Maximal semigroup symmetry and discrete Riesz transforms

Toshiyuki Kobayashi*
the University of Tokyo
E-mail address: toshi@ms.u-tokyo.ac.jp

Andreas Nilsson†
SAAB AB
E-mail address: andreas.nilsson@saabgroup.com

and

Fumihiro Sato
Rikkyo University
E-mail address: sato@rikkyo.ac.jp

to the memory of Professor Garth Gaudry

August 11, 2015

Abstract

We raise a question if the Riesz transform on $\mathbf{T}^n$ or $\mathbf{Z}^n$ is characterized by the "maximal semigroup symmetry" that they satisfy? We prove that this is the case if and only if the dimension $n = 1, 2$ or a multiple of four. This generalizes a theorem of Edwards and Gaudry for the Hilbert transform (*i.e.* the $n = 1$ case) on $\mathbf{T}$ and $\mathbf{Z}$, and extends a theorem of Stein for the Riesz transform on $\mathbf{R}^n$. Unlike the $\mathbf{R}^n$ case, we show that there exist infinitely many, linearly independent multiplier operators that enjoy the same maximal semigroup symmetry as the Riesz transforms on $\mathbf{T}^n$ and $\mathbf{Z}^n$ if $n \geq 3$ and is not a multiple of four.

---

*Partially supported by Grant-in-Aid for Scientific Research (A)(25247006), Japan Society for the Promotion of Science.

†Partially supported by Japan Society for the Promotion of Science.

2000 Mathematics Subject Classification. 42B15; Secondary 22E46, 42B20.

Key words and phrases. Multiplier, translation invariant operator, Riesz transform, Hilbert transform, Fourier series, semigroup representation, Hasse–Minkowski principle

Contents

1 Introduction **2**

2 Maximal semigroup symmetry of translation invariant operators on $\mathbf{T}^n$ **6**
2.1 The Hilbert transform on the circle $\mathbf{T}$ 6
2.2 Covariance of vector-valued multipliers on $\mathbf{Z}^n$ 8
2.3 Riesz transform on $\mathbf{T}^n$ 10

3 Proof of main theorems for $\mathbf{T}^n$ **11**
3.1 From semigroup to group invariance 11
3.2 Reduction to number theory 13
3.3 Proof of Theorem A for $\mathbf{T}^n$ 14
3.4 Proof of Theorem B for $\mathbf{T}^n$ 19

4 Translation invariant operators on $\mathbf{Z}^n$ **20**
4.1 One-dimensional case 20
4.2 Maximal semigroup symmetry 21
4.3 Maximal semigroup symmetry of Riesz transform for $\mathbf{Z}^n$ 23

5 Saturated semigroup symmetry **25**
5.1 Characterization of the Riesz transform on $\mathbf{T}^n$ 25
5.2 Characterization of the Riesz transform on $\mathbf{Z}^n$ 26

1 Introduction

Classical multipliers such as the Hilbert transform on $\mathbf{R}$ or the Riesz transform on $\mathbf{R}^n$ are translation invariant operators with additional "symmetries" that can be formulated in terms of group representations (see (1.1.1) below). E.M. Stein proved that a covariance property under the conformal group characterizes the Riesz transform on $\mathbf{R}^n$ up to scalar multiplication, see Fact 1.3. Extending his idea, we provided in [KN1] a general framework to characterize specific operators on $\mathbf{R}^n$ by a covariance property with respect to arbitrary (finite-dimensional) representation 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 $\mathbf{Z}^n$ and $\mathbf{T}^n$ by means of algebraic conditions (*semigroup symmetry*).

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

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

Condition 1.1. *$T_j \circ l_g$, $(1 \leq j \leq N)$ 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 $\mathrm{GL}(n, \mathbf{R})$.*

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

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

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

where V is an N-dimensional complex vector space. Suppose that H is a subgroup of $\mathrm{GL}(n, \mathbf{R})$ and that $\pi : H \to \mathrm{GL}_{\mathbf{C}}(V)$ 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 $\mathcal{B}_H(L^2(\mathbf{R}^n), V \otimes L^2(\mathbf{R}^n))$ the vector space of bounded translation invariant operators T satisfying (1.1.1).

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

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

It is isomorphic to the direct product group $\mathbf{R}_+ \times \mathrm{O}(n)$, 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 $\mathbf{R}^n$:

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

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

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

Now, Stein's characterization of Riesz transforms ([S, Section 3.1]) can be formulated as follows:

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

We write $(\mathbf{R}^n)^\wedge$ $(\simeq \mathbf{R}^n)$ for the dual space of $\mathbf{R}^n$. In [KN1, Corollary 2.1.2], Fact 1.3 is extended to the following:

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

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

where

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

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) $\dim V = 1$ (*e.g.* 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 M. Sato, see [Sa])

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 $\mathbf{T}^n$ and $\mathbf{Z}^n$ is defined as translation invariant operator $L^2(\mathbf{F}^n) \to \mathbf{C}^n \otimes L^2(\mathbf{F}^n), (\mathbf{F} = \mathbf{T}, \mathbf{Z})$ in Definitions 2.5 and 4.10 respectively, in an analogous fashion to the $\mathbf{R}^n$ case. We shall observe that for the Riesz transform on $\mathbf{T}$ and $\mathbf{Z}$, (*i.e.* the Hilbert transform on $\mathbf{T}$ and $\mathbf{Z}$) the algebraic structure to formulate the invariance condition (1.1.1) fits better with semigroups rather than groups.

In [EG], Edwards and Gaudry proved a discrete analog of Fact 1.3 for $n = 1$, giving a characterization of the Hilbert transforms on $\mathbf{T}$ and $\mathbf{Z}$ by "semigroup symmetry".

The goal of this article is to formulate the maximal semigroup symmetry for vector-valued translation invariant operators on $\mathbf{T}^n$ and $\mathbf{Z}^n$ in general and to investigate to what extent Edwards–Gaudry's characterization works for the Riesz transforms on $\mathbf{T}^n$ and $\mathbf{Z}^n$ 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 $\mathbf{R}^n$ case. For a formulation of "invariant multipliers" on $\mathbf{T}^n (= \mathbf{R}^n/\mathbf{Z}^n)$ or $\mathbf{Z}^n$ one natural way is to use only injective linear transformations that preserve the lattice $\mathbf{Z}^n$. Namely, the semigroup

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

Unlike the $\mathbf{R}$ case, we note

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

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

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

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

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

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

translation invariant if $T \circ \tau_\alpha = (\mathrm{id} \otimes \tau_\alpha) \circ T$ *for all* $\alpha \in \mathbf{R}^n$;

non-degenerate if $\mathbf{C}$*-span*$\{Tf(t) : f \in L^2(\mathbf{T}^n), t \in \mathbf{T}^n\}$ *is equal to* V.

A semigroup symmetry for T is a pair (G, π) where G is a subsemigroup of $\mathrm{M}^{reg}(n, \mathbf{Z})$, and $\pi : G \to GL_{\mathbf{C}}(V)$ 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 non-degenerate translation invariant operator $T : L^2(\mathbf{T}^n) \to V \otimes L^2(\mathbf{T}^n)$ there exists a unique maximal semigroup symmetry. In fact, let G be a subset of $\mathrm{M}^{reg}(n, \mathbf{Z})$ consisting of all g for which there exists $A \in \mathrm{GL}_{\mathbf{C}}(V)$ 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 $G \to \mathrm{GL}_{\mathbf{C}}(V)$, $g \mapsto A$ 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 $l^2(\mathbf{Z}^n)$, but it is slightly more involved, see Section 4.2.*

Example 1.8. *Let $G_{\mathbf{T}} = \mathrm{CO}(n, \mathbf{Z}) := \mathrm{CO}(n) \cap \mathrm{M}(n, \mathbf{Z})$, $G_{\mathbf{R}} = \mathrm{CO}(n)$ and $\pi(g) = |\det g|^{-1/n} g$. Let $G_{\mathbf{Z}} = \mathrm{CO}(n, \mathbf{Z})$ and $\rho(g) = |\det g|^{n+1/n}\, {}^t g^{-1}$. Then $(G_{\mathbf{T}}, \pi)$ and $(G_{\mathbf{R}}, \pi)$ are the maximal semigroup symmetries for the Riesz transforms on $\mathbf{T}^n$ and $\mathbf{R}^n$ respectively and the pair $(G_{\mathbf{Z}}, \rho)$ is the maximal semigroup symmetry for the Riesz transforms on $\mathbf{Z}^n$, see Propositions 2.6 and 4.11. Note that $G_{\mathbf{R}}$ is in fact a group, but $G_{\mathbf{T}}$ and $G_{\mathbf{Z}}$ are just semigroups.*

Definition-Proposition 1.6 asserts that any non-degenerate translation invariant operator gives rise to the unique semigroup symmetry. Conversely, we may ask:

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 $\mathbf{R}^n$ for all dimensions n. Edwards and Gaudry proved that this is also the case for the Hilbert transform on the circle $\mathbf{T}$ and on $\mathbf{Z}$ (*i.e.* the Riesz transform on the torus $\mathbf{T}^n$ and on $\mathbf{Z}^n$ for $n = 1$), see Fact 2.1 and Fact 4.1, respectively.

Here are the main results of this article.

Theorem A. *If the dimension $n = 1, 2$ or a multiple of four, then the maximal semigroup symmetry $(\mathrm{CO}(n, \mathbf{Z}), |\det g|^{-1/n} g)$ and $(\mathrm{CO}(n, \mathbf{Z}), |\det g|^{n+1/n}\, {}^t g^{-1})$ characterizes the Riesz transforms on $\mathbf{T}^n$ and $\mathbf{Z}^n$ respectively.*

Theorem B. *Suppose* $n \geq 3$ *and* $n \not\equiv 0 \pmod 4$. *Then there exist infinitely many linearly independent multipliers on* $\mathbf{T}^n$ *and* $\mathbf{Z}^n$ *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 $\mathbf{T}^n$ and $\mathbf{Z}^n$ are very different from Stein's theorem in the $\mathbf{R}^n$ case.

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

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

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

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

2.1 The Hilbert transform on the circle T

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

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

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

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

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

Clearly the operator T_m is translation invariant, that is,

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

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

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

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

$$\begin{aligned} D_a f(t) &:= f(at) \qquad \text{if } f \in L^2(\mathbf{T}) && (2.1.1)\\ D_a F(\alpha) &:= F(a\alpha) \qquad \text{if } F \in l^2(\mathbf{Z}) && (2.1.2) \end{aligned}$$

respectively. Then we have

$$D_a \circ \mathcal{F} \circ D_a = \mathcal{F}. \tag{2.1.3}$$

In other words, we have

$$(\mathcal{F} \circ D_a f)(\beta) = \begin{cases} (\mathcal{F}f)(a^{-1}\beta) & \beta \in a\mathbf{Z} \\ 0 & \beta \in \mathbf{Z} \setminus a\mathbf{Z}. \end{cases}$$

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

$$H \circ D_a = \operatorname{sgn}(a) D_a \circ H \quad \text{for any } a \in \mathbf{Z} \setminus \{0\}. \tag{2.1.4}$$

Conversely, suppose that a multiplier operator T_m satisfies (2.1.4). 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 (2.1.3). In terms of the multiplier m, this amounts to

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

Using (2.1.3) again, we have

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

for any $f \in L^2(\mathbf{T})$. Hence $m(a\alpha) = \operatorname{sgn}(a) m(\alpha)$ for any $a \in \mathbf{Z} \setminus \{0\}$ and $\alpha \in \mathbf{Z}$. 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:

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

$$T_m \circ D_a = \operatorname{sgn}(a) D_a \circ T_m \quad \textit{for all } a \in \mathbf{Z} \setminus \{0\},$$

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 $\mathrm{M}^{reg}(1, \mathbf{Z}) \cong \mathbf{Z} \setminus \{0\}$ in the sense of Definition-Proposition 1.6.

2.2 Covariance of vector-valued multipliers on $\mathbf{Z}^n$

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

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

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

We define the Fourier transform

$$\mathcal{F} : L^2(\mathbf{T}^n) \to l^2(\mathbf{Z}^n) \tag{2.2.1}$$

by $(\mathcal{F}f)(\alpha) := \int_{\mathbf{T}^n} f(x) e^{-2\pi i \langle \alpha, x \rangle} dx$ for $\alpha \in \mathbf{Z}^n$. 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 $\mathbf{C}$. Given a bounded function $m : \mathbf{Z}^n \to V$, we define a linear operator

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

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

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

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

$$m(g\alpha) = \pi(g) m(\alpha) \quad \text{for all } \alpha \in \mathbf{Z}^n \text{ and all } g \in H. \tag{2.2.2}$$

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 ${}^t g \in \mathrm{M}^{reg}(n, \mathbf{Z})$ if and only if $g \in \mathrm{M}^{reg}(n, \mathbf{Z})$.

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

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

Proof. Since $m \mapsto e^{-2\pi i\langle\alpha,m\rangle}$ is a character of the finite group $\mathbf{Z}/{}^tg\mathbf{Z}^n$, the formula follows from Schur's orthogonality relation and from the identity $\sharp(\mathbf{Z}^n/{}^tg\mathbf{Z}) = |\det g|$. □

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

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

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

Proof.

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

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:

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

for all $g \in H$. This is clearly equivalent to the condition (2.2.2). □

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 $t = 0$ we obtain

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

Since $m(\alpha) = \mathcal{F}\kappa(\alpha) = (\kappa * e^{2\pi i\langle\alpha,\cdot\rangle})(0) = T_m(e^{2\pi i\langle\alpha,\cdot\rangle})(0)$, we obtain $\pi(g)m(\alpha) = m(g\alpha)$. Conversely, if $\pi(g)m(\alpha) = m(g\alpha)$. Then the same argument gives

$$\pi(g)(T_m(e^{2\pi i\langle\alpha,\cdot\rangle})(0)) = T_m(e^{2\pi i\langle\alpha,{}^tg\cdot\rangle})(0). \tag{2.2.3}$$

By definition, $T_m(L_g e^{2\pi i\langle\alpha,\cdot\rangle})(s) = T_m(e^{2\pi i\langle\alpha,{}^tg\cdot\rangle})(s) = \tau_{-s}T_m(e^{2\pi i\langle\alpha,{}^tg\cdot\rangle})(0)$. Since T_m is translation invariant this is $T_m(\tau_{-s}e^{2\pi i\langle\alpha,{}^tg\cdot\rangle})(0) = T_m(e^{2\pi i\langle\alpha,{}^tg\cdot+{}^tgs\rangle})(0)$

Using the linearity of T_m we can rewrite this as $e^{2\pi i\langle\alpha,{}^tgs\rangle}T_m(e^{2\pi i\langle\alpha,{}^tg\cdot\rangle})(0)$. By (2.2.3) we obtain $e^{2\pi i\langle\alpha,{}^tgs\rangle}\pi(g)T_m(e^{2\pi i\langle\alpha,\cdot\rangle})(0)$. By linearity we have

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

Using the translation invariance again, we see that this equals

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

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 $L^2(\mathbf{T}^n)$. □

2.3 Riesz transform on $\mathbf{T}^n$

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

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

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

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

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 scalar.

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

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

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

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

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

namely, $(\pi(g) \otimes L_g) \circ R = R \circ L_g$ for all $g \in \mathrm{CO}(n, \mathbf{Z})$. It remains to prove that (H, π) is the maximal semigroup symmetry. For this we use Proposition 2.2. Let $g \in \mathrm{M}^{reg}(n, \mathbf{Z})$ and suppose that there exists $A \in \mathrm{GL}(n, \mathbf{C})$ such that $m_R(g\alpha) = Am_R(\alpha)$, for all $\alpha \in \mathbf{Z}^n$. We shall show that $g \in \mathrm{CO}(n, \mathbf{Z})$. Indeed, as $m_R(\alpha) = -i\frac{\alpha}{\|\alpha\|}$ we obtain $\frac{g\alpha}{\|g\alpha\|} = A\frac{\alpha}{\|\alpha\|}$. Taking norms, this implies in particular that $A \in \mathrm{O}(n)$ since $\|A\alpha\| = \|\alpha\|$, for all $\alpha \in \mathbf{Z}^n$. 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 $\vec{A}_i = \frac{\vec{g}_i}{\|\vec{g}_i\|}$, *i.e.* $A = (\lambda_1 \vec{g}_1, \ldots, \lambda_n \vec{g}_n)$. 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 $\lambda = |\det g|^{-\frac{1}{n}}$. Hence $g \in \mathrm{CO}(n) \cap \mathrm{M}(n, \mathbf{Z}) = H$, and $A = \pi(g)$. Therefore (H, π) is the maximal semigroup symmetry of the Riesz transform. □

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

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

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

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

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

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

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

Example 3.2. 1) $\widetilde{\mathrm{M}^{reg}(n, \mathbf{Z})} = \mathrm{GL}(n, \mathbf{Q})$.

2) $\widetilde{\mathrm{CO}(n, \mathbf{Z})} = \mathrm{CO}(n, \mathbf{Q})$

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

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

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

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

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

Lemma 3.3. *Let H be a subsemigroup of $\mathrm{M}^{reg}(n, \mathbf{Z})$, $\pi : H \to \mathrm{GL}_{\mathbf{C}}(V)$ a semigroup homomorphism, and $m : \mathbf{Z}^n \to V$ a function satisfying (2.2.2). We further assume that there is a map $A : \mathbf{N}_+ \to \mathrm{GL}_{\mathbf{C}}(V)$ satisfying the following two conditions: for any $k \in \mathbf{N}_+$,*

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

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

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

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

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

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

First let us prove

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

for $(g, \alpha) \in Y$ with $g^{-1} \in H$. Since $g^{-1} \in H$ and $g\alpha \in \mathbf{Z}^n$, we have from the identity (2.2.2) 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 (2.2.2) holds under the assumption $g \in H$ 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 $(g, \alpha) \in Y$. We set $g' := g_2 \cdots g_N$. Since $g' \in \mathrm{GL}(n, \mathbf{Q})$, we can find $k \in \mathbf{N}_+$ such that $kg'\alpha \in \mathbf{Z}^n$. Since both $(g_1, g'k\alpha)$ and $(g', k\alpha)$ belong to Y, we have from the inductive hypothesis that

$$\begin{aligned} m(g_1 g' k\alpha) &= \widetilde{\pi}(g_1)m(g'k\alpha), \\ m(g'k\alpha) &= \widetilde{\pi}(g')m(k\alpha). \end{aligned}$$

Therefore we have

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

By the assumption (3.1.1), this implies $A(k)m(g\alpha) = \tilde{\pi}(g)A(k)m(\alpha)$. 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 $\alpha \in \mathbf{Z}^n$ 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 we have $\tilde{m}(g\alpha) = \tilde{\pi}(g)m(\alpha) = \tilde{\pi}(h)m(\beta) = \tilde{m}(h\beta)$, 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 $\mathrm{M}^{reg}(n, \mathbf{Z})$, $\pi : H \to \mathrm{GL}_{\mathbf{C}}(V)$ a semigroup homomorphism, and $m : \mathbf{Z}^n \to V$ a map satisfying (2.2.2). If H contains kI_n for all $k \in \mathbf{N}_+$ then there exists a unique extension $\tilde{m} : \mathbf{Q}^n \to V$ of m satisfying*

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

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

3.2 Reduction to number theory

Let

$$p_n : \mathrm{CO}(n, \mathbf{Q}) \to \mathbf{Q}^n \setminus \{0\} \tag{3.2.1}$$

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 $T : L^2(\mathbf{T}^n) \to \mathbf{C}^n \otimes L^2(\mathbf{T}^n)$ 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 $\mathbf{T}^n$.*

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

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

$$m(g\alpha) = |\det g|^\nu g m(\alpha) \tag{3.2.2}$$

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

1) $m(0) = 0$ and $m(e_1) \in \mathbf{C}e_1$.

2) If $p_n : \mathrm{CO}(n, \mathbf{Q}) \to \mathbf{Q}^n \setminus \{0\}$ is surjective, then there exists $c \in \mathbf{C}$ such that

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

Proof of Lemma 3.7. 1) For $j = 1, 2, \dots, n$, we denote by $g_{(j)}$ the diagonal matrix $\mathrm{diag}(1, \dots, 1, -1, 1, \dots, 1)$ whose j th entry is -1. Then $g_{(j)} \in \mathrm{CO}(n, \mathbf{Z})$ and $g_{(j)}e_1 = e_1$ $(2 \le j \le n)$. Applying $g = g_{(j)}$ to (3.2.2), 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 $2 \leq j \leq n$. Thus we have shown $m(e_1) = ce_1$ for some $c \in \mathbf{C}$. The same argument with $1 \leq j \leq n$ applied to $m(0)$ shows $m(0) = 0$.

2) By 1), we have $m(e_1) = ce_1$ for some $c \in \mathbf{C}$. By Proposition 3.1, m extends uniquely to a function $\tilde{m} : \mathbf{Q}^n \to \mathbf{C}^n$ satisfying (3.2.2) for any $g \in \mathrm{CO}(n, \mathbf{Q})$ and $\alpha \in \mathbf{Q}^n$. Take any $\alpha \in \mathbf{Q}^n \setminus \{0\}$. If p_n is surjective, we can find $g \in \mathrm{CO}(n, \mathbf{Q})$ such that $p_n(g) = \alpha$, that is, $ge_1 = \alpha$. Applying (3.2.2), we get

$$\tilde{m}(\alpha) = |\det g|^\nu g\tilde{m}(e_1) = c\,|\det g|^\nu ge_1 = c\,|\det g|^\nu \alpha.$$

On the other hand, taking the norms of the identity $ge_1 = \alpha$, we have $|\det g| = \|\alpha\|^n$ because $g \in \mathrm{CO}(n, \mathbf{Q})$. Thus $\tilde{m}(\alpha)$ is of the form $c\,\|\alpha\|^{n\nu}\alpha$. Now taking $m = \tilde{m}|_{\mathbf{Z}^n}$, we get the second statement. □

3.3 Proof of Theorem A for $\mathbf{T}^n$

In this subsection, we classify all the positive integers n such that $p_n : \mathrm{CO}(n, \mathbf{Q}) \to \mathbf{Q}^n \setminus \{0\}$ 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 $\mathbf{Q}^n$ by

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

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

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

(i) $n = 1, 2$ *or a multiple of four.*

(ii) $p_n : \mathrm{CO}(n, \mathbf{Q}) \to \mathbf{Q}^n \setminus \{0\}$ *is surjective.*

(iii) $\#(\mathbf{Z}^n \setminus \{0\}/\sim) = 1$.

(iv) $\#(\mathbf{Z}^n \setminus \{0\}/\sim) < \infty$.

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

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

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

(i) $x \sim y$, *i.e. there exists $g \in \mathrm{CO}(n, \mathbf{Q})$ 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 $\det : \mathrm{CO}(n, \mathbf{Q}) \to \mathbf{Q}^\times$. Suppose $g \in \mathrm{CO}(n, \mathbf{Q})$. Then ${}^t gg = \alpha I_n$ for some $\alpha > 0$. Taking the determinant, we get $|\det g|^2 = \alpha^n$. Therefore for $x \in \mathbf{Q}^n$, we have

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

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

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

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

Lemma 3.10. *For $a \in \mathbf{Q}^\times$, 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 $\mathbf{Q}^n$ are equivalent.*

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

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

Proposition 3.11. *Let*

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

Then we have the following characterization of Λ

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

Proof. Owing to Lemma 3.10, it suffices to find a necessary and sufficient condition on $a \in \mathbf{Q}^\times$ such that the quadratic forms $\|x\|^2$ and $a\|x\|^2$ are equivalent on $\mathbf{Q}^n$. For this, we recall that the Hasse–Minkowski theorem says that two quadratic forms over $\mathbf{Q}$ are equivalent if and only if they have the same signature, discriminant modulo the squares $(\mathbf{Q}^\times)^2$ in $\mathbf{Q}^\times$ and invariants ϵ_p for all prime numbers p, see [Se, IV, 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 non-trivial solution in $\mathbf{Q}_p^3$, 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 $\mathbf{Q}^\times/(\mathbf{Q}^\times)^2$ if and only if $a^n \in (\mathbf{Q}^\times)^2$. 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 [Se, Section III.1.1 Proposition 2 i)]. Hence for n odd the only condition is that a is a square. Therefore $\Lambda = (\mathbf{Q}^\times)^2$.

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

Case III: $n \equiv 2 \pmod 4$. Since $\frac{n(n-1)}{2}$ 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, we have

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

where ϵ is defined by $\epsilon(u) = (u-1)/2 \pmod 2$, see [Se, III, 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

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

None of the conditions give any restriction on α_0 and the last condition follows from the first because $3^2 \equiv 1 \pmod 4$. 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 $p_i \equiv 3 \pmod 4$. 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 [D]. 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 $\mathbf{Q}^n$, [D, Theorems 2 and 3] can be reformulated as the statement that the subgroup $\Lambda = \mathbf{Q}_+$ for $n \equiv 0 \pmod 4$, and Λ is equal to the group of non-zero norms in the algebraic extension $\mathbf{Q}+\mathbf{Q}[i]$ for $n \equiv 2 \pmod 4$. 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 in [D, page 404]. The Diophantine equation $a^2 + b^2 = c$ has an integer solution if and only if $\operatorname{ord}_p c$ is even for every prime $p \equiv 3 \pmod 4$, see [IR, Section 17.6, Corollary 1]. Here $\operatorname{ord}_p c$ is the largest non-negative integer k such that $p^k | c$ by

$p^{k+1} \nmid c$. This proves Proposition 3.11 because the rational solutions differ from the integer solutions only by a square in the denominator. $\square$

Remark 3.12. *There is a natural isomorphism*

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

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

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

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

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

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

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

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

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

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

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

$$e_1 \sim x \quad \text{for any } \; x \in \mathbf{Q}^n \setminus \{0\},$$

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

(ii)$'$ $\|x\|^2 \in \Lambda$ for any $x \in \mathbf{Q}^n \setminus \{0\}$.

(i) $\Rightarrow$ (ii)$'$: This implication is trivial if $n = 1$. For $n = 2$, suppose $x = {}^t(x_1, x_2) \in \mathbf{Q}^2 \setminus \{0\}$. Then $g := \begin{pmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{pmatrix} \in \mathrm{CO}(2, \mathbf{Q})$ and $p_2(g) = x$. This shows that p_2 is surjective. For $n \equiv 0 \pmod 4$, (ii)$'$ holds immediately by $\Lambda = \mathbf{Q}_+$ (see Proposition 3.11).

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

(iii) $\Rightarrow$ (iv) Obvious.

(iv) $\Rightarrow$ (i) This follows from Lemma 3.14 below. $\square$

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

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 $i \neq j$, we have

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

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

$$\gamma_i \sim \gamma_j \Rightarrow \sqrt{\frac{1 + p_i^2}{1 + p_j^2}} \in \mathbf{Q}^\times. \tag{3.3.5}$$

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 $\gamma_i \nsim \gamma_j$ and $\#(\mathbf{Z}^n \setminus \{0\}/\sim) = \infty$ if n is odd.

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

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

By a theorem of Lagrange (see [Se, 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

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

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

Remark 3.15. *As we see from Theorems A and B and from Proposition 3.8, the surjectivity of $p_n : \mathrm{CO}(n, \mathbf{Q}) \to \mathbf{Q}^n \setminus \{0\}$ 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 $\mathbf{Q}$ by $\mathbf{Z}$. By using the fields $\mathbf{R}, \mathbf{C}, \mathbf{H}$ and $\mathbf{O}$, we see that $p_n : \mathrm{CO}(n, \mathbf{Z}) \to \mathbf{Z}^n \setminus \{0\}$ 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 $\mathbf{T}^n$

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

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

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

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

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

is well-defined and satisfies (3.4.1). Further, we have

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

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

Suppose $\beta \neq 0$. If $\beta = g_1\alpha = g_2\alpha$ for $g_1, g_2 \in \mathrm{CO}(n, \mathbf{Q})$, then $g_1 g_2^{-1}\beta = \beta$. Taking the norm, we see $|\det(g_1 g_2^{-1})| = 1$ because $g_1 g_2^{-1} \in \mathrm{CO}(n, \mathbf{Q})$. 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 $g \in \mathrm{CO}(n, \mathbf{Z})$. 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 $g' \in \mathrm{CO}(n, \mathbf{Q})$ 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 $\gamma_j \in \mathbf{Z}^n$ ($j = 1, 2, \ldots$) 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}'s 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. Clear from Lemma 3.17 and from the equivalence (i) $\Leftrightarrow$ (iv) in Proposition 3.8. □

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

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

4.1 One-dimensional case

In this subsection we review the characterization results for the Hilbert transform on $\mathbf{Z}$ obtained by Edwards and Gaudry in [EG].

Let

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

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

We recall from (2.1.2) that $D_a : l^2(\mathbf{Z}) \to l^2(\mathbf{Z})$ is a dilation for $a \in \mathbf{Z} \setminus \{0\}$.

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

Fact 4.1 ([EG, Theorem 6.8.5]). *Let T be a translation invariant operator on $l^2(\mathbf{Z})$ which, for every $a \in \mathbf{Z} \setminus \{0\}$, satisfies the relation*

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

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

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

Fact 4.2 ([EG, Lemma 6.8.4]). *If T is a translation invariant operator on $l^2(\mathbf{Z})$ such that*

$$T \circ D_a = \sigma(a) D_a \circ T \tag{4.1.1}$$

for all $a \in \mathbf{Z} \setminus \{0\}$, where $\sigma(a)$ is a non-zero complex-valued function on $\mathbf{Z} \setminus \{0\}$. Then $\sigma \equiv 1$ and T is a constant multiple of the identity.

We shall analyze Fact 4.2 for the higher dimensional case in the next subsection.

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

4.2 Maximal semigroup symmetry

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

Definition 4.3. *A bounded linear operator $T : l^2(\mathbf{Z}^n) \to V \otimes l^2(\mathbf{Z}^n)$ is said to be*

1) translation invariant *if $T \circ \tau_\beta = (\mathrm{id} \otimes \tau_\beta) \circ T$, for all $\beta \in \mathbf{Z}^n$;*

2) non-degenerate *if $\mathbf{C}\text{-}\operatorname{span}\{Tf(\alpha) : f \in l^2(\mathbf{Z}^n), \alpha \in \mathbf{Z}^n\}$ is equal to V.*

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

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

Then T is non-degenerate if and only if $\kappa(\mathbf{Z}^n)$ spans the vector space V over $\mathbf{C}$. From now on assume that T is translation invariant and non-degenerate.

We will make frequent use of Kronecker's delta function

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

in the present section.

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

C0) $(A \otimes L_g) \circ Tf = T \circ L_g f$, for all $f \in l^2(\mathbf{Z}^n)$.

C1) $(A \otimes L_g) \circ Tf = T \circ L_g f$, for all $f \in l^2(\mathbf{Z}^n)$ with $\operatorname{Supp} f \subset {}^t g\mathbf{Z}^n$.

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 $\alpha \in \mathbf{Z}^n$.

Obviously C0) implies C1).

Lemma 4.4. *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 $g \in \mathrm{M}(n, \mathbf{Z})$, the implication is clear from $T\delta_0 = \kappa$.
C3) $\Rightarrow$ C1): Take any $f \in l^2(\mathbf{Z})$ such that $\operatorname{Supp} f \subset {}^t g\mathbf{Z}^n$. Then

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

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

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

and by the condition C3) this is

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

which gives the condition C1). □

Lemma 4.5. *Assume that T is non-degenerate and satisfies the condition C3) for the two pairs (g, A) and (g, A') with $A, A' \in \mathrm{GL}_{\mathbf{C}}(V)$. Then $A = A'$.*

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

The characterization theorem of Edwards and Gaudry (Fact 4.1) leads us to the following definition.

Definition 4.6 (semigroup symmetry)**.** *Let $T : l^2(\mathbf{Z}^n) \to V \otimes l^2(\mathbf{Z}^n)$ be a translation invariant bounded operator. A semigroup symmetry for T is a pair (G, π) where G is a subsemigroup of $\mathrm{M}^{reg}(n, \mathbf{Z})$, and $\pi : G \to \mathrm{GL}_{\mathbf{C}}(V)$ 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 non-degenerate translation invariant operator.

Proposition 4.7 (maximal semigroup symmetry)**.** *Given a translation invariant and non-degenerate bounded linear V-valued operator $T : l^2(\mathbf{Z}^n) \to V \otimes l^2(\mathbf{Z}^n)$. We define G to be a subset of $\mathrm{M}^{reg}(n, \mathbf{Z})$ consisting of g for which there exists $A \in \mathrm{GL}_{\mathbf{C}}(V)$ 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 $\pi : G \to \mathrm{GL}_{\mathbf{C}}(V)$. The pair (G, π) gives the maximal semigroup symmetry for T.*

Proof. The uniqueness for A follows directly from Lemma 4.5 because T is non-degenerate. 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 C1)-C3) in Lemma 4.4 asserts that (G, π) is a maximal semigroup symmetry for the translation invariant bounded operator $T : l^2(\mathbf{Z}^n) \to V \otimes l^2(\mathbf{Z}^n)$ 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 $\alpha \in \mathbf{Z}^n$ and $g \in G$. On the other hand, it turns out that the condition C0) is too strong, as Fact 4.2 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 4.8. *Let T be a translation invariant bounded operator $T : l^2(\mathbf{Z}^n) \to V \otimes l^2(\mathbf{Z}^n)$ such that the following diagram*

$$\begin{array}{ccc} l^2(\mathbf{Z}^n) & \xrightarrow{T} & V \otimes l^2(\mathbf{Z}^n) \\ {\scriptstyle L_g}\downarrow & & \downarrow{\scriptstyle \pi(g)\otimes L_g} \\ l^2(\mathbf{Z}^n) & \xrightarrow{T} & V \otimes l^2(\mathbf{Z}^n) \end{array} \tag{4.2.1}$$

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

For the proof we use the following:

Lemma 4.9. *Suppose $T : l^2(\mathbf{Z}^n) \to V \otimes l^2(\mathbf{Z}^n)$ is a translation invariant bounded linear operator with kernel $\kappa : \mathbf{Z}^n \to V$. If the condition C0) holds for (g, A) for some $A \in \mathrm{GL}_{\mathbf{C}}(V)$, then $\operatorname{Supp}\kappa \subset {}^t g\mathbf{Z}^n$.*

Proof of Lemma 4.9. Take $\gamma \notin {}^t g\mathbf{Z}^n$. $L_g\delta_\gamma = 0$, and therefore $AT\delta_\gamma({}^t g\alpha) = 0$, for all $\alpha \in \mathbf{Z}^n$ by C0). Since $A \in \mathrm{GL}_{\mathbf{C}}(V)$ we obtain $T\delta_\gamma({}^t g\alpha) = 0$, which is equivalent to $\kappa({}^t g\alpha - \gamma) = 0$ for all $\alpha \in \mathbf{Z}^n$. This implies that

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

□

Proof of Proposition 4.8. By Lemma 4.9, the support of the kernel κ must be contained in the set ${}^t g\mathbf{Z}^n$. Therefore $\operatorname{Supp}\kappa \subset \bigcap_{g\in H} {}^t g\mathbf{Z}^n = \{0\}$. Hence T must be of the form in the statement of the proposition. □

4.3 Maximal semigroup symmetry of Riesz transform for $\mathbf{Z}^n$

The results obtained in this section are similar to the ones obtained for $\mathbf{T}^n$, but there is a new feature to take into account, see Fact 4.1 and Fact 4.2.

Definition 4.10. *The Riesz transforms for $\mathbf{Z}^n$ are defined by convolving with the kernels K_j $(1 \le j \le n)$,*

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

i.e. the discrete version of the corresponding kernel for the Riesz transforms on $\mathbf{R}^n$, see Definition 1.2.

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

Proposition 4.11. *The maximal semigroup symmetry of the Riesz transform on* $\mathbf{Z}^n$ *is given by* $(\mathrm{CO}(n, \mathbf{Z}), \rho)$, *where*

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

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

Lemma 4.12. *Let* $\kappa = (K_1, \ldots, K_n)$ *be the kernel of the Riesz transform. Assume there exist* $A \in \mathrm{GL}_{\mathbf{C}}(V)$ *and* $g \in \mathrm{M}^{reg}(n, \mathbf{Z})$ *such that*

$$A\kappa(\alpha) = \kappa({}^t g\alpha), \;\; \textit{for all } \alpha \in \mathbf{Z}^n$$

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

Proof. Since $\kappa(\alpha) = C_n \frac{\alpha}{\|\alpha\|^{n+1}}$, where C_n is a non-zero 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 $1 \leq i \leq n$, we denote by ${}^t g_i$ the i-th column vector of ${}^t g$. Applying the equation (4.3.1) to $\alpha = e_i$, the i-th unit vector, we get $Ae_i = \frac{({}^t g)_i}{\|({}^t g)_i\|^{n+1}}$. For $n = 1$ this is what we wanted to prove, so let $n > 1$. Then

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

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

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

Since $g \in \mathrm{M}^{reg}(n, \mathbf{Z})$, ${}^t g_i$ 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 $(g_i, g_j) = 0$. Hence $g \in \mathrm{CO}(n, \mathbf{Z})$. Then $|\det g| = \|g_i\|^n$ for all i. Since $Ae_i = {}^t g_i/\|{}^t g_i\|^{n+1}$ $(1 \leq i \leq n)$, we get $A = |\det g|^{-(n+1)/n}\, {}^t g$. □

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

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

for all $\alpha \in \mathbf{Z}^n$ and $g \in \mathrm{CO}(n, \mathbf{Z})$ by Proposition 4.11. This is equivalent to

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

for all $\alpha \in \mathbf{Z}^n$ and $g \in \mathrm{CO}(n, \mathbf{Z})$. 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 $n \equiv 0 \pmod 4$. Hence Theorem A for $\mathbf{Z}^n$ is proved.
Suppose $n > 2$ and $n \not\equiv 0 \pmod 4$. 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's 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 $\delta_\gamma \in l^2(\mathbf{Z}^n)$). $\square$

5 Saturated semigroup symmetry

For $n > 2$ and $n \not\equiv 0 \pmod 4$, 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 $\mathbf{T}^n$ and $\mathbf{Z}^n$. We may ask what are other invariance conditions that can single out the Riesz transforms on $\mathbf{T}^n$ and $\mathbf{Z}^n$. In this section, we introduce a little more technical condition (*saturated semigroup symmetry*) which characterizes the Riesz transforms on $\mathbf{T}^n$ and $\mathbf{Z}^n$ (up to scalar) for all dimensions n.

5.1 Characterization of the Riesz transform on $\mathbf{T}^n$

We define the following set

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

Let $f_\alpha(x) := e^{2\pi i \langle \alpha, x \rangle}$ for $\alpha \in \mathbf{Z}^n$. For any $(g, \alpha) \in \Xi$, the function $L_{{}^t g} f_\alpha$ is well-defined as a function on $\mathbf{T}^n$ 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 $T : L^2(\mathbf{T}^n) \to \mathbf{C}^n \otimes L^2(\mathbf{T}^n)$ satisfies a *saturated semigroup symmetry* for Ξ if it satifies 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

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

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

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

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

Proof. As in the proof of Proposition 2.2, the multiplier $m : \mathbf{Z}^n \to \mathbf{C}^n$ 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 $\nu \in \mathbf{R}$. If a function $F : \mathbf{Z}^n \to \mathbf{C}^n$ satisfies the condition*

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

then F is unique up to multiplication with a scalar.

Proof. Since for any $\alpha \in \mathbf{Z}^n$ there exists an element $g \in \mathrm{CO}(n)$ such that $(g, e_1) \in \Xi$ and $\alpha = ge_1$ the proof follows in the same way as in the proof of Lemma 3.7. □

5.2 Characterization of the Riesz transform on $\mathbf{Z}^n$

In a similar way as in the previous subsection, the Riesz transform on $\mathbf{Z}^n$ is recovered from the saturated semigroup symmetry for Ξ for all dimension n:

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

$$L_{{}^t g}(T\delta_0)(\alpha) = |\det g|^{-\frac{n-1}{n}} g(T\delta_0(\alpha)), \tag{5.2.1}$$

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

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

$$\kappa(g\alpha) = |\det g|^{-\frac{n-1}{n}} g\kappa(\alpha). \tag{5.2.2}$$

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

References

[B] Bourbaki, N. *Algebra I*, Springer-Verlag (1989)

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

[EG] Edwards, R. E. and Gaudry, G. I. *Littlewood–Paley and Multiplier Theory*, Springer-Verlag (1977)

[IR] Ireland, K. and Rosen, M. *A Classical Introduction to Modern Number Theory*, Springer-Verlag, Graduate texts in Mathematics, **84** (1990)

[KN1] Kobayashi, T. and Nilsson, A. *Group invariance and L^p-bounded operators*, *Math. Z.* **260** (2008), 335–354.

[KN2] Kobayashi, T. and Nilsson, A. *Indefinite higher Riesz transforms*, *Ark. Mat.* **47** (2009), 331–344.

[Sa] Sato, M. *Theory of prehomogeneous vector spaces (algebraic part)*, *Nagoya Math. J.* **120**, pp 1–34 (1990), (English translation of Sato's lectures from Shintani's notes Sugaku-no-Ayumi **15**, 83–157 (1970) [Translated by M. Muro])

[Sch] Schmutz, E. *Rational points on the unit sphere*, Central European Journal *of Mathematics* **6** pp 482–487 (2008).

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

[S] Stein, E. M. *Singular integrals and differentiability properties of functions*, Princeton University Press (1970)

[SW] Stein, E. M. and Weiss, G. *Introduction to Fourier analysis on Euclidean spaces*, Princeton University Press (1971)