Turkish Journal of Mathematics

Volume 48 | Number 5 Article 2

9-10-2024

Rings and finite fields whose elements are sums or differences of tripotents and potents

ADEL ABYZOV

STEPHEN COHEN

PETER DANCHEV

DANIEL TAPKIN

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2024) 48: 817 – 839
© TÜBİTAK
doi:10.55730/1300-0098.3543

Rings and finite fields whose elements are sums or differences of tripotents and potents

Adel ABYZOV[1], **Stephen COHEN**[2], **Peter DANCHEV**[3,*], **Daniel TAPKIN**[4]
[1]Department of Algebra and Mathematical Logic, Kazan Federal University, Republic of Tatarstan, Russia
[2]University of Glasgow, Scotland, UK
[3]Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria
[4]Department of Algebra and Mathematical Logic, Kazan Federal University, Republic of Tatarstan, Russia

Received: 08.03.2024 • **Accepted/Published Online:** 20.05.2024 • **Final Version:** 10.09.2024

Abstract: We significantly strengthen results on the structure of matrix rings over finite fields and apply them to describe the structure of the so-called weakly n-torsion clean rings. Specifically, we establish that, for any field F with either exactly seven or strictly more than nine elements, each matrix over F is presentable as a sum of of a tripotent matrix and a q-potent matrix if and only if each element in F is presentable as a sum of a tripotent and a q-potent, whenever $q>1$ is an odd integer. In addition, if Q is a power of an odd prime and F is a field of odd characteristic, having cardinality strictly greater than 9, then, for all $n\geq 1$, the matrix ring $\mathbb{M}_n(F)$ is weakly $(Q-1)$-torsion clean if and only if F is a finite field of cardinality Q.

A novel contribution to the ring-theoretical theme of this study is the classification of finite fields $\mathbb{F}_Q$ of odd order in which every element is the sum of a tripotent and a potent. In this regard, we obtain an expression for the number of consecutive triples $\gamma-1,\gamma,\gamma+1$ of nonsquare elements in $\mathbb{F}_Q$; in particular, $\mathbb{F}_Q$ contains three consecutive nonsquare elements whenever $\mathbb{F}_Q$ contains more than nine elements.

Key words: (Weakly) n-torsion clean rings, idempotents, tripotents, potents, units, finite fields, Gauss and Jacobi sums

1. Introduction

In this paper, all rings are assumed to be associative with unity but not necessarily commutative unless explicitly specified. Our terminology and notation are, for the most part, standard, being in agreement with those from [11]. Specifically, for such a ring R, $U(R)$ denotes the group of units, $\mathrm{Id}(R)$ is the set of idempotents and $J(R)$ the Jacobson radical of R, respectively. Further, the finite field with Q elements will be denoted by $\mathbb{F}_Q$, and $\mathbb{M}_k(R)$ will stand for the $k\times k$ matrix ring over R, $k\in\mathbb{N}$.

As usual, an element d of a ring R is termed *nilpotent*, provided $d^j=0$ for some integer $j\geq 2$. Moreover, we will say a nil ideal I of R is *nil of index* k if, for any $r\in I$, we have $r^k=0$ and k is the minimal natural number with this property. Likewise, we will say that I is nil of bounded index if it is nil of index k, for some fixed k. Reciprocally, an element t of R is said to be *potent* if there is a natural number $i>1$ with the property $t^i=t$ (actually, t is called *i-potent*). When $i=2$ the element is called *idempotent*, whereas when $i=3$ the element is called *tripotent*.

*Correspondence: danchev@math.bas.bg
2010 *AMS Mathematics Subject Classification:* 11T30; 16D60; 16S34; 16U60.

The main theorem we establish characterizes the structure of those rings whose elements can be represented as a sum or a difference of tripotents (or, even, nilpotents) and potents. It represents an improvement of a recent result of Abyzov and Tapkin, namely [2, Theorem 14].

Theorem 1.1 *Let $q>1$ be an odd integer, and R an integral ring which is not isomorphic to $\mathbb{F}_3$, $\mathbb{F}_5$ or $\mathbb{F}_9$. Then the following seven statements are equivalent.*

(1) For each (for some) $n\in\mathbb{N}$, every matrix in $\mathbb{M}_n(R)$ can be presented as a sum of an idempotent matrix and a q-potent matrix.

(2) For each (for some) $n\in\mathbb{N}$, every matrix in $\mathbb{M}_n(R)$ can be presented as a sum of a nilpotent matrix and a q-potent matrix.

(3) For each (for some) $n\in\mathbb{N}$, every matrix in $\mathbb{M}_n(R)$ can be presented as a sum of a tripotent matrix and a q-potent matrix.

(4) For each (for some) $n\in\mathbb{N}$, every matrix in $\mathbb{M}_n(R)$ can be presented as a sum or a difference of a q-potent matrix and an idempotent matrix.

(5) Every element in R is the sum of a q-potent and a tripotent.

(6) Every element in R is the sum or a difference of a q-potent and an idempotent.

(7) R is a finite field such that $(|R|-1)\mid(q-1)$.

Specifically, the significant addition to [2, Theorem 14] in Theorem 1.1 is the equivalence of statement (1) with statements (3) and (5) (subject only to the exclusion of rings isomorphic to $\mathbb{F}_5$ and $\mathbb{F}_9$, as well as $\mathbb{F}_3$). The key to this improvement is the following theorem on finite fields which seems to be new as a complete result.

Theorem 1.2 *Let $Q=p^r$, where p is an odd prime and $r\in\mathbb{N}$, and N_Q be the number of triples $\gamma-1,\gamma,\gamma+1$ of consecutive nonsquare elements of $\mathbb{F}_Q$. If $Q\leq 9$, then $N_Q=0$; if $Q>9$, then*

$$N_Q\geq\frac{1}{8}\Big(Q-2\sqrt{Q}-3\Big),$$

with equality if and only if $p\equiv 3\pmod 4$ and $r=2s$, where s is odd.

Hence N_Q is positive if and only if $Q>9$.

We remark that, in the proof of Theorem 1.2, we give an exact expression for N_Q in every case.

Our discussion of finite fields, including the proof of Theorem 1.2, occupies Sections 2–4. This leads on to the proof of Theorem 1.1 itself in Section 5.

Moving on, we present applications of Theorem 5 in Section 6. As a guide we list the principal results here.

In the first, we use the abbreviation LCM to stand for least common multiple.

Theorem 1.3 *Let $Q\in\mathbb{N}$ be a prime power and let $F=\mathbb{F}_Q$ be a field with at least four elements. Set $d=\mathrm{LCM}(Q-1,2)+1$. Then, for any $n\in\mathbb{N}$, every matrix from the ring $\mathbb{M}_n(F)$ can be written as a sum of an idempotent matrix and an invertible d-potent matrix.*

The next theorem concerns the matrix ring over a *commutative* ring R.

Theorem 1.4 *Suppose $q>1$ is an odd integer and R is a commutative ring, not of characteristic 2, that does not possess a homomorphic image isomorphic to $\mathbb{F}_3$, and $q-1\in U(R)$. Then the following assertions are equivalent.*

(1) Every matrix in $\mathbb{M}_n(R)$ is a sum of an idempotent matrix and an invertible q-potent matrix.

(2) There exists a positive integer n such that each matrix in $\mathbb{M}_n(R)$ is a sum of an idempotent matrix and an invertible q-potent matrix.

(3) Every matrix in $\mathbb{M}_n(R)$ is a sum of an idempotent matrix and a q-potent matrix.

(4) There exists a positive integer n such that each matrix in $\mathbb{M}_n(R)$ is a sum of an idempotent matrix and a q-potent matrix.

(5) The ring R satisfies the identity $x^q=x$.

Further results are motivated by the notion of a torsion clean ring whose meaning we now summarize. A decomposition $r=e+u$ of an element r in a ring R will be called *n-torsion clean* decomposition of r if $e\in \mathrm{Id}(R)$ and $u\in U(R)$ is n-torsion, i.e. $u^n=1$. We shall say that such a decomposition of r is *strongly n-torsion clean* if, additionally, e and u commute (see, e.g., [9]). In the presence of such notation, we will say that the element r is *weakly n-torsion clean* decomposed if $r=u+e$ or $r=u-e$. If, in addition, $ue=eu$, the element r will be said to have a weakly n-torsion clean decomposition with the *strong property.*

Theorem 1.5 *Suppose that $q>1$ is an odd integer and R is an integral ring not isomorphic to $\mathbb{F}_3$ having characteristic different from 2. Then the following two conditions are equivalent.*

(1) For every (for some) $n\in\mathbb{N}$, the ring $\mathbb{M}_n(R)$ is $(q-1)$-torsion clean.

(2) R is a finite field and $|R|=q$.

Definition 1.6 *A ring R is said to be weakly n-torsion clean (with the strong property) if there is $n\in\mathbb{N}$ such that every element of R has a weakly n-torsion clean decomposition (with the strong property) and n is the minimal possible such natural number in these two equalities.*

Equipped with Definition 1.6, we can now add a further equivalent statement to those appearing in Theorem 1.5 provided $|R|>9$.

Theorem 1.7 *Let p be an odd prime, and $q=p^\alpha$ for some integer $\alpha\geq 0$. If R is an integral ring of characteristic not equal to 2 and $|R|>9$, then the following three conditions are equivalent.*

(1) For every (for some) $n\in\mathbb{N}$, the ring $\mathbb{M}_n(R)$ is $(q-1)$-torsion clean.

(2) For every (for some) $n\in\mathbb{N}$, the ring $\mathbb{M}_n(R)$ is weakly $(q-1)$-torsion clean.

(3) R is a finite field and $|R|=q$.

In this connection, simple calculations yield two somewhat surprising facts. First, $\mathbb{Z}_3$ is simultaneously weakly 1-torsion clean and 2-torsion clean. Secondly, $\mathbb{Z}_5$ is simultaneously weakly 2-torsion clean and 4-torsion clean. Some more detailed information about these properties of rings will be given in the sequel.

Finally, in the case when the ring R is commutative, it is convenient to introduce here the following additional notions. Let $g(x) = x^n - \sum_{i=0}^{n-1} a_i x^i \in R[x]$ be a monic polynomial of degree $n \geq 1$. The *companion matrix* of $g(x) := g$ is the $n \times n$ matrix of the kind:

$$C(g) = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix}.$$

The *trace* of $g(x)$ is then defined as the trace of $C(g)$, namely $\mathrm{tr}(g) = \mathrm{tr}(C(g)) = a_{n-1}$. Moreover, the *spectrum* of the square matrix A is denoted by $\mathrm{spec}(A)$ and the block-diagonal matrix with quadratic blocks $A_1, ..., A_k$ on diagonals is designed as $A_1 \oplus ... \oplus A_k$.

2. Sums of n-potents and tripotents in finite fields

In Sections 2–4, for the benefit the reader accustomed to the literature on finite fields, we shall generally use $\mathbb{F}_q$ to denote the typical finite field of cardinality a prime power q (rather than $\mathbb{F}_Q$ as in the Introduction).

For $n \in \mathbb{N}$ with $n-1$ a divisor of $q-1$, define C_n to be the set of n-potents of $\mathbb{F}_q$. A routine check shows that the idempotents are exactly $C_2 = \{0, 1\}$. If q is even (and so a power of 2), then the tripotents are $C_3 = C_2$. If q is odd (and so a power of an odd prime), then $C_3 = \{0, \pm 1\}$. Further, $C_q = \mathbb{F}_q$, i.e. every element is a q-potent. Also, when q is odd, $C_{(q+1)/2}$ is the set of elements of $\mathbb{F}_q$ that are squares in $\mathbb{F}_q$. However, it is the possibility that every element of $\mathbb{F}_q$ might be the sum of a $(q+1)/2$-potent and a tripotent that poses the greatest challenge. To this end, we shall determine the number of consecutive triples $\gamma - 1, \gamma, \gamma + 1$ of nonsquare elements of $\mathbb{F}_q$, thereby counting the number of $\gamma \in \mathbb{F}_q$ which can be central in such a triple.

With regard to statement (5) of Theorem 1.1, we shall identify all finite fields $\mathbb{F}_q$ with the property that every element is presentable as the sum of an n-potent element and a tripotent element of $\mathbb{F}_q$. Moreover, since the nonzero n-potent elements $\gamma \in \mathbb{F}_q$ are those for which $\gamma^{n-1} = 1$, which is the same as those for which $\gamma^{m-1} = 1$, where $m - 1 = \gcd(n-1, q-1)$, we can replace n by m or, more simply, assume $(n-1)|(q-1)$. Under this assumption then the cardinality of C_n is precisely n.

We now apply Theorem 1.2 to the question of whether all members of $\mathbb{F}_q$ can be sums of n-potents and tripotents.

Lemma 2.1 *Let q be a prime power and n an integer such that $1 < n \leq q$ and $(n-1)|(q-1)$. Then every element of $\mathbb{F}_q$ is a sum of an n-potent and a tripotent if and only if either $n = q$ or $q \in \{3, 5, 7, 9\}$ and $n = \frac{q+1}{2}$.*

Proof Evidently, we can assume $q > 2$ and $1 < n < q$.

First, we deal with the case when q is even, i.e. $q(\neq 2)$ is a power of 2. As we have noted, then here $C_3 = C_2 = \{0, 1\}$. Then the elements $0, 1$ are both in C_n and $C_n + 1$ and the condition that every member of $\mathbb{F}_q$ is a sum of an n-potent and a tripotent is equivalent to

$$C_n \cup (C_n + 1) = \mathbb{F}_q. \tag{2.1}$$

We can, therefore, suppose $q \geq 4$ and $n - 1 \leq \frac{q-1}{3}$ (since $q - 1$ is odd). Consequently, $C_n \cup (C_n + 1)$ has cardinality at most $2n - 2 \leq \frac{2q-2}{3} < q$, so that (2.1) cannot hold.

Now suppose q is odd. Then the set of tripotents $C_3 = \{0, 1, -1\}$. Obviously, for any n with $(n - 1)|(q - 1)$, we have $0, 1 \in C_n$ and so $-0 \in C_n \cap (C_n - 1)$ and $1 \in C_n \cap (C_n + 1)$ and the condition that every member of $\mathbb{F}_q$ is the sum of an n-potent and a tripotent is equivalent to

$$D := C_n \cup (C_n - 1) \cup (C_n + 1) = \mathbb{F}_q. \tag{2.2}$$

Now, if d is the cardinality of D, then $d \leq 3n - 2$. Hence, if $n - 1 \leq \frac{q-1}{3}$, i.e. $n \leq \frac{q+2}{3}$ and (2.2) holds, then

$$q \leq 3n - 2 \leq 3\left(\frac{q+2}{3}\right) - 2 = q,$$

where equality throughout implies that n is odd (since q is odd). But if n is odd, then also $-1 \in C_n \cap (C_n - 1)$ and actually $d \leq 3n - 3$ which implies that (2.2) cannot hold.

Hence, we can suppose $n - 1 = \frac{q-1}{2}$, and C_n is the set of squares (including 0) in $\mathbb{F}_q$. Now, by (2.2), it is *not* true that every element in $\mathbb{F}_q$ is the sum of an n-potent and a tripotent if and only if there exists a nonsquare $\gamma \in \mathbb{F}_q$ such that both $\gamma + 1$ and $\gamma - 1$ are also nonsquares, i.e. $q \leq 9$ by a crucial application of Theorem 1.2. □

We comment that originally we derived a proof of Lemma 2.1 in the case in which q is prime by means of [5, Theorem 2.3], with $\ell = 3$.

It is appropriate now to continue with the application of Lemma 2.1 to the full matrix ring $M_n(R)$. Recall that a nonzero ring is said to be *an integral ring* or, in other words, *an integral domain*, provided that it is commutative and also does not possess nontrivial zero divisors (i.e. the product of any two nonzero elements is again nonzero). Specifically, we have a surprising result. It is worth noting that, for convenience of Section 5, we frame it using notation that differs from the rest of this section in regard to the meaning of the symbols n and q.

Lemma 2.2 *Let $q > 1$ be an integer and let R be an integral ring. If, for some $n \in \mathbb{N}$, each matrix in $\mathbb{M}_n(R)$ is representable as a sum of a tripotent and a q-potent, then R is a finite field and*

(1) If $|R| \in \{3, 5, 7, 9\}$, then $\frac{(|R|-1)}{2} \,|\, (q - 1)$;

(2) if $|R| \notin \{3, 5, 7, 9\}$, then $(|R| - 1) \,|\, (q - 1)$.

Proof Suppose that for some $n \in \mathbb{N}$ every element from $\mathbb{M}_n(R)$ can be written as a sum of a tripotent and a q-potent. With a choice of $a \in R$, there exist $A, B \in \mathbb{M}_n(R)$ with the properties $aI_n = A + B$, $A^3 = A$ and

$B^q = B$. Denote by F the field of fractions of R. It is not too difficult to see that, for some invertible matrix $C \in \mathbb{M}_n(F)$, the matrix CAC^{-1} is upper triangular with elements on the main diagonal equal to either 0 or ± 1 only. It now easily follows from the equality $aI_n = CAC^{-1} + CBC^{-1}$ that either $a^q = a$ or $(a \pm 1)^q = (a \pm 1)$. In fact, the matrices aI_n and CAC^{-1} are upper triangular, hence the matrix CBC^{-1} is also upper triangular. Since $(CAC^{-1})^3 = CAC^{-1}$ and $(CBC^{-1})^q = CBC^{-1}$, similar equalities hold for the diagonal elements. In particular, the diagonal elements of the matrix CAC^{-1} are 0, ± 1. Thus, comparing the diagonal elements for an element a, one of the elements a, $a+1$, $a-1$ is a q-potent, as claimed. This means that R is a finite ring, and hence a finite field. Therefore, any element from R is the sum of a tripotent and a q-potent. We, finally, can employ to get our claim, as expected. □

3. Proof of Theorem 1.2

We proceed to the detailed argument which will evaluate N_q in every case and verify Theorem 1.2. Suppose throughout q is an odd prime and let λ be the quadratic character on $\mathbb{F}_q$. Thus, we have the following:

$$\sum_{\alpha} \lambda(\alpha) = \sum_{\alpha \neq 0} \lambda(\alpha) = 0, \tag{3.1}$$

where $\sum_{\alpha}$ stands for $\sum_{\alpha \in \mathbb{F}_q}$ and $\sum_{\alpha \neq 0}$ means that $\alpha = 0$ is excluded from the sum. We need further evaluations of character sums. The first can be found in [6, Theorem 2.1.2].

Lemma 3.1 *Suppose q is an odd prime power. Let $f(x) = x^2 + bx + c \in \mathbb{F}_q[x]$. Assume $b^2 - 4c \neq 0$. Then*

$$\sum_{\alpha \in \mathbb{F}_q} \lambda(f(\alpha)) = -1.$$

The next result concerns the Jacobsthal sum $J(a) = \sum_{\alpha} \lambda(x(x^2 + a)), a \in \mathbb{F}_q$. Recall that

$$\lambda(-1) = \begin{cases} 1, & \text{if } q \equiv 1 \pmod 4, \\ -1, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Hence, by replacing α by $-\alpha$ in the expression for $J(a)$, we see that if $q \equiv 3 \pmod 4$, then $J(a) = 0$. On the other hand, when $q \equiv 1 \pmod 4$, we use the following evaluation from [10, Theorem 2].

Lemma 3.2 (Katre and Rajwade, 1987) *Suppose $q = p^r \equiv 1 \pmod 4$, where p is an odd prime. If $p \equiv 3 \pmod 4$ (so that r is even), let $s = (-1)^{r/2}\sqrt{q}$. If $p \equiv 1 \pmod 4$, define s uniquely by $q = s^2 + t^2, p \nmid s, s \equiv 1 \pmod 4$. Then*

$$J(a) = \begin{cases} -2s, & \text{if } a \text{ is a fourth power in } \mathbb{F}_q, \\ 2s, & \text{if } a \text{ is a square but not a fourth power in } \mathbb{F}_q. \end{cases}$$

Now, let N_q be the number of consecutive triples of nonsquares $\gamma - 1, \gamma, \gamma + 1 \in \mathbb{F}_q$. Evidently, we have

$$N_q = \frac{1}{8} \sum_{\alpha \neq 0, \pm 1} (1 - \lambda(\alpha))(1 - \lambda(\alpha - 1))(1 - \lambda(\alpha + 1)). \tag{3.2}$$

Now, set

$$S_1 = \sum_{\alpha \neq 0,\pm 1} \lambda(\alpha); \quad S_2 = \sum_{\alpha \neq 0,\pm 1} \lambda(\alpha - 1); \quad S_3 = \sum_{\alpha \neq 0,\pm 1} \lambda(\alpha + 1)$$

and

$$T_1 = \sum_{\alpha \neq 0,\pm 1} \lambda(\alpha(\alpha - 1)); \; T_2 = \sum_{\alpha \neq 0,\pm 1} \lambda(\alpha(\alpha + 1)); \; T_3 = \sum_{\alpha \neq 0,\pm 1} \lambda(\alpha^2 - 1).$$

Then

$$N_q = \frac{1}{8}\left(q - 3 - \sum_{i=1}^{3} S_i + \sum_{i=1}^{3} T_i - J(-1)\right).$$

From (3.1),

$$S_1 = \sum_{\alpha} \lambda(\alpha) - 1 - \lambda(-1) = -1 - \lambda(-1); \; S_2 = -\lambda(-2) - \lambda(-1); \; S_3 = -1 - \lambda(2),$$

whereas, from Lemma 3.1,

$$T_1 = \sum_{\alpha \neq -1} \lambda(\alpha(\alpha - 1)) = -1 - \lambda(2); \; T_2 = -1 - \lambda(2); \; T_3 = -1 - \lambda(-1).$$

Further, $J(-1) = 0$ if $q \equiv 3 \pmod 4$. But, when $q \equiv 1 \pmod 4$, by Lemma 3.2, we have

$$J(-1) = \begin{cases} -2s, & \text{if } q \equiv 1 \pmod 8, \\ 2s, & \text{if } q \equiv 5 \pmod 8. \end{cases}$$

We also have the well-known facts that

$$\lambda(2) = \begin{cases} 1, & \text{if } q \equiv \pm 1 \pmod 8, \\ -1, & \text{if } q \equiv \pm 3 \pmod 8, \end{cases}$$

and

$$\lambda(-2) = \begin{cases} 1, & \text{if } q \equiv 1 \text{ or } 3 \pmod 8, \\ -1, & \text{if } q \equiv 5 \text{ or } 7 \pmod 8. \end{cases}$$

We now evaluate N_q from (3.2) and the various expressions for $S_i, T_i, J(-1)$. We require to consider five cases.

Case 1: *If* $q \equiv 7 \pmod 8$, *then* $N_q = \dfrac{q-7}{8}$.

Proof Here $\lambda(-1) = -1, \lambda(2) = 1, \lambda(-2) = -1$. Thus $S_1 = 0, S_2 = 2, S_3 = -2, T_1 = T_2 = -2, T_3 = 0$ while $J(-1) = 0$. Hence

$$8N_q = (q - 3 + 0 - 4) = q - 7.$$

□

Small examples of Case 1 include $N_7 = 0, N_{23} = 2$.

Case 2: *If* $q \equiv 3 \pmod 8$, *then* $N_q = \dfrac{q-3}{8}$.

Proof Now $\lambda(-1) = -1, \lambda(2) = -1, \lambda(-2) = 1$. Thus $S_1 = S_2 = S_3 = T_1 = T_2 = T_3 = 0$. Also, $J(-1) = 0$. □

Small examples of case 2 include $N_3 = 0, N_{11} = 1, N_{19} = 2$.

Case 3: If $q \equiv 5 \pmod 8$, then

$$N_q = \frac{q - 2s - 3}{8},$$

where $q = s^2 + t^2$, $s \equiv 1 \pmod 4$.

Proof Here $q = p^r$, where also $p \equiv 5 \pmod 8$ and r is odd. We have $\lambda(-1) = 1, \lambda(2) = \lambda(-2) = -1$. Hence, $S_1 = -2, S_2 = S_3 = 0, T_1 = T_2 = 0, T_3 = -2$.

Further, let γ be a primitive element in $\mathbb{F}_q$. Then $-1 = \gamma^{\frac{q-1}{2}}$ is the square of $\gamma^{\frac{q-1}{4}}$ but not a fourth power, since $\frac{q-1}{4}$ is odd. Hence $J(-1) = 2s$. □

In case 3, since $|s| < \sqrt{q}$, then $N_q > \frac{1}{8}(q - 2\sqrt{q} - 3)$.

Small examples of case 3 include $N_5 = 0$ (since $5 = 1^2 + 2^2$), $N_{13} = 2$ (since $13 = (-3)^2 + 2^2$), $N_{29} = 2$ (since $29 = 5^2 + 2^2$).

Case 4: *If* $q = p^r \equiv 1 \pmod 8$, *where* $p \equiv 1 \pmod 4$, *then*

$$N_q = \frac{q + 2s - 3}{8},$$

where $q = s^2 + t^2$, $s \equiv 1 \pmod 4$.

Proof Here $\lambda(-1) = \lambda(2) = \lambda(-2) = 1$. Hence, $S_1 = S_2 = S_3 = T_1 = T_2 = T_3 = -2$. This time $\frac{q-1}{4}$ is even and so -1 is a fourth power and $J(-1) = -2s$. □

Small examples of case 4 include $N_{17} = 2$ (since $17 = 1^2 + 4^2$), $N_{25} = 2$ (since $25 = (-3)^2 + 4^2$), $N_{169} = 22$ (since $169 = 5^2 + 12^2$), $N_{289} = 32$ (since $289 = (-15)^2 + 8^2$).

Case 5: *If* $q = p^r \equiv 1 \pmod 8$, *where* $p \equiv 3 \pmod 4$, *then* q *is a square and*

$$N_q = \frac{1}{8}\left(q + (-1)^{r/2}\sqrt{q} - 3\right).$$

Proof As in case 4, each S_i and T_i has the value -2. Again (-1) is a fourth power in $\mathbb{F}_q$ so that, by Lemma 3.2, $J(-1) = -2s = -2(-1)^{r/2}\sqrt{q}$. □

In case 5, when $r = 2m$ with m odd, then $N_q = \frac{1}{8}(q - 2\sqrt{q} - 3)$. As can be observed from the formulae in every other case $N_q > \frac{1}{8}(q - 2\sqrt{q} - 3)$. Thus, Theorem 1.2 follows as a corollary from cases 1–5.

Small examples of case 5 include $N_9 = 0, N_{49} = 4, N_{81} = 12$.

4. Sums of potents and tripotents in finite fields

Our original proof of Lemma 2.1 invoked a deep theorem from [7] on the existence of three consecutive primitive elements of a a finite field $\mathbb{F}_q$. Recall that a *primitive element* in $\mathbb{F}_q$ is a generator of the (cyclic) multiplicative group.

Theorem 4.1 ([7], Theorem 1) *Let q be an odd prime power. Then the finite field $\mathbb{F}_q$ contains three consecutive primitive elements $\gamma-1,\gamma,\gamma+1$ whenever $q>169$. Indeed, the only fields that do not contain three consecutive primitive elements are those for which $q\in\mathcal{S}=\{3,5,7,9,13,25,29,61,81,121,169\}$.*

Now, when q is odd, then a primitive element in $\mathbb{F}_q$ is a nonsquare so that Theorem 4.1 implies Lemma 2.1 (for $q>169$). But the proof of Theorem 4.1 is rather intricate both theoretically and computationally and it was desirable to provide a simpler wholly theoretical argument which Theorem 1.2 provides. On the other hand, Theorem 4.1 yields a further strong result on the existence of representations as a sum of potents and tripotents that we include here although it is not need for the remainder of the paper.

Therefore, let $q>2$ be a prime power. Call an element $a\in\mathbb{F}_q$ a *(proper) potent* if $a\in C_n$ for some n with $(n-1)|(q-1)$ and $n<q$ and define the set of all potents of $\mathbb{F}_q$ as the set

$$C=\bigcup_{\substack{n-1|q-1\\ n<q}} C_n. \tag{4.1}$$

For each n such that $(n-1)|(q-1)$, let c_n be the cardinality of C_n and c the cardinality of C. Then $c_n=n$, from which it is not too surprising that the condition of Lemma 2.1 is satisfied by so few pairs (q,n) with $n<q$. On the other side,

$$c=q-(q-1)\sum_{l|q-1}\left(1-\frac{1}{\ell}\right),$$

where the sum is over all distinct *primes* ℓ dividing $q-1$.

For example, if $2042024=1429^2$, then $c=1673621$ so that $c>0.8195q$ which means C is a large subset of $\mathbb{F}_q$. This makes it apparently more likely that all members of $\mathbb{F}_q$ could be sums of potents and tripotents. Nevertheless, Theorem 4.1 yields the following striking assertion.

Theorem 4.2 *Let $q>2$ be a prime power. Then every element of $\mathbb{F}_q$ is a sum of a potent (i.e. a member of C) and a tripotent if and only if $q\in\mathcal{S}$ as defined in Theorem 4.1.*

Proof First, suppose q is odd. Then $0,1\in C$ and $-1\in C-1$. Hence, the property that every member of $\mathbb{F}_q$ is the sum of a potent and a tripotent is equivalent to the assertion that

$$C\cup(C-1)\cup(C+1)=\mathbb{F}_q. \tag{4.2}$$

Suppose that $q\notin\mathcal{S}$ as displayed in Theorem 4.1. Then, there exists $\gamma\in\mathbb{F}_q$ such that each of $\gamma-1,\gamma,\gamma+1$ is a primitive element. Hence, γ is not in the left-side of (4.2) and, therefore, (4.2) does not hold.

On the other hand, if $q\in\mathcal{S}$, then by Theorem 4.1, for any $\gamma(\neq 0,\pm1)\in\mathbb{F}_q$, we have that $\gamma\in$ (at least one of) $C,C-1,C+1$ and so the relation (4.2) holds.

Finally, suppose $q>2$ is even. Then $0,1\in$ (both) C and $C+1$ and the fact that every element $\gamma\in\mathbb{F}_q$ is the sum of a potent and a tripotent (= idempotent) is equivalent to an assertion that $C\cup(C+1)=\mathbb{F}_q$. But this cannot hold since it was shown already in [8, Theorem 2.1] that $\mathbb{F}_q$ necessarily contains consecutive primitive elements, $\gamma,\gamma+1$. □

5. Decompositions of matrices into tripotents and potents

In this section we shall explore some special decompositions of matrices into a sum or a difference of a tripotent and a potent, thus augmenting some results from [3]. Now, Lemma 2.2 being established, we have all the ingredients towards the proof of Theorem 1.1.

Proof of Theorem 1.1. If the ring R is not isomorphic to $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, or $\mathbb{F}_9$, then the equivalence (1)–(7) follows from [2, Theorem 14] in combination with Lemma 2.2. If, however, $R \cong \mathbb{F}_7$, then, by virtue of Lemma 2.1 and the fact that q is odd, then any element from $\mathbb{F}_7$ is the sum of a tripotent and a q-potent. Hence, $(|\mathbb{F}_7|-1)\,|\,q-1$. Therefore, the equivalence of statements (1)–(7) in the case where $R \cong \mathbb{F}_7$ is immediate from [2, Theorem 14]. □

It was shown in [2, Theorem 19, Corollary 20] that, in the matrix ring $\mathbb{M}_{3k}(\mathbb{F}_3)$, there exists a matrix which cannot be presented as a sum of an idempotent and a tripotent. This example can be extended to the following one.

Proposition 5.1 *For every natural number k, in the ring $\mathbb{M}_{3k}(\mathbb{F}_3)$ there is a matrix that is not representable neither in the sum nor in the difference of a tripotent and an idempotent.*

Proof Put $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in M_3(\mathbb{F}_3)$. Then, a routine check shows that the matrix $B = \underbrace{A \oplus ... \oplus A}_{k}$ satisfies the desired condition. In fact, with reference to [2, Theorem 19], any matrix with a minimal polynomial $m(x) = x^3 - x \pm 1$ cannot be presented as a sum of an idempotent and a tripotent. If we assume for a moment that $B = f - e$, where $f^3 = f$ and $e^2 = e$, then it is plain that the matrix $(-B)$ is the sum of an idempotent and a tripotent. But the minimal polynomial of $(-B)$ is $x^3 - x + 1$, which contradicts the aforementioned theorem. □

It is also worth noting that by virtue of [2, Theorem 14], for every $n \in \mathbb{N}$ there is a matrix from $\mathbb{M}_n(\mathbb{F}_5)$ which is not presentable as a sum of an idempotent and a tripotent. We give an important explicit example in the case in which $n = 3$.

Example 5.2 *The matrix $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in \mathbb{M}_3(\mathbb{F}_5)$ is neither a sum nor a difference of a tripotent and an idempotent.*

Proof Put $m(x) = x^3 - x - 1$.

Assume that $A = f + \varepsilon e$ for some $e^2 = e$, $f^3 = f$ and $\varepsilon \in \{-1, 1\}$. It is straightforward that A, $A - 1$ and $A + 1$ are not tripotents. Thus, $e \neq 0, 1$. Therefore, there exists a unit $C \in \mathbb{M}_3(\mathbb{F}_5)$ such that $CeC^{-1} = I_k \oplus (0)_{n-k}$ for some $1 \leq k \leq 2$. Put $A' = CAC^{-1}$ and $f' = CfC^{-1} = \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix}$ with $F_{11} \in M_k(\mathbb{F}_5)$ and $F_{22} \in M_{n-k}(\mathbb{F}_5)$. We have

$$A' = f' + \varepsilon(I_k \oplus (0)_{n-k}) = \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix} + \varepsilon \begin{pmatrix} I_k & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} F_{11} + \varepsilon I_k & F_{12} \\ F_{21} & F_{22} \end{pmatrix}.$$

Put $(f')^3 = \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix}$. It is clear that $f_{ij} = \sum\limits_{a<b} F_{ia}F_{ab}F_{bj}$. Since $m(A') = 0$, we deduce

$$\begin{pmatrix} F_{11} + (1+\varepsilon)I_k & F_{12} \\ F_{21} & F_{22} + I_{n-k} \end{pmatrix} = 1 + A' = (A')^3 = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix}$$

for some g_{ij}. Taking into account that $(f')^3 = (f')$, we obtain the following equalities:

$$F_{11} + (1+\varepsilon)I_k = g_{11} = (F_{11} + \varepsilon I_k)^3 + (F_{11} + \varepsilon I_k)F_{12}F_{21} + F_{12}F_{21}(F_{11} + \varepsilon I_k) + F_{12}F_{22}F_{21} =$$

$$= \left(\sum_{a<b} F_{1a}F_{ab}F_{b1}\right) + 3F_{11} + \varepsilon(3F_{11}^2 + I_k + 2F_{12}F_{21}) = 4F_{11} + \varepsilon(3F_{11}^2 + I_k + 2F_{12}F_{21}),$$

$$F_{12} = g_{12} = (F_{11} + \varepsilon I_k)^2 F_{12} + (F_{11} + \varepsilon I_k)F_{12}F_{22} + F_{12}F_{21}F_{12} + F_{12}F_{22}F^2 =$$

$$= \left(\sum_{a<b} F_{1a}F_{ab}F_{b2}\right) + \varepsilon(2F_{11}F_{12} + \varepsilon F_{12} + F_{12}F_{22}) = F_{12} + \varepsilon((2F_{11} + \varepsilon I_k)F_{12} + F_{12}F_{22}),$$

$$F_{21} = g_{21} = F_{21}(F_{11} + \varepsilon I_k)^2 + F_{21}F_{12}F_{21} + F_{22}F_{21}(F_{11} + \varepsilon I_k) + F_{22}^2 F_{21} =$$

$$= \left(\sum_{a<b} F_{2a}F_{ab}F_{b1}\right) + \varepsilon(F_{21}(2F_{11} + \varepsilon I_k) + F_{22}F_{21}) = F_{21} + \varepsilon(F_{21}(2F_{11} + \varepsilon I_k) + F_{22}F_{21}),$$

$$F_{22} + I_{n-k} = g_{22} = F_{21}(F_{11} + \varepsilon I_k)F_{12} + F_{21}F_{12}F_{22} + F_{22}F_{21}F_{12} + F_{22}^3 =$$

$$= \left(\sum_{a<b} F_{2a}F_{ab}F_{b2}\right) + \varepsilon F_{21}F_{12} = F_{22} + \varepsilon F_{21}F_{12}.$$

This yields a system of equations of the form

$$\begin{cases} F_{11}^2 + \varepsilon F_{11} = 2\varepsilon I_k + F_{12}F_{21} \\ (2F_{11} + \varepsilon I_k)F_{12} = -F_{12}F_{22} \\ F_{21}(2F_{11} + \varepsilon I_k) = -F_{22}F_{21} \\ F_{21}F_{12} = \varepsilon I_{n-k}. \end{cases}$$

It follows that

$$F_{22}^2 = (-F_{22}F_{21})(-F_{12}F_{22}) = F_{21}(2F_{11} + \varepsilon I_k)^2 F_{12} = F_{21}\left(-(F_{11}^2 + \varepsilon F_{11}) + I_k\right)F_{12} =$$

$$= F_{21}((1-2\varepsilon)I_k - F_{12}F_{21})F_{12} = (1-2\varepsilon)F_{21}F_{12} - (F_{21}F_{12})^2 = -2\varepsilon I_{n-k}.$$

However, trivially neither 2 nor 3 is a square in $\mathbb{F}_5$. Thus, it must be that $n-k$ is even and so $k = 1$. Hence, in this case, the ranks of F_{21} and F_{12} do not exceed 1, whereas $F_{21}F_{12} = I_2$, a contradiction. □

6. Applications to (weakly, strongly) n-torsion clean rings

Here we apply the results from the previous section to variations of n-torsion cleanness. In particular, we shall incorporate the proofs of each of Theorems 1.4–1.7 at appropriate stages of the discussion.

To start with, however, we give some technical material.

Proposition 6.1 *If R is a commutative ring of even characteristic at most 4 (that is, 4 annihilates the identity element of R), then R is weakly 2^n-torsion clean if and only if R is 2^n-torsion clean.*

Proof One direction is elementary; therefore, we concentrate on the other. If $r = u+e$, the proof is complete; thus, let us assume that $r = u - e$. Thus, one easily checks that $r = (u - 2e) + e$, where $(u - 2e)^2 = u^2$ which gives that $(u - 2e)^{2^n} = u^{2^n}$ for all $n \in \mathbb{N}$, as required. □

Lemma 6.2 *Suppose that R is a ring and the element $a \in R$ possesses weakly n-torsion clean decomposition with the strong property. Then the equality $(a^n - 1)((a \pm 1)^n - 1) = 0$ holds.*

Proof Assuming first that $a = v + e$ is the desired weakly n-torsion clean decomposition of a satisfying $ve = ev$, we derive as in [9] that the equation $(a^n - 1)((a - 1)^n - 1) = 0$ is valid.

Therefore, assume now that $a = v - e$, where $v^n = 1$, $e^2 = e$ and $ve = ev$. Hence $ve = (a + 1)e$, so that $(ve)^n = ((a + 1)e)^n = (a + 1)^n e$. But $a^n - 1 = (a^n - 1)e$, that is, $(a^n - 1)(1 - e) = 0$ whence $(a+1)^n e = e = a^n e - a^n + 1$. By simple manipulations, we deduce in turn that $1 = (a+1)^n - a^n e + a^n$, whence $a^n - 1 = -(a+1)^n + a^n e$, whence $(a^n - 1)e = a^n e - (a+1)^n e$, whence $a^n - 1 = (a^n - (a+1)^n)e$. Consequently, $(a^n - 1)e = (a^n - (a + 1)^n)e$ and so $(a + 1)^n e - e = ((a + 1)^n - 1)e = 0$. Finally, $(a^n - 1)((a + 1)^n - 1) = (a^n - 1)e((a + 1)^n - 1) = (a^n - 1)((a + 1)^n - 1)e = 0$, as stated. □

Proposition 6.3 *Let F be a field not isomorphic to any of the fields $\mathbb{F}_3$, $\mathbb{F}_5$ or $\mathbb{F}_9$. Then F is weakly n-torsion clean if and only if F is finite and $n = |F| - 1$.*

Proof Let F be a weakly n-torsion clean field. Since F contains only the trivial idempotents 0 and 1, it is clear by Lemma 6.2 that F is finite. Moreover, every element of F is the sum of a $(n + 1)$-potent and a tripotent. By Lemma 2.1, either $(|F| - 1) \mid n$ or $|F| \in \{3, 5, 7, 9\}$. But it is easily be checked that each element of a finite field F has a weakly $(|F| - 1)$-torsion clean decomposition. Thus, it is enough to consider only the cases of $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, and $\mathbb{F}_9$.

Thus, a direct calculation justifies each of the following assertions.

(1) $\mathbb{F}_3$ is weakly 1-torsion clean.

(2) $\mathbb{F}_5$ is weakly 2-torsion clean.

(3) $\mathbb{F}_7$ is not a weakly 3-torsion clean, because $6 \in \mathbb{F}_7$ cannot be represented as the sum of elements from the sets $\{1, 2, 4\}$ and $\{-1, 0, 1\}$. Therefore, $\mathbb{F}_7$ is 6-torsion clean and the desired equality holds.

(4) Expressing $\mathbb{F}_9$ as $\mathbb{F}_3[x]/(x^2 + x + 2)$, we write ξ for the image of x. A direct inspection shows that the invertible 4-potents of $\mathbb{F}_9$ are 1, 2, $2\xi + 1$ and $\xi + 2$, whence it is clear that $\mathbb{F}_9$ is weakly 4-torsion clean.

Conversely, by analogous manipulations as above, it is obvious that every element of a finite field F has a weakly $(|F| - 1)$-torsion clean decomposition, as required. □

The following assertion is also useful. Its proof is a slight version of that from [9]; therefore, we omit the details leaving them to the interested reader.

Lemma 6.4 *Let $n \in \mathbb{N}$ and let R be a ring satisfying the identity $(x^n - 1)((x \pm 1)^n - 1) = 0$. Then the following two points hold.*

1. *R has finite nonzero characteristic;*
2. *$J(R)$ is a nil ideal.*

Now, we are in a position to establish the following theorem.

Theorem 6.5 *Let $n \in \mathbb{N}$. Suppose R is a weakly n-torsion clean ring having the strong property. Then the following assertions hold.*

1. *R is a PI-ring satisfying the polynomial identity $(x^n - 1)((x \pm 1)^n - 1) = 0$.*
2. *R has finite nonzero characteristic.*
3. *$J(R)$ is a nil ideal.*

Proof The claim follows at once by combination of Lemmas 6.2 and 6.4. □

We define, in general, a ring to be *weakly clean* if each its element can be written as either the sum or difference of a unit and an idempotent, and refer the interested reader to [4] for more details (mainly in the commutative case).

Subsuming the assertions alluded to above along with the methods developed in [9], we now arrive at our central statement.

Theorem 6.6 *For a ring R, the following two conditions are equivalent.*

1. *There exists $n \in \mathbb{N}$ such that R is a weakly n-torsion clean abelian ring.*
2. *The ring R is abelian weakly clean such that $U(R)$ is of finite exponent.*

By combining the ideas presented above, closely following [9], we derive the following consequence.

Corollary 6.7 *For a ring R, the following two points are equivalent.*

1. *R is weakly n-torsion clean with the strong property for some $n \in \mathbb{N}$.*
2. *R is weakly clean with the strong property and $U(R)$ is of finite exponent.*

Furthermore, taking into account Lemma 2.2 or Proposition 6.3, one sees that all (weakly) n-torsion clean fields have to be finite. In this direction, Theorem 14 in [2] gives a complete description of those finite fields whose matrices are a sum of an idempotent and a q-potent for some odd integer $q > 1$. in particular, if the field $\mathbb{F}_Q$ is not isomorphic to $\mathbb{F}_3$, then each finite matrix over $\mathbb{F}_Q$ is the sum of an idempotent and a q-potent. However, this is not true for fields of characteristic 2. To avoid this restriction on the number q to be odd, we will discuss the representations of matrices over $\mathbb{F}_Q$ of an idempotent and an $(\mathrm{LCM}(Q-1,2)+1)$-potent.

We proceed to the goal of the proof of Theorem 1.3 through a further series of lemmas.

Lemma 6.8 *Let $Q \geq 5$ be a prime power and let $p = p(x) \in \mathbb{F}_Q[x]$ be a unitary polynomial of degree $n \geq 1$. Put $d = \mathrm{LCM}(Q-1,2)+1$. Then the matrix $C(p) \in \mathbb{M}_n(\mathbb{F}_Q)$ is the sum of an idempotent matrix and an invertible d-potent matrix.*

Proof Fix an arbitrary primitive element ξ of the field $\mathbb{F}_Q$ such that $\xi \neq 1 - \xi$. In particular, if $Q = 5$, then we choose ξ to be equal to the element 3. Since $Q \geq 5$, there exists an element $k \in \mathbb{F}_q$ having the property $0 \notin k + \{-1, 0, 1, 2, -\xi, \xi - 1\}$. Since the matrix $C(p) - kI_n$ is obviously cyclic, then for some invertible matrix $V \in M_n(\mathbb{F}_Q)$ and a unitary polynomial $p_1 \in \mathbb{F}_Q[x]$ the following equality is fulfilled, namely:

$$C(p) - kI_n = VC(p_1)V^{-1}.$$

Assume now that $n \geq 2$ and that $\mathrm{tr}(p_1) \neq 1-k$. We distinguish three basic cases depending on $\mathrm{tr}(p_1)$.

Case 1: Assume $\mathrm{tr}(p_1) = 1$. In accordance with [2, Lemma 3] there is a decomposition $C(p_1) = e + f$, where $e^2 = e, f^3 = f = f^d$ and $\mathrm{spec}(f) \subseteq \{-1, 0, 1\}$. Obviously, the d-potent $f + kI_n$ inverts satisfying the equality

$$C(p) = C(p) - kI_n + kI_n = V(e+f)V^{-1} + kI_n = VeV^{-1} + V(f + kI_n)V^{-1}.$$

Case 2: Assume $\mathrm{tr}(p_1) = 0$. According to [2, Lemma 2] there is a decomposition $C(p_1) = e + f$, where $f^q = f = f^d, e^2 = e$ and $\mathrm{spec}(f) \subseteq \{-1, 0, -\xi, \xi - 1\}$. In particular, if $m = 2$, then the decomposition of the matrix $C(p_1)$ has the form

$$\begin{pmatrix} 0 & a_0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1-\xi & \xi(1-\xi) \\ 1 & \xi \end{pmatrix} + \begin{pmatrix} \xi - 1 & a_0 - \xi(1-\xi) \\ 0 & -\xi \end{pmatrix}.$$

Then the d-potent $f + kI_n$ inverts and also satisfies the equality $C(p) = VeV^{-1} + V(f + kI_n)V^{-1}$.

Case 3: Assume $\mathrm{tr}(p_1) \neq 0, 1$. In view of [2, Lemma 1], we can decompose $C(p_1) = e + f$, where $f^d = f$ and $\mathrm{spec}(f) \subseteq \{-1, 0, \mathrm{tr}(p_1) - 1\}$. In view of the choice of the element k, the d-potent element $f + kI_n$ is seen to be invertible and one may write that $C(p) = VeV^{-1} + V(f + kI_n)V^{-1}$.

We next assume for a moment that $\mathrm{tr}(p_1) = a_{n-1} = 1 - k$. It follows from the initial choice of the element k that $1 - k \notin \{-1, 0, 1\}$. Since the matrix $-C(p_1)$ is cyclic, for some invertible matrix $W \in \mathbb{M}_n(\mathbb{F}_q)$ and a unitary polynomial $p_2 \in \mathbb{F}_q[x]$ the following equality is true, namely,

$$-C(p_1) = WC(p_2)W^{-1}.$$

Moreover,

$$\mathrm{tr}(p_2) = \mathrm{tr}(-C(p_1)) = k - 1 \neq 0, 1.$$

Therefore, using [2, Lemma 1], we get that $C(p_2) = e + f$, where $\mathrm{spec}(f) \subseteq \{-1, 0, k-2\}$. Furthermore, one deduces that

$$C(p_1) + kI_n = -WC(p_2)W^{-1} + kI_n = W(-e-f)W^{-1} + kI_n$$

$$= W(I_n - e)W^{-1} + W(-f + (k-1)I_n)W^{-1}.$$

Also, the equality $(-f + (k-1)I_n)^q = (-1)^q f + (k-1)I_n$ holds. Consequently, the element $-f + (k-1)I_n$ must be a d-potent. However, because of the inclusion $\mathrm{spec}((-f + (k-1)I_n)) \subseteq \{k, k-1, 1\}$, one infers that $V(-f + (k-1))V^{-1}$ is an invertible d-potent.

Finally, it remains to treat the case when $n = 1$. To that goal, for the element $a \in \mathbb{F}_Q$, which differs from $-k$, the decomposition $a = e_a + f_a = 0 + a$ ensures the invertibility of the q-potent $(f_a + k)$. If, however, we have that $a = -k$, then we may write that $-k = e_{-k} + f_{-k} = 1 + (-k-1)$, as required. □

Note that Lemma 6.8 restricted our attention to fields containing at least five elements. On the other hand, in [9] it was conjectured that in the ring $\mathbb{M}_n(\mathbb{F}_2)$ each element is the sum of an idempotent and an invertible $(n+1)$-potent. It follows, however, from [2] and Proposition 5.1 above that the structure of the

matrices considered over $\mathbb{F}_3$ are also not completely described. Nevertheless, we can offer in the sequel some description of matrices over the field $\mathbb{F}_4$ consisting of four elements.

In the next statement the notation $\mathbb{M}_{n,p}(R)$ means the set of matrices of size $n \times p$ over a ring R.

Lemma 6.9 *Let R be a commutative ring, r and s polynomials over R, and $A \in \mathbb{M}_n(R)$, $B \in \mathbb{M}_{n,p}(R)$, $C \in \mathbb{M}_p(R)$ such that $r(A) = 0$ and $s(C) = 0$. Then the equality $(rs)(M) = 0$ holds for the upper triangular block-matrix*

$$M = \begin{pmatrix} A & B \\ [0] & C \end{pmatrix}.$$

Proof This follows straightforwardly from the equation $(rs)(M) = r(M)s(M)$, which we leave to be proved by the interested reader. □

Lemma 6.10 *Let $p \in \mathbb{F}_4[x]$ be a unitary polynomial of degree $n \geq 3$, where n is odd. Then the matrix $C(p) \in \mathbb{M}_n(\mathbb{F}_4)$ is a sum of an idempotent matrix and an invertible 7-potent matrix.*

Proof We have $\mathbb{F}_4 = \{0, 1, \xi, \xi + 1\}$, where $\xi^2 + \xi + 1 = 0$. Let $n = 2k + 1$ for some positive integer k. We shall consider three case associated with the value of $\mathrm{tr}(p)$.

Case 1: Assume $\mathrm{tr}(p) = 0$. Since the matrix $C(p) - \xi I_n$ is cyclic, for some invertible matrix $V \in \mathbb{M}_n(\mathbb{F}_4)$ and some unitary polynomial $p_1 \in \mathbb{F}_4[x]$ then the following equality is valid, namely,

$$C(p) - \xi I_n = VC(p_1)V^{-1},$$

where $\mathrm{tr}(p_1) = \xi$. We also define the idempotent $e = (1) \oplus A_1 \oplus A_2 \ldots \oplus A_k \in \mathbb{M}_n(\mathbb{F}_4)$, where $A_1 = A_2 = \cdots = A_k = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$. In this case, the matrix $C(p_1) - e$ is an upper triangular block: precisely, we have that $C(p_1) - e = \begin{pmatrix} H & T \\ 0 & 1 + \xi \end{pmatrix}$, where $H = B_1 \oplus B_2 \oplus \ldots \oplus B_k$ and $B_1 = B_2 = \cdots = B_k = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$.

Since the matrix H is annihilated by the polynomial $r(x) = x(x - 1)$, while the matrix $(1 + \xi)$ is annihilated by the polynomial $s(x) = x - (1 + \xi)$, Lemma 6.9 allows us to conclude that the matrix $C(p) - e$ under the product rs, so that it is a 4-potent. As in the proof of Lemma 6.8, we observe that $(C(p_1) - e) + \xi I_n$ is an invertible 4-potent, whence the matrix $C(p)$ is a sum of an idempotent and an invertible 7-potent.

Case 2: Assume $\mathrm{tr}(p) \in \{\xi, \xi + 1\}$. Since the matrix $C(p) - \mathrm{tr}(p)I_n$ is cyclic, for some invertible matrix $V \in \mathbb{M}_n(\mathbb{F}_4)$ and a unitary polynomial $p_1 \in \mathbb{F}_4[x]$ the following equality is valid, namely,

$$C(p) - \mathrm{tr}(p)I_n = VC(p_1)V^{-1},$$

where $\mathrm{tr}(p_1) = 0$. As in the preceding case 1, we define the idempotent $e \in \mathbb{M}_n(\mathbb{F}_4)$. Hence, the matrix $C(p_1) - e$ is an upper triangular block: specifically, we have that $C(p_1) - e = \begin{pmatrix} H & T \\ 0 & 1 \end{pmatrix}$, where $H = B_1 \oplus B_2 \oplus \ldots \oplus B_k$ and all matrices B_i are as in case 1 above.

We deduce consequently that

$$(C(p_1) - e) + \mathrm{tr}(p)I_n = \begin{pmatrix} H + \mathrm{tr}(p)I_{n-1} & T \\ 0 & 1 + \mathrm{tr}(p) \end{pmatrix}.$$

But the matrix $H+\mathrm{tr}(p)I_{n-1}$ is annihilated by the polynomial $r(x)=(x-\mathrm{tr}(p))(x-1-\mathrm{tr}(p))$, and the matrix $(1+\mathrm{tr}(p))$ by the polynomial $s(x)=x-1-\mathrm{tr}(p)$. Hence, an application of Lemma 6.9 guarantees that the matrix $(C(p_1)-e)+\mathrm{tr}(p)I_n$ vanishes under the product rs, and so additionally under the polynomial $x^7-x=x(x^3-1)^2$. Accordingly, $(C(p_1)-e)+\mathrm{tr}(p)I_n$ is an invertible 7-potent, whence the matrix $C(p)$ is a sum of an idempotent and an invertible 7-potent.

Case 3: Assume $\mathrm{tr}(p)=1$. Again, $C(p)-(1+\xi)I_n=VC(p_1)V^{-1}$ with $\mathrm{tr}(p_1)=\xi$. Similarly, one chooses $e=(1)\oplus A_1\oplus A_2\oplus\ldots\oplus A_k$ such that $A_1=A_2=\cdots=A_{k-1}=\begin{pmatrix}0&0\\1&1\end{pmatrix}$, $A_k=\begin{pmatrix}1&0\\1&0\end{pmatrix}$. In that case, the matrix $C(p_1)-e$ is an upper triangular block: concretely, we have that $C(p_1)-e=\begin{pmatrix}H&T\\0&\xi\end{pmatrix}$, where $H=B_1\oplus B_2\oplus\ldots\oplus B_k$ and $B_1=B_2=\cdots=B_{k-1}=\begin{pmatrix}1&0\\1&0\end{pmatrix}$, $B_k=\begin{pmatrix}1&0\\1&1\end{pmatrix}$.

Furthermore, one derives that

$$(C(p_1)-e)+(1+\xi)I_n=\begin{pmatrix}H+(1+\xi)I_{n-1}&T\\0&1\end{pmatrix}.$$

Since $H+(1+\xi)I_{n-1}$ is annihilated by the polynomial $r(x)=(x-1-\xi)(x-\xi)^2$, and the matrix (ξ) by the polynomial $s(x)=x-1$, applying Lemma 6.9 again yields the fact that the matrix $(C(p_1)-e)+(1+\xi)I_n$ vanishes under the product rs, and thus too under the polynomial $x^7-x=x(x^3-1)^2$. Now, the matrix $(C(p_1)-e)+(1+\xi)I_n$ must be an invertible 7-potent, whence the matrix $C(p)$ is a sum of an idempotent and an invertible 7-potent. □

Lemma 6.11 *Let $p\in\mathbb{F}_4[x]$ be a unitary polynomial of degree $n\geq 2$, wheren even. Then the matrix $C(p)\in\mathbb{M}_n(\mathbb{F}_4)$ is a sum of an idempotent matrix and an invertible 7-potent matrix.*

Proof Assume that $n=2k\geq 2$. Fix an arbitrary primitive element ξ of the field $\mathbb{F}_4$. We further define the element $d\in\mathbb{F}_4$ in the following manner: $d=1+\xi$ if $\mathrm{tr}(p)=1+\xi$, or $d=\xi$ otherwise. The choice of d guarantees that the elements d, $1+d$ and $1+\mathrm{tr}(p)+d$ are nonzero for each value of $\mathrm{tr}(p)$.

Since the matrix $C(p)-dI_n$ is cyclic, for some invertible matrix $V\in\mathbb{M}_n(\mathbb{F}_4)$ and unitary polynomial $p_1\in\mathbb{F}_4[x]$ the following equality is true, namely,

$$C(p)-dI_n=VC(p_1)V^{-1},$$

where $\mathrm{tr}(p_1)=\mathrm{tr}(p)$. Also, define the idempotent $e=A_1\oplus A_2\oplus\ldots\oplus A_k\in\mathbb{M}_n(\mathbb{F}_4)$, where $A_1=A_2=\cdots=A_k=\begin{pmatrix}0&0\\1&1\end{pmatrix}$. In that case, the matrix $C(p_1)-e$ is an upper triangular block: exactly, we have that $C(p_1)-e=\begin{pmatrix}H&T\\0&1+\mathrm{tr}(p)\end{pmatrix}$, where $H=(0)\oplus B_1\oplus B_2\oplus\ldots\oplus B_k$ and $B_1=B_2=\cdots=B_k=\begin{pmatrix}1&0\\1&0\end{pmatrix}$.

We thus obtain that

$$(C(p_1)-e)+dI_n=\begin{pmatrix}H+dI_{n-1}&T\\0&1+\mathrm{tr}(p)+d\end{pmatrix}.$$

Because the matrix $H+dI_{n-1}$ is annihilated by the polynomial $r(x)=(x-d)(x-1-d)$ and the matrix $(1+\mathrm{tr}(p)+d)$ by the polynomial $s(x)=x-(1+\mathrm{tr}(p)+d)$, one may conclude from Lemma 6.9 that the

matrix $(C(p_1)-e)+dI_n$ vanishes under the product rs, and hence under the polynomial $x^7-x=x(x^3-1)^2$. Therefore, $(C(p_1)-e)+dI_n$ has to be an invertible 7-potent, whence $C(p)$ must be a sum of an idempotent and an invertible 7-potent. □

Now, at last we are ready for the proof of Theorem 1.3.

Proof of Theorem 1.3. Given $A\in\mathbb{M}_n(\mathbb{F}_q)$ with $q\geq 4$. One checks that the matrix A is similar to a matrix of the type $A_1\oplus A_2\oplus\ldots\oplus A_k$, where A_i is a Frobenius block for each $1\leq i\leq k$. If $q\geq 5$, then Lemma 6.8 tells us that the matrix A is a sum of an idempotent matrix and an invertible d-potent matrix. But if $q=4$, then $d=7$ and so we may apply Lemmas 6.10 and 6.11 to get the desired conclusion. □

Furthermore, we observe that Theorem 1.3 yields a valuable corollary.

Corollary 6.12 *Suppose $q>1$ is an odd integer and R is an integral ring not isomorphic to any of the fields $\mathbb{F}_2$ or $\mathbb{F}_3$. Then the following three conditions are equivalent.*

(1) For every (for some) $n\in\mathbb{N}$, each matrix in the matrix ring $\mathbb{M}_n(R)$ can be expressed as a sum of an idempotent matrix and an invertible q-potent matrix.

(2) For every (for some) $n\in\mathbb{N}$, each matrix in the matrix ring $\mathbb{M}_n(R)$ can be expressed as a sum of an idempotent matrix and a q-potent matrix.

(3) R is a finite field and $(|R|-1)\mid q-1$.

In addition, if $2\in U(R)$ and R is not isomorphic to $\mathbb{F}_3$, $\mathbb{F}_5$ or $\mathbb{F}_9$, then each of the conditions $(1)-(3)$ is also equivalent to the further condition that follows.

(4) For every (for some) $n\in\mathbb{N}$, each matrix in the matrix ring $\mathbb{M}_n(R)$ can be expressed as a sum of an involution and an invertible q-potent matrix.

Proof The equivalence of statements (2) and (3) is immediately from [2, Theorem 14]. Further, the implication $(1)\Rightarrow(2)$ is clear, and the implication $(3)\Rightarrow(1)$ follows at once from Theorem 1.3.

$(3)\Rightarrow(4)$. Let $x\in\mathbb{M}_n(R)$. Then, since $(3)\Rightarrow(1)$, one writes that $(x+1)/2=e+u$, where u is an invertible q-potent matrix and $e^2=e$. Therefore, $x=2u+(2e-1)$, where $2u=(2u)^q$ is an invertible element, and $(2e-1)^2=1$, as required.

$(4)\Rightarrow(3)$. It follows directly from Theorem 1.1. □

Specializing R to be a commutative ring, we obtain a proof of Theorem 1.4.

Proof of Theorem 1.4. The implications $(1)\Rightarrow(2)$, $(2)\Rightarrow(4)$ and $(3)\Rightarrow(4)$ are obvious.

$(4)\Rightarrow(5)$. Take n such that every matrix in $\mathbb{M}_n(R)$ is a sum of an idempotent matrix and a q-potent matrix. From condition (3) of Corollary 6.12, for every prime ideal I of the ring R, the quotient ring R/I is a field satisfying the identity $x^q=x$. So, $J(R)=Nil(R)$ is true and thus R is semiregular by [12, Lemma 16.6].

Consider now a maximal indecomposable factor $S=R/I$ of the ring R. By using [12, Remark 29.7(2)], [12, Proposition 32.2] and Corollary 6.12, the factor-ring S is a local ring, the quotient $S/J(S)$ is a field of characteristic p in which the identity $x^q=x$ holds, and $J(S)$ is a nil ideal. We next wish to prove that $J(S)=0$. To achieve the claim, we assume on the contrary that $J(S)\neq 0$. However, if $pS\neq J(S)$, then

$J(S/pS) \neq 0$ and so there exists nonzero $a \in J(S/pS)$ with identity $a^2 = 0$. By hypothesis, we write that

$$aI_n = E_1 + E_2, E_1^2 = E_1, E_2^q = E_2,$$

for some $E_1, E_2 \in \mathbb{M}_n(S/pS)$. Since it is well known that every idempotent matrix is diagonalizable over a local commutative ring, it can be assumed without loss of generality that the matrices E_1, E_2 are of diagonal form. Indeed, since $a \neq 0$, it must be that $E_1 \neq 0$. Therefore, for some element b on the main diagonal of the matrices E_2, the equalities $a = 1 + b, b^{q-1} = 1$ hold. Then,

$$0 = a^p = (1 + b)^p = 1 + b^p,$$

and thus $b^p = -1$. Since by condition $(q - 1, p) = 1$, the equality $1 = t_1(q - 1) + t_2 p$ holds for some integers t_1 and t_2. But since t_2 is odd, we then have $b = (b^{(q-1)})^{t_1}(b^p)^{t_2} = -1$ which yields $a = 0$, that is the desired contradiction.

If now $pS = J(S)$, then $J(S) \neq 0$ implies $pS \neq p^2S$. We put $a = p + p^2S \in S/p^2S$. By hypothesis, there exists $E_1, E_2 \in \mathbb{M}_n(S/p^2S)$ such that

$$aI_n = E_1 + E_2, E_1^2 = E_1, E_2^q = E_2.$$

From $a^2 = 0$, we readily see that

$$aI_n - E_2 = E_1 = E_1^q = -E_2^q + qaI_nE_2^{q-1} = -E_2 + qaI_nE_2^{q-1}.$$

Then, $aI_n = qaI_nE_2^{q-1}$. It once again can be assumed without loss of generality that the matrices E_1, E_2 are of diagonal form. Therefore, for some element b on the main diagonal of the matrices E_2, the equality $a = aqb^{q-1}$ holds. Since $b^q = b$, we obtain $(q-1)ab = 0$ and since $(q-1) \in U(S/p^2S)$, we arrive at $ab = 0$. Consequently, $a = aqb^{q-1} = 0$, which is a new contradiction. Thus, finally, $J(S) = 0$, which substantiates our claim.

Furthermore, by virtue of the above reasoning, all Pierce stalks of R are isomorphic to the finite fields $\mathbb{F}_t$ with $t - 1 \mid q - 1$. Invoking [12, Corollary 11.10], the ring R has identity $x^q = x$.

(5) $\Rightarrow$ (1), (5) $\Rightarrow$ (3). Let n be an arbitrary natural number and take $A \in \mathbb{M}_n(R)$. Consider the subring S of the ring R, generated by the elements of the matrix A. One straightforwardly verifies that the ring S is finite. Hence, one decomposes $S \cong P_1 \times \ldots \times P_m$, for some finite fields P_i with identities $x^q = x$ and for any $1 \leq i \leq m$. Now, with Corollary 6.12 at hand, every P_i satisfy the conditions of points (1) and (3), whence so does S. □

We observe that Theorem 1.4 requires the condition $q - 1 \in U(R)$, which is vital to obtaining this result. As a matter of fact, let us take an odd prime p and consider the ring $\mathbb{Z}/p^2\mathbb{Z}$. Therefore, we come to the following assertion.

Lemma 6.13 *Suppose that p is an odd prime and $q \in \mathbb{N}$. Then the following two conditions are equivalent:*

(1) Every element of $\mathbb{Z}/p^2\mathbb{Z}$ is a sum of an idempotent and a q-potent.

(2) $p(p-1) \mid q - 1$.

Proof (1) $\Rightarrow$ (2). Suppose that every element of $\mathbb{Z}/p^2\mathbb{Z}$ is a sum of an idempotent and a q-potent. Since $U(\mathbb{Z}/p^2\mathbb{Z})$ is a cyclic group of order $p(p-1)$, there exists $q' \in \mathbb{N}$ such that $q' - 1 \mid p(p-1)$ and the set of

q-potents of $\mathbb{Z}/p^2\mathbb{Z}$ coincides with the set of q'-potents. If $q'-1=p(p-1)$, then $p(p-1)\mid q-1$, as required. Otherwise, the inequality $q'-1\leq \frac{p(p-1)}{2}$ holds, and cardinality of the set of elements that are a sum of an idempotent and a q'-potent is not greater than the number $2(1+\frac{p(p-1)}{2})<p^2$.

(2) $\Rightarrow$ (1). It is clear that every element of $\mathbb{Z}/p^2\mathbb{Z}$ is either a $(p(p-1)+1)$-potent or a sum of 1 and a $(p(p-1)+1)$-potent, as required. □

The next example will substantiate the above observations.

Example 6.14 *Suppose that p is an odd prime and $q\in\mathbb{N}$. Then the following two conditions are equivalent.*

(1) Every element of $\mathbb{M}_2(\mathbb{Z}/p^2\mathbb{Z})$ is a sum of an idempotent matrix and a q-potent matrix.

(2) $p(p-1)\mid q-1$.

Proof (1) $\Rightarrow$ (2). Take $a\in\mathbb{Z}/p^2\mathbb{Z}$. Then, there exist matrices $E_1,E_2\in\mathbb{M}_2(\mathbb{Z}/p^2\mathbb{Z})$, such that $aI_2=E_1+E_2$, $E_1^2=E_1$, $E_2^q=E_2$. Since it is well known that every idempotent matrix is diagonalizable over a local commutative ring, it can be assumed without loss of generality that the matrices E_1,E_2 are of diagonal form. We, therefore, can conclude with the aid of Lemma 6.13 that every element of $\mathbb{Z}/p^2\mathbb{Z}$ is a sum of an idempotent and a q-potent, and $p(p-1)\mid q-1$.

(2) $\Rightarrow$ (1). Take $A\in\mathbb{M}_2(\mathbb{Z}/p^2\mathbb{Z})$ and let $\pi:\mathbb{M}_2(\mathbb{Z}/p^2\mathbb{Z})\to\mathbb{M}_2(\mathbb{Z}/p\mathbb{Z})$ denote the reduction map. The matrix $\pi(A)$ is similar to its rational canonical form. Then the standard theory of determinants will imply that every invertible matrix in $\mathbb{M}_2(\mathbb{Z}/p\mathbb{Z})$ can be lifted upon π. Therefore, without loss of generality, we may assume that A is presentable in one of the two following forms: $\begin{pmatrix}a&0\\0&b\end{pmatrix}+j$ or $\begin{pmatrix}0&a\\1&b\end{pmatrix}+j$, where $a,b\in\mathbb{Z}/p^2\mathbb{Z}$ and $j\in J(\mathbb{M}_2(\mathbb{Z}/p^2\mathbb{Z}))$. We now distinguish three cases as follows.

Case 1: Suppose that $A=\begin{pmatrix}0&a\\1&b\end{pmatrix}$.

If $b\not\equiv 1 \mod p^2$, then

$$\begin{pmatrix}0&a\\1&b\end{pmatrix}=\begin{pmatrix}0&0\\1&1\end{pmatrix}+\begin{pmatrix}0&a\\0&b-1\end{pmatrix}.$$

Since $b-1\in U(\mathbb{Z}/p^2\mathbb{Z})$, we have $(b-1)^{p(p-1)}=1$ and b is annihilated by the polynomial $x^{p(p-1)}-1$. In view of Lemma 6.9, the matrix $\begin{pmatrix}0&a\\0&b-1\end{pmatrix}$ is annihilated by $x(x^{p(p-1)}-1)$, i.e. it is a $(p(p-1)+1)$-potent.

If $b\equiv 1 \mod p^2$, then

$$\begin{pmatrix}0&a\\1&b\end{pmatrix}=\begin{pmatrix}1&0\\1&0\end{pmatrix}+\begin{pmatrix}-1&a\\0&b\end{pmatrix}.$$

Since $x^{p(p-1)}-1=(x+1)g(x)$ for some polynomial $g(x)$ over $\mathbb{Z}$ and $b+1$ is invertible in $\mathbb{Z}/p^2\mathbb{Z}$, we conclude that b is annihilated by $g(x)$. In virtue of Lemma 6.9, the matrix $\begin{pmatrix}-1&a\\0&b\end{pmatrix}$ is annihilated by $(x+1)g(x)$, i.e. it is a $(p(p-1)+1)$-potent.

Case 2: Suppose that $A=\begin{pmatrix} pk & a \\ 1+pm & b \end{pmatrix}$. Take $u=(1+pm)^{-1}$. We have

$$\begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}\begin{pmatrix} pk & a \\ 1+pm & b \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & u^{-1} \end{pmatrix}=\begin{pmatrix} pk & au^{-1} \\ 1 & b \end{pmatrix}.$$

Next,

$$\begin{pmatrix} 1 & -pk \\ 0 & 1 \end{pmatrix}\begin{pmatrix} pk & au^{-1} \\ 1 & b \end{pmatrix}\begin{pmatrix} 1 & pk \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 0 & au^{-1}-bpk \\ 1 & b+pk \end{pmatrix}.$$

Thus, case 2 is reduced to case 1.

Case 3: Suppose that $A=\begin{pmatrix} a & pk \\ pm & b \end{pmatrix}$.

If a and b are both units, then

$$\begin{pmatrix} a & pk \\ pm & b \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}+\begin{pmatrix} a & pk \\ pm & b \end{pmatrix}.$$

It is enough to show that $\begin{pmatrix} a & pk \\ pm & b \end{pmatrix}^{p(p-1)}=I_2$.

If $a=b$, then

$$\begin{pmatrix} a & pk \\ pm & a \end{pmatrix}^{p(p-1)}=\left(aI_2+\begin{pmatrix} 0 & pk \\ pm & 0 \end{pmatrix}\right)^{p(p-1)}=a^{p(p-1)}I_2+\frac{p(p-1)}{2}a^{p(p-1)-1}\begin{pmatrix} 0 & pk \\ pm & 0 \end{pmatrix}=I_2,$$

because $2\mid(p-1)$.

If $a\neq b$ and $a-b\in U(\mathbb{Z}/p^2\mathbb{Z})$, then simple induction shows that

$$\begin{pmatrix} a & pk \\ pm & b \end{pmatrix}^{r}=\begin{pmatrix} a^r & pk\sum\limits_{i=0}^{r-1}a^ib^{r-i} \\ pm\sum\limits_{i=0}^{r-1}a^ib^{r-i} & b^r \end{pmatrix}=\begin{pmatrix} a^r & pk\frac{a^r-b^r}{a-b} \\ pm\frac{a^r-b^r}{a-b} & b^r \end{pmatrix}.$$

Since a and b are units, we have $\begin{pmatrix} a & pk \\ pm & b \end{pmatrix}^{p(p-1)}=I_2$.

If $a-b\in p\mathbb{Z}/p^2\mathbb{Z}$ and $a-b\neq 0$, then

$$0=a^{p(p-1)}-b^{p(p-1)}=(a-b)(\sum_{i=0}^{p(p-1)-1}a^ib^{p(p-1)-1-i}).$$

Thus $\sum_{i=0}^{p(p-1)-1}a^ib^{p(p-1)-1-i}\in pZ/p^2Z$ and

$$\begin{pmatrix} a & pk \\ pm & b \end{pmatrix}^{p(p-1)}=\begin{pmatrix} a^{p(p-1)} & pk\sum\limits_{i=0}^{p(p-1)-1}a^ib^{p(p-1)-1-i} \\ pm\sum\limits_{i=0}^{p(p-1)-1}a^ib^{p(p-1)-1-i} & b^{p(p-1)} \end{pmatrix}=I_2.$$

If, however, a and b are both not units, then

$$\begin{pmatrix} a & pk \\ pm & b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} a-1 & pk \\ pm & b-1 \end{pmatrix}$$

and $\begin{pmatrix} a-1 & pk \\ pm & b-1 \end{pmatrix}$ is a $(p(p-1)+1)$-potent, as we saw earlier.

Finally, if b and $a-1$ are units, then

$$\begin{pmatrix} a & pk \\ pm & b \end{pmatrix} = \begin{pmatrix} 1 & pk \\ pm & 0 \end{pmatrix} + \begin{pmatrix} a-1 & 0 \\ 0 & b \end{pmatrix}$$

is a sum of idempotent and a $(p(p-1)+1)$-potent. We thus have obtained a similar decomposition if a and $b-1$ are units, as expected. □

We now provide two final lemmas.

Lemma 6.15 *Let $q>1$ be an integer, $\mathbb{F}_q$ a finite field and $n \in \mathbb{N}$. Then the following two statements are equivalent.*

(1) Every element of $\mathbb{F}_q$ admits an n-torsion clean presentation.

(2) $(q-1) \mid n$.

Proof (1) $\Rightarrow$ (2). In view of Lemma 2.1 it is necessary to consider only the fields $\mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_9$. Assume by way of contradiction that each element of these fields is n-torsion clean, but n is not divisible by $(q-1)$. To obtain the desired contradiction, we first observe the obvious fact that the set of $(n+1)$-potents in the field $\mathbb{F}_q$ coincides with the set of $(1+\mathrm{GCD}(n, q-1))$-potents. But $\frac{(q-1)}{2} \mid n$ in virtue of Lemma 2.1, whence $\mathrm{GCD}(n, q-1) = \frac{(q-1)}{2}$ and so in the field every element is a sum of an idempotent and of an invertible $\left(\frac{q+1}{2}\right)$-potent. Since the number of $\left(\frac{q+1}{2}\right)$-potents is exactly $\frac{(q-1)}{2}$, it follows that the number of n-torsion clean elements does not exceed $q-1$, which is impossible, as desired.

(2) $\Rightarrow$ (1). It is straightforward. □

Lemma 6.16 *Let $q>1$ be an integer and let R be an integral ring. If, for some $n \in \mathbb{N}$, each matrix from the ring $\mathbb{M}_n(R)$ is n-torsion clean, then R is a finite field and $(|R|-1) \mid n$.*

Proof By Lemma 2.2, the ring R is necessarily a finite field. Moreover, all elements of R admit an n-torsion clean presentation. But now Lemma 6.15 assures that $(|R|-1) \mid n$, as promised. □

At this point the proof of Theorem 1.5 is obtained by combining Corollary 6.12 with Lemma 6.15. Indeed, we can extract further corollaries of Theorem 1.3 and Corollary 6.12 as follows.

Corollary 6.17 *Suppose $k, n > 1$ are positive integers Then the ring $\mathbb{M}_n(\mathbb{F}_{2^k})$ is d-torsion clean, where $d \in \{2^k-1, 2^{k+1}-2\}$.*

Proof It follows from Lemma 6.16 that $2^k - 1 \mid d$. But Theorem 1.3 enables us to deduce that $d \leq 2^{k+1} - 2$, as requested. □

Corollary 6.18 *Let p be an odd prime, and $q = p^\alpha$ for some integer $\alpha \geq 0$. If R is an integral ring of odd characteristic and $|R| > 9$, then the following four conditions are equivalent.*

(1) For every (for some) $n \in \mathbb{N}$, each matrix in the matrix ring $\mathbb{M}_n(R)$ can be expressed as a sum of an idempotent matrix and an invertible q-potent matrix.

(2) For every (for some) $n \in \mathbb{N}$, each matrix in the matrix ring $\mathbb{M}_n(R)$ can be expressed as a sum or a difference of an invertible q-potent matrix and an idempotent matrix.

(3) For every (for some) $n \in \mathbb{N}$, each matrix in the matrix ring $\mathbb{M}_n(R)$ can be expressed as a sum of a tripotent matrix and a q-potent matrix.

(4) R is a finite field with $(|R| - 1) \mid q - 1$.

Proof It follows from Lemma 2.2 and Corollary 6.12. □

As a consequence, this statement yields the characterization Theorem 1.7, which is our principal result.

It was also asked in [9] whether the equality $n = \exp(U(R))$ holds if the ring R strongly n-torsion clean. We shall partially address this query by using the following helpful assertion.

Theorem 6.19 ([1], Theorem 6) *Let F be a finite field of characteristic p, $n, q \in \mathbb{N}$, and $q > 1$ is odd. The following statements are equivalent.*

(1) Every matrix $A \in \mathbb{M}_n(F)$ is a sum of a q-potent and an idempotent that commute.

(2) The number $N = LCM(|F| - 1, |F|^2 - 1, ..., |F|^n - 1)p^t$ is a divisor of $q - 1$, where p^t is the least nonnegative integer power of p that is greater or equal to m.

Actually, in the proof of the implication (2) $\Rightarrow$ (1) was obtained a stronger result like this: *every matrix $A \in \mathbb{M}_n(F)$ is a sum of an invertible q-potent and an idempotent that commute.* In particular, one can be seen that the number $LCM(|F| - 1, |F|^2 - 1, ..., |F|^m - 1)p^t$ is equal exactly to $\exp(U(\mathbb{M}_n(F)))$.

We, thereby, can extract the following important consequence that is our final result.

Corollary 6.20 *Let F be a finite field of odd characteristic and $n \in \mathbb{N}$. Then the ring $\mathbb{M}_n(F)$ is strongly $\exp(U(\mathbb{M}_n(F)))$-torsion clean.*

Acknowledgments

The authors are deeply grateful to two anonymous referees who refereed this submission. Their professional suggestions have been very helpful in improving the presentation and have stimulated us to pursue further research on the subject.

The work of the third-named author P. V. Danchev was supported in part by the Junta de Andalucía, FQM 264.

The research of A. N. Abyzov and D. T. Tapkin was supported by Russian Science Foundation and the Cabinet of Ministers of the Republic of Tatarstan within the framework of scientic project no. 23-21-10086 and was performed under the development programme of the Volga Region Mathematical Center (agreement no. 075-2-2024-1438).

References

[1] Abyzov AN, Tapkin DT. On rings with $x^n - x$ nilpotent. Journal of Algebra and Its Applications 2022; 21 (6): 2250111. https://doi.org/10.1142/S0219498822501110

[2] Abyzov AN, Tapkin DT. Rings over which every matrices are sums of idempotent and q-potent matrices. Siberian Mathematical Journal 2021; 62 (1): 1-13. https://doi.org/10.1134/S0037446621010018

[3] Abyzov AN, Tapkin DT. When is every matrix over a ring the sum of two tripotents? Linear Algebra and Its Applications 2021; 630: 316-325. https://doi.org/10.1016/j.laa.2021.09.007

[4] Ahn MS, Anderson DD. Weakly clean rings and almost clean rings. Rocky Mountain Journal of Mathematics 2006; 36 (3): 783-798. https://doi.org/10.1216/rmjm/1181069429

[5] Buell DA, Hudson RH. On runs of consecutive quadratic residues and quadratic nonresidues. BIT Numerical Mathematics 1984; 24 (2): 243-247. https://doi.org/10.1007/BF01937490

[6] Berndt BC, Evans RJ, Williams KS. Gauss and Jacobi Sums. Canadian Mathematical Society Series of Monographs and Advanced Texts. NY, USA: John Wiley & Sons., Inc., 1998.

[7] Cohen SD, Oliveira e Silva T, Trudgian T. On consecutive primitive elements in a finite field. Bulletin of the London Mathematical Society 2015; 47 (3): 418-426. https://doi.org/10.1112/blms/bdv018

[8] Cohen SD. Consecutive primitive roots in a finite field. Proceedings of the American Mathematical Society 1985; 93 (2): 189-197. https://doi.org/10.2307/2044741

[9] Danchev PV, Matczuk J. n-torsion clean rings. In: Leroy A, Lomp C, López-Permouth S, Oggier F (editors). Rings, Modules and Codes. Contemporary Mathematics, volume 727. Providence, RI, USA: American Mathematical Society, 2019, pp. 71-82. https://doi.org/10.1090/conm/727/14625

[10] Katre SA, Rajwade AR. Resolution of the sign ambiguity in the determination of the cyclotomomic numbers of order 4 and the corresponding Jacobsthal sum. Mathematica Scandinavica 1987; 60: 52-62. https://doi.org/10.7146/math.scand.a-12171

[11] Lam TY. A First Course in Noncommutative Rings (2nd edition). Graduate Texts in Mathematics, volume 131. NY, USA: Springer-Verlag, 2001. https://doi.org/10.1007/978-1-4419-8616-0

[12] Tuganbaev AA. Rings Close to Regular. Mathematics and Its Applications, volume 545. Dordrecht, the Netherlands: Kluwer Academic Publishers, 2002. https://doi.org/10.1007/978-94-015-9878-1