Palestine Journal of Mathematics

Vol. 4(2) (2015) , 271–276

Approach to Square Roots Applying Square Matrices

H. Méndez-Delgadillo, P. Lam-Estrada and M. R. Maldonado-Ramírez

Communicated by Jose Luis López-Bonilla

MSC 2010 Classifications: Primary 15B36; Secondary 97I30, 13G05.

Keywords and phrases: sequences of rational numbers, 2×2 matrices, integral domain.

All the authors wish to thanks SNI, México, and COFAA-IPN, México.

Abstract. Let m be a square free positive integer. If $a+b\sqrt{m}$ is a unit of the integral domain $\mathbb{Z}[\sqrt{m}\,]$ and A is the 2×2 matrix corresponding to $a+b\sqrt{m}$, then we obtain two sequences of rational numbers $\{a_n\}_{n\in\mathbb{N}}$ and $\{b_n\}_{n\in\mathbb{N}}$ such that $\lim\limits_{n\to\infty} \dfrac{a_n}{b_n} = \sqrt{m}$, where a_n and b_n are the entries of the first column of A^n.

1 Introduction

Let m be a square free integer. We consider the integral domain $\mathbb{Z}[\sqrt{m}\,] = \{a+b\sqrt{m} \mid a, b \in \mathbb{Z}\}$. The **norm** function of $\mathbb{Z}[\sqrt{m}\,]$ is the function $N : \mathbb{Z}[\sqrt{m}\,] \longrightarrow \mathbb{Z}$ given by $N(a+b\sqrt{m}\,) := (a+b\sqrt{m}\,)(a-b\sqrt{m}\,) = a^2 - b^2m$, for each $a+b\sqrt{m} \in \mathbb{Z}[\sqrt{m}\,]$. We have the following properties for the norm:

For each $a+b\sqrt{m}$, $c+d\sqrt{m} \in \mathbb{Z}[\sqrt{m}\,]$

(i) $N((a+b\sqrt{m}\,)(c+d\sqrt{m}\,)) = N(a+b\sqrt{m}\,)N(c+d\sqrt{m}\,)$ (The norm is multiplicative).

(ii) $a+b\sqrt{m}$ is a unit if and only if $N(a+b\sqrt{m}\,) = \pm 1$, that is, $a^2 - b^2m = \pm 1$.

When $m < -1$, the multiplicative group of units $\mathbb{Z}[\sqrt{m}\,]^*$ consists only of 1 and -1; if $m = -1$, the units are 1, -1, i and $-i$, in this case $\mathbb{Z}[\,i\,]$ is the integral domain of **Gaussian integers**. If $m > 1$, then $\mathbb{Z}[\sqrt{m}\,]$ has an infinity of units, because $X^2 - mY^2 = \pm 1$ is the Pell's equation which has an infinity of integer solutions (see [5]). Further, if $a+b\sqrt{m}$ is a unit, then $(a+b\sqrt{m}\,)^n$ is also a unit.

We denote by $\mathfrak{M}_{2\times 2}(\mathbb{Z})$ the set of all 2×2 matrices with integer entries. Let $GL_2(\mathbb{Q})$ be the multiplicative group of invertible 2×2 matrices with rational entries, which is called the **general lineal group of degree** 2 **over** $\mathbb{Q}$. The subset of all matrices of $GL_2(\mathbb{Q})$ with determinant 1 is a normal subgroup of $GL_2(\mathbb{Q})$ called the **special lineal group of degree** 2 **over** $\mathbb{Q}$ and denoted by $SL_2(\mathbb{Q})$.

For each $\lambda \in \mathbb{Q}$, let

$$G_\lambda = \left\{ A \in GL_2(\mathbb{Q}) \,\middle|\, A = \begin{bmatrix} a & b\lambda \\ b & a \end{bmatrix} \right\}$$

and let

$$L_\lambda = \{A \in G_\lambda \mid \det(A) = \pm 1\}.$$

On the other hand, let m be a square free integer and let

$$T_m = \left\{ A \in \mathfrak{M}_{2\times 2}(\mathbb{Z}) \,\middle|\, A = \begin{bmatrix} a & bm \\ b & a \end{bmatrix} \right\}.$$

In this paper we study some of the properties of G_λ, L_λ and T_m. We obtain the field of quotients of T_m. Finally, if m is a square free positive integer and $a+b\sqrt{m}$ is a unit of $\mathbb{Z}[\sqrt{m}\,]$, then we obtain two sequences of rational numbers $\{a_n\}_{n\in\mathbb{N}}$ and $\{b_n\}_{n\in\mathbb{N}}$ such that $\lim\limits_{n\to\infty} \dfrac{a_n}{b_n} = \sqrt{m}$, where a_n and b_n are the entries of the first column of A^n, with $A = \begin{bmatrix} a & bm \\ b & a \end{bmatrix}$.

2 Square matrices corresponding to units of the integral domain $\mathbb{Z}[\sqrt{m}\,]$

With the previous notation, we have the following results.

Theorem 2.1. *If $\lambda \in \mathbb{Q}$, then*

(i) *G_λ is an abelian subgroup of $GL_2(\mathbb{Q})$;*

(ii) *$G_\lambda \cap SL_2(\mathbb{Q})$ is a subgroup of G_λ;*

(iii) *L_λ is a subgroup of G_λ containing to subgroup $G_\lambda \cap SL_2(\mathbb{Q})$;*

(iv) *$G_\lambda \cap SL_2(\mathbb{Q})$ is a subgroup of L_λ of index 2.*

Proof. (i): Since the determinant function is multiplicative, it is sufficient to note that for each A and B elements of G_λ, with

$$A = \begin{bmatrix} a & b\lambda \\ b & a \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} c & d\lambda \\ d & c \end{bmatrix},$$

we have

$$AB = \begin{bmatrix} ac + bd\lambda & (ad + bc)\lambda \\ ad + bc & ac + bd\lambda \end{bmatrix} = BA \quad \text{and} \quad A^{-1} = \frac{1}{a^2 - b^2\lambda} \begin{bmatrix} a & -b\lambda \\ -b & a \end{bmatrix}.$$

(ii) and (iii): They are obvious.

(iv): Applying the determinant function, we have det : $L_\lambda \longrightarrow \{-1,\ 1\}$ is an epimorphism whose kernel is the subgroup $G_\lambda \cap SL_2(\mathbb{Q})$ of L_λ. Then the affirmation follows from First Isomorphism Theorem. □

Theorem 2.2. *If $\lambda \in \mathbb{Z}$, then*

(i) *$G_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$ is an abelian monoid;*

(ii) *$L_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$ is a submonoid of $G_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$;*

(iii) *The elements of $L_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$ are the invertible elements of the monoid $G_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$;*

(iv) *$L_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$ is a multiplicative group.*

Proof. (i) and (ii) are immediate. (iv) follows from (ii) and (iii). Therefore, we will prove (iii). Let $A \in G_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$ be an invertible element. We write

$$A = \begin{bmatrix} a & b\lambda \\ b & a \end{bmatrix},$$

where $a, b \in \mathbb{Z}$. Then, since $A^{-1} \in G_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$, we have $a/\det(A)$ and $b/\det(A)$ are integers. Let $t_1,\ t_2 \in \mathbb{Z}$ be such that $a = \det(A)t_1$ and $b = \det(A)t_2$. Hence,

$$\begin{aligned} \det(A) &= a^2 - b^2\lambda = \det(A)^2 t_1^2 - \det(A)^2 t_2^2 \lambda \\ &= \det(A)^2 (t_1^2 - t_2^2\lambda). \end{aligned}$$

This implies that $\det(A)(t_1^2 - t_2^2\lambda) = 1$; accordingly, $\det(A) = \pm 1$. Therefore, $A \in L_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$. Finally, since each element of $L_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$ is an invertible element of $G_\lambda \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$, theorem is proved. □

Theorem 2.3. *If m is a square free integer, then*

(i) *T_m is a commutative subring with identity of $\mathfrak{M}_{2\times 2}(\mathbb{Z})$;*

(ii) *If T_m^* is the multiplicative group of units of T_m, then $T_m^* = L_m \cap \mathfrak{M}_{2\times 2}(\mathbb{Z})$. In particular, T_m^* is a subgroup of L_m.*

(iii) *the rings T_m and $\mathbb{Z}[\sqrt{m}\,]$ are isomorphic. In particular, T_m is an integral domain;*

(iv) *the isomorphism in (iii) induces an isomorphism between the multiplicative groups T_m^* and $(\mathbb{Z}[\sqrt{m}\,])^*$;*

(v) $T_m/(T_m \cap SL_2(\mathbb{Q})) \cong \{-1,\ 1\}$.

Proof. (i): It is clear.

(ii): It follows from Theorem 2.2, (iii).

(iii): The isomorphism is given as follows:

$$\begin{array}{cccc} \phi: & T_m & \longrightarrow & \mathbb{Z}[\sqrt{m}\,] \\ & \begin{bmatrix} a & bm \\ b & a \end{bmatrix} & \longmapsto & a + b\sqrt{m}\,. \end{array}$$

(iv): It follows from (iii).

(v): It is a consequence of Theorem 2.1, (iv). □

We can expand the field of quotients $\mathbb{Q}(\sqrt{m}\,)$ of $\mathbb{Z}[\sqrt{m}\,]$ as following.

Theorem 2.4. *Let Q_m be the set of all matrices of the form*

$$A = \begin{bmatrix} a & bm \\ b & a \end{bmatrix}$$

with $a, b \in \mathbb{Q}$. Then,

(i) *Q_m is a field isomorphic $\mathbb{Q}(\sqrt{m}\,)$. This is, Q_m is the field of quotients of T_m;*

(ii) *there exists a monomorphism of the multiplicative group $\mathbb{Q}(\sqrt{m}\,)^*$ in $GL_2(\mathbb{Q})$.*

(iii) *The group $GL_2(\mathbb{Q})$ has the chain of subgroups*

$$Q_m^* \cap SL_2(\mathbb{Q}) < L_m < G_m = Q_m^* < GL_2(\mathbb{Q}).$$

Proof. (i): It is straightforward to verify that Q_m is a field with the usual operations, and that the correspondence

$$\begin{bmatrix} a & bm \\ b & a \end{bmatrix} \longrightarrow a + b\sqrt{m}$$

determines an isomorphism between the fields Q_m and $\mathbb{Q}(\sqrt{m}\,)$.

(ii): The inverse correspondence in (i) induces the monomorphism of the multiplicative group $\mathbb{Q}(\sqrt{m}\,)^*$ in $GL_2(\mathbb{Q})$.

(iii): It is immediately. □

3 The Main Results

Theorem 3.1. *If λ is a positive rational number, and $\{a_n\}_{n\in\mathbb{N}}$, $\{b_n\}_{n\in\mathbb{N}}$ are two sequences of positive rational numbers such that $|a_n^2 - b_n^2\lambda| = 1$ for each $n \in \mathbb{N}$ and $\lim_{n\to\infty} a_n = \infty = \lim_{n\to\infty} b_n$, then*

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \sqrt{\lambda} = \lim_{n\to\infty} \frac{b_n}{a_n}\,\lambda.$$

Proof. Since for all $n \in \mathbb{N}$

$$\left|\frac{a_n^2}{b_n^2} - \lambda\right| = \frac{1}{b_n^2} \quad \text{and} \quad \left|1 - \frac{b_n^2}{a_n^2}\,\lambda\right| = \frac{1}{a_n^2}\ ,$$

we have

$$\lim_{n\to\infty} \left|\frac{a_n^2}{b_n^2} - \lambda\right| = \lim_{n\to\infty} \frac{1}{b_n^2} = 0 \quad \text{and} \quad \lim_{n\to\infty} \left|1 - \frac{b_n^2}{a_n^2}\,\lambda\right| = \lim_{n\to\infty} \frac{1}{a_n^2} = 0\,.$$

Hence

$$\lim_{n\to\infty} \left(\frac{a_n^2}{b_n^2} - \lambda\right) = 0 \quad \text{and} \quad \lim_{n\to\infty} \left(1 - \frac{b_n^2}{a_n^2}\,\lambda\right) = 0\,,$$

equivalently

$$\lim_{n\to\infty} \frac{a_n^2}{b_n^2} = \lambda = \lim_{n\to\infty} \frac{b_n^2}{a_n^2}\, \lambda^2 \,.$$

Therefore,

$$\lim_{n\to\infty} \frac{a_n}{b_n} = \sqrt{\lambda} = \lim_{n\to\infty} \frac{b_n}{a_n}\, \lambda \,.$$

□

Let x be an arbitrary real number. The **integral part** of x is the greatest integer n such that $n \leq x < n+1$ and is denoted by $\lfloor x \rfloor$, this is $\lfloor x \rfloor$ is the integer number so that $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Theorem 3.2. *Let m be a square free integer, and*

$$A = \begin{bmatrix} a & bm \\ b & a \end{bmatrix} \in Q_m$$

where a, b are two rational numbers. Then the powers of A, A^n with $n \in \mathbb{N}$, are given as follows:

$$A^n = \begin{bmatrix} a_n & b_n m \\ b_n & a_n \end{bmatrix}$$

where

$$a_n = \begin{cases} \displaystyle\sum_{0\leq t\leq \frac{n}{2}} \binom{n}{2t} a^{2t} b^{n-2t} m^{\frac{n}{2}-t} & \text{if } n \text{ even} \\ \displaystyle\sum_{0\leq t\leq \frac{n-1}{2}} \binom{n}{2t+1} a^{2t+1} b^{n-2t-1} m^{\frac{n-1}{2}-t} & \text{if } n \text{ odd} \end{cases} \tag{3.1}$$

and

$$b_n = \begin{cases} \displaystyle\sum_{0\leq t\leq \frac{n-2}{2}} \binom{n}{2t+1} a^{2t+1} b^{n-2t-1} m^{\frac{n-2}{2}-t} & \text{if } n \text{ even} \\ \displaystyle\sum_{0\leq t\leq \frac{n-1}{2}} \binom{n}{2t} a^{2t} b^{n-2t} m^{\frac{n-1}{2}-t} & \text{if } n \text{ odd} \end{cases} \tag{3.2}$$

Proof. By induction, it has that the powers of A are of the form

$$A^n = \begin{bmatrix} a_n & b_n m \\ b_n & a_n \end{bmatrix} \in Q_m$$

for all $n \in \mathbb{N}$. On the other hand, if $n \in \mathbb{N}$, then we have

$$\begin{aligned} (a + b\sqrt{m}\,)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} (\sqrt{m}\,)^{n-k} \\ &= \sum_{0\leq t\leq \lfloor \frac{n}{2} \rfloor} \binom{n}{2t} a^{2t} b^{n-2t} (\sqrt{m}\,)^{n-2t} \\ &\quad + \sum_{0\leq t\leq \lfloor \frac{n-1}{2} \rfloor} \binom{n}{2t+1} a^{2t+1} b^{n-2t-1} (\sqrt{m}\,)^{n-2t-1} \end{aligned} \tag{3.3}$$

More precisely, if n is even number, then

$$(a+b\sqrt{m}\,)^n = \sum_{0\le t\le \frac{n}{2}} \binom{n}{2t} a^{2t} b^{n-2t} m^{\frac{n}{2}-t} + \left(\sum_{0\le t\le \frac{n-2}{2}} \binom{n}{2t+1} a^{2t+1} b^{n-2t-1} m^{\frac{n-2}{2}-t} \right) \sqrt{m} \tag{3.4}$$

and if n is odd number now it has

$$(a+b\sqrt{m}\,)^n = \sum_{0\le t\le \frac{n-1}{2}} \binom{n}{2t+1} a^{2t+1} b^{n-2t-1} m^{\frac{n-1}{2}-t} + \left(\sum_{0\le t\le \frac{n-1}{2}} \binom{n}{2t} a^{2t} b^{n-2t} m^{\frac{n-1}{2}-t} \right) \sqrt{m} \tag{3.5}$$

If ψ is the isomorphism of the Theorem 2.4, (i), between the fields Q_m and $\mathbb{Q}(\sqrt{m}\,)$, then

$$\begin{aligned}(a+b\sqrt{m}\,)^n &= \psi(A)^n = \psi(A^n) = \psi\left(\begin{bmatrix} a_n & b_n m \\ b_n & a_n \end{bmatrix}\right) \\ &= a_n + b_n\sqrt{m}.\end{aligned}$$

Therefore the theorem holds of the equations (3.4) and (3.5). □

Theorem 3.3. *Let m be a square free positive integer and*

$$A = \begin{bmatrix} a & bm \\ b & a \end{bmatrix} \in Q_m$$

where a, b are two positive rational numbers and the powers of A are given as follows:

$$A^n = \begin{bmatrix} a_n & b_n m \\ b_n & a_n \end{bmatrix}$$

for all $n \in \mathbb{N}$. If $\det(A) = \pm 1$, then

(i) $\det(A^n) = \pm 1$ *for each $n \in \mathbb{N}$. This is, $|a_n^2 - b_n^2 m| = 1$ for each $n \in \mathbb{N}$;*

(ii) $\lim\limits_{n\to\infty} a_n = \infty = \lim\limits_{n\to\infty} b_n$*;*

(iii) $\lim\limits_{n\to\infty} \dfrac{a_n}{b_n} = \sqrt{m} = \lim\limits_{n\to\infty} \dfrac{b_n m}{a_n}$.

Proof. (i): Applying induction, it is sufficient to observe that the determinant function is multiplicative.

(ii): It follows of Theorem 3.2, because a y b are positive rational numbers.

(iii): It is a consequence of Theorem 3.1. □

4 Example

Taking $m = 2$, we have $1+\sqrt{2} \in \mathbb{Z}[\sqrt{2}\,]$ is a unit with $N(1+\sqrt{2}\,) = -1$. The matrix corresponding to $1+\sqrt{2}$ is

$$A = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$$

where

$$A^2 = \begin{bmatrix} 3 & 4 \\ 2 & 3 \end{bmatrix},\ A^3 = \begin{bmatrix} 7 & 10 \\ 5 & 7 \end{bmatrix},\ A^4 = \begin{bmatrix} 17 & 24 \\ 12 & 17 \end{bmatrix}, \ldots,\ A^n = \begin{bmatrix} a_n & 2b_n \\ b_n & a_n \end{bmatrix}, \ldots$$

Thus, the sequences whose terms are

$$1,\ 3/2,\ 7/5,\ 17/12, \ldots, a_n/b_n, \ldots \text{ and } 2,\ 4/3,\ 10/7,\ 24/17, \ldots, 2b_n/a_n, \ldots,$$

they are converging to $\sqrt{2}$.

References

[1] D.M. Burton, *A first course in rings and ideals*, Addison-Wesley, 1970.

[2] T.W. Hungerford, *Algebra*, Graduate Texts in Mathematics **73**, Springer-Verlag New York, Inc., 1974.

[3] G. Karpilovsky, *Topics in field theory*, Mathematics Studies **155**, Notas de Matemática (124), North-Holland, 1989.

[4] S. Lang, *Algebra*, Graduate Texts in Mathematics **211**, Springer-Verlag New York, Inc., 2002.

[5] I.M. Niven, H.S. Zukermann and H.L. Montgomery, *An introduction to the theory of numbers*, John Wiley & Sons, Inc., 1991.

Author information

H. Méndez-Delgadillo, Departamento de Matemáticas, Escuela Superior de Física y Matemáticas, Instituto Politécnico Nacional; Academia de Matemáticas, Instituto de la Educación Media Superior, México, D. F..
E-mail:

P. Lam-Estrada, Departamento de Matemáticas, Escuela Superior de Física y Matemáticas, Instituto Politécnico Nacional, México, D. F..
E-mail: plam@esfm.ipn.mx

M. R. Maldonado-Ramírez, Departamento de Matemáticas, Escuela Superior de Física y Matemáticas, Instituto Politécnico Nacional, México, D. F..
E-mail: rosalia@esfm.ipn.mx

Received: May 4, 2014.

Accepted: July 11, 2014.