantine equation*

$$x^2 - x + 1 = (2k+1)y$$

has integer solutions if and only if $2k+1$ is either a product of powers of prime numbers of the form $6n+1$ for some $n \geq 1$, or such a product multiplied by 3 (allowing $n = 0$ in this case). That is, the equation is solvable if and only if

$$2k+1 \in \left\{\prod p_i^{e_i} \mid p_i \equiv 1 \pmod 6\right\} \cup \left\{3 \cdot \prod p_i^{e_i} \mid p_i \equiv 1 \pmod 6\right\}.$$

Proof. We start with the Diophantine equation

$$x^2 - x + 1 = (2k+1)y.$$

Multiplying both sides by 4 we get $(2x-1)^2 + 3 = 4(2k+1)y$. Thus, the equation has integer solutions iff the congruence

$$T^2 \equiv -3 \pmod{4(2k+1)} \quad \text{where } T = 2x - 1.$$

is solvable.

We factor the modulus as $4(2k+1) = 2^2(2k+1)$. The congruence $T^2 \equiv -3 \bmod 4$ becomes:

$$T^2 \equiv 1 \mod 4 \Rightarrow T \equiv 1, 3 \mod 4$$

So solutions modulo 4 always exist. The solvability now depends on whether

$$T^2 \equiv -3 \pmod{2k+1}$$

is solvable. That is, we must determine when -3 is a quadratic residue modulo $2k+1$.

Note that if $9 \mid m$ then $T^2 \equiv -3 \pmod{2k+1}$ has no integer solutions.

Let p be an odd prime greater than 3. We use the Legendre symbol $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$ and standard results for

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{p}{3}\right)$$

and so $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$. Thus, -3 is a quadratic residue modulo p if and only if $\left(\frac{p}{3}\right) = 1$, which holds precisely when $p \equiv 1 \pmod 3$. As mentioned in Lemma 4.4, **3**, these primes are exactly those of the form $p = 6n+1$.

Further, we perform the extension to powers of prime numbers with Corollary 4.6 and to composite moduli via the Chinese Remainder Theorem (CRT)**.**

Let $m = 2k + 1$ be a product of odd primes.

- If all prime factors of m are congruent to $1 \pmod 3$ (i.e., $6n+1$), then -3 is a quadratic residue modulo each factor. By the CRT, it is also a quadratic residue modulo m.
- If $m = 3 \cdot m'$, where m' is a product of primes $\equiv 1 \pmod 6$, then $-3 \equiv 0 \pmod 3$, so it is trivially a quadratic residue mod 3. Since it is also a residue modulo m', CRT implies it is a residue modulo m.

Therefore, -3 is a quadratic residue modulo m is a necessary condition.

Conversely, suppose -3 is a quadratic residue modulo some odd prime p. Then

$$\left(\frac{-3}{p}\right) = 1 \Rightarrow \left(\frac{p}{3}\right) = 1 \Rightarrow p \equiv 1 \pmod 3 \Rightarrow p = 6n + 1$$

as p is odd. Similarly, the same holds for products of such primes and their product with 3. □

Corollary 4.8. *Let $m > 1$ be any positive integer. In the residue class ring $\mathbb{Z}_m$ there exist complementable units if and only if m is either a product of powers of prime numbers of the form $6n + 1$ for some $n \geq 1$, or such a product multiplied by 3 (allowing $n = 0$ in this case).*

We now present several examples of complementary units in some small order residue class rings.

$(2, 2)$ in $\mathbb{Z}_3$, $(3, 5)$ in $\mathbb{Z}_7$, $(4, 10)$ in $\mathbb{Z}_{13}$, $(5, 17)$ in $\mathbb{Z}_{21}$, $(6, 26)$ in $\mathbb{Z}_{31}$, $(7, 37)$ in $\mathbb{Z}_{43}$.

$(8, 12)$ in $\mathbb{Z}_{19}$, $(11, 27)$ in $\mathbb{Z}_{37}$, $(17, 23)$ in $\mathbb{Z}_{39}$, $(19, 31)$ in $\mathbb{Z}_{49}$, $(8, 50)$ in $\mathbb{Z}_{57}$, $(14, 48)$ in $\mathbb{Z}_{61}$, $(30, 38)$ in $\mathbb{Z}_{67}$.

However, a pair of complementable units in a given $\mathbb{Z}_n$ may not be unique (if it exists). An example: $(10, 82)$ and $(17, 75)$ in $\mathbb{Z}_{91}$.

While no simple, universal formula seems to exist for all values of n – particularly when dealing with composite moduli – if $6n + 1 = p$ is prime, then square roots of $-3 \bmod p$ can be computed using the Tonelli–Shanks algorithm. Even so, a detailed discussion of this method falls outside the scope of this paper.

However, in a significant number of special cases, we can identify the complementary units.

Proposition 4.9. *The equation $x^2 - x + 1 \equiv 0 \pmod{2k + 1}$ is solvable if $2k + 1 = m(m + 1) + 1$, for some positive integer $m \geq 1$.*

Proof. We just verify that $(m+1)^2-(m+1)+1 = m^2+m+1 \equiv 0 \pmod{m(m-1)+1}$. Hence $m + 1$ is a solution.

A second solution exists: m^2+1. Indeed, $(m^2+1)^2-(m^2+1)+1 = m^4+m^2+1 = (m^2 + m + 1)(m^2 - m + 1)$. □

Therefore

Corollary 4.10. *For every positive integer m, $m+1$ and m^2+1 are complementary units in $\mathbb{Z}_{m^2+m+1}$.*

Proof. Indeed, $(m + 1) + (m^2 + 1) = (m^2 + m + 1) + 1$. □

Remark. The cases listed in the above proposition (i.e., $2k+1 = m(m+1)+1$), belong to the set described in Theorem 4.7, that is, product of powers of prime numbers of the form $6n+1$, possibly multiplied by 3. This follows directly from the existence of complementary units in $\mathbb{Z}_{m^2+m+1}$ and the previous corollary.

4.2. **In $\mathbb{M}_2(R)$ for commutative rings.** By matrix multiplication, we can state the complementable conditions in the general $n \times n$ case.

Theorem 4.11. *The complementable $n \times n$ units over any commutative ring R are the matrices $U = [a_{ij}]_{1 \le i,j \le n}$ such that*

(i) for every $i \in \{1, ..., n\}$, $a_{ii}(1 - a_{ii}) = 1 + \sum_{\substack{j=1 \\ j \neq i}}^{n} a_{ij}a_{ji}$,

(ii) for every $i, j \in \{1, ..., n\}$, $i \neq j$, $a_{ij}(1 - a_{jj}) = \sum_{\substack{k=1 \\ k \neq j}}^{n} a_{ik}a_{kj}$.

Proof. Start with an invertible matrix $U = [a_{ij}] \in \mathbb{M}_n(R)$ for a commutative ring R. Then $U(I_n - U) = I_n$ amounts to the conditions in the statement. □

Let R be a commutative ring and let $s \in R$. Denote $D(s) = \{t \in R : st = 0\}$, the set of the zero divisors associated to s and by $D(R)$ the set of all the zero divisors of R.

Proposition 4.12. *The complementable 2×2 units over any commutative ring R are the matrices $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $a(1-a) - bc = 1 = d(1-d) - bc$ and $b(1-a-d) = 0 = c(1-a-d)$. In particular,*

(i) if $1 - Tr(U)$ is not a zero divisor, the complementable 2×2 units are scalar (i.e., aI_2, for some complementable element a of R),

(ii) if $Tr(U) = 1$, the complementable 2×2 units are of form $\begin{bmatrix} a & b \\ c & 1-a \end{bmatrix}$ with $a(1-a) = 1 + bc$.

Proof. For the $n = 2$ case, (like in the previous case, we start with an invertible matrix $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{M}_2(R)$ for a commutative ring R. Then $U(I_2 - U) = I_2$ amounts to the following four conditions:

$$\begin{array}{c} a(1-a) - bc = 1 = d(1-d) - bc, \\ b(1-a-d) = 0 = c(1-a-d) \end{array}.$$

From the first two equalities we get $(a-d)(1-a-d) = 0$ and so, if $1-a-d$ is not zero but zero divisor, $b, c, a-d \in D(1-a-d)$.

The special cases follow.

Case (i). $1 - Tr(U) = 1 - a - d$ is not a zero divisor.

Then $b = c = a-d = 0$ and so $a = d$. Finally $U = aI_2$, with any complementable element a of R.

Case (ii). $Tr(U) = 1$, i.e., $a + d = 1$. Then $d = 1 - a$ and $a(1-a) = 1 + bc$. Finally, $U = \begin{bmatrix} a & b \\ c & 1-a \end{bmatrix}$, with $a(1-a) = 1 + bc$. Since $\det(U) = 1$, according to Lemma 4.1 (iii), the complementary unit is the inverse U^{-1}. □

Examples. In $\mathbb{Z}_{13}$, $(4,10)$ are complementary units and in $\mathbb{Z}_{21}$, $(5,15)$ are complementary units.

The first two examples correspond to the special cases in the previous proof.

(i) The scalar matrices $4I_2$, $10I_2$ are complementary units in $\mathbb{M}_2(\mathbb{Z}_{13})$, and $5I_2$, $15I_2$ are complementary units in $\mathbb{M}_2(\mathbb{Z}_{21})$

(ii) The matrix $U = \begin{bmatrix} 7 & 6 \\ 8 & 7 \end{bmatrix}$ is a complementable unit in $\mathbb{M}_2(\mathbb{Z}_{13})$, with $U^{-1} = \begin{bmatrix} 7 & 7 \\ 5 & 7 \end{bmatrix}$ as complementary unit.

Note that $\mathbb{Z}_{21}$ has zero divisors, namely $D(\mathbb{Z}_{21}) = 3\mathbb{Z}_{21} \cup 7\mathbb{Z}_{21}$.

(iii)a Consider $U = \begin{bmatrix} 3 & 7 \\ 14 & 10 \end{bmatrix} \in \mathbb{M}_2(\mathbb{Z}_{21})$ which has $b, c \in D(\mathbb{Z}_{21})$, $1-a-d = 9 \in D(\mathbb{Z}_{21})$ and $\det(U) = 16 \in U(\mathbb{Z}_{21})$. We can check $a(1-a)-bc = 1 = d(1-d)-bc$, $Tr(U) = a+d = 13 \neq 1$, $I_2 - U = \begin{bmatrix} 19 & 14 \\ 7 & 12 \end{bmatrix}$, $\det(I_2-U) = 4 \in U(\mathbb{Z}_{21})$. Finally, $U(I_2-U) = \begin{bmatrix} 106 & 126 \\ 336 & 316 \end{bmatrix} = I_2$, whence U and $I_2 - U$ are complementary units with trace $\neq 1$ and det $\neq 1$.

(iii)b Take $U = \begin{bmatrix} 10 & 7 \\ 14 & 12 \end{bmatrix}$ over $\mathbb{Z}_{21}$, which is Case (ii), above. Here $Tr(U) = a+d = 1$ and the complementary unit is $I_2 - U = U^{-1} = \begin{bmatrix} 12 & 14 \\ 7 & 10 \end{bmatrix}$.

Remarks. 1) With $b, c \in D(7) = 3\mathbb{Z}_{21}$, computer found 32 complementable units, all with trace $a+d = 1$. With $b, c \in D(3) = \{0, 7, 14\}$, computer found 16 complementable units. Only 8 of these have trace $= 1$ and the other 8 have trace $\in \{10, 13\}$. These occur in pairs, since $I_2 - (I_2 - U) = U$.

2) The Cayley-Hamilton's theorem for every 2×2 matrix A over any commutative ring R reads as follows:

$$A^2 - Tr(A)A + \det(A)I_2 = 0_2.$$

It gives precisely our starting equation, whenever $Tr(A) = \det(A) = 1$. Therefore, over any commutative ring R, the 2×2 matrices whose *trace and determinant equal to* 1, are complementable units (this is case (ii) in Proposition 4.12). This actually shows that complementable 2×2 units abound.

From Lemma 4.1, (ii) it follows that the complementary unit is precisely the inverse.

To provide some more examples in the ring $\mathbb{M}_2(\mathbb{Z})$, note that for any given integer b (or c), the solutions of the quadratic Diophantine equation $a^2 - a + bc + 1 = 0$, with unknowns a, c (resp. a, b), often give complementable 2×2 integral units. The solutions were found using [4] (or [1]).

For $c = 1$ we obtain $U_n = \begin{bmatrix} 1-2n & -4n^2+2n-1 \\ 1 & 2n \end{bmatrix}$, infinitely many complementable units, for each integer n. The complementary unit is the inverse U_n^{-1}.

For $c = 3$ we obtain $V_n = \begin{bmatrix} 2-6n & -12n^2+6n-1 \\ 3 & 6n-1 \end{bmatrix}$, infinitely many complementable units, for each integer n. Again, the complementary unit is the inverse V_n^{-1}.

For $c = 2, 4, 5, 6, 8, 9, 10, 11, 12$ there are no complementable units. There are many complementable units also for $c = 7, 13$ and many others.

Acknowledgement. The author is grateful to both referees for their careful reading and helpful suggestions, which improved the presentation, and to Mihai Cipu for generously sharing his expertise in number theory.

5. Declarations

There are no competing interests and no funding.

References

[1] Alpern, D. *Quadratic Equation Solver*. www.alpertron.com.ar/ quad.htm

[2] D. A. Buell *Binary Quadratic Forms*. Springer-Verlag, NY, 1989.

[3] G. Călugăreanu *UU rings*. Carpathian Journal of Mathematics **31** (2) (2015), 157-163.

[4] W. C. Matthews *Solving the Diophantine equation*. www.numbertheory.org/ php/ generalquadratic.html

[5] C. Miguel *On the sumsets of exceptional units in a finite commutative ring*. Monatshefte fur Mathematik **186** (2) (2018), 315-320.

[6] T. Nagell *Les points exceptionnels rationnels sur certaines cubiques du premier genre*. (French) Acta Arith. **5** (1959), 333-357.

[7] T. Nagell *Les points exceptionnels sur les cubiques* $ax^3 + by^3 + cz^3 = 0$. (French) Acta Sci. Math. (Szeged) **21** (1960), 173-180.

[8] T. Nagell *Sur une propriété des unités d'un corps algébrique*. (French) Ark. Mat. **5** (1964), 343-356.

[9] T. Nagell *Sur les unités dans les corps biquadratiques primitifs du premier rang*. (French) Ark. Mat. **7** (1968), 359-394.

[10] T. Nagell *Quelques problèmes relatifs aux unités algébriques*. (French) Ark. Mat. **8** (1969), 115-127.

[11] Sander, J.W. *Sums of exceptional units in residue class rings*. Journal of Number Theory 159 (2016), 1-6.

[12] Šter J. *Lifting units in clean rings*. Journal of Algebra **381** (2013) 200-208.

[13] Vamos P. *2-good rings*. Quarterly J. Math. **56** (3) (2005), 417-430.

[14] Yang, Q.-H., Zhao, Q.-Q. *On the sumsets of exceptional units in* $\mathbb{Z}_n$. Monatshefte fur Mathematik **182** (2) (2017), 489-493.

Department of Mathematics, Babeş-Bolyai University, Cluj-Napoca, 400084, Romania
Email address: calu@math.ubbcluj.ro