On Rédei matrices with minimal rank

Yutaka SUEYOSHI

Abstract. The 4-rank of the narrow ideal class groups of quadratic number fields can be computed from the rank of certain \( \{0, 1\} \)-matrices defined by Rédei. A lower bound of the rank of Rédei’s matrices was also given by Rédei. In this paper, we give a characterization of Rédei’s matrices with minimal rank.

1 Introduction

Let \( k \) be a quadratic number field and \( d \) the discriminant of \( k \). In [4], Rédei gave an upper bound of the narrow 4-class rank of \( k \) (i.e. the 4-rank of the narrow ideal class group of \( k \)), in terms of the numbers of the positive and the negative prime discriminants contained in \( d \). More precisely, for a prime number \( p \), let \( p^* = (-1)^{(p-1)/2} p \) \((p \neq 2, -4, 8 \) or \(-8 \) \( p = 2 \)) denote the prime discriminants and let \( d = p_1^* \cdots p_s^* \cdot p_{s+1}^* \cdots p_{s+t}^* \) be the unique decomposition of \( d \) into a product of prime discriminants, where \( p_1^*, \cdots, p_s^* \) are positive and \( p_{s+1}^* \cdots, p_{s+t}^* \) are negative. Let \( r_4^+(k) \) denote the narrow 4-class rank of \( k \). Then Rédei’s theorem reads as follows:

\[
r_4^+(k) \leq s + \left\lfloor \frac{t-1}{2} \right\rfloor.
\]

Define the Rédei matrix \( R_k = (a_{ij}) \in \mathbf{M}_{(s+t)\times(s+t)}(\mathbb{Z}/2\mathbb{Z}) \) by

\[
(-1)^{a_{ij}} = \begin{cases} 
\left( \frac{p_i^*}{p_j} \right) & (i \neq j), \\
\left( \frac{d/p_i^*}{p_i} \right) & (i = j),
\end{cases}
\]

where \( \left( \frac{D}{p} \right) \) denotes the Kronecker symbol. Since \( r_4^+(k) = s + t - 1 - \text{rank} \ R_k \ [3, 5, 6] \), Rédei’s theorem is equivalent to the inequality

\[
\text{rank} \ R_k \geq t - 1 - \left\lfloor \frac{t-1}{2} \right\rfloor = \left\lfloor \frac{t}{2} \right\rfloor.
\]

We say the Rédei matrix \( R_k \) has minimal rank, if the equality \( \text{rank} \ R_k = \left\lfloor \frac{t}{2} \right\rfloor \) holds. In the case where \( d = p_1^* \cdots p_s^* \) and \( p_i^* \)'s are congruent to 3 \((\text{mod } 4) \) (i.e. \( s = 0 \) and \( p_i^* \)'s are congruent to 3 \((\text{mod } 4) \) \( 2 \).

AMS subject classification: Primary: 11R29; secondary: 11R11.
Key words and phrases: Class group, 4-rank, quadratic fields, Rédei matrix.
odd), Kingan gave a characterization of the Rédei matrices with minimal rank as follows.

**Theorem (Kingan[2]).** Suppose that $s = 0$ and $p_i$'s are odd. Then $R_k$ has minimal rank if and only if the equality $R_k^2 = R_k$ holds.

In this paper, we give a characterization of the Rédei matrices with minimal rank, in the general case.

## 2 A characterization of Rédei matrices

In this section, we give a characterization of Rédei matrices. We say a square matrix $A = (a_{ij}) \in \text{M}_{t \times t}(\mathbb{Z}/2\mathbb{Z})$ is **antisymmetric** if $a_{ij} + a_{ji} = 1$ for all $i \neq j$. If we denote by $I_t$ the $t \times t$ identity matrix and by $J_t$ the $t \times t$ matrix each of whose entries equals 1, then $A$ is antisymmetric if and only if $A + {}^tA = I_t + J_t$.

Let $k$ and $d = p_1^* \cdots p_s^* p_{s+1}^* \cdots p_{s+t}^*$ be as in §1. By the definition of the Rédei matrix, the sum of all rows of $R_k$ is equal to the zero vector $0 = (0, \cdots, 0) \in (\mathbb{Z}/2\mathbb{Z})^{s+t}$ (row vectors with $s + t$ entries).

**Proposition.** (1) Let $k$ and $d = p_1^* \cdots p_s^* t$ be as above. If $-4 \notin \{p_{s+1}^*, \cdots, p_{s+t}^*\}$, then

$$R_k = \begin{pmatrix}
C & {}^tB \\
B & A
\end{pmatrix},$$

where $C \in \text{M}_{s \times s}(\mathbb{Z}/2\mathbb{Z})$ is symmetric, $A \in \text{M}_{t \times t}(\mathbb{Z}/2\mathbb{Z})$ is antisymmetric and $B \in \text{M}_{t \times s}(\mathbb{Z}/2\mathbb{Z})$. If $-4 \in \{p_{s+1}^*, \cdots, p_{s+t}^*\}$, then, by changing the order of $p_{s+i}$'s, we can assume that $p_{s+t}^* = -4$. In this case, we have

$$R_k = \begin{pmatrix}
C & {}^tB & {}^tc \\
B & A & {}^tb \\
0_s & 1_{t-1} & a
\end{pmatrix},$$

where $C \in \text{M}_{s \times s}(\mathbb{Z}/2\mathbb{Z})$ is symmetric, $A \in \text{M}_{(t-1) \times (t-1)}(\mathbb{Z}/2\mathbb{Z})$ is antisymmetric, $B \in \text{M}_{(t-1) \times s}(\mathbb{Z}/2\mathbb{Z})$, $0_s = (0, \cdots, 0) \in (\mathbb{Z}/2\mathbb{Z})^s$, $1_{t-1} = (1, \cdots, 1) \in (\mathbb{Z}/2\mathbb{Z})^{t-1}$, $c \in (\mathbb{Z}/2\mathbb{Z})^s$, $b \in (\mathbb{Z}/2\mathbb{Z})^{t-1}$ and $a \in \mathbb{Z}/2\mathbb{Z}$.

(2) Conversely, let $R \in \text{M}_{(s+t) \times (s+t)}(\mathbb{Z}/2\mathbb{Z})$ be such that the sum of all its rows is equal to the zero vector. If $R$ has the form

$$R = \begin{pmatrix}
C & {}^tB \\
B & A
\end{pmatrix},$$

where $C \in \text{M}_{s \times s}(\mathbb{Z}/2\mathbb{Z})$ is symmetric, $A \in \text{M}_{t \times t}(\mathbb{Z}/2\mathbb{Z})$ is antisymmetric and $B \in \text{M}_{t \times s}(\mathbb{Z}/2\mathbb{Z})$, then there exist infinitely many quadratic fields $k$ such that $R_k = R$ and $-4$ is not contained in the prime discriminants of $k$. On the other hand, if $R$ has the form
\[
R = \begin{pmatrix}
C & tB & tC \\
B & A & tB \\
0_s & 1_{t-1} & a
\end{pmatrix},
\]

where \(C \in M_{s \times s}(\mathbb{Z}/2\mathbb{Z})\) is symmetric, \(A \in M_{(t-1) \times (t-1)}(\mathbb{Z}/2\mathbb{Z})\) is antisymmetric, \(B \in M_{(t-1) \times s}(\mathbb{Z}/2\mathbb{Z})\), \(c \in (\mathbb{Z}/2\mathbb{Z})^s\), \(b \in (\mathbb{Z}/2\mathbb{Z})^{t-1}\) and \(a \in \mathbb{Z}/2\mathbb{Z}\), then there exist infinitely many quadratic fields \(k\) such that \(R_k = R\) and \(-4\) is contained in the prime discriminants of \(k\).

**Proof.** (1) The assertion follows from the quadratic reciprocity law.
(2) The assertion follows from Dirichlet’s arithmetic progression theorem. \(\square\)

### 3 A lower bound of the rank of Rédei matrices

In this section, using Proposition in §2, we give a simple proof of Rédei’s theorem on the lower bound of the rank of Rédei matrices. In the case where \(s = 0\) and \(p_i\)’s are odd, a similar proof can be found in Lemma 3.2 in [1].

**Theorem (Rédei[4]).** Let \(k\) and \(d = p_1^{t_1}\cdots p_s^{t_s}\cdot p_{s+1}^{t_{s+1}}\cdots p_{s+t}^{t_{s+t}}\) be as in §1. Then

\[
\text{rank } R_k \geq \left\lfloor \frac{t}{2} \right\rfloor.
\]

**Proof.** First, assume that \(-4 \notin \{p_{s+1}^{t_{s+1}}, \ldots, p_{s+t}^{t_{s+t}}\}\). Then, by Proposition, we have

\[
R_k = \begin{pmatrix}
C & tB \\
B & A \\
0_s & 1_{t-1} & a
\end{pmatrix},
\]

where \(C, B\) and \(A\) are as in Proposition. Since

\[
\text{rank } (A + tA) = \text{rank } (I_t + J_t) = \begin{cases}
t & (t : \text{even}) \\
t - 1 & (t : \text{odd})
\end{cases}
\]

and \(\text{rank } (A + tA) \leq \text{rank } A + \text{rank } tA = 2 \text{rank } A\), we obtain \(\text{rank } R_k \geq \text{rank } A \geq \left\lfloor \frac{t}{2} \right\rfloor\).

Next, assume that \(p_{s+t}^{t_{s+t}} = -4\). Then, by Proposition, we have

\[
R_k = \begin{pmatrix}
C & tB & tC \\
B & A & tB \\
0_s & 1_{t-1} & a
\end{pmatrix},
\]

where \(C, B, A, c, b\) and \(a\) are as in Proposition. In this case, we have

\[
\text{rank } R_k \geq \text{rank } \begin{pmatrix}
C & tB & tO_s \\
B & A & tO_{t-1} \\
0_s & 1_{t-1} & 0
\end{pmatrix} \geq \left\lfloor \frac{t}{2} \right\rfloor,
\]

3
because \( \begin{pmatrix} A & t0_{t-1} \\ 1_{t-1} & 0 \end{pmatrix} \) is antisymmetric. \( \square \)

4 Rédei matrices with minimal rank

In this section, we give a characterization of the Rédei matrices with minimal rank, in the general case.

**Theorem.** Let \( k \) and \( d = p_1^* \cdots p_s^* \cdot p_{s+1}^* \cdots p_{s+t}^* \) be as in §1. If \(-4 \not\in \{p_{s+1}^*, \ldots, p_{s+t}^*\}\) and

\[
R_k = \begin{pmatrix} C & tB \\ B & A \end{pmatrix},
\]

where \( C \in M_{s \times s}(\mathbb{Z}/2\mathbb{Z}) \) is symmetric, \( A \in M_{t \times t}(\mathbb{Z}/2\mathbb{Z}) \) is antisymmetric and \( B \in M_{t \times s}(\mathbb{Z}/2\mathbb{Z}) \), then \( R_k \) has minimal rank if and only if the equalities

\[
C = O, \quad B = O \quad \text{and} \quad A^2 = A.
\]

hold. If \( p_{s+t}^* = -4 \) and

\[
R_k = \begin{pmatrix} C & tB & tC \\ B & A & \hat{t}b \\ 0_s & \hat{t}b & a \end{pmatrix},
\]

where \( C \in M_{s \times s}(\mathbb{Z}/2\mathbb{Z}) \) is symmetric, \( A \in M_{(t-1) \times (t-1)}(\mathbb{Z}/2\mathbb{Z}) \) is antisymmetric, \( B \in M_{(t-1) \times s}(\mathbb{Z}/2\mathbb{Z}) \), \( c \in (\mathbb{Z}/2\mathbb{Z})^s \), \( \hat{b} \in (\mathbb{Z}/2\mathbb{Z})^{t-1} \) and \( a \in \mathbb{Z}/2\mathbb{Z} \), then \( R_k \) has minimal rank if and only if the equalities

\[
C = O, \quad B = O, \quad c = 0_s, \quad A^2 = A
\]

hold and \( \begin{pmatrix} \hat{t}b \\ a \end{pmatrix} \) is a linear combination of the column vectors of \( \begin{pmatrix} A \\ 1_{t-1} \end{pmatrix} \).

**Proof.** First, assume that \(-4 \not\in \{p_{s+1}^*, \ldots, p_{s+t}^*\}\). For any matrix \( M \), we denote by \( c(M) \) and \( r(M) \) the column space and the row space of \( M \), respectively. Since

\[
0 \leq \dim(c(A) \cap c(tA)) = \dim(c(A) + c(tA)) - \dim(c(A) + c(tA)) \leq 2 \text{ rank } A - \dim(c(A) + tA) = 2 \text{ rank } A - \text{ rank } (J_t + J_t) = \begin{cases} 2 \text{ rank } A - t & (t : \text{ even}), \\
2 \text{ rank } A - (t - 1) & (t : \text{ odd}), 
\end{cases}
\]

4
we have
\[
\text{rank } R_k \geq \text{rank } A \geq \left\{ \begin{array}{c}
\frac{t}{2} & (t \text{ : even}) \\
\frac{t-1}{2} & (t \text{ : odd})
\end{array} \right\} = \left\lceil \frac{t}{2} \right\rceil.
\]

If \( R_k \) has minimal rank, then we have
\[
\text{rank } R_k = \text{rank } A = \left\lceil \frac{t}{2} \right\rceil
\]
and therefore \( c(A) \cap c(\tilde{t}A) = \{\tilde{t}0_t\} \). Furthermore, it follows from \( \text{rank } R_k = \text{rank } A \) that \( c(B) \subset c(A) \) and \( r(\tilde{t}B) \subset r(A) \). Hence we have \( c(B) \subset c(A) \cap c(\tilde{t}A) = \{\tilde{t}0_t\} \). This implies that \( B = O \) and \( C = O \). On the other hand, since \( \tilde{t}A = A + I_t + J_t \), we have \( \tilde{t}A \cdot A = A^2 + A + J_tA = A^2 + A \). However, the column vector of \( \tilde{t}A \cdot A \) is contained in \( c(\tilde{t}A) \) and the column vector of \( A^2 + A \) is contained in \( c(A) \). Hence we have \( \tilde{t}A \cdot A = A^2 + A = O \), i.e. \( A^2 = A \). Conversely, if \( C = O \), \( B = O \) and \( A^2 = A \), then it follows from the discussion above that \( \tilde{t}A \cdot A = O \). This implies that \( \text{rank } A \leq t - \text{rank } \tilde{t}A \). Hence we have \( \text{rank } A \leq \left\lfloor \frac{t}{2} \right\rfloor \)
and therefore \( \text{rank } R_k = \text{rank } A = \left\lfloor \frac{t}{2} \right\rfloor \).

Next, assume that \( p_{s+t}^* = -4 \). If \( R_k \) has minimal rank, then, in the inequalities
\[
\text{rank } R_k \geq \text{rank } \begin{pmatrix} C & \tilde{t}B & \tilde{t}0_s \\ B & A & \tilde{t}0_{t-1} \\ 0_s & 1_{t-1} & 0 \end{pmatrix} \geq \left\lceil \frac{t}{2} \right\rceil,
\]
the equalities hold. Hence the antisymmetric matrix \( \begin{pmatrix} A & \tilde{t}0_{t-1} \\ 1_{t-1} & 0 \end{pmatrix} \) also has minimal rank. Therefore, as in the discussion above, we obtain \( B = O \), \( C = O \), \( c = 0_s \) and
\[
\begin{pmatrix} A & \tilde{t}0_{t-1} \\ 1_{t-1} & 0 \end{pmatrix}^2 = \begin{pmatrix} A & \tilde{t}0_{t-1} \\ 1_{t-1} & 0 \end{pmatrix}.
\]
In particular, we have \( A^2 = A \). Furthermore, \( \begin{pmatrix} \tilde{t}b \\ a \end{pmatrix} \) is a linear combination of the column vectors of \( \begin{pmatrix} A \\ 1_{t-1} \end{pmatrix} \). The converse is easy. \( \square \)

References


Department of Computer and Information Sciences
Faculty of Engineering, Nagasaki University
1-14 Bunkyo-machi, Nagasaki 852-8521
Japan
e-mail: sueyoshi@net.nagasaki-u.ac.jp