Classification of Finitely Generated Abelian Groups

Theorem 1. *Let A be a finitely generated abelian group. Then there is an isomorphism:*

$$A \cong \mathbb{Z}^r \times \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_\ell^{a_\ell}}$$

where the a_i are positive integers, r is a non-negative integer, and the p_i are positive primes, not necessarily distinct.

Proof: Note that in this entire proof, we will be dealing exclusively with abelian groups, so we will always write the group operation additively.

We need some setup before we start. Let T be the subset of A consisting of all the elements of finite order. It's called the **torsion subgroup** of A, a name justified by the following lemma:

Lemma 2. *The torsion subgroup of an abelian group A is a subgroup of A.*

Proof: We just need to show that T contains 0, and is closed under $+$ and $-$. It's obvious that T contains 0, so let x and y be elements of T. Then there are integers n and m such that $nx = my = 0$. If we let N be the least common multiple of n and m, then $Nx \pm Ny = 0$. This means that T is closed under addition and subtraction, so we win. ♣

If the theorem is true (which of course it is, or it wouldn't be a theorem), then T had better end up being the product of all those cyclic groups. So throughout this proof, think about T as being the object that will eventually end up being the product of those cyclic groups. It will be convenient to talk about the subgroups $T(p_i)$ of T: $T(p_i)$ is defined to be the subgroup of elements of T whose finite order is a power of p_i.

Better yet, A is abelian, so T is a normal subgroup. This means we can talk about the quotient group $F = A/T$. Again, if the theorem is true, F had better end up being isomorphic to $\mathbb{Z}^r$ for some integer r. So for the rest of this proof, think of F as being isomorphic to $\mathbb{Z}^r$.

One important thing to note is that F is finitely generated, because generators of A reduce modulo T to generators of F.

The proof is pretty long, so we'll need a plan. Here's the plan:

(1) Show that F is isomorphic to a subgroup of $\mathbb{Z}^k$ for some integer k.
(2) Show that every subgroup of $\mathbb{Z}^k$ is isomorphic to $\mathbb{Z}^r$ for some r.
(3) Show that A is isomorphic to $F \times T$.
(4) Show that T is isomorphic to the product $T(p_1) \times \ldots \times T(p_\ell)$.
(5) Show that $T(p_i)$ is isomorphic to the product of cyclic groups in a unique way.
(6) Finish the proof of the theorem.

Step 1: Show that F is isomorphic to a subgroup of $\mathbb{Z}^k$ for some integer k.

First, we make a quick definition:

Definition 1. *Let $v_1, \ldots, v_k$ be elements of an abelian group A. We say that $v_1, \ldots, v_k$ are* **linearly independent** *if the only integers $a_1, \ldots, a_k$ satisfying $a_1v_1 + \ldots + a_kv_k = 0$ are the integers $a_1 = \ldots = a_k = 0$. Note that this is just like the definition of linearly independence in linear algebra, except that the coefficients are integers.*

First, note that F contains no elements of finite order, because if $na \equiv 0 \pmod{T}$, then na has finite order m, meaning that $mna = 0$, so $a \in T$ and therefore $a = 0$ in $F = A/T$.

Let $v_1, \ldots, v_k$ be a maximal linearly independent subset of F. By this I mean that there are no linearly independent sets containing $v_1, \ldots, v_k$ as a proper subset. It might happen that $v_1, \ldots, v_k$ generate F, but just in case they don't, let's choose finitely many more generators $v_{k+1}, \ldots, v_m$ so that $v_1, \ldots, v_m$ are generators of F.

By the maximality of $v_1, \ldots, v_k$, we know that for every i greater than k, there are integers $\alpha_i, a_{i1}, \ldots, a_{ik}$, not all zero, such that $\alpha_i v_i = a_{i1}v_1 + \ldots + a_{ik}v_k$. Moreover, α_i in particular can't be zero, because otherwise we'd have a nontrivial linear dependence relation between $v_1, \ldots, v_k$. The magic step is now to choose α to be the least common multiple of all the α_i. Then for every v_j (j from 1 to m!), the element αv_j is a linear combination of $v_1, \ldots, v_k$. Define a homomorphism $f\colon F \to < v_1, \ldots, v_k > \cong \mathbb{Z}^k$ by $f(x) = \alpha x$. Since F contains no elements of finite order, this is an injective homomorphism, so F is isomorphic to $\mathrm{im} f$. Step 1 is done!

Step 2: Show that every subgroup of $\mathbb{Z}^k$ is isomorphic to $\mathbb{Z}^r$ for some r.

Before we get to the guts of Step 2, we need a couple of extremely interesting and useful lemmas.

Lemma 3. *Let A be an abelian group, and let $\phi\colon A \to \mathbb{Z}^n$ be an onto homomorphism. Then there is a homomorphism $\psi\colon \mathbb{Z}^n \to A$ such that $\phi \circ \phi = id$.*

Definition 2. *If $\phi\colon A \to B$ is an onto homomorphism, then a homomorphism $\psi\colon B \to A$ satisfying $\phi \circ \psi = id$ is called a* **section** *of ϕ.*

I think of onto homomorphisms (and, indeed, onto functions in general) as being vertical, with the domain being dropped on the range. A section of such a vertical map is a function aimed straight up: each element of B is mapped to an element of A that is directly above it, so that when you plug the raised element back into ϕ, it falls right back down where it came from. This is, for any $b \in B$, we have $\phi(\psi(b)) = b$.

This, in a weird way, is what inspires the name "section" for such homomorphisms. If the "lifting" of ψ is somehow uniform, then the image of ψ is a sort of cross section of A.

Proof: Let e_i be the ith standard unit basis vector in $\mathbb{Z}^n$ – that is, let e_i be the vector with all zeroes, except a 1 in the ith coordinate. Because ϕ is onto, there is at least one element a_i such that $\phi(a_i) = e_i$. (There may be more than one choice of a_i – pick any one.) Define $\psi(x_1, \ldots, x_n) = x_1a_1 + \ldots + x_na_n$. It's easy to check that this a well defined homomorphism that satisfies all the criteria of the lemma, so we're done. ♣

Lemma 4. *Let $\phi\colon A \to B$ be an onto homomorphism of abelian groups, and let $\psi\colon B \to A$ be a section of ϕ. Then $A \cong \ker(\phi) \times im(\psi)$.*

Proof: Define $f\colon A \to \ker(\phi) \times \mathrm{im}(\psi)$ by $f(a) = (a - \psi(\phi(a)), \psi(\phi(a)))$, and define $h\colon \ker(\phi) \times \mathrm{im}(\psi) \to A$ by $h(x, y) = x + y$. It's straightforward to check that f and h are mutually inverse homomorphisms (so do it!), which means they're the isomorphisms we're looking for. ♣

We're ready to attack Step 2 now. It is precisely the following lemma:

Lemma 5. *Let $F \subseteq \mathbb{Z}^n$ be any subgroup. Then $F \cong \mathbb{Z}^r$ for some $r \leq n$.*

Proof of Lemma: We proceed by induction on n. We start the induction with $n = 1$. Let F be a subgroup of $\mathbb{Z}$. If $F = \{0\}$, then we're already done, because $\{0\} \cong \mathbb{Z}^0$. Otherwise, F must contain at least one nonzero element, which might as well be positive because if $x \in F$ then $-x \in F$. Let k be the smallest positive element of F. Then the subgroup $< k >$ is contained in F, and if $x \in F$, then the greatest common divisor g of k and x is also in F, since there are integers a and b such that $g = ax + bk \in F$. But g is positive, and it's in F, and it can't be smaller than k, so it must be equal to k! This means that g is in $< k >$, so $F =< k > \cong \mathbb{Z}^1$.

Now assume that the lemma is true for $m < n$. Let $\pi\colon \mathbb{Z}^n \to \mathbb{Z}$ be defined by $\pi(a_1, \ldots, a_n) = a_1$. Then $\ker \pi \cong \mathbb{Z}^{n-1}$, so by induction $\ker \pi \cap F \cong \mathbb{Z}^m$ for some $m \leq n - 1$. We now have an onto homomorphism $\pi\colon F \to H$ for some subgroup H of $\mathbb{Z}$. By induction, $H \cong \mathbb{Z}^i$ for some i. By Lemma 3, there is a section ψ of π, which by Lemma 4 means that $F \cong \ker \pi \times \mathrm{im}\psi \cong \mathbb{Z}^m \times \mathbb{Z}^i \cong \mathbb{Z}^r$ for some integer r, as desired. So long, Step 2.

Step 3: Show that A is isomorphic to $F \times T$.

This is easy. The quotient homomorphism $q\colon A \to F \cong \mathbb{Z}^r$ has a section $\psi\colon F \to A$, by Lemma 3. By Lemma 4, this means that $A \cong \ker(q) \times \mathrm{im}\psi \cong T \times F$.

Note that this also means that T is finitely generated, since $T \cong A/F$, and reducing generators of A modulo F will give generators for T.

Step 4: Show that T is isomorphic to the product $T(p_1) \times \ldots \times T(p_\ell)$.

Since T is finitely generated, and all its elements have finite order, and since it's abelian, it follows that T is finite. This is because if $t_1, \ldots, t_k$ are generators of T, then any element of T can be written as $a_1 t_1 + \ldots a_k t_k$ for integers $a_1, \ldots, a_k$. Since each of the t_i have finite order, we can assume that the coefficients a_i can all be reduced modulo the order n_i of t_i. We conclude that there are only finitely many elements of T.

Thus, say T has m elements, and factor $m = p_1^{n_1} \ldots p_\ell^{n_\ell}$. For each i, define the subgroup $T(p_i)$ to be the set of elements of order p_i^α for some nonnegative integer α. It's easy to check that $T(p_i)$ is a group, and that $p_i^{n_i} g = 0$ for all $g \in T(p_i)$. We will now deal with Step 4.

First, define integers $\alpha_1, \ldots, \alpha_\ell$ by the Chinese Remainder Theorem so that $\alpha_i \equiv 0 \bmod p_j^{n_j}$ for $i \neq j$, but $\alpha_i \equiv 1 \bmod p_i^{n_i}$. Then define $h\colon T \to T(p_1) \times \ldots \times T(p_\ell)$ by:

$$h(g) = (\alpha_1 g, \ldots, \alpha_\ell g)$$

Further, define $f\colon T(p_1) \times \ldots \times T(p_\ell) \to T$ by:

$$f(g_1, \ldots, g_\ell) = g_1 + \ldots + g_\ell$$

It's clear that both f and h are homomorphisms, since $p_i^{n_i}(\alpha_i)$ is a multiple of m, and therefore $p_i^{n_i}(\alpha_i g) = 0$ (remember that the order of g will divide the order m of the group T), and so $\alpha_i g \in T(p_i)$ and h is well defined. We will now show that f and h are mutually inverse, and therefore that they are isomorphisms.

We have $f(h(g)) = f(\alpha_1 g, \ldots, \alpha_\ell g) = \alpha_1 g + \ldots + \alpha_\ell g = (\alpha_1 + \ldots + \alpha_\ell) g$. But for each i, we know that $\alpha_1 + \ldots \alpha_\ell \equiv 1 \bmod p_i^{n_i}$, so by the Chinese Remainder Theorem, it follows that $\alpha_1 + \ldots + \alpha_\ell \equiv 1 \bmod m$. Therefore, we find that $(\alpha_1 + \ldots + \alpha_\ell) g = (1 + Nm) g = g$, and $f(h(g)) = g$, as desired.

Conversely, we have $h(f(g_1, \ldots, g_\ell)) = (\alpha_1 g_1, \ldots, \alpha_\ell g_\ell)$, so to finish the claim we need only prove that $\alpha_i g_i = g_i$ for all i. To do this, note that since $g_i \in T(p_i)$, we know that the

order of g_i will divide m, and so since $g_i \in T(p_i)$, it follows that $p_i^{n_i} g_i = 0$. Thus, we get $\alpha_i g_i = (1 + N p_i^{n_i}) g_i = g_i$, as desired.

Step 5: Show that $T(p_i)$ is isomorphic to the product of cyclic groups in a unique way.

Step 5 is precisely the following lemma.

Lemma 6. *Let p be a prime, and let G be a finite abelian group with the property that every element of G has order equal to some power of p. Then G is isomorphic to $\mathbb{Z}_{p^{m_1}} \times \ldots \times \mathbb{Z}_{p^{m_t}}$ for some positive integers m_i, and moreover this product representation is unique up to permutation of the factors.*

Proof of Lemma: Let d be the order of G. If d is relatively prime to p, then $d = 1$ (since if G is nontrivial it will contain some element of order p), in which case the lemma is trivially true. We now proceed by induction on d.

Let $g \in G$ be the element of maximal order, say p^a, and let H be the subgroup $\langle g \rangle$ generated by g. Consider the group G/H. It has $d/p^a < d$ elements, and clearly every element of G/H has order equal to some power of p, so by induction we can write $G/H \cong \mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_s}}$, where $a_i \leq a$ for each i (since g has maximal order in G).

Claim 7. $G \cong H \times (G/H)$.

Proof of Claim: Let $g_1 + H, \ldots, g_s + H$ be the elements of G/H which correspond, respectively, to the vectors $(1, 0, \ldots, 0), \ldots, (0, 0, \ldots, 1)$ in $\mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_s}}$. Then we have $G/H \cong \langle g_1 + H \rangle \times \ldots \times \langle g_s + H \rangle$. Moreover, we know that $(g_i + H)$ has order p^{a_i} in G/H, so that $p^{a_i} g_i = rg$ for some integer r. We wish to show that we can take $r = 0$.

If not, then write $r = p^u r'$ for some integer r' which is relatively prime to p. Then rg has order p^{a-u}: certainly $p^{a-u} rg = p^a r' g = 0$, and if $nrg = 0$ for some n, then $p^a | nr$, so $p^{a-u} | n$. Therefore, g_i has order p^{a-u+a_i} in G. But g has maximal order amongst all elements of G, so $a \geq a - u + a_i$ and hence $u \geq a_i$.

But this means we can write $p^{a_i} g_i = rg = p^u r' g$, so that:

$$p^{a_i}(g_i - p^{u-a_i} r' g) = 0$$

Since $p^{u-a_i} r' g \in H$, if we replace g_i with $g_i - p^{u-a_i} r' g$, then we may assume that $r = 0$ and that g_i has order exactly p^{a_i} in G. In particular, notice that for any integer n, that if $ng_i \in H$, then $ng_i = 0$.

Let N be the subgroup of G generated by the g_i. Then N is isomorphic to G/H via the quotient map q: it certainly maps onto G/H, and if $q(\sum z_i g_i) = 0$ for some integers z_i, then $\sum z_i g_i \in H$, so by the structure of G/H, this means that $z_i g_i \in H$ for each i. (Remember that $g_i + H$ corresponds to the vector $(0, 0, \ldots, 1, \ldots, 0) \in \mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_s}}$.) But we just proved that $z_i g_i \in H$ if and only if $z_i g_i = 0$ in G, so we conclude that $\sum z_i g_i \in N$ reduces to 0 modulo H if and only if $\sum z_i g_i = 0$ in G, and hence that reduction modulo H maps N isomorphically onto G/H.

Thus, to prove the claim, we just need to show that $H + N = G$ and $H \cap N = \{0\}$. The former claim is easy: if $x \in G$, then we can write $x \cong y \bmod H$ for some $y \in N$, so $x = y + h$ for some $y \in N$, $h \in H$. Now assume that $x \in H \cap N$. Then $q(x) = 0$ and $x \in N$, which by the previous paragraph means that $x = 0$ in G. So we're done. ♣

Since $H \cong \mathbb{Z}_{p^a}$, this means that $G \cong \mathbb{Z}_{p^a} \times \mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_s}}$, so we've proven the existence part of the Lemma.

To prove uniqueness, assume that $G \cong \mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_s}} \cong \mathbb{Z}_{p^{b_1}} \times \ldots \times \mathbb{Z}_{p^{b_t}}$. For any positive integer A, it's clear that if $m \leq A$, then there are exactly p^m elements g of $\mathbb{Z}_{p^A}$ such that $p^m g = 0$; otherwise, there are p^A.

For any positive integer A, let k_A be the number of integers i such that $a_i = A$, and let ℓ_A be the number of integers i such that $b_i = A$. If we can show that $k_A = \ell_A$ for all A, then it will follow that the two product representations are the same. By considering the two product representations of G, we can compute that in $\mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_s}}$, the number of elements g satisfying $p^A g = 0$ is:

$$(p^A)^{\sum_{B \geq A} k_B} \prod_{B<A} (p^B)^{k_B}$$

and in $\mathbb{Z}_{p^{b_1}} \times \ldots \times \mathbb{Z}_{p^{b_t}}$, the number of elements g satisfying $p^A g = 0$ is:

$$(p^A)^{\sum_{B \geq A} \ell_B} \prod_{B<A} (p^B)^{\ell_B}$$

Since these two numbers must be the same, we can equate exponents of p:

$$\sum_{B \geq A} A k_B + \sum_{B<A} B k_B = \sum_{B \geq A} A \ell_B + \sum_{B<A} B \ell_B$$

This is true for all positive integers A, so it's true for $A+1$ as well:

$$\sum_{B>A} (A+1) k_B + \sum_{B \leq A} B k_B = \sum_{B>A} (A+1) \ell_B + \sum_{B \leq A} B \ell_B$$

By subtracting the first equation from the second, we find:

$$\sum_{B>A} k_B = \sum_{B>A} \ell_B$$

for any positive integer A. So this too must be true for $A-1$:

$$\sum_{B \geq A} k_B = \sum_{B \geq A} \ell_B$$

By subtracting the further two equations, we find that $k_A = \ell_A$. But this means that the two product representations are equal! So we're done. ♣

Step 6: Finish the proof of the theorem.

This is now routine. We know that $A \cong F \times T \cong \mathbb{Z}^r \times T(p_1) \times \ldots \times T(p_\ell) \cong \mathbb{Z}^r \times \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_\ell^{a_\ell}}$, so all that's left is to prove the uniqueness of the decomposition. Well, r is uniquely determined because it's the size of the maximal linearly independent subset of A. The primes p_i are uniquely determined because they're precisely the prime divisors of the order of T, and the groups $T(p_i)$ are uniquely determined up to isomorphism because they're defined solely in terms of the group operation of A, which is preserved by isomorphisms. And finally, the uniqueness of the decomposition of $T(p_i)$ is proven by Step 5. Ta da!