

ON RADON TRANSFORMS ON FINITE GROUPS

JOONAS ILMAVIRTA

ABSTRACT. If G is a finite group, is a function $f : G \rightarrow \mathbb{C}$ determined by its sums over all cosets of cyclic subgroups of G ? In other words, is the Radon transform on G injective? This inverse problem is a discrete analogue of asking whether a function on a compact Lie group is determined by its integrals over all geodesics. We discuss what makes this new discrete inverse problem analogous to well-studied inverse problems on manifolds and we also present some alternative definitions. We use representation theory to prove that the Radon transform fails to be injective precisely on Frobenius complements. We also give easy-to-check sufficient conditions for injectivity and noninjectivity for the Radon transform, including a complete answer for abelian groups and several examples for nonabelian ones.

1. INTRODUCTION

Before introducing the problem we wish to study, let us begin with an older problem. Given a closed Riemannian manifold M and a smooth function $f : M \rightarrow \mathbb{C}$, can we recover the function f if we know its integral over all closed geodesics? This problem was first considered by Funk [3] in 1913 in the case $M = S^2$ – it turned out that one can only recover the even part of the function. This problem has since received attention from several authors, and results have been proven on essentially two types of manifolds: those with algebraic structure (symmetric spaces, Grassmannians and Lie groups [10, 4, 5, 6, 9]) and those with negative curvature or some other similar structure (see for example [2]).

This problem was recently considered on compact Lie groups [9] and the aim of the present paper is to extend that approach to finite groups. We ask whether a function $f : G \rightarrow \mathbb{C}$ on a finite group G can be determined from its integrals over all closed geodesics. In other words, we ask whether the Radon transform that sends a function to its integrals over all closed geodesics is injective.

The first problem is to make sense of the question. The integral is, of course, a sum, but the definition of a geodesic is less obvious. We

Date: February 4, 2015.

2010 Mathematics Subject Classification. 20F99, 44A99, 44A12, 20C99, 20B10.

Key words and phrases. Inverse problems, finite groups, representation theory, Radon transforms, Frobenius complements.

define a closed geodesic to be a translate of a cyclic subgroup; as it turns out, this is in many ways analogous closed geodesics on a Lie group (see section 2.2). A more careful formulation of the problem is given in section 2.

1.1. Summary of results. In the case of finite abelian groups, we give a complete answer to our problem. The Radon transform is injective on a finite abelian group if and only if it is not cyclic (see theorem 3.5). It follows, for example, that the Radon transform is not injective on any finite abelian group of squarefree order.

We also give a complete answer for product groups. The Radon transform fails to be injective on a product if and only if the constituents have noninjective Radon transform and coprime order (see theorem 4.1).

Our answers in other cases are far less complete using elementary methods. We show that the Radon transform is injective on all symmetric, alternating and dihedral groups, but noninjective on all dicyclic groups. We also give sufficient and necessary conditions for the Radon transform to be injective, but none of our conditions is both sufficient and necessary. For these results, see section 5.

We give a representation theoretical characterization of the finite groups where the Radon transform is injective (see theorem 6.9). It turns out that the Radon transform fails to be injective on G if and only if G is a Frobenius complement. (This is true whenever the functions on which the Radon transform operates take values in a field of characteristic zero, not necessarily complex numbers.) This is equivalent with the existence of a fixed-point-free representation in a suitable sense; see theorem 6.9. Tools from representation theory also allow us to give a second proof of the result for abelian groups and a characterization of the kernel of the Radon transform when it is not injective (see theorem 6.8).

Many of the other results follow from this characterization and known properties of Frobenius complements. We however prefer to give more elementary proofs of our results – in particular proofs written in the language of Radon transforms. The characterization result is also a new characterization of Frobenius complements. We will discuss this matter again in remark 6.10 and under it.

For any given finite group it is a straightforward but tedious exercise to see if the Radon transform is injective (see section 2.5). We do not consider this a satisfactory solution to our problem. Our results, besides providing some understanding of the problem at hand, also significantly speed up the aforementioned banal exercise.

We will also discuss some generalizations and variations of the problem in section 7. We present some remarks about the Radon transform on infinite discrete groups in section 7.1 and we introduce the discrete

geodesic flow in section 7.2. In section 7.3 we will introduce a variant of the Radon transform where geodesics are assumed to satisfy an additional maximality condition and study its basic properties.

2. DESCRIPTION OF THE PROBLEM

2.1. Definition of geodesics. Let G be a finite group. For any integer $n \geq 2$ let C_n denote the cyclic group of order n . A geodesic of length n on the group G is a mapping $C_n \ni t \mapsto x\gamma(t) \in G$, where $x \in G$ and $\gamma : C_n \rightarrow G$ is a nontrivial homomorphism. The variable $t \in C_n$ is the discrete analogue of time (or arc length). We will often ignore length and refer only to geodesics, by which we mean geodesics of all possible lengths. We denote by Γ_n the set of all nontrivial homomorphisms $C_n \rightarrow G$.

Note that the definition of a geodesic is symmetric between left and right multiplication, although the definition is given only with left translations (by the element x). If γ is a nontrivial homomorphism, so is $t \mapsto x^{-1}\gamma(t)x$.

It is common to identify a curve with its image. Similarly, geodesics in our setting can be thought of as mappings to G or as subsets of G . With this identification we could redefine geodesics to be cosets of cyclic subgroups that contain more than one point. Note that the length of a geodesic and the number of points in its image may not coincide, but in this case each point in the image has equally large preimage.

We will show that only geodesics whose length is a prime number matter. In this case identifying the mapping and the point is safe, since a homomorphism $C_p \rightarrow G$ is nontrivial if and only if it is injective if p is a prime. Also, any subgroup of prime order is automatically cyclic, which would allow for an even shorter definition, but at the cost of diminished clarity.

If the group G were infinite, there could also be infinitely long geodesics, corresponding to homomorphisms $\mathbb{Z} \rightarrow G$. We restrict ourselves to finite groups for simplicity. The Radon transform in infinite discrete groups is discussed briefly in section 7.1, and it turns out that our inverse problem can behave very differently on infinite groups.

Actually, on finite groups every geodesic corresponds to a homomorphism from \mathbb{Z} , as such a homomorphism must factor through some finite cyclic group. (Every geodesic on a finite group is necessarily periodic.) But it is technically convenient to restrict attention to homomorphisms from finite cyclic groups.

This is not the only reasonable definition of a geodesic in a finite group. For an alternative, see section 7.3.

Geodesics on finite groups can also be thought of as trajectories of a discrete time dynamical system. See section 7.2 for this aspect.

2.2. Comparison of discrete and continuous geodesics. There are several reasons to see these as natural generalizations of geodesics on Lie groups (with a bi-invariant metric). From now on, we assume all Lie groups to have dimension one or higher, so that finite groups are not Lie groups. This is not essential, but makes it easier to distinguish the two cases. By geodesics on Lie groups we mean only the periodic ones here.

For every nontrivial group there exist geodesics. — The same is true for compact Lie groups of nonzero dimension.

Geodesics remain geodesics under left and right translations. Left translations were built into the definition, and right invariance is due to the fact that if $\gamma : C_n \rightarrow G$ is a homomorphism, so is the map $\gamma_x : C_n \rightarrow G$ with $\gamma_x(t) = x^{-1}\gamma(t)x$. — The same is true for compact Lie groups.

If the finite group G is abelian, it is a product of cyclic groups. — If a connected, compact Lie group is abelian, it is a product of copies of S^1 (a torus, that is).

Subgroups are totally geodesic; that is, if $\gamma : C_n \rightarrow H$ is a geodesic on a subgroup $H < G$, then it is also a geodesic on G . — The same is true for compact Lie groups.

The groups C_n are abelian and once a generator has been fixed, there is a natural meaning to going forward or backward, and there are no other directions. — A similar description fits S^1 .

A geodesic is uniquely determined by giving two adjacent points¹ on it. — A geodesic on a Lie group is uniquely determined by a point and a direction (although it need not be closed).

The one property of geodesics that our generalization does not capture is minimization of length. This was only expected, as distance is much less of a meaningful concept on a finite group. There are studies of norms on finite groups [1], but the author is unaware of a pre-existing theory of geodesics.

2.3. The Radon transform on finite groups. Let G again be a finite group and let $A^{\mathbb{C}}$ denote the set of complex valued functions on a set A . Recall that Γ_n denotes the set of nontrivial homomorphisms $C_n \rightarrow G$. For $f \in G^{\mathbb{C}}$ and $\gamma \in \Gamma_n$, $n \geq 2$, we denote

$$R_n f(x, \varphi) = \sum_{t \in C_n} f(x\gamma(t)).$$

This is the sum of f over the geodesic defined by the homomorphism γ and shifted by x . The mapping $R_n : G^{\mathbb{C}} \rightarrow (G \times \Gamma_n)^{\mathbb{C}}$ is analogous to the Radon transform on Lie groups. Since it is a discrete analogue of an integral transform, we find it natural to describe it as a sum transform.

¹Two elements t and s of a cyclic group can be naturally considered adjacent if ts^{-1} generates the group.

A similar definition of the Radon transform on Lie groups was given in [9]. To make the similarity to the classical Radon transform on \mathbb{R}^n even more transparent, we remark that every straight line in \mathbb{R}^n is a translate of a nontrivial Lie homomorphism $\mathbb{R} \rightarrow \mathbb{R}^n$.

We want to consider geodesics of all lengths at once, so we will denote by Rf the sequence $(R_n f)_{n=2}^\infty$ of all of the sum transforms R_n . Therefore when we say that R is injective, we mean that f can be recovered if we know $R_n f$ for all n . By the kernel of R we mean $\ker R = \bigcap_{n=1}^\infty \ker R_n \subset \mathbb{C}^G$, and injectivity is equivalent with $\ker R = 0$.

We call R the (discrete) Radon transform on the group G . Our main problem is to find out when this transform is injective.

By definition R consists of infinitely many sum transforms, but as we will see in lemma 2.1, it suffices to consider only those n that are prime factors of $|G|$.

It is no way crucial that we assume the functions to take values in \mathbb{C} . Our results remain intact when \mathbb{C} is replaced with any vector space over a field of characteristic zero. Working over the complex numbers becomes technically very useful in section 6, where we use representation theory.

It is obvious that if the Radon transform is injective over a field, then it is also injective over any subfield. The converse is also true, but less obvious. Let \mathbb{F} be a subfield of \mathbb{K} and let $R^\mathbb{F}$ and $R^\mathbb{K}$ be the corresponding Radon transforms on G . We can regard \mathbb{K} as a vector space over \mathbb{F} , and we can use its dual space \mathbb{K}^* to deduce injectivity over \mathbb{K} from injectivity over \mathbb{F} . If $f \in \mathbb{K}^G$ and $u \in \mathbb{K}^*$, we have $u(R^\mathbb{K} f) = R^\mathbb{F} u(f)$. If $R^\mathbb{F}$ is injective, then $R^\mathbb{K} f = 0$ implies that $u(f) = 0$ for all $u \in \mathbb{K}^*$ and therefore that $f = 0$.

This argument for field extensions also works with other vector spaces. If we want to study the Radon transforms of functions taking values in a vector space, it suffices to consider the problem with functions that take values in the underlying field or any subfield. Therefore our results (which are stated over \mathbb{C}) are true over any vector space over any field of characteristic zero. The Radon transform itself makes sense if the functions take values in any abelian group.

The classical Radon transform has also been considered on noncompact manifolds. The Radon transform in Euclidean spaces has applications in medical and other imaging and has been widely studied. In the Radon transform one typically integrates over hyperplanes and in the X-ray transform over lines, but we refer to all integral transforms of this kind as Radon transforms for simplicity. For an introduction to the classical Radon transform, see [7, 11].

2.4. Comparison of discrete and continuous Radon transforms.

In section 2.2 we compared geodesics in the discrete and continuous settings and highlighted the similarities between the two theories.

There are also differences between the continuous and discrete theories, and this is reflected in the differences in injectivity results for the Radon transform. The analogous study of the Radon transform on Lie groups was based on finding toric subgroups and reducing the problem to the abelian case. There are only four compact, connected Lie groups that do not have a two dimensional torus as a subgroup: the trivial group, $SO(2)$, $SO(3)$ and $SU(2)$.

The analogous approach does not work with finite groups. The discrete analogue of an at least two dimensional toric subgroup is a non-cyclic abelian subgroup. Unfortunately there is no simple description of groups with such subgroups. In particular there are infinitely many groups without such subgroups.

The most immediate analogue of a maximal torus would be a maximal abelian subgroup, but two such subgroups are not necessarily conjugate. In this sense a better analogue is given by Sylow p -subgroups, since any two Sylow p -subgroups are conjugate just like any two maximal tori, but Sylow p -subgroups need not be abelian. The existence of convenient subgroups is a much more complicated issue in finite groups.

Another difference lies in the internal symmetries of geodesics. As mentioned in section 2.2, a discrete geodesic has a well defined direction once a generator is chosen in the cyclic group. There are many possible choices, corresponding to automorphisms of the cyclic group. There is no natural generator for the cyclic subgroup corresponding to a geodesic, so there is no “natural direction” of discrete geodesics. The group S^1 that underlies continuous geodesics has only two automorphisms – the nontrivial one is the reversal – and the only ambiguity is in choosing one of the two directions.

These structural differences between discrete and continuous geometry of groups leads us to a different course of action than in [9].

2.5. Some simple observations. Let us begin our enquiry by presenting some first observations.

Given any single finite group G it is a straightforward task to see whether the Radon transform is injective or not. There are finitely many points and geodesics on G , so the Radon transform is a linear operator between finite dimensional spaces. Checking injectivity therefore reduces to forming a matrix and calculating its rank.

Even in more general situations, dimension counting arguments suffice for proving that the Radon transform has a nontrivial kernel. More elaborate arguments are needed to prove that the transform is injective, if that is the case.

Suppose we know the sum of $f : G \rightarrow \mathbb{C}$ over all geodesics and want to reconstruct f . It suffices to reconstruct f at e . Indeed, let $\tau_x g : G \rightarrow \mathbb{C}$, $\tau_x f(y) = f(xy)$, be the left translation of f by $x \in G$ and let S be the assumedly existing solution operator that takes $Rf \mapsto f(e)$.

Since geodesics are translation invariant, we know $R\tau_x f$ as well. Then $S(R\tau_x f) = f(x)$.

Besides sums over geodesics, we shall also be occasionally interested in sums over the whole group. If $\gamma : C_n \rightarrow G$ is a homomorphism, then

$$(1) \quad \sum_{x \in G} f(x) = \frac{1}{n} \sum_{x \in G} R_n f(x, \gamma).$$

The Radon transform thus determines the average of the function.

The following lemma demonstrates that we only need to consider geodesics of prime length. Therefore, if we know all subgroups of prime order, we immediately know all relevant geodesics.

Lemma 2.1. *Let G be a finite group. The Radon transforms $R_n f$ of $f : G \rightarrow \mathbb{C}$ is uniquely determined for each $n \geq 2$ by the knowledge of $R_p f$ for every prime p .*

Proof. Consider the Radon transform $R_n f$ for some composite number $n = km$. It suffices to prove that $R_n f$ is determined by $R_k f$ and $R_m f$. Take any nontrivial homomorphism $\gamma : C_n \rightarrow G$. Let $\alpha : C_m \rightarrow C_n$ be the embedding that multiplies by k (where we have identified $C_m = \mathbb{Z}/m\mathbb{Z}$ and similarly for C_n and C_k).

Now $\gamma \circ \alpha : C_m \rightarrow G$ is a homomorphism. If it is trivial, then $\gamma(k) = e$ and we may define a homomorphism $\beta : C_k \rightarrow G$ by letting $\beta(t) = \gamma(t)$. Then $R_n f(x, \gamma) = m R_k f(x, \beta)$.

If $\gamma \circ \alpha$ is not trivial, then $R_n f(x, \gamma) = \frac{1}{m} \sum_{t \in C_m} R_m f(x\gamma(t), \gamma \circ \alpha)$. In either case $R_n f(x, \gamma)$ is determined by $R_k f$ and $R_m f$. \square

Lemma 2.2. *Let G be a finite group. If the Radon transform is injective on any subgroup $H < G$, then it is injective on G as well.*

Proof. Let $f : G \rightarrow \mathbb{C}$ be a function which we wish to recover from its Radon transform. If we restrict our attention to geodesics that lie in H , we obtain the Radon transform of $f|_H$ on H . This is transform injective, so it determines $f|_H$, whence f can be recovered everywhere in G . \square

We will repeatedly use the following special case of lemma 2.2, so we state it separately.

Lemma 2.3. *Suppose $G = G_1 \times G_2$, where each G_i is a finite abelian group. If R is injective on G_1 , it is injective on G .*

3. ABELIAN GROUPS

We consider first the case where the finite group G is abelian. For the sake of a simple presentation, we will only present our lemmas in the generality we need here. By Kronecker's decomposition theorem any finite abelian group G can be written as a product $G = C_{p_1^{k_1}} \times \cdots \times C_{p_N^{k_N}}$ for some N , where each p_i is a prime and each k_i a natural number.

Lemma 3.1. *Suppose $G = C_{p_1^{k_1}} \times \cdots \times C_{p_N^{k_N}}$ and $\gamma : C_p \rightarrow G$ is a homomorphism. If $\pi_i : G \rightarrow C_{p_i^{k_i}}$ is the projection, the homomorphism $\pi_i \circ \gamma$ is trivial unless $p = p_i$.*

Proof. This proof follows from the observation that there are no non-trivial homomorphisms $C_p \rightarrow C_{q^k}$ for distinct primes p and q . \square

Lemma 3.2. *If $G = C_{p^k}$ for p prime, then R is not injective.*

Proof. By lemma 2.1 it suffices to consider geodesics of prime length, and thus only geodesics of length p . There are p^{k-1} such geodesics (identifying geodesics that differ by an automorphism of C_{p^i}), so $R_p f$ only gives p^{k-1} numbers. This is not enough to determine a function on the group G for dimensional reasons. \square

Lemma 3.3. *If G is cyclic, then R is not injective.*

Proof. We use again the decomposition $G = C_{p_1^{k_1}} \times \cdots \times C_{p_N^{k_N}}$. If $N = 1$, the claim is given by lemma 3.2. We assume thus that $N \geq 2$.

The primes p_1, \dots, p_N are distinct, since otherwise G would not be cyclic. We only need to consider geodesics of these prime lengths.

For any i let $f_i : C_{p_i^{k_i}} \rightarrow \mathbb{C}$ be a nontrivial function in the kernel of R_{p_i} , whose existence is guaranteed by lemma 3.2. Define $f : G \rightarrow \mathbb{C}$ by letting $f(x_1, \dots, x_N) = f_1(x_1) \cdots f_N(x_N)$. It remains to prove that $f \in \ker R$.

Indeed, take any index i and consider a homomorphism $\gamma \in \Gamma_{p_i}$ and $x \in G$. By lemma 3.1 there is a homomorphism $\varphi : C_{p_i} \rightarrow C_{p_i^{k_i}}$ such that $\gamma(t) = (e, \dots, e, \varphi(t), e, \dots, e)$ where φ occurs in the i th position. Now

$$R_{p_i} f(x, \gamma) = R_{p_i} f_i(x_i, \varphi) \prod_{n \in \{1, \dots, N\} \setminus \{i\}} f_n(x_n) = 0. \quad \square$$

Lemma 3.4. *If $G = C_p \times C_p$ for a prime p , then R_p is injective.*

Proof. Each point in G corresponds to a unique homomorphism $C_p \rightarrow G$, so $\#\Gamma_p = p^2 - 1$. Each $x \in G \setminus \{e\}$ belongs to the image of $p - 1$ homomorphisms $C_p \rightarrow G$, since the automorphism group of C_p has order $p - 1$. Thus

$$(2) \quad \sum_{\gamma \in \Gamma_p} R_p f(x, \gamma) = (p^2 - p)f(x) + (p - 1) \sum_{y \in G} f(y)$$

for every $x \in G$.

If $R_p f = 0$, the identities (1) and (2) give $f(x) = 0$ for every $x \in G$. Thus $\ker R_p$ is trivial. \square

In fact, the proof gives a reconstruction formula in the case $G = C_p \times C_p$, valid for any $x \in G$ and $\varphi \in \Gamma_p$:

$$f(x) = \frac{1}{p^2 - p} \sum_{\gamma \in \Gamma_p} R_p f(x, \gamma) - \frac{1}{p^2} \sum_{y \in G} R_p f(y, \varphi).$$

Compare this with the normal operator of the X-ray or Radon transform in the Euclidean case².

Theorem 3.5. *Let G be a nontrivial finite abelian group. Then the following are equivalent:*

- (1) G is not cyclic.
- (2) G contains a square of a cyclic group.
- (3) R is injective on G .

Proof. Equivalence of the first two conditions follows from the fact that G is a product of cyclic groups. In fact, both of these conditions are equivalent with the statement that at least one prime occurs at least twice in the decomposition $G = C_{p_1^{k_1}} \times \cdots \times C_{p_N^{k_N}}$. Lemma 3.3 shows that the third condition implies the first one. Lemmas 3.4 and 2.3 show that the second condition implies the third one. \square

4. PRODUCT GROUPS

4.1. Direct products. We now turn to the question of determining injectivity of the Radon transform on a product group if the corresponding results are known on the constituent groups. We are able to give a rather complete answer.

Theorem 4.1. *Let G_1 and G_2 be two finite groups. Then the Radon transform is not injective on $G_1 \times G_2$ if and only if it is not injective on either of the constituent groups and the orders of the constituent groups are coprime.*

Proof. We need to show the following:

- (1) If the Radon transform is injective on either constituent group, then it is injective on the product.
- (2) If the orders of the constituent groups have a common prime factor, then the Radon transform is injective on the product.
- (3) If the orders of the constituent groups are coprime and the Radon transform is noninjective on both, then it is noninjective on the product.

1. This is the statement of lemma 2.3.

2. Let p be a prime that divides $|G_i|$ for both $i = 1, 2$. By the existence of Sylow subgroups each G_i has a subgroup isomorphic to the cyclic group C_p . Thus the product $G_1 \times G_2$ has a subgroup isomorphic to $C_p \times C_p$. By lemma 2.2 and theorem 3.5 the Radon transform is injective on $G_1 \times G_2$.

3. It suffices to consider geodesics of prime length. Let p be a prime and $\gamma : C_p \rightarrow G_1 \times G_2$ a nontrivial homomorphism. By assumption

²If R^* is the adjoint of R , the normal operator R^*R of R is such that $R^*Rf(x)$ is the integral over the integrals over all lines passing through x . The normal operator can be used to invert the Radon transform [7].

p can only divide the order of one of the two groups G_1 and G_2 , so γ composed with one of the projections must be trivial. Thus if f_i is in the kernel of the Radon transform on G_i , the function $f(x_1, x_2) = f_1(x_1)f_2(x_2)$ is in the kernel of the Radon transform on G . \square

4.2. Semidirect products. The above result about direct products does not generalize easily to semidirect products. Let us attempt to describe this issue.

Let N and H be finite groups and $\varphi : H \rightarrow \text{Aut}(N)$ a homomorphism, and consider the semidirect product $G = N \rtimes_{\varphi} H$. We consider N and H as subgroups of G . We want to study cyclic subgroups of G if $|N|$ and $|H|$ are coprime; such study was at the heart of the proof of theorem 4.1.

Let p be a prime that divides $|N|$ but not $|H|$ and consider an element $nh \in G$ of order p , where $n \in N$ and $h \in H$. Now $(nh)^p = \tilde{n}\tilde{h}$ with $\tilde{n} = n\varphi_h(n)\varphi_{h^2}(n)\cdots\varphi_{h^{p-1}}(n) \in N$ and $\tilde{h} = h^p \in H$. The condition $(nh)^p = e_G$ implies that $\tilde{n} = e_N$ and $\tilde{h} = e_H$, the latter of which implies that $h = e_H$ since p does not divide $|H|$. Thus $\langle nh \rangle \leq N < G$.

If, instead, p divides $|H|$ but not $|N|$, we *cannot* draw the conclusion that $\langle nh \rangle \leq H < G$ without assuming anything much short of φ being trivial and hence the product being direct. The problem is that \tilde{n} and h can both be nontrivial even though $(nh)^p = e_G$. For example, let q be a prime distinct from p and let $H = C_p$ and let N be the product of p copies of C_q indexed by C_p . Let H act on N by permuting the indices. For any $h \in H \setminus \{e_H\}$ and $n = (a_1, \dots, a_p) \in C_q^p = N$ such that $a_1 a_2 \cdots a_p = e_{C_q}$ a simple calculation shows that $\tilde{n} = e_N$ and $\tilde{h} = e_H$.

To further demonstrate problems with semidirect products, let us mention two examples. All dihedral are semidirect products of cyclic groups. The Radon transform fails to be injective in all cyclic groups, but is injective on all dihedral groups. On the other hand, it is never injective on a dicyclic group, and Dic_6 is a semidirect product of Dic_2 and C_3 . It is not clear whether there is a simple version of theorem 4.1 for semidirect products. These and other examples are studied in the next section.

5. NONABELIAN GROUPS

Combining theorem 3.5 with lemma 2.2 we see that the Radon transform is injective on G if G contains an abelian subgroup that is not cyclic. This condition is simple, but it does not cover all nonabelian groups.

A natural construction whose relation to injectivity of the Radon transform one may consider is the quotient. It does not hold that if the Radon transform is injective on G , it would also be injective on any quotient G/H . The argument generalizing the one for Lie groups (see [9, Proposition 2.4]) fails at a critical point.

Let us present it here: Let G be a finite group, H its normal subgroup, $\pi : G \rightarrow G/H$ the projection, $\gamma : C_p \rightarrow G$ a geodesic and $f : G/H \rightarrow \mathbb{C}$ a function. Indicating the underlying group by a superscript in the transform, we get $R_p^G(\pi^*f)(x, \gamma) = R_p^{G/H}f(\pi(x), \pi \circ \gamma)$. It seems that if R_p^G is injective, then we could recover π^*f and thus f from the knowledge of $R_p^{G/H}f$. The reason why this fails is that $\pi \circ \gamma$ may be trivial and hence may not correspond to a geodesic. If we allowed trivial homomorphisms in our definition of geodesics, every Radon transform on every (finite or infinite) group would be trivially injective.

Let us give a more specific example. Let H be a finite group with an injective Radon transform and let $n \geq 2$ be an integer. The Radon transform is injective on $G = H \times C_n$ by lemma 2.3. But $H \times \{e\}$ is a normal subgroup of G and the quotient equals C_n , but the Radon transform is not injective on C_n because of lemma 3.3.

Also, there is an example where the Radon transform is not injective on G , but it is injective on the quotient G/H . Indeed, if $G = Q_8$ is the quaternion group and H its only two element subgroup, then $G/H = C_2 \times C_2$. The Radon transform is not injective on G ($Q_8 = Dic_2$; see proposition 5.4) but is injective on $C_2 \times C_2$.

Proposition 7.4 does give a result involving quotient groups. It involves a variant of the Radon transform which we call the maximal Radon transform, but we refrain from discussing it before we introduce it in section 7.3 in order to avoid confusion.

5.1. Groups with an injective Radon transform. Let us give explicit examples of families of finite groups where the Radon transform is injective.

Proposition 5.1. *The Radon transform is injective on the dihedral group D_n if and only if $n \geq 3$.*

Proof. The groups D_1 and D_2 are cyclic, so noninjectivity follows from theorem 3.5. Suppose thus that $n \geq 3$.

Let $f : D_n \rightarrow \mathbb{C}$ be a function that we wish to reconstruct from its Radon transforms. By translation invariance of the problem it suffices to reconstruct $f(e)$.

We may classify elements of D_n as reflections and rotations. Let $\gamma_1, \dots, \gamma_n$ be the homomorphisms $C_2 \rightarrow D_n$ going through the reflections. There is a single homomorphism $\varphi : C_n \rightarrow D_n$ passing through all rotations. Let $r \in D_n$ be any reflection, so that the geodesic $C_n \ni t \mapsto r\varphi(t) \in D_n$ passes through all reflections. Now it is easy to observe that

$$\sum_{i=1}^n R_2 f(e, \gamma_i) - R_n f(r, \varphi) = n f(e). \quad \square$$

Proposition 5.2. *The Radon transform is injective on the symmetric group S_n if and only if $n \geq 3$.*

Proof. This follows from the previous theorem and lemma 2.2, since $S_n = D_n$ for $n \leq 3$ and S_n contains D_3 as a subgroup if $n \geq 4$. \square

Proposition 5.3. *The Radon transform is injective on the alternating group A_n if and only if $n \geq 4$.*

Proof. The groups A_2 and A_3 are cyclic, so the Radon transform is not injective on them by theorem 3.5. The group A_4 contains $C_2 \times C_2$ as a subgroup and A_4 is a subgroup of A_n for $n \geq 5$, so the claim follows from lemmas 2.2 and 3.4. \square

5.2. Groups with a noninjective Radon transform. Let us start with a more explicit example and then present a more general condition for recognizing groups where the Radon transform is not injective.

Proposition 5.4. *The Radon transform is not injective on any dicyclic group Dic_n , $n \geq 2$.*

Proof. The dicyclic group Dic_n is generated by two elements a and b that satisfy $a^{2n} = e$, $b^2 = a^n$ and $ab = ba^{-1}$. The elements of Dic_n can be written uniquely as $b^m a^k$ with $0 \leq m \leq 1$ and $0 \leq k \leq 2n - 1$, and so the group has order $4n$.

Let A be the cyclic subgroup spanned by a . This subgroup is isomorphic to C_{2n} . All cyclic subgroups of Dic_n that have order other than four are contained in A ; it is easy to check that every element in $Dic_n \setminus A$ has order four. Therefore all geodesics of prime order are contained in A or its complement.

Now let $f : C_{2n} \rightarrow \mathbb{C}$ be a nontrivial function in the kernel of the Radon transform (such functions exist by theorem 3.5). We may naturally regard f as a function on A and extend it by zero to Dic_n . The resulting function is in the kernel of the Radon transform on Dic_n . \square

Proposition 5.5. *Let G be a finite group and let S denote the set of its cyclic subgroups of prime order. Then the Radon transform is not injective on G if*

$$(3) \quad \sum_{H \in S} |H|^{-1} < 1 + \frac{|S| - 1}{|G|}.$$

Proof. It suffices to consider geodesics of prime order by lemma 2.1. Let p be a prime and let $\gamma : C_p \rightarrow G$ be a nontrivial homomorphism. The image $\gamma(C_p)$ is a cyclic subgroup of order p . The group G is composed of $|G|/p$ left translates of $\gamma(C_p)$; these are precisely the geodesics corresponding to the homomorphism γ .

Let $f : G \rightarrow \mathbb{C}$ be any function. Summing over the Radon transform of f on these geodesics gives the sum of f over the whole G ; see (1). The number of independent numbers contained in the Radon transform of f

is therefore at most $1 + \sum_{H \in \mathcal{S}} (|G|/|H| - 1)$, where the ± 1 s correspond to the sum of f over the whole group. If this number is strictly less than $|G|$, the Radon transform has nontrivial kernel for dimensional reasons. \square

Groups satisfying the condition of proposition 5.5 include all cyclic groups and the dicyclic groups Dic_n for $2 \leq n \leq 14$. The smallest dicyclic group not satisfying (3) is Dic_{15} with an inequality, and the smallest one with the opposite inequality is Dic_{30} . Taking n to be a primorial (a product of distinct primes less than a given number), we see that the inequality (3) can be violated as badly as we wish. Nevertheless, the Radon transform remains noninjective by proposition 5.4, which demonstrates that the condition of proposition 5.5 is far from sharp.

6. A REPRESENTATION THEORETICAL APPROACH

6.1. Representations on finite groups. As before, let G be a finite group. If V is a vector space, a homomorphism $\rho : G \rightarrow GL(V)$ is called a representation of the group G and V is called the representation space of ρ . The underlying field of the vector space V could be anything, but we restrict our attention to the complex numbers. Representation theory is particularly convenient over this field.

We will only consider finite dimensional representations, and we refer to the dimension of the space V as the dimension $\dim(\rho)$ of the representation ρ . The space V can be equipped with an inner product so that $\rho(x)$ is unitary for all $x \in G$. We shall identify V with $\mathbb{C}^{\dim(\rho)}$ and assume that ρ is unitary with respect to the usual inner product.

Two representations ρ and σ are equivalent if they have the same dimension and there is a unitary change of basis U so that $U\rho(x)U^{-1} = \sigma(x)$ for all $x \in G$. The representation ρ reducible if there is a nontrivial splitting so that $V = V_1 \oplus V_2$ and $\rho(x)V_i = V_i$ for all $x \in G$ and $i = 1, 2$. A representation is faithful if it is an injective homomorphism.

We denote by \hat{G} the set of all irreducible representations of the group G , including only one representation from each equivalence class. The representations in \hat{G} can be reconstructed by decomposing the regular representation of G .

For basics of representation theory of finite groups we refer to [15]. The representation theoretical approach presented here is similar to the one presented in [9, Section 3] in the context of Lie groups.

6.2. Fourier analysis on finite groups. We wish to define the Fourier transform on finite groups analogously to the definition on Lie groups [9, 14].

We denote $\widehat{\mathbb{C}^G} = \bigoplus_{\rho \in \hat{G}} \mathbb{C}^{(\dim(\rho))^2}$. The space $\mathbb{C}^{(\dim(\rho))^2}$ is to be understood as the space of square matrices operating on the representation

space of ρ . An alternative, less coordinate dependent option would be to define $\widehat{\mathbb{C}}^G$ as the direct sum of the spaces of endomorphism of the representation spaces of the representations in \hat{G} .

We define the Fourier transform as map $\mathbb{C}^G \rightarrow \widehat{\mathbb{C}}^G$, $f \mapsto \tilde{f}$, given by

$$\tilde{f}(\rho) = \sum_{x \in G} f(x)\rho(x)$$

for $f \in \mathbb{C}^G$ and ρ . Note that $\tilde{f}(\rho)$ is indeed an endomorphism of the representation space of ρ . We will denote the inner product of two matrices by $A : B = \text{tr}(A^T B)$.

If the group G is cyclic, the Fourier transform defined above is just the usual discrete Fourier transform. For functions depending on several variables only one of which ranges in G , the Fourier transform is taken with respect to that variable.

Lemma 6.1. *For $x \in G$ we have*

$$\sum_{\rho \in \hat{G}} \dim(\rho) \text{tr}(\rho(x)) = \begin{cases} |G|, & x = e \\ 0, & x \neq e. \end{cases}$$

Proof. The mapping $x \mapsto \text{tr}(\rho(x))$ is called the character of the representation ρ . One of the standard orthogonality results for characters (see eg. [15, Section 2.3]) states that

$$\sum_{\rho \in \hat{G}} \overline{\text{tr}(\rho(y))} \text{tr}(\rho(x)) = \begin{cases} |G|/c(x), & x \text{ and } y \text{ conjugate} \\ 0, & \text{otherwise,} \end{cases}$$

where $c(x)$ is the size of the conjugacy class of x in G . Choosing $y = e$ and observing that $\text{tr}(\rho(e)) = \dim(\rho)$ gives the desired result. \square

Lemma 6.2. *The Fourier transform is a linear bijection.*

Proof. We will actually prove that the Fourier transform is an isometry when $\widehat{\mathbb{C}}^G$ is equipped with a suitable inner product. This suffices since the Fourier transform is a linear mapping between two spaces of the same (finite) dimension.

Let $f, g \in \mathbb{C}^G$. Using lemma 6.1 and $\rho(x)^* : \rho(y) = \text{tr}(\rho(x^{-1}y))$ we have

$$\begin{aligned} & \frac{1}{|G|} \sum_{\rho \in \hat{G}} \dim(\rho) \tilde{f}(\rho)^* : \tilde{f}(\rho) \\ &= \sum_{x, y \in G} \overline{f(x)} f(y) \frac{1}{|G|} \sum_{\rho \in \hat{G}} \dim(\rho) \rho(x)^* : \rho(y) \\ &= \sum_{x \in G} \overline{f(x)} f(x). \end{aligned} \quad \square$$

6.3. The Radon transform. For a representation $\rho \in \hat{G}$ and a homomorphism $\gamma \in \Gamma_n$ we denote

$$I(\rho, \gamma) = \sum_{t \in C_n} \rho(\gamma(t)).$$

The matrix $I(\rho, \gamma)$ is simply the sum of the representation ρ over the geodesic γ . Observe that if γ^{-1} denotes the pointwise inverse of γ , we have $I(\rho, \gamma^{-1}) = I(\rho, \gamma) = I(\rho, \gamma)^*$.

The next lemma provides the connection between representation theory and the Radon transform.

Lemma 6.3. *If $f \in \mathbb{C}^G$, $\rho \in \hat{G}$ and $\gamma \in \Gamma_n$, we have $\widetilde{Rf}(\rho, \gamma) = \tilde{f}(\rho)I(\rho, \gamma)$, where the Fourier transform is taken with respect to the first variable of Rf .*

Proof. The proof is a mere calculation:

$$\begin{aligned} \widetilde{Rf}(\rho, \gamma) &= \sum_{x \in G} \sum_{t \in C_n} f(x\gamma(t))\rho(x) \\ &= \sum_{y \in G} f(y)\rho(y) \sum_{t \in C_n} \rho(\gamma^{-1}(t)) \\ &= \tilde{f}(\rho)I(\rho, \gamma). \end{aligned} \quad \square$$

Lemma 6.3 provides a new approach to the Radon transform. We want to study whether the Radon transform is injective, that is, whether $Rf = 0$ implies $f = 0$. This problem has now been reduced to asking the following: if $\rho \in \hat{G}$ and A is a $\dim(\rho) \times \dim(\rho)$ matrix satisfying $AI(\rho, \gamma) = 0$ for all nontrivial homomorphisms γ , does A necessarily vanish?

To study this problem further, let us give the matrix $I(\rho, \gamma)$ a description.

Lemma 6.4. *Suppose $\gamma \in \Gamma_n$ and $\rho \in \hat{G}$. Let $g \in S_n$ be a generating element and let V be the representation space of ρ . Then $n^{-1}I(\rho, \gamma) : V \rightarrow V$ is the orthogonal projection to the subspace fixed by $\rho(\gamma(g))$.*

Proof. Since the matrix $\rho(\gamma(g))$ is unitary, a unitary change of basis turns it into a diagonal matrix with n th roots of unity as entries. If $z \in \mathbb{C}$ satisfies $z^n = 1$, then $z + z^2 + \cdots + z^n$ is n if $z = 1$ and zero otherwise. Applying this to each entry in the diagonal matrix proves the claim. \square

We have now found enough tools to give a second proof of theorem 3.5 about the Radon transform on finite abelian groups.

Second proof of theorem 3.5. Let G be a finite, abelian group of at least two elements. All of its irreducible representations are one dimensional and we identify matrices with complex numbers.

If G is cyclic, there is a faithful irreducible representation ρ . Since $\rho(x) \neq 1$ whenever $x \in G \setminus \{e\}$, lemma 6.4 implies that $I(\rho, \gamma) = 0$ for

all nontrivial homomorphisms $\gamma : C_n \rightarrow G$ for all n . If $f \in \mathbb{C}^G$ is such that $\tilde{f}(\rho) = 1$ and $\tilde{f}(\sigma) = 0$ for $\sigma \in \hat{G} \setminus \{\rho\}$, lemma 6.3 shows that $\widetilde{Rf} = 0$. By lemma 6.2 this implies $Rf = 0$ although $f \neq 0$, so the Radon transform is not injective.

Suppose then that G is not cyclic. Then there is a cyclic group C_p so that G has a subgroup isomorphic to $C_p \times C_p$. Let $\rho \in \hat{G}$. Now $\sigma = \rho|_{C_p \times C_p}$ is a one dimensional representation of $C_p \times C_p$. Every element in $C_p \times C_p$ has order 1 or p , so every value of σ is a p th root of unity. There are only p such roots so σ cannot be faithful. Therefore G has no faithful irreducible representations.

Now let $\rho \in \hat{G}$. Since it is not faithful, there is $x \in G \setminus \{e\}$ so that $\rho(x) = 1$. Let n be the order of x and let $\gamma : C_n \rightarrow G$ be a homomorphism containing x in its image. It follows from lemma 6.4 that $I(\rho, \gamma) = 1$ and then from lemma 6.3 that $Rf = 0$ implies $f = 0$. \square

We can extract the following more general statements from the previous proof: If G has a one dimensional faithful representation, the Radon transform cannot be injective. But if no irreducible representation is faithful, the Radon transform is injective.

We can also give a representation theoretical characterization of the finite groups where the Radon transform is injective and characterize the kernel when it is not injective. In order to do so, let us introduce some notation.

For $\rho \in \hat{G}$, let

$$k(\rho) = \bigcap_{p|G} \bigcap_{\gamma \in \Gamma_p} \ker(I(\rho, \gamma))$$

where the outer intersection is over all primes p that divide $|G|$. Here $I(\rho, \gamma)$ is understood as a linear mapping $\mathbb{C}^{\dim(\rho)} \rightarrow \mathbb{C}^{\dim(\rho)}$ so $k(\rho)$ is a subspace of $\mathbb{C}^{\dim(\rho)}$. Let $K^*(\rho)$ denote the space of square matrices with the conjugate transpose of each row belonging to $k(\rho)$.

The spaces $k(\rho)$ and $K^*(\rho)$ can be thought of as the vector and matrix kernels of the representation ρ . They describe the kernel of the Radon transform as we shall see next.

Lemma 6.5. *Let $\rho \in \hat{G}$. A square matrix A satisfies $AI(\rho, \gamma) = 0$ for all $\gamma \in \Gamma_p$ for all primes p if and only if $A \in K^*(\rho)$.*

Proof. Recall that $I(\rho, \gamma)^* = I(\rho, \gamma)$. The matrix A satisfies $AI(\rho, \gamma) = 0$ if and only if each row a of A satisfies $I(\rho, \gamma)a^* = 0$. The claim follows now directly from the definition of $K^*(\rho)$. \square

For a representation $\rho : G \rightarrow GL(V)$, let

$$F_\rho = \{v \in V; \rho(x)v = v \text{ for some } x \in G \setminus \{e\}\}$$

denote the set of fixed points.

Lemma 6.6. *Let G be a finite group and $\rho : G \rightarrow GL(V)$ an irreducible representation. Then either V is spanned by F_ρ or $F_\rho = \{0\}$.*

Proof. If $F_\rho = \{0\}$, then F_ρ clearly does not span V . We will show that the converse implication is also true.

If $v \in F_\rho$, then $\rho(x)v = v$ for some $x \in G \setminus \{e\}$. Then $\rho(yxy^{-1})\rho(y)v = \rho(y)v$ for any $y \in G$ and so $\rho(y)v \in F_\rho$ for all $y \in G$. Thus F_ρ is G -invariant, and so is its linear span. Now if F_ρ does not span V , its span has a nontrivial G -invariant complement by Maschke's theorem. But since ρ is irreducible, this complement must be V itself, so $F_\rho = \{0\}$. \square

Let us denote the set of irreducible representations of G without fixed points by

$$FPF(G) = \{\rho \in \hat{G}; F_\rho = \{0\}\}.$$

Lemma 6.7. *Let G be a finite group and $\rho : G \rightarrow GL(V)$ a unitary irreducible representation. Then either $F_\rho = \{0\}$ and $k(\rho) = V$ or F_ρ spans V and $k(\rho) = 0$.*

Proof. We will show that $k(\rho)$ and the span S of F_ρ are orthogonal complements of each other in V .

Suppose $v \in V$ satisfies $\rho(x)v = v$ for some nontrivial $x \in G$. If we take a minimal geodesic γ passing through e and x , it follows from lemma 6.4 that $I(\rho, \gamma)$ is an orthogonal projection to a subspace of V containing v . Therefore every vector in $k(\rho)$ is orthogonal to every $v \in S$. On the other hand, if a vector $w \in V$ is orthogonal to S , it is annihilated by every $I(\rho, \gamma)$ and thus $w \in k(\rho)$. This proves the desired orthogonality. \square

Theorem 6.8. *Let G be a finite group and $f : G \rightarrow \mathbb{C}$. Then $Rf = 0$ if and only if $\tilde{f}(\rho) \in K^*(\rho)$ for all $\rho \in \hat{G}$, or, equivalently, $\tilde{f}(\rho) = 0$ for all $\rho \in \hat{G} \setminus FPF(G)$.*

Proof. By lemma 2.1 it suffices to consider geodesics of prime length. By lemmas 6.2 and 6.3 we know that $Rf = 0$ if and only if $\tilde{f}(\rho)I(\rho, \gamma) = 0$ for all $\rho \in \hat{G}$ and $\gamma \in \Gamma_p$ for all primes p . Invoking lemma 6.5 then shows that $Rf = 0$ if and only if $\tilde{f}(\rho) \in K^*(\rho)$ for all $\rho \in \hat{G}$. The last claimed equivalence follows from lemma 6.7. \square

Theorem 6.9. *Let G be a finite group. The following are equivalent:*

- (1) *The Radon transform is injective on G .*
- (2) *$k(\rho) = 0$ for all $\rho \in \hat{G}$.*
- (3) *$FPF(G) = \emptyset$.*
- (4) *G is not a Frobenius complement.*

Proof. Equivalence of the first three statements is provided by theorem 6.8 and lemma 6.2. Equivalence of the last two statements is a well-known characterization of Frobenius complements. \square

Remark 6.10. The mentioned characterization is a folklore result (see eg. the first paragraph of [16]) in representation theory of finite groups. The fact that every Frobenius complements have such fixed-point-free representations is given in [12, Theorem 18.1v] but we have been unable to find a reference for the reverse direction in the literature. For more information about Frobenius groups, we refer the reader to [12, Section 18], [8, Section V.8] and [13, Section 4.6].

Unfortunately, Frobenius complements are not easy to recognize. There are some characterization results (see eg. [12, 16]) and the some of the results given in the present paper in Sections 3–5 follow from known properties of Frobenius complements. We point out that theorem 6.9 provides a new characterization of Frobenius complements in terms of the Radon transform.

7. GENERALIZATIONS AND VARIATIONS

7.1. Remarks on infinite groups. The situation in infinite groups is quite different. To demonstrate this difference, let us consider the group \mathbb{Z} . In the definition of geodesics we should replace the finite cyclic groups with the infinite cyclic group \mathbb{Z} . To make sense of the Radon transform, we should restrict our attention to functions in $\ell^1(\mathbb{Z})$. The Radon transform of a function in $\ell^1(\mathbb{Z})$ contains the sums over all cosets of infinite cyclic subgroups of \mathbb{Z} .

The Radon transform on this space is injective. Indeed, fix any $n \in \mathbb{Z}$ and consider the geodesic $\gamma_{n,m} : \mathbb{Z} \rightarrow \mathbb{Z}$, $\gamma_{n,m}(t) = n + mt$, for $m \geq 1$. If $f \in \ell^1(\mathbb{Z})$, it follows from summability that

$$f(n) = \lim_{m \rightarrow \infty} \sum_{t \in \mathbb{Z}} f(\gamma_{n,m}(t)).$$

Therefore the Radon transform is injective.

It follows from this and lemma 2.2 that if an infinite group G contains \mathbb{Z} as a subgroup (or, equivalently, has an element of infinite order), then the Radon transform is injective on $\ell^1(G)$. Restricting the Radon transform to periodic geodesics removes this phenomenon, but it also removes all geodesics from \mathbb{Z} .

For an example of different kind, consider the (additive) quotient group $G = \mathbb{Q}/\mathbb{Z}$. Every element has finite order, so the Radon transform is reasonable for any function $f : G \rightarrow \mathbb{C}$. Now it is an elementary calculation to observe that the function $f(x + \mathbb{Z}) = e^{2\pi i x}$ has zero Radon transform. It follows from this noninjectivity result that all finite subgroups of G are cyclic; for if there was a noncyclic finite subgroup, the Radon transform would be injective by lemma 2.2 and theorem 3.5.

We conclude our discussion of infinite groups with the following open problem. We have observed that for an infinite group G where every element has finite order, the Radon transform is injective if there is a finite subgroup on which it is injective. Is the converse true? Since all

elements have finite order, the functions $f : G \rightarrow \mathbb{C}$ need not satisfy any summability condition.

7.2. Discrete flows. One can also generalize geodesic flows to discrete settings without group structure. Let X be a set. A curve on X is a mapping from \mathbb{Z} (or an integer interval) to X . Let $s : X \times X \rightarrow X$ be a function. We say that a curve is an s -geodesic if for any two adjacent points $a, b \in X$ on a curve, the next point after a and b is $s(a, b)$.

To make this resemble geodesic flow, we want the function s to satisfy the following: $s(a, b) = b \iff a = b$ and $s(a, b) = c \iff s(c, b) = a$. These conditions ensure that the reverse of an s -geodesic is also an s -geodesic and that a nonconstant s -geodesic never terminates.

On a group we set $s(a, b) = ba^{-1}b$. This satisfies the above requirements and gives rise to geodesics as discussed in this article. If X is finite, every geodesic is periodic also without group structure.

We can now define the Radon transform corresponding to the successor function s by replacing the geodesics defined in section 2.1 by s -geodesics.

A flow satisfying the above requirements need not come from a group structure. On any set X one can define a flow by $s(a, b) = a$; all nonconstant geodesics have length two. If X were a group, a geodesic through the identity would be a cyclic subgroup and thus $|X|$ would have to be even, although the flow can be defined for any $|X|$.

The Radon transform corresponding to this particular flow is injective on any set X with at least three elements. To prove this, observe that the Radon transform Rf of a function $f : X \rightarrow \mathbb{C}$ gives the sum of f over any pair of points in X .

This flow can also be seen as a discrete time dynamical system on $X \times X$ taking (a, b) to $(b, s(a, b))$. The diagonal $\Delta \subset X \times X$ is precisely the set of stationary points. Projections of nontrivial orbits of this system to the first (or second) component are precisely the s -geodesics in the space X .

7.3. A variant of the Radon transform. Above we defined geodesics as cosets of nontrivial cyclic subgroups. Now we change this definition and require geodesics to be additionally maximal³. A cyclic subgroup is maximal if it is not contained in a larger cyclic subgroup. We call these new geodesics maximal geodesics and the corresponding transform the maximal Radon transform and denote it by \bar{R} instead of R . Note that by lemma 2.1 it suffices to analyze the *minimal* nontrivial geodesics to study the nonmaximal Radon transform.

This definition causes several changes to the theory. There are (typically strictly) fewer maximal geodesics than geodesics. Thus if \bar{R} is injective, so is R . Also, not all subgroups are totally geodesic (w.r.t.

³This definition was suggested by Peter Michor.

maximal geodesics). Totally geodesic subgroups correspond to Lie subgroups. Positive dimensional Lie groups can have both Lie subgroups and discrete subgroups, and this structure has now its discrete counterpart. Many of the results change, and we illustrate these changes in this section without developing a full theory of the maximal Radon transform.

In the case of Lie groups (with geodesics parameterized by S^1), every maximal abelian subgroup is totally geodesic. This is also true in the case of maximal discrete geodesics if the subgroup is cyclic or the whole group is abelian, but not necessarily otherwise. Consider for example the symmetric group S_5 and the subgroup H generated by $(1, 2)$ and $(3, 4)$. This is a maximal abelian subgroup, but the cyclic subgroup generated by $(1, 2)$ is maximal in H but not in S_5 . The subgroup of S_5 generated by $(1, 2)$ is contained in the one generated by $(1, 2)(3, 4, 5)$.

Proposition 7.1. *For any prime $p > 1$, the maximal Radon transform is injective in $C_p \times C_p$. On the other hand, the maximal Radon transform is not injective on any cyclic group.*

Proof. The proof of the first claim is the same as that of lemma 3.4 since all geodesics are maximal.

The second one follows from the fact that if \bar{R} were injective, R would also be, contradicting lemma 3.3. Another way to see this is that there is only one maximal cyclic subgroup, namely the group itself, so any function with zero average is in the kernel of the maximal Radon transform. \square

Recall that if G is a finite group and p is a prime, then a Sylow p -subgroup of G is a maximal subgroup of G such that the order of each element is a power of p . A Sylow subgroup is a Sylow p -subgroup for some prime p .

Proposition 7.2. *Consider the finite group $G = G_1 \times G_2$ where G_1 is cyclic and $|G_1|$ and $|G_2|$ are coprime. The maximal Radon transform is not injective on G .*

In particular, if G is a finite abelian group with a cyclic Sylow subgroup, the maximal Radon transform is not injective on it.

Proof. Let $\pi_i : G \rightarrow G_i$, $i = 1, 2$, be the two natural projections. We will first show that if C is a maximal cyclic subgroup of G , then $\pi_1(C) = G_1$.

Suppose C is a cyclic subgroup of G so that $\pi_1(C) \neq G_1$. We will show that it is not maximal. If g is a generator of C and g_1 a generator of G_1 , we know that $g_1 \notin \pi_1(C)$. But g_1 generates G_1 , so there is an integer m so that $g_1^m = \pi_1(g)$. Let n_1 and n_2 be the orders of g_1 and $\pi_2(g)$, respectively. Since n_1 and n_2 are coprime by assumption, there is an integer c so that $c \equiv m \pmod{n_1}$ and $c \equiv 1 \pmod{n_2}$. If

we let $h = (g_1, \pi_2(g))$, we have $h^m = g$. But h is not contained in the cyclic subgroup C generated by g , so C is not maximal.

There is a nonzero function $f : G_1 \rightarrow \mathbb{C}$ with zero average (this is essentially the second claim of proposition 7.1). Let us define $g : G \rightarrow \mathbb{C}$ by $g = f \circ \pi_1$. Since maximal geodesics have surjective projections to G_1 , the sum of g over every maximal geodesic is a multiple of the sum of f over G_1 and thus zero. Therefore g is a nonzero function but $\bar{R}g = 0$.

The second claim follows from Kronecker's decomposition theorem and the first claim. \square

Proposition 7.3. *Let G be a finite group and let S denote the set of its maximal cyclic subgroups. Then the maximal Radon transform is not injective on G if*

$$\sum_{H \in S} |H|^{-1} < 1 + \frac{|S| - 1}{|G|}.$$

Proof. The proof is essentially the same as that of proposition 5.5. \square

The following proposition is a discrete analogue of [9, Proposition 2.4]. When compared to the case of Lie groups, H should be understood as a discrete subgroup.

Proposition 7.4. *Let G be a finite group and H such a subgroup that no cyclic subgroup of H is a maximal subgroup of G . If the maximal Radon transform is injective on G , then the (nonmaximal) Radon transform is injective on the quotient G/H .*

Before embarking on the proof, let us take a moment to put the statement in some context since the situation is quite delicate. The analogous result is true for a Lie group G and a discrete normal subgroup H where both Radon transforms are the usual Radon transform on Lie groups [9, Proposition 2.4]. Proposition 7.4 is not symmetric: we assume injectivity of \bar{R}^G (which is a stronger condition than injectivity of R^G) and we obtain injectivity of $R^{G/H}$ (weaker than injectivity of $\bar{R}^{G/H}$). We have again indicated the underlying group by a superscript in the transform. As discussed in the beginning of section 5, the statement is false if we consider R^G and $R^{G/H}$.

The statement is also false if we consider \bar{R}^G and $\bar{R}^{G/H}$. Consider for example the group $G = C_6 \times C_6$ on which maximal Radon transform is injective⁴. Take any subgroup H with two elements; it will satisfy the assumption of proposition 7.4 because all maximal geodesics have

⁴We do not have an elegant proof for this fact, but it is easy to check computationally. There are 12 maximal cyclic subgroups and each has 6 distinct cosets. A function $f : G \rightarrow \mathbb{C}$ can be regarded as a vector in \mathbb{C}^{36} and the question is whether the 72 conditions (sums over geodesics) determine it uniquely. The rank of the corresponding 36×72 matrix turns out to be 36.

length six. Now the maximal Radon transform is not injective on $G/H \approx C_3 \times C_6$ by proposition 7.2.

Proof of proposition 7.4. Suppose $f : G/H \rightarrow \mathbb{C}$ satisfies $R^{G/H} f = 0$. If $\pi : G \rightarrow G/H$ is the natural projection, we want to show that $\pi^* f : G \rightarrow \mathbb{C}$ (and thus f itself) vanishes by considering its maximal Radon transform. To this end, let $\gamma : C_n \rightarrow G$ be any homomorphism whose image is a maximal cyclic subgroup and let $x \in G$. Then

$$\bar{R}^G(\pi^* f)(x, \gamma) = R^G(\pi^* f)(x, \gamma) = R^{G/H} f(\pi(x), \pi \circ \gamma).$$

Suppose we know that $\pi \circ \gamma : C_n \rightarrow G/H$ is nontrivial. Then we get $\pi^* f = 0$ using the assumption $R^{G/H} f = 0$ and injectivity of \bar{R}^G .

Let us then show that $\pi \circ \gamma$ is indeed nontrivial. If g is a generator of C_n , we want to show that $\pi(\gamma(g)) \neq e$. If this were not the case, we would have $\gamma(g) \in H$, whence $\gamma(C_n) \subset H$. We have assumed that $\gamma(C_n)$ is a maximal cyclic subgroup of G and that H cannot contain such a subgroup. This contradiction concludes the proof. \square

ACKNOWLEDGEMENTS

This work was supported by the Academy of Finland (Centre of Excellence in Inverse Problems Research) and an ERC Starting Grant. The author wishes to express his gratitude to the help received at Math-Overflow. The folklore characterization of Frobenius complements via representation theory would never have made it here without discussions with Frieder Ladisch.

REFERENCES

- [1] V. Batagelj. Norms and distances over finite groups. *Journal of Combinatorics, Information & System Sciences*, 20:243–252, 1995.
- [2] N. S. Dairbekov and V. A. Sharafutdinov. Some problems of integral geometry on Anosov manifolds. *Ergodic Theory and Dynamical Systems*, 23:59–74, 2 2003.
- [3] P. Funk. Über Flächen mit lauter geschlossenen geodätischen Linien. *Math. Ann.*, 74(2):278–300, 1913.
- [4] E. L. Grinberg. Radon transforms on higher Grassmannians. *J. Differential Geom.*, 24(1):53–68, 1986.
- [5] E. L. Grinberg. Integration over minimal spheres in Lie groups and symmetric spaces of compact type. In *75 years of Radon transform (Vienna, 1992)*, Conf. Proc. Lecture Notes Math. Phys., IV, pages 167–174. Int. Press, Cambridge, MA, 1994.
- [6] E. L. Grinberg and S. G. Jackson. On the kernel of the maximal flat Radon transform on symmetric spaces of compact type. 2014. arXiv:1406.7219.
- [7] S. Helgason. *The Radon Transform*. Birkhäuser, 2. edition, 1999.
- [8] B. Huppert. *Endliche Gruppen. I*. Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin-New York, 1967.
- [9] J. Ilmavirta. On Radon transforms on compact Lie groups. *Proceedings of the American Mathematical Society*, 2014. To appear, arXiv:1410.2114.

- [10] J. Ilmavirta. On Radon transforms on tori. *Fourier Analysis and Applications*, 2014. To appear, arXiv:1402.6209.
- [11] F. Natterer. *The Mathematics of Computerized Tomography*. Society for Industrial and Applied Mathematics, 2001.
- [12] D. Passman. *Permutation groups*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.
- [13] L. Ribes and P. Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, 2000.
- [14] M. Ruzhansky and V. Turunen. *Pseudo-differential operators and symmetries: Background Analysis and Advanced Topics*, volume 2 of *Pseudo-Differential Operators. Theory and Applications*. Birkhäuser Verlag, Basel, 2010.
- [15] J. P. Serre. *Linear Representations of Finite Groups*, volume 42 of *Graduate Texts in Mathematics*. Springer New York, 1977.
- [16] A. Shalev. A new characterization of Frobenius complements. *Israel J. Math.*, 87(1-3):153–160, 1994.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF JYVÄSKYLÄ,
P.O.BOX 35 (MAD) FI-40014 UNIVERSITY OF JYVÄSKYLÄ, FINLAND
E-mail address: joonas.ilmavirta@jyu.fi