COMBINATORIAL THEORY **5 (3)** (2025), #5 combinatorial-theory.org

On the determination of sets by their subset sums

Andrea Ciprietti[1] and Federico Glaudo*[2]

[1]*Department of Mathematics, University of Pisa, Pisa, Italy*
andreaciprietti99@gmail.com
[2]*School of Mathematics, Institute for Advanced Study, Princeton NJ, U.S.A.*
fglaudo@ias.edu

Submitted: Sep 12, 2024; Accepted: Mar 19, 2025; Published: Sep 15, 2025

Abstract. Let A be a multiset with elements in an abelian group. Let $\mathrm{FS}(A)$ be the multiset containing the $2^{|A|}$ sums of all subsets of A.

We study the reconstruction problem "Given $\mathrm{FS}(A)$, is it possible to identify A?". We prove that, up to identifying multisets through a natural equivalence relation, the function $A \mapsto \mathrm{FS}(A)$ is injective (and thus the reconstruction problem is solvable) if and only if every order n of a torsion element of the abelian group satisfies a number-theoretical property related to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$.

The core of the proof relies on a delicate study of the structure of cyclotomic units. Moreover, as a tool, we develop an inversion formula for a novel discrete Radon transform on finite abelian groups that might be of independent interest.

Keywords. Subset sums, inverse problems, Radon transform, cyclotomic extension

Mathematics Subject Classifications. 11P70, 05B10, 11R18, 44A12

1. Introduction

Let G be an abelian group and let $A = \{a_1, a_2, \dots, a_{|A|}\}$ be a finite multiset (i.e., a set with repeated elements) with elements in G (see Section 2.1 for a formal definition of multiset). Its *subset sums multiset* $\mathrm{FS}(A)$, that is, the multiset containing the $2^{|A|}$ sums over all subsets of A (taking into account multiplicities), is defined as

$$\mathrm{FS}(A) \coloneqq \Big\{ \sum_{i\in I} a_i : I \subseteq \{1, 2, \dots, |A|\} \Big\}.$$

*Supported by the National Science Foundation under Grant No. DMS-1926686.

We study the following reconstruction question:

If one is given $\mathrm{FS}(A)$*, is it possible to identify* A*?*

As we will see, this strikingly simple question features a rich structure and its solution spans a wide range of mathematics: from the theory of cyclotomic units, to an inversion formula for a novel discrete Radon transform. Before going deeper into the problem, let us give some background on related results in the literature.

If, instead of $\mathrm{FS}(A)$, one is given the sums over all the $\binom{|A|}{s}$ subsets with fixed size equal to s (e.g., if $s = 2$, the sums over all pairs), the reconstruction problem has been studied in the case of a free abelian group $G = \mathbb{Z}^d$ [SS58, GFS62]. For pairs (i.e., $s = 2$), the reconstruction is possible when the size of A is not a power of 2 [SS58, Theorem 1 and Theorem 2]. For s-subsets with $s > 2$, the reconstruction is possible if the size of A does not belong to a finite subset of *bad* sizes [GFS62, Section 4] (see also [BL96, AZ97] for a precise analysis of certain values of $s > 2$). See the recent survey [Fom19] for a detailed presentation of the history of this problem.

If, instead of $\mathrm{FS}(A)$, one is given $A + A$ (i.e., the sum of any two elements of A, not necessarily distinct), the problem has been studied extensively for infinite sets of nonnegative integers (see, for example, [Lev04, CL16, Hel17, KS19] and the survey [Nat08]).

It might seem that if one is only provided with the sums of s-subsets (i.e., subsets with size s) then the reconstruction is strictly harder than if one is provided the sums of all subsets. This is false because the information is not ordered and thus, even if we have more information, it is harder to determine which value corresponds to which subset.

Let us now go back to the reconstruction problem for FS. The first important observation is the following one. Given a multiset A and a subset $B \subseteq A$ whose sum equals 0 (i.e., $\sum_{b\in B} b = 0$), if we flip the signs of elements of B then FS does not change. So, if $A' := (A \setminus B) \cup (-B)$, then $\mathrm{FS}(A) = \mathrm{FS}(A')$ (see Figure 1.1 for an explanation).

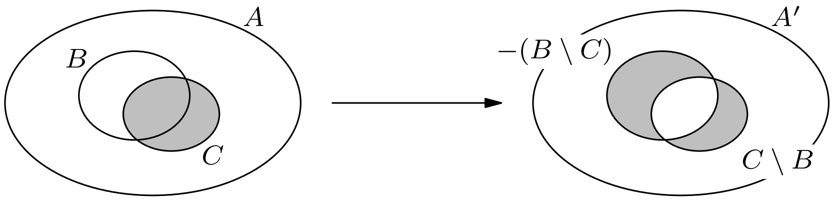


Figure 1.1: Proof by picture of $A \sim_0 A' \implies \mathrm{FS}(A) = \mathrm{FS}(A')$. The set C in A (highlighted in gray) and the set $(C \setminus B) \cup (-(B \setminus C))$ in A' (highlighted in gray) have the same sum because the sum of the elements in B is assumed to be 0. Thus, we have a bijection between the subsets of A and A' which keeps the sum unchanged, hence $\mathrm{FS}(A) = \mathrm{FS}(A')$.

Hence, if we only know $\mathrm{FS}(A)$, the best we can hope for is to identify the equivalence class of A with respect to the following equivalence relation.

Definition 1.1. Given two multisets A, A' with elements in G, we say that $A \sim_0 A'$ if and only if A' can be obtained from A by flipping the signs of the elements of a subset of A with null sum, i.e., if there exists $B \subseteq A$, with $\sum_{b\in B} b = 0$, such that $A' = (A \setminus B) \cup (-B)$.

We have already observed that if $A \sim_0 A'$ then $\mathrm{FS}(A) = \mathrm{FS}(A')$. If the group is $G = \mathbb{Z}$, this turns out to be an "if and only if" (see Proposition 6.4), while if $G = \mathbb{Z}/2\mathbb{Z}$ it is not (indeed, in $\mathbb{Z}/2\mathbb{Z}$ one has $\mathrm{FS}(\{0,1\}) = \{0,0,1,1\} = \mathrm{FS}(\{1,1\})$). It is natural to consider the class of abelian groups such that the double implication holds, i.e., the fibers of FS coincide with the equivalence classes of $\sim_0$.

Definition 1.2. An abelian group G is FS-regular if, for any two multisets A, A' with elements in G, it holds $\mathrm{FS}(A) = \mathrm{FS}(A')$ if and only if $A \sim_0 A'$.

We have already observed that $\mathbb{Z}/2\mathbb{Z}$ is not FS-regular; moreover, any group containing a subgroup that is not FS-regular cannot be FS-regular. The next smallest non-FS-regular group is elusive; in fact, it turns out that $\mathbb{Z}/n\mathbb{Z}$ is FS-regular for $n = 3, 5, 7, 9, 11, 13, 15$. But $\mathbb{Z}/17\mathbb{Z}$ is not FS-regular, and then $\mathbb{Z}/n\mathbb{Z}$ is FS-regular for $n = 19, 21, 23, 25, 27, 29$ and not FS-regular for $m = 31, 33$. These small examples suggest that the FS-regularity of G may be related to the behavior of powers of two in G (notice that $17, 31, 33$ are adjacent to a power of two).

Our main result is the characterization of FS-regular groups. In order to state our result, we need to introduce a subset of the natural numbers.

Definition 1.3. Let O_{FS} be the set of odd natural numbers $n \geqslant 1$ such that $(\mathbb{Z}/n\mathbb{Z})^*$ is covered by $\{\pm 2^j : j \geqslant 0\}$; more precisely, for each $x \in \mathbb{Z}$ relatively prime with n there exists $j \geqslant 0$ such that either $x - 2^j$ or $x + 2^j$ is divisible by n.

Remark 1.4. The first few elements of O_{FS} are

$$O_{\mathrm{FS}} = \{1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 35, 37, 39, 45, 47, 49, \dots\},$$

and the first few *missing* odd numbers are

$$(2\mathbb{N} + 1) \setminus O_{\mathrm{FS}} = \{17, 31, 33, 41, 43, 51, 57, 63, 65, 73, 85, 89, 91, 93, 97, 99, \dots\}.$$

Let us remark that if $n \in O_{\mathrm{FS}}$ then also all divisors of n belong to O_{FS}. Moreover, if $n \in O_{\mathrm{FS}}$ then n has at most two distinct prime factors. We prove these and some other basic properties of the set O_{FS} at the end of Section 3.

We can now state our main theorem.

Theorem 1.5 (Characterization of FS-regular groups)**.** *An abelian group G is* FS*-regular if and only if* $\mathrm{ord}(g) \in O_{\mathrm{FS}}$ *for all $g \in G$ with finite order.*

As a tool in the proof of Theorem 1.5 (see Section 1.1) we define a novel discrete Radon transform for abelian groups and we prove an inversion formula for it. We refer to Section 5 for some motivation on the definition and for an in-depth discussion of the existing related literature. Since the inversion formula for the Radon transform may have other applications beyond the scope of this paper, we state it here for the interested readers.

Theorem 1.6 (Inversion formula for the discrete Radon transform)**.** *Let $n, d \geqslant 1$ be positive integers. Given a function $f : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{C}$, its discrete Radon transform $Rf = R_{n,d}f$: $\mathrm{Hom}((\mathbb{Z}/n\mathbb{Z})^d, \mathbb{Z}/n\mathbb{Z}) \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ is defined as*

$$Rf(\psi, c) = \sum_{x\colon \psi(x)=c} f(x).$$

One can reconstruct the values of f from Rf through the formula, valid for any $x \in (\mathbb{Z}/n\mathbb{Z})^d$,

$$f(x) = \frac{1}{n^{d-1}\varphi(n)} \sum_{\psi\in\mathrm{Hom}((\mathbb{Z}/n\mathbb{Z})^d,\mathbb{Z}/n\mathbb{Z})} Rf(\psi, \psi(x)) \prod_{p|\psi}(1 - p^{d-1}),$$

where the notation $p \mid \psi$ shall be understood as the fact that the prime *p, divisor of n, divides all the elements in the image of ψ, or equivalently that ψ takes values into $p\mathbb{Z}/n\mathbb{Z}$. The function φ denotes Euler's totient function.*

1.1. Sketch of the proof and structure of the paper

Let us briefly describe the strategy that the proof follows, postponing a more detailed presentation to the dedicated sections.

For the negative part of the statement, it is sufficient to show that $\mathbb{Z}/n\mathbb{Z}$ is not FS-regular if $n \notin O_{\mathrm{FS}}$. For this, we construct an explicit counterexample in Proposition 4.1.

Proving that if the orders belong to O_{FS} then the group is FS-regular is more complicated and relies on some nontrivial properties of the units of cyclotomic fields and on the inversion formula for a novel discrete Radon transform on finite abelian groups. The proof is divided into three steps.

Step 1: Proof for $G = \mathbb{Z}/n\mathbb{Z}$. Through the polynomial identity[1]

$$\sum_{s\in\mathrm{FS}(A)} t^s \equiv \prod_{a\in A}(1 + t^a) \pmod{t^n - 1},$$

we reduce the FS-regularity of $\mathbb{Z}/n\mathbb{Z}$ to the study of the kernel of the map

$$\mathbb{Z}^n \ni x = (x_0, x_1, \dots, x_{n-1}) \mapsto \left(\prod_{j=0}^{n-1}(1 + \omega_d^j)^{x_j}\right)_{d|n},$$

where $\omega_d \in \mathbb{C}$ is a d-th primitive root of unity and the codomain of the map consists of tuples indexed by the divisors of n. Thanks to a dimensional argument, identifying the kernel of such map is equivalent to identifying its image, which is exactly what we do in Lemma 4.7. This is the hardest and most technical proof of the paper. Up to this point, we have used only that n is odd. The fact that $n \in O_{\mathrm{FS}}$ is needed in the computation of the rank of the image, which relies on the theory of cyclotomic units (see Lemma 4.4).

This step is carried out in Section 4.

[1] Instead of using polynomials modulo $t^n - 1$, one can also consider the Fourier transform of the characteristic functions of $\mathrm{FS}(A)$ and reach the same conclusion.

Step 2: $\mathbb{Z}/n\mathbb{Z}$ **is** FS**-regular** $\implies$ $(\mathbb{Z}/n\mathbb{Z})^d$ **is** FS**-regular.** Take A, A' multisets with elements in $(\mathbb{Z}/n\mathbb{Z})^d$ such that $\mathrm{FS}(A) = \mathrm{FS}(A')$. Given a homomorphism $\psi : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{Z}/n\mathbb{Z}$, by linearity, it holds $\mathrm{FS}(\psi(A)) = \mathrm{FS}(\psi(A'))$, and since $\mathbb{Z}/n\mathbb{Z}$ is FS-regular this implies that $\psi(A) \sim_0 \psi(A')$. So, we know that $\psi(A) \sim_0 \psi(A')$ for all homomorphisms $\psi : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{Z}/n\mathbb{Z}$. In order to deduce that $A \sim_0 A'$, we introduce a discrete Radon transform for finite abelian groups (see Definition 5.1) and we use its invertibility to reconstruct a multiset $B \in \mathcal{M}((\mathbb{Z}/n\mathbb{Z})^d)$ from the family of its *projections*

$$\left\{\psi(B) : \psi \in \mathrm{Hom}((\mathbb{Z}/n\mathbb{Z})^d, \mathbb{Z}/n\mathbb{Z})\right\}.$$

This step is performed in Section 5.

Step 3: G **is** FS**-regular** $\implies$ $G \oplus \mathbb{Z}$ **is** FS**-regular.** In this step, we exploit crucially that $\mathbb{Z}$ is totally ordered. The argument is short and purely combinatorial. This is done in Section 6.

Once these three steps are established, Theorem 1.5 follows naturally, as shown in Section 7. Let us remark here that our proof is not constructive, hence it does not provide an efficient algorithm to find the $\sim_0$-equivalence class of A if $\mathrm{FS}(A)$ is known[2].

To make the paper accessible to a broad audience, in Section 2 we recall basic facts about multisets, abelian groups, and cyclotomic units.

2. Notation and preliminaries

2.1. Multisets

A *multiset* with elements in a set X is an unordered collection of elements of X which may contain a certain element more than once [Bli89]. For example, $\{1, 1, 2, 2, 3\}$ is a multiset. Rigorously, a multiset A is encoded by a function $\mu_A : X \to \mathbb{Z}_{\geqslant 0}$ ($\mathbb{Z}_{\geqslant 0}$ denotes the set of nonnegative integers) such that $\mu_A(x)$ represents the multiplicity of the element x in A. For example, if $A = \{1, 1, 2, 2, 3\}$ then $\mu_A(1) = 2$, $\mu_A(2) = 2$, $\mu_A(3) = 1$.

A multiset A is *finite* if $\sum_{x \in X} \mu_A(x) < \infty$. The cardinality of a finite multiset $A \in \mathcal{M}(X)$ is given by $|A| := \sum_{x \in X} \mu_A(x)$.

Given a set X, let us denote with $\mathcal{M}(X)$ the family of finite multisets with elements in X.

Let us define the usual set operations on multisets. Notice that all of them are the natural generalization of the standard version when one takes into account the multiplicity of elements. Fix two multisets $A, B \in \mathcal{M}(X)$.

Membership. We say that $x \in X$ is an element of A, denoted by $x \in A$, if $\mu_A(x) \geqslant 1$.

Inclusion. We say that A is a subset of B, denoted by $A \subseteq B$, if $\mu_A(x) \leqslant \mu_B(x)$ for all $x \in X$.

Union. The union $A \cup B \in \mathcal{M}(X)$ is defined as $\mu_{A \cup B}(x) := \mu_A(x) + \mu_B(x)$. Hence, $\{1\} \cup \{1, 2\} = \{1, 1, 2\}$.

[2]The nonconstructive part of the proof is contained Section 4. In fact, we show that a certain map is injective by proving its surjectivity and then applying a standard dimension argument. This kind of reasoning does not produce an efficient way to invert the map we have proven to be injective.

Cartesian product. The Cartesian product $A \times B \in \mathcal{M}(X \times X)$ is defined as $\mu_{A\times B}((x_1, x_2)) = \mu_A(x_1)\mu_B(x_2)$.

Difference. If $A \subseteq B$, the difference $B \setminus A$ is defined as $\mu_{B\setminus A}(x) \coloneqq \mu_B(x) - \mu_A(x)$.

Pushforward. Given a function $f : X \to Y$, the pushforward $f(A) \in \mathcal{M}(Y)$ of the multiset A (denoted also by $\{f(a) : a \in A\}$) is defined as

$$\mu_{f(A)}(y) = \sum_{x\in f^{-1}(y)} \mu_A(x).$$

Power set The power set of A (the family of subsets of A), denoted by $\mathcal{P}(A) \in \mathcal{M}(\mathcal{M}(X))$, is a multiset defined recursively as follows. For the empty multiset, we have $\mathcal{P}(\varnothing) \coloneqq \{\varnothing\}$; otherwise let $a \in A$ be an element of A and define

$$\mathcal{P}(A) \coloneqq \mathcal{P}(A \setminus \{a\}) \cup \Big\{A' \cup \{a\} : A' \in \mathcal{P}(A \setminus \{a\})\Big\}.$$

Notice that $|\mathcal{P}(A)| = 2^{|A|}$. Whenever we iterate over the subsets of A (e.g., $\{f(A') : A' \subseteq A\}$ or $\sum_{A'\subseteq A} f(A')$), the iteration has to be understood over $\mathcal{P}(A)$ (hence the subsets are counted with multiplicity).

Taking the complement is an involution of the power set, i.e., $\mathcal{P}(A) = \{A \setminus A' : A' \in \mathcal{P}(A)\}$, and we have the following identity for the power set of a union

$$\mathcal{P}(A \cup B) = \{A' \cup B' : (A', B') \in \mathcal{P}(A) \times \mathcal{P}(B)\}.$$

Sum (and product) If the set X is an additive abelian group, we can define the sum $\sum A \in X$ of the elements of A as

$$\sum A \coloneqq \sum_{x\in X} \mu_A(x)x.$$

Analogously, if X is a multiplicative abelian group, one can define the product $\prod A$ of the elements of A.

2.2. Abelian groups

Let us recall some basic facts about abelian groups that we will use extensively later on.

Any finitely generated abelian group is isomorphic to a finite product of cyclic groups [Lan02, Chapter I, Section 8]. We denote with $\mathbb{Z}/n\mathbb{Z}$ the cyclic group with n elements.

Given some elements $g_1, g_2, \dots, g_k \in G$ of an abelian group, we denote with $\langle g_1, g_2, \dots, g_k\rangle$ the subgroup generated by such elements. Given an element $g \in G$, its order (which may be equal to ∞) is denoted by $\operatorname{ord}(g)$.

For an abelian group G, its rank $\operatorname{rk}(G)$ is the cardinality of a maximal set of $\mathbb{Z}$-independent[3] elements of G. Let us list some useful properties of the rank (see [Lan02, Chapter I and XVI]).

[3]Some elements $g_1, g_2, \dots, g_k \in G$ are $\mathbb{Z}$-independent if, whenever $\sum_i a_i g_i = 0$ for some $a_1, a_2, \dots, a_k \in \mathbb{Z}$, it holds $a_1 = a_2 = \dots = a_k = 0$.

- Any finitely generated abelian group G is isomorphic to $\mathbb{Z}^{\mathrm{rk}(G)} \oplus G'$ where G' is a finite abelian group.
- Given two abelian groups G, H, it holds $\mathrm{rk}(G \oplus H) = \mathrm{rk}(G) + \mathrm{rk}(H)$.
- For a homomorphism $\phi : G \to H$ of abelian groups, it holds $\mathrm{rk}(G) = \mathrm{rk}(\ker \phi) + \mathrm{rk}(\mathrm{Im}\ \phi)$.
- An abelian group has null rank if and only if all elements have finite order.
- Let G_1, G_2, G_3 be three abelian groups and $\phi_1 : G_1 \to G_2$, $\phi_2 : G_2 \to G_3$ be two homomorphisms with full rank, i.e., $\mathrm{rk}(\mathrm{Im}\ \phi_1) = \mathrm{rk}(G_2)$ and $\mathrm{rk}(\mathrm{Im}\ \phi_2) = \mathrm{rk}(G_3)$. Then $\phi_2 \circ \phi_1 : G_1 \to G_3$ has full rank as well, i.e., $\mathrm{rk}(\mathrm{Im}\ \phi_2 \circ \phi_1) = \mathrm{rk}(G_3)$
- Given an abelian group G, let us denote with $G \otimes \mathbb{Q}$ its tensor product (as a $\mathbb{Z}$-module) with $\mathbb{Q}$ (see [Lan02, Chapter XVI]). The dimension of $G \otimes \mathbb{Q}$ as vector space over $\mathbb{Q}$ coincides with $\mathrm{rk}(G)$.
- For a homomorphism $\phi : G \to H$ of abelian groups, let $\phi \otimes \mathbb{Q} : G \otimes \mathbb{Q} \to H \otimes \mathbb{Q}$ be its tensorization with $\mathbb{Q}$. It holds $\mathrm{rk}(\mathrm{Im}\ \phi) = \dim_{\mathbb{Q}}(\mathrm{Im}\,(\phi \otimes \mathbb{Q}))$.

2.3. Units of cyclotomic fields

Given $n \geqslant 1$, let $\omega_n := \exp(2\pi i/n)$ be the primitive n-th root of unity with minimum positive argument.

The algebraic number field $\mathbb{Q}(\omega_n)$ is called *cyclotomic field*. It is well-known that the ring of integers of $\mathbb{Q}(\omega_n)$ coincides with $\mathbb{Z}[\omega_n]$. Our main focus is the group of units of $\mathbb{Q}(\omega_n)$, that consists of the invertible elements of its ring of integers.

For $0 < r < n$ and $s \geqslant 1$ coprime with n, the element $\xi := \frac{1-\omega_n^{rs}}{1-\omega_n^r}$ is a unit of $\mathbb{Q}(\omega_n)$. Indeed $\xi = 1 + \omega_n^r + \cdots + \omega_n^{(s-1)r} \in \mathbb{Z}[\omega_n]$ and, if $u \in \mathbb{N}$ is such that n divides $us - 1$, then

$$\xi^{-1} = \frac{1-\omega_n^{rus}}{1-\omega_n^{rs}} = 1 + \omega_n^{rs} + \cdots + \omega_n^{(u-1)rs} \in \mathbb{Z}[\omega_n].$$

It turns out that these units are sufficient to generate a subgroup of finite index of the units of $\mathbb{Q}(\omega_n)$. The following statement follows from [Was97, Theorem 8.3 and Theorem 4.12].

Theorem 2.1. *For any odd $n \geqslant 3$, the multiplicative group $C_n \subseteq \mathbb{C}$ generated by*

$$\left\{ \frac{1-\omega_n^{rs}}{1-\omega_n^r} : 0 < r < n,\ s \geqslant 1 \text{ coprime with } n \right\}$$

is a subgroup of finite index of the units of $\mathbb{Q}(\omega_n)$.

Thus, applying Dirichlet's unit Theorem (see [Mar77, Theorem 38]), we are able to compute the rank of C_n (since it coincides with the rank of the group of units of $\mathbb{Q}(\omega_n)$).

Corollary 2.2. *For any odd $n \geqslant 3$, we have $\mathrm{rk}(C_n) = \frac{\varphi(n)}{2} - 1$, where φ is Euler's totient function (and C_n is defined in Theorem 2.1).*

The units of $\mathbb{Q}(\omega_n)$ satisfy a family of nontrivial relations known as distribution relations (see [Was97, 151]). We recall here the relations in the form we will need. Notice that $1+\omega_n^j$ is a unit for $1 \leqslant j < n$ because of the identity $1+\omega_n^j = \frac{1-\omega_n^{2j}}{1-\omega_n^j} \in C_n$.

Proposition 2.3 (Distribution relations)**.** *Let $n \geqslant 1$ be an odd integer and let p be one of its prime divisors*[4]*. For any $0 \leqslant j < \frac{n}{p}$, the identity*

$$\prod_{k=0}^{p-1}(1+\omega_n^{j+kn/p}) = 1+\omega_n^{jp}$$

holds.

Proof. The numbers $\{1+\omega_n^{j+kn/p}\}_{0\leqslant k<p}$ are the roots of the monic polynomial $(t-1)^p - \omega_n^{jp} \in \mathbb{C}[t]$. Therefore, their product equals the constant term of the polynomial multiplied by $(-1)^p$, which is $((-1)^p - \omega_n^{jp})(-1)^p = 1+\omega_n^{jp}$. □

3. Definitions and basic facts

In this section we give some fundamental definitions (some of them are already present in the introduction, we repeat them here for the ease of the reader) and we prove some basic results which will be useful multiple times in the paper. Even though they are not necessary for the rest of the paper, for completeness, we present and prove the main properties of the set O_{FS} which appears in the main theorem of this work.

Definition 3.1. Let G be an additive abelian group and take $A \in \mathcal{M}(G)$. The *subset sums multiset* of A is (we adopt the notation of [TV06])

$$\mathrm{FS}(A) := \left\{\sum B : B \in \mathcal{P}(A)\right\},$$

that is, the multiset whose elements are the sums of the subsets of A.

When studying the injectivity of FS, one soon notices that if we take a multiset $A \in \mathcal{M}(G)$ and we flip the sign of a subset of its elements with zero sum, obtaining another multiset $A' \in \mathcal{M}(G)$, then the subset sums do not change, i.e., $\mathrm{FS}(A) = \mathrm{FS}(A')$. Therefore, the following definition and the results of Lemma 3.3 should appear natural.

Definition 3.2. Given an additive abelian group G, we define the equivalence relations $\sim$ and $\sim_0$ over $\mathcal{M}(G)$ as follows:

- Given $A, A' \in \mathcal{M}(G)$, $A \sim A'$ if A' is obtained from A by changing the sign of the elements of a subset of A. More formally, $A \sim A'$ if and only if there exists $B \subseteq A$ such that $A' = (A \setminus B) \cup (-B)$.

[4]The identity holds, with the same proof, also without the assumption that p is prime.

- Given $A, A' \in \mathcal{M}(G)$, $A \sim_0 A'$ if A' is obtained from A by changing the sign of the elements of a zero-sum subset of A. More formally, $A \sim_0 A'$ if and only if there exists $B \subseteq A$ with null sum $\sum B = 0_G$ such that $A' = (A \setminus B) \cup (-B)$.

Notice that the relations $\sim$ and $\sim_0$ are reflective and transitive.

Lemma 3.3. *Given two multisets $A, A' \in \mathcal{M}(G)$ with elements in an abelian group G, we have the following statements concerning the relationship between $\sim_0$, $\sim$ and* FS.

(1) If $A \sim_0 A'$ then $\mathrm{FS}(A) = \mathrm{FS}(A')$.

(2) If $A \sim A'$, then there is $g \in G$ such that $\mathrm{FS}(A) = \mathrm{FS}(A') + g$.

(3) Assume that G does not have elements with order 2. If $\mathrm{FS}(A) = \mathrm{FS}(A')$ and $A \sim A'$, then $A \sim_0 A'$.

(4) If $\mathrm{FS}(A) = \mathrm{FS}(A') + g$ for some $g \in G$, then there exists $\mathcal{M}(G) \ni A'' \sim A'$ such that $\mathrm{FS}(A) = \mathrm{FS}(A'')$.

Proof. The following paragraph describes a very simple bijection in a very complicated way, this is due to the formalism necessary to handle the multiplicities of elements in multisets. We suggest the reader to refer to the picture Figure 1.1, which shall be much clearer than the proof itself.

If $A \sim A'$, then, by definition, there is $B \subseteq A$ such that $A' = (A \setminus B) \cup (-B)$. So, we have

$$\begin{aligned}\mathcal{P}(A') &= \Big\{C \cup (-D) : (C, D) \in \mathcal{P}(A \setminus B) \times \mathcal{P}(B)\Big\}\\ &= \Big\{C \cup (-(B \setminus D)) : (C, D) \in \mathcal{P}(A \setminus B) \times \mathcal{P}(B)\Big\}\end{aligned}$$

and therefore

$$\begin{aligned}\mathrm{FS}(A') &= \Big\{\sum C + \sum D - \sum B : (C, D) \in \mathcal{P}(A \setminus B) \times \mathcal{P}(B)\Big\}\\ &= \Big\{\sum C + \sum D : (C, D) \in \mathcal{P}(A \setminus B) \times \mathcal{P}(B)\Big\} - \sum B \\ &= \mathrm{FS}(A) - \sum B.\end{aligned} \tag{3.1}$$

This proves *(2)*.

Notice that if $A \sim A'$ and $\sum B = 0$, then Equation (3.1) implies that $\mathrm{FS}(A) = \mathrm{FS}(A')$. Hence also *(1)* are proven.

Let us show *(3)*. The assumption $\mathrm{FS}(A) = \mathrm{FS}(A')$, together with Equation (3.1), implies that $\mathrm{FS}(A) = \mathrm{FS}(A) - \sum B$. By taking the sum of the elements of the two multisets, we get

$$\sum(\mathrm{FS}(A)) = \sum(\mathrm{FS}(A) - \sum B) = \sum(\mathrm{FS}(A)) - |\,\mathrm{FS}(A)| \cdot \sum B,$$

thus $2^{|A|} \sum B = 0_G$. Since G has no elements of order 2, we deduce $\sum B = 0_G$ and therefore $A \sim_0 A'$ as desired.

In order to prove *(4)*, notice that $0_G \in \mathrm{FS}(A)$ and thus $-g \in \mathrm{FS}(A')$; so there is $B \subseteq A'$ such that $\sum B = -g$. Let $A'' \sim A$ be the multiset $A'' := (A' \setminus B) \cup (-B)$. The formula Equation (3.1) (with $A, A' \to A', A''$) yields $\mathrm{FS}(A'') = \mathrm{FS}(A') - \sum B = \mathrm{FS}(A') + g = \mathrm{FS}(A)$ as desired. □

Let us recall the definition of FS-regular groups already given in the introduction.

Definition 3.4. An abelian group G is FS-regular if, for any $A, A' \in \mathcal{M}(G)$, $\mathrm{FS}(A) = \mathrm{FS}(A')$ if and only if $A \sim_0 A'$.

Notice that if G is FS-regular, then also its subgroups are FS-regular. Moreover, it is always true that $A \sim_0 A'$ implies $\mathrm{FS}(A) = \mathrm{FS}(A')$ (see Lemma 3.3-*(1)*) and therefore the content of the FS-regularity is the opposite implication, which does not hold for all groups.

As anticipated in the introduction, the main result of our work brings into play a subset O_{FS} of the natural numbers. We recall its definition and explore some basic properties of these numbers.

Definition 3.5. Let O_{FS} be the set of odd natural numbers $n \geqslant 1$ such that $(\mathbb{Z}/n\mathbb{Z})^*$ is covered by $\{\pm 2^j : j \geqslant 0\}$; more precisely, for each $x \in \mathbb{Z}$ relatively prime with n there exists $j \geqslant 0$ such that either $x - 2^j$ or $x + 2^j$ is divisible by n.

The sequence of the elements of O_{FS} greater than 1 is given by OEIS A333854, while the complement (in the odd integers greater than 1) is A333855.

Proposition 3.6. *Let n be an element of O_{FS}. Then, all the positive divisors of n are in O_{FS} as well.*

Proof. Take a positive divisor d of n. Let $x \in \mathbb{Z}$ be relatively prime with d. There exists $m \in \mathbb{Z}$ so that $x + md$ is relatively prime with n. Since $n \in O_{\mathrm{FS}}$, there exists $j \in \mathbb{N}$ such that either $x + md - 2^j$ or $x + md + 2^j$ is a multiple of n, and thus a multiple of d as well. Therefore either $x - 2^j$ or $x + 2^j$ is a multiple of d. □

In the following, we denote by $\mathrm{ord}_n(x)$ the multiplicative order of x in $\mathbb{Z}/n\mathbb{Z}$, and by φ Euler's totient function.

Proposition 3.7. *An odd positive integer n is a member of O_{FS} if and only if one of the following holds:*

(i) $\mathrm{ord}_n(2) = \varphi(n)$*;*

(ii) $\mathrm{ord}_n(2) = \varphi(n)/2$ *and either* $4 \nmid \varphi(n)$ *or* $2^{\varphi(n)/4} \not\equiv -1 \pmod{n}$.

Proof. Notice that, in $\mathbb{Z}/n\mathbb{Z}$, it holds

$$|\{\pm 2^j : j \geqslant 0\}| \leqslant 2|\{2^j : j \geqslant 0\}| = 2\,\mathrm{ord}_n(2). \tag{3.2}$$

Thus, if $n \in O_{\mathrm{FS}}$ then necessarily $\mathrm{ord}_n(2) \geqslant \varphi(n)/2$.

If $\mathrm{ord}_n(2) = \varphi(n)$, then $\{\pm 2^j : j \geqslant 0\} = \{2^j : j \geqslant 0\} = (\mathbb{Z}/n\mathbb{Z})^*$.

If $\mathrm{ord}_n(2) = \varphi(n)/2$, then in order to have equality in (3.2) it is necessary and sufficient that $2^j \not\equiv -2^{j'} \pmod{n}$ for all $j, j' \geqslant 0$, which is equivalent to $2^j \not\equiv -1 \pmod{n}$ for all $j \geqslant 0$. If $4 \nmid \varphi(n)$, the latter is impossible. Otherwise, the only $0 \leqslant j < \varphi(n)$ for which the congruence can be true is $\varphi(n)/4$, hence (ii) follows. □

Proposition 3.8. *If $n \in O_{\mathrm{FS}}$, then n is divided by at most two distinct primes.*

Proof. In view of Proposition 3.6 and working by contradiction, it is sufficient to show that $pqr \notin O_{\mathrm{FS}}$ whenever p, q, r are distinct odd primes.

Since $q-1$ and $r-1$ are even, $p-1$ divides $h := (p-1)(q-1)(r-1)/4$, and thus $2^h \equiv 1 \pmod p$. Likewise, $2^h \equiv 1$ modulo q and r. This implies that $2^h \equiv 1 \pmod{pqr}$, therefore $\mathrm{ord}_{pqr}(2) \mid h = \varphi(pqr)/4$. By Proposition 3.7, we deduce that $pqr \notin O_{\mathrm{FS}}$. □

One might wonder whether it is true that every $n \in O_{\mathrm{FS}}$ has at least one multiple in O_{FS}. This is false: a counterexample is $3p$ with $p = 3511$. It can be verified that $\mathrm{ord}_{3p}(2) = p-1$ and $2^{(p-1)/2} \not\equiv -1 \pmod{3p}$, and thus $3p \in O_{\mathrm{FS}}$ thanks to Proposition 3.7. Proposition 3.8 tells us that any multiple of $3p$ that belongs to O_{FS} must be of the form $3^a \cdot p^b$, so it is enough to check that $9p$ and p^2 are not in O_{FS}, which is true (since $\mathrm{ord}_{9p}(2) = p-1$ and $\mathrm{ord}_{p^2}(p) = (p-1)/2$). The number $p = 3511$ is a Wieferich prime (cf. [CDP97]), that is, a prime p such that p^2 divides $2^{p-1}-1$ (and, in fact, one of the only two known such primes). It is natural to use a Wieferich prime p in this construction because, even if $p \in O_{\mathrm{FS}}$, the fact that $\mathrm{ord}_{p^2}(2) \mid p-1$ guarantees that $p^2 \notin O_{\mathrm{FS}}$.

4. FS-regularity of cyclic groups

In this section we characterize the FS-regular finite cyclic groups; the two main results are Proposition 4.1 and Proposition 4.9.

To show that if $n \notin O_{\mathrm{FS}}$ then $\mathbb{Z}/n\mathbb{Z}$ is not FS-regular we produce an explicit counterexample.

Proposition 4.1. *For any $n \notin O_{\mathrm{FS}}$, the group $\mathbb{Z}/n\mathbb{Z}$ is not* FS*-regular.*

Proof. If n is even, then $\mathbb{Z}/2\mathbb{Z}$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$ and thus it is sufficient to show that $\mathbb{Z}/2\mathbb{Z}$ is not FS-regular. As a counterexample to FS-regularity in $\mathbb{Z}/2\mathbb{Z}$, it is enough to notice that

$$\mathrm{FS}(\{0,1\}) = \{0,0,1,1\} = \mathrm{FS}(\{1,1\}),$$

while $\{0,1\} \not\sim_0 \{1,1\}$ as multisets with values in $\mathbb{Z}/2\mathbb{Z}$.

Let us now consider the case of n odd. There exists $k \in (\mathbb{Z}/n\mathbb{Z})^* \setminus \{\pm 2^j \bmod n\}_{j\in\mathbb{N}}$ since $n \notin O_{\mathrm{FS}}$. Moreover, let $d := \varphi(n)$ be so that $n \mid 2^d - 1$. Consider the multisets $A, A' \in \mathcal{M}(\mathbb{Z}/n\mathbb{Z})$ defined as

$$A := \{2^0,\, 2^1,\, \dots,\, 2^{d-1}\} \quad \text{and} \quad A' := k \cdot A = \{2^0k,\, 2^1k,\, \dots,\, 2^{d-1}k\}.$$

The choice of k implies that $A \cap A' = (-A) \cap A' = \varnothing$ and, in particular, $A \not\sim_0 A'$.

We have that[5]

$$\begin{aligned}\mathrm{FS}(A) &= \{0, 1, 2, \ldots, 2^d - 1\} = \{0\} \cup \bigcup_{i=1}^{\frac{2^d-1}{n}} \{0, 1, \ldots, n-1\} \\ &= \{0\} \cup \bigcup_{i=1}^{\frac{2^d-1}{n}} k \cdot \{0, 1, \ldots, n-1\} = \{k \cdot 0, k \cdot 1, \ldots, k \cdot (2^d - 1)\} \\ &= \mathrm{FS}(A'). \end{aligned}$$ □

The proof that $\mathbb{Z}/n\mathbb{Z}$ is FS-regular when $n \in O_{\mathrm{FS}}$ is more involved. The rest of this section is devoted to establish this result by reducing it to a statement about the units of the cyclotomic field $\mathbb{Q}(\omega_n)$.

Before delving into the proof, let us present the relation between the problem at hand and the units of the cyclotomic field $\mathbb{Q}(\omega_n)$, to clarify the importance of Definitions 4.3 and 4.5. Let us remark that there is an alternative, but equivalent, perspective on the whole argument that instead of using polynomials computes the Fourier transform of $\mu_{\mathrm{FS}(A)}$ (see [Ter99, Part I] for an introduction to the Fourier transform on finite abelian groups).

Given two multisets $A, A' \in \mathcal{M}(\mathbb{Z}/n\mathbb{Z})$, the condition $\mathrm{FS}(A) = \mathrm{FS}(A')$ is equivalent to the polynomial identity

$$\prod_{a \in A}(1 + t^a) = \prod_{a' \in A'}(1 + t^{a'}) \pmod{t^n - 1},$$

which is equivalent to

$$\prod_{j=0}^{n-1}(1 + \omega_d^j)^{\mu_A(j) - \mu_{A'}(j)} = 1,$$

for all divisors $d \mid n$ (because a polynomial is divisible by $t^n - 1$ if and only if it has ω_d as root for all divisors $d \mid n$). Therefore, we are interested in the kernel of the map which takes a vector $x \in \mathbb{Z}^n$ and produces the tuple, indexed by the divisors $d \mid n$,

$$\left(\prod_{j=0}^{n-1}(1 + \omega_d^j)^{x_j}\right)_{d \mid n}. \tag{4.1}$$

Since this map is a homomorphism between abelian groups, studying its kernel is tightly linked to the study of its image. In fact, the crux of this section is the determination of the image of such map (see Lemma 4.7).

The multiplicative group generated by $1 + \omega_d^0, 1 + \omega_d^1, \ldots, 1 + \omega_d^{n-1}$ is introduced in Definition 4.3, while its rank is computed in Lemma 4.4 (the assumption $n \in O_{\mathrm{FS}}$ is necessary to compute the rank). Then, in Definition 4.5 we introduce the notation that allows studying the map mentioned in Equation (4.1) and we go on to prove its *moral* surjectivity (i.e., its image has full rank) in Lemma 4.7 (notice that we do not need $n \in O_{\mathrm{FS}}$, n being odd suffices). Finally, in Proposition 4.9, we join all the pieces to obtain the desired result.

[5] The unions are taken over $\frac{2^d-1}{n}$ copies of the same multiset and shall be interpreted in the multiset sense, so that the result is a multiset where each element appears $\frac{2^d-1}{n}$ times.

Remark 4.2. Let us mention a connection, observed in [Gai23], between the topic of this section and a conjecture of Livingston (see [Pat17, CD20]).

We are concerned with the multiplicative relations satisfied by the factors $1 + \omega_n^j$ for $j = 0, 1, \ldots, n-1$ (and simultaneously by $1 + \omega_d^j$ for $d \mid n$, but we omit this *important* detail in this remark). Since $1 + \omega_d^j = 2\omega_{2d}^j \cos(j\pi/n)$, such multiplicative relations can be shown to be equivalent to the linear relations satisfied by $\log(2\sin(j\pi/n))$. The existence of a nontrivial linear relation of this kind is exactly the content of the conjecture of Livingston mentioned above.

Given an odd positive integer n, recall that, for $1 \leqslant j < n$, $1 + \omega_n^j$ is a unit of $\mathbb{Q}(\omega_n)$ (see Section 2.3).

Definition 4.3. Given an odd positive integer $n \geqslant 1$, let K_n be the multiplicative subgroup of $\mathbb{C}$ generated by $\{1 + \omega_n^j : 0 \leqslant j < n\}$. Note that we include $1 + \omega_n^0 = 2$ among the generators.

Lemma 4.4. *If $n \geqslant 3$ and $n \in O_{\mathrm{FS}}$, it holds $\mathrm{rk}(K_n) = \frac{\varphi(n)}{2}$, where φ denotes Euler's totient function. Moreover, it holds $\mathrm{rk}(K_1) = 1$.*

Proof. For $n = 1$, $K_n = \langle 2 \rangle \cong \mathbb{Z}$, which has rank 1.

Let us now consider K_n for $n \geqslant 3$ and $n \in O_{\mathrm{FS}}$. Notice that all generators of K_n apart from the element 2 are units of $\mathbb{Q}(\omega_n)$, while the inverse of 2 is not an algebraic integer. Therefore, one obtains $K_n \cong \langle 2 \rangle \oplus \tilde{K}_n$, where $\tilde{K}_n := \langle 1 + \omega_n^j : 1 \leqslant j < n \rangle$.

It remains to compute the rank of $\tilde{K}_n$. We have already observed that $\tilde{K}_n$ is a subgroup of C_n (defined in the statement of Theorem 2.1). Using that $n \in O_{\mathrm{FS}}$ we are going to prove that C_n is a subgroup of $\tilde{K}_n \cup (-\tilde{K}_n)$.[6]

To show that $C_n \subseteq \tilde{K}_n \cup (-\tilde{K}_n)$, it is sufficient to show that all generators of C_n belong to $\tilde{K}_n$ or to $-\tilde{K}_n$. Let us fix $s \geqslant 1$ coprime with n. Since $n \in O_{\mathrm{FS}}$, there exists $j \geqslant 0$ such that $\omega_n^{2^j} = \omega_n^s$ or $\omega_n^{2^j} = \omega_n^{-s}$.

If $\omega_n^{2^j} = \omega_n^s$, then, for any $0 < r < n$, we have

$$\frac{1 - \omega_n^{rs}}{1 - \omega_n^r} = \frac{1 - \omega_n^{2^j r}}{1 - \omega_n^r} = \prod_{k=0}^{j-1} (1 + \omega_n^{2^k r}) \in \tilde{K}_n.$$

To handle the case $\omega_n^{2^j} = \omega_n^{-s}$, let us observe that $\omega_n = \frac{1+\omega_n}{1+\omega_n^{-1}} \in \tilde{K}_n$. Therefore, for any $0 < r < n$, we have

$$\frac{1 - \omega_n^{rs}}{1 - \omega_n^r} = -\omega_n^{rs} \frac{1 - \omega_n^{2^j r}}{1 - \omega_n^r} \in -\tilde{K}_n.$$

We have shown $\tilde{K}_n \subseteq C_n \subseteq \tilde{K}_n \cup (-\tilde{K}_n)$ and thus $\mathrm{rk}(\tilde{K}_n) = \mathrm{rk}(C_n) = \varphi(n)/2 - 1$ (recall Corollary 2.2). Hence we conclude $\mathrm{rk}(K_n) = \mathrm{rk}(\langle 2 \rangle \oplus \tilde{K}_n) = 1 + \mathrm{rk}(\tilde{K}_n) = \varphi(n)/2$. □

Definition 4.5. Given a positive integer $n \geqslant 1$, for $0 \leqslant j < n$, let e_j^n be the j-th canonical generator of $\mathbb{Z}^n = \bigoplus_{j=0}^{n-1} \mathbb{Z}$. The index j of e_j^n shall be interpreted modulo n, i.e., $e_j^n := e_{j \bmod n}^n$, when $j \geqslant n$.

[6]One may check that $-1 \notin \tilde{K}_7$, while $-1 \in C_7$. So it is not true in general that C_n and $\tilde{K}_n$ coincide. On the other hand, for some values of n (e.g., $n = 3, 5, 9$) one has $-1 \in \tilde{K}_n$.

For a positive divisor d of n, let $\pi^n_d : \mathbb{Z}^n \to \mathbb{Z}^d$ be the unique homomorphism such that $\pi^n_d(e^n_j) := e^d_j$ $(= e^d_{j \bmod d})$ for all $0 < j < n$.

Let $F_n : \mathbb{Z}^n \to K_n$ be the unique group homomorphism such that $F_n(e^n_j) = 1 + \omega^j_n$ for each $0 \leqslant j < n$; or equivalently

$$F_n(x) = F_n(x_0, \ldots, x_{n-1}) := \prod_{j=0}^{n-1} (1 + \omega^j_n)^{x_j}.$$

Lemma 4.6. *Let $\mathbb{F}$ be a field and let V be a $\mathbb{F}$-vector space. Given a subset $S \subseteq V$, we denote with $\langle S \rangle_{\mathbb{F}}$ the subspace generated by the elements of S.*

Given k vectors $v_1, v_2, \ldots, v_k \in V$, for any $\lambda \in \mathbb{F}$ which is not a root of unity (i.e., $\lambda^q \neq 1$ for all positive integers $q \geqslant 1$) and for any function $\sigma : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$, we have

$$\langle v_j - \lambda v_{\sigma(j)} : 1 \leqslant j \leqslant k \rangle_{\mathbb{F}} = \langle v_j : 1 \leqslant j \leqslant k \rangle_{\mathbb{F}}.$$

Proof. We prove the statement by induction on k. For $k = 0$ there is nothing to prove.

If σ is not surjective then we can assume without loss of generality that $\sigma(j) \neq k$ for all $1 \leqslant j \leqslant k$. Hence, we can apply the inductive hypothesis and obtain

$$\langle v_j - \lambda v_{\sigma(j)} : 1 \leqslant j \leqslant k-1 \rangle_{\mathbb{F}} = \langle v_j : 1 \leqslant j \leqslant k-1 \rangle_{\mathbb{F}}.$$

Since $v_{\sigma(k)} \in \langle v_j : 1 \leqslant j \leqslant k-1 \rangle_{\mathbb{F}}$, we obtain

$$\langle v_j - \lambda v_{\sigma(j)} : 1 \leqslant j \leqslant k \rangle_{\mathbb{F}} = \langle v_1, v_2, \ldots, v_{k-1}, v_k - \lambda v_{\sigma(n)} \rangle_{\mathbb{F}} = \langle v_j : 1 \leqslant j \leqslant k \rangle_{\mathbb{F}},$$

which is what we sought.

If σ is surjective, then it must be a permutation. In particular there exists $q \geqslant 1$ such that $\sigma^q(j) = j$ for all $1 \leqslant j \leqslant k$. Thus, for any $1 \leqslant \ell \leqslant k$, we have the telescopic sum

$$\sum_{i=0}^{q-1} \lambda^i \big(v_{\sigma^i(\ell)} - \lambda v_{\sigma(\sigma^i(\ell))} \big) = (1 - \lambda^q) v_\ell.$$

Since $1 - \lambda^q \neq 0$ by assumption, we deduce that

$$v_\ell \in \langle v_j - \lambda v_{\sigma(j)} : 1 \leqslant j \leqslant k \rangle_{\mathbb{F}}$$

for all $1 \leqslant \ell \leqslant k$, which implies the statement. □

The following lemma is the core of the whole argument. It tells us that the map $(F_d \circ \pi^n_d)_{d|n}$ is *morally* surjective. Or equivalently, that we can independently prescribe the values of its entries and we will be able to find a vector x such that $(F_d(\pi^n_d(x)))_{d|n}$ corresponds to the values we have prescribed (up to multiplying everything by a factor).

Lemma 4.7. *For any odd positive integer n, the image of the map $(F_d \circ \pi^n_d)_{d|n} : \mathbb{Z}^n \to \oplus_{d|n} K_d$ is a finite-index subgroup of $\oplus_{d|n} K_d$.*

Proof. Let us fix a divisor d of n. We are going to identify some elements of the kernel of F_d, which is equivalent to producing nontrivial relations in K_d. For any divisor p of d and any $0 \leqslant j < d/p$, let

$$v^d_{p,j} \coloneqq e^d_{jp} - \sum_{k=0}^{p-1} e^d_{j+kd/p}.$$

Thanks to Proposition 2.3, we know that $F_d(v^d_{p,j}) = 1$ for all prime divisors p of d and all $0 < j < d/p$. Therefore, we have identified the subspace

$$\mathbb{Z}^d \supseteq D_d \coloneqq \langle v^d_{p,j} \rangle_{p|d \text{ prime},\, 0 \leqslant j < d/p}$$

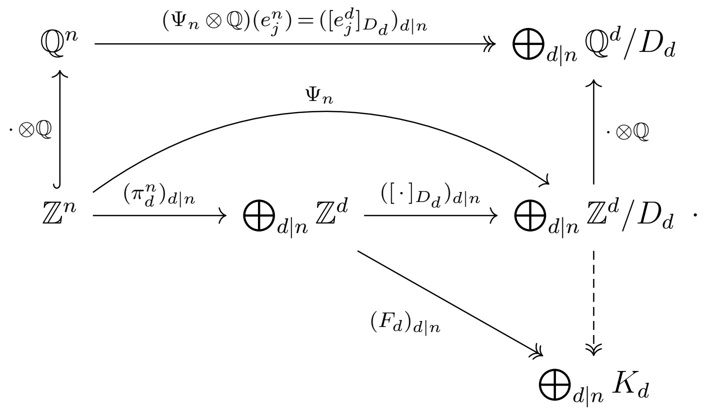
of the kernel of F_d. Let us identify with $[\,\cdot\,]_{D_d} : \mathbb{Z}^d \to \mathbb{Z}^d/D_d$ the projection to the quotient.

We claim that $\Psi_n \coloneqq ([\pi^n_d]_{D_d})_{d|n} : \mathbb{Z}^n \to \bigoplus_{d|n} \mathbb{Z}^d/D_d$ has full rank (i.e., the rank of its image coincides with the rank of its codomain). This claim implies the desired result since F_d is surjective for all d.

In order to show that Ψ_n has full rank we consider its tensorization with $\mathbb{Q}$ and show that it is surjective as a linear map between $\mathbb{Q}$-vector spaces. With a mild abuse of notation, we keep denoting with $(e^d_j)_{0 \leqslant j < d}$ the canonical basis of $\mathbb{Q}^d$ and we keep denoting with D_d the $\mathbb{Q}$-subspace generated by $\{v^d_{p,j}\}_{p|d \text{ prime},\, 0 \leqslant j \leqslant d/p}$.

Thanks to the basic properties of the tensor product, we have $(\mathbb{Z}^d/D_d) \otimes \mathbb{Q} = \mathbb{Q}^d/D_d$ and the tensorization $\Psi_n \otimes \mathbb{Q} : \mathbb{Q}^n \to \bigoplus_{d|n} \mathbb{Q}^d/D_d$ satisfies $(\Psi_n \otimes \mathbb{Q})(e^n_j) = ([e^d_j]_{D_d})_{d|n} \in \bigoplus_{d|n} \mathbb{Q}^d/D_d$ for all $0 \leqslant j < n$.

The following commutative diagram shall clarify all the steps of the proof up to now.



To prove the surjectivity of the linear map $\Psi_n \otimes \mathbb{Q} : \mathbb{Q}^n \to \bigoplus_{d|n} \mathbb{Q}^d/D_d$ we show explicitly that the canonical generators of the codomain belong to the image of the map.

Given a subset $S \subseteq \{d \geqslant 1 : d \mid n\}$ and an index $0 \leqslant j < n$, let $u_{S,j} = (u^d_{S,j})_{d|n} \in \bigoplus_{d|n} \mathbb{Q}^d/D_d$ be the element defined by

$$\mathbb{Q}^d/D_d \ni u^d_{S,j} \coloneqq \begin{cases} 0 & \text{if } d \notin S, \\ [e^d_j]_{D_d} & \text{if } d \in S. \end{cases}$$

The index j of $u_{S,j}$ should be interpreted modulo n (e.g. $u_{S,n} = u_{S,0}$).

Notice that $(u_{\{d\},j})_{d|n,\,0\leqslant j<n}$ is a set of generators of $\bigoplus_{d|n}\mathbb{Q}^d/D_d$. Moreover, it holds $(\Psi_n\otimes\mathbb{Q})(e^n_j)=u_{\{d\geqslant 1:\, d|n\},\,j}$.

We say that a set S is *solvable* if $u_{S,j}$ belongs to the image of $\Psi_n\otimes\mathbb{Q}$ for all $0\leqslant j<n$. Thanks to the previous observations, we know that $\{d\geqslant 1 : d\mid n\}$ is solvable and that the surjectivity of $\Psi_n\otimes\mathbb{Q}$ is equivalent to the fact that all singletons $\{d\}$ are solvable. Notice that if $S\subseteq T\subseteq\{d\geqslant 1 : d\mid n\}$ is solvable, then also $T\backslash S$ is solvable. Indeed, if $(\Psi_n\otimes\mathbb{Q})(x)=u_{S,j}$ and $(\Psi_n\otimes\mathbb{Q})(y)=u_{T,j}$, then $(\Psi_n\otimes\mathbb{Q})(y-x)=u_{T\backslash S,\,j}$. Our main tool to show the solvability of a set is the following sub-lemma.

Lemma 4.8. *Let $S\subseteq\{d\geqslant 1 : d\mid n\}$ be a solvable subset and let $p\mid n$ be a prime number. Let us define*[7] $\upsilon_p(S)\coloneqq\max_{d\in S}\upsilon_p(d)$ *as the maximal p-adic valuation of an element of S. Then, the subset $\{d\in S : \upsilon_p(d)=\upsilon_p(S)\}$ is also solvable.*

Proof. Let $S'\coloneqq\{d\in S : \upsilon_p(d)=\upsilon_p(S)\}$. Let m be the minimum common multiple of the elements of S. Notice that $\upsilon_p(m)=\upsilon_p(S)$.

If $\upsilon_p(S)=0$, then $S'=S$ and the statement is obvious. From now on we assume that $\upsilon_p(S)>0$.

We claim that, for any $0\leqslant j<n$, it holds

$$u_{S,j}-\frac{1}{p}\sum_{k=0}^{p-1}u_{S,j+km/p}=u_{S',j}-\frac{1}{p}u_{S',jp}. \tag{4.2}$$

We prove Equation (4.2) by looking at the projections of both sides onto $\mathbb{Q}^d/D_d$ and considering various cases depending on the divisor d.

- If $d\notin S$, then $d\notin S'$ (since $S'\subseteq S$) and thus we have

$$u^d_{S,j}-\frac{1}{p}\sum_{k=0}^{p-1}u^d_{S,j+km/p}=0=u^d_{S',j}-\frac{1}{p}u^d_{S',jp}.$$

- If $d\in S$ and $\upsilon_p(d)<\upsilon_p(S)$, then $d\mid\frac{m}{p}$ and therefore $u^d_{S,j+km/p}=[e^d_{j+km/p}]_{D_d}=[e^d_j]_{D_d}=u^d_{S,j}$. Since $\upsilon_p(d)<\upsilon_p(S)$ implies that $d\notin S'$, we deduce

$$u^d_{S,j}-\frac{1}{p}\sum_{k=0}^{p-1}u^d_{S,j+km/p}=u^d_{S,j}-\frac{1}{p}\sum_{k=0}^{p-1}u^d_{S,j}=0=u^d_{S',j}-\frac{1}{p}u^d_{S',jp}.$$

- If $d\in S$ and $\upsilon_p(d)=\upsilon_p(S)$, then it holds

$$\left\{0,\ \frac{m}{p}\bmod d,\ 2\frac{m}{p}\bmod d,\ldots,\ (p-1)\frac{m}{p}\bmod d\right\}=\left\{0,\ \frac{d}{p},\ 2\frac{d}{p},\ldots,\ (p-1)\frac{d}{p}\right\}. \tag{4.3}$$

[7] Here $\upsilon_p(x)$ denotes the p-adic valuation of a nonzero integer x, i.e., the maximum exponent $h\geqslant 0$ such that p^h divides x.

To prove the latter identity, notice that for any $0 \leqslant k < p$, we have

$$\left(k\frac{m}{p} \bmod d\right) = \left(k\frac{m}{d} \bmod p\right)\frac{d}{p}$$

and therefore the identity between sets follows from the fact that m/d is not divisible by p. Exploiting Equation (4.3) and recalling that $v^d_{p,j} \in D_d$, we obtain

$$\begin{aligned} u^d_{S,j} - \frac{1}{p}\sum_{k=0}^{p-1} u^d_{S,\,j+km/p} &= \Big[e^d_j - \frac{1}{p}\sum_{k=0}^{p-1} e^d_{j+km/p}\Big]_{D_d} = \Big[e^d_j - \frac{1}{p}\sum_{k=0}^{p-1} e^d_{j+kd/p}\Big]_{D_d} \\ &= \Big[e^d_j - \frac{1}{p}(e^d_{jp} - v^d_{p,j})\Big]_{D_d} = \Big[e^d_j - \frac{1}{p}e^d_{jp}\Big]_{D_d} \\ &= u^d_{S',j} - \frac{1}{p}u^d_{S',jp}, \end{aligned}$$

where in the last steps we used that $d \in S'$ (which is equivalent to the assumptions $d \in S$ and $v_p(d) = v_p(S)$).

Since we have covered all possible cases, Equation (4.2) is proven.

The set S is solvable, therefore the left-hand side of Equation (4.2) belongs to the image of $\Psi_n \otimes \mathbb{Q}$, and thus also $u_{S',j} - \frac{1}{p}u_{S',jp}$ belongs to $\operatorname{Im}(\Psi_n \otimes \mathbb{Q})$ for all $0 \leqslant j < n$. Lemma 4.6, applied with $v_j := u_{S',j}$, $\lambda := 1/p$, and $\sigma(j) := (jp \bmod n)$, guarantees that also $u_{S',j}$ belongs to the image of $\Psi_n \otimes \mathbb{Q}$ for all $0 \leqslant j < n$, which proves that S' is solvable as desired. □

As a simple consequence of Lemma 4.8, we claim that if S is solvable, then, for any prime divisor p of n and for any $0 \leqslant h \leqslant v_p(n)$, we have that $\{s \in S : v_p(s) = h\}$ is also solvable. Let us prove it by induction on h, starting from $h = v_p(n)$ and going backward to $h = 0$.

If $\{s \in S : v_p(s) = v_p(n)\}$ is empty, then it is solvable; otherwise we can apply Lemma 4.8 and obtain again that it is solvable. Now, we assume that $\{s \in S : v_p(s) = h'\}$ is solvable for $h' > h$. Then, since the difference of solvable sets is solvable, we deduce that $\tilde{S} := \{s \in S : v_p(s) \leqslant h\}$ is solvable. If $\{s \in S : v_p(s) = h\}$ is empty, then it is solvable; otherwise we can apply Lemma 4.8 on the set $\tilde{S}$ and obtain again that $\{s \in S : v_p(s) = h\}$ is solvable as desired.

We can now conclude by showing that singletons $\{d\}$ are solvable for each $d \mid n$. This follows directly from the fact that $\{d \geqslant 1 : d \mid n\}$ is solvable and that if S is solvable then $\{s \in S : v_p(s) = h\}$ is solvable for all prime divisors $p \mid n$ and all $h \geqslant 0$. □

Proposition 4.9. *For any $n \in O_{\mathrm{FS}}$, the group $\mathbb{Z}/n\mathbb{Z}$ is* FS*-regular.*

Proof. Let $A, A' \in \mathcal{M}(\mathbb{Z}/n\mathbb{Z})$ be two multisets such that $\mathrm{FS}(A) = \mathrm{FS}(A')$; we shall prove that $A \sim_0 A'$.

By definition of the map FS, it holds the polynomial identity in $\mathbb{Z}[t]/(t^n - 1)$

$$\sum_{j=0}^{n-1} \mu_{\mathrm{FS}(A)}(j)t^j \equiv \sum_{s\in \mathrm{FS}(A)} t^s \equiv \prod_{a\in A}(1+t^a) \equiv \prod_{j=0}^{n-1}(1+t^j)^{\mu_A(j)} \pmod{t^n - 1},$$

Thus the condition $\mathrm{FS}(A) = \mathrm{FS}(A')$ is equivalent to

$$\prod_{j=0}^{n-1}(1+t^j)^{\mu_A(j)} \equiv \prod_{j=0}^{n-1}(1+t^j)^{\mu_{A'}(j)} \pmod{t^n - 1}.$$

For any divisor $d \mid n$, ω_d is a root of $t^n - 1$ and therefore the latter identity implies

$$\prod_{j=0}^{n-1}(1+\omega_d^j)^{\mu_A(j)} = \prod_{j=0}^{n-1}(1+\omega_d^j)^{\mu_{A'}(j)}$$

which, recalling Definition 4.5, is equivalent to

$$F_d\Big(\pi_d^n\big((\mu_A(j) - \mu_{A'}(j))_{0\leqslant j<n}\big)\Big) = 1.$$

We have just shown that the vector $(\mu_A(j) - \mu_{A'}(j))_{0\leqslant j<n} \in \mathbb{Z}^n$ belongs to the kernel of the map $(F_d \circ \pi_d^n)_{d|n} : \mathbb{Z}^n \to \oplus_{d|n} K_d$. Let us now switch our attention to the study of such kernel.

$$\begin{array}{ccccccc}
\mathcal{M}(\mathbb{Z}/n\mathbb{Z}) & \xhookrightarrow{A\mapsto(\mu_A(j))_{0\leqslant j<n}} & & \mathbb{Z}^n & \xrightarrow{(F_d\circ\pi_{n,d})_{d|n}} & \oplus_{d|n}K_d \\
\Big\downarrow \scriptstyle\mathrm{FS} & & & \Big\downarrow \scriptstyle x\mapsto\prod_{j=0}^{n-1}(1+t^j)^{x_j} & & \Big\downarrow \\
\mathcal{M}(\mathbb{Z}/n\mathbb{Z}) & \hookrightarrow \mathbb{Z}^n & \xrightarrow[x\mapsto\sum_{j=0}^{n-1}x_jt^j]{\cong} & \frac{\mathbb{Z}[t]}{(t^n-1)} & \xrightarrow[[q]\mapsto(q(\omega_d))_{d|n}]{\cong} & \oplus_{d|n}\mathbb{Z}[\omega_d]
\end{array} .$$

Figure 4.1: A commutative diagram depicting the relation, explained at the beginning of the proof of Proposition 4.9, between the map FS and the map $(F_d \circ \pi_d^n)_{d|n}$.

Due to basic properties of the rank (see Section 2.2), we have

$$\begin{aligned}
\mathrm{rk}\left(\ker((F_d\circ\pi_d^n)_{d|n})\right) &= n - \mathrm{rk}\left(\mathrm{Im}\left((F_d\circ\pi_d^n)_{d|n}\right)\right) = n - \mathrm{rk}\Big(\bigoplus_{d|n}K_d\Big) \\
&= n - \sum_{d|n}\mathrm{rk}(K_d) = n - 1 - \sum_{1<d|n}\frac{\varphi(d)}{2} = \frac{n-1}{2},
\end{aligned}$$

where we have used Lemma 4.7 and Lemma 4.4.

Let us now exhibit a subgroup L_n of $\mathbb{Z}^n$ which is included in the kernel of $(F_d \circ \pi_d^n)_{d|n}$ (in hindsight, it coincides with such kernel). Let $L_n \subseteq \mathbb{Z}^n$ be the subgroup[8]

$$L_n := \left\{ x \in \mathbb{Z}^n : \begin{array}{l} x_0 = 0, \\ x_j + x_{n-j} = 0 \text{ for all } 1 \leqslant j \leqslant \dfrac{n-1}{2}, \\ \displaystyle\sum_{j=1}^{\frac{n-1}{2}} j\cdot x_j \text{ is divisible by } n \end{array} \right\}.$$

[8]Notice that L_n is the subgroup generated by the vectors $(\mu_B(j)-\mu_{B'}(j))_{0\leqslant j<n}$ for any two multisets $B \sim_0 B'$.

For any $d \mid n$ and $x \in L_n$, we have

$$F_d(\pi_d^n(x)) = \prod_{j=0}^{n-1}(1+\omega_d^j)^{x_j} = \prod_{j=1}^{(n-1)/2}(1+\omega_d^j)^{x_j}(1+\omega_d^{-j})^{-x_j} \prod_{j=1}^{(n-1)/2}\omega_d^{j\cdot x_j}$$
$$= \omega_d^{\sum_{j=1}^{(n-1)/2} j\cdot x_j} = 1,$$

and this proves that L_n is a subgroup of the kernel of $(F_d \circ \pi_d^n)_{d|n}$.

Notice that $\mathrm{rk}(L_n) = \frac{n-1}{2} = \mathrm{rk}\left(\ker((F_d\circ\pi_d^n)_{d|n})\right)$, so for any $x \in \ker((F_d\circ\pi_d^n)_{d|n})$ there exists $\alpha \geqslant 1$ such that $\alpha x \in L_n$ and therefore x itself must satisfy the first two conditions in the definition of L_n, that is

$$\ker((F_d\circ\pi_d^n)_{d|n}) \subseteq \left\{x \in \mathbb{Z}^n : x_0 = 0,\ x_j + x_{n-j} = 0 \text{ for all } 1 \leqslant j \leqslant \frac{n-1}{2}\right\}.$$

The latter inclusion, together with the vector $(\mu_A(j) - \mu_{A'}(j))_{0\leqslant j<n} \in \mathbb{Z}^n$ belonging to the kernel we are studying, implies

$$\mu_A(0) = \mu_{A'}(0) \ \text{ and } \ \mu_A(j) + \mu_A(n-j) = \mu_{A'}(j) + \mu_{A'}(n-j) \text{ for all } 1 \leqslant j \leqslant n,$$

that is equivalent to $A \sim A'$. Finally, we conclude $A \sim_0 A'$ taking advantage of Lemma 3.3-*(3)*. □

5. Radon transform for finite abelian groups

In this section we will introduce a Radon transform for finite abelian groups and we will show an inversion formula for it. Then we will apply this tool to upgrade Proposition 4.9 to the same statement with $\mathbb{Z}/n\mathbb{Z}$ replaced by $(\mathbb{Z}/n\mathbb{Z})^d$ for an arbitrary $d \geqslant 1$.

Let us introduce the discrete Radon transform.

Definition 5.1. Let $n, d \geqslant 1$ be positive integers. Given a function $f : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{C}$, its Radon transform Rf is the function $Rf = R_{n,d}f : \mathrm{Hom}((\mathbb{Z}/n\mathbb{Z})^d, \mathbb{Z}/n\mathbb{Z}) \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ given by

$$Rf(\psi, c) := \sum_{\substack{x\in(\mathbb{Z}/n\mathbb{Z})^d \\ \psi(x)=c}} f(x),$$

for all homomorphisms $\psi : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{Z}/n\mathbb{Z}$ and all $c \in \mathbb{Z}/n\mathbb{Z}$.

We named this transformation Radon transform in analogy with the continuous Radon transform on $\mathbb{R}^n$ [Hel99] which, given a function $f : \mathbb{R}^d \to \mathbb{R}$, produces another function Rf which takes an $(n-1)$-affine hyperplane and returns the integral of f over such hyperplane. Notice that affine hyperplanes are exactly the fibers of linear functionals $\mathbb{R}^n \to \mathbb{R}$ and thus the continuous Radon transform on $\mathbb{R}^d$ coincides (up to adapting the definition to a non-discrete setting) with our definition if $\mathbb{Z}/n\mathbb{Z}$ is replaced by $\mathbb{R}$.

One may wonder if Definition 5.1 would work even if $\mathbb{Z}/n\mathbb{Z}$ was replaced everywhere by an arbitrary finite abelian group G. Although everything would still hold, it is not appropriate to give such a definition. Indeed, any finite abelian group G is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^k$ for $n, k \geqslant 1$ (where n is the largest order of an element in G). Hence the Radon transform on G^d shall be defined as the restriction of $R_{n,kd}$ to $\mathrm{Hom}(G^d, \mathbb{Z}/n\mathbb{Z}) \times \mathbb{Z}/n\mathbb{Z}$; that is, by understanding G^d as a subgroup of $(\mathbb{Z}/n\mathbb{Z})^{kd}$ and using the Radon transform of the latter (which uses homomorphisms with codomain equal to $\mathbb{Z}/n\mathbb{Z}$ instead of G; notice that $\mathbb{Z}/n\mathbb{Z}$ is a subgroup of G).

In the literature, one can find many definitions of discrete Radon transform:

- The definition given in [DG85] (and investigated in [FG87, Fil89, Vel97, DV04]), which boils down to the convolution with the characteristic function of a fixed set, is completely unrelated to ours.

- The very general definition given in [Bol87] coincides with ours for the group $(\mathbb{Z}/p\mathbb{Z})^d$ (p being prime) and in that work it is named $(d-1)$-*planes transform*. The assumptions of the criterion [Bol87, Theorem 1] to establish the existence of an inversion formula of a Radon transform do not hold for our Radon transform (for example for the group $(\mathbb{Z}/4\mathbb{Z})^2$). Let us remark that the $(d-1)$-planes transform defined for $\mathbb{F}_{p^k}$ does not coincide with our Radon transform on $(\mathbb{Z}/p^k\mathbb{Z})^d$ when $k > 1$ (in particular, proving the invertibility of the $(d-1)$-planes transform seems to be considerably easier due to the larger number of symmetries).

- The recent work [CHM18] defines a Radon transform which is almost equivalent to our discrete Radon transform on $(\mathbb{Z}/p\mathbb{Z})^d$, where p is a prime number. In that paper the Radon transform (which they call *classical Radon transform* to distinguish it from the one of Diaconis and Graham) coincides with the restriction of ours to the homomorphisms $\psi \in \mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})^d, \mathbb{Z}/p\mathbb{Z})$ such that $\psi(0, 0, \dots, 0, 1) \neq 0$. Due to this restriction, they cannot establish a full inversion formula [CHM18, Theorem 1].

- In the work [AI08], the authors define a discrete Radon transform on $\mathbb{Z}^d$ which is equivalent to the Radon transform on $\mathbb{Z}^d$ with our notation (if one allows the group to be non-finite in the definition). An inversion formula [AI08, Theorem 4.1] is proven for such discrete Radon transform. Joining the methods of [AI08] with ours, it might be possible to produce inversion formulas for the discrete Radon transform on groups $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z})^d$ that are neither finite nor torsion-free. We do not investigate this as it goes beyond the scope of the paper.

- An alternative definition of discrete Radon transform for finite abelian groups is provided in [Ilm14]. The *maximal Radon transform* defined in this reference [Ilm14, Section 7.3] computes the sum of the function f over all translations of maximal cyclic subgroups of G.

  It is not hard to check that, for p prime, the *maximal Radon transform* on $(\mathbb{Z}/p\mathbb{Z})^2$ coincides with ours. In this special case, the author proves the invertibility of the Radon transform [Ilm14, Lemma 3.4]. In general his definition does not coincide with ours and, in particular, the *maximal Radon transform* is not invertible in many important cases [Ilm14, Propositions 7.2, 7.3].

The invertibility of the discrete Radon transform we have defined follows directly from the invertibility of the Fourier transform on finite abelian groups (see [Ter99, Part I] for an introduction to the Fourier transform on finite abelian groups) (cf. [Hel99, Theorem 3.1], [Str82]). The inversion formula one obtains in this way uses all the values of the Radon transform to recover $f(0)$.

The inversion formula we prove is *stronger*, indeed $f(x)$ can be recovered using only the values of the Radon transform on the *hyperplanes containing* x, that is from the values of $Rf(\psi, \psi(x))$ for all $\psi \in \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}^d, \mathbb{Z}/n\mathbb{Z})$. Notice that, since the Radon transform is not surjective onto its codomain, it is not strange that it admits different inversion formulas.

To avoid lengthy formulas, we are going to use the notation $\mathrm{Hom}_n^d := \mathrm{Hom}((\mathbb{Z}/n\mathbb{Z})^d, \mathbb{Z}/n\mathbb{Z})$.

Definition 5.2. A function $\lambda : \mathrm{Hom}_n^d \to \mathbb{C}$ is an *inverting function* for the Radon transform on $(\mathbb{Z}/n\mathbb{Z})^d$ if

$$f(0) = \sum_{\psi \in \mathrm{Hom}_n^d} \lambda(\psi) Rf(\psi, 0). \tag{5.1}$$

for all functions $f : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{C}$.

Let us remark that if λ is an inverting function for the Radon transform on $(\mathbb{Z}/n\mathbb{Z})^d$ then, for all $x \in (\mathbb{Z}/n\mathbb{Z})^d$,

$$f(x) = \sum_{\psi \in \mathrm{Hom}_n^d} \lambda(\psi) Rf(\psi, \psi(x)).$$

This identity follows from Equation (5.1) applied to the function $\tilde{f} := f(\,\cdot\, + x)$.

Thanks to the observation above, the inversion formula stated in Theorem 1.6 is equivalent to the fact that the function $\lambda_{n,d} : \mathrm{Hom}_{n,d} \to \mathbb{Q}$, defined by

$$\lambda_{n,d}(\psi) := \frac{1}{n^{d-1}\varphi(n)} \prod_{p \mid \psi} (1 - p^{d-1}), \tag{5.2}$$

is an inverting function for the Radon transform on $(\mathbb{Z}/n\mathbb{Z})^d$.

Let us begin with two simple technical lemmas that will be useful in the proof of the inversion formula.

Lemma 5.3. *Let $n, d \geqslant 1$ be positive integers. A function $\lambda : \mathrm{Hom}_n^d \to \mathbb{C}$ is an inverting function for the Radon transform on $(\mathbb{Z}/n\mathbb{Z})^d$ if and only if it satisfies, for all $x \in (\mathbb{Z}/n\mathbb{Z})^d$,*

$$\sum_{\substack{\psi \in \mathrm{Hom}_n^d \\ \psi(x)=0}} \lambda(\psi) = \begin{cases} 1 & \text{if } x = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For any $f : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{C}$ and any $\lambda : \mathrm{Hom}_n^d \to \mathbb{C}$, it holds

$$\begin{aligned} \sum_{\psi \in \mathrm{Hom}_n^d} \lambda(\psi) Rf(\psi, 0) &= \sum_{\psi \in \mathrm{Hom}_n^d} \lambda(\psi) \sum_{\substack{x \in (\mathbb{Z}/n\mathbb{Z})^d \\ \psi(x)=0}} f(x) \\ &= \sum_{x \in (\mathbb{Z}/n\mathbb{Z})^d} f(x) \sum_{\substack{\psi \in \mathrm{Hom}_n^d \\ \psi(x)=0}} \lambda(\psi). \end{aligned}$$

Thanks to this identity, the desired statement follows because f can be chosen arbitrarily. □

In the next lemma we show that inverting functions behave nicely with respect to products.

Lemma 5.4. *Let $m, n, d \geqslant 1$ be positive integers such that m and n are coprime. Let $\lambda_m : \mathrm{Hom}_m^d \to \mathbb{C}$ and $\lambda_n : \mathrm{Hom}_n^d \to \mathbb{C}$ be inverting functions for the Radon transform on $(\mathbb{Z}/m\mathbb{Z})^d$ and $(\mathbb{Z}/n\mathbb{Z})^d$ respectively.*

Let $\pi_m : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ and $\pi_m^d : (\mathbb{Z}/mn\mathbb{Z})^d \to (\mathbb{Z}/m\mathbb{Z})^d$ be the canonical projections. Define π_n and π_n^d analogously. Let $\iota_m : \mathrm{Hom}_{mn}^d \to \mathrm{Hom}_m^d$ be the map such that, for all $\psi \in \mathrm{Hom}_{mn}^d$, it holds $\iota_m(\psi) \circ \pi_m^d = \pi_m \circ \psi$. Define ι_n analogously.

The function $\lambda_{mn} : \mathrm{Hom}_{mn}^d \to \mathbb{C}$ defined as

$$\lambda_{mn}(\psi) \coloneqq \lambda_m(\iota_m(\psi))\lambda_n(\iota_n(\psi))$$

is an inverting function for the Radon transform on $(\mathbb{Z}/mn\mathbb{Z})^d$.

Proof. The map $(\iota_m, \iota_n) : \mathrm{Hom}_{mn}^d \to \mathrm{Hom}_m^d \times \mathrm{Hom}_n^d$ is an isomorphism (induced by the isomorphism $(\pi_m, \pi_n) : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$). Moreover, given $\psi \in \mathrm{Hom}_{mn}^d$ and $x \in (\mathbb{Z}/mn\mathbb{Z})^d$, the condition $\psi(x) = 0$ is equivalent to $\iota_m(\psi)(\pi_m^d(x)) = 0$ and $\iota_n(\psi)(\pi_n^d(x)) = 0$.

Thus, for all $x \in (\mathbb{Z}/mn\mathbb{Z})^d$, we have

$$\begin{aligned}
\sum_{\substack{\psi \in \mathrm{Hom}_{mn}^d \\ \psi(x)=0}} \lambda_{mn}(\psi) &= \sum_{\substack{\psi \in \mathrm{Hom}_{mn}^d \\ \iota_m(\psi)(\pi_m^d(x))=0 \\ \iota_n(\psi)(\pi_n^d(x))=0}} \lambda_m(\iota_m(\psi))\lambda_n(\iota_n(\psi)) \\
&= \Bigg(\sum_{\substack{\psi \in \mathrm{Hom}_m^d \\ \psi(\pi_m^d(x))=0}} \lambda_m(\psi) \Bigg) \Bigg(\sum_{\substack{\psi \in \mathrm{Hom}_n^d \\ \psi(\pi_n^d(x))=0}} \lambda_n(\psi) \Bigg) \\
&= \begin{cases} 1 & \text{if } \pi_m^d(x) = 0 \text{ and } \pi_n^d(x) = 0, \\ 0 & \text{otherwise,} \end{cases}
\end{aligned}$$

where in the last step we used that λ_m and λ_n are inverting functions and we have applied Lemma 5.3. Since $x = 0$ if and only if $\pi_m^d(x) = 0$ and $\pi_n^d(x) = 0$, the identity above implies that λ_{mn} is an inverting function for the Radon transform on $(\mathbb{Z}/mn\mathbb{Z})^d$ thanks to Lemma 5.3. □

We are ready to prove that $\lambda_{n,d}$ (see Equation (5.2)) is an inverting function for the Radon transform on $(\mathbb{Z}/n\mathbb{Z})^d$.

Proof of Theorem 1.6. We have already observed that if we can prove the inversion formula for $x = 0$, then the general case follows. Hence, our goal is to prove the inversion formula for $f(0)$.

For any $m, n \geqslant 1$ coprime, it holds $\lambda_{mn,d}(\psi) = \lambda_{m,d}(\iota_m(\psi))\lambda_{n,d}(\iota_n(\psi))$ (see Lemma 5.4 for the definition of ι_m, ι_n). This identity follows from the fact that Euler's totient function satisfies $\varphi(m)\varphi(n) = \varphi(mn)$ and, for a prime $p \mid m$, the condition $p \mid \psi$ is equivalent to the condition

$p \mid \iota_m(\psi)$. Therefore, thanks to Lemma 5.4, since any number n can be factored into a product of prime powers, if we are able to prove that $\lambda_{n,d}$ is an inverting function when n is a prime power then the full result follows.

It remains to prove that $\lambda_{n,d}$ is an inverting function for $n = p^k$ prime power. In order to do that we start from a *bad* but simple inversion formula and we exploit the symmetries of the Radon transform to upgrade it to the desired inversion formula.

Notice that any character of $(\mathbb{Z}/n\mathbb{Z})^d$ can be represented uniquely as $(\mathbb{Z}/n\mathbb{Z})^d \ni x \mapsto \omega_n^{\psi(x)} \in \mathbb{C}$, with $\psi \in \mathrm{Hom}_n^d$. Hence, by using this bijection between the characters and the homomorphisms, the inversion formula for the Fourier transform on $(\mathbb{Z}/n\mathbb{Z})^d$ (see [Ter99, Chapter 10, Theorem 2]) can be stated as

$$f(0) = \frac{1}{n^d} \sum_{\psi \in \mathrm{Hom}_n^d} \hat{f}(\psi) = \frac{1}{n^d} \sum_{\psi \in \mathrm{Hom}_n^d} \sum_{x \in (\mathbb{Z}/n\mathbb{Z})^d} f(x)\omega_n^{-\psi(x)}.$$

By definition of Rf, the previous identity becomes

$$f(0) = \frac{1}{n^d} \sum_{\psi \in \mathrm{Hom}_n^d} \sum_{0 \leqslant c < n} \omega_n^{-c} Rf(\psi, c).$$

Notice that this is already a valid inversion formula for the Radon transform, but not the one we are looking for.

By exploiting the invariance of the Radon transform $Rf(a\psi, ac) = Rf(\psi, c)$, for any $0 \leqslant a < n$ coprime with n, we can continue the previous identity (recall that φ denotes Euler's totient function)

$$= \frac{1}{n^d} \sum_{\psi \in \mathrm{Hom}_n^d} \sum_{0 \leqslant c < n} Rf(\psi, c) \frac{1}{\varphi(n)} \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^*} \omega_n^{-ac}.$$

To proceed further, we remember that the sum of the primitive roots coincides with the Möbius μ function; hence we get

$$= \frac{1}{n^d} \sum_{\psi \in \mathrm{Hom}_n^d} \sum_{g \mid n} \frac{\mu(n/g)}{\varphi(n/g)} \sum_{\substack{0 \leqslant c < n \\ \gcd(c,n)=g}} Rf(\psi, c).$$

Now, let us use that $n = p^k$ is a prime power. Since μ is zero when evaluated over non-squarefree numbers, we may assume that $n/g = 1$ or $n/g = p$ in the latter formula. Thus we obtain

$$= \frac{1}{p^{kd}} \sum_{\psi \in \mathrm{Hom}_n^d} \Big(Rf(\psi, 0) - \frac{1}{p-1} \sum_{t=1}^{p-1} Rf(\psi, tp^{k-1}) \Big).$$

Thanks to the identity

$$\sum_{t=0}^{p-1} Rf(\psi, tp^{k-1}) = Rf(p\psi, 0),$$

we can continue our long chain of equalities

$$= \frac{1}{p^{kd}} \sum_{\psi \in \mathrm{Hom}_n^d} \Big(\frac{p}{p-1} Rf(\psi, 0) - \frac{1}{p-1} Rf(p\psi, 0) \Big).$$

Notice that we have written $f(0)$ using only the values of the Radon transform over hyperplanes containing 0. Let us observe that, for $\psi \in \mathrm{Hom}_n^d$, there can be either 0 or p^d different $\psi' \in \mathrm{Hom}_n^d$ such that $p\psi' = \psi$, depending on whether $p \mid \psi$ or not (recall that $p \mid \psi$ is equivalent to $p \mid \psi(x)$ for all $x \in (\mathbb{Z}/n\mathbb{Z})^d$). Thanks to this observation, we obtain that $f(0)$ is equal to

$$= \frac{1}{p^{kd}} \sum_{\psi \in \mathrm{Hom}_n^d} Rf(\psi, 0) \Big(\frac{p}{p-1} - \frac{p^d}{p-1} [\, p \mid \psi \,] \Big),$$

where $[\,\cdot\,]$ denotes the Iverson bracket. Through some simple algebraic manipulation, we finally deduce

$$f(0) = \frac{1}{n^{d-1}\varphi(n)} \sum_{\psi \in \mathrm{Hom}_n^d} Rf(\psi, 0)(1 - p^{d-1}[\, p \mid \psi \,]),$$

which is the desired inversion formula for $n = p^k$. □

Let us apply this inversion formula to establish the FS-regularity of the group $(\mathbb{Z}/n\mathbb{Z})^d$ when $n \in O_{\mathrm{FS}}$. The idea is to project through an homomorphism onto $\mathbb{Z}/n\mathbb{Z}$, use the FS-regularity of $\mathbb{Z}/n\mathbb{Z}$ proven in Proposition 4.9, and then recover the FS-regularity of $(\mathbb{Z}/n\mathbb{Z})^d$ thanks to the invertibility of the Radon transform on $(\mathbb{Z}/n\mathbb{Z})^d$.

Proposition 5.5. *For any $n \in O_{\mathrm{FS}}$ and any $d \geqslant 1$, the group $(\mathbb{Z}/n\mathbb{Z})^d$ is* FS*-regular.*

Proof. For a multiset $B \in \mathcal{M}((\mathbb{Z}/n\mathbb{Z})^d)$, by definition of the Radon transform on $((\mathbb{Z}/n\mathbb{Z})^d$ (see Definition 5.1), one has $R\mu_B(\psi, c) = \mu_{\psi(B)}(c)$ (recall that μ_B denotes the multiplicity of elements in the multiset B, see Section 2.1) for $\psi \in \mathrm{Hom}_n^d$ and any $c \in \mathbb{Z}/n\mathbb{Z}$. Therefore, the inversion formula of Theorem 1.6 (recall also Equation (5.2)) implies

$$\mu_B(x) = \sum_{\psi \in \mathrm{Hom}_n^d} \lambda_{n,d}(\psi)\mu_{\psi(B)}(\psi(x)), \tag{5.3}$$

for all $x \in (\mathbb{Z}/n\mathbb{Z})^d$. Notice that this formula allows us to reconstruct B given all its projections $\psi(B)$ onto $\mathbb{Z}/n\mathbb{Z}$.

Take two multisets $A, A' \in \mathcal{M}((\mathbb{Z}/n\mathbb{Z})^d)$ such that $\mathrm{FS}(A) = \mathrm{FS}(A')$; our goal is to prove that $A \sim_0 A'$.

For any $\psi \in \mathrm{Hom}_n^d$, it holds $\mathrm{FS}(\psi(A)) = \mathrm{FS}(\psi(A'))$ and therefore, since we have shown that $\mathbb{Z}/n\mathbb{Z}$ is FS-regular in Proposition 4.9, we have $\psi(A) \sim_0 \psi(A')$. Thus (we use only $\psi(A) \sim \psi(A')$), we deduce that for any $\psi \in \mathrm{Hom}_n^d$,

$$\mu_{\psi(A)}(x) + \mu_{\psi(A)}(-x) = \mu_{\psi(A')}(x) + \mu_{\psi(A')}(-x) \tag{5.4}$$

for all $x \in (\mathbb{Z}/n\mathbb{Z})^d$.

Joining Equations (5.3) and (5.4), we obtain

$$\begin{aligned}\mu_A(x)+\mu_A(-x) &= \sum_{\psi\in\mathrm{Hom}_n^d}\lambda_{n,d}(\psi)\big(\mu_{\psi(A)}(\psi(x))+\mu_{\psi(A)}(-\psi(x))\big)\\ &= \sum_{\psi\in\mathrm{Hom}_n^d}\lambda_{n,d}(\psi)\big(\mu_{\psi(A')}(\psi(x))+\mu_{\psi(A')}(-\psi(x))\big)\\ &= \mu_{A'}(x)+\mu_{A'}(-x)\end{aligned}$$

for all $x\in(\mathbb{Z}/n\mathbb{Z})^d$. The latter identity is equivalent to $A\sim A'$, which implies $A\sim_0 A'$ thanks to Lemma 3.3-*(3)*. □

6. FS-regularity of products with $\mathbb{Z}$

In this section we show that multiplying by $\mathbb{Z}$ does not break the FS-regularity of a group (see Proposition 6.4). In order to do it, we will need two technical lemmas. The second one, Lemma 6.3, gives a condition equivalent to FS-regularity which comes handy in the proof of the main result of this section.

Lemma 6.1. *Let G be an abelian group without elements of order 2. Given three multisets A, A', $B\in\mathcal{M}(G)$, if $A+\mathrm{FS}(B)=A'+\mathrm{FS}(B)$, then $A=A'$.*

Proof. Let us first prove the result when $B=\{b\}$ is a singleton. We prove the result by induction on the cardinality of A.

If $|A|=0$, then $\varnothing=A+\mathrm{FS}(B)=A'+\mathrm{FS}(B)$ and thus $A'=\varnothing$.

To handle the case $|A|>0$, we begin by showing that A and A' have a common element. We argue by contradiction, hence we assume that A and A' are disjoint.

Take any $a\in A$. We have $a+b\in A+\mathrm{FS}(B)=A'+\{0,b\}$. Since $a\notin A'$, it must hold $a+b\in A'$. By repeating this argument (swapping the role of A and A' and replacing a with $a+b$) we obtain that $a+2b\in A$. Repeating such argument k times, we obtain that $a+kb\in A$ if k is even, and $a+kb\in A'$ if k is odd. Since A and A' are finite, b must have finite order, otherwise the elements $(a+kb)_{k\in\mathbb{N}}$ would be all distinct. Let $\mathrm{ord}(b)$ be the order of b; by assumption $\mathrm{ord}(b)$ is odd. We have the contradiction $A\ni a=a+\mathrm{ord}(b)b\in A'$; therefore we have proven that A and A' have a common element.

Now pick $\bar a\in A\cap A'$. It holds

$$\begin{aligned}(A\setminus\{\bar a\})+\mathrm{FS}(B) &= (A+\mathrm{FS}(B))\setminus\{\bar a,\,\bar a+b\}\\ &= (A'+\mathrm{FS}(B))\setminus\{\bar a,\,\bar a+b\}=(A'\setminus\{\bar a\})+\mathrm{FS}(B).\end{aligned}$$

Therefore, by the induction hypothesis, $A\setminus\{\bar a\}=A'\setminus\{\bar a\}$, which is equivalent to $A=A'$.

Let us now treat general multisets B. We proceed by induction on the cardinality of B; the case $|B|=0$ is trivial and the case $|B|=1$ is already established, so we may assume $|B|>1$.

Pick an element $\bar b\in B$. We have

$$A+\mathrm{FS}(B)=(A+\mathrm{FS}(B\setminus\{\bar b\}))+\mathrm{FS}(\{\bar b\}),$$

and likewise for A'. Applying the induction hypothesis for the three multiset $A+\mathrm{FS}(B\setminus\{\bar{b}\}), A'+\mathrm{FS}(B\setminus\{\bar{b}\}), \{\bar{b}\}$, yields the relation $A+\mathrm{FS}(B\setminus\{\bar{b}\}) = A'+\mathrm{FS}(B\setminus\{\bar{b}\})$, and one more application yields the sought $A = A'$. □

Remark 6.2. Lemma 6.1 admits a beautiful short proof by computing the Fourier transform (refer to [HR79, Chapter VI] for an introduction to the Fourier analysis on groups) of the multiplicity functions of the two multisets $A + \mathrm{FS}(B)$ and $A' + \mathrm{FS}(B)$ and using the assumption that G has no elements of order 2 to deduce that a character $\chi \in \hat{G}$ cannot take the value -1. This proof was suggested to us by Noah Kravitz. We decided to keep the combinatorial proof since it is more in line with the *elementary* spirit of this section.

Lemma 6.3. *Let G be an abelian group without elements of order 2. The group G is* FS*-regular if and only if, for all $A, A' \in \mathcal{M}(G)$ such that $\mathrm{FS}(A) = \mathrm{FS}(A') + g$ for some $g \in G$, it holds $A \sim A'$.*

Proof. Assume that G is FS-regular and take $A, A' \in \mathcal{M}(G)$ such that $\mathrm{FS}(A) = \mathrm{FS}(A') + g$ for some $g \in G$. Applying Lemma 3.3-*(4)*, we produce a multiset $A'' \in \mathcal{M}(G)$ such that $A'' \sim A'$ and $\mathrm{FS}(A) = \mathrm{FS}(A'')$; then we deduce $A \sim_0 A''$ because G is FS-regular. So, we get $A \sim_0 A'' \sim A'$ which implies $A \sim A'$ by transitivity.

Let us now show the converse. Given $A, A' \in \mathcal{M}(G)$ such that $\mathrm{FS}(A) = \mathrm{FS}(A')$, the condition described in the statement implies $A \sim A'$ which implies $A \sim_0 A'$ thanks to Lemma 3.3-*(3)*. Therefore we have proven the FS-regularity of G. □

Proposition 6.4. *If G is an* FS*-regular abelian group, then also $G \oplus \mathbb{Z}$ is* FS*-regular.*

Proof. We begin by setting up some notation. For $B \in \mathcal{M}(G \oplus \mathbb{Z})$ and $z \in \mathbb{Z}$, define

$$\begin{aligned} B_{<z} &= \{(g, z') \in B : z' < z\}, \\ B_{\leqslant z} &= \{(g, z') \in B : z' \leqslant z\}, \\ B_{=z} &= \{(g, z') \in B : z' = z\}. \end{aligned}$$

Let $A, A' \in \mathcal{M}(G \oplus \mathbb{Z})$ be two multisets such that $\mathrm{FS}(A) = \mathrm{FS}(A') + (\bar{g}, \bar{z})$ for some $\bar{g} \in G$ and $\bar{z} \in \mathbb{Z}$; we want to prove that $A \sim A'$. This claim is equivalent to the FS-regularity of G thanks to Lemma 6.3.

Up to changing the signs[9] of $A_{<0}$ and $A'_{<0}$, we may assume that $A_{<0} = \varnothing$ and $A'_{<0} = \varnothing$. We will use repeatedly, without explicitly mentioning it, that the first coordinate of the elements of A and A' is nonnegative.

Recall that, by assumption, $\mathrm{FS}(A) = \mathrm{FS}(A') + (\bar{g}, \bar{z})$. Since $(0_G, 0)$ belongs to both $\mathrm{FS}(A)$ and $\mathrm{FS}(A')$ (and the first coordinate of all the elements of both multisets is nonnegative), it must be $\bar{z} = 0$. So, it holds $\mathrm{FS}(A) = \mathrm{FS}(A') + (\bar{g}, 0)$.

We prove, by induction on z, that $A_{\leqslant z} \sim A'_{\leqslant z}$ and $\mathrm{FS}(A_{\leqslant z}) = \mathrm{FS}(A'_{\leqslant z}) + (\bar{g}, 0)$. One can deduce $A \sim A'$ by taking z sufficiently large.

[9] Formally, we are substituting A and A' with $\tilde{A} := (A \setminus A_{<0}) \cup (-A_{<0})$ and $\tilde{A}' := (A' \setminus A'_{<0}) \cup (-A'_{<0})$. Notice that $A \sim \tilde{A}$ and $A' \sim \tilde{A}'$.

Notice that
$$\mathrm{FS}(A_{=0}) = \mathrm{FS}(A)_{=0} = \mathrm{FS}(A')_{=0} + (\bar{g}, 0).$$
By taking the projection on G of both sides of the latter identity, since G is FS-regular, we can apply Lemma 6.3 and get $A_{=0} \sim A'_{=0}$. This concludes the first step of the induction, that is $z = 0$ (since $A_{=0} = A_{\leqslant 0}$ and $A'_{=0} = A'_{\leqslant 0}$).

For $z \geqslant 1$, we show that $A_{=z} = A'_{=z}$ which immediately implies, thanks to the inductive assumption, that $A_{\leqslant z} \sim A'_{\leqslant z}$ and $\mathrm{FS}(A_{\leqslant z}) = \mathrm{FS}(A'_{\leqslant z}) + (\bar{g}, 0)$.

Given a multiset $B \in \mathcal{M}(G \oplus \mathbb{Z})$ such that $B_{<0} = \varnothing$ (later on B will be a subset of A or A'), if $\sum B = (g, z)$ for some $g \in G$ and $z \geqslant 1$ then either $B = B_{<z}$ or $B = B_{=z} \cup B_{=0}$ and $B_{=z}$ is a singleton. Hence, one has

$$\begin{aligned} \mathrm{FS}(A)_{=z} &= \mathrm{FS}(A_{<z})_{=z} \cup (A_{=z} + \mathrm{FS}(A_{=0})), \\ \mathrm{FS}(A')_{=z} &= \mathrm{FS}(A'_{<z})_{=z} \cup (A'_{=z} + \mathrm{FS}(A'_{=0})), \end{aligned}$$

and therefore, recalling that $\mathrm{FS}(A) = \mathrm{FS}(A') + (\bar{g}, 0)$, we get

$$\begin{aligned} \mathrm{FS}(A_{<z})_{=z} \cup (A_{=z} + \mathrm{FS}(A_{=0})) &= \mathrm{FS}(A)_{=z} = \mathrm{FS}(A')_{=z} + (\bar{g}, 0) \\ &= (\mathrm{FS}(A'_{<z})_{=z} + (\bar{g}, 0)) \cup (A'_{=z} + \mathrm{FS}(A'_{=0}) + (\bar{g}, 0)). \end{aligned} \tag{6.1}$$

By inductive assumption, $\mathrm{FS}(A_{=0}) = \mathrm{FS}(A'_{=0}) + (\bar{g}, 0)$ and $\mathrm{FS}(A_{<z}) = \mathrm{FS}(A'_{<z}) + (\bar{g}, 0)$; hence Equation (6.1) implies

$$A_{=z} + \mathrm{FS}(A_{=0}) = A'_{=z} + \mathrm{FS}(A_{=0})$$

and we deduce $A_{=z} = A'_{=z}$ thanks to Lemma 6.1 (since G is FS-regular it cannot have elements of order 2, see Proposition 4.1). □

7. Proof of the Main Theorem

The proof of the main theorem of this paper is routine work now that we have established Propositions 4.1, 4.9, 5.5 and 6.4.

Proof of Theorem 1.5. If there is a torsion element $g \in G$ such that $\mathrm{ord}(g) \notin O_{\mathrm{FS}}$, then $\mathbb{Z}/\mathrm{ord}(g)\mathbb{Z}$ is a subgroup of G. Thanks to Proposition 4.1, we know that $\mathbb{Z}/\mathrm{ord}(g)\mathbb{Z}$ is not FS-regular and therefore also G is not FS-regular.

We prove the converse implication in three steps: first for groups with structure $(\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z})^d$, then for finitely generated groups, and finally for any group.

Let us assume that G is an abelian group such that $\mathrm{ord}(g) \in O_{\mathrm{FS}}$ whenever $g \in G$ has finite order.

Step 1: $G = (\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z})^d$. The assumption on the order of the elements of G guarantees that $n \in O_{\mathrm{FS}}$. Hence, Proposition 5.5 shows that $(\mathbb{Z}/n\mathbb{Z})^d$ is FS-regular. Thanks to Proposition 6.4, we obtain that also $(\mathbb{Z}/n\mathbb{Z})^d \oplus \mathbb{Z}^d$ is FS-regular.

Step 2: G is finitely generated. Let n be the maximum order of an element in G with finite order. By assumption $n \in O_{\mathrm{FS}}$. The classification of finitely generated abelian groups (see Section 2.2) guarantees that G is a subgroup of $(\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z})^d$ for some $d \geqslant 1$. By the previous step, we know that $(\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z})^d$ if FS-regular and thus also G is FS-regular (being a subgroup of an FS-regular group).

Step 3: No restrictions on G. Let $A, A' \in \mathcal{M}(G)$ be two multisets such that $\mathrm{FS}(A) = \mathrm{FS}(A')$; we want to prove that $A \sim_0 A'$. Let $\tilde{G} := \langle A \cup A' \rangle$ be the group generated by the elements of A and A'. The condition on the orders is inherited by $\tilde{G}$ and, since $\tilde{G}$ is finitely generated, the previous step guarantees that $\tilde{G}$ is FS-regular; in particular $A \sim_0 A'$ as desired. □

Acknowledgements

The authors are thankful to Fabio Ferri for providing valuable suggestions and references about the theory of cyclotomic units, and also to Michele D'Adderio, Elia Bruè for their feedback on an early draft of this work. We want to thank Noah Kravitz because his comments led to a considerable improvement of the inversion formula for the discrete Radon transform.

References

[AI08] Ahmed Abouelaz and Abdallah Ihsane. Diophantine integral geometry. *Mediterr. J. Math.*, 5(1):77–99, 2008. doi:10.1007/s00009-008-0137-2.

[AZ97] Tewodros Amdeberhan and Melkamu Zeleke. On injectivity of the combinatorial Radon transform of order five. *J. Comput. Appl. Math.*, 83(2):251–255, 1997. doi:10.1016/S0377-0427(97)00109-X.

[BL96] Jan Boman and Svante Linusson. Examples of non-uniqueness for the combinatorial Radon transform modulo the symmetric group. *Math. Scand.*, 78(2):207–212, 1996. doi:10.7146/math.scand.a-12583.

[Bli89] Wayne D. Blizard. Multiset theory. *Notre Dame J. Formal Logic*, 30(1):36–66, 1989. doi:10.1305/ndjfl/1093634995.

[Bol87] Ethan D. Bolker. The finite Radon transform. In *Integral geometry (Brunswick, Maine, 1984)*, volume 63 of *Contemp. Math.*, pages 27–50. Amer. Math. Soc., Providence, RI, 1987. doi:10.1090/conm/063/876312.

[CD20] Tapas Chatterjee and Sonika Dhillon. Linear independence of logarithms of cyclotomic numbers and a conjecture of Livingston. *Can. Math. Bull.*, 63(1):31–45, 2020. doi:10.4153/S0008439519000468.

[CDP97] Richard Crandall, Karl Dilcher, and Carl Pomerance. A search for Wieferich and Wilson primes. *Math. Comp.*, 66(217):433–449, 1997. doi:10.1090/S0025-5718-97-00791-6.

[CHM18] Yung Duk Cho, Jong Yoon Hyun, and Sunghwan Moon. Inversion of the classical Radon transform on $\mathbb{Z}_p^n$. *Bull. Korean Math. Soc.*, 55(6):1773–1781, 2018. doi:10.4134/BKMS.b171064.

[CL16] Yong-Gao Chen and Vsevolod F. Lev. Integer sets with identical representation functions. *Integers*, 16:Paper No. A36, 4, 2016.

[DG85] Persi Diaconis and R. L. Graham. The Radon transform on Z_2^k. *Pacific J. Math.*, 118(2):323–345, 1985. doi:10.2140/pjm.1985.118.323.

[DV04] Michelle R. DeDeo and Elinor Velasquez. The Radon transform on $\mathbb{Z}_n^k$. *SIAM J. Discrete Math.*, 18(3):472–478, 2004. doi:10.1137/S0895480103430764.

[FG87] P. Frankl and R. L. Graham. The Radon transform on abelian groups. *J. Combin. Theory Ser. A*, 44(1):168–171, 1987. doi:10.1016/0097-3165(87)90071-9.

[Fil89] James Allen Fill. The Radon transform on Z_n. *SIAM J. Discrete Math.*, 2(2):262–283, 1989. doi:10.1137/0402023.

[Fom19] Dmitri V. Fomin. Is the multiset of n integers uniquely determined by the multiset of its s-sums? *Amer. Math. Monthly*, 126(5):400–417, 2019. doi:10.1080/00029890.2019.1577088.

[Gai23] Konstantinos Gaitanas. On subset sums of $\mathbb{Z}_n^\times$ which are equally distributed modulo n. *Arch. Math.*, 121:47–54, 2023. doi:10.1007/s00013-023-01853-2.

[GFS62] B. Gordon, A. S. Fraenkel, and E. G. Straus. On the determination of sets by the sets of sums of a certain order. *Pacific J. Math.*, 12(1):187–196, 1962. doi:10.2140/pjm.1962.12.187.

[Hel99] Sigurdur Helgason. *The Radon transform*, volume 5 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, second edition, 1999. doi:10.1007/978-1-4757-1463-0.

[Hel17] Charles Helou. Characterization of representation functions. *Integers*, 17:Paper No. A44, 6, 2017.

[HR79] Edwin Hewitt and Kenneth A. Ross. *Abstract harmonic analysis. Vol. I*, volume 115 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, second edition, 1979. Structure of topological groups, integration theory, group representations.

[Ilm14] Joonas Ilmavirta. On radon transforms on finite groups. 2014. arXiv:1411.3829.

[KS19] Sándor Z. Kiss and Csaba Sándor. On the structure of sets which have coinciding representation functions. *Integers*, 19:Paper No. A66, 29, 2019.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002. doi:10.1007/978-1-4613-0041-0.

[Lev04] Vsevolod F. Lev. Reconstructing integer sets from their representation functions. *Electron. J. Combin.*, 11(1):Research Paper 78, 6, 2004. doi:10.37236/1831.

[Mar77] Daniel A. Marcus. *Number fields*. Universitext. Springer-Verlag, New York-Heidelberg, 1977.

[Nat08] Melvyn B. Nathanson. Inverse problems for representation functions in additive number theory. In *Surveys in number theory*, volume 17 of *Dev. Math.*, pages 89–117. Springer, New York, 2008.

[Pat17] Siddhi Pathak. On a conjecture of Livingston. *Can. Math. Bull.*, 60(1):184–195, 2017. doi:10.4153/CMB-2016-065-1.

[SS58] J. L. Selfridge and E. G. Straus. On the determination of numbers by their sums of a fixed order. *Pacific J. Math.*, 8(4):847–856, 1958. doi:10.2140/pjm.1958.8.847.

[Str82] Robert S. Strichartz. Radon inversion—variations on a theme. *Amer. Math. Monthly*, 89(6):377–384, 420–423, 1982. doi:10.2307/2321649.

[Ter99] Audrey Terras. *Fourier analysis on finite groups and applications*, volume 43 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999. doi:10.1017/CBO9780511626265.

[TV06] Terence Tao and Van Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006. doi:10.1017/CBO9780511755149.

[Vel97] Elinor Velasquez. Radon transform on finite symmetric spaces. *Pacific J. Math.*, 177(2):369–376, 1997. doi:10.2140/pjm.1997.177.369.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997. doi:10.1007/978-1-4612-1934-7.