

# Algebra

David Joseph Stith

We will make use of the following three theorems in the proofs that follow:

**2.2 Theorem.** *Every finitely generated abelian group  $G$  is (isomorphic to) a finite direct sum of cyclic groups, each of which is either infinite or of order a power of a prime.*

**2.3 Lemma.** *If  $m$  is a positive integer and  $m = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$  ( $p_1, \dots, p_t$  distinct primes and each  $n_i > 0$ ), then  $\mathbf{Z}_m \cong \mathbf{Z}_{p_1^{n_1}} \oplus \mathbf{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbf{Z}_{p_t^{n_t}}$ .*

**2.5 Lemma.** *Let  $G$  be an abelian group,  $m$  an integer and  $p$  a prime integer. Then*

- (i)  $mG = \{mu \mid u \in G\}$  is a subgroup of  $G$ .
- (v)  $p^m \mathbf{Z}_{p^n} \cong \mathbf{Z}_{p^{n-m}}$  ( $m < n$ ).

**Theorem.** *If  $G$  is finite abelian of order  $n$ , then  $G$  has a subgroup of order  $m$  for each integer  $m$  that divides  $n$ .*

Suppose  $G$  is finite abelian of order  $n$  and  $m|n$ . We know by Theorem 2.2 that  $G \cong \sum_{i=1}^t \mathbf{Z}_{p_i^{k_i}}$  for primes  $p_i$  and positive integer powers  $k_i$ . Then since

$$n = |G| = \left| \sum_{i=1}^t \mathbf{Z}_{p_i^{k_i}} \right| = \prod_{i=1}^t \left| \mathbf{Z}_{p_i^{k_i}} \right| = \prod_{i=1}^t p_i^{k_i}$$

we have that  $m$  can be expressed as  $m = \prod_{i=1}^t p_i^{s_i}$  where  $0 \leq s_i \leq k_i$  for every  $i$ .

Now let  $A = \sum_{i=1}^t \mathbf{Z}_{p_i^{s_i}}$  so that  $|A| = m$ . We will show that  $A$  is isomorphic to a subgroup of  $G$  and hence  $G$  has a subgroup of order  $m$ . By Lemma 2.5 (i) and (v) we have that for each  $i$ ,

$$\mathbf{Z}_{p_i^{s_i}} \cong p^{k_i - s_i} \mathbf{Z}_{p_i^{k_i}} < \mathbf{Z}_{p_i^{k_i}}$$

Therefore

$$A = \sum_{i=1}^t \mathbf{Z}_{p_i^{s_i}} \cong \sum_{i=1}^t p^{k_i - s_i} \mathbf{Z}_{p_i^{k_i}} < \sum_{i=1}^t \mathbf{Z}_{p_i^{k_i}} = G$$

Therefore

$$\left| \sum_{i=1}^t p^{k_i - s_i} \mathbf{Z}_{p_i^{k_i}} \right| = |A| = m$$

so that  $G$  has a subgroup of order  $m$ .

Therefore if  $G$  is finite abelian of order  $n$ , then  $G$  has a subgroup of order  $m$  for each integer  $m$  that divides  $n$ . **Q.E.D.**

**Theorem.** *If  $m$  is a square-free integer ( $m$  is not divisible by the square of any prime number), then every abelian group of order  $m$  is cyclic.*

Let  $G$  be an abelian group of order  $m$  where  $m$  is not divisible by the square of any prime number. We need to show that  $G$  is cyclic.

We know that  $m = \prod_{i=1}^t p_i^{n_i}$  for distinct primes  $p_i$  and positive integers  $n_i$ . But if any  $n_i > 1$  then  $p_i^2 | m$  which contradicts  $m$  being a square-free integer. Therefore  $m = \prod_{i=1}^t p_i$ . Then by Theorem 2.2,  $G \cong \sum_{i=1}^t \mathbf{Z}_{p_i}$  since the prime factorization of  $m$  is unique, and hence by Lemma 2.3,  $G \cong \mathbf{Z}_m$ . Therefore  $G$  is cyclic.

Therefore if  $m$  is a square-free integer, then every abelian group of order  $m$  is cyclic.  
**Q.E.D.**