MATRICES OVER ORDERS IN ALGEBRAIC NUMBER FIELDS
AS SUMS OF $k$-TH POWERS

S. A. KATRE AND SANGITA A. KHULE

(Communicated by David E. Rohrlich)

Dedicated to the memory of David R. Richman

Abstract. David R. Richman proved that for $n \geq k \geq 2$ every integral $n \times n$ matrix is a sum of seven $k$-th powers. In this paper, in light of a question proposed earlier by M. Newman for the ring of integers of an algebraic number field, we obtain a discriminant criterion for every $n \times n$ matrix $(n \geq k \geq 2)$ over an order of an algebraic number field to be a sum of (seven) $k$-th powers.

1. Introduction

M. Newman [1] showed that, for $n \geq 2$, every matrix in $M_n \mathbb{Z}$ is a sum of 7 or 9 squares according as $n$ is even or odd. He then posed the problem for the ring of integers (i.e. the maximal order) of an algebraic number field.

Vaserstein [3], [4] showed that every integral $n \times n$ matrix $(n \geq 2)$ is a sum of three squares by proving the following

**Theorem A.** A matrix $A$ in $M_n R$ ($R$ a commutative ring with 1 and $n \geq 2$) is a sum of squares if and only if $A$ is a sum of three squares if and only if $\text{tr}.A \equiv \text{square} \pmod{2R}$.

David R. Richman [2] showed that, for $n \geq k \geq 2$, every $n \times n$ integral matrix is a sum of seven $k$-th powers using his following key-result:

**Theorem B.** Let $n \geq 2$, $R$ a commutative ring with 1. The following are equivalent:

(i) $M$ is a sum of $k$-th powers in $M_n R$.

(ii) $M$ is a sum of seven $k$-th powers in $M_n R$.

(iii) $M \in M_n R$ 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

$$\text{tr}.M = x_0^p + px_1^{p-1} + p^2 x_2^{p-2} + \cdots + p^e x_e.$$ 

If $F$ is a field of characteristic 0, then it follows from Theorems A and B that every matrix in $M_n F$ ($n \geq 2$) is a sum of three squares, and for $n \geq k \geq 2$, every matrix in $M_n F$ is a sum of seven $k$-th powers in $M_n F$. The same result also follows

Received by the editors April 21, 1998.

1991 Mathematics Subject Classification. Primary 11P05, 11R04, 15A33; Secondary 11C20, 11E25, 15A24.

Key words and phrases. Algebraic number fields, order, sums of powers, discriminant, matrices.

©1999 American Mathematical Society

671
for matrices over \( \mathbb{Z} \). However, if we consider the ring of integers or other orders in algebraic number fields, then we find that for some of these rings such a result is true, whereas for some other rings we get counter-examples. For instance, if \( R = \mathbb{Z}[i] \), then \( R/2R = \{0, 1, 1, \bar{1}+1\} \). Here \( \bar{0} \) and \( \bar{1} \) are the only squares, and an \( n \times n \) matrix over \( \mathbb{Z}[i] \) \((n \geq 2)\) whose trace is \( \equiv i \mod 2R \) is not a sum of squares in \( \mathbb{Z}[i] \). On the contrary, every element of \( R/3R \) is a cube, so every \( n \times n \) matrix \((n \geq 3)\) over \( \mathbb{Z}[i] \) is a sum of seven cubes. One has exactly the reverse situation for \( R = \mathbb{Z}[\omega] \), \( \omega = \exp(2\pi i/3) \), and we get that every \( n \times n \) matrix \((n \geq 2)\) over \( \mathbb{Z}[\omega] \) is a sum of 3 squares, but for every \( n \geq 3 \), we find matrices over \( \mathbb{Z}[\omega] \) which are not sums of cubes in \( \mathbb{Z}[\omega] \).

In this paper, we take up this problem (earlier raised by Newman) for orders in algebraic number fields and obtain the following discriminant criterion:

**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 \((k, \text{disc.} R) = 1\).

2. **Matrices over the ring of integers of an algebraic number field**

Henceforth, let \( K \) denote an algebraic number field and \( \mathcal{O} \) the ring of integers of \( K \). The discriminant of \( K \) or the discriminant of \( \mathcal{O} \) denotes the discriminant of any integral basis of \( K \) (i.e. a \( \mathbb{Z} \)-basis of \( \mathcal{O} \)). In this section we prove

**Proposition 1.** Let \( n \geq k \geq 2 \). Every \( n \times n \) matrix over \( \mathcal{O} \) is a sum of (seven) \( k \)-th powers if and only if \((k, \text{disc.} K) = 1\).

For this, we first note the following lemmas:

**Lemma 1.** Let \( R \) be a commutative ring with 1. Let \( p \) be a prime. The following are equivalent:

(i) Every element of \( R \) is a \( p \)-th power \( \mod pR \).

(ii) For every \( e \geq 1 \), given any \( x \in R \), there are elements \( x_0, x_1, \ldots, x_e \) depending upon \( p \) and \( e \) such that

\[
x = x_0^p + px_1^{p-1} + p^2x_2^{p-2} + \cdots + p^e x_e.
\]

**Proof.** (ii) \( \Rightarrow \) (i) is clear. To prove (i) \( \Rightarrow \) (ii), first prove by induction that \( a \equiv b \mod pR \Rightarrow a^p \equiv b^p \mod p^{e+1}R \). Then (ii) can be proved by induction by noting that if \( x_i \equiv y_i^p \mod pR \), then \( x_i^{p^{e-i}} \equiv y_i^{p^{e-i+1}} \mod p^{e-i+1}R \) so that \( p^e y_i^{(e+1)-i} \equiv p^e y_i^{(e+1)-i} \mod p^{e+1}R \).

**Lemma 2.** Let \( R \) be a commutative ring with unity. Let \( n \geq k \geq 2 \). The following are equivalent:

(1) Every matrix in \( M_nR \) is a sum of \( k \)-th powers in \( M_nR \).

(2) Every matrix in \( M_nR \) is a sum of seven \( k \)-th powers in \( M_nR \).

(3) For every \( p \) dividing \( k \), every element of \( R \) is a \( p \)-th power \( \mod pR \).

**Proof.** (1) \( \Leftrightarrow \) (2) is due to Theorem B of Richman. (1) \( \Leftrightarrow \) (3) is obtained by combining Theorem B and Lemma 1, and by noting that every \( x \in R \) is the trace of the diagonal matrix diag \( \{x, 0, 0, \ldots, 0\} \).
Lemma 3. Let \( p \) be a prime. The following are equivalent:

(i) Every element of \( O \) is a \( p \)-th power \( \pmod{pO} \).

(ii) \( p \), \( disc.K \) = 1.

Proof. \( (\Leftarrow) \) Let \( (p, disc.K) = 1 \). Then \( p \) is unramified in \( K \), so \( pO = \varphi_1\varphi_2\cdots\varphi_r \), where \( \varphi_1, \varphi_2, \ldots, \varphi_r \) are distinct primes of \( O \). Then by the Chinese remainder theorem, \( O/pO \cong O/\varphi_1 \oplus \cdots \oplus O/\varphi_r \). Each \( O/\varphi_i \) is a finite field of characteristic \( p \), so every element of \( O/\varphi_i \) and hence of \( O/pO \) is a \( p \)-th power.

\( (\Rightarrow) \) Suppose \( p \mid disc.K \). Then \( p \) is ramified in \( K \). Let \( \varphi \) be a prime divisor of \( p \) which ramifies. Take \( x \in \varphi \) such that \( x \not\equiv \varphi^2 \). Then \( x \not\equiv y^p \pmod{pO} \) for any \( y \in O \). For otherwise, \( \varphi \mid x \Rightarrow \varphi \mid y^p \Rightarrow \varphi \mid y \Rightarrow \varphi^2 \mid x \) (as \( \varphi^2 \mid pO \)), a contradiction.

\( \Box \)

Proof of Proposition 1. Follows by combining Lemma 2 and Lemma 3.

Corollary 1. Let \( m \) be a squarefree integer. Let \( O \) be the ring of integers of \( K = \mathbb{Q}(\sqrt{m}) \) i.e. \( O = \mathbb{Z}[\sqrt{m}] \) if \( m \equiv 2, 3 \pmod{4} \) and \( O = \mathbb{Z}[(1 + \sqrt{m})/2] \) if \( m \equiv 1 \pmod{4} \). Let \( n \geq k \geq 2 \). Then every matrix in \( M_n O \) is a sum of (seven) \( k \)-th powers if and only if \( (k, m) = 1 \) and either

(i) \( k \) is odd, or

(ii) \( k \) is even and \( m \equiv 1 \pmod{4} \).

Proof. \( Disc.\mathbb{Q}(\sqrt{m}) = \begin{cases} m, & \text{if } m \equiv 1 \pmod{4}, \\ 4m, & \text{if } m \equiv 2, 3 \pmod{4}. \end{cases} \)

\( \Box \)

Corollary 2. Let \( m \geq 1 \) and \( \zeta_m \) be a primitive \( m \)-th root of unity. The ring of integers of the cyclotomic field \( K = \mathbb{Q}(\zeta_m) \) is \( O = \mathbb{Z}[\zeta_m] \).

Let \( n \geq k \geq 2 \). Then every \( n \times n \) matrix over \( \mathbb{Z}[\zeta_m] \) is a sum of (seven) \( k \)-th powers if and only if either

(i) \( (k, m) = 1 \), or

(ii) \( m \equiv 2 \pmod{4} \) and \( (k, m) = 2 \).

Proof. Note that \( \mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m}) \), if \( m \) is odd. Also for \( m \not\equiv 2 \pmod{4} \), the prime divisors of \( disc. \mathbb{Q}(\zeta_m) \) are the same as the prime divisors of \( m \).

\( \Box \)

3. MATRICES OVER ORDERS IN ALGEBRAIC NUMBER FIELDS

An order in a algebraic number field \( K \) is a ring containing \( 1 \), and which is a finitely generated \( \mathbb{Z} \)-submodule of \( K \) of maximum rank, i.e. of rank \( N = \text{deg}(K/\mathbb{Q}) \). One notes that \( O \) is an order of \( K \) and \( O \) contains every order; hence \( O \) 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 \( R \).

Lemma 4. If \( K \) is a number field of degree \( N \), \( O \) the ring of integers of \( K \), and \( R \) an order of \( K \), then there are a \( \mathbb{Z} \)-basis \( \theta_1, \theta_2, \ldots, \theta_N \) of \( O \) and a \( \mathbb{Z} \)-basis \( \alpha_1, \alpha_2, \ldots, \alpha_N \) of \( R \) such that \( \alpha_i = f_i \theta_i \), \( f_i \in \mathbb{Z} \), \( f_i > 0 \), and moreover

\[ f_1 \mid f_2 \mid \cdots \mid f_N. \]

Proof. Start with any \( \mathbb{Z} \)-bases \( \eta_1, \ldots, \eta_N \) and \( \beta_1, \ldots, \beta_N \) of \( O \) and \( R \) respectively. Let \( A \in M_N \mathbb{Z} \) such that \( [\beta_1, \ldots, \beta_N] = [\eta_1, \ldots, \eta_N]A \). As \( \mathbb{Z} \) is a PID, there exist unimodular matrices \( P \) and \( Q \) such that \( PAQ = \text{diag}.[f_1, f_2, \ldots, f_N] \) is the Smith normal form of \( A \), so that \( f_1 \mid f_2 \mid \cdots \mid f_N \). As rank of \( A \) is \( N \), each \( f_i \neq 0 \). We
may also assume that each $f_i > 0$. Now

$$[\beta_1, \ldots, \beta_N]Q = [\eta_1, \ldots, \eta_N]P^{-1}(PAQ).$$

Call $[\beta_1, \ldots, \beta_N]Q = [\alpha_1, \ldots, \alpha_N]$ and $[\eta_1, \ldots, \eta_N]P^{-1} = [\theta_1, \ldots, \theta_N]$. \hfill $\square$

Lemma 5. With the bases of $O$ and $R$ as in Lemma 4, one has

$\text{index of } R \text{ in } O = f_1f_2 \cdots f_N$ and $\text{disc.} R = (f_1f_2 \cdots f_N)^2 \text{disc.} K$.

Proof. Clear. \hfill $\square$

Lemma 6. Let $R$ be a commutative ring with 1. Let $p$ be a prime and $R/pR$ a finite ring. The following are equivalent:

(i) Every element of $R$ is a $p$-th power (mod $pR$).

(ii) $x \in R$, $x^p \in pR \Rightarrow x \in pR$.

Proof. Let the map $\phi: R/pR \to R/pR$ be given by $\alpha \to \alpha^p$. Then $\phi$ is a homomorphism. Now

(i) $\iff \phi$ is onto $\iff \phi$ is one-one (as $R/pR$ is finite) $\iff \ker \phi$ is trivial $\iff$ (ii). \hfill $\square$

Proof of Theorem 1. ($\Leftarrow$) Suppose $(k, \text{disc.} R) = 1$. Let $p$ be any prime divisor of $k$. Then $(p, \text{disc.} R) = 1$, and by Lemma 5, $(p, \text{disc.} K) = 1$. As $R/pR$ is finite, in view of Lemmas 2 and 6, it suffices to prove that $x \in R, x^p \in pR \Rightarrow x \in pR$. Thus let $x \in R, x^p \in pR$. Then $x^p \in pO$. As $(p, \text{disc.} K) = 1$, by Lemma 3 and Lemma 6, $x \in pO$. Let $\theta_1, \ldots, \theta_N$ and $\alpha_1, \ldots, \alpha_N$ be bases of $O$ and $R$ respectively, chosen as in Lemma 4. As $x \in R$, let $x = \sum_{i=1}^N a_i\alpha_i$. Then $x = \sum_{i=1}^N a_i f_i\theta_i$. As $x \in pO$, there is $b_i \in Z$ such that $a_i f_i = p b_i \ (1 \leq i \leq N)$. As $(p, \text{disc.} R) = 1$, by Lemma 5, $(p, f_i) = 1$, so $p \ | \ a_i$ for each $i$. Hence $x \in pR$.

($\Rightarrow$) Suppose $(k, \text{disc.} R) \neq 1$. Let $p$ be a prime such that $p \ | \ (k, \text{disc.} R)$. Now, $\text{disc.} R = (f_1 \cdots f_N)^2 \text{disc.} K$.

Case (i). Suppose $(p, f_i) = 1$ for all $1 \leq i \leq N$. Then $p \mid \text{disc.} K$.

Assume, for contradiction, that every matrix in $M_nR$ is a sum of $k$-th powers. Then by Lemma 2, every element of $R$ is a $p$-th power mod $pR$, say $\alpha_i \equiv \gamma_i^p$ (mod $pR$). Let $b_i, c_i \in Z$ such that $1 = b_i p + c_i f_i$. Then $\theta_i = b_i p \theta_i + c_i f_i \theta_i \equiv c_i \alpha_i \equiv c_i \gamma_i^p$ (mod $pO$) (noting that $c_i \equiv c_i^p$ (mod $pZ$)). Thus if $x = \sum_{i=1}^N a_i \theta_i \in O$ with $a_i \in Z$, then $x \equiv (\sum a_i c_i \gamma_i)^p$ (mod $pO$). This gives $(p, \text{disc.} K) = 1$, by Lemma 3. Contradiction.

Case (ii). Suppose $p \mid f_j$ for some $j$. Due to the choice of the $f_j$’s as in Lemma 4, we have $f_1 \mid f_2 \mid \cdots \mid f_N$, so $p \mid f_N$. Also, $f_N \theta_i \in R$ for all $1 \leq i \leq N$, and so $f_N \alpha \in R$, for every $\alpha \in O$. In particular $\beta = f_N(f_N^{p-2} \gamma_N^p) \in R$. As $p \mid f_N, \alpha_N^p = f_N \beta \in pR$. However, $\alpha_N \in pR$, as $\alpha_1, \ldots, \alpha_N$ is a $Z$-basis of $R$. Hence from Lemma 2 it follows that there are matrices in $M_nR$ that are not sums of $k$-th powers in $M_nR$. \hfill $\square$

Remark 1. Let $(k, \text{disc.} R) > 1$. Let $p$ be the smallest prime divisor of $(k, \text{disc.} R)$. Then, for every $n \geq p$, there are $n \times n$ matrices which are not sums of $p$-th powers, and hence which are not sums of $k$-th powers in $M_nR$. \hfill $\square$

Remark 2. Combining Theorem A and Theorem 1, we see that for an order $R$, if $\text{disc.} R$ is odd (i.e. $\equiv 1$ (mod 4)), then for every $n \geq 2$, every matrix in $M_nR$ is a sum of three squares. Also, if $\text{disc.} R$ is even (i.e. $\equiv 0$ (mod 4)), then for every $n \geq 2$, there are matrices in $M_nR$ which are not sums of squares in $M_nR$. \hfill $\square$
Corollary 3. Let $m$ be a squarefree integer, and $f$ denote a positive integer. If $m \equiv 1 \pmod{4}$, the orders of $Q(\sqrt{m})$ are $R_f = \mathbb{Z} + f((1 + \sqrt{m})/2)\mathbb{Z}$. If $m \equiv 2, 3 \pmod{4}$, the orders are $R_f = \mathbb{Z} + f\sqrt{m}\mathbb{Z}$. Then for $n \geq k \geq 2$ every $n \times n$ matrix over $M_n R_f$ is a sum of (seven) $k$-th powers if and only if $(k, fm) = 1$ and either (i) $k$ is odd or (ii) $k$ is even and $m \equiv 1 \pmod{4}$.

Proof. If $m \equiv 1 \pmod{4}, disc. R_f = f^2m$.

If $m \equiv 2, 3 \pmod{4}, disc. R_f = 4f^2m$. □

Example 1. $Disc.\mathbb{Z}[i\sqrt{m}] = 4m$, when $m$ is not a perfect square. Hence for every $n \geq 2$, there are matrices over $\mathbb{Z}[i\sqrt{m}]$ which are not sums of squares in $M_n\mathbb{Z}[i\sqrt{m}]$ (although they have to be sums of three squares in $M_n Q(\sqrt{m})$).

Example 2. $Disc.\mathbb{Z}[i] = -4$, so for every $n \geq 2$, there are $n \times n$ matrices over $\mathbb{Z}[i]$, which are not sums of squares. Hence for $k$ even, for every $n \geq 2$, there are $n \times n$ matrices over $\mathbb{Z}[i]$ which are not sums of $k$-th powers. However, for $k$ odd, for every $n \geq k$, every $n \times n$ matrix over $\mathbb{Z}[i]$ is a sum of seven $k$-th powers.

References


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