Lemma 11.1. *Let G be a finite Abelian group of order $p^n m$ where p is a prime and p doesn't divide m. Then $G = H \times K$ where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^n$.*

Proof. We need to show H and K are subgroups of G. Obviously, H and K are non-empty. By two-steps:

1. For any $a\ b \in H$, $(ab)^{p^n} = a^{p^n} b^{p^n} = ee = e$
2. For any $a \in H$, $(a^{-1})^{p^n} = (a^{p^n})^{-1} = e^{-1} = e$

Thus H is a subgroup of G, similarly, K is a subgroup of G. Since G is Abelian, H and K are normal in G.

Then we need to show $H \cap K = \{e\}$. Suppose $g \in G$ such that $g^{p^n} = g^m = e$. Then $|g|$ divides both p^n and m. Since p doesn't divide m, $\gcd(p^n, m) = 1$, so g has to be e.

Finally, we need to show $G = HK$. It is obviously that $HK \subseteq G$, we focus on $G \subseteq HK$. By $\gcd(p^n, m) = 1$, we know $p^n s + mt = 1$. For any $g \in G$, let $k = g^{p^n s}$ and $h = gk^{-1}$. $k^m = (g^{p^n s})^m = g^{p^n ms} = (g^{p^n m})^s = e^s = e$, thus $k \in K$.

$$\begin{aligned} h^{p^n} &= (gk^{-1})^{p^n} \\ &= g^{p^n} (g^{-p^n s})^{p^n} \\ &= g^{p^n - p^n s p^n} \\ &= g^{p^n (1 - p^n s)} \\ &= g^{p^n mt} \\ &= (g^{p^n m})^t \\ &= e^t \\ &= e \end{aligned}$$

Thus $h \in H$, and $hk = gk^{-1}k = g$, $g \in HK$.

How do I find out $g^{p^n s}$? Well, we want to prove that $g = hk$ for some h and k, and we can use g^{p^n} to remove h, but know it is $g^{p^n} = k^{p^n}$, which may not be k. We know $\langle k^{p^n} \rangle = \langle k \rangle$ by $\gcd(p^n, |k|) = 1$, so there is a i such that $(k^{p^n})^i = k$. Now look at $p^n s + mt = 1$, we find $p^n s \bmod m = 1$, which is what we want, so $(k^{p^n})^s = k$.

Since K is a subgroup of G, $|K|$ divides $|G| = p^n m$. But p can not divides $|K|$, if it does, there is a element g of order p in K since K is Abelian, then

$g^m = e$ which implies p divides m, which is unacceptable. Similarly, $|H|$ divides $|G| = p^n m$, let q a prime that divides m, q can not divides $|H|$, if it does, there is a element g of order q in H since K is Abelian, then $g^p = e$ which implies q divides p, which is unacceptable. So $|K|$ divides m and $|H|$ divides p^n, then $|K| \leq m$ and $|H| \leq p^n$, also $|G| = |H||K|$, so $|H| = p^n$ and $|K| = m$. □

Lemma 11.2. *Let G be an Abelian group of order p^n, where p is prime and n is non-negative. Let $a \in G$ such that $|a|$ is maximum in G. Then $G = \langle a \rangle \times K$ for some K.*

Proof. TODO. □

Lemma 11.3.

Theorem 11.1 (Homomorphism respect Internal Direct Product)**.** *Let $G = H \times K$, and $\phi : G \to \overline{G}$ a homomorphism. Prove that $\phi(G) = \phi(H) \times \phi(K)$.*

Proof. Since H and K are normal, so are $\phi(H)$ and $\phi(K)$. Also, $H \cap K = \{e\}$, therefore $\phi(H) \cap \phi(K) = \{e\}$. For any $\phi(g) \in \phi(G)$ for some $g \in G$, we know $g = hk$ for some $h \in H$ and $k \in K$. Then $\phi(g) = \phi(hk) = \phi(h)\phi(k)$, $\phi(G) \subseteq \phi(H)\phi(K)$. Since $\phi(H)$ and $\phi(K)$ are subgroups of $\phi(G)$, therefore $\phi(H)\phi(K) \subseteq \phi(G)$. Thus $\phi(G) = \phi(H)\phi(K)$. □

Lemma 11.4. *Let G be a finite Abelian group of order power of p. $G = H_0 \times H_1 \times \cdots \times H_{m-1} = K_0 \times K_1 \times \cdots \times K_{n-1}$ where H and K are non-trivial cyclic subgroups. $|H_i| \geq |H_j|$ if $i < j$, same for K. Prove that $m = n$ and $|H_i| = |K_i|$ for all i.*

This proof is based on the textbook one.

Proof. TODO: fix gap We induction on $|G|$. If $|G| = 1$, then it is trivial. Suppose $|G| = p^a$, and we consider the following function: $\phi(x) = x^p$. □

Lemma 11.5 (Existence of Subgroups of Abelian Groups)**.** *Let G be a finite Abelian group of order n, and m be a divisor of n. Then there is a subgroup of G of order m.*

Proof. This proof is come from textbook. Induction on n.

- Base: $n = 1$ is trivial.

- Induction: Let k be a prime divisor of m, we know there is subgroup K of order k in G. Use the induction hypothesis on G/K, it is possible because $|G/K| < |G|$. Then we know there is a subgroup H/K of G/K of order m/k (by Exercise 10.59), since m/k is a divisor of $|G/K| = n/k$. Since $|H/K| = |H|/|K| = m/k$ and $|K| = k$, it is easy to show $|H| = m$.

□