MATH 436 Notes: Finitely generated Abelian groups.

Jonathan Pakianathan

November 1, 2003

1 Direct Products and Direct Sums

We discuss two universal constructions in this section. We start with the direct product construction:

Definition 1.1 (Direct Products). *Let $\{G_\alpha\}_{\alpha\in I}$ be a collection of groups indexed by an index set I. We may form the Cartesian product $\prod_{\alpha\in I} G_\alpha$. The elements of this Cartesian product can be denoted by tuples $(a_\alpha)_{\alpha\in I}$.*

We refer to the entry a_α as the αth component of this tuple. We define a multiplication on this Cartesian product componentwise, i.e., $(a_\alpha)\star(b_\alpha) = (a_\alpha \star_\alpha b_\alpha)$ where $\star_\alpha$ is the group multiplication in G_α.

It is easy to check that this makes $\prod_{\alpha\in I} G_\alpha$ into a group with identity element $(e_\alpha)_{\alpha\in I}$ where e_α is the identity element of G_α for each $\alpha \in I$.

When the index set $I = \{1, 2, \ldots, n\}$ is finite we usually write $\prod_{\alpha\in I} G_\alpha$ as $\prod_{i=1}^n G_i$ or sometimes more simply as $G_1 \times \cdots \times G_n$. Finally when the index set $I = \mathbb{N}$ we write $\prod_{\alpha\in\mathbb{N}} G_\alpha$ as $\prod_{i=0}^\infty G_i$.

Now we talk about the second construction called the direct sum construction which is similar but as we shall see, different in essential ways!

Definition 1.2 (Direct Sums). *Let $\{G_\alpha\}_{\alpha\in I}$ be a collection of groups indexed by an index set I. The direct sum of the collection is denoted by $\oplus_{\alpha\in I} G_\alpha$ and is defined to be the subgroup of elements in $\prod_{\alpha\in I} G_\alpha$ which have only finitely many nontrivial components, i.e.,*

$$\oplus_{\alpha\in I} G_\alpha = \{(a_\alpha)_{\alpha\in I} \in \prod_{\alpha\in I} G_\alpha | a_\alpha = e_\alpha \text{ for all but finitely many } \alpha \in I\}.$$

It is not hard to check that $\oplus_{\alpha\in I}G_\alpha$ is a normal subgroup of $\prod_{\alpha\in I}G_\alpha$.

It is trivial to see that for $|I|<\infty$, $\oplus_{\alpha\in I}G_\alpha=\prod_{\alpha\in I}G_\alpha$. However when $|I|=\infty$, these groups are quite different as the next example will show!

Example 1.3 (Difference between direct sums and direct products). *Let us consider $\prod_{i=0}^{\infty}\mathbb{Z}/2\mathbb{Z}$. Thus in this example $G_i=\mathbb{Z}/2\mathbb{Z}$ for all $i\in\mathbb{N}$. Explicitly we have:*

$$\prod_{i=0}^{\infty}\mathbb{Z}/2\mathbb{Z}=\{(a_0,a_1,a_2,\dots)|a_i\in\mathbb{Z}/2\mathbb{Z}\text{ for all }i\in\mathbb{N}\}.$$

and the group structure is given by componentwise addition modulo 2.

As a set, $\prod_{i=0}^{\infty}\mathbb{Z}/2\mathbb{Z}$ is the set of all binary sequences and a simple Cantor diagonal argument shows that this set is uncountable.

For example, **supposing the direct product were countable** *then $\prod_{i=0}^{\infty}\mathbb{Z}/2\mathbb{Z}=\{f_1,f_2,\dots\}$. Then writing $f_i=(a_{i0},a_{i1},a_{i2},\dots)$ we can create $f=(b_0,b_1,\dots)\in\prod_{i=0}^{\infty}\mathbb{Z}/2\mathbb{Z}$ by insisting $b_i\neq a_{ii}$. Then clearly $f\neq f_i$ for all i and so our original listing of $\prod_{i=0}^{\infty}\mathbb{Z}/2\mathbb{Z}$ was incomplete thus giving a contradiction.*

Now $\oplus_{i=0}^{\infty}\mathbb{Z}/2\mathbb{Z}$ is the subgroup of binary sequences which are eventually 0. Let $F_n=\{(a_0,\dots,a_{n-1},0,0,\dots)|a_i\in\mathbb{Z}/2\mathbb{Z}\text{ for }i=0,\dots,n-1\}$. Then $|F_n|=2^n$ for all $n\in\mathbb{N}$ and $\oplus_{i=0}^{\infty}\mathbb{Z}/2\mathbb{Z}=\cup_{n=1}^{\infty}F_n$ is thus a countable union of finite sets and hence is countable.

Hence there is no bijection between $\prod_{n=0}^{\infty}\mathbb{Z}/2\mathbb{Z}$ and $\oplus_{n=0}^{\infty}\mathbb{Z}/2\mathbb{Z}$ and so there is no isomorphism between them. Thus the direct sum and the direct product in this case are nonisomorphic groups.

Definition 1.4 (Projection and inclusion maps). *Given a direct product $G=\prod_{\alpha\in I}G_\alpha$ we have canonical projection maps $\pi_\beta:G\to G_\beta$ given by $\pi_\beta((a_\alpha)_{\alpha\in I})=a_\beta$. It is easy to check that $\pi_\beta:G\to G_\beta$ is an epimorphism of groups for each $\beta\in I$. We call π_β the projection to the βth factor.*

These projection maps restrict to give epimorphisms $\pi_\beta:\oplus_{\alpha\in I}G_\alpha\twoheadrightarrow G_\beta$ also.

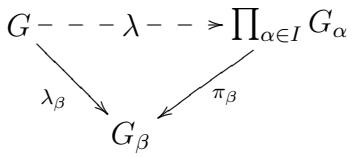
We also have canonical monomorphisms $i_\beta:G_\beta\hookrightarrow\oplus_{\alpha\in I}G_\alpha$ given by $i_\beta(g)=(a_\alpha)_{\alpha\in I}$ where $a_\beta=g$ and $a_\alpha=e_\alpha$ for $\alpha\neq\beta$.

Thus we may regard the image of i_β as an isomorphic copy of G_β inside of $\oplus_{\alpha\in I}G_\alpha$.

We may also regard i_β as a map into $\prod_{\alpha\in I}G_\alpha$ and so similar statements hold for the direct product.

The direct product construction has an important universal property that we will later discuss in the context of category theory. This is stated and proved in the next proposition:

Proposition 1.5 (Universal product property of direct products). *Let $\{G_\alpha\}_{\alpha\in I}$ be a collection of groups and suppose there is a group G and group homomorphisms $\lambda_\beta : G \to G_\beta$ for each $\beta \in I$. Then there is a* **unique** *homomorphism λ making the following diagram commute for all $\beta \in I$:*



In fact $\lambda(g) = (\lambda_\alpha(g))_{\alpha\in I}$ for all $g \in G$.
Thus there is a natural bijection between the sets

$$\prod_{\alpha\in I} Hom(G, G_\alpha) \leftrightarrow Hom(G, \prod_{\alpha\in I} G_\alpha)$$

given by $(\lambda_\alpha)_{\alpha\in I} \leftrightarrow \lambda$. Here $Hom(G, H)$ denotes the set of all homomorphisms from G to H.

Proof. In order for the diagram to commute, i.e., $\pi_\beta \circ \lambda = \lambda_\beta$ for all $\beta \in I$, it is clear that we need to define $\lambda(g) = (\lambda_\alpha(g))_{\alpha\in I}$ for all $g \in G$. This gives uniqueness.

It is then a simple check to see that λ so defined is indeed a homomorphism of groups. This gives existance.

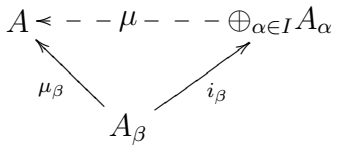
□

A dual property holds for direct sums as long as we restrict ourselves to Abelian groups. For the rest of this section, we will be dealing with Abelian groups so it is useful to review some conventions:

If A is an Abelian group then it is common to denote the group operation $\star$ by $+$. It is then also common to denote the identity e by 0 and call it zero. Finally we denote $x^n = x \star \cdots \star x$ by nx and write $\sum_{i=1}^n x_i$ for $x_1 + \cdots + x_n$.

Also if $\{x_1, x_2, \dots\}$ is a sequence of elements of A such that all but finitely many of the x_i are zero then we define $\sum_{i=1}^\infty x_i$ as the sum of the nonzero elements. ($\sum_{i=1}^\infty x_i$ is defined to be 0 if all the elements are zero). We will use these conventions throughout the remainder of this section.

Proposition 1.6 (Universal coproduct property of direct sums of Abelian groups). *Let $\{A_\alpha\}_{\alpha\in I}$ be a collection of Abelian groups and suppose there is an Abelian group A and group homomorphisms $\mu_\beta : A_\beta \to A$ for each $\beta \in I$. Then there is a* **unique** *homomorphism μ making the following diagram commute for all $\beta \in I$:*



In fact $\mu((a_\alpha)_{\alpha\in I}) = \sum_{\alpha\in I}\mu_\alpha(a_\alpha)$ for all $(a_\alpha)_{\alpha\in I} \in \oplus_{\alpha\in I}A_\alpha$.
Thus there is a natural bijection between the sets

$$\prod_{\alpha\in I} Hom(A_\alpha, A) \leftrightarrow Hom(\oplus_{\alpha\in I}A_\alpha, A)$$

given by $(\mu_\alpha)_{\alpha\in I} \leftrightarrow \mu$.

Proof. First of all notice that for any $(a_\alpha)_{\alpha\in I} \in \oplus_{\alpha\in I}A_\alpha$ we may write $(a_\alpha)_{\alpha\in I} = \sum_{\alpha\in I} i_\alpha(a_\alpha)$ where the sum is finite.

Thus if $\mu : \oplus_{\alpha\in I}A_\alpha \to A$ is a homomorphism then we have $\mu((a_\alpha)_{\alpha\in I}) = \sum \mu(i_\alpha(a_\alpha))$. In order to make the diagram commute for all $\alpha \in I$, we need $\mu \circ i_\alpha = \mu_\alpha$ and so we see that μ has to be uniquely given by the formula $\mu((a_\alpha)_{\alpha\in I}) = \sum \mu_\alpha(a_\alpha)$. This shows uniqueness.

In order to verify existance of a homomorphism μ we need to verify that the formula $\mu((a_\alpha)_{\alpha\in I}) = \sum_{\alpha\in I}\mu_\alpha(a_\alpha)$ actually defines a homomorphism. It is clear that it is a function $\oplus_{\alpha\in I}A_\alpha \to A$. On the other hand

$$\mu((a_\alpha) + (b_\alpha)) = \mu((a_\alpha + b_\alpha)) = \sum_{\alpha\in I}\mu_\alpha(a_\alpha + b_\alpha) = \sum_{\alpha\in I}(\mu_\alpha(a_\alpha) + \mu_\alpha(b_\alpha))$$

By the associativity and commutativity of A, we may rearrange this last sum as $\sum_{\alpha\in I}\mu_\alpha(a_\alpha) + \sum_{\alpha\in I}\mu_\alpha(b_\alpha) = \mu((a_\alpha)) + \mu((b_\alpha))$ and thus μ is indeed a homomorphism. This proves existance. However do note that this only worked because A was an Abelian group also!

The rest of the proposition is a rephrasing of the diagram property. □

We end this section with some basic properties of direct sums of Abelian groups:

Proposition 1.7. *Let $\{A_\alpha\}_{\alpha\in I}$ and $\{B_\alpha\}_{\alpha\in I}$ be two collections of Abelian groups indexed by the set I such that $B_\alpha \leq A_\alpha$ for all $\alpha \in I$.*

Then $\oplus_{\alpha\in I} B_\alpha \leq \oplus_{\alpha\in I} A_\alpha$ and furthermore

$$\oplus_{\alpha\in I} A_\alpha / \oplus_{\alpha\in I} B_\alpha \cong \oplus_{\alpha\in I}(A_\alpha/B_\alpha).$$

Proof. First note as we are dealing with Abelian groups, all subgroups are always normal. It is clear that $\oplus_{\alpha\in I} B_\alpha \leq \oplus_{\alpha\in I} A_\alpha$. Let $\phi_\alpha : A_\alpha \twoheadrightarrow A_\alpha/B_\alpha$ be the canonical quotient epimorphism with kernel B_α for all $\alpha \in I$.

Define $\mu : \oplus_{\alpha\in I} A_\alpha \to \oplus_{\alpha\in I}(A_\alpha/B_\alpha)$ by $\mu((a_\alpha)_{\alpha\in I}) = (\phi_\alpha(a_\alpha))_{\alpha\in I}$ for all $(a_\alpha)_{\alpha\in I} \in \oplus_{\alpha\in I} A_\alpha$. It is easy to check that μ is a homomorphism with the stated codomain and that it is in fact an epimorphism as each ϕ_α is.

Finally it is also easy to check that $ker(\mu) = \oplus_{\alpha\in I} B_\alpha$ and so the first isomorphism theorem shows that μ induces an isomorphism between $\oplus_{\alpha\in I} A_\alpha / \oplus_{\alpha\in I} B_\alpha$ and $\oplus_{\alpha\in I}(A_\alpha/B_\alpha)$. □

Proposition 1.8. *Let 0 denote the trivial Abelian group of order 1 and let $\sigma \in \Sigma_n$ be a fixed permutation. Then:*
(a) $A \oplus 0 \cong A$ for all Abelian groups A.
(b) If $A_1, \ldots, A_n$ are Abelian groups then

$$A_1 \oplus A_2 \oplus \cdots \oplus A_n \cong A_{\sigma(1)} \oplus A_{\sigma(2)} \oplus \cdots \oplus A_{\sigma(n)}.$$

Thus for example we have $A \oplus B \cong B \oplus A$ in general for any Abelian groups A, B.
(c) For any three Abelian groups A, B and C we have

$$(A \oplus B) \oplus C \cong A \oplus B \oplus C \cong A \oplus (B \oplus C).$$

Proof. For (a), it is a simple check to show that $\mu : A \oplus 0 \to A$ given by $\mu((a, 0)) = a$ for all $a \in A$ is the desired isomorphism.
For (b), it is a simple check to show that $\lambda : A_1 \oplus \cdots \oplus A_n \to A_{\sigma(1)} \oplus \cdots \oplus A_{\sigma(n)}$ given by $\lambda((a_1, \ldots, a_n)) = (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$ is the desired isomorphism.
For (c), the isomorphisms are easily verified to be given by

$$((a, b), c) \leftrightarrow (a, b, c) \leftrightarrow (a, (b, c))$$

for all $a \in A, b \in B$ and $c \in C$. □

2 Free Abelian Groups

Just as the concept of basis is important in the study of real vector spaces in linear algebra, it is equally useful to consider Abelian groups which possess a "basis". However of course in an Abelian group A, there is generally no concept of scalar multiplication with an arbitrary real number. However as nx is defined for $x \in A, n \in \mathbb{Z}$, we have the concept of multiplication with an integer. This motivates the next definition:

Definition 2.1 ($\mathbb{Z}$-basis). *A $\mathbb{Z}$-basis for an Abelian group A is a subset $X \subset A$ with the following properties:*
(1) $< X >= A$ i.e., every $a \in A$ may be written as $a = \sum_{x \in X} n_x x$ where $n_x \neq 0$ for only finitely many $x \in X$.
(2) X is $\mathbb{Z}$-independent i.e., for any collection of integers $\{n_x\}_{x \in X}$ such that only finitely many are nonzero we have

$$\sum_{x \in X} n_x x = 0 \implies n_x = 0 \text{ for all } x \in X.$$

Example 2.2. *Consider an arbitrary direct sum of integers, $\oplus_{\alpha \in I} \mathbb{Z}$. For each $\beta \in I$, let $\hat{e}_\beta \in \oplus_{\alpha \in I} \mathbb{Z}$ be the element with βth component 1 and all other components 0. It is a simple exercise to verify that $\{\hat{e}_\alpha\}_{\alpha \in I}$ is a $\mathbb{Z}$-basis for $\oplus_{\alpha \in I} \mathbb{Z}$. This is called the canonical $\mathbb{Z}$-basis for $\oplus_{\alpha \in I} \mathbb{Z}$.*

Thus for example the set $\{(1,0,0),(0,1,0),(0,0,1)\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}^3 = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$.

The next proposition shows that the previous example pretty much covers all the cases of Abelian groups which have a $\mathbb{Z}$-basis!

Proposition 2.3 (Abelian groups with a $\mathbb{Z}$-basis). *Let A be an Abelian group with basis X. Then every element $a \in A$ can be written* **uniquely** *as $a = \sum_{x \in X} n_x x$ where all but finitely many of the $n_x \in \mathbb{Z}$ are zero.*

The map $\Theta : \oplus_{x \in X} \mathbb{Z} \to A$ given by $\Theta((n_x)_{x \in X}) = \sum_{x \in X} n_x x$ is an isomorphism of Abelian groups which takes the canonical basis element $\hat{e}_x$ to x for all $x \in X$.

Proof. It is easy to check that the map Θ given in the statement of the proposition is a homomorphism of groups. It is onto by property (1) of a $\mathbb{Z}$-basis and it has trivial kernel by property (2) of a $\mathbb{Z}$-basis. Thus it is an isomorphism and it is easy to check that $\Theta(\hat{e}_x) = x$ for all $x \in X$.

Since Θ is a bijection, it follows that each $a \in A$ can be written as $a = \sum_{x \in X} n_x x$ for a unique set of integers $\{n_x\}_{x \in X}$ of which only finitely many are nonzero. This completes the proof. $\square$

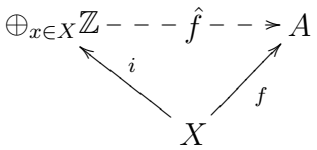
Definition 2.4 (Free Abelian group on X). *The group $\oplus_{x \in X} \mathbb{Z}$ is called the free Abelian group on X. It has a canonical basis $\{\hat{e}_x | x \in X\}$ which is in bijective correspondence with X.*

We have seen that an Abelian group A with $\mathbb{Z}$-basis X is isomorphic to $\oplus_{x \in X} \mathbb{Z}$ under an isomorphism that takes $a = \sum_{x \in X} n_x x \in A$ to $(n_x)_{x \in X} \in \oplus_{x \in X} \mathbb{Z}$. The integer n_x is called the component of a with respect to the basis element x.

The following theorem shows that $\mathbb{Z}$-basis share common important traits with basis that occur in linear algebra:

Theorem 2.5 (Free Property of Free Abelian Groups). *Let X be a set and $\oplus_{x \in X} \mathbb{Z}$ be the free Abelian group on X and let $i : X \to \oplus_{x \in X} \mathbb{Z}$ be the function defined by $i(x) = \hat{e}_x$.*

If A is an Abelian group and $f : X \to A$ is any function, then there exists a **unique** *homomorphism $\hat{f} : \oplus_{x \in X} \mathbb{Z} \to A$ that makes the following diagram commute:*



The homomorphism $\hat{f}$ is given by $\hat{f}((n_x)_{x \in X}) = \sum_{x \in X} n_x f(x)$. Thus if the set $\{f(x) | x \in X\}$ generates A then $\hat{f}$ is an epimorphism.

Finally if we let $Hom_{Set}(X, A)$ denote the set of all functions from X to A we see that there is a natural bijection

$$Hom_{Set}(X, A) \leftrightarrow Hom(\oplus_{x \in X} \mathbb{Z}, A)$$

given by $f \leftrightarrow \hat{f}$.

Proof. Since $i(x) = \hat{e}_x$ then we may write $(n_x)_{x \in X} = \sum_{x \in X} n_x i(x)$ for all $(n_x)_{x \in X} \in \oplus_{x \in X} \mathbb{Z}$. Any homomorphism $\hat{f}$ making the diagram in the statement of the theorem commute, would then have:

$$\hat{f}((n_x)_{x \in X}) = \sum_{x \in X} n_x \hat{f}(i(x)) = \sum_{x \in X} n_x f(x).$$

This shows the uniqueness of $\hat{f}$ and that it would be defined by the formula $\hat{f}((n_x)_{x\in X}) = \sum_{x\in X} n_x f(x)$.

It is a simple check using that A is Abelian, that $\hat{f}$ defined in this way is indeed a homomorphism which proves existance.

The rest of the Theorem is a rephrasing of the diagram. □

This yields the following important corollary!

Corollary 2.6 (Abelian groups are quotients of free Abelian groups). *Let A be an Abelian group and X a set of generators for A (We could take $X = A$ for example). Then there is an epimorphism $\hat{f} : \oplus_{x\in X}\mathbb{Z} \to A$, and thus A is a quotient of a free Abelian group.*

Let $\mathbb{Z}^n = \mathbb{Z}\oplus\cdots\oplus\mathbb{Z}$ denote the n-fold direct sum of $\mathbb{Z}$ with itself. If A is finitely generated, generated by n generators then $A \cong \mathbb{Z}^n/H$ where $H \leq \mathbb{Z}^n$.

Proof. For the first part we let $f : X \to A$ be the inclusion map $f(x) = x$ for all $x \in X$ and apply Theorem 2.5 to get an epimorphism $\hat{f} : \oplus_{x\in X}\mathbb{Z} \twoheadrightarrow A$.

In the case that $|X| = n$ then clearly $\oplus_{x\in X}\mathbb{Z}$ is isomorphic to $\mathbb{Z}^n$ and so we get an epimorphism $\mathbb{Z}^n \twoheadrightarrow A$ with kernel H say. The first isomorphism theorem then shows us that $A \cong \mathbb{Z}^n/H$. □

From the previous corollary, it follows that to classify all the finitely generated Abelian groups, we need only classify the subgroups H of $\mathbb{Z}^n$ and their corresponding quotients groups.

Before we do this, let us show that the cardinality of a basis is an invariant of a free Abelian group.

Theorem 2.7 (Any two basis for a Free Abelian group have the same cardinality). *Let A be an Abelian group and let X and Y be two $\mathbb{Z}$-basis for A. Then there is a bijection from X to Y i.e., X and Y have the same cardinality.*

In particular if n, m are nonnegative integers with $\mathbb{Z}^m \cong \mathbb{Z}^n$ then $n = m$.

Proof. The two $\mathbb{Z}$-basis sets for A set up an isomorphism

$$\oplus_{x\in X}\mathbb{Z} \cong A \cong \oplus_{y\in Y}\mathbb{Z}.$$

Under this isomorphism the subgroup $2A = \{2a | a \in A\}$ has induced isomorphisms

$$\oplus_{x\in X}2\mathbb{Z} \cong 2A \cong \oplus_{y\in Y}2\mathbb{Z}.$$

By Proposition 1.7 we have

$$\oplus_{x\in X}\mathbb{Z}/2\mathbb{Z} \cong A/2A \cong \oplus_{y\in Y}\mathbb{Z}/2\mathbb{Z}.$$

In particular there is a bijection between the sets $\oplus_{x\in X}\mathbb{Z}/2\mathbb{Z}$ and $\oplus_{y\in Y}\mathbb{Z}/2\mathbb{Z}$.

If $|X| < \infty$ then $|\oplus_{x\in X}\mathbb{Z}/2\mathbb{Z}| = 2^{|X|}$. Thus $|\oplus_{y\in Y}\mathbb{Z}/2\mathbb{Z}|$ is also finite and so $|Y| < \infty$ and $2^{|Y|} = 2^{|X|}$ which yields $|X| = |Y|$ as desired.

So it only remains to consider the case $|X| = |Y| = \infty$.

Let $P_{finite}(X) = \{S \subset X || S| < \infty\}$ be the set of finite subsets of X. Then there is a bijection $\Theta : P_{finite}(X) \to \oplus_{x\in X}\mathbb{Z}/2\mathbb{Z}$ given by $\Theta(S) = (n_x)_{x\in X}$ where $n_x \in \mathbb{Z}/2\mathbb{Z}$ and $n_x = \bar{1} \leftrightarrow x \in S$.

The bijection between $\oplus_{x\in X}\mathbb{Z}/2\mathbb{Z}$ and $\oplus_{y\in Y}\mathbb{Z}/2\mathbb{Z}$ thus induces a bijection between $P_{finite}(X)$ and $P_{finite}(Y)$ and so these two sets have the same cardinality. However for infinite sets X we have $P_{finite}(X)$ has the same cardinality as X (See Hungerford) and so this shows X and Y have the same cardinality in this case as desired.

□

We may now define

Definition 2.8 (Rank of a Free Abelian group). *If A is a free Abelian group with $\mathbb{Z}$-basis X. The rank of A is defined to be the cardinality of X. Thus any free Abelian group of rank n is isomorphic to $\mathbb{Z}^n$.*

There are some properties of $\mathbb{Z}$-basis which are not similar to those in linear algebra - the next example emphasizes these:

Example 2.9 (Basis for $\mathbb{Z}^1$). *Since $\mathbb{Z}$ is a free Abelian group of rank 1, the previous theorem shows that every basis for $\mathbb{Z}$ has cardinality 1. Since the only cyclic generators of $\mathbb{Z}$ are ± 1 we have that the only basis for $\mathbb{Z}$ are $\{1\}$ and $\{-1\}$.*

Thus note that $\{2, 3\}$ is a generating set for $\mathbb{Z}$ which does not contain a $\mathbb{Z}$-basis of $\mathbb{Z}$ as a subset.

Similarly note that $\{2\}$ is a $\mathbb{Z}$-independent subset of $\mathbb{Z}$ which cannot be extended to a $\mathbb{Z}$-basis of $\mathbb{Z}$.

So in these two respects, $\mathbb{Z}$-basis are different than basis in vector spaces.

We will now classify the subgroups of $\mathbb{Z}^n$ after a preliminary example:

Example 2.10. *We have previously seen that any nontrivial subgroup H of $\mathbb{Z}^1 = \mathbb{Z}$ is of the form $d\mathbb{Z}$ for a nonnegative integer $d \geq 1$ and is hence itself free Abelian of rank 1 with basis $\{d\}$. This led to the classification of all one-generated Abelian groups as the cyclic groups $\mathbb{Z}$ or $\mathbb{Z}/d\mathbb{Z}$ for $d \geq 1$.*

Now picture the group $\mathbb{Z}^2$ as the subgroup of the Euclidean plane $(\mathbb{R}^2, +)$ consisting of vectors with integer entries. Then $H = \{(2s, 3t) | s, t \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}^2$.

Notice if $\{\hat{e}_1, \hat{e}_2\}$ is the canonical basis for $\mathbb{Z}^2$ then $\{2\hat{e}_1, 3\hat{e}_2\}$ is a $\mathbb{Z}$-basis for H and so H itself is abstractly isomorphic to $\mathbb{Z}^2$. In fact the isomorphism $\Theta : H \to \mathbb{Z}^2$ is given by $\Theta((2s, 3t)) = (s, t)$ for all $s, t \in \mathbb{Z}$.

If $T = \{(s, s) | s \in \mathbb{Z}\}$ then $T \leq \mathbb{Z}^2$ and T is free Abelian of rank 1 with basis $\{(1, 1)\}$. So T is (abstractly) isomorphic to $\mathbb{Z}^1$.

Theorem 2.11 (Structure of subgroups of $\mathbb{Z}^n$). *Let $H \neq (0)$ be a nontrivial subgroup of $\mathbb{Z}^n$. Then there exists a $\mathbb{Z}$-basis $\{\hat{z}_1, \ldots, \hat{z}_n\}$ of $\mathbb{Z}^n$ and integers $1 \leq d_1 | d_2 | d_3 | \ldots | d_r$ for some $1 \leq r \leq n$ such that $\{d_1\hat{z}_1, \ldots, d_r\hat{z}_r\}$ is a $\mathbb{Z}$-basis for H.*

Proof. We prove this by induction on n. For $n = 1$ we have proven this before so assume $n > 1$ and that the theorem is proven for all free Abelian groups of smaller rank.

Let $\{\hat{e}_1, \ldots, \hat{e}_n\}$ be the canonical basis of $\mathbb{Z}^n$. Since $H \neq (0)$, there is a nonzero element $h \in H$. If we write $h = \sum_{i=1}^n n_i\hat{e}_i$ then at least one n_i is a nonzero integer and hence is either positive or negative. If all the components are nonpositive, then $-h \in H$ has a positive component.

Thus we see that there is some element of H with a positive component with respect to a $\mathbb{Z}$-basis of $\mathbb{Z}^n$. This motivates the following outlandish definition!

Let $d_1 > 0$ be the smallest positive integer than occurs as a component of an element $h \in H$ with respect to some $\mathbb{Z}$-basis of $\mathbb{Z}^n$. Since every nonempty set of positive integers has a smallest element, d_1 is well-defined.

In other words for **any** $h \in H$ and **any** $\mathbb{Z}$-basis $\{\hat{x}_1, \ldots, \hat{x}_n\}$ of $\mathbb{Z}^n$ if we write $h = \sum_{i=1}^n n_i\hat{x}_i$ then we have $(n_i > 0 \implies n_i \geq d_1)$ for all $1 \leq i \leq n$.

By the definition of d_1, there exists a $\mathbb{Z}$-basis $\{\hat{x_1}, \ldots, \hat{x_n}\}$ of $\mathbb{Z}^n$ and an element $h \in H$ such that $h = d_1\hat{x_1} + s_2\hat{x_2} + \ldots s_n\hat{x_n}$. (Here we reorder the basis if necessary to ensure d_1 occurs as the first component.)

Now we perform the division algorithm and write $s_j = q_j d_1 + r_j$ where $0 \leq r_j < d_1$ for $j = 2, \ldots, n$. Plugging this into the expression for h above

we find upon rearranging:

$$\begin{aligned} h &= d_1(\hat{x_1} + q_2\hat{x_2} + \cdots + q_n\hat{x_n}) + r_2\hat{x_2} + \ldots r_n\hat{x_n} \\ &= d_1\hat{y_1} + r_2\hat{y_2} + \ldots r_n\hat{y_n}. \end{aligned}$$

where $\{\hat{y_1}, \ldots, \hat{y_n}\}$ is the $\mathbb{Z}$-basis of $\mathbb{Z}^n$ given by $\hat{y_1} = \hat{x_1} + q_2\hat{x_2} + \cdots + q_n\hat{x_n}$ and $\hat{y_k} = \hat{x_k}$ for $k = 2, \ldots, n$.

Since $0 \leq r_k < d_1$ for $k = 2, \ldots, n$ and d_1 is the minimial positive component of an element of H with respect to any $\mathbb{Z}$-basis of $\mathbb{Z}^n$ we see that $r_2 = r_3 = \cdots = r_n = 0$ and so $h = d_1\hat{y_1} \in H$.

Thus we conclude that there is a $\mathbb{Z}$-basis $\{\hat{y_1}, \ldots, \hat{y_n}\}$ of $\mathbb{Z}^n$ such that $d_1\hat{y_1} \in H$.

Now $< \hat{y_2}, \ldots, \hat{y_n} >= \{a_2\hat{y_2} + \cdots + a_n\hat{y_n} | a_i \in \mathbb{Z}\}$ is clearly a free Abelian group of rank $n-1$. Let $T = H \cap < \hat{y_2}, \ldots, \hat{y_n} >$. Thus by induction there is a $\mathbb{Z}$-basis of $< \hat{y_2}, \ldots, \hat{y_n} >$ call it $\{\hat{z_2}, \ldots, \hat{z_n}\}$ and $1 \leq d_2 | d_3 | \ldots | d_r$ such that $\{d_2\hat{z_2}, \ldots, d_r\hat{z_r}\}$ is a $\mathbb{Z}$-basis for T. Setting $\hat{z_1} = \hat{y_1}$ we then have a $\mathbb{Z}$-basis $\{\hat{z_1}, \ldots, \hat{z_n}\}$ of $\mathbb{Z}^n$ such that $d_1\hat{z_1} \in H$ and such that $\{d_2\hat{z_2}, \ldots, d_r\hat{z_r}\}$ is a $\mathbb{Z}$-basis for $T = H \cap < \hat{z_2}, \ldots, \hat{z_n} >$.

Suppose $h \in H$ and write $h = \sum_{i=1}^{n} a_i\hat{z_i}$. Write $a_1 = qd_1 + r$ where $0 \leq r < d_1$. Then $h - qd_1\hat{z_1} \in H$ as $d_1\hat{z_1} \in H$ and a simple computation shows $h - qd_1\hat{z_1} = r\hat{z_1} + \sum_{i=2}^{n} a_i\hat{z_i}$. Again since $0 \leq r < d_1$ and d_1 is the minimal possible positive component of an element of H we conclude $r = 0$.

Thus $h - qd_1\hat{z_1} \in H \cap < \hat{z_2}, \ldots, \hat{z_n} >= T$ and so $h = qd_1\hat{z_1} + \sum_{i=2}^{r} q_i(d_i\hat{z_i})$. This shows that $\{d_1\hat{z_1}, d_2\hat{z_2}, \ldots, d_r\hat{z_r}\}$ span H. This set is automatically $\mathbb{Z}$-independent as $\{\hat{z_1}, \ldots, \hat{z_n}\}$ is $\mathbb{Z}$-independent as it is a $\mathbb{Z}$-basis for $\mathbb{Z}^n$. Thus we see that $\{d_1\hat{z_1}, \ldots, d_r\hat{z_r}\}$ is a $\mathbb{Z}$-basis for H with $1 \leq d_1$ and $d_2 | d_3 | \ldots | d_r$.

In order to be finished it only remains to show $d_1 | d_2$.

Well $d_1\hat{z_1} + d_2\hat{z_2} \in H$. Writing $d_2 = td_1 + r'$ for $0 \leq r' < d_1$ we find $d_1(\hat{z_1} + t\hat{z_2}) + r'\hat{z_2} \in H$. Thus r' is a nonnegative component of an element of H with respect to the $\mathbb{Z}$-basis $\{\hat{z_1} + t\hat{z_2}, \hat{z_2}, \ldots, \hat{z_n}\}$ of $\mathbb{Z}^n$. Since $r' < d_1$ this forces $r' = 0$ and so $d_2 = td_1$ and so $d_1 | d_2$ as desired. Thus by induction we are done!

□

This theorem has a few important corollaries:

Corollary 2.12. *If $H \leq \mathbb{Z}^n$ then H is free Abelian of rank r where $0 \leq r \leq n$.*

Corollary 2.13. *If A is a finitely generated Abelian group then A is a finite direct sum of cyclic groups. More precisely there are integers $k, s \geq 0$ and integers $1 < s_1|s_2|\ldots|s_k$ such that*

$$A \cong \mathbb{Z}^s \oplus \mathbb{Z}/s_1\mathbb{Z} \oplus \mathbb{Z}/s_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/s_k\mathbb{Z}.$$

This is called the decomposition of A into **invariant factors**.

Proof. Since A is finitely generated, there exists an epimorphism from a free Abelian group F of finite rank onto A.

Let H be the kernel of this epimorphism then $A \cong F/H$.

However by Theorem 2.11 there is a $\mathbb{Z}$-basis $\{\hat{z}_1, \ldots, \hat{z}_n\}$ of F and integers $1 \leq d_1|d_2|\ldots|d_r$ such that $\{d_1\hat{z}_1, \ldots, d_r\hat{z}_r\}$ is a $\mathbb{Z}$-basis for H.

Using this $\mathbb{Z}$-basis we get an isomorphism $\Theta : F \to \mathbb{Z}^n$ which takes H to $d_1\mathbb{Z} \oplus \cdots \oplus d_r\mathbb{Z} \oplus 0^{n-r}$. This induces an isomorphism of $A \cong F/H$ with $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \mathbb{Z}^{n-r}$. Finally we may drop 0 factors corresponding to $\mathbb{Z}/1\mathbb{Z} = 0$ to get the form described in the statement of the corollary. □

3 Finitely generated Abelian groups

We have seen that any finitely generated Abelian group is isomorphic to a finite direct sum (product) of cyclic groups.

The next proposition is useful when it comes to regrouping the finite factors in the direct sum in Corollary 2.13:

Proposition 3.1. *Let n, m be positive integers such that $gcd(n, m) = 1$. Then $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z}$.*

Thus if $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ where $p_1 < \cdots < p_k$ are distinct prime numbers we have

$$\mathbb{Z}/n\mathbb{Z} \cong \oplus_{i=1}^{k} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}.$$

Proof. The second part follows from repeated application of the first so we only prove the first part.

Suppose $s(1, 1) = (s, s) = (0, 0)$ in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$. Then $n|s$ and $m|s$. Thus $lcm(m, n)|s$. Since $lcm(m, n) = \frac{mn}{gcd(m,n)} = mn$. This shows that $o((1, 1)) = mn = |\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}|$. Thus we conclude that this group is cyclic generated by $(1, 1)$ and so $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/nm\mathbb{Z}$.

□

Example 3.2 (Caution!). *It follows from the previous proposition that* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. *However the reader is warned that if the numbers are not relatively prime this fails. For example* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}/4\mathbb{Z}$ *as the second group has elements of order* 4 *but the first group does not!*

Using Proposition 3.1 in Corollary 2.13 we get the following corollary:

Corollary 3.3. *If* A *is a finitely generated Abelian group then there exist integers* $s, r \geq 0$ *and prime numbers* $p_1 \leq p_2 \leq \cdots \leq p_r$ *together with positive integers* $\alpha_1, \ldots, \alpha_r$ *such that*

$$A \cong \mathbb{Z}^s \oplus \mathbb{Z}/p_1^{\alpha_1} \oplus \mathbb{Z}/p_2^{\alpha_2} \oplus \cdots \oplus \mathbb{Z}/p_k^{\alpha_k}$$

with the property that if $p_i = p_{i+1}$ *then* $\alpha_i \leq \alpha_{i+1}$.

This is called the decomposition of A *into* **elementary divisors**.

Both the decomposition of A into invariant factors and into elementary divisors turns out to be unique. We will prove these with a sequence of lemmas!

Lemma 3.4 (Number of $\mathbb{Z}$'s is unique). *Let* A *be an Abelian group such that* $A \cong \mathbb{Z}^n \oplus T$ *where* T *is a finite Abelian group. Then* A_{tor} *the subgroup of torsion elements of* A *has* $A_{tor} \cong T$ *and* $A/A_{tor} \cong \mathbb{Z}^n$.

Thus if T *and* S *are finite Abelian groups then*

$$\mathbb{Z}^n \oplus T \cong A \cong \mathbb{Z}^m \oplus S$$

implies

$$T \cong A_{tor} \cong S$$

and

$$\mathbb{Z}^n \cong A/A_{tor} \cong \mathbb{Z}^m.$$

Thus in particular $n = m$.

Proof. In $\mathbb{Z}^n \oplus T$ it is clear that the subgroup of torsion elements is $0 \oplus T$, Thus under the isomorphism $A \cong \mathbb{Z}^n \oplus T$ we get an induced isomorphism $A_{tor} \cong 0 \oplus T$ and hence $A/A_{tor} \cong \mathbb{Z}^n \oplus T/0 \oplus T$. Thus $A_{tor} \cong T$ and $A/A_{tor} \cong \mathbb{Z}^n \oplus 0 \cong \mathbb{Z}^n$.

The other statements in the lemma directly follow from these. The final conclusion that $n = m$ follows as the final isomorphism shows that A/A_{tor} is a free Abelian group with both a basis of size m and one of size n. □

Lemma 3.4 shows that to show that the invariant factor and elementary divisor decompositions of a finitely generated Abelian group are unique, it is enough to consider finite Abelian groups. We do this next.

Definition 3.5. *Given an Abelian group A and a prime p, we define*

$$A_p = \{a \in A | o(a) = p^k \text{ for some } k \geq 0\}.$$

We also define

$$A[p] = \{a \in A | o(a) = 1 \text{ or } p\}.$$

It is easy to check that since A is Abelian, we have $A[p] \leq A_p \leq A$.

We also define $pA = \{pa | a \in A\}$ and again it is easy to check that $pA \leq A$.

Lemma 3.6 (Working a prime at a time). *Suppose A is a finite Abelian group and $A \cong \oplus_{p \in P} T_p$ where P is a set of primes and T_p is a finite Abelian p-group for each $p \in P$.*

Then $A_p \cong T_p$ for all $p \in P$.

If S_p is also a finite Abelian p-group for each $p \in P$, then

$$\oplus_{p \in P} S_p \cong A \cong \oplus_{p \in P} T_p$$

implies

$$S_p \cong A_p \cong T_p$$

for all $p \in P$.

Proof. Fix a prime $q \in P$, the elements of order a power of q in $\oplus_{p \in P} T_p$ are clearly $0 \oplus T_q \oplus 0$. Thus under the isomorphism $A \cong \oplus_{p \in P} T_p$ we have an induced isomorphism $A_q \cong 0 \oplus T_q \oplus 0 \cong T_q$.

The rest of the lemma is a direct consequence of this. □

Lemma 3.7. *For any prime p and $k \geq 1$ we have $p(\mathbb{Z}/p^k\mathbb{Z}) = (p\mathbb{Z}/p^k\mathbb{Z}) \cong \mathbb{Z}/p^{k-1}\mathbb{Z}$.*

Proof. Consider the isomorphism $\Theta : p\mathbb{Z} \to \mathbb{Z}$ given by $\Theta(pn) = n$ for all $n \in \mathbb{Z}$. For $k \geq 1$, it is easy to check that this isomorphism restricts to an isomorphism from $p^k\mathbb{Z}$ to $p^{k-1}\mathbb{Z}$ and hence induces an isomorphism $p\mathbb{Z}/p^k\mathbb{Z} \cong \mathbb{Z}/p^{k-1}\mathbb{Z}$ which is what we desired to prove. □

If p is a prime and P is a finite Abelian p-group then Corollary 3.3 shows that $P \cong \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \ldots \mathbb{Z}/p^{\alpha_r}\mathbb{Z}$ for some $r \geq 0$ and $1 \leq \alpha_1 \leq \cdots \leq \alpha_r$. We now show that this sequence of α_j's is uniquely determined by P.

Lemma 3.8 (Uniqueness of elementary divisors for Abelian p-groups). *Let p be a prime and A a finite Abelian p-group. Suppose*

$$\mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_k}\mathbb{Z} \cong A \cong \mathbb{Z}/p^{\beta_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\beta_s}\mathbb{Z}$$

where $1 \leq \alpha_1 \leq \cdots \leq \alpha_k$ and $1 \leq \beta_1 \leq \cdots \leq \beta_s$ with $k, s \geq 0$.

Then $k = s$ and $\alpha_j = \beta_j$ for all j.

Proof. We prove the lemma by induction on P. If $|P| = 1$ or p it is trivial so assume $|P| > p$ and the lemma is proven for all Abelian p-groups of smaller order.

If $\mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_k}\mathbb{Z} \cong A \cong \mathbb{Z}/p^{\beta_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\beta_s}\mathbb{Z}$ then in particular we have $p^{\alpha_1+\cdots+\alpha_k} = p^{\beta_1+\cdots+\beta_s}$ which yields

$$\alpha_1 + \cdots + \alpha_k = \beta_1 + \cdots + \beta_s.$$

The isomorphism above induces an isomorphism

$$p(\mathbb{Z}/p^{\alpha_1}\mathbb{Z}) \oplus \cdots \oplus p(\mathbb{Z}/p^{\alpha_k}\mathbb{Z}) \cong pA \cong p(\mathbb{Z}/p^{\beta_1}\mathbb{Z}) \oplus \cdots \oplus p(\mathbb{Z}/p^{\beta_s}\mathbb{Z}).$$

and hence by Lemma 3.7 an isomorphism

$$\mathbb{Z}/p^{\alpha_1-1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_k-1}\mathbb{Z} \cong pA \cong \mathbb{Z}/p^{\beta_1-1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\beta_s-1}\mathbb{Z}$$

Thus $|pA| < |A|$ and hence by the induction hypothesis we can conclude that the set α_j's and β_j's which are strictly bigger than one agree. (Note if $\alpha_j = 1$ then the corresponding factor $\mathbb{Z}/p^{\alpha_j-1}\mathbb{Z} = 0$ and we cannot conclude anything directly.)

However using the equation $\alpha_1 + \cdots + \alpha_k = \beta_1 + \cdots + \beta_s$ we can now conclude the number of α_j which equal one is equal to the number of β_j which equal one and hence $r = s$ and $\alpha_j = \beta_j$ for all j. Thus by induction, we are done. □

By Lemmas 3.4, 3.6 and 3.8, it follows that the decomposition of a finitely generated Abelian group into elementary divisors is **unique**.

From this one can argue that the decomposition of a finitely generated Abelian group into invariant factors is also unique. We do that next:

Theorem 3.9 (Uniqueness of Decompositions). *Let A be a finitely generated Abelian group A. Then A can be decomposed as:*

$$A \cong \mathbb{Z}^s \oplus \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

where $s, k \geq 0$, $p_1 \leq p_2 \leq \cdots \leq p_k$ are primes, and α_j are positive integers such that $p_i = p_{i+1}$ implies $\alpha_i \leq \alpha_{i+1}$. This **elementary divisor** *decomposition is unique in the sense that k, s, the p_j's and the α_j's are uniquely determined from A.*

A can also be decomposed as:

$$A \cong \mathbb{Z}^s \oplus \mathbb{Z}/s_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/s_r\mathbb{Z}$$

where $s, r \geq 0$ and $1 < s_1|s_2|\ldots|s_r$. This **invariant factor** *decomposition is also unique in the sense that s, r and the s_j's are uniquely determined from A.*

Proof. We have already shown the existance of both decompositions and the uniqueness of the elementary divisor decomposition so it remains only to convince the reader of the uniqueness of the invariant factor decomposition. Since s has been determined to be uniquely determined in this decomposition, we only have to consider the case of a finite Abelian group A.

We will present a reversible algorithm that goes from the invariant factor decomposition to the elementary divisor decomposition. It will then follow that the invariant factor decomposition is unique as the elementary divisor decomposition is.

Let $A \cong \mathbb{Z}/s_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/s_r\mathbb{Z}$ where $r \geq 1$ and $1 < s_1|s_2|\ldots|s_r$. Let $s_r = p_1^{\beta_{1r}} \ldots p_k^{\beta_{kr}}$ be the unique decomposition of s_r into distinct primes $p_1 < \cdots < p_k$ with $\beta_{ir} \geq 1$ for each $1 \leq i \leq k$.

Note since $s_j|s_{j+1}|s_r$ for all $1 \leq j < r$ we may write $s_j = p_1^{\beta_{1j}} \ldots p_k^{\beta_{kj}}$ for unique integers $\beta_{ij} \geq 0$. Note $s_j|s_{j+1}$ gives $\beta_{ij} \leq \beta_{i,j+1}$ for all $1 \leq i \leq k$.

By Propostion 3.1, it follows that $A \cong \oplus_{i,j}\mathbb{Z}/p_i^{\beta_{ij}}\mathbb{Z}$. Thus by the uniqueness of the elementary divisor decomposition, the (nonzero) β_{ij} are determined. Thus the s_j are determined and the invariant factor decomposition is hence unique.

□