

The Structure of Abelian Groups

Charley Crissman

August 2, 2009

1 Introduction

The goal of this section is to completely understand a large class of abelian groups which includes all finite abelian groups. We will apply this knowledge in many different ways, but among the outcomes will be:

1. We will be able to list (up to isomorphism) all abelian groups of order n for each $n \in \mathbb{N}$.
2. We will be able to determine exactly when two finite products of cyclic groups are isomorphic (for example, we will show that $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$, whereas for example $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \not\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$).
3. Later, when we discuss rings and fields, we will use this knowledge to show that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for p prime.

2 Some Preliminary Generalities

Here are two general propositions about quotients that we will use again and again.

Proposition 2.1. *Let G_1 and G_2 be groups and let $N_1 \triangleleft G_1$ and $N_2 \triangleleft G_2$ be normal subgroups. Then $N_1 \times N_2 = \{(n_1, n_2) \mid n_1 \in N_1, n_2 \in N_2\}$ is a normal subgroup of $G_1 \times G_2$, and*

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2).$$

Proof. Define a homomorphism $\phi : G_1 \times G_2 \rightarrow (G_1/N_1) \times (G_2/N_2)$ by $\phi(g_1, g_2) = (g_1N_1, g_2N_2)$. The map ϕ is clearly a surjective homomorphism. The kernel of ϕ is precisely $N_1 \times N_2$, since $(g_1N_1, g_2N_2) = (N_1, N_2)$ if and

only if $g_1 \in N_1$ and $g_2 \in N_2$. Hence $N_1 \times N_2$ is a normal subgroup of $G_1 \times G_2$, and

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$$

by the first isomorphism theorem. \square

By induction, we have:

Corollary 2.2. *Let G_1, \dots, G_n be groups and for each i let $N_i \triangleleft G_i$ be a normal subgroup. Then $N_1 \times \dots \times N_n$ is a normal subgroup of $G_1 \times \dots \times G_n$, and*

$$(G_1 \times \dots \times G_n)/(N_1 \times \dots \times N_n) \cong (G_1/N_1) \times \dots \times (G_n/N_n).$$

Proposition 2.3. *Let G_1 and G_2 be groups and let $N_1 \triangleleft G_1$ and $N_2 \triangleleft G_2$ be normal subgroups. Suppose there is an isomorphism $\phi : G_1 \rightarrow G_2$ such that $\phi(N_1) = N_2$. Then the map $\bar{\phi} : G_1/N_1 \rightarrow G_2/N_2$ defined by $\bar{\phi}(gN_1) = \phi(g)N_2$ is an isomorphism.*

Proof. Note that since ϕ is a bijection and $\phi(N_1) = N_2$, we have $\phi^{-1}(N_2) = N_1$, hence for all $g \in G_1$, $\phi(g) \in N_2$ if and only if $g \in N_1$. Consider the map $f : G_1 \rightarrow G_2/N_2$ defined by $f(g) = \phi(g)N_2$. This is just the composition of ϕ with the canonical homomorphism $G_2 \rightarrow G_2/N_2$, so in particular f is a surjective homomorphism. An element $g \in G_1$ is in the kernel of f if and only if $\phi(g)N_2 = N_2$, i.e. if and only if $\phi(g) \in N_2$. Hence by the above, $\ker(f) = N_1$. The conclusion follows by the first isomorphism theorem. \square

3 Products of Finite Cyclic Groups: Powers of Primes

The question we would like to answer is: when is $\mathbb{Z}/a_1\mathbb{Z} \times \dots \times \mathbb{Z}/a_n\mathbb{Z}$ isomorphic to $\mathbb{Z}/b_1\mathbb{Z} \times \dots \times \mathbb{Z}/b_m\mathbb{Z}$? We will start by answering this question in the case when all the a_i and b_i are powers of the same prime p , and we will use this to solve the question in general.

In this section, we always will use additive notation for abelian groups.

Recall the following proposition from class:

Proposition 3.1. *Suppose $n, m \in \mathbb{N}$ and $n|m$. Then $m\mathbb{Z} \leq n\mathbb{Z}$ and $n\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\frac{m}{n}\mathbb{Z}$.*

Powers of Primes

Proposition 3.2. *Let $p \in \mathbb{N}$ be prime, and let*

$$A = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_n}\mathbb{Z}$$

and

$$B = \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_m}\mathbb{Z}$$

where all of the a_i and b_i are natural numbers with $1 \leq a_1 \leq a_2 \cdots \leq a_n$ and $1 \leq b_1 \leq b_2 \leq \cdots \leq b_m$. Then $A \cong B$ if and only if $n = m$ and $a_i = b_i$ for all i .

Proof. We do induction on the largest power of p appearing in either expression, i.e. on $\max(a_n, b_m)$. The case $\max(a_n, b_m) = 0$ is trivial since then $A \cong \{0\} \cong B$ and $n = m = 0$. Now, suppose A and B are as above and suppose that $\phi : A \rightarrow B$ is an isomorphism. Then $\phi(pA) = pB$ (where $pA = \{pa \mid a \in A\}$ is the subgroup of p th multiples of elements of A), so $pA \cong pB$ and $A/pA \cong B/pB$.

Let's first look at A/pA and B/pB . We have

$$pA = p\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times p\mathbb{Z}/p^{a_n}\mathbb{Z},$$

so

$$A/pA \cong \frac{\mathbb{Z}/p^{a_1}\mathbb{Z}}{p\mathbb{Z}/p^{a_1}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}/p^{a_n}\mathbb{Z}}{p\mathbb{Z}/p^{a_n}\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z} (n \text{ times})$$

by the third isomorphism theorem. Likewise

$$B/pB \cong \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z} (m \text{ times}).$$

Thus in particular $|A/pA| = p^n$ and $|B/pB| = p^m$. Since $A/pA \cong B/pB$, we have $p^n = p^m$, hence $n = m$.

Now consider $pA \cong pB$. We have:

$$pA = p\mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times p\mathbb{Z}/p^{a_n}\mathbb{Z} \cong \mathbb{Z}/p^{a_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_n-1}\mathbb{Z},$$

and likewise

$$pB \cong \mathbb{Z}/p^{b_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_n-1}\mathbb{Z}.$$

Now, if $a_i = 1$, then $a_i - 1 = 0$, so in this case $\mathbb{Z}/p^{a_i-1}\mathbb{Z} = \mathbb{Z}/1\mathbb{Z} \cong \{0\}$, so in each expression we have to ignore those factors where $a_i = 1$ or $b_i = 1$.

Suppose that $a_1 = \dots = a_k = 1$ and $a_{k+1} \geq 2$. Likewise, suppose that $b_1 = \dots = b_\ell = 1$ and $b_{\ell+1} \geq 2$. Then from $pA \cong pB$ we get

$$\mathbb{Z}/p^{a_{k+1}-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{a_n-1}\mathbb{Z} \cong \mathbb{Z}/p^{b_{\ell+1}-1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{b_n-1}\mathbb{Z}.$$

Hence by induction we have $n - k = n - \ell$, so $k = \ell$. Likewise by induction we conclude that $a_i - 1 = b_i - 1$ (so $a_i = b_i$) for $k + 1 \leq i \leq n$. And for $1 \leq i \leq k$ we have $a_i = 1 = b_i$, so $a_i = b_i$ for all i . \square

Examples 3.3. 1. We have $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, as we already know.

2. Likewise, we now know that

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},$$

which could have been unpleasant to prove before.

4 Torsion

We now wish to extend the above theorem to a theorem about all products of finite cyclic groups. Recall that if a natural number n has prime factorization $n = p_1^{n_1} \cdots p_k^{n_k}$, then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z},$$

so every cyclic group is a product of cyclic groups of the form $\mathbb{Z}/p^r\mathbb{Z}$, hence

Proposition 4.1. *Every product of finite cyclic groups is isomorphic to a group of the form*

$$\mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_k^{n_k}\mathbb{Z},$$

where $p_1, \dots, p_k \in \mathbb{N}$ are (not necessarily distinct) prime numbers, and $n_1, \dots, n_k \in \mathbb{N}$.

So it suffices to understand groups of the above form. To do this, we need a tool.

Definition 4.2. Let A be an abelian group. The *torsion subgroup* of A , denoted $T(A)$, is the set of elements $a \in A$ having finite order. For each prime $p \in \mathbb{N}$, the *p-torsion subgroup* of A , denoted $T_p(A)$, is the set of elements $a \in A$ such that $o(a)$ is a power of p .

Remark 4.3. Notice that since isomorphisms preserve orders of elements, if $\phi : A \rightarrow B$ is an isomorphism, then also $T(A) \cong T(B)$ and $T_p(A) \cong T_p(B)$.

Examples 4.4. 1. $T(\mathbb{Z}) = \{0\}$ (we say \mathbb{Z} is *torsion-free*). Likewise $T(\mathbb{Q}) = \{0\}$.

2. If A is a finite abelian group, then $T(A) = A$.

3. $T_2(\mathbb{Z}/6\mathbb{Z}) = \{0, 3\} = \langle 3 \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Proposition 4.5. *Let A be an abelian group, and let $p \in \mathbb{N}$ be a prime. Then $T(A)$ and $T_p(A)$ are subgroups of A .*

Proof. Both $T(A)$ and $T_p(A)$ contain the identity element $0 \in A$, so both are nonempty. Suppose that $a, b \in A$ have orders $n, m \in \mathbb{N}$, so $na = 0 = mb$ (recall we're writing our groups additively!). Then

$$nm(a - b) = m(na) - n(mb) = m0 - n0 = 0,$$

hence $a - b$ has finite order, so $T(A)$ is a subgroup of A . Note moreover that $o(a - b)$ divides nm , so if both n and m are powers of p , then so is $o(a - b)$, so also $T_p(A)$ is a subgroup of A . \square

We also need to understand how torsion behaves in products. This will make torsion very easy for us to calculate in the examples we care about.

Proposition 4.6. *Let A and B be abelian groups and let $p \in \mathbb{N}$ be a prime. Then $T(A \times B) = T(A) \times T(B)$ and $T_p(A \times B) = T_p(A) \times T_p(B)$.*

Proof. Let $(a, b) \in A \times B$ be arbitrary. Then $k(a, b) = (ka, kb) = (0, 0)$ if and only if $ka = kb = 0$. Hence (a, b) has finite order if and only if both a and b do, which proves that $T(A \times B) = T(A) \times T(B)$. Moreover, we have already proven that if both a and b have finite order, then $o(a, b) = \text{lcm}(o(a), o(b))$. Hence $o(a, b)$ is a power of p if and only if $o(a)$ and $o(b)$ are, so $T_p(A \times B) = T_p(A) \times T_p(B)$. \square

Example 4.7. $T_3(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) = \mathbb{Z}/3\mathbb{Z} \times \{0\}$.

Corollary 4.8. *Suppose that*

$$A = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \mathbb{Z}/p^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_k}\mathbb{Z} \times \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{n_\ell}\mathbb{Z},$$

where $p \in \mathbb{N}$ is prime and p_1, \dots, p_ℓ are primes different from p . Then

$$T_p(A) = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \mathbb{Z}/p^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_k}\mathbb{Z} \times \{0\} \times \cdots \times \{0\}.$$

Proof. By the previous proposition, we have

$$T_p(A) = T_p(\mathbb{Z}/p^{e_1}\mathbb{Z}) \times \cdots \times T_p(\mathbb{Z}/p^{e_k}\mathbb{Z}) \times T_p(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \cdots \times T_p(\mathbb{Z}/p_\ell^{n_\ell}\mathbb{Z}).$$

Now, every element of $\mathbb{Z}/p^{e_i}\mathbb{Z}$ has order dividing p^{e_i} , hence has order a power of p , so $T_p(\mathbb{Z}/p^{e_i}\mathbb{Z}) = \mathbb{Z}/p^{e_i}\mathbb{Z}$ for all i . Likewise, every element of $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$ has order dividing $p_i^{n_i}$, hence the only element in this group with order a power of p is 0, so $T_p(\mathbb{Z}/p_i^{n_i}\mathbb{Z}) = \{0\}$ for all i , and the statement follows. \square

5 Products of Finite Cyclic Groups: General Case

We are now ready to prove our main theorem about products of finite cyclic groups:

Theorem 5.1. *Suppose that*

$$A = \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{a_n}\mathbb{Z}$$

and

$$B = \mathbb{Z}/q_1^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/q_m^{b_m}\mathbb{Z}$$

where $p_1 \leq \cdots \leq p_n$ and $q_1 \leq \cdots \leq q_m$ are primes (not necessarily distinct) and $a_i, b_i \in \mathbb{N}$ such that $a_i \leq a_{i+1}$ whenever $p_i = p_{i+1}$ and likewise for the b_i 's (i.e. we arrange the a_i, b_i in increasing order whenever possible).

Then $A \cong B$ if and only if $n = m$, $p_i = q_i$ for all i , and $a_i = b_i$ for all i .

Proof. Suppose that $A \cong B$. Then we have $T_p(A) \cong T_p(B)$ for all primes $p \in \mathbb{N}$. $T_p(A)$ is just the direct product of the factors $\mathbb{Z}/p_i^{a_i}\mathbb{Z}$ where $p_i = p$, and likewise for $T_p(B)$. By Prop 3.2, the number of factors and the powers of p appearing in $T_p(A)$ and $T_p(B)$ must be equal; since this is true for all primes p , the theorem follows. \square

Example 5.2. Suppose we want to determine whether $\mathbb{Z}/48\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}$. We break both sides up into prime factors: the left-hand side is isomorphic to

$$\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

while the right-hand side is isomorphic to

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}.$$

By the previous theorem, these groups are not isomorphic.

6 Finitely-Generated Abelian Groups

We want to extend the previous theorem in two ways: first, we want to allow some infinite cyclic factors, i.e. some copies of \mathbb{Z} ; second, we want to show that *every* finite abelian group is actually of the form in Theorem 5.1. This will give us a complete picture of all finite abelian groups. We will do slightly better, and classify all *finitely generated* abelian groups, since it is no more work to do so.

Definition 6.1. Let A be an abelian group. We say that A is n -generated if there exist elements $a_1, \dots, a_n \in A$ such that every element of A is of the form

$$a = \sum_{i=1}^n m_i a_i$$

for some integers $m_1, \dots, m_n \in \mathbb{Z}$. The elements a_1, \dots, a_n are called *generators* for A . We say that A is *finitely generated* (abbreviated f.g.) if A is n -generated for some $n \in \mathbb{N}$.

- Examples 6.2.**
1. \mathbb{Z} is 1-generated. In general, A is 1-generated iff cyclic.
 2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is 2-generated but not 1-generated. A generating set is $\{(1, 0), (0, 1)\}$.
 3. \mathbb{Q} is not finitely generated. As we have seen in the homework, any 2-generated subgroup of \mathbb{Q} is actually 1-generated, i.e. cyclic. By induction, this shows that any n -generated subgroup of \mathbb{Q} is cyclic. So if \mathbb{Q} were n -generated, it would be cyclic, but it is not.

Proposition 6.3. *Let A be an abelian group. Then A is n -generated if and only if there exists a surjective homomorphism $\phi : \mathbb{Z}^n \rightarrow A$.*

Proof. Suppose that A is n -generated, with generators a_1, \dots, a_n . Define $\phi : \mathbb{Z}^n \rightarrow A$ by

$$\phi(m_1, \dots, m_n) = \sum_{i=1}^n m_i a_i.$$

It is easy to see that ϕ is a homomorphism, and ϕ is surjective precisely because a_1, \dots, a_n generate A .

On the other hand, suppose that $\phi : \mathbb{Z}^n \rightarrow A$ is a surjective homomorphism. For each i from 1 to n , let e_i be the element of \mathbb{Z}^n with 1 in the i th entry

and 0 in all other entries. Let $a_i = \phi(e_i)$. Then every element $a \in A$ is of the form

$$a = \phi(m_1, \dots, m_n) = \phi\left(\sum_{i=1}^n m_i e_i\right) = \sum_{i=1}^n m_i \phi(e_i) = \sum_{i=1}^n m_i a_i,$$

hence a_1, \dots, a_n generate A . \square

Corollary 6.4. *Let A and B be abelian groups, suppose that $f : A \rightarrow B$ is a surjective homomorphism, and suppose that A is n -generated. Then B is n -generated.*

Proof. Since A is n -generated, there is a surjective homomorphism $\phi : \mathbb{Z}^n \rightarrow A$. Then $f \circ \phi : \mathbb{Z}^n \rightarrow B$ is a surjective homomorphism, so B is n -generated. \square

Theorem 6.5. *Let A be an n -generated abelian group. Then every subgroup of A is n -generated.*

Proof. Let $H \leq A$ be arbitrary. Let $\phi : \mathbb{Z}^n \rightarrow A$ be a surjective homomorphism. Then $\phi^{-1}(H) \leq \mathbb{Z}^n$, and $\phi : \phi^{-1}(H) \rightarrow H$ is surjective. Hence it suffices to show that $\phi^{-1}(H)$ is n -generated, so we can assume that $A = \mathbb{Z}^n$. Now we prove the theorem by induction on n . If $n = 1$, then $A = \mathbb{Z}$, and every subgroup of \mathbb{Z} is cyclic, i.e. 1-generated.

Suppose the theorem is true for n ; we want to show it holds for $n + 1$. Let $H \leq \mathbb{Z}^{n+1}$ be arbitrary, and let

$$\begin{aligned} \pi : \quad \mathbb{Z}^{n+1} &\rightarrow \mathbb{Z} \\ (a_1, \dots, a_{n+1}) &\mapsto a_{n+1}. \end{aligned}$$

The map π is clearly a homomorphism, so $\pi(H) \leq \mathbb{Z}$. If $\pi(H) = \{0\}$ then $H \subseteq \mathbb{Z}^n \times \{0\} \cong \mathbb{Z}^n$, so H is n -generated by induction. On the other hand, if $\pi(H) \neq 0$, then $\pi(H) = a\mathbb{Z}$ for some $a \in \mathbb{N}$, and we can choose some $h \in H$ such that $\pi(h) = a$.

Now, let $h' \in H$ be arbitrary. Then $\pi(h') \in a\mathbb{Z}$, hence $\pi(h') = ac$ for some $c \in \mathbb{Z}$. Thus we have

$$\pi(h' - ch) = \pi(h') - c\pi(h) = ac - ac = 0,$$

thus $h' - ch \in \ker(\pi) = \mathbb{Z}^n \times \{0\}$. Hence every element of H is of the form $ch + x$ for some $x \in \mathbb{Z}^n \times \{0\} \cap H =: H'$ and some $c \in \mathbb{Z}$.

Now, $H' \subseteq \mathbb{Z}^n \times \{0\} \cong \mathbb{Z}^n$, so by induction H' is n -generated, say by

a_1, \dots, a_n . Then every element of H' can be written as $m_1a_1 + \dots + m_na_n$ for some $m_1, \dots, m_n \in \mathbb{Z}$, so every element of H can be written as

$$m_1a_1 + \dots + m_na_n + ch$$

for some $m_1, \dots, m_n, c \in \mathbb{Z}$. Thus a_1, \dots, a_n, h generate H , so H is $(n + 1)$ -generated. \square

7 Rank and Free Abelian Groups

Now we bring a little “generalized linear algebra” into the picture; we’ll need this to deal with factors of \mathbb{Z} , and this will be a key part of our induction step in the proof of the main theorem.

Definition 7.1. Let A be an abelian group. A set of n distinct elements $\{a_1, \dots, a_n\} \subseteq A$ is called \mathbb{Z} -linearly independent (or just linearly independent if there is no possible confusion) if for all $m_1, \dots, m_n \in \mathbb{Z}$, we have that

$$\sum_{i=1}^n m_i a_i = 0$$

if and only if $m_1 = m_2 = \dots = m_n = 0$. We define the *rank* of A to be the size of the largest set of \mathbb{Z} -linearly independent elements in A .

We call A *free of rank n* if A has a set of n linearly independent generators. Such a set of generators is called a *basis* for A .

Proposition 7.2. *A is free of rank n if and only if $A \cong \mathbb{Z}^n$.*

Proof. Let a_1, \dots, a_n be a basis for A , and let $\phi : \mathbb{Z}^n \rightarrow A$ be defined by

$$\phi(m_1, \dots, m_n) = \sum_{i=1}^n m_i a_i.$$

We know that ϕ is a surjective homomorphism, so it suffices to show that ϕ is injective. Suppose $(m_1, \dots, m_n) \in \ker(\phi)$. Then by definition $\sum_{i=1}^n m_i a_i = 0$. Since the elements a_i are linearly independent, it follows that $m_i = 0$ for all i , hence $(m_1, \dots, m_n) = (0, \dots, 0)$. Thus $\ker(\phi) = \{0\}$, so ϕ is injective, and hence an isomorphism. \square

Proposition 7.3. *If A is free of rank n , then $\text{rank}(A) = n$.*

Proof. By definition, A has an n -element basis, hence in particular has an n -element linearly independent subset, so $\text{rank}(A) \geq n$.

We want to show that $\text{rank}(A) \leq n$. We can assume that $A = \mathbb{Z}^n$ by the previous proposition. Let a_1, \dots, a_{n+1} be $n + 1$ elements of \mathbb{Z}^n ; we have to show that a_1, \dots, a_{n+1} are *not* \mathbb{Z} -linearly independent. Consider \mathbb{Z}^n as a subgroup of \mathbb{Q}^n in the obvious way. The group \mathbb{Q}^n is an n -dimensional \mathbb{Q} -vector space, so the $n + 1$ elements $a_1, \dots, a_{n+1} \in \mathbb{Q}^n$ are \mathbb{Q} -linearly dependent, i.e. there exist rational numbers $\frac{c_1}{d_1}, \dots, \frac{c_{n+1}}{d_{n+1}} \in \mathbb{Q}$, not all equal to 0, such that

$$\sum_{i=1}^{n+1} a_i \frac{c_i}{d_i} = 0.$$

But now, multiplying by $d_1 d_2 \cdots d_{n+1}$, we get that

$$\sum_{i=1}^{n+1} a_i \cdot (c_i d_1 \cdots d_{i-1} d_{i+1} \cdots d_{n+1}) = 0.$$

Since all of the d_i are nonzero and at least one of the c_i are nonzero, we conclude that a_1, \dots, a_{n+1} are \mathbb{Z} -linearly dependent, as desired. \square

Corollary 7.4. *Let $n, m \in \mathbb{N}$. Then $\mathbb{Z}^n \cong \mathbb{Z}^m$ if and only if $n = m$.*

Corollary 7.5. *Let A be an abelian group. Suppose that A is n -generated. Then $\text{rank}(A) \leq n$.*

Proof. Let $\phi : \mathbb{Z}^n \rightarrow A$ be a surjective homomorphism. Suppose that $a_1, \dots, a_k \in A$ are linearly independent. Since ϕ is surjective, there exist $b_1, \dots, b_k \in \mathbb{Z}^n$ such that $\phi(b_i) = a_i$. Suppose that

$$\sum_{i=1}^k m_i b_i = 0.$$

Then applying ϕ , we have

$$0 = \phi \left(\sum_{i=1}^k m_i b_i \right) = \sum_{i=1}^k m_i \phi(b_i) = \sum_{i=1}^k m_i a_i.$$

Since the a_i are linearly independent, we have $m_1 = m_2 = \cdots = m_k = 0$. Hence the b_i are also linearly independent. By the previous proposition, $k \leq n$, hence $\text{rank}(A) \leq n$. \square

Finally, we need one last simple proposition about rank:

Proposition 7.6. *Let A and B be abelian groups of finite rank. Then $\text{rank}(A \times B) \geq \text{rank}(A) + \text{rank}(B)$.*

Proof. Suppose that $\text{rank}(A) = k$ and $\text{rank}(B) = \ell$. Let $a_1, \dots, a_k \in A$ be linearly independent, and let $b_1 \dots b_\ell$ be linearly independent. Then I claim that $(a_1, 0), \dots, (a_k, 0), (0, b_1), \dots, (0, b_\ell)$ are linearly independent in $A \times B$. Suppose that

$$\sum_{i=1}^k m_i(a_i, 0) + \sum_{j=1}^{\ell} n_j(0, b_j) = (0, 0).$$

Then

$$\sum_{i=1}^k m_i a_i = 0 \quad \text{and} \quad \sum_{j=1}^{\ell} n_j b_j = 0.$$

Hence by linear independence we have $m_1 = \dots = m_k = 0$ and $n_1 = \dots = n_\ell = 0$, as desired. \square

8 The Big Theorem

Theorem 8.1 (The Structure Theorem for Finitely Generated Abelian Groups, Uniqueness Part). *Suppose that*

$$A = \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{a_n}\mathbb{Z} \times \mathbb{Z}^r$$

and

$$B = \mathbb{Z}/q_1^{b_1}\mathbb{Z} \times \dots \times \mathbb{Z}/q_m^{b_m}\mathbb{Z} \times \mathbb{Z}^s$$

where $p_1 \leq \dots \leq p_n$ and $q_1 \leq \dots \leq q_m$ are primes (not necessarily distinct) and $a_i, b_i \in \mathbb{N}$ such that $a_i \leq a_{i+1}$ whenever $p_i = p_{i+1}$ and likewise for the b_i 's (i.e. we arrange the a_i, b_i in increasing order whenever possible).

Then $A \cong B$ if and only if $r = s$, $n = m$, $p_i = q_i$ for all i , and $a_i = b_i$ for all i .

Proof. Suppose that $A \cong B$. Then $T(A) \cong T(B)$, and

$$T(A) = \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_n^{a_n}\mathbb{Z} \times \{0\}$$

while

$$T(B) = \mathbb{Z}/q_1^{b_1}\mathbb{Z} \times \dots \times \mathbb{Z}/q_m^{b_m}\mathbb{Z} \times \{0\}.$$

By Theorem 5.1 we get that $n = m$, $p_i = q_i$ for all i , and $a_i = b_i$ for all i . Now, we also have $A/T(A) \cong B/T(B)$. But $A/T(A) \cong \mathbb{Z}^r$ and $B/T(B) \cong \mathbb{Z}^s$. By Corollary 7.4 we have $r = s$. \square

Theorem 8.2 (The Structure Theorem for Finitely Generated Abelian Groups, Existence Part). *Let A be a finitely-generated abelian group. Then A is isomorphic to a group of the form*

$$\mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{a_n}\mathbb{Z} \times \mathbb{Z}^r.$$

This will follow from:

Theorem 8.3. *Let H be a subgroup of \mathbb{Z}^n . Then*

1. H is free of rank $m \leq n$, and
2. There exist a basis y_1, \dots, y_n of \mathbb{Z}^n and integers $a_1, \dots, a_m \in \mathbb{Z}$ such that a_1y_1, \dots, a_my_m is a basis for H .

Proof. The theorem is trivial if $H = \{0\}$, so we can assume $H \neq \{0\}$, so H has some element with a non-zero coordinate, and hence there is some homomorphism $\phi : \mathbb{Z}^n \rightarrow \mathbb{Z}$ such that $\phi(H) \neq \{0\}$. Consider the set

$$S = \{k \in \mathbb{N} \mid k\mathbb{Z} = \phi(H) \text{ for some homomorphism } \phi : \mathbb{Z}^n \rightarrow \mathbb{Z}\}.$$

Then S is nonempty, so has a smallest element a_1 . Let $f : \mathbb{Z}^n \rightarrow \mathbb{Z}$ be a homomorphism such that $f(H) = a_1\mathbb{Z}$, and let $y \in H$ be an element such that $f(y) = a_1$.

I claim now that $a_1 \mid \phi(y)$ for every homomorphism $\phi : \mathbb{Z}^n \rightarrow \mathbb{Z}$. Indeed, suppose $\phi : \mathbb{Z}^n \rightarrow \mathbb{Z}$ is another homomorphism, and let $\ell = \phi(y)$. Then there exist $q, r \in \mathbb{Z}$, $0 \leq r < a_1$ such that $\ell = qa_1 + r$. Let $\phi' : \mathbb{Z}^n \rightarrow \mathbb{Z}$ be the homomorphism defined by

$$\phi'(z) = \phi(z) - q \cdot f(z).$$

It is easy to check that this is a homomorphism, and we have $\phi'(y) = \ell - qa_1 = r$. Hence $r\mathbb{Z} \subseteq \phi'(H)$. Now, if $r \neq 0$, then $\phi'(H) = r'\mathbb{Z} \neq 0$ for some r' dividing r , and so in particular $r' \in S$. But then $0 < r' \leq r < a_1$, which contradicts the minimality of a_1 in S . Thus $r = 0$, and hence a_1 divides ℓ .

Apply this statement to the projection homomorphisms

$$\begin{aligned} \pi_i : \quad \mathbb{Z}^n &\rightarrow \mathbb{Z} \\ (a_1, \dots, a_n) &\mapsto a_i. \end{aligned}$$

We see that a_1 divides $\pi_i(y)$ for all i . Write $\pi_i(y) = a_1b_i$ for some $b_i \in \mathbb{Z}$. Then we have

$$y = (a_1b_1, a_1b_2, \dots, a_1b_n).$$

Define

$$y_1 = (b_1, b_2, \dots, b_n).$$

Then $a_1 y_1 = y$ and $a_1 f(y_1) = f(a_1 y_1) = f(y) = a_1$, so $f(y_1) = 1$.

I claim that we can take y_1 as our first basis element for \mathbb{Z}^n and $y = a_1 y_1$ as our first basis element for H . I claim first that we have:

1. $\mathbb{Z}^n = \mathbb{Z}y_1 \times \ker(f)$ and
2. $H = \mathbb{Z}a_1 y_1 \times (\ker(f) \cap H)$.

To prove (1), let $x \in \mathbb{Z}^n$ be arbitrary; we have $x = f(x)y_1 + (x - f(x)y_1)$. Now,

$$f(x - f(x)y_1) = f(x) - f(x)f(y_1) = f(x) - f(x) = 0,$$

so $x - f(x)y_1 \in \ker(f)$, hence $\mathbb{Z}^n = \mathbb{Z}y_1 + \ker(f)$, and we have to show that $\mathbb{Z}y_1 \cap \ker(f) = 0$. So, suppose that $f(cy_1) = 0$. Then $0 = c \cdot f(y_1) = c \cdot 1 = c$, hence $cy_1 = 0$. This proves (1).

To prove (2), note first that the proof of part (1) already showed that $\mathbb{Z}a_1 y_1 \cap (\ker(f) \cap H) = 0$ as a special case of $\mathbb{Z}y_1 \cap \ker(f) = 0$. Now, suppose that $x \in H$. Then since $f(H) = a_1 \mathbb{Z}$, we have $a_1 | f(x)$, hence we can write $f(x) = ba_1$ with $b \in \mathbb{Z}$. Then

$$x = f(x)y_1 + (x - f(x)y_1) = ba_1 y_1 + (x - ba_1 y_1) \in \mathbb{Z}a_1 y_1 + (\ker(f) \cap H).$$

We now prove part (1) of the theorem by induction on the rank m of H , which is finite since H is finitely generated (here we have used both Theorem 6.5 and Corollary 7.5). If $\text{rank}(H) = 0$, then every element of H has finite order, so $H = \{0\}$ since 0 is the only element of \mathbb{Z}^n with finite order. Suppose on the other hand that $m > 0$. Then since $H = \mathbb{Z}a_1 y_1 \times (\ker(f) \cap H)$ and $\mathbb{Z}a_1 y_1$ is free of rank 1, we have that $m = \text{rank}(H) \geq 1 + \text{rank}(\ker(f) \cap H)$, hence $(\ker(f) \cap H)$ has rank $\leq m - 1$. By induction, $(\ker(f) \cap H)$ is free, hence H is free. The fact that $\text{rank}(H) \leq n$ will follow from (2).

Finally, we prove part (2) of the theorem by induction on n . By part (1), we have that $\ker(f)$ is free, and hence free of rank $n - 1$. By the induction hypothesis applied to $\ker(f)$ and its subgroup $\ker(f) \cap H$, there exist a basis y_2, \dots, y_n of $\ker(f)$ and integers $a_2, \dots, a_m \in \mathbb{Z}$ such that $a_2 y_2, \dots, a_m y_m$ is a basis of $\ker(f) \cap H$. Hence y_1, \dots, y_n is a basis of \mathbb{Z}^n and $a_1 y_1, \dots, a_m y_m$ is a basis of H . \square

Proof of Theorem 8.2. Let A be an n -generated abelian group, and let $\phi : \mathbb{Z}^n \rightarrow A$ be a surjective homomorphism. Let $H = \ker(\phi)$. Then $A \cong \mathbb{Z}^n / H$,

so we need only show that \mathbb{Z}^n/H is isomorphic to a group of the desired form. By the previous proposition, we can choose a new basis for \mathbb{Z}^n such that, with respect to this new basis, H is of the form

$$H = a_1\mathbb{Z} \times \cdots \times a_m\mathbb{Z} \times \{0\} \times \cdots \times \{0\}.$$

Then

$$\mathbb{Z}^n/H \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_m\mathbb{Z} \times \mathbb{Z}^{n-m},$$

as desired. □

Example 8.4. Let's list all abelian groups of order 36. We have $36 = 2^2 \cdot 3^2$, so every abelian group of order 36 is isomorphic to one of:

1. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/36\mathbb{Z}$,
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$,
3. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, or
4. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Example 8.5. Let H be the subgroup of \mathbb{Z}^2 generated by $(2, 4)$. Then \mathbb{Z}^2/H is a finitely generated abelian group, so we should be able to write it as a direct product of cyclic groups. Let e_1, e_2 be the standard basis of \mathbb{Z}^2 , so every element of H is of the form $2ne_1 + 4ne_2$. Let's choose a new basis of \mathbb{Z}^2 : replace e_1 by $e_1 + 2e_2$, i.e. take the basis $\{e'_1 = e_1 + 2e_2, e'_2 = e_2\}$. It is easy to check that this is still a basis. With respect to this basis, every element of H is of the form $2ne'_1$ for some $n \in \mathbb{Z}$, i.e. H is the subgroup generated by $2e'_1$. Hence we have

$$\mathbb{Z}^2/H \cong \mathbb{Z}^2/(2\mathbb{Z} \times \{0\}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$