Q. Basis Theorem for Finite Abelian Groups

Prerequisite: *Exercise P.*

As a provisional definition, let us call a finite abelian group "decomposable" if there are elements $a_1, \ldots, a_n \in G$ such that:
(D1) For every $x \in G$, there are integers $k_1, \ldots, k_n$ such that $x = a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n}$.
(D2) If there are integers $l_1, \ldots, l_n$ such that $a_1^{l_1} a_2^{l_2} \cdots a_n^{l_n} = e$ then $a_1^{l_1} = a_2^{l_2} = \cdots = a_n^{l_n} = e$.
If (D1) and (D2) hold, we will write $G = [a_1, a_2, \ldots, a_n]$. Assume this in parts 1 and 2.

1 Let G' be the set of all products $a_2^{l_2} \cdots a_n^{l_n}$, as $l_2, \ldots, l_n$ range over $\mathbb{Z}$. Prove that G' is a subgroup of G, and $G' = [a_2, \ldots, a_n]$.
2 Prove: $G \cong \langle a_1 \rangle \times G'$. Conclude that $G \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_n \rangle$.

In the remaining exercises of this set, let p be a prime number, and assume G is a finite abelian group such that the order of every element in G is some power of p. Let $a \in G$ be an element whose order is the highest possible in G. We will argue by induction to prove that G is "decomposable." Let $H = \langle a \rangle$.

3 Explain why we may assume that $G/H = [Hb_1, \ldots, Hb_n]$ for some $b_1, \ldots, b_n \in G$.

By Exercise O, we may assume that for each $i = 1, \ldots, n$, $\text{ord}(b_i) = \text{ord}(Hb_i)$. We will show that $G = [a, b_1, \ldots, b_n]$.

4 Prove that for every $x \in G$, there are integers $k_0, k_1, \ldots, k_n$ such that

$$x = a^{k_0} b_1^{k_1} \cdots b_n^{k_n}$$

5 Prove that if $a^{l_0} b_1^{l_1} \cdots b_n^{l_n} = e$, then $a^{l_0} = b_1^{l_1} = \cdots = b_n^{l_n} = e$. Conclude that $G = [a, b_1, \ldots, b_n]$.
6 Use Exercise P5, together with parts 2 and 5 above, to prove: Every finite abelian group G is a direct product of cyclic groups of prime power order. (This is called the basis theorem of finite abelian groups.)

It can be proved that the above decomposition of a finite abelian group into cyclic p-groups is unique, except for the order of the factors. We leave it to the ambitious reader to supply the proof of uniqueness.