J. Aust. Math. Soc. **100** (2016), 216–240
doi:10.1017/S144678871500049X

MAXIMAL SEMIGROUP SYMMETRY AND DISCRETE RIESZ TRANSFORMS

TOSHIYUKI KOBAYASHI✉, ANDREAS NILSSON and FUMIHIRO SATO

(Received 26 April 2015; accepted 4 August 2015; first published online 14 December 2015)

Communicated by C. Meaney

To the memory of Professor Garth Gaudry

Abstract

We raise a question of whether the Riesz transform on $\mathbb{T}^n$ or $\mathbb{Z}^n$ is characterized by the 'maximal semigroup symmetry' that the transform satisfies. We prove that this is the case if and only if the dimension is one, two or a multiple of four. This generalizes a theorem of Edwards and Gaudry for the Hilbert transform on $\mathbb{T}$ and $\mathbb{Z}$ in the one-dimensional case, and extends a theorem of Stein for the Riesz transform on $\mathbb{R}^n$. Unlike the $\mathbb{R}^n$ case, we show that there exist infinitely many linearly independent multiplier operators that enjoy the same maximal semigroup symmetry as the Riesz transforms on $\mathbb{T}^n$ and $\mathbb{Z}^n$ if the dimension n is greater than or equal to three and is not a multiple of four.

2010 *Mathematics subject classification*: primary 42B15; secondary 22E46, 42B20.

Keywords and phrases: multiplier, translation invariant operator, Riesz transform, Hilbert transform, Fourier series, semigroup representation, Hasse–Minkowski principle.

1. Introduction

Classical multipliers such as the Hilbert transform on $\mathbb{R}$ or the Riesz transform on $\mathbb{R}^n$ are translation invariant operators with additional 'symmetries' that can be formulated in terms of group representations (see (1.1.1) below). Stein proved that a covariance property under the conformal group characterizes the Riesz transform on $\mathbb{R}^n$ up to scalar multiplication; see Fact 1.3. Extending his idea, we provided in [6] a general framework to characterize specific operators on $\mathbb{R}^n$ by a covariance property with respect to arbitrary (finite-dimensional) representations of a subgroup of the affine transformation group. The object of this paper is its *discrete* analog, concerning the characterization of bounded translation invariant operators on $\mathbb{Z}^n$ and $\mathbb{T}^n$ by means of algebraic conditions (*semigroup symmetry*).

The first author was partially supported by a Grant-in-Aid for Scientific Research (A) (25247006), Japan Society for the Promotion of Science and the second author was also partially supported from the same society.

To be more explicit, we begin with a brief review of translation invariant operators and symmetry for the $\mathbb{R}^n$ case. A bounded operator $T : L^2(\mathbb{R}^n) \to L^2(\mathbb{R}^n)$ is said to be *translation invariant* if $T \circ \tau_s = \tau_s \circ T$ for any $s \in \mathbb{R}^n$, where τ_s is the translation defined by $(\tau_s f)(x) := f(x - s)$ for $f \in L^2(\mathbb{R}^n)$.

A further invariance is defined not for a single operator, but for a family of operators. Suppose that $T = \{T_1, \ldots, T_N\}$ is a family of linearly independent, bounded translation invariant operators on $L^2(\mathbb{R}^n)$. Then the 'symmetry' of T may be formulated as follows.

Condition 1.1. $T_j \circ l_g$ $(1 \le j \le N)$ is a linear combination of $l_g \circ T_1, \ldots, l_g \circ T_N$ as long as g belongs to some subgroup of $\mathrm{GL}(n, \mathbb{R})$.

Here $(l_g f)(x) := f(g^{-1}x)$ for $g \in \mathrm{GL}(n, \mathbb{R})$ and $f \in L^2(\mathbb{R}^n)$.

In a coordinate-free fashion, we regard T as a bounded translation invariant operator

$$T : L^2(\mathbb{R}^n) \to V \otimes L^2(\mathbb{R}^n),$$

where V is an N-dimensional complex vector space. Suppose that H is a subgroup of $\mathrm{GL}(n, \mathbb{R})$ and that $\pi : H \to \mathrm{GL}_{\mathbb{C}}(V)$ is a group homomorphism. Then Condition 1.1 may be reformulated by means of the pair (H, π), as the following covariance with respect to the group H:

$$(\pi(g) \otimes l_g) \circ T = T \circ l_g \quad \text{for any } g \in H. \tag{1.1.1}$$

We denote by $\mathcal{B}_H(L^2(\mathbb{R}^n), V \otimes L^2(\mathbb{R}^n))$ the vector space of bounded translation invariant operators T satisfying (1.1.1).

The conformal group $\mathrm{CO}(n)$ of the Euclidean space $\mathbb{R}^n$ is defined by

$$\mathrm{CO}(n) := \{g \in \mathrm{GL}(n, \mathbb{R}) : {}^t g g \in \mathbb{R}^\times \cdot I_n\}.$$

It is isomorphic to the direct product group $\mathbb{R}_+ \times \mathrm{O}(n)$, and the projection to the second factor is given by a group homomorphism

$$\pi : \mathrm{CO}(n) \to \mathrm{O}(n), \quad g \mapsto |\det g|^{-1/n} g. \tag{1.1.2}$$

We recall the definition of the (classical) Riesz transform on $\mathbb{R}^n$.

Definition 1.2. For $1 \le p < \infty$, we define translation invariant operators on $L^p(\mathbb{R}^n)$ by

$$R_j(f)(x) = \lim_{\epsilon \to 0} c_n \int_{|y| > \epsilon} \frac{y_j}{|y|^{n+1}} f(x - y)\, dy \quad \text{for } j = 1, \ldots, n$$

with $c_n = \Gamma(n + 1/2)/\pi^{(n+1)/2}$. Then the Riesz transform on $\mathbb{R}^n$ is defined to be $R = (R_1, \ldots, R_n)$.

Now, Stein's characterization of Riesz transforms [10, Section 3.1] can be formulated as follows.

Fact 1.3. Let $H := \mathrm{CO}(n)$ acting on $V := \mathbb{R}^n$, and $\pi : H \to \mathrm{GL}(n, \mathbb{C})$ as in (1.1.2). Then the space $\mathcal{B}_H(L^2(\mathbb{R}^n), V \otimes L^2(\mathbb{R}^n))$ is one dimensional and spanned by the Riesz transform R on $\mathbb{R}^n$.

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

We write $(\mathbb{R}^n)^\wedge$ ($\simeq \mathbb{R}^n$) for the dual space of $\mathbb{R}^n$. In [5, Corollary 2.1.2], Fact 1.3 is extended to the following fact.

FACT 1.4. Let H be a subgroup of $\mathrm{GL}(n,\mathbb{R})$ such that its contragredient action has a dense orbit $\mathcal{O}$ in $(\mathbb{R}^n)^\wedge$. We write H_1 for the stabilizer of H at a point p in $\mathcal{O}$. Then, for any representation $\pi : H \to \mathrm{GL}_{\mathbb{C}}(V)$,

$$\dim \mathcal{B}_H(L^2(\mathbb{R}^n), V \otimes L^2(\mathbb{R}^n)) \leq \dim V^{H_1},$$

where

$$V^{H_1} := \{v \in V : \pi(h)v = v \text{ for any } h \in H_1\}.$$

We note that $\dim V^{H_1}$ is independent of the choice of $p \in \mathcal{O}$.

In particular, a family of bounded operators is determined uniquely up to a scalar multiple if $\dim V^{H_1} \leq 1$. This assumption is fulfilled, for example, if:

(1) $\dim V = 1$ (in this case, the translation invariant operator T is given by the convolution with a kernel which is the Fourier transform of a bounded relative invariant of a prehomogeneous vector space in the sense of Sato; see [7]);

or

(2) (H, H_1) is a reductive symmetric pair and V is an arbitrary (finite-dimensional) irreducible representation of H.

In Stein's example (see Fact 1.3), $(H, H_1) = (\mathrm{CO}(n), \mathrm{O}(n-1))$ is a reductive symmetric pair.

The Riesz transform on $\mathbb{T}^n$ and $\mathbb{Z}^n$ is defined as the translation invariant operator $L^2(\mathbb{F}^n) \to \mathbb{C}^n \otimes L^2(\mathbb{F}^n)$ ($\mathbb{F} = \mathbb{T}, \mathbb{Z}$) in Definitions 2.5 and 4.11, respectively, in an analogous fashion to the $\mathbb{R}^n$ case. We shall observe that for the Riesz transform on $\mathbb{T}$ and $\mathbb{Z}$ (namely, the Hilbert transform on $\mathbb{T}$ and $\mathbb{Z}$), the algebraic structure to formulate the invariance condition (1.1.1) fits better with semigroups rather than groups.

In [3], Edwards and Gaudry proved a discrete analogue of Fact 1.3 for $n = 1$, giving a characterization of the Hilbert transforms on $\mathbb{T}$ and $\mathbb{Z}$ by 'semigroup symmetry'.

The goal of this article is to formulate the maximal semigroup symmetry for vector-valued translation invariant operators on $\mathbb{T}^n$ and $\mathbb{Z}^n$ in general and to investigate to what extent Edwards–Gaudry's characterization works for the Riesz transforms on $\mathbb{T}^n$ and $\mathbb{Z}^n$ in higher dimensions.

As a higher dimensional generalization of Edwards and Gaudry's results, we need to adapt the general framework, Condition 1.1 in the $\mathbb{R}^n$ case. For a formulation of 'invariant multipliers' on $\mathbb{T}^n$ ($= \mathbb{R}^n/\mathbb{Z}^n$) or $\mathbb{Z}^n$, one natural way is to use only injective linear transformations that preserve the lattice $\mathbb{Z}^n$. Namely, the semigroup

$$\mathrm{M}^{reg}(n,\mathbb{Z}) := \{g \in \mathrm{M}(n,\mathbb{Z}) : \det g \neq 0\}.$$

Unlike the $\mathbb{R}$ case, we note that

$$\mathrm{M}^{reg}(n,\mathbb{Z}) \supsetneq GL(n,\mathbb{Z}) := \{g \in M(n,\mathbb{Z}) : g \text{ is an automorphism of } \mathbb{Z}^n\}.$$

In the Introduction we discuss only $\mathbb{T}^n$ for simplicity of the exposition.

The semigroup $\mathrm{M}^{reg}(n, \mathbb{Z})$ acts on $L^2(\mathbb{T}^n)$ by

$$(L_g f)(x) := f({}^t g x) \quad \text{for } f \in L^2(\mathbb{T}^n).$$

Here we have used the operator L_g in the $\mathbb{T}^n$ case instead of the previous $l_g : f(t) \mapsto f(g^{-1}t)$ in the $\mathbb{R}^n$ case because $g^{-1}t$ is not necessarily well defined for $t \in \mathbb{T}^n$ if $\det g \neq \pm 1$.

Definition 1.5 (Semigroup symmetry). Let $T : L^2(\mathbb{T}^n) \to V \otimes L^2(\mathbb{T}^n)$ be a bounded linear operator. We say that T is:

$$\textit{translation invariant} \text{ if } T \circ \tau_\alpha = (\mathrm{id} \otimes \tau_\alpha) \circ T \quad \text{for all } \alpha \in \mathbb{R}^n;$$
$$\textit{nondegenerate} \text{ if } \mathbb{C}\text{-span}\{T f(t) : f \in L^2(\mathbb{T}^n), t \in \mathbb{T}^n\} \text{ is equal to } V.$$

A semigroup symmetry for T is a pair (G, π), where G is a subsemigroup of $\mathrm{M}^{reg}(n, \mathbb{Z})$ and $\pi : G \to GL_{\mathbb{C}}(V)$ is a semigroup homomorphism such that

$$(\pi(g) \otimes L_g) \circ T = T \circ L_g \quad \text{for any } g \in G. \tag{1.1.3}$$

We define a partial order of semigroup symmetries by $(G', \pi') \prec (G, \pi)$ if $G' \subset G$ and $\pi' = \pi|_G$. By Zorn's lemma, there exists a maximal element of this partial order. Actually, it is unique, as the following construction shows.

Definition–Proposition 1.6 (Maximal semigroup symmetry). For a nondegenerate translation invariant operator $T : L^2(\mathbb{T}^n) \to V \otimes L^2(\mathbb{T}^n)$, there exists a unique maximal semigroup symmetry. In fact, let G be a subset of $\mathrm{M}^{reg}(n, \mathbb{Z})$ consisting of all g for which there exists $A \in \mathrm{GL}_{\mathbb{C}}(V)$ satisfying $(A \otimes L_g) \circ T = T \circ L_g$. Then G is a semigroup and A is determined uniquely by $g \in G$. The correspondence $G \to \mathrm{GL}_{\mathbb{C}}(V)$, $g \mapsto A$ defines a semigroup homomorphism, which we denote by π. Then (G, π) is the maximal semigroup symmetry for the operator T.

Remark 1.7. An analogous notion is defined for $l^2(\mathbb{Z}^n)$, but it is slightly more involved; see Section 4.2.

Example 1.8. Let $G_{\mathbb{T}} = \mathrm{CO}(n, \mathbb{Z}) := \mathrm{CO}(n) \cap \mathrm{M}(n, \mathbb{Z})$, $G_{\mathbb{R}} = \mathrm{CO}(n)$ and $\pi(g) = |\det g|^{-1/n} g$. Let $G_{\mathbb{Z}} = \mathrm{CO}(n, \mathbb{Z})$ and $\rho(g) = |\det g|^{(n+1)/n}\, {}^t g^{-1}$. Then $(G_{\mathbb{T}}, \pi)$ and $(G_{\mathbb{R}}, \pi)$ are the maximal semigroup symmetries for the Riesz transforms on $\mathbb{T}^n$ and $\mathbb{R}^n$, respectively, and the pair $(G_{\mathbb{Z}}, \rho)$ is the maximal semigroup symmetry for the Riesz transforms on $\mathbb{Z}^n$; see Propositions 2.6 and 4.12. Note that $G_{\mathbb{R}}$ is in fact a group, but $G_{\mathbb{T}}$ and $G_{\mathbb{Z}}$ are just semigroups.

Definition–Proposition 1.6 asserts that any nondegenerate translation invariant operator gives rise to the unique semigroup symmetry. Conversely, we may ask the following question.

Question 1.9. Does the maximal semigroup symmetry recover the original operator?

Fact 1.3 asserts that this is the case for the Riesz transform on $\mathbb{R}^n$ for all dimensions n. Edwards and Gaudry proved that this is also the case for the Hilbert transform on the circle $\mathbb{T}$ and on $\mathbb{Z}$ (namely, the Riesz transform on the torus $\mathbb{T}^n$ and on $\mathbb{Z}^n$ for $n = 1$); see Facts 2.1 and 4.2, respectively.

Here are the main results of this article.

THEOREM A. *If the dimension n is one, two or a multiple of four, then the maximal semigroup symmetry given by the pair* $(\mathrm{CO}(n,\mathbb{Z}), |\det g|^{-1/n} g)$ *and* $(\mathrm{CO}(n,\mathbb{Z}), |\det g|^{n+1/n}\ {}^t g^{-1})$ *characterizes the Riesz transforms on $\mathbb{T}^n$ and $\mathbb{Z}^n$, respectively.*

THEOREM B. *Suppose that $n \geq 3$ and $n \not\equiv 0 \bmod 4$. Then there exist infinitely many linearly independent multipliers on $\mathbb{T}^n$ and $\mathbb{Z}^n$, respectively, satisfying the same semigroup symmetry with the Riesz transform.*

Theorem A contains the aforementioned results of Edwards and Gaudry as special cases when $n = 1$. Theorem B shows that the features of invariant multipliers for $\mathbb{T}^n$ and $\mathbb{Z}^n$ are very different from Stein's theorem in the $\mathbb{R}^n$ case.

In Section 5, we introduce a stronger invariance condition (*saturated semigroup symmetry*) and prove that this condition characterizes the Riesz transforms on $\mathbb{T}^n$ and $\mathbb{Z}^n$ for arbitrary n.

Notation. $\mathbb{N} = \{0, 1, 2, \ldots\}$, $\mathbb{N}_+ = \{1, 2, \ldots\}$, $\mathbb{N}_- = \{-1, -2, \ldots\}$, $\mathbb{R}^\times = \{r \in \mathbb{R} : r \neq 0\}$, $\mathbb{R}_+ = \{r \in \mathbb{R} : r > 0\}$, $\mathbb{Q}^\times = \mathbb{Q} \cap \mathbb{R}^\times$, $\mathbb{Q}_+ = \mathbb{Q} \cap \mathbb{R}_+$, $\mathrm{M}^{reg}(n,\mathbb{Z}) = \{g \in \mathrm{M}(n,\mathbb{Z}) : \det g \neq 0\}$ (semigroup), $\mathrm{CO}(n,\mathbb{Z}) = \mathrm{CO}(n) \cap \mathrm{M}(n,\mathbb{Z})$ (semigroup).

2. Maximal semigroup symmetry of translation invariant operators on $\mathbb{T}^n$

In Sections 2 and 4, we shall appeal to the general framework in the Introduction to discuss if the maximal symmetry gives a characterization of the Riesz transforms on $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$ and $\mathbb{Z}^n$.

2.1. The Hilbert transform on the circle $\mathbb{T}$. We begin with a quick review of Edwards and Gaudry's characterization of the Hilbert transform on $\mathbb{T}$ in the one-dimensional case.

We define the Fourier transform on $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, $\mathcal{F} : L^2(\mathbb{T}) \to l^2(\mathbb{Z})$ by

$$\mathcal{F}(f)(\alpha) := \int_{\mathbb{T}} f(t) e^{-2\pi i \alpha t}\, dt \quad (\alpha \in \mathbb{Z}).$$

Given a bounded function m on $\mathbb{Z}$, we define a *multiplier operator* $T_m : L^2(\mathbb{T}) \to L^2(\mathbb{T})$ by

$$\mathcal{F}(T_m f)(\alpha) = m(\alpha)\mathcal{F}(f)(\alpha).$$

Clearly, the operator T_m is translation invariant, that is,

$$T_m \circ \tau_s = \tau_s \circ T_m \quad \text{for any } s \in \mathbb{T},$$

where $\tau_s f(t) := f(t-s)$. Conversely, any translation invariant operator bounded on $L^2(\mathbb{T})$ is of the form T_m for some $m \in l^\infty(\mathbb{Z})$. In particular, the Hilbert transform on $\mathbb{T}$, to be denoted by H, is defined to be the multiplier operator T_m with m defined by

$$m(\alpha) := \begin{cases} -i & \text{if } \alpha \in \mathbb{N}_+, \\ 0 & \text{if } \alpha = 0, \\ i & \text{if } \alpha \in \mathbb{N}_-. \end{cases}$$

Let us examine the additional invariance conditions that the Hilbert transform H satisfies. For $a \in \mathbb{Z}\backslash\{0\}$, we define dilations D_a on $L^2(\mathbb{T})$ and $l^2(\mathbb{Z})$ by

$$\begin{aligned} D_a f(t) &:= f(at) \quad && \text{if } f \in L^2(\mathbb{T}), \\ D_a F(\alpha) &:= F(a\alpha) \quad && \text{if } F \in l^2(\mathbb{Z}), \end{aligned} \tag{2.1.1}$$

respectively. Then

$$D_a \circ \mathcal{F} \circ D_a = \mathcal{F}. \tag{2.1.2}$$

In other words,

$$(\mathcal{F} \circ D_a f)(\beta) = \begin{cases} (\mathcal{F} f)(a^{-1}\beta) & \text{if } \beta \in a\mathbb{Z}, \\ 0 & \text{if } \beta \in \mathbb{Z}\backslash a\mathbb{Z}. \end{cases}$$

Then it is easy to see that the Hilbert transform H on $\mathbb{T}$ satisfies the identity

$$H \circ D_a = \operatorname{sgn}(a) D_a \circ H \quad \text{for any } a \in \mathbb{Z}\backslash\{0\}. \tag{2.1.3}$$

Conversely, suppose that a multiplier operator T_m satisfies (2.1.3). By composition with $D_a \circ \mathcal{F}$, we obtain the identity

$$D_a \circ \mathcal{F} \circ T_m \circ D_a = \operatorname{sgn}(a) \mathcal{F} \circ T_m$$

because of (2.1.2). In terms of the multiplier m, this amounts to

$$D_a(m(\alpha)\mathcal{F}(D_a f)(\alpha)) = \operatorname{sgn}(a) m(\alpha) \mathcal{F}(f)(\alpha) \quad \text{for any } f \in L^2(\mathbb{T}).$$

Using (2.1.2) again,

$$m(a\alpha)\mathcal{F}(f)(\alpha) = \operatorname{sgn}(a) m(\alpha) \mathcal{F}(f)(\alpha)$$

for any $f \in L^2(\mathbb{T})$. Hence, $m(a\alpha) = \operatorname{sgn}(a)m(\alpha)$ for any $a \in \mathbb{Z}\backslash\{0\}$ and $\alpha \in \mathbb{Z}$. The substitution $\alpha = 0$ and $a = -1$ shows that $m(0) = 0$ and substituting $\alpha = 1$ shows that m is a constant multiple of the sign function. This is essentially the argument of Edwards and Gaudry, who proved the following fact.

Fact 2.1 [3, Theorem 6.8.3]. Suppose that T_m is a multiplier operator on $L^2(\mathbb{T})$, associated to $m \in l^\infty(\mathbb{Z})$. If T_m satisfies the identity

$$T_m \circ D_a = \operatorname{sgn}(a) D_a \circ T_m \quad \text{for all } a \in \mathbb{Z}\backslash\{0\},$$

then m is a constant multiple of the sign function. Hence, T_m is a constant multiple of the Hilbert transform.

It should be noted that the above relative invariance is the maximal semigroup symmetry with the subgroup $\mathrm{M}^{reg}(1, \mathbb{Z}) \cong \mathbb{Z}\backslash\{0\}$ in the sense of Definition-Proposition 1.6.

2.2. Covariance of vector-valued multipliers on $\mathbb{Z}^n$. In this subsection, we translate the semigroup symmetry of translation invariant operators on $\mathbb{T}^n$ into a covariance of vector-valued multipliers on $\mathbb{Z}^n \cong (\mathbb{T}^n)\widehat{}$ by using the Fourier transform.

Let $\mathbb{T}^n$ be the n-torus $\mathbb{R}^n/\mathbb{Z}^n$. Then the standard inner product on $\mathbb{R}^n$ induces a pairing

$$\langle\ ,\ \rangle : \mathbb{Z}^n \times \mathbb{T}^n \to \mathbb{T}, \quad (\alpha, x) \mapsto \sum_{i=1}^n \alpha_i x_i.$$

We define the Fourier transform

$$\mathcal{F} : L^2(\mathbb{T}^n) \to l^2(\mathbb{Z}^n)$$

by $(\mathcal{F} f)(\alpha) := \int_{\mathbb{T}^n} f(x) e^{-2\pi i\langle\alpha,x\rangle}\, dx$ for $\alpha \in \mathbb{Z}^n$. The Fourier transform $\mathcal{F}$ is a unitary operator between the two Hilbert spaces up to scaling.

Let V be a finite-dimensional vector space over $\mathbb{C}$. Given a bounded function $m : \mathbb{Z}^n \to V$, we define a linear operator

$$l^2(\mathbb{Z}^n) \to V \otimes l^2(\mathbb{Z}^n), \quad g \mapsto (\alpha \mapsto g(\alpha)m(\alpha)),$$

which is obviously a bounded operator. Via the Fourier transform, we get a bounded linear operator

$$T_m : L^2(\mathbb{T}^n) \to V \otimes L^2(\mathbb{T}^n), \quad f \mapsto \mathcal{F}^{-1}(m\mathcal{F} f).$$

The operator T_m is called a *multiplier operator* and is translation invariant. Conversely, any translation invariant bounded operator is of the form T_m with some bounded function (*multiplier*) $m : \mathbb{Z}^n \to V$ by the general theory of translation invariant operators. By definition, we have $\mathcal{F}(T_m f)(\alpha) = m(\alpha) \otimes \mathcal{F} f(\alpha)$. By abuse of notation, we shall write simply $\mathcal{F}(T_m f) = m \otimes \mathcal{F} f$.

PROPOSITION 2.2. *Let H be a subsemigroup of $\mathrm{M}^{reg}(n,\mathbb{Z})$ and $\pi : H \to \mathrm{GL}_{\mathbb{C}}(V)$ a semigroup homomorphism. The multiplier operator $T_m : L^2(\mathbb{T}^n) \to V \otimes L^2(\mathbb{T}^n)$ satisfies the condition (1.1.3) for the pair (H,π) if and only if the multiplier $m : \mathbb{Z}^n \to V$ satisfies*

$$m(g\alpha) = \pi(g)m(\alpha) \quad \textit{for all } \alpha \in \mathbb{Z}^n \textit{ and all } g \in H. \tag{2.2.1}$$

For the proof of Proposition 2.2, we use the following two lemmas. (An alternative proof will also be given at the end of this subsection.) We denote by ${}^t g$ the transposed matrix of g. Clearly, ${}^t g \in \mathrm{M}^{reg}(n,\mathbb{Z})$ if and only if $g \in \mathrm{M}^{reg}(n,\mathbb{Z})$.

LEMMA 2.3. *For $g \in \mathrm{M}^{reg}(n,\mathbb{Z})$ and $\alpha \in g^{-1}\mathbb{Z}^n$,*

$$\sum_{m\in\mathbb{Z}^n/{}^t g\mathbb{Z}^n} e^{-2\pi i\langle\alpha,m\rangle} = \begin{cases} |\det g| & \textit{if } \alpha \in \mathbb{Z}^n, \\ 0 & \textit{if } \alpha \notin \mathbb{Z}^n. \end{cases}$$

PROOF. Since $m \mapsto e^{-2\pi i\langle\alpha,m\rangle}$ is a character of the finite group $\mathbb{Z}/{}^t g\mathbb{Z}^n$, the formula follows from Schur's orthogonality relation and from the identity $\sharp(\mathbb{Z}^n/{}^t g\mathbb{Z}) = |\det g|$. □

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

The formula of $\mathcal{F} \circ L_g$ on $\mathbb{T}^n$ for $g \in \mathrm{GL}(n, \mathbb{Z})$ can be obtained easily as the formula of the Fourier transform on $\mathbb{R}^n$ for affine transforms. However, for $g \in \mathrm{M}^{reg}(n, \mathbb{Z})$, we need to note that $L_g : L^2(\mathbb{T}^n) \to L^2(\mathbb{T}^n)$ is not surjective.

Lemma 2.4. *For $g \in \mathrm{M}^{reg}(n, \mathbb{Z})$ and $\beta \in \mathbb{Z}^n$,*

$$\mathcal{F}(L_g f)(\beta) = \begin{cases} (\mathcal{F} f)(g^{-1}\beta) & \text{if } \beta \in g\mathbb{Z}^n, \\ 0 & \text{if } \beta \notin g\mathbb{Z}^n. \end{cases}$$

Proof.

$$\begin{aligned} \mathcal{F}(L_g f)(\beta) &= \int_{\mathbb{R}^n/\mathbb{Z}^n} f({}^t g x) e^{-2\pi i \langle \beta, x \rangle}\, dx \\ &= |\det g|^{-1} \int_{\mathbb{R}^n/{}^t g\mathbb{Z}^n} f(y) e^{-2\pi i \langle \beta, {}^t g^{-1} y \rangle}\, dy \\ &= |\det g|^{-1} \sum_{m \in \mathbb{Z}^n/{}^t g\mathbb{Z}^n} \int_{\mathbb{R}^n/\mathbb{Z}^n} f(y+m) e^{-2\pi i \langle g^{-1}\beta, y+m \rangle}\, dy \\ &= |\det g|^{-1} \sum_{m \in \mathbb{Z}^n/{}^t g\mathbb{Z}^n} e^{-2\pi i \langle g^{-1}\beta, m \rangle} \int_{\mathbb{R}^n/\mathbb{Z}^n} f(y) e^{-2\pi i \langle g^{-1}\beta, y \rangle}\, dy. \end{aligned}$$

By using Lemma 2.3, we get the lemma. □

Proof of Proposition 2.2. Via the Fourier transform, we see that the condition (1.1.3) is equivalent to the following condition by Lemma 2.4:

$$\pi(g) h(g^{-1}\beta) m(g^{-1}\beta) = m(\beta) h(g^{-1}\beta) \quad \text{for any } \beta \in g\mathbb{Z}^n \text{ and } h \in l^2(\mathbb{Z}^n)$$

for all $g \in H$. This is clearly equivalent to the condition (2.2.1). □

Alternative proof of Proposition 2.2. Assume that T_m satisfies (1.1.3). Then, specializing to the function $f(t) := e^{2\pi i \langle \alpha, t \rangle}$ and setting $t = 0$,

$$\pi(g)(T_m(e^{2\pi i \langle \alpha, \cdot \rangle})(0)) = T_m(e^{2\pi i \langle \alpha, {}^t g \cdot \rangle})(0) = T_m(e^{2\pi i \langle g\alpha, \cdot \rangle})(0).$$

Since $m(\alpha) = \mathcal{F}\kappa(\alpha)$, which can be rewritten as $(\kappa * e^{2\pi i \langle \alpha, \cdot \rangle})(0)$ and by definition this is equal to $T_m(e^{2\pi i \langle \alpha, \cdot \rangle})(0)$, we obtain $\pi(g) m(\alpha) = m(g\alpha)$. Conversely, if $\pi(g) m(\alpha) = m(g\alpha)$, then the same argument gives

$$\pi(g)(T_m(e^{2\pi i \langle \alpha, \cdot \rangle})(0)) = T_m(e^{2\pi i \langle \alpha, {}^t g \cdot \rangle})(0). \tag{2.2.2}$$

By definition, $T_m(L_g e^{2\pi i \langle \alpha, \cdot \rangle})(s) = T_m(e^{2\pi i \langle \alpha, {}^t g \cdot \rangle})(s) = \tau_{-s} T_m(e^{2\pi i \langle \alpha, {}^t g \cdot \rangle})(0)$. Since T_m is translation invariant, this is equal to $T_m(\tau_{-s} e^{2\pi i \langle \alpha, {}^t g \cdot \rangle})(0) = T_m(e^{2\pi i \langle \alpha, {}^t g \cdot + {}^t g s \rangle})(0)$. Using the linearity of T_m, we can rewrite this as $e^{2\pi i \langle \alpha, {}^t g s \rangle} T_m(e^{2\pi i \langle \alpha, {}^t g \cdot \rangle})(0)$. By (2.2.2), we obtain $e^{2\pi i \langle \alpha, {}^t g s \rangle} \pi(g) T_m(e^{2\pi i \langle \alpha, \cdot \rangle})(0)$. By linearity,

$$\pi(g) T_m(e^{2\pi i \langle \alpha, \cdot + {}^t g s \rangle})(0) = \pi(g) T_m(\tau_{-{}^t g s} e^{2\pi i \langle \alpha, \cdot \rangle})(0).$$

Using the translation invariance again, we see that this equals

$$\pi(g) \tau_{-{}^t g s} T_m(e^{2\pi i \langle \alpha, \cdot \rangle})(0) = \pi(g) T_m(e^{2\pi i \langle \alpha, \cdot \rangle})({}^t g s) = \pi(g) L_g T_m(e^{2\pi i \langle \alpha, \cdot \rangle})(s).$$

Thus, we have proved the identity $T_m \circ L_g = \pi(g) L_g \circ T_m$ for functions of the type $e^{2\pi i \langle \alpha, \cdot \rangle}$. By linearity and continuity of T_m, this implies that the identity holds in general since trigonometric polynomials are dense in $L^2(\mathbb{T}^n)$. □

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

2.3. Riesz transform on $\mathbb{T}^n$. As a higher-dimensional generalization of the Hilbert transform, the Riesz transforms $R_1, \ldots, R_n$ on the n-torus $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$ are defined as below.

Definition 2.5 [11, Section VII.3]. We define $R_j : L^2(\mathbb{T}^n) \to L^2(\mathbb{T}^n)$ $(1 \le j \le n)$ to be the multiplier operator T_{m_j}, where

$$m_j(\alpha) = \begin{cases} -i\dfrac{\alpha_j}{\|\alpha\|} & \text{if } \alpha \neq 0, \\ 0 & \text{if } \alpha = 0. \end{cases}$$

The resulting bounded linear operator $R = (R_1, \ldots, R_n) : L^2(\mathbb{T}^n) \to \mathbb{C}^n \otimes L^2(\mathbb{T}^n)$ is said to be the Riesz transform on $\mathbb{T}^n$. It is a discrete analogue of the Riesz transform on $\mathbb{R}^n$.

Let us find what kind of symmetry the Riesz transform satisfies and then discuss whether or not such an invariance condition recovers the Riesz transform up to a scalar.

We recall that $\mathrm{CO}(n,\mathbb{Z})$ is the semigroup given by $\mathrm{CO}(n) \cap \mathrm{M}(n,\mathbb{Z})$.

Proposition 2.6. *The maximal symmetry of the Riesz transform R on $\mathbb{T}^n$ is given by the pair (H, π), where*

$$H := \mathrm{CO}(n,\mathbb{Z}),$$
$$\pi : H \to \mathrm{GL}(n,\mathbb{C}),\ g \mapsto |\det g|^{-1/n} g.$$

Proof. It is easy to see that the Riesz transform satisfies the condition

$$L_g \circ R = |\det g|^{-1/n} g \circ R \circ L_g \quad \text{for any } g \in \mathrm{CO}(n,\mathbb{Z}), \tag{2.3.1}$$

namely, $(\pi(g) \otimes L_g) \circ R = R \circ L_g$ for all $g \in \mathrm{CO}(n,\mathbb{Z})$. It remains to prove that (H, π) is the maximal semigroup symmetry. For this, we use Proposition 2.2. Let $g \in \mathrm{M}^{reg}(n,\mathbb{Z})$ and suppose that there exists $A \in \mathrm{GL}(n,\mathbb{C})$ such that $m_R(g\alpha) = Am_R(\alpha)$ for all $\alpha \in \mathbb{Z}^n$. We shall show that $g \in \mathrm{CO}(n,\mathbb{Z})$. Indeed, as $m_R(\alpha) = -i(\alpha/\|\alpha\|)$, we obtain $(g\alpha/\|g\alpha\|) = A(\alpha/\|\alpha\|)$. Taking norms, this implies in particular that $A \in \mathrm{O}(n)$ since $\|A\alpha\| = \|\alpha\|$ for all $\alpha \in \mathbb{Z}^n$. We write $g = (\vec{g}_1, \ldots, \vec{g}_n)$ and $A = (\vec{A}_1, \ldots, \vec{A}_n)$. Then, for $\alpha = e_i$, we obtain $\vec{A}_i = \vec{g}_i/\|\vec{g}_i\|$, that is, A is of the form $(\lambda_1\vec{g}_1, \ldots, \lambda_n\vec{g}_n)$. Now, by putting $\alpha = e_i + e_j$, we find that $\lambda_i = \lambda_j$ because $\vec{g}_1, \ldots, \vec{g}_n$ are linearly independent. So, $A = \lambda g$, but it is also in $\mathrm{O}(n)$; hence, $\lambda = |\det g|^{-1/n}$. Hence, $g \in \mathrm{CO}(n) \cap \mathrm{M}(n,\mathbb{Z}) = H$ and $A = \pi(g)$. Therefore, (H, π) is the maximal semigroup symmetry of the Riesz transform. □

3. Proof of main theorems for $\mathbb{T}^n$

In this section, we complete the proof of Theorems A and B for the n-torus $\mathbb{T}^n$.

3.1. From semigroup to group invariance. Owing to Proposition 2.2, the analytic problem (Question 1.9) reduces to an algebraic invariance of multipliers $m : \mathbb{Z}^n \to V$.

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

Under certain mild conditions, we can extend this algebraic semigroup symmetry to a larger group invariance.

In this subsection, we formulate this in Lemma 3.5, which includes the following proposition as a special case.

PROPOSITION 3.1. *Let* $\pi : \mathrm{CO}(n,\mathbb{Z}) \to \mathrm{GL}_{\mathbb{C}}(V)$ *be a semigroup homomorphism and* $m : \mathbb{Z}^n \to V$ *a function satisfying*

$$m(g\alpha) = \pi(g)m(\alpha) \quad \text{for all } g \in \mathrm{CO}(n,\mathbb{Z}) \text{ and } \alpha \in \mathbb{Z}^n.$$

Then there exist unique extensions $\tilde{\pi} : \mathrm{CO}(n,\mathbb{Q}) \to \mathrm{GL}_{\mathbb{C}}(V)$ *(group homomorphism) and* $\tilde{m} : \mathbb{Q}^n \to V$ *of* π *and* m*, respectively, satisfying*

$$\tilde{m}(g\alpha) = \tilde{\pi}(g)\tilde{m}(\alpha) \quad \text{for all } g \in \mathrm{CO}(n,\mathbb{Q}) \text{ and } \alpha \in \mathbb{Q}^n.$$

In order to deal with a general setting, let H be a subsemigroup in $\mathrm{M}^{reg}(n,\mathbb{Z})$ and define $\tilde{H}$ to be the subgroup in $\mathrm{GL}(n,\mathbb{Q})$ generated by g and g^{-1} for $g \in H$.

EXAMPLE 3.2.
(1) $\widetilde{\mathrm{M}^{reg}(n,\mathbb{Z})} = \mathrm{GL}(n,\mathbb{Q})$.
(2) $\widetilde{\mathrm{CO}(n,\mathbb{Z})} = \mathrm{CO}(n,\mathbb{Q})$.

PROOF. The first statement follows from the fact that $kI_n \in \mathrm{M}^{reg}(n,\mathbb{Z})$ for any $k \in \mathbb{N}_+$. To see the second statement, we first observe an obvious inclusion: $\widetilde{\mathrm{CO}(n,\mathbb{Z})} \subset \mathrm{CO}(n,\mathbb{Q})$. Conversely, let $g \in \mathrm{CO}(n,\mathbb{Q})$. Then there exists $k \in \mathbb{Z}$ such that $kg \in \mathrm{CO}(n,\mathbb{Z})$. It follows that $g = (kI_n)^{-1}(kg) \in \widetilde{\mathrm{CO}(n,\mathbb{Z})}$. □

Here is the universality for the extension $H \rightsquigarrow \tilde{H}$: any semigroup homomorphism $\pi : H \to \mathrm{GL}_{\mathbb{C}}(V)$ extends to a group homomorphism $\tilde{\pi} : \tilde{H} \to \mathrm{GL}_{\mathbb{C}}(V)$ (see [1, Ch. 1, Section 2.4, Theorem 1 and Remark 2]).

Suppose that H is a subsemigroup of $\mathrm{M}^{reg}(n,\mathbb{Z})$. Since $\tilde{H}$ is a subgroup of $\mathrm{GL}(n,\mathbb{Q})$, we can define a subset U_H of $\mathbb{Q}^n$ by

$$U_H := \tilde{H}\mathbb{Z}^n = \{hv : h \in \tilde{H}, v \in \mathbb{Z}^n\}.$$

We note that $\mathbb{Z}^n \subset U_H$.

LEMMA 3.3. *Let* H *be a subsemigroup of* $\mathrm{M}^{reg}(n,\mathbb{Z})$*,* $\pi : H \to \mathrm{GL}_{\mathbb{C}}(V)$ *a semigroup homomorphism and* $m : \mathbb{Z}^n \to V$ *a function satisfying (2.2.1). We further assume that there is a map* $A : \mathbb{N}_+ \to \mathrm{GL}_{\mathbb{C}}(V)$ *satisfying the following two conditions: for any* $k \in \mathbb{N}_+$*,*

$$\begin{aligned} A(k)\pi(g) &= \pi(g)A(k) \quad && \text{for all } g \in H, \\ m(k\alpha) &= A(k)m(\alpha) \quad && \text{for all } \alpha \in \mathbb{Z}^n. \end{aligned} \tag{3.1.1}$$

Then m *extends uniquely to a function* $\tilde{m} : U_H \to V$ *satisfying*

$$\tilde{m}(g\alpha) = \tilde{\pi}(g)\tilde{m}(\alpha) \quad \text{for all } g \in \tilde{H} \text{ and } \alpha \in U_H. \tag{3.1.2}$$

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

REMARK 3.4. The extension $\tilde{m}$ is not necessarily bounded even though we assume the multiplier m to be bounded.

PROOF OF LEMMA 3.3. We set

$$Y := \{(g, \alpha) \in \tilde{H} \times \mathbb{Z}^n : g\alpha \in \mathbb{Z}^n\}.$$

We have an obvious inclusion $H \times \mathbb{Z}^n \subset Y$ because $H \subset \mathrm{M}^{reg}(n, \mathbb{Z})$.

First let us prove that

$$m(g\alpha) = \tilde{\pi}(g)m(\alpha) \tag{3.1.3}$$

for $(g, \alpha) \in Y$ with $g^{-1} \in H$. Since $g^{-1} \in H$ and $g\alpha \in \mathbb{Z}^n$, we have from the identity (2.2.1) that

$$m(\alpha) = m(g^{-1}g\alpha) = \pi(g^{-1})m(g\alpha).$$

As $\pi(g^{-1})$ is invertible, this can be rewritten as $\widetilde{\pi}(g)m(\alpha) = m(g\alpha)$. Hence, (2.2.1) holds under the assumption that $g \in H$ or $g \in H^{-1}$.

For the general case, let $(g, \alpha) \in Y$. We write $g \in \tilde{H}$ as $g = g_1 \cdots g_N$ $(g_1, \ldots, g_N \in H \cup H^{-1})$ and will show (3.1.3) by induction on N. Suppose that $(g, \alpha) \in Y$. We set $g' := g_2 \cdots g_N$. Since $g' \in \mathrm{GL}(n, \mathbb{Q})$, we can find $k \in \mathbb{N}_+$ such that $kg'\alpha \in \mathbb{Z}^n$. Since both $(g_1, g'k\alpha)$ and $(g', k\alpha)$ belong to Y, we have from the inductive hypothesis that

$$m(g_1g'k\alpha) = \widetilde{\pi}(g_1)m(g'k\alpha),$$
$$m(g'k\alpha) = \widetilde{\pi}(g')m(k\alpha).$$

Therefore,

$$m(kg\alpha) = m(g_1g'k\alpha) = \tilde{\pi}(g_1)\tilde{\pi}(g')m(k\alpha) = \tilde{\pi}(g)m(k\alpha).$$

By the assumption (3.1.1), this implies that $A(k)m(g\alpha) = \tilde{\pi}(g)A(k)m(\alpha)$. As $A(k)$ commutes with $\pi(g)$ for all $g \in H$, it commutes also with $\tilde{\pi}(g)$ for all $g \in \tilde{H}$. Hence, we get the identity $A(k)m(g\alpha) = A(k)\tilde{\pi}(g)m(\alpha)$. Since $A(k)$ is invertible, we obtain $m(g\alpha) = \tilde{\pi}(g)m(\alpha)$. Thus, we have shown that (3.1.3) holds for all $(g, \alpha) \in Y$.

We are ready to define $\tilde{m}$ by the relative invariance

$$\tilde{m}(g\alpha) = \tilde{\pi}(g)m(\alpha)$$

for $\alpha \in \mathbb{Z}^n$ and $g \in \tilde{H}$. To see that $\tilde{m}$ is well defined, let $g\alpha = h\beta$. Then $\alpha = g^{-1}h\beta$; hence, $m(\alpha) = m(g^{-1}h\beta) = \pi(g^{-1}h)m(\beta)$ because $(g^{-1}h, \beta) \in Y$. Thus,

$$\tilde{m}(g\alpha) = \tilde{\pi}(g)m(\alpha) = \tilde{\pi}(h)m(\beta) = \tilde{m}(h\beta),$$

which proves that $\tilde{m}$ is well defined. In this way, $\tilde{m}$ is defined for all elements in U_H and the invariance (3.1.2) is now clear. □

LEMMA 3.5. *Let H be a subsemigroup of $\mathrm{M}^{reg}(n, \mathbb{Z})$, $\pi : H \to \mathrm{GL}_{\mathbb{C}}(V)$ a semigroup homomorphism and $m : \mathbb{Z}^n \to V$ a map satisfying (2.2.1). If H contains kI_n for all $k \in \mathbb{N}_+$, then there exists a unique extension $\tilde{m} : \mathbb{Q}^n \to V$ of m satisfying*

$$\tilde{m}(g\alpha) = \tilde{\pi}(g)\tilde{m}(\alpha) \quad \textit{for all } g \in \tilde{H} \textit{ and } \alpha \in \mathbb{Q}^n.$$

PROOF. The assumption of Lemma 3.3 is fulfilled by putting $A(k) := \pi(kI)$. Then $\tilde{m}$ extends to $\mathbb{Q}^n = \tilde{H}\mathbb{Z}^n$. □

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

3.2. Reduction to number theory. Let

$$p_n : \mathrm{CO}(n, \mathbb{Q}) \to \mathbb{Q}^n \backslash \{0\}$$

be the projection by taking the first column vector. We prove that the conclusion of Theorem A holds if p_n is surjective. In the next subsection, we determine explicitly for which n, p_n is surjective.

Lemma 3.6. *Let $T : L^2(\mathbb{T}^n) \to \mathbb{C}^n \otimes L^2(\mathbb{T}^n)$ be a bounded translation invariant operator satisfying (2.3.1). If p_n is surjective, then T is a constant multiple of the Riesz transform on $\mathbb{T}^n$.*

Proof. Owing to Proposition 2.2, Lemma 3.6 is reduced to the following combinatorial lemma with $\nu = -1/n$. □

Lemma 3.7. *Let $\nu \in \mathbb{C}$. Suppose that $m : \mathbb{Z}^n \to \mathbb{C}^n$ satisfies*

$$m(g\alpha) = |\det g|^{\nu} g m(\alpha) \tag{3.2.1}$$

for any $\alpha \in \mathbb{Z}^n$ and $g \in \mathrm{CO}(n, \mathbb{Z})$. Let $e_1 := {}^t(1, 0, \ldots, 0)$. Then:

(1) *$m(0) = 0$ and $m(e_1) \in \mathbb{C}e_1$;*

(2) *if $p_n : \mathrm{CO}(n, \mathbb{Q}) \to \mathbb{Q}^n \backslash \{0\}$ is surjective, then there exists $c \in \mathbb{C}$ such that*

$$m(\alpha) = c\, \|\alpha\|^{n\nu} \alpha \quad (\alpha \in \mathbb{Z}^n \backslash \{0\}).$$

Proof of Lemma 3.7. (1) For $j = 1, 2, \ldots, n$, we denote by $g_{(j)}$ the diagonal matrix $\mathrm{diag}(1, \ldots, 1, -1, 1, \ldots, 1)$ whose jth entry is -1. Then $g_{(j)} \in \mathrm{CO}(n, \mathbb{Z})$ and $g_{(j)} e_1 = e_1$ $(2 \le j \le n)$. Applying $g = g_{(j)}$ to (3.2.1), we get $m(e_1) = m(g_{(j)} e_1) = g_{(j)} m(e_1)$. Hence, the jth entry of $m(e_1)$ vanishes for $2 \le j \le n$. Thus, we have shown that $m(e_1) = c e_1$ for some $c \in \mathbb{C}$. The same argument with $1 \le j \le n$ applied to $m(0)$ shows that $m(0) = 0$.

(2) By (1), we have $m(e_1) = c e_1$ for some $c \in \mathbb{C}$. By Proposition 3.1, m extends uniquely to a function $\tilde{m} : \mathbb{Q}^n \to \mathbb{C}^n$ satisfying (3.2.1) for any $g \in \mathrm{CO}(n, \mathbb{Q})$ and $\alpha \in \mathbb{Q}^n$. Take any $\alpha \in \mathbb{Q}^n \backslash \{0\}$. If p_n is surjective, we can find $g \in \mathrm{CO}(n, \mathbb{Q})$ such that $p_n(g) = \alpha$, that is, $g e_1 = \alpha$. Applying (3.2.1),

$$\tilde{m}(\alpha) = |\det g|^{\nu} g \tilde{m}(e_1) = c\, |\det g|^{\nu} g e_1 = c\, |\det g|^{\nu} \alpha.$$

On the other hand, taking the norms of the identity $g e_1 = \alpha$, we have $|\det g| = \|\alpha\|^n$ because $g \in \mathrm{CO}(n, \mathbb{Q})$. Thus, $\tilde{m}(\alpha)$ is of the form $c\, \|\alpha\|^{n\nu} \alpha$. Now taking $m = \tilde{m}|_{\mathbb{Z}^n}$, we get the second statement. □

3.3. Proof of Theorem A for $\mathbb{T}^n$. In this subsection, we classify all the positive integers n such that $p_n : \mathrm{CO}(n, \mathbb{Q}) \to \mathbb{Q}^n \backslash \{0\}$ is surjective (see Proposition 3.8). In particular, the equivalence of (i) and (ii) completes the proof of Theorem A by virtue of Lemma 3.6. To state the invariance conditions in Proposition 3.8, we introduce an equivalence relation $\sim$ on $\mathbb{Q}^n$ by

$$x \sim y \Leftrightarrow x = gy \quad \text{for some } g \in \mathrm{CO}(n, \mathbb{Q}).$$

This equivalence relation on $\mathbb{Q}^n$ induces the one on its subset $\mathbb{Z}^n \backslash \{0\}$, and we write $\mathbb{Z}^n \backslash \{0\}/\sim$ for the set of equivalence classes.

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

Proposition 3.8. *The following four conditions on $n \in \mathbb{N}_+$ are equivalent:*

(i) *n is one, two or a multiple of four;*
(ii) *$p_n : \mathrm{CO}(n, \mathbb{Q}) \to \mathbb{Q}^n \backslash \{0\}$ is surjective;*
(iii) *$\#(\mathbb{Z}^n \backslash \{0\}/\sim) = 1$;*
(iv) *$\#(\mathbb{Z}^n \backslash \{0\}/\sim) < \infty$.*

The rest of this subsection is devoted to the proof of Proposition 3.8. We define a subgroup Λ of $\mathbb{Q}^\times$ by

$$\Lambda := \{|\det g|^{2/n} : g \in \mathrm{CO}(n, \mathbb{Q})\}. \tag{3.3.1}$$

Lemma 3.9. *For $x, y \in \mathbb{Q}^n \backslash \{0\}$, the following two conditions are equivalent:*

(i) *$x \sim y$, that is, there exists $g \in \mathrm{CO}(n, \mathbb{Q})$ such that $y = gx$;*
(ii) $\dfrac{\|y\|^2}{\|x\|^2} \in \Lambda$.

Proof. The key to the proof is the understanding of the image of $\det : \mathrm{CO}(n, \mathbb{Q}) \to \mathbb{Q}^\times$. Suppose that $g \in \mathrm{CO}(n, \mathbb{Q})$. Then ${}^t g g = \alpha I_n$ for some $\alpha > 0$. Taking the determinant, we get $|\det g|^2 = \alpha^n$. Therefore, for $x \in \mathbb{Q}^n$,

$$\|gx\|^2 = |\det g|^{2/n} \, \|x\|^2. \tag{3.3.2}$$

Now the implication (i) $\Rightarrow$ (ii) is clear.

(ii) $\Rightarrow$ (i) We take $g \in \mathrm{CO}(n, \mathbb{Q})$ such that $|\det g|^{2/n} = \|y\|^2/\|x\|^2$. This implies that $\|y\| = \|gx\|$ by (3.3.2). By Witt's theorem (see [9, Section IV.1, Theorem 3] for instance), there exists $h \in \mathrm{O}(n, \mathbb{Q})$ such that $y = hgx$. Hence, $x \sim y$. □

We say that two quadratic forms on $\mathbb{Q}^n$ are equivalent if they are conjugate by an element in $\mathrm{GL}(n, \mathbb{Q})$. The following elementary lemma clarifies the role of the set Λ in our context.

Lemma 3.10. *For $a \in \mathbb{Q}^\times$, the following two conditions are equivalent:*

(i) *$a \in \Lambda$;*
(ii) *the quadratic forms $\|x\|^2 = \sum_{i=1}^n x_i^2$ and $a\|x\|^2$ on $\mathbb{Q}^n$ are equivalent.*

Proof. (i) $\Rightarrow$ (ii) Let $a \in \Lambda$. By the definition (3.3.1) of Λ, $a = |\det g|^{2/n}$ for some $g \in \mathrm{CO}(n, \mathbb{Q})$. This implies that ${}^t g I_n g = a I_n$ and therefore the quadratic forms $\|x\|^2$ and $a\|x\|^2$ on $\mathbb{Q}^n$ are conjugate by $g \in \mathrm{CO}(n, \mathbb{Q})$.

(ii) $\Rightarrow$ (i) Suppose that the quadratic form $a\|x\|^2$ is conjugate to $\|x\|^2$, that is, $aI_n = {}^t g I_n g$ for some $g \in \mathrm{GL}(n, \mathbb{Q})$, which implies that $g \in \mathrm{CO}(n, \mathbb{Q})$. Then we have $a = |\det g|^{2/n} \in \Lambda$. □

Proposition 3.11. *Let*

$$\mathcal{A} := \Big\{ \prod_{\substack{p_j:\mathit{prime} \\ e_j \in \mathbb{Z}}} p_j^{e_j} : e_j \text{ is odd only if } p_j = 2 \text{ or} \equiv 1 \bmod 4 \Big\}.$$

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

Then we have the following characterization of Λ*:*

$$\Lambda = \begin{cases} (\mathbb{Q}^\times)^2 & \textit{if } n \textit{ is odd,} \\ \mathcal{A} & \textit{if } n \equiv 2 \bmod 4, \\ \mathbb{Q}_+ & \textit{if } n \equiv 0 \bmod 4. \end{cases}$$

Proof. Owing to Lemma 3.10, it suffices to find a necessary and sufficient condition on $a \in \mathbb{Q}^\times$ such that the quadratic forms $\|x\|^2$ and $a\|x\|^2$ are equivalent on $\mathbb{Q}^n$. For this, we recall that the Hasse–Minkowski theorem says that two quadratic forms over $\mathbb{Q}$ are equivalent if and only if they have the same signature, discriminant modulo the squares $(\mathbb{Q}^\times)^2$ in $\mathbb{Q}^\times$ and invariants ϵ_p for all prime numbers p; see [9, Ch. IV, Section 3.3, Corollary to Theorem 9]. We recall that the Hilbert symbol $(a, b)_p$ is defined to be 1 if the equation $z^2 - ax^2 - by^2 = 0$ has a nontrivial solution in $\mathbb{Q}_p^3$ and -1 otherwise. Then ϵ_p is defined by $\epsilon_p(f) = \prod_{i<j}(a_i, a_j)_p$ for a quadratic form $f \sim a_1X_1^2 + \cdots + a_nX_n^2$.

The signatures of $\|x\|^2$ and $a\|x\|^2$ coincide if and only if $a > 0$ because $\|x\|^2$ is positive definite.

The discriminants of $\|x\|^2$ and $a\|x\|^2$ are given by 1 and a^n, respectively. They coincide in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ if and only if $a^n \in (\mathbb{Q}^\times)^2$. For n odd, this means that a itself must be a square. For n even, this does not give any restriction.

Finally, we consider the invariants ϵ_v. For $\|x\|^2$, we have $\epsilon_v = 1$ and, for $a\|x\|^2$, it is $(a, a)_v^{n(n-1)/2}$.

Case I: n is odd. Then we have seen above that a is a square; thus, $(a, a) = 1$ according to [9, Section III.1.1, Proposition 2(i)]. Hence, for n odd the only condition is that a is a square. Therefore, $\Lambda = (\mathbb{Q}^\times)^2$.

Case II: $n \equiv 0 \bmod 4$. Since $n(n-1)/2$ is even, $(a, a)_v^{n(n-1)/2} = 1$. Thus, all the invariants are the same as long as $a > 0$. Thus, we have $\Lambda = \mathbb{Q}_+$.

Case III: $n \equiv 2 \bmod 4$. Since $n(n-1)/2$ is odd, $(a, a)_v^{n(n-1)/2} = (a, a)_v$. Let $a = 2^{\alpha_0} \cdot p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$. For a prime number p,

$$(a, a)_p = \begin{cases} (-1)^{\alpha_i \epsilon(p)} & \text{if } p = p_i \text{ for some } i \ (1 \le i \le k), \\ (-1)^{\epsilon(p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k})} & \text{if } p = 2, \\ 1 & \text{otherwise,} \end{cases}$$

where ϵ is defined by $\epsilon(u) = (u-1)/2 \bmod 2$; see [9, Ch. III, Section 1.2, Theorem 1] for instance. Thus, to have $(a, a)_p = 1$ for all prime numbers p, it is necessary and sufficient to have

$$\begin{cases} \alpha_i \equiv 0 \bmod 2 & \text{whenever } p_i \equiv 3 \bmod 4 \ (1 \le i \le k), \\ p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k} \equiv 1 \bmod 4. \end{cases}$$

None of the conditions give any restriction on α_0 and the last condition follows from the first because $3^2 \equiv 1 \bmod 4$. Hence, we conclude that the set Λ consists of all rational numbers of the form $2^{\alpha_0} \cdot p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$, where the powers α_i are even if $p_i \equiv 3 \bmod 4$. Therefore, $\Lambda = \mathcal{A}$. □

ALTERNATIVE PROOF OF PROPOSITION 3.11. We would like to present a second proof based on some results by Dieudonné; see [2]. This proof of Proposition 3.11 is shorter but less direct. As before, the situation immediately reduces to the case when n is even. In our setting where we are considering the equivalence of the quadratic forms $\|x\|^2$ and $a\|x\|^2$ on $\mathbb{Q}^n$, [2, Theorems 2 and 3] can be reformulated as the statement that the subgroup $\Lambda = \mathbb{Q}_+$ for $n \equiv 0 \bmod 4$, and Λ is equal to the group of nonzero norms in the algebraic extension $\mathbb{Q} + \mathbb{Q}[i]$ for $n \equiv 2 \bmod 4$. The latter set consists of rational numbers c for which there exist rational solutions to the equation $a^2 + b^2 = c$; see also the remark on [2, page 404]. The Diophantine equation $a^2 + b^2 = c$ has an integer solution if and only if $\mathrm{ord}_p\, c$ is even for every prime $p \equiv 3 \bmod 4$; see [4, Section 17.6, Corollary 1]. Here $\mathrm{ord}_p\, c$ is the largest nonnegative integer k such that $p^k \mid c$ by $p^{k+1} \nmid c$. This proves Proposition 3.11 because the rational solutions differ from the integer solutions by only a square in the denominator. □

REMARK 3.12. There is a natural isomorphism

$$\mathbb{R}_+ \times \mathrm{O}(n) \xrightarrow{\sim} \mathrm{CO}(n), \quad (\lambda, g) \mapsto \lambda g \tag{3.3.3}$$

for all dimensions n. Further, the isomorphism (3.3.3) induces an isomorphism

$$\mathbb{Q}_+ \times \mathrm{O}(n, \mathbb{Q}) \xrightarrow{\sim} \mathrm{CO}(n, \mathbb{Q})$$

if n is odd because $|\det g|^{1/n} \in \mathbb{Q}$ for all $g \in \mathrm{CO}(n, \mathbb{Z})$ by Proposition 3.11.

Corresponding to the isomorphism (3.3.3), we have an inclusion

$$\mathbb{N}_+ \times \mathrm{O}(n, \mathbb{Z}) \hookrightarrow \mathrm{CO}(n, \mathbb{Z}),$$

where we set $\mathrm{O}(n, \mathbb{Z}) := \mathrm{O}(n) \cap \mathrm{M}(n, \mathbb{Z})$.

REMARK 3.13. The semigroup $\mathrm{CO}(n, \mathbb{Z})$ is strictly larger than the subsemigroup $\mathbb{N}_+ \times \mathrm{O}(n, \mathbb{Z})$ for any $n \geq 2$.

PROOF. The element $g \in \mathrm{CO}(n, \mathbb{Z})$ belongs to the subsemigroup only if $|\det g|^{1/n} \in \mathbb{N}_+$. For even $n = 2k$, the element

$$g := \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

belongs to $\mathrm{CO}(2k, \mathbb{Z})$ but $|\det g|^{1/n} = \sqrt{2} \notin \mathbb{N}_+$ for $k \geq 1$. Hence, this element does not belong to the subsemigroup.

For n odd, we have seen in Remark 3.12 that $\mathrm{CO}(n, \mathbb{Q}) = \mathbb{Q}_+ \times \mathrm{O}(n, \mathbb{Q})$. Taking the intersection with $\mathrm{M}(n, \mathbb{Z})$, we obtain $\mathrm{CO}(n, \mathbb{Z}) = (\mathbb{Q}_+ \times \mathrm{O}(n, \mathbb{Q})) \cap \mathrm{M}(n, \mathbb{Z})$. Since $\mathrm{O}(n, \mathbb{Q})$ is dense in $\mathrm{O}(n, \mathbb{R})$, see for example [8], $\mathbb{Q}^\times \cdot p_n(\mathrm{CO}(n, \mathbb{Z})) = p_n(\mathrm{CO}(n, \mathbb{Q}))$ is dense in $\mathbb{R}^n$. On the other hand, $\mathrm{O}(n, \mathbb{Z})$ is the set of permutation matrices with signs. Thus, $\mathbb{Q}^\times \cdot p_n(\mathbb{N}_+ \times \mathrm{O}(n, \mathbb{Z}))$ is not dense in $\mathbb{R}^n$. Therefore, $\mathbb{N}_+ \times \mathrm{O}(n, \mathbb{Z})$ is a proper subset of $\mathrm{CO}(n, \mathbb{Z})$. □

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

Proof of Proposition 3.8. First we observe that the condition (ii) is equivalent to

$$e_1 \sim x \quad \text{for any } x \in \mathbb{Q}^n \backslash \{0\},$$

which is then equivalent also to the following condition by Lemma 3.9:

(ii)′ $\|x\|^2 \in \Lambda$ for any $x \in \mathbb{Q}^n \backslash \{0\}$.

(i) ⇒ (ii)′: This implication is trivial if $n = 1$. For $n = 2$, suppose that $x = {}^t(x_1, x_2) \in \mathbb{Q}^2 \backslash \{0\}$. Then $g := \left(\begin{smallmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{smallmatrix}\right) \in CO(2, \mathbb{Q})$ and $p_2(g) = x$. This shows that p_2 is surjective. For $n \equiv 0 \bmod 4$, (ii)′ holds immediately by $\Lambda = \mathbb{Q}_+$ (see Proposition 3.11).

(ii) ⇒ (iii): If p_n is surjective, then any element in $\mathbb{Q}^n \backslash \{0\}$ is in the same equivalence class as e_1. This implies (iii).

(iii) ⇒ (iv): This is obvious.

(iv) ⇒ (i): This follows from Lemma 3.14 below. □

Lemma 3.14. *For n odd or* $n \equiv 2 \bmod 4$ *and larger than 2, we have* $\#(\mathbb{Z}^n \backslash \{0\}/\sim) = \infty$.

Proof. Suppose first that n is odd. We define a sequence of integers p_j by setting $p_1 := 1$ and using the recursive relation

$$p_j := \prod_{i=1}^{j-1} (1 + p_i^2).$$

Then, for any $i \neq j$,

$$\mathrm{GCD}(1 + p_j^2, 1 + p_i^2) = 1. \tag{3.3.4}$$

We set $\gamma_j := {}^t(1, p_j, 0, \ldots, 0)$. By Lemma 3.9 and Proposition 3.11,

$$\gamma_i \sim \gamma_j \Rightarrow \sqrt{\frac{1 + p_i^2}{1 + p_j^2}} \in \mathbb{Q}^\times.$$

By (3.3.4), this implies that $1 + p_j^2 = a^2$ for some integer a. But this is impossible because $p_j < \sqrt{1+p_j^2} < p_j + 1$. Hence, $\gamma_i \nsim \gamma_j$. Thus, we conclude that $\#(\mathbb{Z}^n \backslash \{0\}/\sim) = \infty$ if n is odd.

Suppose now that $n > 2$ and $n \equiv 2 \bmod 4$. Let p_k be the kth prime such that $p_k \equiv 3 \bmod 4$, that is,

$$p_1 = 3,\ p_2 = 7,\ p_3 = 11,\ p_4 = 19, \ldots.$$

By a theorem of Lagrange (see [9, Section IV, Appendix, Corollary 1] for example), we can find four integers a_k, b_k, c_k, d_k such that

$$a_k^2 + b_k^2 + c_k^2 + d_k^2 = p_k.$$

We set

$$\gamma_k := {}^t(a_k, b_k, c_k, d_k, 0, \ldots, 0) \in \mathbb{Z}^n.$$

Then $\|\gamma_j\|^2/\|\gamma_i\|^2 = p_j/p_i \notin \Lambda$ by Proposition 3.11. Therefore, $\gamma_i \nsim \gamma_j$ for any $i \neq j$ by Lemma 3.9. Hence, there exist infinitely many $\gamma_j \in \mathbb{Z}^n$ which are not equivalent to each other. □

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

REMARK 3.15. As we see from Theorems A and B and from Proposition 3.8, the surjectivity of $p_n : \mathrm{CO}(n, \mathbb{Q}) \to \mathbb{Q}^n \backslash \{0\}$ is a necessary and sufficient condition on n such that the maximal semigroup symmetry characterizes R. Let us consider the stronger condition of surjectivity of p_n replacing $\mathbb{Q}$ by $\mathbb{Z}$. By using the fields $\mathbb{R}, \mathbb{C}, \mathbb{H}$ and $\mathbb{O}$, we see that $p_n : \mathrm{CO}(n, \mathbb{Z}) \to \mathbb{Z}^n \backslash \{0\}$ is surjective if $n = 1, 2, 4$ and 8, respectively. This gives a partial result of Theorem A in the cases $n = 1, 2, 4$ and 8. This was the original approach when we started this project.

3.4. Proof of Theorem B for $\mathbb{T}^n$. In order to prove Theorem B, we use Proposition 2.2 and construct, for any $\nu \in \mathbb{R}$, infinitely many linearly independent multipliers $m : \mathbb{Z}^n \to \mathbb{C}^n$ for $n \geq 3$, $n \not\equiv 0 \bmod 4$ satisfying the condition

$$m(g\alpha) = |\det g|^\nu g\, m(\alpha) \quad \text{for all } \alpha \in \mathbb{Z}^n \text{ and } g \in \mathrm{CO}(n, \mathbb{Z}). \tag{3.4.1}$$

The case $\nu = -1/n$ will be used in the proof of Theorem B for $\mathbb{T}^n$, and $\nu = -(n + 1)/n$ for $\mathbb{Z}^n$; see Section 4. Proposition 3.1 gives a guiding principle to introduce the following function m_β.

LEMMA 3.16. *Fix $\beta \in \mathbb{Z}^n$ and $\nu \in \mathbb{R}$. Then the map $m_\beta : \mathbb{Z}^n \to \mathbb{C}^n$ given by*

$$m_\beta(\alpha) = \begin{cases} |\det g|^\nu \alpha & \text{if } \alpha = g\beta \text{ for some } g \in \mathrm{CO}(n, \mathbb{Q}), \\ 0 & \text{if } \alpha \nsim \beta \end{cases}$$

is well defined and satisfies (3.4.1). Further,

$$\operatorname{Supp} m_\beta = \{\alpha \in \mathbb{Z}^n : \alpha \sim \beta\}. \tag{3.4.2}$$

PROOF. If $\beta = 0$, then $m_\beta \equiv 0$ and the statement is obvious.

Suppose that $\beta \neq 0$. If $\beta = g_1\alpha = g_2\alpha$ for $g_1, g_2 \in \mathrm{CO}(n, \mathbb{Q})$, then $g_1 g_2^{-1}\beta = \beta$. Taking the norm, we see that $|\det(g_1 g_2^{-1})| = 1$ because $g_1 g_2^{-1} \in \mathrm{CO}(n, \mathbb{Q})$. Therefore, we have $|\det g_1|^\nu \alpha = |\det g_2|^\nu \alpha$ and thus $m_\beta(\alpha)$ is well defined.

Let us verify that m_β satisfies (3.4.1). Suppose that $g \in \mathrm{CO}(n, \mathbb{Z})$. For α such that $\alpha \nsim \beta$, we also have $g\alpha \nsim \beta$. Hence, $m_\beta(\alpha) = m_\beta(g\alpha) = 0$ and (3.4.1) holds. For α such that $\alpha \sim \beta$, we take $g' \in \mathrm{CO}(n, \mathbb{Q})$ such that $\alpha = g'\beta$. By definition,

$$m_\beta(\alpha) = |\det g'|^\nu \alpha,$$
$$m_\beta(g\alpha) = |\det (gg')|^\nu g\alpha.$$

Hence, $m_\beta(g\alpha) = |\det g|^\nu g m_\beta(\alpha)$ and therefore (3.4.1) holds. Thus, Lemma 3.16 is proved. □

LEMMA 3.17. *Retain the notation of Lemma 3.16. Suppose that $\gamma_j \in \mathbb{Z}^n$ $(j = 1, 2, \ldots)$ satisfies $\gamma_i \nsim \gamma_j$ for any $i \neq j$. Then m_{γ_j} $(j = 1, 2, \ldots)$ are linearly independent.*

PROOF. The supports of the m_{γ_j} are disjoint for $j = 1, 2, \ldots$ by (3.4.2). It then follows that m_{γ_j} $(j > 1, 2, \ldots)$ are linearly independent. □

PROOF OF THEOREM B. This is clear from Lemma 3.17 and from the equivalence (i) ⇔ (iv) in Proposition 3.8. □

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

4. Translation invariant operators on $\mathbb{Z}^n$

So far, we have discussed the maximal semigroup symmetry for the Riesz transforms on $\mathbb{T}^n$. In this section, we consider an analogous question for the $\mathbb{Z}^n$ case.

4.1. One-dimensional case. In this subsection, we review the characterization results for the Hilbert transform on $\mathbb{Z}$ obtained by Edwards and Gaudry in [3].

Let

$$\kappa(\alpha) = \begin{cases} 0 & \text{if } \alpha = 0, \\ \dfrac{1}{\pi\alpha} & \text{if } \alpha \neq 0. \end{cases}$$

Then the Hilbert transform H for $\mathbb{Z}$ is defined to be the operator on $l^2(\mathbb{Z})$ as the convolution with h, that is, $Hf = \kappa * f$. Then $H : l^2(\mathbb{Z}) \to l^2(\mathbb{Z})$ is a translation invariant bounded linear operator.

Remark 4.1. Here we follow the definition given in [3]. Note that $\kappa(\alpha)$ is the natural correspondent to the Hilbert kernel on $\mathbb{R}$. This kernel differs slightly from the Fourier transform of $-i\,\mathrm{sgn}\,\theta$, whose kernel can be written as $(((-1)^\alpha - 1)/2)\kappa(\alpha)$.

We recall from (2.1.1) that $D_a : l^2(\mathbb{Z}) \to l^2(\mathbb{Z})$ is a dilation for $a \in \mathbb{Z}\backslash\{0\}$.

Edwards and Gaudry proved the following characterization of the Hilbert transform on $\mathbb{Z}$.

Fact 4.2 [3, Theorem 6.8.5]. Let T be a translation invariant operator on $l^2(\mathbb{Z})$, which, for every $a \in \mathbb{Z}\backslash\{0\}$, satisfies the relation

$$T(D_a f) = a\,D_a T(f)$$

for all functions $f \in l^2(\mathbb{Z})$ with support in $a\mathbb{Z}$. Then T is a constant multiple of the Hilbert transform.

The restriction of the invariance condition to functions with support in $a\mathbb{Z}$ did not appear in the characterization theorem for the $\mathbb{R}^n$ case (Fact 1.3) or the $\mathbb{T}^n$ case (Fact 2.1). However, it cannot be relaxed in the $\mathbb{Z}$ case, as the next fact shows.

Fact 4.3 [3, Lemma 6.8.4]. If T is a translation invariant operator on $l^2(\mathbb{Z})$ such that

$$T \circ D_a = \sigma(a) D_a \circ T$$

for all $a \in \mathbb{Z}\backslash\{0\}$, where $\sigma(a)$ is a nonzero complex-valued function on $\mathbb{Z}\backslash\{0\}$, then $\sigma \equiv 1$ and T is a constant multiple of the identity.

We shall analyze Fact 4.3 for the higher dimensional case in Section 4.2.

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

4.2. Maximal semigroup symmetry. For $\beta \in \mathbb{Z}^n$, we define the translation operator $\tau_\beta : l^2(\mathbb{Z}^n) \to l^2(\mathbb{Z}^n)$ by $(\tau_\beta f)(\alpha) = f(\alpha - \beta)$. For $g \in \mathrm{M}(n, \mathbb{Z})$, let $L_g : l^2(\mathbb{Z}^n) \to l^2(\mathbb{Z}^n)$ be the linear map defined by $L_g f(\alpha) = f({}^t g\alpha)$. Let V be a finite-dimensional complex vector space.

Definition 4.4. A bounded linear operator $T : l^2(\mathbb{Z}^n) \to V \otimes l^2(\mathbb{Z}^n)$ is said to be:

(1) *translation invariant* if $T \circ \tau_\beta = (\mathrm{id} \otimes \tau_\beta) \circ T$ for all $\beta \in \mathbb{Z}^n$;
(2) *nondegenerate* if $\mathbb{C}\text{-}\operatorname{span}\{Tf(\alpha) : f \in l^2(\mathbb{Z}^n), \alpha \in \mathbb{Z}^n\}$ is equal to V.

Any translation invariant operator, $T : l^2(\mathbb{Z}^n) \to V \otimes l^2(\mathbb{Z}^n)$, can be obtained as the convolution with some kernel $\kappa : \mathbb{Z}^n \to V$:

$$Tf(\alpha) = \kappa * f(\alpha) = \sum_{\beta \in \mathbb{Z}^n} f(\beta)\kappa(\alpha - \beta), \quad f \in l^2(\mathbb{Z}^n).$$

Then T is nondegenerate if and only if $\kappa(\mathbb{Z}^n)$ spans the vector space V over $\mathbb{C}$. From now on, we assume that T is translation invariant and nondegenerate.

We will make frequent use of Kronecker's delta function

$$\delta_\gamma(\alpha) = \begin{cases} 1 & \text{if } \alpha = \gamma, \\ 0 & \text{if } \alpha \neq \gamma \end{cases}$$

in the present section.

For $g \in \mathrm{M}(n, \mathbb{Z})$ and $A \in \mathrm{GL}_{\mathbb{C}}(V)$, we consider the following conditions on the pair (g, A):

(C0) $(A \otimes L_g) \circ Tf = T \circ L_g f$ for all $f \in l^2(\mathbb{Z}^n)$;
(C1) $(A \otimes L_g) \circ Tf = T \circ L_g f$ for all $f \in l^2(\mathbb{Z}^n)$ with $\operatorname{Supp} f \subset {}^t g\mathbb{Z}^n$;
(C2) $(A \otimes L_g) \circ T\delta_0 = T \circ L_g \delta_0$;
(C3) $A\kappa({}^t g\alpha) = \kappa(\alpha)$ for all $\alpha \in \mathbb{Z}^n$.

Obviously, (C0) implies (C1).

Lemma 4.5. *The three conditions (C1), (C2) and (C3) are equivalent.*

Proof. First it is obvious that (C1) implies (C2).

(C2) $\Rightarrow$ (C3): Since $L_g \delta_0 = \delta_0$ for any $g \in \mathrm{M}(n, \mathbb{Z})$, the implication is clear from $T\delta_0 = \kappa$.

(C3) $\Rightarrow$ (C1): Take any $f \in l^2(\mathbb{Z})$ such that $\operatorname{Supp} f \subset {}^t g\mathbb{Z}^n$. Then

$$(A \otimes L_g)Tf(\alpha) = A \sum_{\beta \in \mathbb{Z}^n} f(\beta)\kappa({}^t g\alpha - \beta).$$

Since the support of f is contained in ${}^t g\mathbb{Z}^n$, the right-hand side is equal to

$$A \sum_{\gamma \in \mathbb{Z}^n} f({}^t g\gamma)\kappa({}^t g(\alpha - \gamma))$$

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

and, by the condition (C3), this is

$$= \sum_{\gamma\in\mathbb{Z}^n} f({}^t g\gamma)\kappa(\alpha-\gamma) = T(L_g f)(\alpha),$$

which gives the condition (C1). □

Lemma 4.6. *Assume that T is nondegenerate and satisfies the condition (C3) for the two pairs (g, A) and (g, A') with $A, A' \in \mathrm{GL}_{\mathbb{C}}(V)$. Then $A = A'$.*

Proof. Since A is invertible, we have by the condition (C3) that $A^{-1}\kappa(\alpha) = \kappa({}^t g\alpha)$. Since $\kappa(\mathbb{Z}^n)$ spans V, A^{-1} is uniquely determined by g. □

The characterization theorem of Edwards and Gaudry (Fact 4.2) leads us to the following definition.

Definition 4.7 (Semigroup symmetry). Let $T : l^2(\mathbb{Z}^n) \to V \otimes l^2(\mathbb{Z}^n)$ be a translation invariant bounded operator. A semigroup symmetry for T is a pair (G, π), where G is a subsemigroup of $\mathrm{M}^{reg}(n, \mathbb{Z})$ and $\pi : G \to \mathrm{GL}_{\mathbb{C}}(V)$ is a semigroup homomorphism such that T satisfies the equivalent conditions (C1), (C2) and (C3) for $(g, \pi(g))$, $g \in G$.

Among the semigroup symmetries for T, we define a partial order $(G', \sigma) \prec (G, \pi)$ if $G' \subset G$ and $\sigma(g) = \pi(g)$ for $g \in G'$.

The following proposition assures the existence of the unique maximal semigroup symmetry for a nondegenerate translation invariant operator.

Proposition 4.8 (Maximal semigroup symmetry). *Given a translation invariant and nondegenerate bounded linear V-valued operator $T : l^2(\mathbb{Z}^n) \to V \otimes l^2(\mathbb{Z}^n)$, we define G to be a subset of $\mathrm{M}^{reg}(n, \mathbb{Z})$ consisting of g for which there exists $A \in \mathrm{GL}_{\mathbb{C}}(V)$ such that (g, A) satisfies one of the equivalent conditions (C1)–(C3). Then G is a semigroup. Further, A is unique for each $g \in G$. The correspondence $g \mapsto A$ defines a semigroup homomorphism $\pi : G \to \mathrm{GL}_{\mathbb{C}}(V)$. The pair (G, π) gives the maximal semigroup symmetry for T.*

Proof. The uniqueness for A follows directly from Lemma 4.6 because T is nondegenerate. The remaining statement is clear. □

We end this subsection with some comments on the semigroup symmetry, namely, the reason why we have adopted (C1) but not (C0). In fact, the equivalence of (C1)–(C3) in Lemma 4.5 asserts that (G, π) is a maximal semigroup symmetry for the translation invariant bounded operator $T : l^2(\mathbb{Z}^n) \to V \otimes l^2(\mathbb{Z}^n)$ in the sense of condition (C1) if and only if (G, π) is a maximal pair with the following algebraic condition: $\pi(g)\kappa({}^t g\alpha) = \kappa(\alpha)$ for all $\alpha \in \mathbb{Z}^n$ and $g \in G$. On the other hand, it turns out that the condition (C0) is too strong, as Fact 4.3 already suggests in the one-dimensional case. In fact, we have the following proposition asserting that there does not exist an interesting operator T satisfying (C0) if g runs over a ‘sufficiently large’ subsemigroup H.

Proposition 4.9. *Let T be a translation invariant bounded operator from $l^2(\mathbb{Z}^n)$ to $V \otimes l^2(\mathbb{Z}^n)$ such that the following diagram*

$$\begin{array}{ccc} l^2(\mathbb{Z}^n) & \xrightarrow{T} & V \otimes l^2(\mathbb{Z}^n) \\ {\scriptstyle L_g}\downarrow & & \downarrow{\scriptstyle \pi(g)\otimes L_g} \\ l^2(\mathbb{Z}^n) & \xrightarrow{T} & V \otimes l^2(\mathbb{Z}^n) \end{array}$$

commutes for all $g \in H$, that is, the condition (C0) holds for $(g, \pi(g))$ for all $g \in H$. If H satisfies $\bigcap_{g\in H} {}^t g\mathbb{Z}^n = \{0\}$, then $TF = v \otimes F$ for some element $v \in V$.

For the proof, we use the following result.

Lemma 4.10. *Suppose that $T : l^2(\mathbb{Z}^n) \to V \otimes l^2(\mathbb{Z}^n)$ is a translation invariant bounded linear operator with kernel $\kappa : \mathbb{Z}^n \to V$. If the condition (C0) holds for (g, A) for some $A \in \mathrm{GL}_{\mathbb{C}}(V)$, then $\operatorname{Supp}\kappa \subset {}^t g\mathbb{Z}^n$.*

Proof of Lemma 4.10. Take $\gamma \notin {}^t g\mathbb{Z}^n$. Then $L_g\delta_\gamma = 0$ and therefore $AT\delta_\gamma({}^t g\alpha) = 0$ for all $\alpha \in \mathbb{Z}^n$ by (C0). Since $A \in \mathrm{GL}_{\mathbb{C}}(V)$, we obtain $T\delta_\gamma({}^t g\alpha) = 0$, which is equivalent to $\kappa({}^t g\alpha - \gamma) = 0$ for all $\alpha \in \mathbb{Z}^n$. This implies that

$$\operatorname{Supp}\kappa \subset \bigcap_{\gamma\notin {}^t g\mathbb{Z}^n} (\mathbb{Z}^n \setminus ({}^t g\mathbb{Z}^n - \gamma)) = \mathbb{Z}^n \Big\backslash \bigcup_{\gamma\in {}^t g\mathbb{Z}^n} ({}^t g\mathbb{Z}^n - \gamma) = {}^t g\mathbb{Z}^n. \qquad \square$$

Proof of Proposition 4.9. By Lemma 4.10, the support of the kernel κ must be contained in the set ${}^t g\mathbb{Z}^n$. Therefore, $\operatorname{Supp}\kappa \subset \bigcap_{g\in H} {}^t g\mathbb{Z}^n = \{0\}$. Hence, T must be of the form in the statement of the proposition. $\square$

4.3. Maximal semigroup symmetry of Riesz transform for $\mathbb{Z}^n$. The results obtained in this section are similar to the ones obtained for $\mathbb{T}^n$, but there is a new feature to take into account; see Facts 4.2 and 4.3.

Definition 4.11. The Riesz transforms for $\mathbb{Z}^n$ are defined by convolving with the kernels K_j $(1 \le j \le n)$,

$$K_j(\alpha) = \begin{cases} \dfrac{\Gamma(\frac{n+1}{2})}{\pi^{\frac{n+1}{2}}} \dfrac{\alpha_j}{\|\alpha\|^{n+1}} & \text{if } \alpha \neq 0, \\ 0 & \text{if } \alpha = 0. \end{cases}$$

This is the discrete version of the corresponding kernel for the Riesz transforms on $\mathbb{R}^n$; see Definition 1.2.

For $j = 1$, this coincides with the Hilbert transform of Edwards and Gaudry; see Section 4.1.

Proposition 4.12. *The maximal semigroup symmetry of the Riesz transform on $\mathbb{Z}^n$ is given by $(\mathrm{CO}(n,\mathbb{Z}), \rho)$, where*

$$\rho : \mathrm{CO}(n,\mathbb{Z}) \to \mathrm{GL}(n,\mathbb{C}),\ g \mapsto |\det g|^{(n+1)/n}\, {}^t g^{-1}.$$

https://doi.org/10.1017/S144678871500049X Published online by Cambridge University Press

Proof. Clearly, $(\mathrm{CO}(n,\mathbb{Z}),\rho)$ is a semigroup symmetry for $\kappa = (K_1,\ldots,K_n)$. Thus, the proposition follows directly from the following lemma. □

Lemma 4.13. *Let $\kappa = (K_1,\ldots,K_n)$ be the kernel of the Riesz transform. Assume that there exist $A \in \mathrm{GL}_{\mathbb{C}}(V)$ and $g \in \mathrm{M}^{reg}(n,\mathbb{Z})$ such that*

$$A\kappa(\alpha) = \kappa({}^t g\alpha) \quad \textit{for all } \alpha \in \mathbb{Z}^n.$$

Then $g \in \mathrm{CO}(n,\mathbb{Z})$ and $A = |\det g|^{-(n+1)/n}\,{}^t g$.

Proof. Since $\kappa(\alpha) = C_n(\alpha/\|\alpha\|^{n+1})$, where C_n is a nonzero constant depending only on the dimension n, $A\kappa(\alpha) = \kappa({}^t g\alpha)$ implies that

$$A\frac{\alpha}{\|\alpha\|^{n+1}} = \frac{{}^t g\alpha}{\|{}^t g\alpha\|^{n+1}}. \tag{4.3.1}$$

For $1 \le i \le n$, we denote by ${}^t g_i$ the ith column vector of ${}^t g$. Applying Equation (4.3.1) to $\alpha = e_i$, the ith unit vector, we get $Ae_i = ({}^t g)_i/\|({}^t g)_i\|^{n+1}$. For $n = 1$, this is what we wanted to prove, so let $n > 1$. Then

$$A\Big(\frac{e_i + e_j}{\sqrt{2}}\Big) = \Big(\frac{{}^t g_i}{\|{}^t g_i\|^{n+1}} + \frac{{}^t g_j}{\|{}^t g_j\|^{n+1}}\Big)\frac{1}{\sqrt{2}},$$

whereas Equation (4.3.1) with $\alpha = e_i + e_j$ gives

$$A\Big(\frac{e_i + e_j}{\sqrt{2}}\Big) = \frac{(\sqrt{2})^{n+1}}{\sqrt{2}}\frac{{}^t g_i + {}^t g_j}{\|{}^t g_i + {}^t g_j\|^{n+1}}.$$

Since $g \in \mathrm{M}^{reg}(n,\mathbb{Z})$, ${}^t g_i$ and ${}^t g_j$ are linearly independent. Comparing the coefficients of ${}^t g_i$ and ${}^t g_j$ in the two expressions, we obtain $\|{}^t g_i + {}^t g_j\| = \sqrt{2}\|{}^t g_i\| = \sqrt{2}\|{}^t g_j\|$. Then we have $\|{}^t g_i + {}^t g_j\|^2 = \|{}^t g_i\|^2 + \|{}^t g_j\|^2$, which implies that $(g_i, g_j) = 0$. Hence, $g \in \mathrm{CO}(n,\mathbb{Z})$. Then $|\det g| = \|g_i\|^n$ for all i. Since $Ae_i = {}^t g_i/\|{}^t g_i\|^{n+1}$ $(1 \le i \le n)$, we get $A = |\det g|^{-(n+1)/n}\,{}^t g$. □

Proof of Theorems A and B in the $\mathbb{Z}^n$ case. The maximal semigroup symmetry for the Riesz transform on $\mathbb{Z}^n$ imposes the invariance condition on the convolution kernel $\kappa : \mathbb{Z}^n \to V$ (see (C3))

$$|\det g|^{(n+1)/n}\,{}^t g^{-1}\kappa({}^t g\alpha) = \kappa(\alpha)$$

for all $\alpha \in \mathbb{Z}^n$ and $g \in \mathrm{CO}(n,\mathbb{Z})$ by Proposition 4.12. This is equivalent to

$$\kappa(g\alpha) = |\det g|^{-(n+1)/n} g\kappa(\alpha) \tag{4.3.2}$$

for all $\alpha \in \mathbb{Z}^n$ and $g \in \mathrm{CO}(n,\mathbb{Z})$. By Lemma 3.7 with $\nu = -(n+1)/n$ and Proposition 3.8, any κ satisfying (4.3.2) must be a scalar multiple of the convolution kernel of the Riesz transform if $n = 1, 2$ or $n \equiv 0 \bmod 4$. Hence, Theorem A for $\mathbb{Z}^n$ is proved.

Suppose that $n > 2$ and $n \not\equiv 0 \bmod 4$. By Lemma 3.17 with $\nu = -(n+1)/n$ and the equivalence (i) $\Leftrightarrow$ (iv) in Proposition 3.8, there exists infinitely many linearly independent κ satisfying (4.3.2). Then the corresponding translation invariant operators are linearly independent because the convolution kernel determines uniquely the operators (to see this, one may apply $\delta_\gamma \in l^2(\mathbb{Z}^n)$). □

5. Saturated semigroup symmetry

For $n > 2$ and $n \not\equiv 0 \bmod 4$, we have seen in Theorem B that there are infinitely many linearly independent translation invariant operators that satisfy the maximal semigroup symmetry of the Riesz transforms for $\mathbb{T}^n$ and $\mathbb{Z}^n$. We may ask what are other invariance conditions that can single out the Riesz transforms on $\mathbb{T}^n$ and $\mathbb{Z}^n$. In this section, we introduce a little more technical condition (*saturated semigroup symmetry*), which characterizes the Riesz transforms on $\mathbb{T}^n$ and $\mathbb{Z}^n$ (up to a scalar) for all dimensions n.

5.1. Characterization of the Riesz transform on $\mathbb{T}^n$. We define the following set:

$$\Xi := \{(g, \alpha) \in CO(n) \times \mathbb{Z}^n : g\alpha \in \mathbb{Z}^n\}.$$

Let $f_\alpha(x) := e^{2\pi i\langle \alpha, x\rangle}$ for $\alpha \in \mathbb{Z}^n$. For any $(g, \alpha) \in \Xi$, the function $L_{{}^t g} f_\alpha$ is well defined as a function on $\mathbb{T}^n$ by

$$(L_{{}^t g} f_\alpha)(x) := e^{2\pi i\langle \alpha, {}^t g x\rangle} = e^{2\pi i\langle g\alpha, x\rangle}.$$

We say that a bounded translation invariant operator $T : L^2(\mathbb{T}^n) \to \mathbb{C}^n \otimes L^2(\mathbb{T}^n)$ satisfies a *saturated semigroup symmetry* for Ξ if it satisfies the identity

$$(T f_\alpha)(0) = |\det g|^{-1/n} g(T(L_{{}^t g} f_\alpha)(0)) \tag{5.1.1}$$

for all pairs $(g, \alpha) \in \Xi$.

We recall from Proposition 3.1 and Example 3.2 that the invariance condition $m(g\alpha) = |\det g|^{-1/n} g(m(\alpha))$ extends to invariance under the set

$$Y := \{(g, \alpha) \in CO(n, \mathbb{Q}) \times \mathbb{Z}^n : g\alpha \in \mathbb{Z}^n\}.$$

We note that $Y \subsetneq \Xi$. We shall characterize the Riesz transforms on $\mathbb{T}^n$ and $\mathbb{Z}^n$ by using the larger set Ξ.

Then the Riesz transform on $\mathbb{T}^n$ can be recovered from the saturated semigroup symmetry for Ξ for any dimension n.

Theorem 5.1. *If $T : L^2(\mathbb{T}^n) \to \mathbb{C}^n \otimes L^2(\mathbb{T}^n)$ is a bounded translation invariant operator satisfying the identity (5.1.1) for all pairs $(g, \alpha) \in \Xi$, then $T = cR$ for some $c \in \mathbb{C}$, where $R = (R_1, \ldots, R_n)$ is the Riesz transform on $\mathbb{T}^n$.*

Proof. As in the proof of Proposition 2.2, the multiplier $m : \mathbb{Z}^n \to \mathbb{C}^n$ for the operator T satisfies

$$m(\alpha) = |\det g|^{-1/n} g m({}^t g\alpha).$$

The result then follows from Lemma 5.2 below. □

Lemma 5.2. *Fix $\nu \in \mathbb{R}$. If a function $F : \mathbb{Z}^n \to \mathbb{C}^n$ satisfies the condition*

$$F(g\alpha) = |\det g|^\nu g F(\alpha) \quad \textit{for all pairs } (g, \alpha) \in \Xi,$$

then F is unique up to multiplication with a scalar.

Proof. Since for any $\alpha \in \mathbb{Z}^n$ there exists an element $g \in CO(n)$ such that $(g, e_1) \in \Xi$ and $\alpha = g e_1$, the proof follows in the same way as in the proof of Lemma 3.7. □

5.2. Characterization of the Riesz transform on $\mathbb{Z}^n$. In a similar way as in the previous subsection, the Riesz transform on $\mathbb{Z}^n$ is recovered from the saturated semigroup symmetry for Ξ for all dimensions n.

THEOREM 5.3. *Let $T : l^2(\mathbb{Z}^n) \to \mathbb{C}^n \otimes l^2(\mathbb{Z}^n)$ be a bounded translation invariant operator satisfying the identity*

$$L_g(T\delta_0)(\alpha) = |\det g|^{-((n-1)/n)} g(T\delta_0(\alpha)) \tag{5.2.1}$$

for all pairs $(g, \alpha) \in \Xi$. Then $T = cR$ for some $c \in \mathbb{C}$, where $R = (R_1, \ldots, R_n)$ denotes the Riesz transform on $\mathbb{Z}^n$.

PROOF. The condition (5.2.1) is equivalent to that of the corresponding kernel $\kappa : \mathbb{Z}^n \to \mathbb{C}^n$ of T, namely,

$$\kappa(g\alpha) = |\det g|^{-((n-1)/n)} g\kappa(\alpha).$$

Then Lemma 5.2 implies that κ must be a constant multiple of the Riesz transform on $\mathbb{Z}^n$. □

References

[1] N. Bourbaki, *Elements of Mathematics: Algebra I* (Springer, Berlin, 1989).

[2] J. Dieudonné, 'Sur les multiplicateurs des similitudes', *Rend. Circ. Mat. Palermo* (2) **3** (1954), 398–408; reproduced in *Choix d'oevres mathématiques*, Tome II (Hermann, Paris, 1981), 408–418 (in French).

[3] R. E. Edwards and G. I. Gaudry, *Littlewood–Paley and Multiplier Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (2), 90 (Springer, Berlin–Heidelberg, 1977).

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, 84 (Springer, New York, 1990).

[5] T. Kobayashi and A. Nilsson, 'Group invariance and L^p-bounded operators', *Math. Z.* **260** (2008), 335–354.

[6] T. Kobayashi and A. Nilsson, 'Indefinite higher Riesz transforms', *Ark. Mat.* **47** (2009), 331–344.

[7] M. Sato, 'Theory of prehomogeneous vector spaces (algebraic part)—the English translation of Sato's lecture from Shintani's note', *Nagoya Math. J.* **120** (1990), 1–34; English translation of *Sugaku-no-Ayumi* **15** (1970), 83–157 (translated by M. Muro).

[8] E. Schmutz, 'Rational points on the unit sphere', *Cent. Eur. J. Math.* **6** (2008), 482–487.

[9] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, 7 (Springer, New York, 1996).

[10] E. M. Stein, *Singular Integrals and Differentiability Properties of Functions*, Princeton Mathematical Series, 30 (Princeton University Press, Princeton, NJ, 1970).

[11] E. M. Stein and G. Weiss, *Introduction to Fourier Analysis on Euclidean Spaces*, Princeton Mathematical Series, 32 (Princeton University Press, Princeton, NJ, 1971).

TOSHIYUKI KOBAYASHI, Kavli IPMU, Japan
and
Graduate School of Mathematical Sciences, The University of Tokyo,
3-8-1 Komaba Meguro-ku, Tokyo 153-8914, Japan
e-mail: toshi@ms.u-tokyo.ac.jp

ANDREAS NILSSON, SAAB AB, Bröderna Ugglas gata,
58254 Linköping, Sweden
e-mail: andreas.nilsson@saabgroup.com

FUMIHIRO SATO, Department of Mathematics, Rikkyo University,
3-34-1 Nishi-Ikebukuro Toshima-ku, Tokyo 171-8501, Japan
e-mail: sato@rikkyo.ac.jp