# Math 31 Lesson Plan

## Day 27: Fundamental Theorem of Finite Abelian Groups

Elizabeth Gillaspy

November 11, 2011

**Supplies needed:**

- Colored chalk
- Quizzes
- Homework
- 4 envelopes: evals, HW, presentation rubrics, * probs

**Goals for Students:**

Students will:

- Understand the statement and applications of the Fund Thm of Finite Abelian Groups

[**Lecture Notes: Write everything in blue, and every equation, on the board. [Square brackets] indicate anticipated student responses. *Italics* are instructions to myself.**]

*Return quizzes, HW 5. collect homework 6*

I've been hinting at this Fundamental Theorem of Finite Abelian Groups for most of the term, and now we finally meet it. We're not going to discuss the proof in class – you can read it in the textbook, or in Gallian, if you're so inclined – but since it's such a cool (and useful!) theorem I wanted to at least state it. I thought it would be a nice way to end the group theory part of this course.

Which means that we'll be starting with ring theory on Monday – or perhaps today, if we have time.

Are there any questions about Section 13, or the homework, before we get started?

---

I think the Fundamental Theorem will make most sense if we start with an Example: How many different abelian groups are there of size 180?

To figure this out, we start by factoring 180: $180 = 2^2 * 3^2 * 5$. The Fundamental Theorem tells us that the possible groups of order 180 are

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\ \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \\ \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \end{aligned}$$

Can anyone tell me how I figured this out? *don't wait too long for an answer*

Since $180 = 2^2 * 3^2 * 5$, if we want to write a group of size 180 as a direct product, we will need a factor of size 4, a factor of size 9, and a factor of size 5. There are two possible 2-groups (groups whose order is a power of 2) of size $2^2 = 4$ – $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$. Similarly, there are two possible 3-groups of size $3^2 = 9$.] How many 5-groups are there of size 5? [one] Since there is only one possible 5-group of size 5, the groups listed above are the only ways to write 180 as a direct product of cyclic groups.

The Fundamental Theorem tells us that every abelian group is isomorphic to a direct product of cyclic groups. In other words, we don't have to think of any other possibilities for abelian groups of size 180 — nothing more complicated than direct products!

This is most definitely NOT true in the non-abelian case.

People have managed to classify all finite simple groups — abelian and not — but this was a massive undertaking!

---

To get a better understanding of the Fundamental Theorem, we need some more tools — ie, definitions.

DEF: If $p$ is a prime, a <u>$p$-power group</u> is a group $G$ such that $|G| = p^k$ for some positive integer $k$. How many abelian groups of size $p^k$ are there in general?

DEF If $k$ is a positive integer, we say that the <u>number of partitions of $k$</u>, written $p(k)$, is the number of ways to write $k$ as a sum of positive integers. (Order doesn't matter.)

For example, $p(4) = 5$. Grab a partner and try to find all 5 partitions!

Partitions of 4:

$$1+1+1+1; \quad 1+1+2; \quad 1+3; \quad 2+2; \quad 4.$$

The number of abelian groups of size $p^k$ is the number of partitions of $k$. So, how many abelian groups are there of size $3^4 = 81$? What are they? Work with your partner to figure it out. Once you know one, please come write it on the board.

The abelian groups of size $3^4$ are:

$$\begin{aligned} \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3; \\ \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9; \\ \mathbb{Z}_3 \times \mathbb{Z}_{27} \\ \mathbb{Z}_9 \times \mathbb{Z}_9 \\ \mathbb{Z}_{81} \end{aligned}$$

We say that order doesn't matter for partitions, because order doesn't matter for direct products. $A \times B \cong B \times A$ always.

---

Algorithm for finding all the abelian groups of order $n$:

1. Factor $n$ into primes: $n = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m}$.
2. Find all the partitions of $r_1$.
3. Find all the abelian groups of size $p_1^{r_1}$ – there will be $p(r_1)$ of them.
4. Repeat for all the prime factors of $n$.
5. Build direct products of these $p_i$-groups in all the ways possible to end up with a group of size $n$.

Questions about this algorithm?

Please get into groups of 3 or 4. Try to make sure there's one person in your group that you haven't worked with before. Use the Fundamental Theorem (ie, the algorithm above) to find all the abelian groups of the following sizes:

1. 168

2. $1125 = 9 * 125$

3. $1176 = 2^3 * 3 * 7^2$

*once everyone has finished the first two, discuss at board.*

Prime factorization of $168 : 2^3 * 3 * 7$.

Partitions of 3: $1 + 1 + 1, 1 + 2, 3$. Abelian groups of size 168:

$$\begin{aligned}
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \\
\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \\
\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_7
\end{aligned}$$

Prime factorization of $1125 : 3^2 * 5^3$.

Partitions of 2: $1 + 1, 2$. Abelian groups of size 1125:

$$\begin{aligned}
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25} \times \mathbb{Z}_5 \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{125} \\
\mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\
\mathbb{Z}_9 \times \mathbb{Z}_{25} \times \mathbb{Z}_5 \\
\mathbb{Z}_9 \times \mathbb{Z}_{125}
\end{aligned}$$

---

In none of these examples above (well, except $3^4$) do we see $\mathbb{Z}_n$. However, we know that it's an abelian group of size $n$. In the examples above, which one is isomorphic to $\mathbb{Z}_n$? Please try to figure this out in your groups.

[In the examples above, $\mathbb{Z}_n$ is always isomorphic to the last direct product in the list. Example 2 on page 134 tells us that a cyclic group of order $n$ is isomorphic to the direct product of two cyclic subgroups of sizes $k, \ell$ iff $k \cdot \ell = n$ and $(k, \ell) = 1$. So, in general, the abelian group of size $n$ that is a direct product of cyclic $p$-groups is the one that's isomorphic to $\mathbb{Z}_n$.]

Are there more questions about the Fundamental Theorem of Finite Abelian Groups?

I want to talk briefly about Corollary 14.5. Some of you mentioned that we've seen theorems like it before. So let's put all these relevant statements on the board so we can compare:

Corollary 14.5 states that if $G$ is an abelian group of order $n$, and $m|n$ is any divisor of $n$, then $G$ has a subgroup of order $m$.

Theorem 11.7 states that if $G$ is an abelian group and $p|\,|G|$ is a prime, then $G$ has a subgroup of size $p$.

Theorem 5.5 states that if $G$ is a cyclic group of order $n$, then $G$ has a unique subgroup of size $m$ for any $m|n$.

What are some advantages of Corollary 14.5 over our previous results? *Think-pair-share*

Corollary 14.5 is cool because it doesn't require either that $G$ be cyclic or that the divisor of $|G|$ be prime.

**Proof** of Corollary 14.5: If $G$ is an abelian group of size $n$, then the Fundamental Theorem says it can be written as a direct product of cyclic groups of prime-power order. In other words, we can write

$$G = \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}},$$

where the $p_i$s are all primes but not necessarily all different primes. Note that since $|G| = n$, we must have $n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$.

---

If $m|n$, then each of the prime factors of $m$ is also a prime factor of $n$. Can the power of a prime factor of $m$ be bigger than its power in $n$? [no] Moreover, each prime factor of $m$ is raised to a lower power in $m$ than it is in $n$. In other words, we can write $m = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$, where $0 \le s_i \le r_i$ for all $i$.

Note that $\mathbb{Z}_{p_i^{r_i}}$ is cyclic for each $i$, and also that $p_i^{s_i} \mid |\mathbb{Z}_{p_i^{r_i}}|$, since $p_i^{s_i} | p_i^{r_i}$. Hence, by Theorem 5.5, we know that each $\mathbb{Z}_{p_i^{r_i}}$ has a cyclic subgroup of size $p_i^{s_i}$ – call it $P_i$. Then,

$$P_1 \times P_2 \times \dots \times P_k \le G = \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \dots \times \mathbb{Z}_{p_k^{r_k}},$$

and since $|P_i| = p_i^{s_i}$ we know that

$$|P_1 \times P_2 \times \dots \times P_k| = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k} = m.$$

So we have found a subgroup of $G$ of size $m$, as desired. $\square$

*Do an example!*

*Introduce rings if time*