The fundamental theorem about finitely generated abelian groups

**Theorem:** Suppose $A$ is a finitely generated abelian group. Then there are integers $r, s \geq 0$ and $n_1, \ldots, n_s \geq 1$ such that

1. $n_i$ divides $n_{i+1}$ for all $i$.

2. $A$ is isomorphic to the direct sum

$$
\mathbb{Z}^r \oplus \left( \bigoplus_{i=1}^{s} \mathbb{Z}/n_i \right)
$$

3. The integers $r, s, n_1, \ldots, n_s$ both determine and are determined by the isomorphism class of $A$.

**Terminology:** The ideals $n_i\mathbb{Z}$ are called the invariant factors of $A$.  


Example: The isomorphism classes of abelian groups $A$ of order $n$ correspond bijectively to those choices of $(r, s, n_1, \ldots, n_s)$ such that $r = 0$ and $n = \prod_{i=1}^{s} n_i$.

I’ll postpone the proof of the theorem till we consider its generalization to modules over a principal ideal domain.

Note that the subgroup $A_{tor}$ of elements of finite order in $A$ is just

$$A_{tor} = \bigoplus_{i=1}^{s} \mathbb{Z}/n_i.$$  \hspace{1cm} (1)
Since $A_{tor}$ is a finite abelian group, its nilpotent and hence the product of its $p$-Sylows. (One can also show this directly from (1). Applying the theorem to each of the $p$-Sylows of $A_{tor}$ gives a direct sum decomposition

$$A_{tor} = \bigoplus_{\text{prime } p \mid \# A_{tor}} \bigoplus_{i=1}^{b_p} \mathbb{Z}/p^{a_{p,i}} \quad (2)$$

for some integers $a_{p,i}$. The ideal $p^{a_{p,i}}\mathbb{Z}$ are called the elementary divisors of $A_{tor}$.

To find the elementary divisors from the invariant factor description

$$A_{tor} = \bigoplus_{i=1}^{s} \mathbb{Z}/n_i$$

one writes

$$\mathbb{Z}/n_i = \bigoplus_{\text{prime } p \mid n_i} \mathbb{Z}/p^{b_{i,p}}$$

where $p^{b_{i,p}} || n_i$. 

3
To find the invariant factors $n_i$ from the elementary divisor description, note the largest $n_s$ is the product over all $p|\#G$ of the largest power of $p$ appearing in the elementary divisor description

$$A_{tor} = \bigoplus_{\text{prime } p|\#A_{tor}} b_p \bigoplus_{i=1}^{b_p} \mathbb{Z}/p^{a_{p,i}}$$

One then cancels out these summands and continues.

**Random abelian groups:** Statistical questions about randomly chosen abelian groups have recently become relevant to number theory due to work of Cohen and Lenstra ("Heuristics on class groups of number fields. Number theory," Lecture Notes in Math., 1068.) For example, one can consider the asymptotic number of isomorphism classes of abelian groups of order $n$ as $n \to \infty$. Sometimes it is more natural to weight the isomorphism class of $A$ by $1/\#\text{Aut}(A)$. 
Direct limits in categories

**Def:** An index set $I$ is directed if it has a partial order $\leq$ on $I$ such that for each $i, j \in I$ there is a $k \in I$ such that $i \leq k$ and $j \leq k$.

**Example:** $\mathbb{Z}$ with the usual ordering.

**Def:** A directed family of morphisms in a category $\mathcal{C}$ is given by a collection $\{A_i\}_{i \in I}$ of objects in $\mathcal{C}$ together with morphisms $f_{i,j} : A_i \to A_j$ for $i \leq j$ which respect composition. So, if $i \leq j \leq k$ then

$$f_{i,k} = f_{j,k} \circ f_{i,j}$$
**Example 1:** Let $I$ be the positive integers. Define $A_i = \frac{1}{i!} \cdot \mathbb{Z}$, and let

$$f_{i,j}: A_i = \frac{1}{i!} \cdot \mathbb{Z} \to A_j = \frac{1}{j!} \cdot \mathbb{Z}$$

be the inclusion homomorphism.

**Example 2:** Again let $I$ be the positive integers. Define $A_i$ to be the free group on generators $\{x_1, \ldots, x_i\}$, and let $A_i \to A_j$ be the natural inclusion.
**Def:** An object $D$ in $\mathcal{C}$ together with a family of morphisms $\mathbf{d} = \{d_i : A_i \to D\}_{i \in I}$ in $\mathcal{C}$ is a **direct limit** for the family $\{A_i, f_{i,j}\}$ if the following is true:

1. The homomorphism $d_i$ respect the maps $f_{i,j} : A_i \to A_j$ for $i \leq j$. In other words,
   $$d_i = d_j \circ f_{i,j}.$$

2. The pair $(D, \mathbf{d})$ is universal with respect to pairs satisfying condition (1). So if $(D', \mathbf{d}')$ is any other such pair, there is a unique $h : D \to D'$ in $\mathcal{C}$ such that
   $$d'_i = h \circ d_i$$
   for all $i$.

**Notation:** The direct limit is
$$D = \lim_{\longrightarrow} A_i$$
**Example:** Suppose as before that

\[ A_i = \frac{1}{i!} \mathbb{Z} \]

for all \( i \), with \( A_i \to A_j \) being inclusion if \( i \leq j \).

Let's check that \( D = \mathbb{Q} \) with the inclusion maps \( d_i : A_i \to D \) is a direct limit \( \lim_{i} A_i \).

The \( d_i \) certainly satisfy the consistency condition (1).

For condition (2), we need to define \( h : D \to D' \). But each element of \( D \) arises as \( d_i(\alpha) \) for some sufficiently large \( i \) and some \( \alpha \in A_i \). So we define \( h(d_i(\alpha)) = d'_i(\alpha) \). This is consistent (i.e. independent of the choice of \( i \)) because of the consistency condition for \( (D', \{d'_i\}_i) \).

**Exercise:** What happens if \( A_i = \mathbb{Z} \) for all \( i \) and \( f_{i,j} : A_i \to A_j \) is multiplication by \( j!/i! \) for \( i \leq j \)?
Theorem: Direct limit exist in the category of abelian groups.

Proof: Let \( \{A_i\}_{i \in I} \) be a directed family of abelian groups, with transition homomorphisms

\[ f_{i,j} : A_i \to A_j \]

for \( i \leq j \). Define

\[ A = \bigoplus_{i \in I} A_i \]

to be the direct sum of the \( A_i \). Let \( B \) be the submodule of \( A' \) generated by all elements of \( A' \) of the form

\[ (0, 0, 0, \ldots, a_i, 0, \ldots, 0, -f_{i,j}(a_i), 0, \ldots) \]

where \( i \leq j \) and \( a_i \in A_i \).
We claim that the quotient $D = A/B$ is the direct limit of the $A_i$ when we let the homomorphisms $d_i : A_i \to D$ be composition of

$A_i \to A$ defined by $a_i \to (0, \ldots, 0, a_i, 0, \ldots)$ with the quotient hom $A \to D = A/B$.

By construction, $d_i(a_i) - d_j(f_{i,j})(a_i) = 0$ in $D$ for $a_i \in A_i$ and $i \leq j$. So

$$d_i = d_j \circ f_{i,j}.$$ 

Thus the $d_i$ have the right property relative to the $f_{i,j}$. 
Suppose \( D' \) and \( d'_i : A_i \to D' \) for \( i \in I \) form another family of homomorphisms respecting the \( f_{i,j} \).

We get a unique homomorphism

\[
\tilde{h} : \bigsqcup_{i \in I} A_i = \bigoplus_{i \in I} A_i = A \to D'
\]

from the definition of the direct sum as the coproduct in the category of abelian groups. This homomorphism sends \( B \subset A \) to \( \{0\} \) since the \( d'_i \) are compatible with the \( f_{i,j} \). So \( \tilde{h} \) factors in a unique way through a homomorphism

\[
h : D = A/B \to D'.
\]

This completes the proof.
Inverse limits in categories

These result from turning arrows around in the definition of direct limits.

Suppose $I$ is a directed set of indices.

**Def:** An inverse system of morphisms in a category $C$ is given by a collection $\{A_i\}_{i \in I}$ of objects in $C$ together with morphisms $f_{j,i} : A_j \to A_i$ for $i \leq j$ which respect composition. So, if $i \leq j \leq k$ then

$$f_{k,i} = f_{k,j} \circ f_{j,i}$$
Example 1: Suppose $I$ is the set of positive integers, and that $p$ is a prime. Define

$$A_i = \mathbb{Z}/p^i$$

for all $i$. If $i \leq j$ we then have a surjective homomorphism

$$f_{j,i} : A_j = \mathbb{Z}/p^j \to A_i = \mathbb{Z}/p^i$$

which is reduction mod $p^i$.

Example 2: With $I$ again the set of positive integers, let $A_i$ be the group $\mathbb{R}/\mathbb{Z}$ for all $i$. Define

$$f_{j,i} : A_j = \mathbb{R}/\mathbb{Z} \to A_i = \mathbb{R}/\mathbb{Z}$$

to be multiplication by $j!/i!$ for all $i \leq j$. 
**Def:** An object $D$ in $C$ together with a family of morphisms $d = \{d_i : D \to A_i\}_{i \in I}$ in $C$ is an **inverse limit** for the family $\{A_i, f_{j,i}\}$ if the following is true:

1. The homomorphism $d_i$ respect the maps $f_{j,i} : A_j \to A_i$ for $j \leq i$. In other words,
   $$d_j = d_i \circ f_{j,i}.$$

2. The pair $(D, d)$ is universal with respect to pairs satisfying condition (1). So if $(D', d')$ is any other such pair, there is a unique $h : D' \to D$ in $C$ such that
   $$d'_i = d_i \circ h$$
   for all $i$.

**Notation:** The inverse limit is

$$D = \lim_{\to} A_i$$
**Theorem:** Inverse limits exist in the categories of all groups and the category of abelian groups.

**Construction:** Let $D$ be the subgroup of the product

$$
\prod_{i \in I} A_i
$$

consisting of all elements

$$
\prod_{i \in I} a_i
$$

such that $f_{j,i}(a_j) = a_i$ for $i \leq j$. The projection map of the product to $A_i$ gives the required $d_i : D \to A_i$. These are consistent by the definition of $D$ with the $f_{j,i}$. One shows they have the required universal property using the universal property of the product $\prod_{i \in I} A_i$. 
**Example:** Suppose as in our first example that

\[ f_{j,i} : A_j = \mathbb{Z}/p^j \rightarrow A_i = \mathbb{Z}/p^i \]

which is reduction mod $p^i$ for all integers $i \leq j$. The inverse limit

\[ \mathbb{Z}_p = \lim_{\leftarrow i} A_i \]

is called the set of $p$-adic integers.

One can think of an element $\{a_i\}_{i \geq 1}$ in $\mathbb{Z}_p$ as the choice of a compatible sequence of residues $a_i$ in $\mathbb{Z}/p^i$ for all $i$. Compatibility means that the residues reduce to previous choices mod smaller powers of $p$.

Since addition and multiplication respect reduction mod $p^i$ for all $i$, we can both add and multiply elements of $\mathbb{Z}_p$. This shows $\mathbb{Z}_p$ the is a ring.
Exercise: Show that we can think of elements of $\mathbb{Z}_p$ as infinite formal series

$$b = \sum_{i \in 0}^{\infty} b_i p^i \quad (3)$$

in which each $b_i$ is an integer in

$$\{0, 1, 2, \ldots, p - 1\}$$

Associate to $b$ the compatible sequence of residues $\{a_i\}_{i \geq 1}$ defined by

$$a_i = \sum_{k=0}^{i-1} b_i p^i.$$

Show that the addition and multiplication of $\mathbb{Z}_p$ corresponds to formally adding and multiplying series as in (3) and then using the usual rules about carrying mod higher and higher powers of $p$. 
Exercises about $\mathbb{Z}_p$:

1. Show that $\mathbb{Z}_p$ becomes a topological group when we say there is a basis of open sets of the form

$$a + p^j \mathbb{Z}_p$$

as $a$ ranges over $\mathbb{Z}_p$ and $j$ ranges over all positive integers.

2. Show that $\mathbb{Z}_p$ is a complete metric space when we define a metric $|\cdot|_p : \mathbb{Z}_p \to \mathbb{R}$ by

$$|a|_p = p^{-i_0}$$

if $a = \{a_i\}_{i \geq 1}$ and $i_0$ is the smallest non-negative integer for which

$$a_i \not\equiv 0 \mod p^{i_0}$$

for $i \geq i_0$. (Completeness means that Cauchy sequences with respect to $|\cdot|_p$ converge to elements of $\mathbb{Z}_p$.)
Abelian categories

The category $\mathcal{A}$ of abelian groups has some special properties. Namely, for every pair of objects $C, D$ of $\mathcal{A}$, the morphisms

$$\text{Mor}_\mathcal{A}(C, D) = \text{Hom}_\mathcal{A}(C, D)$$

are an abelian group. Furthermore, each $f \in \text{Hom}_\mathcal{A}(C, D)$ has a kernel and a cokernel, which are objects of $\mathcal{A}$. Each such $f$ can be factored as a composition of an surjective homomorphism followed by an injective homomorphism.

**Definition** A category $\mathcal{C}$ is abelian if it is isomorphic to a subcategory of $\mathcal{A}$ which is closed under finite direct sums and also closed under taking kernels and cokernels of homomorphisms in $\mathcal{C}$. 
Example 1: Suppose $G$ is a group. A $G$-module is an abelian group $M$ having a (left) action of $G$ which respects the group law of $M$. Thus

$$g(m_1 + m_2) = gm_1 + gm_2$$

for $g \in G$ and $m_1, m_2 \in M$. A $G$-module homomorphism $M_1 \rightarrow M_2$ is a homomorphism of abelian groups which respects the action of $G$ on $M_1$ and $M_2$. The category $Mod(G)$ of all $G$-modules is an abelian category.

Example 2: We haven’t defined rings $R$ or $R$-modules yet, but the category of $R$-modules for any ring $R$ will be an abelian category.
Comment: One can give an abstract definition of an abelian category. See §II.1 of Hartshorne’s “Algebraic Geometry” or ”Homological Algebra” by Hilton and Stammbach. Our first definition of abelian categories then becomes a Theorem of Peter Freyd.

One requires first that $\text{Mor}_A(C, D)$ is an abelian group for all objects $C$ and $D$ of $A$.

If $f \in \text{Mor}_A(C, D)$, the kernel of $f$ can be defined to be a morphism $h : K \to C$ in $A$ which is universally attracting with respect to morphisms such that $f \circ h$ is the 0 element of $\text{Mor}(K, D)$. One can define cokernels similarly.

A morphism is injective if it the kernel of some morphism from its range, and one can define surjective morphisms similarly.
The axioms for an abelian category $\mathcal{A}$ are:

1. $\text{Mor}_\mathcal{A}(C, D)$ is an abelian group, and the composition of morphisms is linear. So $h \circ (f_1 + f_2) = h \circ f_1 + h \circ f_2$ and similarly on the other side, when these compositions are defined.

2. coproducts of finitely many objects exist.

3. kernels and cokernels of morphisms exist.

4. If $f : K \to C$ is injective, this is the kernel associated to $C \to \text{coker}(f)$. If $h : D \to H$ is surjective, this the cokernel associated to $\ker(h) \to D$.

5. Every morphism can be factored as a composition $f \circ h$ of a surjection $h$ and an injection $f$. 
Presheaves

Suppose $X$ is a topological space. Let $\mathcal{U}_X$ be the set of all open subsets of $X$. We can view $\mathcal{U}_X$ as a category, in which the morphisms are inclusion maps. A presheaf on $X$ is a contravariant functor

$$F : \mathcal{U}_X \to \mathcal{A} \equiv \text{abelian groups}$$

such that $F(\emptyset) = \{0\}$. One typically thinks of $F(U)$ as a set of functions from $U$ to some fixed abelian group $T$. Then if $U \to V$ is an inclusion of sets, $F(V) \to F(U)$ can be thought of as the restriction of functions from $V$ to $U$. Call $F(U)$ the sections of $F$ over $U$.

For instance, we could let $F(U)$ be the additive group of all continuous functions from $U$ to the reals $\mathbb{R}$. 
**Fact:** We can make the set \( P_X \) of all presheaves on \( X \) into an abelian category in the following way.

1. If \( H : \mathcal{U}_X \to \mathcal{A} \) is another presheaf, a morphism \( f : F \to H \) is a just a morphism of functors.

2. We need to define presheaves \( \text{Kernel}(f) \) and \( \text{Cokernel}(f) \) associated to \( f \). To do this, we have for each \( U \in \mathcal{U}_X \) a group homomorphism

\[
f(U) : F(U) \to H(U)
\]

Define \( \text{Ker}(f) \) is the presheaf for which

\[
\text{Ker}(f)(U) = \text{Kernel}(f(U))
\]

and define \( \text{Coker}(f) \) similarly.
**Exercise:** Suppose $X$ is the unit interval $[0, 1]$ on the real line. Define $F$ and $H$ by

$$F(U) = \{\text{Continuous functions } r : U \rightarrow \mathbb{Z}\}$$

$$H(U) = \{\text{Continuous functions } r : U \rightarrow \mathbb{R}\}$$

We have a morphism of presheaves $f : F \rightarrow H$ in which

$$f(U) : F(U) \rightarrow H(U)$$

is induced by $\mathbb{Z} \subset \mathbb{R}$. What are the presheaf kernel and the presheaf cokernel of $f$?

**Exercise:** To a presheaf $F$ associate the abelian group

$$A_F = \prod_{\text{open } U \subset X} F(U).$$

Show that the association of $F$ with $A_F$ makes the category $P_X$ of presheaves on $X$ into a subcategory of the category of abelian groups which satisfies the axioms for an abelian category.
Sheaves

A presheaf $F : \mathcal{U}_X \to \mathcal{A}$ on a topological space $X$ is a presheaf if it satisfies the following additional properties. (Heuristically, these say that the sections of $F$ over any open set $U \subset X$ are determined local information.)

1. (Local information determines sections). Suppose $\{V_i\}_i$ is a covering of an open set $U \subset X$ by open sets. If $s \in F(U)$ has image 0 in $F(V_i)$ for all $i$, then $s = 0$ in $F(U)$.

2. (Patching condition). Suppose conversely that we have sections $s_i \in F(V_i)$ for all $i$ which are consistent, in the sense that $s_i$ and $s_j \in F(U_j)$ have the same image in $F(U_i \cap U_j)$ for all $i, j$. Then there is an $s \in F(U)$ restricting to $s_i$ for all $i$. 