# Math 520A

# Course Supplement on Finite Abelian Groups

***William F. Hammond***

**March 14, 2007**

The structure theorem for finite abelian groups is most conveniently obtained in the context of studying finitely-generated modules over the ring of integers, or, more generally, over principal ideal domains.

On the other hand, the segment of this course on the topic of finite groups is hardly a complete introduction to that subject without at least mention of the structure theorem for finite abelian groups, and it is desirable to have a treatment that fits the context of this part of the course.

The method used here, explained to me by Professor Alexandre Tchernev, is based on analysis of the case of a finite abelian group of prime power order in the spirit of "Nakayama's Lemma" from the subject of commutative algebra.

The structure theorem for finite abelian groups is the following:

**Theorem 1.** *Every finite abelian group is isomorphic to a direct product of finite cyclic groups*

$$\boldsymbol{Z}/m_1\boldsymbol{Z} \times \boldsymbol{Z}/m_2\boldsymbol{Z} \times \ \ldots \ \times \boldsymbol{Z}/m_r\boldsymbol{Z}$$

*where the moduli are positive and successively divisible, i.e.,*

$$1 \leq m_1 | m_2 | \ldots | m_r \quad .$$

In view of the Chinese Remainder Theorem, i.e.,

$$\gcd(m,n) \ = \ 1 \quad \Rightarrow \quad \mathbf{Z}/mn\mathbf{Z} \cong \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \ ,$$

this theorem is equivalent to the following:

**Theorem 2.** *Every finite abelian group is isomorphic to a direct product of finite cyclic groups of prime power order.*

The proof will proceed in stages.

**Proposition 3.** *A finite abelian group is isomorphic to the direct product of its distinct Sylow subgroups.*

*Proof.* If $G$ is a given finite abelian group, then each of its Sylow $p$-subgroups must be normal in $G$ since every subgroup of an abelian group is normal. Since for a given prime $p$ all Sylow $p$-subgroups are conjugate to each other, it follows that for each prime $p$ dividing the order of $G$ there is one and only one Sylow $p$-subgroup $H_p$. Since these subgroups are all normal the map

$$\prod_p H_p \quad \xrightarrow{\varphi} \quad G$$

given by $\varphi(h_1, h_2, \ldots, h_r) = h_1 h_2 \ldots h_r$, where $h_i \in H_{p_i}$ for the distinct primes $p_1, p_2, \ldots, p_r$ dividing $|G|$, must be a group homomorphism. Since the orders of the groups $H_{p_i}$ are pairwise coprime,

the homomorphism $\varphi$ must be injective, and since the domain and target of $\varphi$ both have the same number of elements, $\varphi$ must, since injective, be bijective. Thus $G$ is isomorphic via $\varphi$ to the direct product of its Sylow subgroups.

**Definition 4.** *The* exponent *of a finite group $G$ is the least positive integer $k$ such that $x^k = 1$ for all $x \in G$.*

**Example.** The exponent of the symmetric group $S_4$ (which has order 24) is 12. The largest order of any element in $S_4$ is 4.

**Corollary 5.** *The exponent of a finite abelian group is always the order of at least one of its elements.*

*Proof.* In view of the preceding proposition the question reduces to the case of a finite abelian group having prime power order. In that case the statement is obvious.

To prove theorem 2 it suffices to prove that a finite group with order a power of $p$, where $p$ is prime, is isomorphic to the direct product of cyclic groups. If $A$ is a finite abelian group of order $|A| = p^m$, with group law written additively, then the set $pA = \{\, px \mid x \in A\}$ is a subgroup of $A$, and $\bar{A}$ will denote the quotient

$$\bar{A} \;=\; A/pA \quad .$$

**Lemma 6.** *If $A$ is a finite abelian group of order $p^m$, $p$ prime, then $A \neq pA$ unless $A \cong (0)$.*

*Proof.* If $A$ is non-trivial, then its exponent must be $p^k$ for some $k \geq 1$, and, clearly, the exponent of $pA$ is then $p^{k-1}$. Since $A$ and $pA$ have different exponents, they cannot be equal.

**Example.** If $e_1, \ldots, e_r$ are integers with $e_j \geq 1$ for $1 \leq j \leq r$, then

$$A \cong \mathbf{Z}/p^{e_1}\mathbf{Z} \times \ldots \mathbf{Z}/p^{e_r}\mathbf{Z} \quad \Rightarrow \quad \bar{A} \cong (\mathbf{Z}/p\mathbf{Z})^r \quad .$$

In this example note that if $x_j$ is a generator of the $j$-th factor $\mathbf{Z}/p^{e_j}\mathbf{Z}$ and $\bar{x}_j = \pi(x_j)$, where $\pi$ is the quotient homomorphism from $A$ to $\bar{A}$, then $\bar{x}_1, \ldots, \bar{x}_r$ generate $\bar{A}$. Moreover, $\bar{A}$ is a vector space over the field $\mathbf{Z}/p\mathbf{Z}$, and $\bar{x}_1, \ldots, \bar{x}_r$ is a basis of $\bar{A}$. Unfortunately, showing that a finite abelian group $A$ with order $p^m$ is isomorphic to a direct product of cyclic groups is a bit more complicated than finding a basis of $\bar{A}$ as a vector space over $\mathbf{Z}/p\mathbf{Z}$.

**Proposition 7.** *If $G$ is a finite abelian group of order $p^m$, $p$ prime, and $x_1, \ldots, x_r$ elements of $G$ for which $\bar{x}_1, \ldots, \bar{x}_r$ generate $\bar{G}$, then $x_1, \ldots, x_r$ generate $G$.*

*Proof.* Let $H$ be the subgroup of $G$ generated by $x_1, \ldots, x_r$, and let $\pi : G \to \bar{G}$ be the quotient homorphism. Let $\varphi$ be the homomorphism obtained by following the quotient homomorphism $G \to G/H$ with the quotient homomorphism $G/H \to \overline{(G/H)}$. Clearly $pG$ is contained in the kernel of $\varphi$, hence, by the universal mapping property for quotients one obtains a homomorphism $\bar{\varphi} : \bar{G} \to \overline{(G/H)}$. The image of $\bar{\varphi}$ is the same as the image of $\varphi$, and, therefore, is $\overline{(G/H)}$ since $\varphi$ is the composition of two surjective homomorphisms. The kernel of $\bar{\varphi}$ is the image under $\pi$ of the kernel of $\varphi$. The kernel of $\varphi$ is the subgroup $H + pG$ of $G$ generated by the set $H \cup pG$. Since $\pi(pG) = (0)$, the kernel of $\bar{\varphi}$ is simply $\pi(H)$. But $\pi(H) = \bar{G}$ by hypothesis, and, therefore

$$\overline{(G/H)} \;=\; \text{Image}(\bar{\varphi}) \cong (0) \;,$$

i.e., $p(G/H) = G/H$. Hence, $G/H \cong (0)$, i.e., $G$ is generated by $x_1, \ldots, x_r$.

**Corollary 8.** *If $G$ is a finite abelian group of order $p^m$, $p$ prime, and $x_1, \ldots, x_r$ elements of $G$, then $x_1, \ldots, x_r$ form a minimal set of generators of $G$ if and only if $\bar{x}_1, \ldots, \bar{x}_r$ form a basis of $\bar{G}$ as a vector space over $\boldsymbol{Z}/p\boldsymbol{Z}$.*

**Corollary 9.** *If $G$ is a finite abelian group of order $p^m$, $p$ prime, and $x_1, \ldots, x_k$ elements of $G$ for which $\bar{x}_1, \ldots, \bar{x}_k$ are linearly independent, then there is a minimal set of generators of $G$ containing $x_1, \ldots, x_k$.*

*Proof.* The first of these corollaries is obvious from what was previously shown. The second follows from the fact that any linearly independent set in a finite-dimensional vector space over a field is part of some basis of that vector space.

**Example.** For the group

$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$$

the set $\{(1,1),(0,1)\}$ is a minimal generating set.

**Proposition 10.** *If $G$ is a finite abelian group of order $p^m$, $p$ prime, then $G$ is isomorphic to the direct product*

$$\boldsymbol{Z}/p^{e_1}\boldsymbol{Z} \times \ \ldots \ \times \boldsymbol{Z}/p^{e_r}\boldsymbol{Z}$$

*for some sequence of positive integers $e_1, \ldots, e_r$ with $e_1 \leq \ldots \leq e_r$.*

*Proof.* When $x_1, \ldots, x_r$ is a minimal set of generators of $G$ with $x_j$ having order $p^{e_j}$, it will always be assumed that the sequence is arranged in such a way that the orders increase, i.e., $e_1 \leq \ldots \leq e_r$. Among all so-arranged minimal sets of generators of $G$ choose one for which the sequence of orders is lexicographically smallest. (Note that this is not the case for the particular minimal generating set in the example given above following corollary 9.) Define the group homomorphism $\varphi : \mathbf{Z}^r \to G$ by the formula

$$\varphi(n_1, \ldots, n_r) \ = \ n_1 x_1 + \ldots + n_r x_r \quad .$$

Clearly, $\varphi$ is surjective since $x_1, \ldots, x_r$ generate $G$. The proof of the proposition will have been obtained if it is shown that $(n_1, \ldots, n_r) \in \mathrm{Ker}(\varphi)$ if and only if $n_j \equiv 0 \pmod{p^{e_j}}$ for $1 \leq j \leq r$. Clearly, the simultaneous congruences are sufficient for membership in the kernel. Suppose now that $(n_1, \ldots, n_r)$ is in the kernel, but at least one of the coordinates $n_j$ does not satisfy the desired congruence. Suppose $s$ is the smallest such value of the index $j$. Then

$$n_s x_s + \ldots + n_r x_r \ = \ 0$$

and, therefore,

$$n_s \bar{x}_s + \ldots + n_r \bar{x}_r \ = \ 0 \quad .$$

Since $\bar{x}_s, \ldots, \bar{x}_r$ are linearly independent over the field $\mathbf{Z}/p\mathbf{Z}$, it follows that $n_j \equiv 0 \pmod{p}$ for the indices $j$ with $s \leq j \leq r$. Let $p^k$ be the highest power of $p$ dividing all of the integers $n_s, \ldots, n_r$, and let $n_j = p^k m_j$ for $s \leq j \leq r$. Let $y = m_s x_s + \ldots + m_r x_r$. By the choice of the exponent $k$ one has $m_j \not\equiv 0 \pmod{p}$ for some $j$, $s \leq j \leq r$. Since $\bar{x}_s, \ldots, \bar{x}_r$ are linearly independent over $\mathbf{Z}/p\mathbf{Z}$, one finds that $\bar{y} = m_s \bar{x}_s + \ldots + m_r \bar{x}_r \neq 0$. Hence, the set $\bar{x}_1, \ldots, \bar{x}_{s-1}, \bar{y}$ is linearly independent, and, therefore, by corollary 9, may be completed to a basis $\bar{x}_1, \ldots, \bar{x}_{s-1}, \bar{y}_s, \ldots, \bar{y}_r$ of $\bar{G}$ where $y_s = y$. Since $n_s = p^k m_s \not\equiv 0 \pmod{p^{e_s}}$, one sees that $1 \leq k < e_s$, which is to say that the set $x_1, \ldots, x_{s-1}, y_s, \ldots, y_r$ — which is a minimal generating set by proposition 7 — is lexicographically smaller than $x_1, \ldots, x_r$ contrary to the choice of $x_1, \ldots, x_r$.