We proved that if A is a finite abelian group and $|A| = p_1^{s_1} \cdots p_t^{s_t}$, $p_1 < \cdots < p_t$ prime numbers then

$$A \simeq P_1 \times \cdots \times P_t$$

where $|P_i| = p_i^{s_i}$ (and $P_1, \ldots, P_t$ are unique). Clearly each P_i is a p_i-group. Our next goal is to understand finite abelian p-groups. First we introduce some terminology.

Let G be a group and N a subgroup of G. A subgroup M is called a complement to N in G if $N \cap M = \{e\}$ and $G = N \cdot M$ (show that this implies $G = M \cdot N$ as well). If G is finite, M is a complement to N if and only if $N \cap M = \{e\}$ and $|N| \cdot |M| = |G|$.

Remark: We are not assuming M or N to be normal in G, so it is not true in general that $G \simeq M \times N$. But when both M, N are normal then $G \simeq M \times N$.

Our goal is to prove the following theorem.

Theorem: Let P be a finite abelian p-group and let $a \in P$ be an element of largest possible order. Then the subgroup $\langle a \rangle$ has a complement Q in P. In particular, $P \simeq \langle a \rangle \times Q$.

We start with a general observation:

Proposition 1: Let G be a group and M a subgroup of G. Suppose $f: G \to H$ is a homomorphism such that

(i) $M \cap \ker f = \{e\}$

(ii) $f(M)$ has a complement in H

Then M has a complement in G which contains $\ker f$.

Proof: Let B be a complement to $f(M)$ in H so $f(M) \cap B = \{e\}$ and $f(M) \cdot B = H$. Let $D = f^{-1}(B)$. We will show that D is complement to M in G. First we show that $M \cap D = \{e\}$. In fact, if $a \in M \cap D$ then $f(a) \in f(M) \cap f(D) \subseteq f(M) \cap B = \{e\}$ so $f(a) = e$, i.e. $a \in \ker f$. Since $a \in M$ and $\ker f \cap M = \{e\}$, we get $a = e$.

Now we show that $M \cdot D = G$. Take $g \in G$. Then $f(g) = f(m) \cdot b$ for some $m \in M$ and $b \in B$ (since $H = f(M) \cdot B$). Thus $b = f(m)^{-1} f(g) = f(m^{-1}g)$, so $m^{-1}g \in f^{-1}(B) = D$ and calling $d = m^{-1}g \in D$ we get $g = md \in MD$. Since g was arbitrary, $G = M \cdot D$. This completes our proof that D is a complement of M in G.

As a special case of Proposition 1 we get

Proposition 2: Let G be a group, $M \leq G$ and $N \trianglelefteq G$ such that $M \cap N = \{e\}$. Consider the quotient homomorphism $\pi: G \to G/N$. If $\pi(M)$ has a complement in G/N then M has a complement in G which contains N.

Proof: Since $\ker \pi = N$, this is a special case of Proposition 1 with $f = \pi$. ∎

Proof of Theorem 1: Let $|P| = p^n$, $n \geq 1$. Our proof is by induction on n. When $n=1$ then $P = \langle a \rangle$ and $\{e\}$ is a complement of P in P.

Let $|P| = p^n$, $n \geq 2$ and assume that the theorem holds for abelian p-groups of order less than p^n. Let $a \in P$ be an element of largest order, say order$(a) = p^k$. Then $x^{p^k} = e$ for all $x \in P$ (the order of x is a power of p less or equal than p^k). If $P = \langle a \rangle$ then $\{e\}$ is a complement of $\langle a \rangle$ in P. Suppose $P \neq \langle a \rangle$. Take $b \in P$ which is not in $\langle a \rangle$ of smallest possible order. Then the order of $b^p <$ the order of b, so $b^p \in \langle a \rangle$, which means that $b^p = a^m$ for some m. Note that

$$\text{order of } b^p = \frac{\text{order}(b)}{p} \leq \frac{p^k}{p} = p^{k-1}$$

so order$(a^m) <$ order$(a) = p^k$. As order$(a^m) = \frac{\text{order}(a)}{\gcd(m, \text{order}(a))}$ we see that $p \mid m$. Let $b^{-1} a^{m/p} = c$. Then $c \notin \langle a \rangle$ and $c^p = e$. Since c has order p and $c \notin \langle a \rangle$ we conclude that b must have order p (as b is of smallest order among elements not in $\langle a \rangle$). Since $b \notin \langle a \rangle$, we have $\langle a \rangle \cap \langle b \rangle = \{e\}$. Consider the quotient homomorphism $\pi: P \to P/\langle b \rangle$. Since $\langle a \rangle \cap \ker \pi = \{e\}$, π is injective on $\langle a \rangle$ so $\pi(a)$ has order p^k. Clearly $P/\langle b \rangle$ does not have elements of order larger than p^k (since P does not have such elements) so by inductive assumption $\pi(\langle a \rangle) = \langle \pi(a) \rangle$ has a complement in $P/\langle b \rangle$. It follows from Prop. 2 that $\langle a \rangle$ has a complement in P. ☒

As a simple corollary to Theorem 1 we get the following important result:

Theorem 2: If P is an abelian group of order p^n, p a prime then P is isomorphic to a product of cyclic groups: $P \simeq \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \dots \times \mathbb{Z}_{p^{m_s}}$ with $m_1 \geq m_2 \geq \dots \geq m_s \geq 1$.

Proof: The proof is a straightforward induction on n. If $n=1$ then P is cyclic, so the result holds. Let $|P| = p^n$, $n \geq 2$ and assume the theorem is true for all abelian p-groups of order less than p^n. Let $a \in P$ be an element of largest order p^{m_1}. By Theorem 1, $\langle a \rangle$ has a complement Q in P. Thus implies that $P \simeq \langle a \rangle \times Q \simeq \mathbb{Z}_{p^{m_1}} \times Q$. Since $|Q| < |P|$, by the inductive assumption $Q \simeq \mathbb{Z}_{p^{m_2}} \times \dots \times \mathbb{Z}_{p^{m_s}}$, $m_2 \geq m_3 \geq \dots \geq m_s \geq 1$. Since every element in Q has order $\leq p^{m_1}$, we have $m_1 \geq m_2$. ☒

Remark: The sequence $m_1 \geq m_2 \geq \dots \geq m_s$ is actually unique for a given group P. We leave a proof as a challenging exercise.

Let $A(n)$ denote the number of non-isomorphic abelian groups of order n. By Theorem 2 and the Remark we see that $A(p^n)$ = number of sequences $m_1 \geq m_2 \geq \dots \geq m_s \geq 1$ such that $m_1 + m_2 + \dots + m_s = n$. Such sequences are called partitions of n. Thus $A(p^n) = p(n) \overset{\text{def}}{=}$ number of partitions of n.

The numbers $p(n)$ appear in many areas of mathematics and have been studied extensively.

Using the theorem from last lecture we see that if $\gcd(m,k)=1$ then $A(mk)=A(m)\cdot A(k)$. (every abelian group of order mk is isomorphic to $A\times B$ for unique A of order m and unique B of order n).

Thus, if $n=p_1^{s_1}\cdot\ldots\cdot p_t^{s_t}$, $p_1<\ldots<p_t$ primes then

$$A(n)=p(s_1)\cdot p(s_2)\cdot\ldots\cdot p(s_t),$$ where $p(n)$ is the number of partitions of n.

Combining Theorem 2 with the theorem from last class we get

Theorem: Every finite abelian group is a product of cyclic groups of prime power order.

One can prove a stronger result

Theorem: Let A be a finitely generated abelian group. Then A is isomorphic to $\underbrace{\mathbb{Z}\times\ldots\times\mathbb{Z}}_{m\text{-times}}\times T$ where T is finite and m is some non-negative integer.