MATRICES OVER COMMUTATIVE RINGS AS SUMS OF $k$-TH POWERS

S. A. KATRE AND ANURADHA S. GARGE

(Communicated by Birge Huisgen-Zimmermann)

Abstract. In this paper, for $n, k \geq 2$, and $R$ a commutative and associative ring with unity, we give necessary and sufficient trace conditions for an $n \times n$ matrix over $R$ to be a sum of $k$-th powers of matrices over $R$. We also prove that for $n \geq m \geq 1$, if every $m \times m$ matrix over $R$ is a sum of $k$-th powers of matrices over $R$, then so is every $n \times n$ matrix. As concrete examples, we prove a discriminant criterion for every $n \times n$ matrix over an order $R$ in an algebraic number field to be a sum of cubes and fourth powers of matrices over $R$. We also show that if $q$ is a prime and $n \geq 2$, then every $n \times n$ matrix over the ring $\mathcal{O}$ of integers of a quadratic number field $K$ is a sum of $q$-th powers of matrices over $\mathcal{O}$ if and only if $q$ is coprime to the discriminant of $K$.

1. Introduction and statements of results

For us a ring $R$ will always mean a commutative and associative ring with unity and for $n \geq 1$, $M_n(R)$ the set of $n \times n$ matrices over $R$. The following questions arise in the context of Waring’s problem for matrices over rings:

1. Given a matrix $M \in M_n(R)$, can $M$ be written as a sum of $k$-th powers in $M_n(R)$?
2. Given a ring $R$ and a positive integer $n$, can every $M \in M_n(R)$ be written as a sum of $k$-th powers in $M_n(R)$?
3. Find the least positive integer $g(n,k,R,M)$ such that a given matrix $M \in M_n(R)$ can be written as a sum of $k$-th powers in $M_n(R)$.
4. Find the least positive integer $g(n,k,R)$ such that every $M \in M_n(R)$ (or every matrix in $M_n(R)$ which can be written as a sum of $k$-th powers in $M_n(R)$) can be written as a sum of $g(n,k,R)$ $k$-th powers in $M_n(R)$.

In this paper, we focus mainly on the first and second questions above. More precisely:

- For $n \geq 1$ we obtain trace conditions for a matrix $M$ in $M_n(R)$ to be a sum of $k$-th powers in $M_n(R)$.
- As a consequence we show that for $n \geq m \geq 1$, if every $m \times m$ matrix over $R$ is a sum of $k$-th powers of matrices over $R$, then so is every $n \times n$ matrix.
• For an order $R$ in an algebraic number field $K$, we show that every $2 \times 2$ matrix, and consequently every $n \times n$ matrix, $n \geq 2$, over $R$ is a sum of cubes of matrices over $R$ if and only if $(3, \text{disc } R) = 1$.

• Similarly, for an order $R$ in an algebraic number field $K$, we show that every $2 \times 2$ matrix, and consequently every $n \times n$ matrix, $n \geq 2$, over $R$ is a sum of fourth powers of matrices over $R$ if and only if $(2, \text{disc } R) = 1$.

For the ring of integers of a quadratic number field, we have the following result:

• Let $n \geq 2$, $q \geq 3$ be a prime and $n < q$. If $\mathcal{O}$ denotes the ring of integers of a quadratic number field, then every $n \times n$ matrix over $\mathcal{O}$ is a sum of $q$th powers of matrices over $\mathcal{O}$ if and only if $(q, \text{disc } K) = 1$. This complements the result for $n \geq q$ in Theorem 2.3 in this case.

2. HISTORY OF WARING’S PROBLEM FOR MATRICES

(a) Waring’s problem for matrices over integers:
The origin of Waring’s problem for matrices may be traced back to a problem posed in Canadian Math. Bulletin by I. Connell and solved by L. Carlitz [11] (1968), who proved that every two-by-two matrix over $\mathbb{Z}$ is a sum of at most three squares. He also characterized $2 \times 2$ matrices $M$ for which $g(2, 2, \mathbb{Z}, M) = 1, 2, 3$. Interesting results for “Matrices as sums of squares”, over an arbitrary commutative ring with unity, were obtained by Griffin and Krusemeyer (see [3]).

In [7], M. Newman proved that every matrix in $M_n(\mathbb{Z}), n \geq 2$, is a sum of squares and $g(2, 2, \mathbb{Z}) = 3$, whereas for $n > 2$, $g(n, 2, \mathbb{Z}) \leq 7$ for $n$ even and $g(n, 2, \mathbb{Z}) \leq 9$ for $n$ odd. Here he queried whether this problem could be generalised to the ring of integers of an algebraic number field and also to the case of arbitrary powers.

(b) Waring’s problem for matrices over arbitrary commutative rings:
In his pioneering work, L. N. Vaserstein [10] (1986) showed that for any commutative ring $R$ with unity for $n \geq 2$, every sum of squares in $M_n(R)$ is a sum of 3 squares, and in particular every matrix in $M_n(\mathbb{Z})$ is a sum of 3 squares (see [10]). In another paper [11], he proved that a matrix in $M_n(R)$ is a sum of squares if and only if its trace reduced modulo $2R$ is a square. He also showed that for all sufficiently large $n$ and positive integers $k$, $g(n, k, \mathbb{Z}) \leq 10$. Various other interesting general results for commutative rings and algebras over fields were also obtained by him (see [12], [13]).

Motivated by these results, Richman in [8] obtained the following “trace condition” for a matrix to be a sum of $k$th powers:

**Theorem 2.1** (D. R. Richman [8] Proposition 4.2). Let $R$ be a ring. If $n \geq k \geq 2$ are integers, then the following statements are equivalent:

1. $M$ is a sum of $k$th powers in $M_n(R)$;
2. $M$ is a sum of seven $k$th powers in $M_n(R)$;
3. $M$ belongs to $M_n(R)$ and for every prime power $p^e$ dividing $k$, there are elements $x_0 = x_0(p), \ldots, x_e = x_e(p)$ in $R$ such that

$$\text{trace } M = x_0 p^e + p x_1 p^{e-1} + \cdots + p^e x_e.$$ 

Moreover if $k = p$ is a prime, in condition (2) “seven” can be replaced by “five”. Also condition (3) simplifies to “trace $M = x_0 p + p x_1$, for some $x_0, x_1 \in R$.”
In the same paper, he proved the following theorem:

**Theorem 2.2** (D. R. Richman [8 Proposition 5.5]). Let $R$ be a ring. Let $n \geq 2$. Then, there exists a number $g_k$ (independent of $n$) such that every matrix in $M_n(R)$ whose trace lies in $k!R$ is a sum of $g_k$ $k$-th powers in $M_n(R)$.

(c) Waring’s problem for algebraic number fields: As an answer to the questions posed by M. Newman, Waring’s problem for matrices over the ring $\mathcal{O}$ of integers of an algebraic number field $K$ was first treated by S. A. Katre and S. A. Khule, who gave a discriminant criterion for $n \times n$ matrices ($n \geq 2$) over orders in algebraic number fields to be sums of squares [4] and later for $k$-th powers ($n \geq k \geq 2$) [5].

**Theorem 2.3** (S. A. Katre and S. A. Khule [4 Theorem 1]). Let $R$ be an order in an algebraic number field $K$. Let $n \geq k \geq 2$. Then every $n \times n$ matrix over $R$ is a sum of (seven) $k$-th powers if and only if $(k, \text{disc } R) = 1$.

Note that the main results in [4], [5] and [8] make the assumption that $n \geq k$; that is, the size of the matrix is greater than or equal to the power occurring in the decomposition. This is because the proofs depend heavily on the construction of (an invertible) matrix $M$ in $M_n(R)$ whose characteristic polynomial is of the form $(X - r)^k X^{n-k} - 1$, for some $r$ in $R$, with the tacit assumption $n \geq k$. For $n < k$, this approach does not work. Thus arise the following natural questions:

1. If $n \geq 2$ (more specifically for $2 \leq n < k$), what are the conditions under which an $n \times n$ matrix over a ring $R$ is a sum of $k$-th powers of matrices over $R$?
2. If $2 \leq n < k$, what are the conditions under which every $n \times n$ matrix over an order $R$ in an algebraic number field is a sum of $k$-th powers of matrices over $R$?

The aim of this paper is to give a trace condition in the context of the first question above and a discriminant condition in some special cases in the context of the second question.

### 3. Generalised Trace Conditions for Matrices to be Sums of $k$-th Powers

The conditions obtained by various authors for a matrix to be a sum of $k$-th powers ($k = 2$, Newman, Vaserstein; general $k$ for $n \geq k$, Richman; see Theorem 2.1) are in terms of the trace of the matrix.

The theorem below gives the “generalised trace condition” for a matrix over a commutative ring to be a sum of $k$-th powers (without recourse to a relation between $n$ and $k$).

**Theorem 3.1.** Let $R$ be a ring and $n, k \geq 2$ be integers. Let $M$ belong to $M_n(R)$. Then the following are equivalent:

1. $M$ is a sum of $k$-th powers of matrices in $M_n(R)$.
2. Trace $M$ is a sum of traces of $k$-th powers of matrices in $M_n(R)$.
3. Trace $M$ is in the subgroup of $R$ generated by the traces of $k$-th powers of matrices in $M_n(R)$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Let $M$ be a ring and $n, k \geq 2$ be integers. Then the following are equivalent:

1. Every matrix $M$ in $M_n(R)$ is a sum of $k$-th powers of matrices in $M_n(R)$.
2. Every element of $R$ is a sum of traces of $k$-th powers of matrices in $M_n(R)$.
3. $R$ is generated as a group by the traces of $k$-th powers of matrices in $M_n(R)$.
4. $R$ is generated as a group by the traces of $k$-th powers of matrices in $M_n(R)$ (mod $k!R$).
5. Every element of $R$ is a sum of traces of $k$-th powers of matrices in $M_n(R)$ (mod $k!R$).

Proof. The proof follows from Theorem 3.1 or, by a similar argument, as given for $\alpha \in R$, $\alpha = \text{trace } M$ for $M = \text{diag}(\alpha, 0, \ldots, 0)$. 

The next two corollaries follow immediately from Theorem 3.2 by noting that for $\alpha \in R$, $\alpha^k = \text{trace}(\text{diag}(\alpha, 0, \ldots, 0))^k$.

Corollary 3.3 (Sufficient Condition 1). Let $R$ be a ring and $n, k \geq 2$ be integers. Let $M$ belong to $M_n(R)$. If every element of the quotient ring $R/k!R$ can be expressed as a sum of $k$-th powers of elements in $R/k!R$, then every matrix $M$ in $M_n(R)$ is a sum of $k$-th powers of matrices in $M_n(R)$.

Corollary 3.4 (Sufficient Condition 2). Let $R$ be a ring and $n \geq 1, k \geq 2$ be integers. Let $M$ belong to $M_n(R)$. If every element of $R$ can be written as a sum of $k$-th powers of elements in $R$, then every matrix in $M_n(R)$ is a sum of $k$-th powers of matrices in $M_n(R)$.

An example highlighting that the sufficient conditions (1) and (2) are not necessary is given in §5.

Let $S(n)$ be the statement that every matrix in $M_n(R)$ is a sum of $k$-th powers in $M_n(R)$. Thus Corollary 3.3 says that $S(1) \Rightarrow S(n)$ for all positive integers $n$.

An important observation “$S(m) \Rightarrow S(n)$ for $m \leq n$” based on the generalized trace condition made by the first author is recorded below:

Theorem 3.5. Let $R$ be a ring and $n \geq m \geq 1$ and $k \geq 2$ be integers. If every matrix in $M_m(R)$ is a sum of $k$-th powers in $M_m(R)$, then every matrix in $M_n(R)$ is a sum of $k$-th powers in $M_n(R)$.

---

Let four power.

trace

Lemma 3.9. This follows exactly as above.

Proof. By "(1) ⇒ (2)" in Theorem 2.2 every element α ∈ R is of the form \[ \sum \text{trace} M_i \delta, \text{for some } M_i \in M_n(R) \]. Write \( N_i = (\begin{smallmatrix} M_i & 0 \\ 0 & 0 \end{smallmatrix}) \), with \( N_i \in M_n(R) \).

Then, \( \alpha = \sum \text{trace} N_i^k \). Hence by "(2) ⇒ (1)" in Theorem 2.2 every matrix in \( M_n(R) \) is a sum of \( k \)-th powers of matrices in \( M_n(R) \). \( \square \)

Remark 3.6. In order to prove that for every \( n \geq 2 \), every \( n \times n \) matrix over \( R \) is a sum of \( k \)-th powers of matrices over \( R \) (in case this is true), from Theorem 3.5 above, it is enough to show that every \( 2 \times 2 \) matrix over \( R \) is a sum of \( k \)-th powers of matrices in \( M_2(R) \). It is at present not known whether there is a ring \( R \) and a power \( k \) for which \( S(2) \) is false, but \( S(n) \) holds for some \( n > 2 \). In §5 it is shown that for \( k = 3 \) and for the ring \( \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \), \( S(2) \) and hence \( S(n) \) holds for all \( n \geq 2 \), although \( S(1) \) does not hold. As noted earlier, Newman proved that for \( k = 2 \), for the ring \( \mathbb{Z} \), \( S(n) \) holds for all \( n \geq 2 \), although \( S(1) \) does not hold.

We now give trace conditions for a \( 2 \times 2 \) matrix over a ring \( R \) to be a cube or a fourth power.

Lemma 3.7. Let \( R \) be a ring. Let \( A \) belong to \( M_2(R) \). If \( A = B^3 \), then there exist \( t, \Delta \) in \( R \) such that \( \text{trace} A = t^3 - 3t\Delta \). Conversely, given an element of \( R \) of the form \( t^3 - 3t\Delta, \) for some \( t, \Delta \) in \( R \), there exists \( B \) in \( M_2(R) \) such that \( \text{trace} B^3 = t^3 - 3t\Delta \).

Proof. Let \( A = B^3 \), \( \text{trace} B = t \) and \( \text{det} B = \Delta \). Note that \( B \) satisfies its characteristic polynomial: \( B^2 - tB + \Delta I = 0 \), where \( I \) stands for the \( 2 \times 2 \) identity matrix. This gives that \( B^3 = tB^2 - \Delta B = t(tB - \Delta I) - \Delta B = (t^2 - \Delta)B - t\Delta I \). Hence, \( A = B^3 = (t^2 - \Delta)B - t\Delta I \) and \( \text{trace} A = t(t^2 - \Delta) - 2t\Delta = t^3 - 3t\Delta \).

Conversely, given an element of \( R \) of the form \( t^3 - 3t\Delta, \) for some \( t, \Delta \) in \( R \), the matrix \( B = \begin{pmatrix} 1 & -\Delta \\ 1 & t \end{pmatrix} \) satisfies \( \text{trace} B^3 = t^3 - 3t\Delta \). \( \square \)

Lemma 3.8. Let \( R \) be a ring. Let \( A \) belong to \( M_2(R) \). If \( A = B^4 \), then there exist \( t, \Delta \) in \( R \) such that \( \text{trace} A = t^4 - 4t^2\Delta + 2\Delta^2 \). Conversely, given an element of \( R \) of the form \( t^4 - 4t^2\Delta + 2\Delta^2, \) for some \( t, \Delta \) in \( R \), there exists \( B \) in \( M_2(R) \) such that \( \text{trace} B^4 = t^4 - 4t^2\Delta + 2\Delta^2 \).

Proof. This follows exactly as above. \( \square \)

Lemma 3.9. Let \( R \) be a ring and \( n, q \geq 2 \) be integers with \( q \) prime. Then, \( \text{trace}(M^q) \equiv (\text{trace} M)^q \pmod{qR} \) for all \( M \in M_n(R) \). Also if every \( n \times n \) matrix over \( R \) is a sum of \( q \)-th powers of matrices over \( R \), then every element of \( R \) is a \( q \)-th power \( \pmod{qR} \).

Proof. Let \( M = (m_{ij}) \). Then, \( \text{trace}(M^q) = \sum m_{i_1i_2}m_{i_2i_3} \cdots m_{i_qi_1}, \) where the sum is over the indices \( i_j \), with \( 1 \leq i_1, i_2, \ldots, i_q \leq n \). Note that \( m_{i_1i_2}m_{i_2i_3} \cdots m_{i_qi_1} \) is unchanged after a cyclic permutation of \( i_1, i_2, \ldots, i_q \) and if at least two of \( i_j \) and \( i_k \) are unequal, \( q \) being a prime, there are \( q \) distinct \( q \)-tuples obtained from \( i_1, \ldots, i_q \) by a cyclic change.

So, \( \text{trace}(M^q) \equiv m_{11}^q + \cdots + m_{qq}^q \pmod{qR} \equiv (m_{11} + \cdots + m_{qq})^q \pmod{qR} \), i.e., \( \text{trace}(M^q) \equiv (\text{trace} M)^q \pmod{qR} \). \( \square \)
4. WARING’S PROBLEM FOR MATRICES OVER ORDERS
IN ALGEBRAIC NUMBER FIELDS

We recall in this section basic definitions and a few results from [5] regarding
discriminant conditions for orders.

**Definition 4.1.** An order \( R \) in an algebraic number field \( K \) is a subring of \( K \) containing 1 and which is a \( \mathbb{Z} \)-submodule of \( K \) of maximum rank, i.e. of rank \( n = \deg(K/\mathbb{Q}) \).

The ring of integers, \( \mathcal{O} \), of \( K \) is an order of \( K \) and it contains every order; hence \( \mathcal{O} \) is called the maximal order of \( K \). The discriminant of an order \( R \) is defined to be the discriminant of any \( \mathbb{Z} \)-basis of \( R \).

We recall below the useful “Discriminant criterion”:

**Lemma 4.2 ([5, Lemma 3]).** Let \( p \) be a prime number. Let \( \mathcal{O} \) be the ring of integers of a number field \( K \). Then the following are equivalent:

1. Every element of \( \mathcal{O} \) is a \( p \)-th power (mod \( p \mathcal{O} \)).
2. \( (p, \text{disc } K) = 1 \).

We state some results regarding orders in an algebraic number field.

**Lemma 4.3 ([5, Lemma 6]).** Let \( R \) be a commutative ring with unity. Let \( p \) be a prime and \( R/pR \) a finite ring. Then the following are equivalent:

1. Every element of \( R \) is a \( p \)-th power (mod \( pR \)).
2. \( x \in R, x^p \in pR \) imply \( x \in pR \).

We now state a lemma from [5] in the form that we would be using.

**Lemma 4.4.** Let \( R \) be an order in an algebraic number field \( K \). Let \( p \) be a prime. Then the conditions (1) and (2) in Lemma 4.3 above are equivalent to the condition \( (p, \text{disc } R) = 1 \).

**Proof.** The proof that condition (2) is equivalent to \( (p, \text{disc } R) = 1 \) is a part of the proof of Theorem 1 in [5]. (See [5], §3, for the details.) \( \square \)

**Remark 4.5.** The discriminant of an order can be computed using the free mathematical software KASH. (See [15].)

5. A COUNTERINTUITIVE EXAMPLE

Let \( \mathcal{O}_3 \) denote the additive subgroup of \( \mathcal{O} \), generated by cubes of elements of \( \mathcal{O} \). If \( \mathcal{O}_3 = \mathcal{O} \), then Corollary 3.4 shows that every matrix in \( M_2 \mathcal{O} \) is a sum of cubes of matrices in \( M_2 \mathcal{O} \). That the converse does not hold is seen from the example below.

Let \( K = \mathbb{Q}(\sqrt{5}) \). Then the ring of integers of \( K \) is \( \mathcal{O} = \mathbb{Z}[\frac{1 + \sqrt{5}}{2}] \) and \( \text{disc } K = 5 \). Let \( \alpha = \frac{1 + \sqrt{5}}{2} \). Then, \( \alpha \) satisfies the relation \( \alpha^2 - \alpha - 1 = 0 \). Thus, \( \alpha^2 = \alpha + 1 \) and \( \alpha^3 = 2\alpha + 1 \). Now if \( \beta = u + v\alpha \) is an element of \( \mathcal{O} \), then \( \beta^3 = (u^3 + 3u^2v + v^3) + \alpha (3uv(u + v) + 2v^3) \), which shows that the coefficient of \( \alpha \) in the cube of any arbitrary element of \( \mathcal{O} \) is always even. This observation now shows that \( \alpha \) (or for that matter any element of \( \mathcal{O} \) for which the coefficient of \( \alpha \) is odd) cannot be expressed as a sum of cubes of elements of \( \mathcal{O} \); thus \( \mathcal{O}_3 \neq \mathcal{O} \).

However, Theorem 6.2 shows that every \( 2 \times 2 \) matrix over \( \mathcal{O} \) is a sum of cubes of matrices over \( \mathcal{O} \), as \( (3,5) = 1 \).
Remark 5.1. One also observes here that the elements of $\mathcal{O}$ of the form $a + b\alpha$ with $a, b \in \mathbb{Z}$, $b$ odd, are not sums of cubes even modulo $6\mathcal{O}$. This example thus shows that the Sufficient Condition 1 in Corollary 3.3 is not necessary.

Other examples of this type for a quadratic field $K = \mathbb{Q}(\sqrt{d})$ occur when $d$ is a squarefree integer of the form $5 + 8s$. The ring of integers is then $\mathbb{Z}[\alpha]$, where $\alpha = \frac{1 + \sqrt{5+8s}}{2}$. Then the above relations $\alpha^2 = \alpha + 1$ and $\alpha^3 = 2\alpha + 1$ hold modulo $2\mathcal{O}$, and the same calculations show that $a + b\alpha$, with $a, b \in \mathbb{Z}$, $b$ odd, is not a sum of cubes in $\mathcal{O}$, so $\mathcal{O}_s \neq \mathcal{O}$. If further $s \neq 2 \pmod{3}$, then the discriminant $d = 5 + 8s$ is coprime to 3, so every matrix in $M_2(\mathcal{O})$ is a sum of cubes in $M_2(\mathcal{O})$. We shall see in §7, using a theorem of Bateman and Stemmler, that these are the only quadratic fields of this type.

6. 2 × 2 Matrices as Sums of Cubes and Fourth Powers

Theorem 6.1. Let $R$ be a ring. Then $M \in M_2(R)$ is a sum of cubes in $M_2(R)$ if and only if $\text{trace } M \equiv \text{a cube } \pmod{3R}$.

Proof. Let $S =$ the set of sums of traces of cubes of matrices in $M_2(R)$. Then by the equivalence of conditions (2) and (3) in Theorem 5.1, or using that for $M \in M_2(R), \text{trace}(-M)^3 = -\text{trace } M^3$, we get that $S$ is an abelian group. Now by Lemma 5.7

$$S = \left\{ \sum_{i=1}^{j} (t_i^3 - 3t_i\Delta_i) \mid t_i, \Delta_i \in R, j \geq 1 \right\},$$

Then for $t, \Delta \in R$, $t^3 - 3t\Delta \in S$. Putting $\Delta = 0$, we see that $t^3 \in S$. Since $S$ is a group, $3t\Delta \in S$. Putting $t = 1$, $3\Delta \in S$. Thus $S$ contains the abelian group generated by all elements of the type $t^3$ and $3\Delta$.

Since $R$ is commutative, using $t_1^3 + t_2^3 = (t_1 + t_2)^3 - 3t_1t_2(t_1 + t_2)$ we see that every sum of cubes is a cube modulo $3R$. Thus $S$ consists of all elements of $R$ which are congruent to a cube modulo $3R$, i.e.,

$$S = \{ x_0^3 + 3x_1 \mid x_0, x_1 \in R \}.$$

Now if $\text{trace } M \equiv \text{a cube } \pmod{3R}$, then $\text{trace } M \in S$, so $\text{trace } M$ is a sum of traces of cubes of matrices in $M_2(R)$. Now the equivalence of (1) and (2) in Theorem 3.1 gives the result. \qed

The theorem below gives a criterion for every matrix over a ring $R$ to be a sum of cubes. More specifically, it gives a discriminant condition for an order in an algebraic number field.

Theorem 6.2. Let $R$ be a ring. Let $n \geq 2$. Then, the following are equivalent:

(1) Every matrix in $M_n(R)$ is a sum of cubes of matrices in $M_n(R)$.

(2) Every element of $R$ is a cube $\pmod{3R}$.

If $R$ is an order in an algebraic number field, then these conditions are further equivalent to

(3) $(3, \text{disc } R) = 1$.

Proof. (1) $\Rightarrow$ (2) follows from Lemma 3.9; (2) $\Rightarrow$ (1) follows from Corollary 3.3; (2) $\iff$ (3) follows from Lemma 4.4. \qed
We prove similar results for fourth powers.

**Theorem 6.3.** Let $R$ be a ring. Then $M \in M_2(R)$ is a sum of fourth powers in $M_2(R)$ if and only if trace $M = x_0^4 + 2x_1^2 + 4x_2$, for some $x_0, x_1, x_2 \in R$.

**Proof.** Let $G = \text{the set of sums of fourth powers of matrices in } M_2(R)$. Then, by the equivalence of conditions (2) and (3) in Theorem 6.3, $G$ is an abelian group:

$$G = \left\{ \sum_{i=1}^j (t_i^4 - 4t_i^2\Delta_i + 2\Delta_i^2) \mid t_i, \Delta_i \in R, j \geq 1 \right\}.$$  

In particular, $t^4 - 4t^2\Delta + 2\Delta^2 \in G$, for every $t, \Delta \in R$. Putting $\Delta = 0$, $t^4 \in G$. Putting $t = 0$, we get $2\Delta^2 \in G$. Again as $G$ is a group, $4t^2\Delta \in G$. In particular, for $t = 1$, $4\Delta \in G$. Thus, every element of the form $t^4_0 + 2t^2\Delta_1 + 4t_2 \in G$.

Conversely, let $\alpha = \sum_{i=1}^j (t_i^4 - 4t_i^2\Delta_i + 2\Delta_i^2) \in G$. Now, as $R$ is commutative, we have

$$(t + t')^4 = t^4 + t'^4 + 3[2(t^2t'^2)] + 4tt'(t^2 + t'^2).$$

Hence, we get $\alpha = x_0^4 + \sum_i (\pm 2) y_i^2 + 4\theta$, for some $x_0, y_i, \theta \in R$. Using the above equations, we get $\alpha = x_0^4 - \sum_i 2y_i^2 + 4\theta$, for some $x_0, y_i, \theta \in R$ and using $(s+s')^2 = s^2 + (s')^2 + 2ss'$, $-2s^2 = 2s^2 - 4s^2$, we get

$$\alpha = x_0^4 + 2x_1^2 + 4x_2,$$

for some $x_0, x_1, x_2 \in R$. Thus,

$$G = \{x_0^4 + 2x_1^2 + 4x_2 \mid x_0, x_1, x_2 \in R\}.$$  

Now $M \in M_2(R)$ is a sum of fourth powers in $M_2(R)$ if and only if trace $M \in G$ if and only if trace $M = x_0^4 + 2x_1^2 + 4x_2$, for some $x_0, x_1, x_2 \in R$. \hfill \Box

**Theorem 6.4.** Let $R$ be a ring. Let $n \geq 2$. Then, the following are equivalent:

1. Every matrix in $M_n(R)$ is a sum of fourth powers of matrices in $M_n(R)$.
2. Every element of $R$ is a square (mod 2R).
3. $(2, \text{disc } R) = 1$.

**Proof.** (1) $\Rightarrow$ (2) follows from Lemma 3.9. If $R$ is an order, (2) $\iff$ (3) follows from Lemma 4.3.

It is enough to prove (2) $\Rightarrow$ (1) in the case $n = 2$. (See Theorem 3.3). If every element of $R$ is a square (mod 2R), then for $z \in R$, write $z = a^2 + 2b = (a_1^2 + 2a_2)^2 + 2(b_1^2 + 2b_2)$, with $a, b, a_1, a_2, b_1, b_2 \in R$. Thus, every $z \in R$ is of the form $x_0^4 + 2x_1^2 + 4x_2$, with $x_0, x_1, x_2 \in R$. This proves (1) in view of Theorem 6.3. \hfill \Box

7. **Matrices over the ring of integers of a quadratic number field as sums of $q$-th powers, $q$ prime**

Let $n \geq 2$, $q$ a prime. In this section we obtain results specific to rings of integers $O$ of quadratic number fields $K$ (i.e. $K = \mathbb{Q}(\sqrt{d})$, $d$ a square-free integer). Let $O_q$ be the additive subgroup generated by the $q$-th powers of the elements of $O$. For the ring $O$ of integers of the quadratic number field $K$ we get the following classification (see Theorem 7.3 for details):
• For all primes \( q \geq 5 \), every element of \( \mathcal{O} \) is a sum of \( q \)-th powers if and only if \( (q, \text{disc } K) = 1 \) and only if every \( M \in M_n(\mathcal{O}), n \geq 2 \), is a sum of \( q \)-th powers of matrices over \( \mathcal{O} \).

• For \( q = 2 \), every element of \( \mathcal{O} \) is a sum or difference of squares if and only if \((2, \text{disc } K) = 1 \) if and only if every \( M \in M_n(\mathcal{O}), n \geq 2 \), is a sum of squares of matrices over \( \mathcal{O} \) if and only if \( d \equiv 1 \pmod{4} \). (See also Theorem 2.3)

• For \( q = 3 \), something interesting happens: one gets examples wherein \( \mathcal{O}_3 \neq \mathcal{O} \), yet every \( M \in M_n(\mathcal{O}), n \geq 2 \), is a sum of cubes of matrices over \( \mathcal{O} \).

We begin by recalling the following result:

**Theorem 7.1** (P. T. Bateman, R. M. Stemmle [1 Theorem 3]). Let \( \mathcal{O} \) be the ring of integers of an algebraic number field \( K \) (not necessarily quadratic) and \( q \) be a prime. Let \( \mathcal{O}_q \) be the additive subgroup generated by the \( q \)-th powers of the elements of \( \mathcal{O} \). Then, \( \mathcal{O}_q \neq \mathcal{O} \) if and only if at least one of the following holds:

1. \( q \) is ramified in \( \mathcal{O} \) (i.e. \( q \) divides \( \text{disc } K \)),
2. \( q \) is expressible in the form \( \frac{p^r - 1}{p - 1} \), where \( p \) is a prime, \( r \) and \( d \) are positive integers, \( d \) is a divisor of \( r \), and \( p \) has in \( \mathcal{O} \) a prime factor of degree \( r \).

**Example 7.2.** Let \( K = \mathbb{Q}(\sqrt{d}) \), where \( d \) is a square-free integer. Let \( \mathcal{O} \) be the ring of integers of \( K \). Then,

\[
\text{disc } K = \begin{cases} 
4d & \text{if } d \equiv 2, 3 \pmod{4} \\
\quad d & \text{if } d \equiv 1 \pmod{4}.
\end{cases}
\]

• For \( q = 2 \), condition (2) in Theorem 7.1 is never valid for any prime \( p \). Thus, \( \mathcal{O}_2 \neq \mathcal{O} \) if and only if 2 is ramified in \( \mathcal{O} \) if and only if \( d \equiv 2, 3 \pmod{4} \). Combining this with Theorem 2.3 and Corollary 3.1 we get \( \mathcal{O}_2 = \mathcal{O} \) if and only if 2 is unramified in \( \mathcal{O} \) if and only if \((2, \text{disc } K) = 1 \) if and only if every \( M \in M_n(\mathcal{O}), n \geq 2 \), is a sum of (five) squares if and only if \( d \equiv 1 \pmod{4} \). (See Theorem 2.3)

• For \( q = 3 \), condition (2) in Theorem 7.1 above becomes: \( 3 = \frac{p^r - 1}{p - 1} \), where \( d \) divides \( r \) and \( p \) has in \( \mathcal{O} \) a prime factor of degree \( r \). This is possible if and only if \( p = 2 \) and \( (2) \) is a prime ideal in \( \mathcal{O} \) (i.e., the Kronecker symbol \( \left( \frac{\text{disc } K}{2} \right) = -1 \)), i.e., \( d = 5 + 8s, s \in \mathbb{Z} \). Thus, \( \mathcal{O}_3 \neq \mathcal{O} \) if and only if either 3 is ramified in \( \mathcal{O} \) or \( (2) \) is a prime ideal in \( \mathcal{O} \); i.e., 3 divides \( d \) or \( d = 5 + 8s \). Thus, \( d = 5 + 8s \), with \((3, d) = 1 \), i.e., \( s \neq 2 \pmod{3} \), gives all the quadratic rings for which \( \mathcal{O}_3 \neq \mathcal{O} \), but every matrix in \( M_2(\mathcal{O}) \) is a sum of cubes of matrices in \( M_2(\mathcal{O}) \). (See Theorem 6.2 This answers a query from Volker Schultze.)

We prove the following theorem for the ring \( \mathcal{O} \) of integers of a quadratic number field \( K \):

**Theorem 7.3.** Let \( n, q \geq 2 \) and \( q \) be a prime such that \( n < q \). Let \( K \) be a quadratic number field and \( \mathcal{O} \) its ring of integers. Then \( (q, \text{disc } K) = 1 \) if and only if every \( n \times n \) matrix over \( \mathcal{O} \) is a sum of \( q \)-th powers of matrices over \( \mathcal{O} \).

**Proof.** \((\implies)\) If \( q \) is unramified in \( \mathcal{O} \), i.e. \((q, \text{disc } K) = 1 \), then the only way in which \( \mathcal{O}_q \neq \mathcal{O} \) is when primes \( q \) are of the form given in (2) of Theorem 7.1. However specialization to quadratic number fields shows that there are restrictions on the integers \( r \) and \( d \) occurring in the expression for \( q \). In fact the only nontrivial case occurs when \( r = 2 \) and \( d = 1 \), in which case \( q = \frac{p^2 - 1}{p - 1} = p + 1 \). This case occurs
only when $q = 3$ and $p = 2$. The additional assumption $n < q$ implies $n = 2$. For this case, i.e. $n = 2$ and $q = 3$, the required result now follows from Theorem 6.2.

Now the table in [1] shows that the primes $q$ of the above form are very rare. In fact, all such primes $q \geq 5$ are never of the form $p^2 - 1$, for some prime $p$, having a prime factor of degree 2 in $O$. All the exponents of $p$ in such prime powers are $\geq 3$. Thus, we have that for all primes $q \geq 5$, the only condition for $O = O_q$ to hold is that $(q, \text{disc } K) = 1$. This proves that every $n \times n$ matrix over $O$ is a sum of $q$-th powers of matrices over $O$ (see Corollary 3.4).

$(\iff)$ If every matrix over $O$ is a sum of $q$-th powers of matrices over $O$, then every element of $O$ is a $q$-th power (mod $qO$), so by Lemma 4.2 we get $(q, \text{disc } K) = 1$. □

Remark 7.4. It is expected that for a prime $q \geq 5$, the result in Theorem 7.3 also holds for orders in algebraic number fields just as it holds for $q = 3$.

Remark 7.5. Let $O$ be the ring of integers of a quadratic number field $K$. Let $n, q \geq 2$ be integers and let $q$ be a prime. For $g_k$ as defined in Theorem 2.2, we have:

1. If $n \geq q$, then every $n \times n$ matrix is a sum of at most five $q$-th powers (by Theorem 2.1) if and only if $(q, \text{disc } K) = 1$.
2. If $n < q$ (so $q \geq 3$), then every $n \times n$ matrix over $O$ is a sum of at most $g_k + 2^{q-1} + \frac{q-1}{2} + 1 q$-th powers of matrices over $O$ if and only if $(q, \text{disc } K) = 1$. (See Theorem 2.1, Theorem 2.2 and the results from [9], viz. Theorems 9 and 10, for details.)

8. SOME REMARKS AND OPEN QUESTIONS

- **Matrices over $\mathbb{Z}$ as sums of cubes:** S. A. Katre and D. N. Sheth [6] have obtained a criterion for a $2 \times 2$ matrix over $R$, $R$ an integrally closed domain, to be a cube and have proved that every matrix in $M_2(\mathbb{Z})$ is a sum of at most four cubes. Also, Kshipra G. Wadikar and S. A. Katre [14] have proved that for $n \geq 3$ also, every matrix in $M_n(\mathbb{Z})$ is a sum of four cubes. Whether 4 is minimal is open. Such minimality questions are mostly open for orders and other rings, for general $n$ and $k$.

- **Waring’s problem for matrices over noncommutative rings:** S. A. Katre and K. D. Joshi observed that every element of the division ring of real quaternions, viz. $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$, is a $k$-th power. Quaternions which are not real numbers have exactly $k$ $k$-th roots whereas real numbers have infinitely many quaternion $k$-th roots for $k > 2$. For $k = 2$, there are exactly 2 square roots if the real number is positive and infinitely many square roots if the real number is negative. All these results were first observed by I. Niven in 1940. In [11] Vaserstein proved that for a ring $R$, not necessarily commutative, a matrix $M \in M_n(R)$, $n \geq 2$, is a sum of squares if and only if its trace is a sum of squares (mod $2R$). If $n \geq 2$, every $n \times n$ matrix over real quaternions is a sum of squares whereas there are matrices over integral quaternions which are not sums of squares (viz. those matrices for which at least one of $i, j, k$ has odd coefficients in the trace). For $k > 2$, conditions regarding matrices over noncommutative rings to be sums of $k$-th powers are awaited.
MATRICES OVER COMMUTATIVE RINGS AS SUMS OF $k$-TH POWERS

Acknowledgements

We thank R. Balasubramanian for pointing out to us some work of mathematicians on Waring’s problem for algebraic number fields, and Dinesh Thakur for informing us about the free mathematical software KASH, useful for computations in algebraic number theory. We thank Bhaskaracharya Institute of Mathematics, Pune, for some facilities. The second author would like to thank the Council of Scientific and Industrial Research (C.S.I.R), New Delhi, for awarding a research fellowship during her doctoral studies. The authors thank TIFR, Mumbai, for hospitality, and the first author also thanks Freie University, Berlin, where the paper was finalised, for its hospitality.

References


Department of Mathematics, University of Pune, Pune-411007, India
E-mail address: sakatre@math.unipune.ac.in

Centre for Excellence in Basic Sciences, University of Mumbai, Mumbai-400098, India
E-mail address: anuradha@cbs.ac.in