This file contains revisions to the first printing of my book *Topology of Numbers*. At some point these revisions will be incorporated into the electronic version of the book available on my webpage. Eventually the revisions should make their way into reprintings of the book as well.

Allen Hatcher

A revised proof of Proposition 7.13.

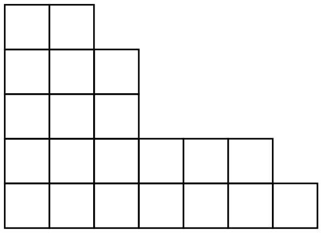
Here is the proposition:

Proposition 7.13. *The factorization of a finite abelian group as a product of cyclic groups of prime power order is unique in the sense that any two such factorizations have the same number of factors of each order.*

The point of the revised proof is to replace some of the formulas in the original proof by a diagram which seems to offer more intuition than the formulas, in keeping with the general theme of the book to use geometry to illuminate algebra. Also included in the revision are a couple paragraphs following the proof which have been modified to uses a similar diagram.

Proof of Proposition 7.13: The idea will be to characterize the number of cyclic factors of each prime power order in an intrinsic way that does not depend on a particular choice of factorization. For a prime p dividing the order of a finite abelian group G let $G(p)$ be the set of elements in G whose order is a power of p, including the identity element 1 of order p^0. Note that an element g has order a power of p exactly when $g^{p^n}=1$ for some n. Given a factorization of G as a product $G_1\times\cdots\times G_k$ of cyclic groups of prime power order, an element $g=(g_1,\cdots,g_k)$ of G has order a power of p exactly when each coordinate g_i has order a power of p since if $g^{p^n}=1$ then $g_i^{p^n}=1$ for each i and conversely if $g_i^{p^{n_i}}=1$ for each i then $g^{p^n}=1$ for n the largest n_i. For the factors G_i whose order is a power of a prime different from p the only way to have $g_i^{p^n}=1$ is when $g_i=1$. We can therefore regard $G(p)$ as the product of the factors G_i whose order is a power of p. This gives a characterization of the product of the factors G_i of order a power of p that does not depend on the choice of the factorization of G.

Thus the problem reduces to the case that $G=G(p)$, i.e., G has order p^n for some n, so we assume this from now on. It remains to give an intrinsic characterization of the number of cyclic factors of order p^r for each r. Suppose we are given a factorization of G as a product $G_1\times\cdots\times G_k$ of cyclic groups of order $p^{n_1},\cdots,p^{n_k}$ with each $n_i\ge 1$. We can assume the exponent sequence $n_1,\cdots,n_k$ is in decreasing order, so $n_1 \geq n_2 \geq \cdots \geq n_k$. Such a sequence can be pictured as an arrangement of boxes into rows and columns, with the i^{th} column containing n_i boxes. The figure at the right shows the box diagram for the sequence $5, 5, 4, 2, 2, 2, 1$. If the order of G is p^n then the total number of boxes is n since the cyclic factor G_i of order p^{n_i} corresponds to the i^{th} column with n_i boxes, so the order of G is $p^n = p^{n_1} \cdots p^{n_k} = p^{n_1+\cdots+n_k}$, hence $n = n_1 + \cdots + n_k$.



Consider the subset $G^{(p)}$ of G consisting of all elements that are p^{th} powers g^p of elements g in G. The p^{th} power of an element $g = (g_1, \cdots, g_k)$ of $G_1 \times \cdots \times G_k$ is $g^p = (g_1^p, \cdots, g_k^p)$ so an element of G is a p^{th} power exactly when each of its coordinates is a p^{th} power. Thus $G^{(p)} = G_1^{(p)} \times \cdots \times G_k^{(p)}$ where $G_i^{(p)}$ consists of the powers g_i^p of elements g_i in G_i. If g_i is a generator of G_i then the elements of $G_i^{(p)}$ are $g_i^p, g_i^{2p}, g_i^{3p}, \cdots, g^{(p^{n_i-1})p} = 1$ so $G_i^{(p)}$ is a cyclic group of order p^{n_i-1}. Thus the box diagram for $G^{(p)} = G_1^{(p)} \times \cdots \times G_k^{(p)}$ is obtained from the box diagram for $G = G_1 \times \cdots \times G_k$ by deleting the bottom row.

Repeating this process, the subset of $G^{(p)}$ consisting of elements that are p^{th} powers $(g^p)^p$ of elements g^p of $G^{(p)}$ is the subset $G^{(p^2)}$ of G consisting of the powers g^{p^2} of elements g in G. The box diagram for $G^{(p^2)} = G_1^{(p^2)} \times \cdots \times G_k^{(p^2)}$ is obtained by deleting the bottom two rows of the diagram for G. Similarly, the powers g^{p^m} of elements g in G form a subset $G^{(p^m)}$ whose box diagram is obtained by deleting the bottom m rows of the diagram for G.

We noted before that if G has order p^n then the total number of boxes in the box diagram for G is n. In the same way the order of $G^{(p)}$ determines the number of boxes above the bottom row. Thus the orders of G and $G^{(p)}$ determine the number of boxes in the bottom row. Similarly, the number of boxes in the m^{th} row up from the bottom is determined by the orders of $G^{(p^{m-1})}$ and $G^{(p^m)}$. The diagram is completely determined by the numbers of boxes in each row, so the diagram is determined by the intrinsic structure of the group G via the intrinsically defined subsets $G^{(p^m)}$. Since the diagram determines the factorization of G as a product of cyclic groups of order a power of p, this finishes the proof. □

The factorization of a finite abelian group as a product of cyclic groups of prime power order is the unique factorization with the largest number of factors since any other factorization with at least as many factors could be factored further into a product with prime power cyclic factors, contradicting the uniqueness statement in the preceding proposition.

On the other hand there can be different factorizations into cyclic factors with the smallest number of factors. For example, if p and q are distinct primes then $C_{p^2q^2} \times C_{pq}$ and $C_{p^2q} \times C_{pq^2}$ are both the group $C_{p^2} \times C_p \times C_{q^2} \times C_q$. A natural way to factor a group G as a product $G_1 \times \cdots \times G_k$ of cyclic groups with the minimum number of factors is by the following procedure. First factor G as a product of cyclic groups of prime power order. Place these groups in the boxes of a box diagram of the type considered in the previous proof, with one group in each box, so that each column consists of the groups of order a power of a fixed prime, arranged in order of decreasing size as one moves upward in the column. Let G_i be the product of the groups in the i^{th} row of the diagram, numbering the rows from the bottom to the top. Each G_i is a cyclic group since it is the product of cyclic groups of coprime orders. We have $G = G_1 \times \cdots \times G_k$ where k is the number of rows, which is the maximum number of prime power cyclic factors of G for any prime.