Elliott Daimler
MATH 4010
Dr. Chastkofsky
MWF 10:20am
March 22, 2022

Homework 7, Sections 9.1-9.2 Solutions

1

Claim: The multiplicative gorup $\mathbb{Z}_{32}^*$ is isomorphic to $\mathbb{Z}_8 \oplus \mathbb{Z}_2$.

Proof. The group $\mathbb{Z}_{32}^*$ is abelian and has 16 elements, $\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$. By the Fundemantal Theorem of Finite Abelian Groups, $\mathbb{Z}_{32}^*$ is isomorphic to the direct sum of cyclic groups of prime order, $P_1 \oplus P_2 \oplus \cdots \oplus P_k$. By the Fundamental Theorem of Arithmetic, the order of a group G has a unique prime factorization $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = |G|$. The prime factorization of $|\mathbb{Z}_{32}^*|$ is 2^4, so $\mathbb{Z}_{32}^*$ is isomorphic to the direct sum of four cyclic groups $P_1 \oplus P_2 \oplus P_3 \oplus P_4$ where each cyclic group has order 2.

The group $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ also has 16 elements, so its prime factorization is $2^4 = |\mathbb{Z}_8 \oplus \mathbb{Z}_2|$. Similarly then, $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ is isomorphic to the direct sum of four cyclic groups $P_1 \oplus P_2 \oplus P_3 \oplus P_4$ where each cyclic group has order 2. Since these are direct sums of the same number of cyclic groups, each cyclic group being the same order, they are isomorphic to one another. □

2

Claim: Let G be a finite abelian group, and let p be a prime number. If p divides the order of G, then G has an element of order p.

Proof. By the Fundamental Theorem of Finite Abelian Groups, G is isomorphic to a direct sum of cyclic groups of prime power order, $G \cong P_1 \oplus P_2 \oplus \cdots \oplus P_k$. Since each group P_i in the direct sum is cyclic, it has an element a of order p_i, where p_i is prime and $p_i = |P_i|$. The order of the direct sum $P_1 \oplus P_2 \oplus \cdots \oplus P_k$ is $|P_1| \cdot |P_2| \cdot \cdots \cdot |P_k| = p_1 p_2 \cdots p_k = |G|$, so any prime p that divides G is equal to the order of some P_i in $P_1 \oplus P_2 \oplus \cdots \oplus P_k$, and consequently is equal to the order of the generator a of the cyclic group P_i.

Assume without loss of generality that there is an element $b \in P_1 \oplus P_2 \oplus \cdots \oplus P_k$ of the form $b = (0, 0, \cdots, a, \cdots, 0)$ where a is in the i^{th} tuple position and all other positions have a value of zero, the identity for each cyclic group. Then under the group operation of the direct sum, the order of b is also p. Since $P_1 \oplus P_2 \oplus \cdots \oplus P_k$ is isomorphic to G, there must be an element of order p in G. So if there is a prime p that divides G, that prime is the order of an element in $P_1 \oplus P_2 \oplus \cdots \oplus P_k$ and thus is the order of an element in G. □