ERGODICITY OF NILPOTENT GROUP ACTIONS, GAUSS'S LEMMA AND MIXING IN THE HEISENBERG GROUP

BENJAMIN R. HAYES

Abstract. We discuss how to associate to a given group an action by automorphisms on a compact abelian group. We describe how to relate questions about the dynamics of this action to group theoretic questions, and apply this to study ergodicity in the case of nilpotent groups. We also discuss the case of mixing in the Heisenberg group.

Contents

1. Background History

Dynamical systems theory starts with the study of a transformation $T\colon X \to X$ of some set X, usually with some additional structure (e.g. topological or measure-theoretic). The transformation usually preserves this structure, and one asks questions about the eventual behavior of the system. One can view the transformation T as an semi-group action of $\mathbb{N}$ on X. If one requires T to be invertible then we have a group action of $\mathbb{Z}$ on X. More generally, one can take any group Γ and study its (structure-preserving) actions on a set X. Paying attention to this more general situation leads to a richer theory, but it can be difficult to produce examples which illustrate the theory. For example a standard requirement is that Γ be abelian, but aside from the classical example of commuting toral automorphisms, finding $\mathbb{Z}^d$ actions on spaces with topological, measure-theoretic or smooth structures can be difficult. For example, it is hard to produce commuting diffeomorphisms of a

Date: July 8, 2009.

smooth manifold. Even if one is considering a single transformation, answering natural questions about the dynamics of such a transformation, e.g. the existence of invariant measures, ergodicity, and mixing can be difficult even if one has powerful tools available (for example, trying to find invariant measures of a smooth transformation on a smooth manifold).

One approach to repair this problem is to find a type of structure analogous to, but more general than, toral automorphisms. The main technique which allows one to say a great deal about toral automorphisms is Fourier analysis. To generalize these ideas, we consider actions by automorphisms of a compact abelian group, where an appropriate generalization of Fourier analysis is possible. This approach also gives countless examples of group actions by any given group Γ on spaces with topological and measure-theoretic structure. Moreover, by choosing one of the nicest topological properties (compactness) and combining it with one of the nicest algebraic properties (commutativity), one has enough structure to guarantee an appropriate measure-theoretic structure as well as answer many natural dynamical questions. For example, given a $\mathbb{Z}^d$ action on a compact abelian group, one can give precise algebraic conditions for mixing and ergodicity (see [6] Chapter VII and II , and for a small taste Section 4 here), as well as explicit formulas for entropy (see [6] Chapter V). In this class of group actions, it is easier to create counterexamples to test and formulate conjectures in the study of the more general theory. This approach also allows one to investigate connections between ergodic theory and other areas of mathematics, particularly commutative algebra and algebraic geometry (though we will not use much algebraic geometry here, examples are provided in [6] Chapter II). Indeed, we will be using measure theory, topology, noncommutative algebra, combinatorial geometry, and elementary number theory, (in fact, we will use all of these in one proof, see Theorem 3.2.1) just to name a few.

Much of the present research on this topic has been in actions by abelian groups, particularly $\mathbb{Z}^d$-actions. We will focus more on non-abelian groups, particularly nilpotent groups in Section 3, and the particular case of the Heisenberg group in Section 4. The Heisenberg group is an important example, being one of the simplest cases of a non-abelian torsion-free group, and most of the results derived here grew out of the study of the Heisenberg group as a particular example.

2. Introduction and Discussion of the Main Problem

Let Γ be a group, whose operation is written multiplicatively. The integral group ring $\mathbb{Z}[\Gamma]$ is the set of all formula sums $\{\sum_{\gamma\in\Gamma} c_\gamma \gamma\}$ with $c_\gamma \in \mathbb{Z}$, and all but finitely many of the c_γ nonzero. Addition in $\mathbb{Z}[\Gamma]$ is defined in the obvious way, and multiplication is defined by extending the multiplication in Γ, and requiring that the distributive law holds. To every element $f \in \mathbb{Z}[\Gamma]$ we will associate a compact abelian group X_f and an action α_f of Γ on X_f by automorphisms (i.e. automorphisms of the group which are simultaneously homeomorphisms).

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, which we think of as the unit circle. We first show that the group of homomorphisms from $\mathbb{Z}[\Gamma]$ (as an additive group) to $\mathbb{T}$, i.e. the dual group of $\mathbb{Z}[\Gamma]$, is isomorphic to $\mathbb{T}^\Gamma$. We describe the isomorphism as follows. Let $f \in \mathbb{Z}[\Gamma]$ and $\theta \in \mathbb{T}^\Gamma$. We may write $f = \sum_{\gamma\in\Gamma} f_\gamma \gamma$ and $\theta = (\theta_\gamma)_{\gamma\in\Gamma}$ and define

$$\langle \theta, f\rangle = \sum_{\gamma\in\Gamma} \theta_\gamma f_\gamma,$$

which can be thought as a "inner product." The map $\theta \mapsto (f \mapsto \langle \theta, f\rangle)$ is an isomorphism between the dual group of $\mathbb{Z}[\Gamma]$ and $\mathbb{T}^\Gamma$.

We define Γ-anti-actions on $\mathbb{Z}[\Gamma]$ and we will dualize to get a Γ-action on $\mathbb{T}^\Gamma$. For any $\gamma \in \Gamma$, let $\lambda_\gamma \colon \mathbb{Z}[\Gamma] \to \mathbb{Z}[\Gamma]$ be defined by $\lambda_\gamma(f) = \gamma^{-1}f$ and $\rho_\gamma \colon \mathbb{Z}[\Gamma] \to \mathbb{Z}[\Gamma]$ be defined by $\rho_\gamma(f) = f\gamma$. Then $\rho_\gamma \circ \rho_\delta = \rho_{\delta\gamma}$ and $\lambda_\gamma \circ \lambda_\delta = \lambda_{\delta\gamma}$. We require of the dual actions $\lambda^\gamma, \rho^\gamma$ that

$$\langle \lambda^\gamma(\theta), f\rangle = \langle f, \lambda_\gamma(\theta)\rangle = \langle \theta, \gamma^{-1}f\rangle \text{ and } \langle \rho^\gamma(\theta), f\rangle = \langle f, \rho_\gamma(\theta)\rangle = \langle \theta, f\gamma\rangle,$$

more explicitly

$$\lambda^\gamma(\theta)_\delta = \langle \lambda^\gamma(\theta), \delta\rangle = \langle \theta, \gamma^{-1}\delta\rangle = \theta_{\gamma^{-1}\delta}$$
$$\rho^\gamma(\theta)_\delta = \langle \rho^\gamma(\theta), \delta\rangle = \langle \theta, \delta\gamma\rangle = \theta_{\delta\gamma}.$$

A consequence of this is that every λ^γ is a automorphism of $\mathbb{T}^\Gamma$ as a topological group (so that λ^γ is a homeomorphism), and $\lambda^\gamma \circ \lambda^\delta = \lambda^{\gamma\delta}$. Similarly ρ^γ is an automorphism of $\mathbb{T}^\Gamma$ and $\rho^\gamma \circ \rho^\delta = \rho^{\gamma\delta}$. So we have an action by automorphisms of $\mathbb{T}^\Gamma$.

It is helpful to think of an element $\theta = (\theta_\gamma)_{\gamma\in\Gamma} \in \mathbb{T}^\Gamma$ as a formal infinite sum $\sum_{\gamma\in\Gamma} \theta_\gamma \gamma$. This is because

$$\lambda^\gamma(\theta) = \gamma\theta = \sum_{\delta\in\Gamma} \theta_\delta(\gamma\delta) \text{ and } \rho^\gamma(\theta) = \theta\gamma^{-1} = \sum_{\delta\in\Gamma} \theta_\delta \delta\gamma^{-1} \tag{2.0.1}$$

so our action on $\mathbb{T}^\Gamma$ is really just by multiplication by group elements. In particular, we can think of $\mathbb{T}^\Gamma$ as simultaneously a left and right $\mathbb{Z}[\Gamma]$ module.

Now suppose we are given $f \in \mathbb{Z}[\Gamma]$. The corresponding dual group X_f of $\mathbb{Z}[\Gamma]/\mathbb{Z}[\Gamma]f$ we think of as an orthogonal complement to $\mathbb{Z}[\Gamma]f$ under the above inner product. So $\theta \in X_f$ if and only if $\langle \theta, gf\rangle = 0$ for all $g \in \mathbb{Z}[\Gamma]$. If $\gamma \in \Gamma$, and $\theta \in X_f$, then

$$\langle \lambda^\gamma(\theta), gf\rangle = \langle \theta, \lambda_\gamma(gf)\rangle = \langle \theta, (\gamma^{-1}g)f\rangle = 0, \text{ for all } g, f \in \mathbb{Z}[\Gamma]. \tag{2.0.2}$$

In particular (by applying the case $\gamma = 1$) for all $\theta, \psi \in X_f$

$$\langle \theta + \psi, gf\rangle = \langle \theta, gf\rangle + \langle \psi, gf\rangle = 0, \text{ for all } g \in \mathbb{Z}[\Gamma].$$

Thus X_f is a subgroup of $\mathbb{T}^\Gamma$. Since for each $f \in \mathbb{Z}[\Gamma]$, the map $\theta \mapsto \langle \theta, f\rangle$ is continuous we know X_f is a closed subset of $\mathbb{T}^\Gamma$. Since $\mathbb{T}^\Gamma$ is compact by Tychonoff's Theorem, we know X_f is a compact abelian group. By (2.0.2), the group X_f is invariant under the automorphism λ^γ so it makes sense to define α_f^γ by restricting λ^γ to X_f. This gives our action α_f by automorphism on the compact abelian group X_f.

Define $\rho_f = \sum_{\delta\in\Gamma} f_\delta \rho_\delta$ and $\rho^f = \sum_{\delta\in\Gamma} f_\delta \rho^\delta$, and the *adjoint of* f by $f^* = \sum_{\delta\in\Gamma} f_\delta \delta^{-1}$. Then $\rho_f(g) = gf$ for all $g \in \mathbb{Z}[\Gamma]$ and by (2.0.1)

$$\rho^f(\theta) = \sum_\delta f_\delta \rho^\delta(\theta) = \theta\left(\sum_{\delta\in\gamma} f_\delta \delta^{-1}\right) = \theta f^*.$$

Then $\theta \in X_f$ if and only if

$$\langle \theta, gf\rangle = \langle \theta f^*, g\rangle = 0$$

for all $g \in \mathbb{Z}[\Gamma]$. By considering $g = \gamma$ for any $\gamma \in \Gamma$, we see that this is the same as $\theta f^* = 0$. Thus X_f is the kernel of right multiplication by f^* on $\mathbb{T}^\Gamma$, which is invariant under left multiplication by Γ.

Since, for any $f \in \mathbb{Z}[\Gamma]$, the group X_f constructed above is a compact abelian group, there exists a Haar measure on X_f, i.e. a unique, translation-invariant, regular, probability measure μ_f with $\mu_f(U) > 0$ for every non-empty open subset U of X_f. A measurable subset $B \subseteq X_f$ is said to be *invariant* under α_f if for all $\gamma \in \Gamma$ we have $\mu_f(\alpha_f^\gamma(B) \triangle B) = 0$, (here $\triangle$ denotes the symmetric difference). The action α_f is called *ergodic* if the only invariant subsets of X_f have measure zero or one. The action α_f is said to be *mixing* if for any two measurable subsets A and B of X_f we have

$$\lim_{\gamma \to \infty} \mu_f(A \cap \alpha_f^\gamma(B)) = \mu_f(A)\mu_f(B).$$

Here $\gamma \to \infty$ is interpreted in the one-point compactification of Γ, where Γ is given the discrete topology. In turns out that for the above actions, there is an algebraic characterization of ergodicity and mixing given as follows, (see [6] Lemma 1.2 and Theorem 1.6).

Theorem 2.0.1. *Let Γ be a countable group and let $f \in \mathbb{Z}[\Gamma]$, the corresponding action α_f is ergodic if and only if for every $p \in \mathbb{Z}[\Gamma] \backslash \mathbb{Z}[\Gamma]f$ the Γ-orbit in $\mathbb{Z}[\Gamma]/\mathbb{Z}[\Gamma]f$*

$$\{\gamma p + \mathbb{Z}[\Gamma]f \colon \gamma \in \Gamma\},$$

is infinite. The corresponding action α_f is mixing if and only if for every $p \in \mathbb{Z}[\Gamma] \setminus \mathbb{Z}[\Gamma]f$ the stabilizer in $\mathbb{Z}[\Gamma]/\mathbb{Z}[\Gamma]f$

$$\mathrm{Stab}(p) = \{\gamma \in \Gamma \colon \gamma p \equiv p \mod \mathbb{Z}[\Gamma]f\}$$

is finite.

Here are a few examples. Suppose $\Gamma = \mathbb{Z}$, and $n \in \mathbb{N}$ suppose $f = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x - 1 \in Z[x^{\pm 1}] \cong \mathbb{Z}[\mathbb{Z}]$. Then $f^* = x^{-n} + a_{n-1}x^{-(n-1)} + a_{n-2}x^{-(n-2)} + \ldots + a_1 x^{-1} - 1$, and X_f is given by

$$\{\theta \in \mathbb{T}^{\mathbb{Z}} \colon \theta f^* = 0\}.$$

If $\theta = (\theta_k)_{k \in \mathbb{Z}}$ this condition becomes

$$\sum_{i=0}^{n} \theta_{k+i} a_i = 0$$

for all $k \in \mathbb{Z}$, in other words

$$\theta_k = \sum_{i=1}^{n} \theta_{k+i} a_i,$$

(here $a_0 = -1$ and $a_n = 1$) because of this recursive relationship one can determine θ from $(\theta_1, \theta_2, \ldots, \theta_n)$. The transformation given by multiplying by x^{-1} acts by

$$(\theta_1, \theta_2, \ldots, \theta_n) \mapsto (\sum_{i=1}^{n} \theta_i a_i, \theta_1, \theta_2, \ldots, \theta_{n-1}).$$

So this action is isomorphic to $T \colon \mathbb{T}^n \to \mathbb{T}^n$ given by

$$T\left(\begin{bmatrix}\theta_1\\ \theta_2\\ \theta_3\\ \vdots\\ \theta_n\end{bmatrix}\right) = \begin{bmatrix} a_1 & a_2 & a_3 & \ldots & 1\\ 1 & 0 & 0 & \ldots & 0\\ 0 & 1 & 0 & \ldots & 0\\ \vdots & \vdots & \ldots & \ddots & \vdots\\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix} \begin{bmatrix}\theta_1\\ \theta_2\\ \theta_3\\ \vdots\\ \theta_n\end{bmatrix} \mod 1,$$

this transformation is invertible since $\det(T) = \pm 1$. Thus the action constructed above is a toral automorphism. The same reasoning goes through if $|a_0 a_1| = 1$, to show that α_f is (isomorphic to) a toral automorphism. If instead the leading coefficients of f are not both ± 1, the above gives an action on a finite-dimensional solenoid (see [6] Example 6.17.) One example that has led to much development is Ledraipper's example, taking $\Gamma = \mathbb{Z}^2$ and $f = 1 + x + y$, for an in-depth discussion of this example and its interesting dynamical properties, see [2] and [6]. More generally, instead of considering single elements $f \in \mathbb{Z}[\Gamma]$, one can consider any left $\mathbb{Z}[\Gamma]$ module, (the case we have been considering is a prinicipal left ideal), it is then true that every action of Γ on a compact abelian group is isomorphic to one of the actions we have constructed. We will only consider principal left-ideals in $\mathbb{Z}[\Gamma]$.

3. Nilpotent Groups and Ergodicity

Definition 3.0.1. A group Γ is called *principally ergodic* if for every $f \in \mathbb{Z}[\Gamma]$, the corresponding action α_f on X_f is ergodic.

For example, if Γ is finite, then Γ is not principally ergodic. The size of the orbit is bounded by the size of the group, and so is finite. In this section, we establish that if Γ is a finitely generated torsion-free nilpotent group that is not isomorphic to the trivial group or the integers, then Γ is principally ergodic. To do this we will establish a version of Gausss Lemma for twisted group rings, as well as discuss Newton polyhedra which will be useful in our discussion of mixing in the case of the Heisenberg Group. We will assume all our rings have an identity, but need not be commutative.

3.1. Twisted Group Rings.

Recall that an element r in a ring R is a unit if it has a left inverse a and a right inverse b. Then

$$b = (ar)b = a(rb) = a,$$

so the left and right inverses agree.

Definition 3.1.1. Let R be a ring, and U its group of units. Let Γ be a group and suppose

$$t \colon \Gamma \times \Gamma \to U$$

satisfies

$$t(x,y)t(xy,z) = t(y,z)t(x,yz), \tag{3.1.1}$$

for all $x, y, z \in U$. We call t a *twisting function* , or a twisting function on Γ. Define the *twisted group ring* $R^t[\Gamma]$ to be a R-algebra with basis $\{\widetilde{x} \colon x \in \Gamma\}$ multiplication subject to $\widetilde{x}\widetilde{y} = t(x,y)\widetilde{xy}$ for all $x, y \in \Gamma$. Equation (3.1.1) is necessary and sufficient for multiplication to be associative. Thus a typical $f \in R^t[\Gamma]$ may be written $\sum_{\gamma \in \Gamma} c_\gamma \widetilde{\gamma}$, with $c_\gamma \in R$ and only finitely many of the c_γ are non-zero. If $f = c_\gamma \widetilde{\gamma}$, with $c_\gamma \in R \setminus \{0\}$, we will call f a *monomial.* Twisted group rings are discussed in more detail in [5], Chapter 1, Section 2.

Here are some examples. If $t(x,y) = 1$, for all $x, y \in \Gamma$ then $R^t[\Gamma]$ is the normal group ring. If $\mathbb{Z}^n$ is written as the multiplicative free abelian group on $\{x_1, x_2, \ldots, x_n\}$ with $t(x_i, x_i) = 1$ and $t(x_i, x_j) = -1$ for $i \neq j$, and extended using

(3.1.1), then $R^t[\mathbb{Z}^n]$ is a Laurent polynomial ring in n anti-commuting variables. Let

$$\mathbb{H} = \left\{ \begin{bmatrix} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{Z} \right\},$$

be the discrete Heisenberg group. Consider $\mathbb{Z}^2$ as the multiplicative free abelian group on $\{x, y\}$. Define $t: \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}[z^{\pm 1}]$ by $t(x^{n_1}y^{m_1}, x^{n_2}y^{m_2}) = z^{n_2 m_1}$. If we set

$$x = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, y = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, z = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

then

$$x^a y^b z^c = \begin{bmatrix} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix}$$

and it is easily verified that z commutes with x and y and $y^n x^m = z^{nm} x^m y^n$. Thus $\mathbb{Z}[\mathbb{H}] \cong \mathbb{Z}[z^{\pm 1}]^t[\mathbb{Z}^2]$.

3.2. **Newton Polyhedra.**

Definition 3.2.1. If A and B are subsets of $\mathbb{R}^n$, define the Minkowski sum

$$A + B = \{\mathbf{a} + \mathbf{b} \colon \mathbf{a} \in A, \mathbf{b} \in B\}.$$

In particular, note that for any $A \subset \mathbb{R}^n$ we have $A + \varnothing = \varnothing + A = \varnothing$. In case $A = \{\mathbf{a}\}$ we shall usually write $\mathbf{a} + B$ instead of $\{\mathbf{a}\} + B$, with similar remarks if $B = \{\mathbf{b}\}$. (Of course, we must violate this convention if A and B are both singletons, but we will never have to consider the case where A and B are both singletons).

If $A \subseteq \mathbb{R}^n$, we use $C(A)$ to denote the convex hull of A, which is the smallest convex set containing A, (such a set exists, since an arbitrary intersection of convex sets is convex). A *hyperplane* in $\mathbb{R}^n$ is a set of the form $\mathbf{a} + V$ where $\mathbf{a} \in \mathbb{R}^n$ and V is a $(n-1)$-dimensional vector subspace of $\mathbb{R}^n$. Equivalently such a set may be given by

$$\{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \mathbf{u} = \mathbf{b}\}$$

for some $\mathbf{u} \in \mathbb{S}^{n-1} = \{\mathbf{x} \in \mathbb{R}^n \colon \|\mathbf{x}\| = 1\}$ (where $\|\mathbf{x}\|$ is the usual Euclidean norm) and $\mathbf{b} \in \mathbb{R}^n$. A *convex polytope* is a subset of $\mathbb{R}^n$ which is the convex hull of a finite set. If P is a convex polytope, a *vertex* $\mathbf{v}$ of P is an element of P for which there is a hyper-plane H such that $H \cap P = \{\mathbf{v}\}$. (This is not the usual definition, but in the case of a convex polytope it is equivalent to the usual definition, see [4], Chapter 3, Section 1.) It is known that every convex polytope has finitely many vertices, and is the convex hull of its vertices, (see [4], Chapter 2, Section 4, Theorem 5.)

Definition 3.2.2. Let R be a ring and Γ a group with t a twisting function on Γ. If $f = \sum_{\gamma \in \Gamma} a_\gamma \widetilde{\gamma} \in R^t[\Gamma]$, the *support* of f denoted $\mathrm{Supp}(f)$ is defined by $\mathrm{Supp}(f) = \{\gamma \in \Gamma \colon a_\gamma \neq 0\}$, (note that $\mathrm{Supp}(0) = \varnothing$).

In the ring $\mathbb{Z}[\mathbb{Z}^n]$ we write $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ as $x^{\mathbf{a}}$ where $\mathbf{a} = (a_1, a_2, \dots, a_n) \in \mathbb{Z}^n$.

Definition 3.2.3. Let R be a ring, and t be a twisting function on $\mathbb{Z}^n$. Given $f \in R^t[\mathbb{Z}^n]$, define the *Newton polyhedron* $N(f)$ by $N(f) = C(\mathrm{Supp}(f))$.

Definition 3.2.4. Let $\mathbf{v} \in \mathbb{R}^n$. Then the partial ordering $\succ_{\mathbf{v}}$ on $\mathbb{R}^n$ is defined as $\mathbf{a} \succ_{\mathbf{v}} b$ if and only if $\mathbf{a} \cdot \mathbf{v} > \mathbf{b} \cdot \mathbf{v}$.

Note that if $\mathbf{v}$ is totally irrational (i.e. has rationally independent coordinates) then the ordering $\succ_{\mathbf{v}}$ is a monomial ordering on $\mathbb{Z}^n$ in the following sense:

(1) $\succ_{\mathbf{v}}$ is a total ordering;

(2) If $\mathbf{a} \succ_{\mathbf{v}} \mathbf{b}$ and $\mathbf{c} \in \mathbb{Z}^n$, then $\mathbf{a} + \mathbf{c} \succ_{\mathbf{v}} \mathbf{b} + \mathbf{c}$. In this case $\succ_{\mathbf{v}}$ will be denoted $>_{\mathbf{v}}$. (See [1], Chapter 2, Section 4.) Also notice that if A, B are bounded subsets of $\mathbb{Z}^n$ and $\mathbf{v}$ is totally irrational, then we have the following easily established equality:

$$\max(A + B) = \max(A) + \max(B);$$

where the max is taken with respect to $>_{\mathbf{v}}$.

The following geometric interpretation can be given to $\succ_{\mathbf{v}}$. Given a element $\mathbf{a} \in \mathbb{R}^n$ we can consider the half-space $H(\mathbf{a}, \mathbf{v})$ whose boundary plane goes through $\mathbf{a}$ and has an outward normal vector $\mathbf{v}$. Then $\mathbf{a} \succ_{\mathbf{v}} \mathbf{b}$ if and only if $H(\mathbf{a}, \mathbf{v}) \supsetneq H(\mathbf{bv})$. It is not hard to see that for any bounded subset A of $\mathbb{R}^n$ any maximum with respect to $\succ_{\mathbf{v}}$ must occur on the boundary of A, which we denote by ∂A. This fact and the geometric interpretation of $\succ_{\mathbf{v}}$ will be crucial in the proof of the following result.

Theorem 3.2.1. (Newton Polyhedron Theorem) *Suppose R is a ring without zero divisors, and that t is a twisting function on $\mathbb{Z}^n$. Then for all $f, g \in R^t[\mathbb{Z}^n]$ we have*

$$N(fg) = N(f) + N(g).$$

Proof. If either $f = 0$ or $h = 0$ is empty the conclusion is immediate (see definition 3.2.2 and the remarks following definition 3.2.3), so suppose neither f nor g is zero. Since multiplication of terms in $R^t[\mathbb{Z}^n]$, corresponds to addition of vectors in $\mathbb{R}^n$ we see that $N(fg) \subseteq N(f) + N(g)$. To see the opposite inclusion, notice that since $N(f) + N(g)$ is a sum of two polytopes, it is also a polytope (see [4],Chapter 3, Section 1, Theorem 4.) Let $\mathbf{v}$ be a vertex in $N(f) + N(g)$. By definition $\mathbf{v}$ is the intersection of a hyper-plane and $N(f) + N(g)$. If $\mathbf{u}$ is the unit-normal to the hyperplane, then $\mathbf{v}$ is a maximum with respect to $\succ_{\mathbf{u}}$ or $\succ_{-\mathbf{u}}$. Without loss of generality, assume $\mathbf{v}$ is a maximum with respect to $\succ_{\mathbf{u}}$. If we move $\mathbf{u}$ a small amount, then the hyper-plane with outward normal $\mathbf{u}$ and through $\mathbf{v}$ still intersects $N(f)+N(g)$ in $\mathbf{v}$ only. The set of points in $\mathbb{R}^n$ with rational dependent coordinates is the countable union of all $(n-1)$-dimensional vector subspaces with basis vectors in $\mathbb{Q}^n$, in particular it has zero n-dimensional measure. So the totally irrational vectors are dense in $\mathbb{R}^n$, and we can find $\mathbf{w}$ so that $\mathbf{w}$ is totally irrational and the hyper-plane through $\mathbf{v}$ with outward normal $\mathbf{w}$ hits P only in $\mathbf{v}$. We now order the elements of $N(f)$ and $N(g)$ with respect to $>_{\mathbf{w}}$. Since $N(f)$ is bounded, we can find a maximal element $\mathbf{a} \in N(f)$, which must be in $\partial N(f)$. If there were more than one maximal element by convexity we could find a line segment between them, which must be an edge. Continuing this edge to its endpoints we see that a non-zero scalar multiple of $\mathbf{w}$ is the difference between two lattice points, which is impossible since $\mathbf{w}$ is totally irrational. Similarly we see that $N(g)$ has a unique maximum $\mathbf{b}$ with respect to $>_{\mathbf{w}}$. Clearly these maximal points must be vertices. Thus if we look at the vertices, which must be lattice points, of $N(f), N(g)$ then $\mathbf{a}, \mathbf{b}$ are the maximum with respect to $>_{\mathbf{w}}$ of the vertices of $N(f), N(g)$ respectively. Thus by our earlier remark

$$\mathbf{a} + \mathbf{b} = \max(N(f) + N(g)) = \mathbf{v}$$

so the monomials corresponding to $\mathbf{a}, \mathbf{b}$ are the only ones whose product corresponds to $\mathbf{v}$. We need to check that the monomials corresponding to $\mathbf{a}, \mathbf{b}$ do not multiply together to be 0. If $c_1\widetilde{x^{\mathbf{a}}}, c_2\widetilde{x^{\mathbf{b}}}$ are any monomials with $c_1, c_2 \in R \setminus \{0\}$ then,

$c_1\widetilde{x^{\mathbf{a}}}c_2\widetilde{x^{\mathbf{b}}} = c_1c_2t(x^{\mathbf{a}}, y^{\mathbf{b}})x^{\mathbf{a}+\mathbf{b}}$ and $c_1c_2t(x^{\mathbf{a}}, y^{\mathbf{b}})$ is not zero, since R has no zero divisors. Thus $\mathbf{v} \in N(fg)$, and since $\mathbf{v}$ was an arbitrary vertex by taking convex hulls we conclude $N(fg) \supseteq N(f) + N(g)$. □

Corollary 3.2.1. *If R is a ring without zero divisors, and t is a twisting function on $\mathbb{Z}^n$, then $R^t[\mathbb{Z}^n]$ has no zero divisors.*

Proof. If $f, g \in R^t[\mathbb{Z}^n] \setminus \{0\}$ then $N(f), N(g) \neq \varnothing$, hence $N(fg) = N(f) + N(g) \neq \varnothing$. □

One could easily establish the above corollary using any monomial ordering on $\mathbb{Z}^n$, but Theorem 3.2.1 gives a much better quantitative result.

3.3. **Gauss's Lemma and the Main Result.** Recall that in a commutative unique factorization domain R, a greatest common divisor (denoted gcd) of a finite set $\{c_1, c_2, \ldots, c_m\} \subseteq R$ exists and is unique up to unit multiples. We set $\gcd(0) = 0$ and $\gcd(c_1, c_2, \ldots, c_m) = 1$ if $\gcd(c_1, c_2, \ldots, c_m)$ is a unit.

Definition 3.3.1. Let Γ be a group and let R be a commutative unique factorization domain, with t a twisting function on Γ. If $f \in R^t[\Gamma]$, write $f = \sum_{\gamma\in\Gamma} f_\gamma\widetilde{\gamma}$. Let $c(f) = \gcd(\{f_\gamma \colon \gamma \in \mathrm{Supp}(f)\})$ and call $c(f)$ the *content* of f. We say that f is *primitive* if $c(f) = 1$.

Under the preceding assumptions, $c(f) \in R$. Thus it is central in $R^t[\Gamma]$, since R is commutative. If $f \in R^t[\Gamma]$ we may write $f = c(f)f_0$ with f_0 primitive. Conversely if $f = cf_0$ with $c \in R$ and f_0 is primitive, then $c(f) = c$.

Lemma 3.3.1. *Let Γ be a group, and R a ring with group of units U. Suppose that t is a twisting function on Γ. If I is an two-sided ideal in R, let $\widetilde{I}$ be the two-sided ideal in $R^t[\Gamma]$ generated by all the elements of I, and let $\overline{U}$ be the group of units of R/I. Let $\overline{t}\colon \Gamma \times \Gamma \to \overline{U}$ be defined as $\overline{t}(x, y) = \overline{t(x, y)}$ Then*

$$R^t[\Gamma]/\widetilde{I} \cong (R/I)^{\overline{t}}[\Gamma].$$

Proof. Let $\phi\colon R^t[\Gamma] \to (R/I)^{\overline{t}}[\Gamma]$ be the homomorphism which for each $\gamma \in \Gamma$ sends $\widetilde{\gamma}$ to $\widetilde{\gamma}$ and sends $c \in R$ to $\overline{c} \in R/I$ (where $\overline{c}$ is the residue of c modulo I) for each $c \in R$. Observe that

$$\phi\left(\sum_{\gamma\in\Gamma} c_\gamma\widetilde{\gamma}\right) = \sum_{\gamma\in\Gamma} \overline{c_\gamma}\widetilde{\gamma} = 0$$

if and only if $c_\gamma \in I$ for all γ. This happens if and only if $\sum_{\gamma\in\Gamma} c_\gamma\widetilde{\gamma} \in \widetilde{I}$. Thus $\ker\phi = \widetilde{I}$ and ϕ is surjective, so the claim follows. □

By an *integral domain* we shall mean a commutative ring without zero divisors. Suppose R is a ring and a is central in R. Given $b \in R$ we say that *a divides b* and write $a|b$, if there is $c \in R$ such that $b = ac$. Since a is central $b = ca$, so there is no ambiguity about left or right divisors.

Proposition 3.3.1. *Let Γ be a group and suppose that for any integral domain R, every twisted group ring $R^t[\Gamma]$ has no zero divisors. Let R be an integral domain, and t a twisting function on Γ.*

(a) *Suppose p is prime in R. Then whenever $f, g \in R^t[\Gamma]$ and $p \nmid f, p \nmid g$, then $p \nmid fg$.*

(b)(Gauss's Lemma) *Assume R is a commutative unique factorization domain. If $f, g \in R^t[\Gamma]$ are primitive, then so is fg.*

(c) (Content Lemma) *Suppose R is a commutative unique factorization domain and $f, g \in R^t[\Gamma]$ then $c(fg) = c(f)c(g)$.*

Proof. (a) Since p is central, we can say $p \nmid f$ without ambiguity, and the two-sided ideal in $R^t[\Gamma]$ generated by p consists of multiples of p. Thus the desired claim is equivalent to the statement that $R^t[\Gamma]/(pR^t[\Gamma])$ has no zero divisors. Since p is prime, R/pR is an integral domain, and the desired claim follows by Lemma 3.3.1 and the hypothesis on Γ.

(b) Let $p \in R$ be irreducible. Since R is a unique factorization domain p is prime. Because f, g are primitive $p \nmid f$, and $p \nmid g$. By (a) $p \nmid fg$. Since $p \in R$ was an arbitrary irreducible element, we know fg is primitive.

(c) We can write $f = c(f)f_0, g = c(g)g_0$, where f_0, g_0 are primitive. Hence $fg = c(f)f_0c(g)g_0 = c(f)c(g)f_0g_0$ and f_0g_0 is primitive by (b); proving the desired claim (see the remark before the statement of Lemma 3.3.1). □

The hypothesis on Γ in the preceding proposition will certainly be satisfied if Γ is a *unique product group*, that is if for any two finite subsets A, B of Γ there is $y \in \Gamma$ which can be written uniquely as ab with $a \in A$ and $b \in B$. This is proved as follows. Let Γ be a unique product group , and R an integral domain with twisting function t. If $f, g \in R^t[\Gamma]$ then $\mathrm{Supp}(f)$ and $\mathrm{Supp}(g)$ are finite sets and hence there is an element $y \in \Gamma$ which can be written uniquely as ab with $a \in \mathrm{Supp}(f), b \in \mathrm{Supp}(g)$, and thus the term corresponding to ab cannot be cancelled in the product fg. It is known that any group which has a linear ordering preserved by right (or left) multiplication is a unique product group, and that the class of groups having such a ordering includes free groups and poly-infinite-cyclic groups (See [5], Chapter 13, Sections 1 and 2). For our next proposition, we will use the following lemma.

Lemma 3.3.2. *Suppose A is a ring which is also an algebra over the ring R. Suppose $\{a_i\}_{i\in I}$ is basis for A over R. Suppose S is a ring and $\phi\colon A \to S$ satisfies the following conditions*

(i) $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in A$,

(ii) $\phi(ra_i) = \phi(r)\phi(a_i)$, for all $i \in I$, and $r \in R$

(iii) $\phi(1) = 1$

(iv) $\phi(a_ia_j) = \phi(a_i)\phi(a_j)$, for all $i, j \in I$. Then ϕ is a ring homomorphism.

Proof. It suffices to check that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in A$. Given $x, y \in A$ since $\{a_i\}_{i\in I}$ is a basis, we know we may write

$$x = \sum_{i\in I} x_ia_i, \quad y = \sum_{i\in I} y_ia_i,$$

with $x_i, y_i \in R$ for all i, and all but finitely many of the x_i, y_i are non-zero. Then by our given assumptions,

$$\phi(xy) = \phi\left(\sum_{i,j} x_ia_iy_ja_j\right) = \sum_{i,j} \phi(x_i)\phi(a_i)\phi(y_j)\phi(a_j) =$$

$$\left(\sum_{i\in I} \phi(x_i)\phi(a_i)\right)\left(\sum_{i\in I} \phi(y_i)\phi(a_i)\right) = \phi(x)\phi(y).$$

□

Proposition 3.3.2. *Let Γ be a group, and let N be a central subgroup of Γ. Let R be a ring. Then*

$$R[\Gamma] \cong R[N]^t[\Gamma/N]$$

for some twisting function t.

Proof. Fix a coset representation $\Gamma/N = \{Na_i\}_{i\in I}$. For any $i, j \in I$ we have that $Na_iNa_j = Na_{i,j}$ for some $a_{i,j} \in \{a_i : i \in I\}$. Hence, $a_ia_j = n_{i,j}a_{i,j}$ for some $n_{i,j} \in N$. Define $t(Na_i, Na_j) = n_{i,j}$. We define $\phi\colon R[\Gamma] \to R[N]^t[\Gamma/N]$ as follows. For any $\gamma \in \Gamma$ we have $\gamma = n_\gamma a_{i(\gamma)}$, with $n_\gamma \in N$ and $i(\gamma) \in I$. Given $f = \sum_{\gamma\in\Gamma} c_\gamma \gamma$ with $c_\gamma \in R$ let $\phi(f) = \sum_{\gamma\in\Gamma} c_\gamma n_\gamma \widetilde{Na_{i(\gamma)}}$. The ring $R[\Gamma]$ is an algebra over R with basis Γ, and it follows from the previous lemma that ϕ is a homomorphism, (this uses the fact that N is central) it is also surjective. Suppose $\sum_{\gamma\in\Gamma} c_\gamma n_\gamma \widetilde{Na_{i(\gamma)}} = 0$. Then

$$\sum_{\gamma\in\Gamma} c_\gamma n_\gamma \widetilde{Na_{i(\gamma)}} = \sum_{i\in I}\left(\sum_{\gamma\in Na_i} c_\gamma n_\gamma\right)\widetilde{Na_i}.$$

By independence of $\{\widetilde{Na_i} : Na_i \in \Gamma/N\}$ over $R[N]$ we conclude for each i that $\sum_{\gamma\in Na_i} c_\gamma n_\gamma = 0$. For fixed i and $\gamma, \delta \in Na_i$ we have $n_\gamma = n_\delta$ implies that $\gamma = \delta$. So by independence of N over R we conclude that $c_\gamma = 0$ for all $\gamma \in \Gamma$. Thus ϕ is an isomorphism. □

We now prove the main theorem of this section.

Theorem 3.3.1. *Let Γ be a group and suppose N is a finitely generated torsion-free central subgroup such that $\{1\} \neq N \neq \Gamma$ and such that $R^t[\Gamma/N]$ has no zero divisors for all integral domains R and twisting functions t. Then Γ is principally ergodic.*

Proof. If $f = 0$, then $\mathbb{Z}[\Gamma]/\{0\} \cong \mathbb{Z}[\Gamma]$, so our claim follows since Γ is necessarily infinite. Suppose $f \neq 0$, and that $h \in \mathbb{Z}[\Gamma]$ is such that the orbit of h is finite in $\mathbb{Z}[\Gamma]/\mathbb{Z}[\Gamma]f$. Let $x \in \Gamma \setminus N$. Consider the set $\{\overline{xh}, \overline{x^2h}, \dots,\}$ where the bar denotes the residue modulo $\mathbb{Z}[\Gamma]f$. By assumption it must be finite. Hence there exists $n \in \mathbb{N}$ such that $x^nh \equiv h \mod \mathbb{Z}[\Gamma]f$. Thus there exists $g_1 \in \mathbb{Z}[\Gamma]$ such that $x^nh = h + g_1f$, i.e.

$$(x^n - 1)h = g_1f. \tag{3.3.1}$$

Similarly, letting $z \in N \setminus \{1\}$, we can find $m \in \mathbb{N}$ and $g_2 \in \mathbb{Z}[\Gamma]$ such that

$$(z^m - 1)h = g_2f. \tag{3.3.2}$$

Since N is a finitely generated torsion-free abelian group, it is isomorphic to $\mathbb{Z}^k$ for some $k \in \mathbb{N}$. Thus $\mathbb{Z}[N]$ is a unique factorization domain. By Proposition 3.3.2 for some twisting function t we have

$$\mathbb{Z}[\Gamma] \cong \mathbb{Z}[N]^t[\Gamma/N]. \tag{3.3.3}$$

Applying the Content Lemma to (3.3.1) we see that $c(h) = c(g_1)c(f)$, since $x \notin N$. Similarly using (3.3.2) we conclude that $(z^m - 1)c(h) = c(g_2)c(f)$, since $z \in N$. Combining we deduce that

$$(z^m - 1)c(g_1)c(f) = c(g_2)c(f).$$

Since f is nonzero, the content of f is nonzero. Since $\mathbb{Z}[N]$ is an integral domain we apply the cancellation law and find that $(z^m - 1)c(g_1) = c(g_2)$. Thus $(z^m - 1)|g_2$

so we can write $g_2 = (z^m - 1)q$, for some $q \in \mathbb{Z}[\Gamma]$. Using equation (3.3.2) and the fact that the assumptions imply that $\mathbb{Z}[\Gamma]$ has no zero divisors, (by (3.3.3) and the assumptions on Γ/N) we see that $h = qf \in \mathbb{Z}[\Gamma]f$. □

Let Γ be a group, recall that the upper central series $\{Z_n(\Gamma)\}$ is defined inductively with $Z_1(\Gamma)$ the center of Γ, and $Z_{n+1}(\Gamma)$ is defined by requiring that $Z_{n+1}(\Gamma)$ is the center of $\Gamma/\Gamma_n(\Gamma)$. The group Γ is said to be *n-step nilpotent* if there is an integer n such that $\Gamma = Z_n(\Gamma)$. In order to apply the preceding Theorem to torsion-free nilpotent groups we need the following three lemmas which are proved in [5]. In [5], these are Lemma 3.4.2, Lemma 11.1.3, and Lemma 13.1.6 respectively.

Lemma 3.3.3. *If Γ is a finitely generated nilpotent group, then all subgroups of Γ are finitely generated.*

Lemma 3.3.4. *Let Γ be a group whose center is torsion-free. Then for all $n \in \mathbb{N}$ we have $Z_{n+1}(\Gamma)/Z_n(\Gamma)$ is torsion-free abelian.*

Lemma 3.3.5. *Let Γ be a group. If there is a series*

$$\{1\} = \Gamma_0 \triangleleft \Gamma_1 \triangleleft \Gamma_2 \triangleleft \cdots \triangleleft \Gamma_n = \Gamma$$

with Γ_{i+1}/Γ_i torsion-free abelian, then Γ has a linear ordering preserved by right multiplication.

We now apply Theorem 3.3.1 to finitely-generated torsion-free nilpotent groups.

Theorem 3.3.2. *Let Γ be a finitely-generated, torsion-free, nilpotent group not isomorphic to the integers or the trivial group. Then Γ is principally ergodic.*

Proof. We show that Γ satisfies the hypothesis of Theorem 3.3.1. If Γ is abelian then since Γ is finitely generated and torsion-free our hypothesis implies that it is isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{N}$, and $n \geq 2$. Then Theorem 3.3.1 applies with $N = \mathbb{Z}$, using Corollary 3.2.1.

If Γ is k-step nilpotent with $k \geq 2$, then since Γ is nilpotent, $1 \neq Z_1(\Gamma) \neq \Gamma$ and $Z_1(\Gamma)$ is torsion-free since Γ is, it is also finitely generated by Lemma 3.3.3. By definition we have

$$\Gamma/Z_1(\Gamma) \triangleright \Gamma/Z_2(\Gamma) \cdots \triangleright \Gamma/Z_k(\Gamma) \cong \{1\}.$$

But

$$(\Gamma/Z_i(\Gamma))/(\Gamma/Z_{i+1}(\Gamma)) \cong Z_{i+1}(\Gamma)/Z_i(\Gamma),$$

which is torsion-free abelian by Lemma 3.3.4 . Thus $\Gamma/Z_1(\Gamma)$ has a linear ordering preserved by right multiplication by Lemma 3.3.5 , and is thus a unique product group. Thus Theorem 3.3.1 applies with $N = Z_1(\Gamma)$. □

For example, let $\mathbb{H}_n$ be the group of all upper-triangular integer matrices with ones on the diagonal, the group $\mathbb{H}_n$ is finitely generated, and we can show $\mathbb{H}_n$ is torsion-free nilpotent as follows. Consider

$$A = \begin{bmatrix} 1 & 0 & \dots & 1 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

that is A has ones on the diagonal, and in the upper right, but nowhere else. Then $\mathbb{Z} \cong \Gamma_1 = \langle A \rangle \subseteq Z_1(\mathbb{H}_n)$ (in fact $\langle A \rangle = Z_1(\mathbb{H}_n)$ but we will not need that). In $\mathbb{H}_n/\Gamma_1$ consider the residues of

$$A_1 = \begin{bmatrix} 1 & 0 & \dots & 1 & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}, \ A_2 = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 1 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}.$$

That is, A_1 only has 1's on the diagonal and in the first row and $n-1$st column, and A_2 only has 1's on the diagonal and in the second row and last column. Then $\mathbb{Z}^2 \cong \langle A_1\Gamma_1, A_2\Gamma_2 \rangle \subseteq Z_1(\mathbb{H}_n/\Gamma_1)$. Continuing diagonally we see that we have a series $\mathbb{Z} \cong \Gamma_1 \lhd \Gamma_2 \cdots \lhd \Gamma_{n-1} = \mathbb{H}_n$, with $\Gamma_i/\Gamma_{i-1} \subseteq Z_1(\mathbb{H}_n/\Gamma_{i-1})$ and Γ_i/Γ_{i-1} torsion-free. This implies that $\mathbb{H}_n$ is torsion-free nilpotent. For $n \geq 3$ this group is not isomorphic to the integers, so the preceding Theorem applies.

The preceding Theorem fails if $\Gamma = \mathbb{Z}$, if $f \in \mathbb{Z}[\mathbb{Z}] = \mathbb{Z}[x^{\pm 1}]$ has a root which is a root of unity, then we can find a divisor p of f, $g \in \mathbb{Z}[x^{\pm 1}]$ and $n \in \mathbb{Z} \setminus \{0\}$ such that

$$(x^n - 1) = gp.$$

If we write $f = pq$, the

$$(x^n - 1)q = gf.$$

Then $q \notin \mathbb{Z}[\mathbb{Z}]f$ but the orbit of q in $\mathbb{Z}[\mathbb{Z}]/\mathbb{Z}[\mathbb{Z}]f$ is $1, x, x^2, \dots, x^n$.

We leave it as an exercise to verify that for $f \in \mathbb{Z}[\mathbb{Z}]$, the corresponding action α_f is ergodic if and only if f has a root which is a root of unity.

3.4. **General Facts About Ergodicity.**

So far in our discussion of this problem we have assumed that our groups are finitely generated. We now solve the problem for groups that are not finitely generated.

Theorem 3.4.1. *Let Γ be a group which is not finitely generated, then Γ is principally ergodic.*

Proof. Let $f \in \mathbb{Z}[\Gamma]$ and $p \in \mathbb{Z}[\Gamma]$ have finite orbit in $\mathbb{Z}[\Gamma]/\mathbb{Z}[\Gamma]f$. Let Γ_0 be the group generated by the elements in $\mathrm{Supp}(f) \cup \mathrm{Supp}(p)$. Since Γ is not finitely generated, we may construct a sequence of groups $\{\Gamma_n\}$ such that $\Gamma_n \subseteq \Gamma_{n+1}$ and Γ_{n+1} is generated over Γ_n by a single element $\gamma_{n+1} \in \Gamma \setminus \Gamma_n$. For all $n \in \mathbb{N}$, let $\Gamma_n p = \{\gamma p + \mathbb{Z}[\Gamma]f : \gamma \in \Gamma_n\}$ and let $\Gamma p = \{\gamma p + \mathbb{Z}[\Gamma]f : \gamma \in \Gamma\}$. Suppose that Γp is finite. Then since $\Gamma_n p \subseteq \Gamma_{n+1} p$ we have that

$$|\Gamma_0 p| \leq |\Gamma_1 p| \leq |\Gamma_2 p| \leq \cdots.$$

Also $|\Gamma_n p| \leq |\Gamma p| < \infty$. Since $|\Gamma_n p|$ is a bounded increasing sequence of integers there exists $N \in \mathbb{N}$ such that

$$|\Gamma_N p| = |\Gamma_{N+1} p| = |\Gamma_{N+2} p| = \cdots.$$

Since these sets have the same finite size and $\Gamma_n p \subseteq \Gamma_{n+1} p$ we have

$$\Gamma_N p = \Gamma_{N+1} p = \Gamma_{N+2} p = \cdots.$$

Thus $\gamma_{N+1} p \equiv yp \mod \mathbb{Z}[\Gamma]\mathrm{f}$ for some $y \in \Gamma_N$. Thus $(\gamma_{N+1} - y)p = gf$ for some $g \in \mathbb{Z}[\Gamma]$. Write $g = g_1 + g_2$ where $\mathrm{Supp}(g_1) \subseteq \Gamma_N$ and $\mathrm{Supp}(g_2) \cap \Gamma_N = \varnothing$. Then

$$\gamma_{N+1} p - g_2 f = g_1 f + yp. \tag{3.4.1}$$

Since $\mathrm{Supp}(p), \mathrm{Supp}(f) \subseteq \Gamma_N$ the support of the right hand side of (3.4.1) is entirely contained in Γ_N. However every element in the support of the left hand side of (3.4.1) takes the form ab with $b \in \Gamma_N$ and $a \notin \Gamma_N$, thus the support of the left hand side is disjoint from Γ_N. Hence the right hand side of (3.4.1) must vanish so that $\gamma_{N+1}p = g_1 f$ and thus $p = \gamma_{N+1}^{-1} g_1 f \in \mathbb{Z}[\Gamma]f$. □

We can use the same technique as above to deduce a general fact about relating ergodicity of actions by some group to a group it has finite index in.

Theorem 3.4.2. *Let Γ be a group and Δ a subgroup of Γ; assume $[\Gamma : \Delta] < \infty$. If Γ is principally ergodic, then so is Δ.*

Proof. We prove the contrapositive, suppose there exists $f \in \mathbb{Z}[\Delta]$ and $p \in \mathbb{Z}[\Delta] \setminus \mathbb{Z}[\Delta]f$ such that $\{\delta p + \mathbb{Z}[\Delta]f : \delta \in \Delta\}$ is finite. We claim that $p \notin \mathbb{Z}[\Gamma]f$, suppose $q \in \mathbb{Z}[\Gamma]$ is such that $p = qf$. Then write $q = q_1 + q_2$ where $q_1 \in \mathbb{Z}[\Delta]$ and $\mathrm{Supp}(q_2) \subseteq \Gamma \backslash \Delta$. Then $p - q_1 f = q_2 f$, and $\mathrm{Supp}(q_2) \subseteq \Gamma \backslash \Delta$, and since $\mathrm{Supp}(f) \subseteq \Delta$ we have $\mathrm{Supp}(q_2 f) \subseteq \Gamma \setminus \Delta$, but $q_2 f = p - q_1 f \in \mathbb{Z}[\Delta]$. These two facts imply that $q_2 f = 0$, hence $p = q_1 f$, a contradiction. Thus $p \notin \mathbb{Z}[\Gamma]f$. Now if the Δ-orbit of p is $\{\delta_1 p + \mathbb{Z}[\Delta]f, \delta_2 p + \mathbb{Z}[\Delta]f, \ldots, \delta_n p + \mathbb{Z}[\Delta]f\}$ and $\Gamma/\Delta = \{a_1\Delta, a_2\Delta, \ldots, a_m\Delta\}$, then the Γ-orbit of p is:

$$\begin{array}{cccc}
\delta_1 p + \mathbb{Z}[\Gamma]f, & \delta_2 p + \mathbb{Z}[\Gamma]f, & \ldots & \gamma_n p + \mathbb{Z}[\Gamma]f \\
a_1\delta_1 p + \mathbb{Z}[\Gamma]f, & a_1\delta_2 p + \mathbb{Z}[\Gamma]f, & \ldots & a_1\delta_n p + \mathbb{Z}[\Gamma]f \\
\vdots & \vdots & \vdots & \vdots \\
a_m\delta_1 p + \mathbb{Z}[\Gamma]f, & a_1\delta_2 p + \mathbb{Z}[\Gamma]f, & \ldots & a_m\gamma_n p + \mathbb{Z}[\Gamma]f.
\end{array}$$

So the Γ-orbit of p is finite. □

4. Mixing and The Heisenberg Group

In this section, we investigate when the actions we have constructed are mixing. We first handle the case of a $\mathbb{Z}^n$-action and then apply this to give a sufficient condition for a mixing $\mathbb{H}$-action. As in the case of ergodicity above, we see that elements in $\mathbb{Z}[\Gamma]$ like $\gamma - 1$ are important to our investigation. For this reason we find the irreducible factorization of $x^{\mathbf{a}} - 1$ with $\mathbf{a} \in \mathbb{Z}^n$.

4.1. Mixing $\mathbb{Z}^d$-Actions.

Recall that the d-th cyclotomic polynomial ϕ_d is defined by

$$\phi_d(x) = \prod_{j:\gcd(j,d)=1, 1 \le j \le d} (x - e^{2\pi i j/n})$$

and is a monic, irreducible, (over $\mathbb{Z}[x]$ and $\mathbb{Z}[x^{\pm 1}]$) integral polynomial. Further

$$x^n - 1 = \prod_{d|n} \phi_d(x),$$

is the irreducible factorization of $x^n - 1$.

Definition 4.1.1. A *generalized cyclotomic polynomial* is a Laurent polynomial of the form $\phi_d(x^{\mathbf{a}})$ for some $d \in \mathbb{N}$, where $\mathbf{a} \in \mathbb{Z}^n$ satisfies $\gcd\{a_1, a_2, \ldots, a_n\} = 1$.

Lemma 4.1.1. *Every generalized cyclotomic polynomial is irreducible in $\mathbb{Z}[\mathbb{Z}^n]$.*

Proof. Let $d \in \mathbb{N}$ and $\mathbf{a} \in \mathbb{Z}^n$ satisfy $\gcd\{a_1, a_2, \ldots, a_n\} = 1$. Suppose $\phi_d(x^{\mathbf{a}}) = fg$. By multiplying by units, we may assume without loss of generality that 1 has nonzero coefficient in f and g. Applying the Newton Polyhedron Theorem, we conclude that

$$N(\phi_d(x^{\mathbf{a}})) = N(f) + N(g).$$

Since $\{0\} \in N(f), \{0\} \in N(g)$ we have $N(f) \subseteq N(f) + N(g)$ and similarly $N(g) \subseteq N(f)+N(g)$. By the above equation, $N(f)+N(g)$ lies entirely in the line spanned by $\mathbf{a}$ and so $N(f)$ and $N(g)$ must be contained in this line, since $N(f) \subseteq N(f)+N(g)$ and $N(g) \subseteq N(f) + N(g)$. Since $\mathbf{a}$ has relatively prime coordinates, it spans the lattice points in this line as a subspace of the module $\mathbb{Z}^n$. Since $N(f)$ and $N(g)$ consist of lattice points in this line, it follows that we can find polynomials $\widetilde{f}, \widetilde{g}$ such that $f = \widetilde{f}(x^{\mathbf{a}}), g = \widetilde{g}(x^{\mathbf{a}})$. Then

$$\phi_d(x^{\mathbf{a}}) = \widetilde{f}(x^{\mathbf{a}})\widetilde{g}(x^{\mathbf{a}}),$$

by irreducibility of ϕ_d in the one-variable case we conclude that one of $\widetilde{f}$, or $\widetilde{g}$ is a unit, so one of f or g is a unit. □

Corollary 4.1.1. *Given $\mathbf{a} \in \mathbb{Z}^n$ write $\mathbf{a} = d\mathbf{a}'$ with $\mathbf{a}'$ having relatively prime coordinates. The irreducible factorization for $x^{\mathbf{a}} - 1$ is*

$$\prod_{j|d} \phi_j(x^{\mathbf{a}'}).$$

The following is known, but we reproduce a proof for completeness.

Proposition 4.1.1. *For any $f \in \mathbb{Z}[\mathbb{Z}^n]$, the corresponding action is not mixing if and only if f is divisible by some generalized cyclotomic polynomial in $\mathbb{Z}[\mathbb{Z}^n]$.*

Proof. If $f = 0$, then α_f is mixing for trivial reasons, so suppose $f \neq 0$. Suppose α_f is not mixing. Let $p \in \mathbb{Z}[\mathbb{Z}^n] \setminus \mathbb{Z}[\mathbb{Z}^n]f$ have infinite stabilizer in $\mathbb{Z}[\mathbb{Z}^n]f$. Then as before we can find $\mathbf{a} \in \mathbb{Z}^n$ and $g \in \mathbb{Z}[\mathbb{Z}^n]$ such that

$$(x^{\mathbf{a}} - 1)p = gf.$$

Write $\mathbf{a} = d\mathbf{a}'$ where $\mathbf{a}'$ has relatively prime coordinates. Then

$$((x^{\mathbf{a}'})^d - 1)p = gf.$$

Since $p \notin \mathbb{Z}[\mathbb{Z}^n]f$ it follows that $(x^{\mathbf{a}} - 1) \nmid g$. Thus by the above corollary there is some $j|d$ such that $\phi_j(x^{\mathbf{a}'}) \nmid g$. Since $\phi_j(x^{\mathbf{a}'})$ divides the left-hand side of the above equation, and is prime and does not divide g, it must divide f. Conversely, suppose $f \in \mathbb{Z}[\mathbb{Z}^n]$ has $f = \phi_j(x^{\mathbf{a}})p$ for some $\mathbf{a}$ with relatively prime coordinates. Then $p \notin \mathbb{Z}[\mathbb{Z}^n]f$, and we can find $g \in \mathbb{Z}[\mathbb{Z}^n]$ such that $g\phi_j(x^{\mathbf{a}}) = x^{j\mathbf{a}} - 1$. Then

$$(x^{j\mathbf{a}} - 1)p = gf$$

so $\mathrm{Stab}(p) \supseteq \{x^{nj\mathbf{a}} \colon n \in \mathbb{N}\}$ and is thus infinite. So α_f is not mixing. □

For $n = 1$, we know by the above proposition that α_f is not mixing if and only if f has a root which is a root of unity. As we remarked before, f having a root of unity is equivalent to α_f not being ergodic. So in the case $n = 1$, we know α_f is ergodic if and only if α_f is mixing. This fails for $n > 1$, because α_f is always ergodic (by Theorem 3.3.2), whereas the above proposition shows α_f can fail to be mixing.

4.2. **Mixing in The Heisenberg Group.**

In order to apply the above to the case of $\mathbb{H}$ we will need to classify the automorphisms of $\mathbb{H}$.

Proposition 4.2.1. *Any automorphism, ψ, of $\mathbb{H}$ takes the form*

$$\begin{aligned}\psi(x) &= x^{a_1}y^{b_1}z^{c_1}\\ \psi(y) &= x^{a_2}y^{b_2}z^{c_2}\\ \psi(z) &= z^{\varepsilon},\end{aligned} \tag{4.2.1}$$

where $\varepsilon = a_1b_2 - a_2b_1$ with $a_i, b_i, c_i \in \mathbb{Z}$ and the only restriction is that $\varepsilon = \pm 1$, and that ψ is extended multiplicatively. Conversely, suppose ψ satisfies 4.2.1 *with $a_i, b_i, c_i \in \mathbb{Z}$ and $\varepsilon = a_1b_2 - a_2b_1 = \pm 1$. If ψ is extended multiplicatively, it is an automorphism.*

Proof. Let ψ be an automorphism of $\mathbb{H}$. Since $\langle z\rangle$ is the center of $\mathbb{H}$ it is a characteristic subgroup and thus $\phi(\langle z\rangle) = \langle z\rangle$. Let

$$\begin{aligned}\psi(x) &= x^{a_1}y^{b_1}z^{c_1}\\ \psi(y) &= x^{a_2}y^{b_2}z^{c_2}.\\ \psi(z) &= z^{\varepsilon},\end{aligned}$$

with $\varepsilon = \pm 1$. Then

$$\psi(y)\psi(x) = x^{a_1+a_2}y^{b_1+b_2}z^{c_1+c_2+a_1b_2},$$

and

$$\psi(x)\psi(y)\psi(z) = x^{a_1+a_2}y^{b_1+b_2}z^{c_1+c_2+\varepsilon+a_2b_1}.$$

Since $yx = xyz$ we must have that $\varepsilon = a_1b_2 - a_2b_1$. Conversely, suppose ψ satisfies (4.2.1). By direction computation and the formula $(x^ay^bz^c)^n = (x^{an}y^{bn}z^{cn+\binom{n}{2}ab})$, we find ψ is a homomorphism. Suppose $\psi(x^ay^bz^c) = 1$. Since the x and y exponents of $\psi(x^ay^bz^c)$ corresponds to multiplying $\begin{bmatrix}a\\ b\end{bmatrix}$ by the matrix

$$\begin{bmatrix}a_1 & a_2\\ b_1 & b_2\end{bmatrix},$$

whose determinant is ± 1 we conclude that $a = b = 0$. But $\psi(z^c) = z^{c\varepsilon}$, so $c\varepsilon = 0$ and thus $x^ay^bz^c = 1$, so ψ is injective. To see that ψ is surjective suppose that $x^ay^bz^c \in \mathbb{H}$. Since $a_1b_2 - a_2b_1 = \pm 1$ we can find integers α, β such that

$$\begin{bmatrix}a_1 & a_2\\ b_1 & b_2\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}a\\ b\end{bmatrix}.$$

Then $\psi(x^\alpha y^\beta) = x^ay^bz^{c'}$, for some $c' \in \mathbb{Z}$. Setting $d = (c - c')/\varepsilon$ we have $\psi(x^\alpha y^\beta z^d) = x^ay^bz^c$, so ψ is an automorphism. □

Proposition 4.2.2. *Let $x^ay^bz^c \in \mathbb{H}$ then there exists $\psi \in Aut(\mathbb{H})$ such that $\psi(x^ay^bz^c) = x^nz^k$ for some $n, k \in \mathbb{Z}$.*

Proof. If $b = 0$, this is clear. If $a = 0$ then the automorphism defined by $x \mapsto y, y \mapsto x, z \mapsto z^{-1}$ works. So suppose $a, b \neq 0$. Let $d = \gcd(a, b) \neq 0$, and $l = \operatorname{lcm}(a, b) \neq 0$. Let $a_1, a_2 \in \mathbb{Z}$ be such that $aa_1 + ba_2 = d$, and $b_1, b_2 \in \mathbb{Z}$ be such that $-b_1a = b_2b = l$. Then

$$a_1b_2 - a_2b_1 = a_1\frac{l}{b} + a_2\frac{l}{a} = \frac{l}{ab}(aa_1 + a_2b) = \frac{ld}{ab} = 1.$$

By the preceding proposition we may define $\psi \in Aut(\mathbb{H})$ by requiring that

$$\psi(x) = x^{a_1}y^{b_1}$$
$$\psi(y) = x^{a_2}y^{b_2}$$
$$\psi(z) = z.$$

By direct computation $\psi(x^a y^b z^c) = x^d z^k$ for some $k \in \mathbb{Z}$. □

Recall that a subset of a ring R is a *right ideal* if it contains 0, and is closed under addition and right multiplication by elements of R. Similarly we have a notion of left ideal. A ring R is *right Noetherian* if every increasing chain of right ideals eventually stabilizes, with similar notions for left Noetherian. Given a ring R and $a \in R$ we will use either $\langle a\rangle_r$ or aR for the right ideal generated by a, with similar notations Ra, and $\langle a\rangle_l$ for left ideals (and multiply-generated left or right ideals). We reserve $\langle a\rangle$ for the two-sided ideal generated by a, (again with similar notation for multiply-generated two-sided ideals).

Lemma 4.2.1. *Let R be a ring without zero-divisors, and suppose $a \in R \setminus \{0\}$ has no right inverse. If R is a right-Noetherian ring, then*

$$\bigcap_{n=1}^{\infty} Ra^n = \{0\}.$$

Proof. Suppose $b \in \bigcap_{n=1}^{\infty} Ra^n \setminus \{0\}$, then $b = r_n a^n$ for some $r_n \in R$. Then $r_{n+1}a^{n+1} = r_n a^n$, since R has no zero divisors and $a \neq 0$ we conclude that $r_{n+1}a = r_n$, so

$$\langle r_n\rangle_r = \langle r_{n+1}a\rangle_r \subseteq \langle r_{n+1}\rangle_r.$$

If $r_{n+1} \in \langle r_n\rangle_r$ then for some $q \in R$ we have

$$r_{n+1} = r_n q = r_{n+1}aq.$$

Since $b \neq 0$, we have $r_{n+1} \neq 0$ so the above implies $1 = aq$, contrary to the hypothesis that a has no right inverse. Thus

$$\langle r_1\rangle_r \subsetneq \langle r_2\rangle_r \subsetneq \cdots$$

and R is not right Noetherian. □

The above theorem is false if we drop the assumption that R has no zero divisors, for instance if $R = \mathbb{Z}/6\mathbb{Z}$ then

$$\bigcap_{n=1}^{\infty} 2^n R = 2R \cap 4R = \{0, 2, 4\},$$

and 2 is not invertible modulo 6.

The above theorem is also false if we drop the assumption that R is right Noetherian. Let

$$R = \mathbb{Z}\left[x, \frac{2}{x^n} : n \in \mathbb{N}\right]$$

Then

$$2 \in \bigcap_{n=1}^{\infty} x^n R \setminus \{0\}$$

and x is not a unit in R. If x were a unit in R, then we could find $p, q \in \mathbb{Z}[x]$ such that

$$x(p(x) + 2q(1/x)) = 1$$

letting d be the degree of q, we find

$$x^d p(x) + 2x^d q(1/x) - x^{d-1} = 0.$$

But this polynomial is not the zero polynomial, for if q_1 is the linear term of q, the coefficient of x^{d-1} in the above polynomial is $2q_1 - 1 \neq 0$, so we have a contradiction.

We now give a necessary condition for any $f \in \mathbb{Z}[\mathbb{H}]$ to have a corresponding action α_f which is not mixing, which of course gives a sufficient for α_f to be mixing.

Since $\langle z \rangle$ is the center of $\mathbb{H}$ it is not difficult to see that

$$\mathbb{Z}[\mathbb{H}]/\langle z-1 \rangle \cong \mathbb{Z}[\mathbb{H}/\langle z \rangle] \cong \mathbb{Z}[\mathbb{Z}^2].$$

By standard abuse of terminology, we identify $\mathbb{Z}[\mathbb{H}]/\langle z-1 \rangle$ with $\mathbb{Z}[\mathbb{Z}^2]$.

Lemma 4.2.2. *Let $f \in \mathbb{Z}[\mathbb{H}] \setminus \{0\}$. If α_f is not mixing, then either $\phi_d(z^{\pm 1}) | f$ for some $d \in \mathbb{N}$ or there exists elements $\gamma \in \mathbb{H} \setminus \langle z \rangle$, and $g \in \mathbb{Z}[\mathbb{H}] \setminus \langle z-1 \rangle$, and $p \in \mathbb{Z}[\mathbb{H}] \setminus \mathbb{Z}[\mathbb{H}]f$ such that*

$$(\gamma - 1)p = gf$$

and $\overline{f} \nmid \overline{p}$, where $\overline{f}, \overline{p}$ are the residues of f, p modulo $z-1$.

Proof. Suppose α_f is not mixing, then as in the proof of Theorem 3.3.1 we may find $p \in \mathbb{Z}[\mathbb{H}] \setminus \langle z-1 \rangle$, and $g \in \mathbb{Z}[\mathbb{H}] \setminus \{0\}$ and $\gamma \in \mathbb{H} \setminus \{1\}$ such that

$$(\gamma - 1)p = gf. \tag{4.2.2}$$

First suppose $\gamma \in \langle z \rangle$ say $\gamma = z^k$ for some $k \in \mathbb{Z} \setminus \{0\}$. Since the center of $\mathbb{H}$ is $< z >$ we apply the Content Lemma to conclude that

$$(z^k - 1)c(p) = c(g)c(f)$$

If $(z^k - 1) | c(g)$, then $(z^k - 1) | g$ and cancelling $(z^k - 1)p = gf$ we conclude $p \in \mathbb{Z}[\mathbb{H}]f$ a contradiction. So $z^k - 1 \nmid c(g)$ and we can find $d | k$ such that $\phi_d(z^{\pm 1}) | c(f)$. This implies $\phi_d(z^{\pm 1}) | f$.

Now suppose $\gamma \notin \langle z \rangle$ and that for all d we have $\phi_d(z^{\pm 1}) \nmid f$. Then in particular $z - 1 \nmid f$. By applying an automorphism to (4.2.2) we may assume, without loss of generality, that $\gamma = x^n z^k$ for some $n, k \in \mathbb{Z}$ (note that any automorphism sends either z to z or z to z^{-1} and thus fixes $\langle z-1 \rangle$) so that

$$(x^n z^k - 1)p = gf. \tag{4.2.3}$$

By hypothesis $(z-1) \nmid f$, so applying the Content Lemma and cancelling common factors of $z-1$ dividing p or g we may assume that $(z-1) \nmid p$ and $(z-1) \nmid g$. Suppose we can find $\widetilde{g}, \widetilde{p}$ such that $\overline{(x^n z^k - 1)} \nmid \overline{\widetilde{g}} \mod z-1$ and

$$(x^n z^k - 1)\widetilde{p} = \widetilde{g}f. \tag{4.2.4}$$

Then $\overline{f} \nmid \overline{\widetilde{p}}$, and applying Proposition 4.1.1 gives the desired conclusion. It remains to show we can find such a $\widetilde{g}, \widetilde{p}$. If g satisfies $\overline{(x^n z^k - 1)} \nmid g$, then we are done. If not, then we can find q such that $\overline{g} = \overline{(x^n z^k - 1)}\overline{q}$, since $\overline{g} \neq 0$ we have $\overline{q} \neq 0$. Thus

$$(\overline{(x^n z^k - 1)}\overline{p} = \overline{(x^n z^k - 1)}\overline{q}\overline{f}$$

so since $\overline{f}, \overline{q} \neq 0$ we have $\overline{p} = \overline{q}\overline{f}$. Thus we can find $g_1, p_1 \in \mathbb{Z}[\mathbb{H}] \setminus \langle z-1 \rangle$ and $\alpha, \beta \in \mathbb{N}$ such that $g = (x^n z^k - 1)q + (z-1)^\alpha g_1$ and $p = qf + (z-1)^\beta p_1$. By expanding (4.2.3) and cancelling, (since $\mathbb{Z}[\mathbb{H}]$ has no zero divisors by Corollary 3.2.1) we conclude

$$(x^n z^k - 1)p_1 = g_1 f.$$

(Note that $\alpha=\beta$ by the Content Lemma since $z-1\nmid f$.) If $\overline{(x^nz^k-1)}\nmid\overline{g_1}$, then we are done, else for some $q_1,g_2\in\mathbb{Z}[\mathbb{H}]$ we have $g_1=(x^nz^k-1)q_1+(z-1)g_2$. By definition of g_1 we have

$$g=(x^nz^k-1)(q+(z-1)^\alpha q_1)+(z-1)^{\alpha+1}g_2\in\langle x^nz^k-1,(z-1)^2\rangle_r.$$

Continuing we may find sequences $\{g_N\},\{p_N\}$ satisfying

$$(x^nz^k-1)p_N=g_Nf,$$

and either $\overline{(x^nz^k-1)}\nmid\overline{g_n}$ (and we are done in this case), or

$$g\in\langle x^nz^k-1,(z-1)^N\rangle_r.$$

Thus either the sequence produces a desired g_N or

$$g\in\bigcap_{N=1}^{\infty}\langle x^nz^k-1,(z-1)^N\rangle_r.$$

We show the latter is impossible. Suppose

$$g\in\bigcap_{N=1}^{\infty}\langle x^nz^k-1,(z-1)^N\rangle_r$$

write $g=\sum_i g^{(i)}y^i$ with $g^{(i)}\in\mathbb{Z}[x^{\pm1},z^{\pm1}]$ (the (i) is not an exponent, and is meant to distinguish g_i and $g^{(i)}$). Then since $g\in\bigcap_{N=1}^{\infty}\langle x^nz^k-1,(z-1)^N\rangle_r$ we must have for all i that

$$g^{(i)}\in\bigcap_{N=1}^{\infty}\left((x^nz^k-1)\mathbb{Z}[x^{\pm1},z^{\pm1}]+(z-1)^N)\mathbb{Z}[x^{\pm1},z^{\pm1}]\right).$$

Write $(n,k)=d(n',k')$ where $\gcd(n',k')=1$. Then by Corollary 4.1.1 we have

$$\bigcap_{N=1}^{\infty}\left((x^nz^k-1)\mathbb{Z}[x^{\pm1},z^{\pm1}]+(z-1)^N)\mathbb{Z}[x^{\pm1},z^{\pm1}]\right)\subseteq$$

$$\bigcap_{N=1}^{\infty}\bigcap_{j|d}\left(\phi_j(x^{n'}z^{k'})\mathbb{Z}[x^{\pm1},z^{\pm1}]+(z-1)^N\mathbb{Z}[x^{\pm1},z^{\pm1}]\right)=$$

$$\bigcap_{j|d}\bigcap_{N=1}^{\infty}\left(\phi_j(x^{n'}z^{k'})\mathbb{Z}[x^{\pm1},z^{\pm1}]+(z-1)^N\mathbb{Z}[x^{\pm1},z^{\pm1}]\right).$$

Since $\phi_j(x^{n'}z^{k'})$ is prime, for all j we have $\mathbb{Z}[x^{\pm1},z^{\pm1}]/\langle\phi_j(x^{n'}z^{k'})\rangle$ is an integral domain, and is Noetherian, since $\mathbb{Z}[x^{\pm1},z^{\pm1}]$ is. Further $z-1$ is not a unit modulo $\phi_j(x^{n'}z^{k'})\mathbb{Z}[x^{\pm1},z^{\pm1}]$. For if $1=\phi_j(x^{n'}z^{k'})k_1+(z-1)k_2$, with $k_1,k_2\in\mathbb{Z}[x^{\pm1},z^{\pm1}]$ then $1\equiv\phi_j(x^{n'})k_2 \mod z-1$, which is impossible since

$$\mathbb{Z}[x^{\pm1},z^{\pm1}]/\langle z-1\rangle\cong\mathbb{Z}[x^{\pm1}],$$

and $\phi_j(x^{n'})$ is not a unit in $\mathbb{Z}[x^{\pm1}]$. Thus by Lemma 4.2.1 applied to the ring $\mathbb{Z}[x^{\pm1},z^{\pm1}]/\langle\phi_j(x^{n'}z^{k'}\rangle$ we conclude that for all j

$$\bigcap_{N=1}^{\infty}\left(\phi_j(x^{n'}z^{k'})\mathbb{Z}[x^{\pm1},z^{\pm1}]+(z-1)^N\mathbb{Z}[x^{\pm1},z^{\pm1}]\right)=\phi_j(x^{n'}z^{k'})\mathbb{Z}[x^{\pm1},z^{\pm1}].$$

Thus for all i we have

$$g^{(i)} \in \bigcap_{j|d} \phi_j(x^{n'}z^{k'})\mathbb{Z}[x^{\pm 1}, z^{\pm 1}] = (x^n z^k - 1)\mathbb{Z}[x^{\pm 1}, z^{\pm 1}].$$

Since this is true for all i, we must have $g \in (x^n z^k - 1)\mathbb{Z}[\mathbb{H}]$. But applying the cancellation law to (4.2.3) we conclude $p \in \mathbb{Z}[\mathbb{H}]f$, a contradiction. Thus there must be some N such that $\overline{(x^n z^k - 1)} \nmid \overline{g_N}$, as noted before this completes the proof. □

Corollary 4.2.1. *Let $f \in \mathbb{Z}[\mathbb{H}] \setminus \{0\}$. If α_f is not mixing, then either $\phi_d(z^{\pm 1})|f$ for some $d \in N$ or $\overline{f}$, the residue of f modulo $\langle z - 1\rangle$, is divisible by a generalized cyclotomic in $\mathbb{Z}[\mathbb{Z}^2]$.*

Proof. If f is not divisible by $\phi_d(z^{\pm 1})|f$ for some $d \in \mathbb{N}$, then by Lemma 4.2.2, we can find elements $g \in \mathbb{Z}[\mathbb{H}] \setminus \langle z - 1\rangle$, and $p \in \mathbb{Z}[\mathbb{H}] \setminus \langle z - 1\rangle$ and $\gamma \in H \setminus \langle z\rangle$, with $\overline{f} \nmid \overline{p}$ such that

$$(\gamma - 1)p = gf.$$

Taking residues modulo $z - 1$, we have

$$(\overline{\gamma} - 1)\overline{p} = \overline{g}\overline{f}.$$

Since $\mathbb{Z}[\mathbb{H}]/\langle z - 1\rangle \cong \mathbb{Z}[\mathbb{Z}^2]$, and $\overline{\gamma} \neq 1 \mod z - 1$, this says that $\overline{\gamma} \in \mathrm{Stab}(\overline{p})$ for the action of $\mathbb{Z}^2$ on $\mathbb{Z}[\mathbb{Z}^2]/\mathbb{Z}^2[\mathbb{Z}^2]f$. Since $\gamma - 1, p, g$ and f are not 0 modulo $z - 1$, and $\overline{f} \nmid \overline{p}$, applying Proposition 4.1.1 we find that $\overline{f}$ is divisible by a generalized cyclotomic polynomial in $\mathbb{Z}[\mathbb{Z}^2]$. □

One might hope that the condition stated in the above corollary is both necessary and sufficient, but an example shows that this is not true. Consider $f = x + z - 2 \in \mathbb{Z}[\mathbb{H}]$. Then $f \equiv x - 1 \mod z - 1$, which is a generalized cyclotomic polynomial. However α_f is still mixing. Suppose that α_f is not mixing, then by Lemma 4.2.2, we can find $p \in \mathbb{Z}[\mathbb{H}] \setminus \langle z - 1\rangle$, and $\gamma \in \mathbb{H} \setminus \langle z\rangle$ with $\overline{x} - 1 \nmid \overline{p}$ such that

$$(\gamma - 1)p = gf.$$

Taking residues modulo $z - 1$, we find

$$(\overline{\gamma} - 1)\overline{p} = \overline{g}(x - 1).$$

Since $x - 1 \nmid p$, this equation tells us that $\overline{x} - 1|\overline{\gamma} - 1$, so that $\gamma = x^n z^k$, for some $n, k \in \mathbb{Z}$, with $n \neq 0$. Writing $p = \sum_j p_j y^j, g = \sum_j g_j y^j$ with $p_j, g_j \in \mathbb{Z}[x^{\pm 1}, z^{\pm 1}]$, we have that

$$\sum_j (x^n z^k - 1)p_j y^j = \sum_j g_j y^j(x + z - 2) = \sum_j g_j(xz^j + z - 2)y^j.$$

Equating coefficients

$$(x^n z^k - 1)p_j = g_j(xz^j + z - 2), \tag{4.2.5}$$

for all j. We claim that $xz^j + z - 2$ is irreducible in $\mathbb{Z}[x^{\pm 1}, z^{\pm 1}]$. Suppose

$$xz^j + z - 2 = q_1 q_2,$$

with $q_1, q_2 \in \mathbb{Z}[x^{\pm 1}, z^{\pm 1}]$. If we think of f, q_1 and q_2 as elements of $\mathbb{Z}[x^{\pm 1}][z^{\pm 1}]$, we see that the x-degree of q_1, q_2 have to add up to the x-degrees of f. So by multiplying by units, we may assume one of q_1, q_2 say q_1 takes the form $q_1 = xp_1(z) + p_2(z)$ and $q_2 \in \mathbb{Z}[z^{\pm 1}]$. Then

$$xz^j + z - 2 = xp_1(z)q_2 + p_2(z)q_2$$

and so $p_1(z)q_2 = z^j$ and each of $p_1(z), q_2$ is a unit. Thus $xz^j + z - 2$ is irreducible in $\mathbb{Z}[x^{\pm 1}, z^{\pm 1}]$, further it is not a cyclotomic polynomial. Therefore, by (4.2.5) we find that $x^n z^k - 1$ divides g_j for all j, which implies that $g \in (x^n z^k - 1)\mathbb{Z}[\mathbb{H}]$. Writing $g = (x^n z^k - 1)q$ we have

$$(x^n z^k - 1)p = (x^n z^k - 1)qf,$$

and cancelling gives $p \in \mathbb{Z}[\mathbb{H}]f$, which is a contradiction. So α_f is mixing.

5. Closing Remarks

Theorems 3.3.2 and 3.4.1 give a complete classification of principal ergodicity for finitely-generated torsion-free nilpotent groups, since we have noted that $\mathbb{Z}$ and $\{1\}$ are not principally ergodic. It would be interesting to find a complete classification of all principally ergodic groups, at least in the torsion-free case. By Theorem 3.4.1, we may as well take our groups to be finitely generated. From our experience with $\mathbb{Z}^d$ and torsion-free nilpotent groups it seems that failing to be principally ergodic is a rank one phenomenon. To this end, I make the following two claims.

Conjecture 5.1. *Every poly-infinite-cyclic group not isomorphic to the trivial group or the integers is principally ergodic.*

Conjecture 5.2. *Every free group of rank at least two is principally ergodic.*

(Note that by Theorems 3.3.2 and 3.4.1 it suffices to handle the case of the free group on two generators). More generally, I believe the following should be true.

Conjecture 5.3. *Every torsion-free group which is not principally ergodic is either the trivial group or virtually cyclic.*

It would also be of interest to see if the converse of Theorem 3.4.2 holds. More generally, it would be nice to know how principal ergodicity behaves under natural group theoretic operations, e.g. quotients, direct products, free products and semidirect products. Also, a complete classification of when α_f is mixing for $f \in \mathbb{Z}[\mathbb{H}]$ is still not known. Corollary 4.2.1 is a starting point. If $\phi_d(z^{\pm 1})|f$ for some $d \in \mathbb{N}$, then as in Proposition 4.1.1, it is not hard to see that α_f is not mixing. Thus one really needs to understand the condition that $\overline{f}$ is divisible by a generalized cyclotomic polynomial in $\mathbb{Z}[\mathbb{Z}^2]$, i.e. that f can be written as $f = \phi_d(\gamma)q + (z-1)h$ where $\gamma \in \mathbb{H} \setminus \langle z \rangle, d \in \mathbb{N}$ and $q, h \in \mathbb{Z}[\mathbb{H}]$. One could attempt to understand conditions on q and h, perhaps by decomposing q and h as we did in the proof of Corollary 4.2.1, but so far no additional progress has been made in this direction.

6. Acknowledgments

I am greatly indebted to Douglas Lind for his guidance, advice, mathematical expertise, and for proofreading more editions of this paper than I care to count. Without him no part of this paper would exist.

References

[1] David Cox, John Little, and Donal OShea, *Ideals, Varieties, and Algorithms*, New York, Springer-Verlag, 2006.

[2] Manfred Einsiedler and Douglas Lind , Algebraic $\mathbb{Z}^d$-Actions of Rank One,2000.

[3] Manfred Einsiedler and Harald Rindler, Algebraic Actions of the Discrete Heisenberg Group and other Non-Abelian Groups, Aequationes Math. 62 (2001), no. 1-2, 117-135.

[4] Branko Grünbaum, *Convex Polytopes*, John Wiley & Sons, 1967.

[5] Donald Passman, *The Algebraic Structure of Group Rings*, Malabar, Fl, Robert E. Krieger Publishing Company, 1977.

[6] Klaus Schmidt, *Dynamical Systems of Algebraic Origin*, Birkhäuser, Basel, 1995.

Department of Mathematics, University of Washington, Seattle,WA 98105
E-mail address: hayes_benjamin@hotmail.com