Hokkaido Mathematical Journal Vol. 27 (1998) p. 213–218

A note on lattices with group actions

Tsuyoshi ATSUMI

(Received October 30, 1996)

Abstract. By using a lattice version of Hayden's result we generalize a Jacobi's formula for the theta series of the dual lattice when a finite group acts on the lattice. This solves a problem posed by Yoshida.

Key words: lattice, group, dual lattice, Jacobi's formula.

1. Introduction

In his paper [6] Yoshida proved the following result.

Result *There is a generalization of MacWilliams identity* [4] *to codes with group actions.*

Moreover he raised the following problem in [6].

Problem What can we say about lattices with group actions? Can we define the equivariant version of theta functions?

We solve the problem above. In this paper we shall prove that there is a lattice version of his result.

We introduce notation and terminology in lattice theory. Let V be the real n-dimensional space $\mathbf{R}^n$. A *lattice* Λ [5] is a subgroup of V satisfying one of the following equivalent conditions:

i) Λ is discrete and V/Λ is compact;

ii) Λ is discrete and generates the $\mathbf{R}$-vector space V;

iii) There exists an $\mathbf{R}$-basis $(e_1, \ldots, e_n)$ of V which is a $\mathbf{Z}$-basis of Λ (i.e. $\Lambda = \mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_n$).

Let

$$\begin{aligned} e_1 &= (e_{11}, \ldots, e_{1n}), \\ e_2 &= (e_{21}, \ldots, e_{2n}), \\ &\vdots \\ e_n &= (e_{n1}, \ldots, e_{nn}) \end{aligned}$$

1991 Mathematics Subject Classification : 11H56, 20B25.

be the coordinates of the basis vectors of Λ given in (iii). The $n \times n$ matrix M with (i,j)-entry equal to e_{ij} is called a generator matrix for Λ. The determinant of Λ is defined to be $\det \Lambda = |\det M|$.

Given two vectors $\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{v} = (v_1, \ldots, v_n)$ of V, their inner product will be denoted by $\mathbf{u} \cdot \mathbf{u}$ or $(\mathbf{u}, \mathbf{u})$. The *dual lattice* $\Lambda^\perp$ of Λ is defined by

$$\Lambda^\perp = \{\mathbf{u} \in \mathbf{R}^n \mid \mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n \in \mathbf{Z} \text{ for } \textit{all } \mathbf{v} \in \Lambda\}.$$

The *theta series* $\Theta_\Lambda(z)$ of a lattice Λ is given by

$$\Theta_\Lambda(z) = \sum_{\mathbf{u} \in \Lambda} q^{\mathbf{u} \cdot \mathbf{u}},$$

where $q = e^{\pi i z}$. Jacobi's formula for the theta series of the dual lattice:

$$\Theta_{\Lambda^\perp}(z) = (\det \Lambda)(i/z)^{n/2} \Theta_\Lambda(-1/z). \tag{1}$$

In section 2 we shall define G-lattices and give our theorem on them, which is a generalization of (1).

In section 3 we shall prove Lemma 1 which does not seem to be trivial and our theorem by using a lattice version of Hayden' theorem.

For notation and terminology, see [2] and [5] for lattice theory, [6] for lattices with group actions.

In particular, G is a finite group, $\mathbf{R}G$ is a group ring over $\mathbf{R}$.

2. Lattices with group actions

From now on we assume that G is a finite permutation group on the coordinates of V. Then we can define a natural action of G on V as follows: If $\mathbf{v} = (v_1, \ldots, v_n) \in V$ and $g \in G$, we let $\mathbf{v}g = (x_1, \ldots, x_n)$ where for $i = 1, \ldots, n$, $x_i = v_{ig^{-1}}$. In this way V becomes an $\mathbf{R}G$-module and every element of $\mathbf{R}G$ is a linear, orthogonal transformation of V. A *G-lattice* is a lattice which is also a $\mathbf{Z}G$-submodule of V.

As in [1], the operator θ is defined by

$$\theta = \frac{1}{|G|} \sum_{g \in G} g.$$

Here we note that $\theta \in \mathbf{R}G$, $V\theta = \{\mathbf{v} \in V \mid \mathbf{v}g = \mathbf{v} \text{ for } \textit{all } g \in G\}$, $\theta^T = \theta$ and $\theta^2 = \theta$, where θ^T is the transpose of θ (see [1]). Let $C_1, \ldots, C_t$ be the orbits of the coordinates of V under the action of G. Let m_i be the orbit

length of C_i. Define $\overline{C}_i$ as the vector of V which has $1/\sqrt{m_i}$ as its entry for every point of C_i and 0 elsewhere. (This definition of the $\overline{C}_i$'s is similar to that in the proof of Theorem 4.3 in [1]). Then each of $\overline{C}_1, \ldots, \overline{C}_t$ is in $V\theta$ and every element $\mathbf{u}$ of $V\theta$ is of the form

$$\mathbf{u} = \sum_{i=1}^{t} x_i \overline{C}_i.$$

The vector space $V\theta$ is of dimension t.

For vectors $\mathbf{a}, \mathbf{b}$ of $V\theta$, the inner product $\mathbf{a} \circ \mathbf{b}$ of $\mathbf{a}$ and $\mathbf{b}$ is defined by

$$\mathbf{a} \circ \mathbf{b} = a_1 b_1 + \cdots + a_t b_t, \tag{2}$$

where $\mathbf{a} = \sum_{i=1}^{t} a_i \overline{C}_i$ and $\mathbf{b} = \sum_{i=1}^{t} b_i \overline{C}_i$.

Let D be a lattice in $V\theta$. (That is, there exists an $\mathbf{R}$-basis consisting of t elements of $V\theta$ which is a $\mathbf{Z}$-basis of D.) $D_G^{\perp}$ is the dual of D in $V\theta$ with respect to the inner product (2). The norm of $\mathbf{u} \in D$ is $\mathbf{u} \circ \mathbf{u}$. We describe the theta series $\Theta_D(z)$ of a sublattice D in $V\theta$ as follows:

$$\Theta_D(z) = \sum_{\mathbf{u} \in D} q^{\mathbf{u} \circ \mathbf{u}},$$

where $q = e^{\pi i z}$. Then we have the following:

Theorem *Let Λ be a G-lattice and let $\Lambda_0 = \{\mathbf{r} \in \Lambda \mid \mathbf{r}\theta \in \Lambda\}$. Then the following holds*:

(i) *$\Lambda_0\theta$ is a lattice.*

(ii) $\Theta_{\Lambda_0^{\perp}\theta}(z) = (\det \Lambda_0\theta)(i/z)^{t/2} \Theta_{\Lambda_0\theta}(-1/z)$.

If G is trivial, that is, $G = \{e\}$, the equation above reduces to (1). Note that $\Lambda_0\theta = \Lambda \cap \Lambda\theta = \{\mathbf{v} \in \Lambda \mid \mathbf{v}g = \mathbf{v} \text{ for } all\ g \in G\}$.

3. Proof of theorem

We prove the following lemma which is part (i) of our theorem.

Lemma 1 *Let Λ be a G-lattice and let $\Lambda_0 = \{\mathbf{r} \in \Lambda \mid \mathbf{r}\theta \in \Lambda\}$. Then $\Lambda_0\theta$ is a lattice.*

Proof. First we shall show that $|G|(\Lambda \cap \Lambda\theta)$ $(= |G|\Lambda_0\theta)$ is a lattice. Let $(e_1, \ldots, e_n)$ be a $\mathbf{Z}$-basis of Λ which is also an $\mathbf{R}$-basis of V. Since $(e_1, \ldots, e_n)$ is an $\mathbf{R}$-basis of V, we see that vectors $|G|e_1\theta, \ldots, |G|e_n\theta$ of

$|G|(\Lambda \cap \Lambda\theta)$ generate $V\theta$. This shows that

$$V\theta \subseteq R(|G|e_1\theta) + \cdots + R(|G|e_n\theta).$$

On the other hand, clearly $|G|(\Lambda \cap \Lambda\theta) \subseteq V\theta$, hence we have

$$V\theta = R(|G|e_1\theta) + \cdots + R(|G|e_n\theta). \tag{3}$$

Λ is a free $\mathbf{Z}$-module and $|G|(\Lambda \cap \Lambda\theta)$ is a $\mathbf{Z}$-submodule of Λ. So there exists a basis $(m_1, \ldots, m_n)$ for Λ, and non-zero elements $\delta_1, \ldots, \delta_r$, $r \leq n$, in $\mathbf{Z}$ such that $\delta_i | \delta_{i+1}$ $1 \leq i \leq r-1$, and such that vectors $\delta_1 m_1, \ldots, \delta_r m_r$ forms a basis for $|G|(\Lambda \cap \Lambda\theta)$ (see [3, pp 97]). Since $(m_1, \ldots, m_n)$ is an $\mathbf{R}$-basis of V, vectors $\delta_1 m_1, \ldots, \delta_r m_r$ are linearly independent over $\mathbf{R}$. From this and (3) it follows that

$$V\theta = \mathbf{R}(\delta_1 m_1) \oplus \cdots \oplus \mathbf{R}(\delta_r m_r),$$

which shows that $r = t$. This proves that $|G|(\Lambda \cap \Lambda\theta)$ is a lattice. So is $\Lambda \cap \Lambda\theta$. □

In order to prove Theorem we need the following proposition which is a lattice version of Hayden's theorem [1].

Proposition 1 *Under the same notation as in Lemma* 1, *we have the following*:

$$(\Lambda_0\theta)^\perp = Ker\,\theta \oplus \Lambda_0^\perp\theta.$$

Proof. Our proof is similar to the proof of Theorem 4.2 in [1]. We note that Λ_0 is a $\mathbf{Z}G$-submodule of G-lattice Λ, $\theta^T = \theta$ and $\theta^2 = \theta$. If $\mathbf{r} \in \Lambda_0$, $\hat{\mathbf{r}} \in \Lambda_0^\perp$ and $\mathbf{y} \in Ker\,\theta^T$, we have

$$(\hat{\mathbf{r}}\theta^T, \mathbf{r}\theta) = (\hat{\mathbf{r}}, \mathbf{r}\theta^2) = (\hat{\mathbf{r}}, \mathbf{r}\theta) \in Z,$$

because $\mathbf{r}\theta \in \Lambda \cap \Lambda\theta \subseteq \Lambda_0$ and

$$(\mathbf{y}, \mathbf{r}\theta) = (\mathbf{y}\theta^T, \mathbf{r}) = 0 \in Z.$$

This shows that

$$Ker\,\theta + \Lambda_0^\perp\theta \subseteq (\Lambda_0\theta)^\perp. \tag{4}$$

If $\mathbf{r} \in \Lambda_0$, $\mathbf{y} \in (\Lambda_0\theta)^\perp$, we have

$$(\mathbf{y}\theta^T, \mathbf{r}) = (\mathbf{y}, \mathbf{r}\theta) \in Z.$$

So

$$\mathbf{y}\theta^T = \mathbf{y}\theta \in \Lambda_0^{\perp}.$$

Hence

$$\mathbf{y} = \mathbf{y} - \mathbf{y}\theta + (\mathbf{y}\theta)\theta \in Ker\,\theta + \Lambda_0^{\perp}\theta.$$

This implies that

$$(\Lambda_0\theta)^{\perp} \subseteq Ker\,\theta + \Lambda_0^{\perp}\theta. \tag{5}$$

(4) and (5) complete the proof of Proposition 1. □

We start to prove Theorem. If $\mathbf{x} = \sum_i x_i\overline{C}_i \in \Lambda_0\theta$ and $\mathbf{y} = \sum_i y_i\overline{C}_i \in \Lambda_0^{\perp}\theta$, by Proposition 1 we have

$$\mathbf{x} \circ \mathbf{y} = (\mathbf{x}, \mathbf{y}) \in Z.$$

So

$$\Lambda_0^{\perp}\theta \subseteq (\Lambda_0\theta)_G^{\perp}. \tag{6}$$

Now take $\mathbf{x} = \sum_i x_i\overline{C}_i \in (\Lambda_0\theta)_G^{\perp}$, $\mathbf{y} = \sum_i y_i\overline{C}_i \in \Lambda_0\theta$. and observe

$$(\mathbf{x}, \mathbf{y}) = \mathbf{x} \circ \mathbf{y} \in Z.$$

This shows that

$$\mathbf{x} \in (\Lambda_0\theta)^{\perp}. \tag{7}$$

Since $\mathbf{x} \in V\theta$, (7) and Proposition 1 imply that $\mathbf{x} \in \Lambda_0^{\perp}\theta$.
Now we proved that

$$(\Lambda_0\theta)_G^{\perp} \subseteq \Lambda_0^{\perp}\theta. \tag{8}$$

From (6) and (8) it follows that

$$(\Lambda_0\theta)_G^{\perp} = \Lambda_0^{\perp}\theta. \tag{9}$$

Now we shall finish the proof of Theorem. Lemma 1 tells us that $\Lambda_0\theta$ is a lattice. Hence, we have Jacobi's formula for the theta series of the dual lattice $(\Lambda_0\theta)_G^{\perp}$ in $V\theta$:

$$\Theta_{(\Lambda_0\theta)_G^{\perp}}(z) = (\det \Lambda_0\theta)(i/z)^{t/2}\Theta_{\Lambda_0\theta}(-1/z).$$

Hence equation (9) establishes our Theorem.

Remark. It is easy to prove that

$$\Lambda/\Lambda_0 \cong \Lambda\theta/\Lambda \cap \Lambda\theta,$$
$$\Lambda_0 = (\Lambda \cap \mathrm{Ker}\,\theta) \oplus (\Lambda \cap \Lambda\theta).$$

References

[1] Bridges W.G., Hall M. and Hayden J.L., *Codes and Designs.* J. Combin. Theory Ser. A **31** (1981), 155–174.

[2] Conway J.H. and Sloane N.J.A., *Sphere Packings, Lattices and Groups.* Springer-Verlag, New York-Berlin-Heidelberg-London-Paris-Tokyo, 1988.

[3] Curtis C.W. and Reiner I., *Representation Theory of Finite Groups and Associative Algebras.* Interscience, New York-London-Sydney, 1966.

[4] MacWilliams F.J. and Sloane N.J.A., *The Theory of The Error-Correcting Codes.* North Holland, Amsterdam-New York-Oxford, 1977.

[5] Serre J.P., *Cours d'Arthmétique.* Presses Universitaires de France, Paris, (1970); English translation, Springer-Verlag, New York-Berlin-Heidelberg-London-Paris-Tokyo, 1973.

[6] Yoshida T., *MacWilliams Identities for Linear Codes with Group Action.* Kumamoto J. Math. **6** (1993), 29–45.

Department of Mathematics
Faculty of Science
Kagoshima University
Kagoshima 890, Japan
E-mail: atsumi@sci.kagoshima-u.ac.jp