Exercise 11.11. *Prove that any finite Abelian group G can be expressed as the external direct product of cyclic group of order $n_0, n_1, \cdots, n_{t-1}$, where n_{i-1} divides n_i for all $i \in [1, t-1]$.*

Proof. induction on t.

- Base: $t = 0$, trivial.
- Induction: Since G can be (uniquely, up to isomorphism) expressed as the external direct product of cyclic groups of prime powered. Let S be the set of those cyclic groups, P and Q are empty sets. First, take $H \in S$ which is isomorphic to Z_{p^n} for some prime p and postive n. Then put the group which is isomorphic to Z_{p^m} where m is maximum to P, and move other groups which has form Z_{p^i} from S to Q. Repeat this procedure untile S is empty.

  For any distinct H $K \in P$, $|H|$ is relative prime to $|K|$, since they have form Z_{p^i} with different p. Therefore, the product of elements in P form a large cyclic group R. And the product of Q form a finite Abelian group, by induction hypothesis, it can be expressed as $K_0 \oplus K_1 \oplus \cdots \oplus K_m$, and they satisfy the property we want to prove.

  The last thing is proving $|K_0|$ divides $|R|$. We now consider the worse situation, K_0 is the product of Q, then elements of Q are relative prime to each other, thus, for any prime p, Q has at most one element of order power of p. For any $H \in Q$, H has form p^i and $H \in S$, then $|H|$ divides $|R|$ due to the way we construct R. So $|K_0|$ divides $|R|$. If K_0 is not the product of Q, then $|K_0|$ divides the order of the product of Q, therefore $|K_0|$ divides $|R|$.

□

Exercise 11.12. *Prove that an Abelian group of order 2^n $(n \geq 1)$ must have an odd number of elements of order 2.*

Proof. Let G be such group, and G can be expressed as $Z_{2^{i_0}} \oplus Z_{2^{i_1}} \oplus \cdots \oplus Z_{2^{i_n}}$ (where $n \in \mathbb{N}$). For any element in $Z_{2^{i_0}} \oplus Z_{2^{i_1}} \oplus \cdots \oplus Z_{2^{i_n}}$, each component of it is either an element of order 2 in corresponding cyclic group or identity (we can do this because 2 is prime), therefore we can express it as an binary string, and the number of strings is 2^n. But we counted string that is all 0 (all identity) which is order 1, so the number of elements of order 2 in $Z_{2^{i_0}} \oplus Z_{2^{i_1}} \oplus \cdots \oplus Z_{2^{i_n}}$ is $2^n - 1$, which is odd. □

Exercise 11.13. *Suppose G is a finite Abelian group. Prove that G has order p^n where p is prime iff the order of every element of G is power of p.*

Proof. ($\Rightarrow$) G can be expressed as the external direct product of cyclic groups of order power of p, then for any element $g \in G$, g can be expressed as $(g_0, g_1, \cdots, g_n)$, and $|g| = \text{lcm}(g_0, g_1, \cdots, g_n)$. Since g_i is in a group of order power of p, so does g_i, therefore $\text{lcm}(g_0, g_1, \cdots, g_n) = \max(g_0, g_1, \cdots, g_n)$, which is power of p.

($\Leftarrow$) Since G is finite Abelian group, it can be expressed as a external direct product of cyclic groups, say $G_0 \oplus G_1 \oplus \cdots \oplus G_n$. Since every element of G is power of p, so are the generators of G_i, therefore $|G_i|$ is power of p, then $|G|$ is power of p. □

Exercise 11.42. *For any Abelian group G of order p^n, where p is prime. Prove that G is cyclic iff G has exactly $\phi(p)$ elements of order p.*

Proof. The $\Rightarrow$ direction is obviously, we focus on the $\Leftarrow$. Suppose G is **NOT** cyclic, then G can be expressed as the direct product of more than one cyclic groups of order power of p. Now G has more than $\phi(p)$ elements of order p, which contradict our hypothesis. □

Exercise 11.45. *The exponent of a finite group G is the smallest integer n such that $x^n = e$ for all $x \in G$. Prove that if G is finite and Abelian, then the exponent of G is the largest order of any element in G.*

Proof. We know G can be write as a direct product of cyclic groups, say $G = G_0 \oplus G_1 \oplus \cdots \oplus G_n$. Induction on n.

- Base: Obviously, the largest order of any element in $G = G_0$ is the exponent of G, which is $|G_0|$ (recall that G_0 is cyclic).

- Induction: Suppose the exponent of $G_0 \oplus G_1 \oplus \cdots \oplus G_{n-1}$ is the largest order of any element in G, denote one such element by $(g_0, g_1, \cdots, g_{n-1})$, and let g_n be the element of largest order in G_n. We claim $|g| = |(g_0, g_1, \cdots, g_n)|$ is the exponent of $G_0 \oplus G_1 \oplus \cdots \oplus G_n$.

  For any element in $G_0 \oplus G_1 \oplus \cdots \oplus G_n$, it can be wrote in $(h_0, h_1, \cdots, h_n)$. Then $(h_i)^{|g|} = e$ for any $i < n$, since $|(g_0, g_1, \cdots, g_{n-1})|$ divides $|g|$ and $|(g_0, g_1, \cdots, g_{n-1})|$ is the exponent of $G_0 \oplus G_1 \oplus \cdots \oplus G_{n-1}$. Also $(h_n)^{|g|} = e$ since h_n divides g_n and g_n divides $|g|$. Therefore $h^{|g|} = e$.

  It is easy to show $|g|$ is largest in G, let n the largest order of elements in G, then $|g| \leq n$, by $h^{|g|} = e$ we know $|g| \geq n$.

$\square$

Exercise 11.46. *If H is a subgroup of a finite Abelian group of even order, and H contains all elements in G of even order, prove that $H = G$.*

Proof. Consider the internal direct product form of G, since $|H|$ is even, so is $|G|$. So there is at least one cyclic subgroup of even order in the direct product form G, we denote the generator of it by h. For any cyclic subgroup of even order in the direct product form of G, the order of their generators are even, therefore they are all in H. Now we consider the cyclic subgroups of odd order, denote the generator by k. Then $|hk|$ is even, $hk \in H$, and cancel h from hk, we know $k \in H$. Therefore, all cyclic subgroups in the internal direct product are subgroups of H, $H = G$. $\square$