Construction of a Hermitian lattice without a basis of minimal vectors

By Poo-Sung Park

Department of Mathematics Education, Kyungnam University, Changwon 631-701, Republic of Korea

(Communicated by Masaki Kashiwara, m.j.a., April 12, 2012)

Abstract: It is known that infinitely many imaginary quadratic fields allow Hermitian lattices which are generated by minimal vectors but have no basis of minimal vectors. In this article we construct systematically such Hermitian lattices over other imaginary quadratic fields. These lattices are binary and unimodular. This construction requires specific non-principal ideals.

Key words: Hermitian lattice; minimal vector.

Kim and the author [4] found two types of binary free Hermitian lattices which are generated by their minimal vectors, but are not generated by any 3 minimal vectors. It was a variant of Conway-Sloane's answer [1].

However, it has not been analyzed how the Hermitian lattices were constructed yet. In this article, we show the structure of those lattices and construct other lattices of the same property.

Let E denote an imaginary quadratic field $\mathbf{Q}(\sqrt{-m})$ with m squarefree positive integer. Let $\mathcal{O}$ be the ring of algebraic integers in E. Then, $\mathcal{O} = \mathbf{Z}[\omega]$, where $\omega = \sqrt{-m}$ if $m \equiv 1, 2 \pmod 4$ or $\omega = \frac{1+\sqrt{-m}}{2}$ if $m \equiv 3 \pmod 4$.

A Hermitian lattice is an $\mathcal{O}$-module equipped with a Hermitian map. In general, every Hermitian lattice L can be written as

$$L = \mathcal{A}_1\mathbf{v}_1 + \mathcal{A}_2\mathbf{v}_2 + \cdots + \mathcal{A}_n\mathbf{v}_n,$$

where $\mathcal{A}_i$ ideals in $\mathcal{O}$ and $\mathbf{v}_i$ vectors in $E \otimes_{\mathcal{O}} L$.

Those coefficient ideals $\mathcal{A}_i$ and generators $\mathbf{v}_i$ are not uniquely determined, but the product $\prod \mathcal{A}_i = \mathcal{A}_1\mathcal{A}_2\cdots\mathcal{A}_n$ is an invariant of L, which is called the *Steinitz class* [2]. That is, if

$$\begin{aligned} L &= \mathcal{A}_1\mathbf{v}_1 + \mathcal{A}_2\mathbf{v}_2 + \cdots + \mathcal{A}_n\mathbf{v}_n \\ &= \mathcal{B}_1\mathbf{w}_1 + \mathcal{B}_2\mathbf{w}_2 + \cdots + \mathcal{B}_n\mathbf{w}_n, \end{aligned}$$

then $\prod \mathcal{A}_i$ and $\prod \mathcal{B}_i$ are equivalent in the ideal class group $\mathrm{Cl}(E)$. Thus if we can find specific non-principal ideals whose product is principal, we can construct a free lattice generated by more vectors than its rank.

Let $\mathcal{A}$ be an ideal in $\mathcal{O}$. Choose the smallest positive integer a in $\mathcal{A}$ and the smallest positive integer c such that $b + c\omega$ belongs to $\mathcal{A}$ for some integer b. Then, a and c are uniquely determined and b is uniquely determined with $0 \le b < a$. Since c is chosen to be the smallest, if $r\omega \in \mathcal{A}$ for some integer $r \in \mathbf{Z}$, then r should be divisible by c. Similarly, if $s + t\omega$ is in $\mathcal{A}$, both s and t are divisible by c.

Let $(a, b + c\omega)$ denote the ideal generated by a and $b + c\omega$. Similarly, let $[a, b + c\omega]$ denote the $\mathbf{Z}$-module generated by a and $b + c\omega$. The above choice of a, b and c guarantees that $\mathcal{A} = (a, b + c\omega) = [a, b + c\omega]$. Now, we may assume $c = 1$, since $\mathcal{A}\mathbf{v} = (\frac{1}{c}\mathcal{A})(c\mathbf{v})$.

This situation yields the following lemma, which was stated partially in [5, Lemma 1].

Lemma 1. *Let a and b be positive integers. Then $\mathbf{Z}$-module $[a, b + \omega]$ becomes an ideal if and only if a divides $N(b + \omega)$, where $N(\cdot)$ stands for the norm map.*

Proof. It is enough to prove that $[a, b + \omega] \supset (a, b + \omega)$ if $a | N(b + \omega)$.

Let x and y be arbitrary integers. Note that

$$(x + y\omega)a = (x - yb)a + ya(b + \omega)$$

and

$$\begin{aligned} &(x + y\omega)(b + \omega) \\ &\quad = -yN(b + \omega) + (x + by + (\mathrm{Tr}\,\omega)y)(b + \omega), \end{aligned}$$

where $\mathrm{Tr}(\cdot)$ stands for the trace map.

Both are in $[a, b + \omega]$. We are done. □

We need a non-principal ideal of the form $(a, b + \omega)$, so that the ideal satisfies the condition $N(a) = N(b + \omega)$. If a positive integer m is

2000 Mathematics Subject Classification. Primary 11E39; Secondary 11H50.

doi: 10.3792/pjaa.88.75

squarefree and $m \not\equiv 3 \pmod 4$, the condition $N(a) = N(b+\omega)$ implies $m = a^2 - b^2$ and thus $m \equiv 1 \pmod 4$.

Lemma 2. *Let m be a positive squarefree integer and $m \equiv 1 \pmod 4$. Assume that $m = a^2 - b^2$ with $0 < 2b < a$. If $\mathcal{A}$ is an ideal generated by a and $b+\omega$, then $N(\alpha) \geq a^2$ for every $\alpha \in \mathcal{A}$ and thus $\mathcal{A}$ is not principal.*

Proof. Thanks to Lemma 1, we can consider $\mathcal{A}$ as a $\mathbf{Z}$-module $[a, b+\omega]$. For arbitrary integers x and y,

$$\begin{aligned} N(xa + y(b+\omega)) &= (xa + y(b+\omega))(xa + y(b+\overline{\omega})) \\ &= a^2x^2 + 2abxy + b^2y^2 + y^2m \\ &= a(ax^2 + 2bxy + ay^2) \\ &\geq a(2a\sqrt{x^2y^2} + 2bxy) \\ &\geq a^2|xy|, \end{aligned}$$

since $a \geq 2b$. □

If a positive integer m is squarefree and $m \equiv 3 \pmod 4$, the condition $N(a) = N(b+\omega)$ implies $m = (2a)^2 - (2b+1)^2$.

Lemma 3. *Let m be a positive squarefree integer and $m \equiv 3 \pmod 4$. Assume that $m = (2a)^2 - (2b+1)^2$ with $0 < 2b+1 < a$. If $\mathcal{A}$ is an ideal generated by a and $b+\omega$, then $N(\alpha) \geq a^2$ for every $\alpha \in \mathcal{A}$ and thus $\mathcal{A}$ is not principal.*

Proof. Consider a $\mathbf{Z}$-module $[a, b+\omega]$. For arbitrary integers x and y,

$$\begin{aligned} N(xa + y(b+\omega)) &= (xa + y(b+\omega))(xa + y(b+\overline{\omega})) \\ &= a(ax^2 + (1+2b)xy + ay^2) \\ &\geq a(2a\sqrt{x^2y^2} + (1+2b)xy) \\ &\geq a^2|xy|, \end{aligned}$$

since $a \geq 2b+1$. □

We use the above non-principal ideals to construct a free lattice. The following lemma shows such a way, which is an algorithmic version of [3, 81:5], [2, Theorem 2].

Lemma 4. *Given a binary lattice $L = \mathcal{A}_1\mathbf{v}_1 + \mathcal{A}_2\mathbf{v}_2$, there are vectors $\mathbf{w}_1$ and $\mathbf{w}_2$ such that*

$$L = \mathcal{O}\mathbf{w}_1 + \mathcal{O}\mathbf{w}_2$$

if $\mathcal{A}_1\mathcal{A}_2$ is principal.

Proof. Assume that $L = \mathcal{A}_1\mathbf{v}_1 + \mathcal{A}_2\mathbf{v}_2$ and $\mathcal{A}_i = (\alpha_i, \beta_i)\mathcal{O}$. If $\mathcal{A}_1\mathcal{A}_2 = \gamma\mathcal{O}$, then

$$p\alpha_1\alpha_2 + q\alpha_1\beta_2 + r\beta_1\alpha_2 + s\beta_1\beta_2 = \gamma$$

for some $p, q, r, s \in \mathcal{O}$.

Putting

$$\begin{aligned} x_1 &= \alpha_1 \in \mathcal{A}_1, \quad & x_2 &= r\alpha_2 + s\beta_2 \in \mathcal{A}_2, \\ y_1 &= -\beta_1 \in \mathcal{A}_1, \quad & y_2 &= p\alpha_2 + q\beta_2 \in \mathcal{A}_2 \end{aligned}$$

and

$$\begin{pmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{pmatrix},$$

one can verify that $\mathbf{w}_1, \mathbf{w}_2 \in L$ and

$$\begin{aligned} \begin{pmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{pmatrix} &= \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}^{-1} \begin{pmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix} \\ &= \frac{1}{\gamma} \begin{pmatrix} y_2 & -x_2 \\ -y_1 & x_1 \end{pmatrix} \begin{pmatrix} \mathbf{w}_1 \\ \mathbf{w}_2 \end{pmatrix}. \end{aligned}$$

Then

$$\alpha_1\mathbf{v}_1, \beta_1\mathbf{v}_1, \alpha_2\mathbf{v}_2, \beta_2\mathbf{v}_2 \in \mathcal{O}\mathbf{w}_1 + \mathcal{O}\mathbf{w}_2$$

since $\alpha_1\alpha_2, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2 \in \gamma\mathcal{O}$. Therefore

$$L = \mathcal{A}_1\mathbf{v}_1 + \mathcal{A}_2\mathbf{v}_2 = \mathcal{O}\mathbf{w}_1 + \mathcal{O}\mathbf{w}_2.$$

□

The main idea of this article is to convert a binary diagonal lattice with non-principal coefficient ideals into a binary free lattice. Then, four vectors generate the lattice, but three of them cannot generate it.

Theorem 1. *Let m be a positive squarefree integer and $m = a^2 - b^2$ with a odd and b even satisfying $0 < 2b < a$. Choose two integers A and B such that $aA + 2bB = 1$. Then the binary unimodular Hermitian lattice L with Gram matrix*

$$\begin{pmatrix} a(1+B^2) & B + (1+B^2)(-b+\sqrt{-m}) \\ B + (1+B^2)(-b-\sqrt{-m}) & a(1+B^2) + A \end{pmatrix}$$

over $\mathbf{Q}(\sqrt{-m})$ has minimal vectors of squared length a, is generated by its 8 minimal vectors, but is not generated by any 3 minimal vectors.

Proof. Let $\mathcal{A}_1 = (a, b+\sqrt{-m})$ and $\mathcal{A}_2 = (a, b-\sqrt{-m})$. From Lemma 2 the ideals $\mathcal{A}_1$ and $\mathcal{A}_2$ are not principal.

Since $\gcd(a, 2b) = 1$, there exist integers A and B satisfying $aA + 2bB = 1$ and thus $\mathcal{A}_1\mathcal{A}_2 = a\mathcal{O}$.

Let $\mathbf{v}_1$ and $\mathbf{v}_2$ be vectors with

$$\mathbf{v}_1 \cdot \mathbf{v}_1 = \mathbf{v}_2 \cdot \mathbf{v}_2 = \frac{1}{a}, \quad \mathbf{v}_1 \cdot \mathbf{v}_2 = 0.$$

Then $L = \mathcal{A}_1\mathbf{v}_1 + \mathcal{A}_2\mathbf{v}_2$ by letting $p = A, q = r = B, s = 0$ in Lemma 4.

It is clear that L is generated by 8 minimal vectors

$$\pm a\mathbf{v}_1, \quad \pm(b+\sqrt{-m})\mathbf{v}_1, \quad \pm a\mathbf{v}_2, \quad \pm(b-\sqrt{-m})\mathbf{v}_2$$

of squared length a. But any 3 vectors of them cannot generate L. □

The condition of a and b on m can be written as $m = k\ell \equiv 1 \pmod 4$ with $0 < \ell < k < 3\ell$. Then $a = (k+\ell)/2$ and $b = (k-\ell)/2$. For example, when $m = 21 = 7 \times 3$, we obtain a Hermitian lattice from $a = 5$, $b = 2$, $A = 1$, $B = -1$:

$$\begin{pmatrix} 10 & -5+2\sqrt{-21} \\ -5-2\sqrt{-21} & 11 \end{pmatrix}$$

which has minimal vectors of squared length 5 but is not generated by 3 of them.

Theorem 2. *Let m be a positive squarefree integer and $m = (2a)^2 - (2b+1)^2$ with $0 < 2b+1 < a$. Choose two integers A and B such that $aA + (2b+1)B = 1$. Then the binary unimodular Hermitian lattice L with Gram matrix*

$$\begin{pmatrix} a(1+B^2) & B+(1+B^2)(-b-1+\omega) \\ B+(1+B^2)(-b-1+\overline{\omega}) & a(1+B^2)+A \end{pmatrix}$$

over $\mathbf{Q}(\sqrt{-m})$ has minimal vectors of squared length a, is generated by its 8 minimal vectors, but is not generated by any 3 minimal vectors.

Proof. The proof is similar to the above theorem. Since $\gcd(a, 2b+1) = 1$, there exist integers A and B satisfying $aA + (2b+1)B = 1$. Then, by letting $p = A, q = r = B, s = 0$ in Lemma 4,

$$L = (a, b+\omega)\mathbf{v}_1 + (a, b+\overline{\omega})\mathbf{v}_2$$

with

$$\mathbf{v}_1 \cdot \mathbf{v}_1 = \mathbf{v}_2 \cdot \mathbf{v}_2 = \frac{1}{a}, \quad \mathbf{v}_1 \cdot \mathbf{v}_2 = 0.$$

The minimal vectors are

$$\pm a\mathbf{v}_1, \quad \pm(b+\omega)\mathbf{v}_1, \quad \pm a\mathbf{v}_2, \quad \pm(b+\overline{\omega})\mathbf{v}_2$$

of squared length a. Any 3 vectors of them cannot generate L. □

The condition of a and b on m can be written as $m = k\ell \equiv 3 \pmod 4$ with $0 < \ell < k < 3\ell$. Then $a = (k+\ell)/4$ and $b = (k-\ell-2)/4$.

One can describe the first type of lattices in [4] by using the above theorem. That is, from $m = 4a^2 - 1 = (2a+1)(2a-1)$, if we let $b = 0$, $A = 0$, and $B = 1$, then the lattice $(a, \omega)\mathbf{v}_1 + (a, \overline{\omega})\mathbf{v}_2$ has Gram matrix

$$\begin{pmatrix} 2a & -1+2\omega \\ -1+2\overline{\omega} & 2a \end{pmatrix} = \begin{pmatrix} 2a & \sqrt{-m} \\ -\sqrt{-m} & 2a \end{pmatrix}.$$

Remark. The above methods can be applied to infinitely many imaginary quadratic fields, but not all such lattices are generated by this method. For example, the second type of lattices

$$\begin{pmatrix} 2a+1 & \sqrt{-m} \\ -\sqrt{-m} & 2a+1 \end{pmatrix}$$

in [4] is constructed over $\mathbf{Q}(\sqrt{-m})$ when $m = (2a+1)^2 - 2$ for $a \geq 2$. It is generated by its minimal vectors of squared length $2a$, but they cannot compose a basis.

Acknowledgements. The author would like thank ChongGyu Lee for his helpful comments. This work was supported by Kyungnam University Foundation Grant, 2010.

References

[1] J. H. Conway and N. J. A. Sloane, A lattice without a basis of minimal vectors, Mathematika **42** (1995), no. 1, 175–177.

[2] C. Fieker and M. E. Pohst, On lattices over number fields, in *Algorithmic number theory (Talence, 1996)*, 133–139, Lecture Notes in Comput. Sci., 1122, Springer, Berlin, 1996.

[3] O. T. O'Meara, *Introduction to quadratic forms*, Spinger-Verlag, New York, 1973.

[4] B. M. Kim and P.-S. Park, Hermitian lattices without a basis of minimal vectors, Proc. Amer. Math. Soc. **136** (2008), no. 9, 3041–3044.

[5] R. Sasaki, On a lower bound for the class number of an imaginary quadratic field, Proc. Japan Acad. Ser. A Math. Sci. **62** (1986), no. 1, 37–39.