Orders of Elements in Finite Abelian Groups
by Patrick Brosnan
November 11, 2011

Suppose G is a finite group. For each $d \in \mathbf{Z}_+$, write $a_G(d)$ for the number of elements of order d in G. The purpose of these notes is to prove the following.

Theorem 1. *Suppose G and H are finite abelian groups, and suppose that, for every $k \in \mathbf{Z}_+$, $a_G(k) = a_H(k)$. Then $G \cong H$.*

I'm writing notes on this because someone tried to use it on Midterm 2 claiming that I proved it in class. I didn't. However, as you will see, the main idea did come up in class. (So I gave quite a bit of credit to the student.)

The function $a_G : \mathbf{Z}_+ \to \mathbf{N}$ is a little difficult to deal with. So we define a related function b_G by setting $b_G(k) = \#\{g \in G : o(g)|k\}$. Note that $b_G(k) = \#\{g \in G : g^k = e\}$. This makes it easier to deal with because $G[k] := \{g \in G : g^k = e\}$ is a subgroup of G provided that G is abelian.

Lemma 2. *We have $b_G(k) = \sum_{j|k} a_G(j)$.*

Proof. If $g^k = e$ then $o(g)|k$.

Lemma 2 implies that the function a_G determines the function b_G. In fact, b_G also determines a_G. But the formula is more complicated, and we won't even need to know that b_G determines a_G in these notes. Here's the basic idea though: if p is a prime, $a_G(p) = b_G(p) - b_G(1) = b_G(p) - 1$. But $a_G(p^2) = b_G(p^2) - a_G(p) - a_G(1) = b_G(p^2) - (b_G(p) - 1) - 1 = b_G(p^2) - b_G(p)$. By similar considerations, you can compute $a_G(p^n)$ and also $a_G(k)$ for any $k \in \mathbf{Z}_+$. The fancier (and more fun) way to do this is to use something called the Möbius function.

Proposition 3. *Suppose $G = \mathbf{Z}/d_1 \times \cdots \times \mathbf{Z}/d_r$ with $d_1, \ldots, d_r$ positive integers satisfying $d_1|d_2| \cdots |d_r$ and $d_1 > 1$. Then $b_G(k) = \prod_{i=1}^r (k, d_i)$.*

Proof. In the group $\mathbf{Z}/d_i[k]$ there are (k, d_i) elements. This was a result proved in class. If $G = X \times Y$ where X and Y are abelian groups then $G[k] = X[k] \times Y[k]$. It follows that $G[k] = \prod(\mathbf{Z}/d_i)[k]$ so $b_G(k) = \#G[k] = \prod_{i=1}^r (k, d_i)$.

Proposition 4. *Suppose G and H are finite abelian groups with*

$$\begin{aligned} G &= \mathbf{Z}/d_1 \times \cdots \times \mathbf{Z}/d_r, \quad d_1|d_2| \cdots |d_r; \\ H &= \mathbf{Z}/e_1 \times \cdots \times \mathbf{Z}/e_s, \quad e_1|e_2| \cdots |e_s \end{aligned}$$

where the d_i, e_j are integers strictly greater that 1. If $b_G = b_H$ then $r = s$ and $d_i = e_i$ for all $i = 1, \cdots r$. In particular, $G \cong H$.

Proof. We have $d_1^r = \prod_{i=1}^r (d_1, d_i) = b_G(d_1) = b_H(d_1) = \prod_{i=1}^s (d_1, e_i) \leq d_1^s$. So $d_1^r \leq d_1^s$. Since $d_1 > 1$, it follows that $r \leq s$. Switching the roles of G and H, it follows that $s \leq r$. So $r = s$.

Now G and H are a counterexample to the proposition. Then there is an $i < r$ such that $d_j = e_j$ for $j \leq i$ but $d_{i+1} \neq e_{i+1}$. Without loss of generality, we can assume that $e_{i+1} < d_{i+1}$. (Otherwise switch G and H.) Therefore $(d_{i+1}, e_{i+1}) < d_{i+1}$. It follows that

$$\begin{aligned} d_1 \cdots d_i d_{i+1}^{r-i} &= b_G(d_{i+1}) \\ &= b_H(d_{i+1}) \\ &= d_1 \cdots d_i \prod_{j=i+1}^{r} (e_j, d_{i+1}) \\ &< d_1 \cdots d_i d_{i+1}^{r-i} \end{aligned}$$

But this is a contradiction.

Proof of Theorem 1. If $a_G(k) = b_H(k)$ for all k, then Lemma 2 says that $b_G(k) = b_H(k)$ for all k. So $G \cong H$.

Now here is what I proved in class, and we can get it as a corollary.

Proposition 5. *Suppose*

$$\begin{aligned} G &= \mathbf{Z}/d_1 \times \cdots \times \mathbf{Z}/d_r, \quad d_1|d_2|\cdots|d_r; \\ &= \mathbf{Z}/e_1 \times \cdots \times \mathbf{Z}/e_s, \quad e_1|e_2\cdots|e_s \end{aligned}$$

where the d_i, e_j are integers strictly greater that 1. Then $r = s$ and $d_i = e_i$ for all i.

Proof. Set $G = H$ in Proposition 4.

Now, on the exam there was at least one person claiming that Theorem 1 holds for non-abelian groups. This is not the case.

Example 6. *Let $G = \mathbf{Z}/3 \times \mathbf{Z}/3 \times \mathbf{Z}/3$. Let H denote the subset of 3×3 matrices with coefficients in the field $\mathbf{Z}/3$ of the following form*

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 0. \end{pmatrix}$$

Then $a_G(k) = b_G(k)$ for all k, but G and H are not isomorphic.

Proof. To show that $a_G(k) = b_G(k)$ for all k, it suffices to show that every non-identity element of G or H is of order 3. This is clear for G. For H you can see it directly but multiplying matrices. However G is abelian but H is not because, for example,

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

do not commute. So G and H are not isomorphic.