Theorem 1. Let $G$ be an abelian group and $n > 1$. Let $A_n = \{a^n | a \in G\}$. Then $A_n$ is a subgroup. In the case that $G$ is not abelian, $A_n$ may not be a subgroup.

Proof. Assume that $G$ is abelian. Since $e = e^n \in A_n$, $A_n \neq \emptyset$. Suppose that $b, c \in A_n$. Then $b = a^n$ and $c = d^n$ for some $a, c \in G$. Then $bc = a^nb^n = (ab)^n$, since $G$ is abelian. Hence $ab \in A_n$. Also, $b^{-1} = (a^n)^{-1} = (a^{-1})^n \in A_n$. Hence $A_n$ is a subgroup of $G$.

To see that we need $G$ to be abelian, take $G = S_3$ and $n = 3$. Using the notation from class, since $\rho^3 = (\rho^2)^3 = i$, and $\sigma_j^3 = \sigma_j$ for $1 \leq j \leq 3$, we get $A_3 = \{i, \sigma_1, \sigma_2, \sigma_3\}$. This set is not closed under multiplication, so it is not a subgroup. (Using the results of section 2.4, we can see that $A_3$ is not a subgroup because it has size 4, and $4 \nmid 6$.)

Theorem 2. Suppose that $G$ is a group with no proper subgroups. Then $G$ is cyclic of order $p$, where $p$ is prime. (To be technically correct, we must assume that $|G| > 1$.)

Proof. By hypothesis, the only subgroups of $G$, are $\{e\}$ and $G$. If $G = \{e\} = \langle e \rangle$ it is clearly cyclic. Assume that $|G| > 1$. Then there is an element $a \in G - \{e\}$. The cyclic subgroup $\langle a \rangle$ is not $\langle e \rangle$, so it must be $G$. Thus $G$ is cyclic.

We next show that $G = \langle a \rangle$ is finite. If $a^2 = e$ then $|G| = 2$. Otherwise $\langle a^2 \rangle = G$ by the hypothesis. Hence $a = a^{2k}$ for some $k$ and then $e = a^{2k-1}$, showing that $G$ is finite (and of odd order).

Suppose that $|G| = n$. According to class Theorem 15, the subgroups of $G$ are in 1-1 correspondence with the positive divisors of $n$. Since $G$ has no non-trivial subgroups, the only divisors of $n$ are 1 and $n$, showing that $n$ is prime.

Theorem 3. The relation on $\mathbb{R}$ defined by $a \sim b$ if and only if $a - b \in \mathbb{Q}$ is an equivalence relation.

Proof. For every $a \in \mathbb{R}$, $a - a = 0 \in \mathbb{Q}$, so $a \sim a$. Hence $\sim$ is reflexive. Assume that $a \sim b$. Then $b - a = -(a - b) \in \mathbb{Q}$, since the rationals are closed under negation. Thus $b \sim a$, so $\sim$ is symmetric. Suppose in addition that $b \sim c$. Then $a - c = (a - b) + (b - c) \in \mathbb{Q}$, since $\mathbb{Q}$ is closed under addition. This shows that $\sim$ is transitive. Thus $\sim$ is an equivalence relation.
Theorem 4. In $\mathbb{Z}_{16}$ let $H = \{[0], [4], [8], [12]\}$. The index of $H$ in $\mathbb{Z}_{16}$ is $i_{\mathbb{Z}_{16}}(H) = 4$. We give the four cosets below.

**Proof.** By Lagrange’s Theorem, $i_{\mathbb{Z}_{16}}(H) = |\mathbb{Z}_{16}|/|H| = 16/4 = 4$. Thus there are four cosets of $H$. These cosets are

- $H + [0] = \{[0], [4], [8], [12]\}$
- $H + [1] = \{[1], [5], [9], [13]\}$
- $H + [2] = \{[2], [6], [10], [14]\}$, and

Since each of the 16 elements of $\mathbb{Z}_{16}$ appears once in the above list, we have listed all the cosets. □

Theorem 5. We list below all the elements of $U_{18}$, find their orders, and show that $U_{18}$ is cyclic.

**Proof.** We have $U_{18} = \{[k] \mid \gcd(k, 18) = 1\} = \{[1], [5], [7], [11], [13], [17]\}$. Since $|U_{18}| = 6$, every element has an order which is a divisor of 6, i.e., 1, 2, 3, or 6.

We first show that $U_{18}$ is cyclic and $U_{18} = \langle [5] \rangle$. We have $[5]^2 = [25] = [7]$ and $[5]^3 = [7][5] = [35] = [-1]$. Thus $o([5]) > 3$. By Lagrange’s theorem, $o([5]) = 6$, which shows that $U_{18} = \langle [5] \rangle$, since we must get each of the six elements (otherwise a cancellation argument would give a smaller order).


Theorem 6. Let $G$ be a finite abelian group with elements $a_1, \ldots, a_n$. Let $x = a_1 \cdot a_2 \cdots a_n$. Then $x^2 = e$. If $|G|$ is odd, then $x = e$.

**Proof.** Let $G$ be a finite abelian group and $x$ as given. Then $x^{-1} = a_n^{-1} \cdots a_1^{-1}$. But each element has a unique inverse, so this is just a list of all the elements of $G$ in a different order. Since $G$ is abelian, the order doesn’t matter, i.e., $x^{-1} = x$, from which we see that $x^2 = e$. Note that this shows that $o(x) \leq 2$.

Suppose now that $|G|$ is odd. By Lagrange’s theorem, $o(x)||G|$, and $|G|$ is odd, so $o(x) = 1$. The only element of order 1 is $e$. Hence $x = e$. □
Theorem 7. Let $G$ be a cyclic group of order $n$. Then $G$ has \( \varphi(n) \) elements which generate $G$.

Proof. Let $G = (a)$ be a cyclic group of order $n$. Thus $a^n = e$ and $a^i \neq e$ for $0 < i < n$. We claim that $G = (a^k)$ if and only if $\gcd(k, n) = 1$. Note that if $k = q \cdot n + k'$ with $0 \leq k' < n$, then $a^k = (a^n)^q a^{k'} = a^{k'}$. There are \( \varphi(n) \) integers between 1 and $n - 1$ which are relatively prime to $n$, so if we show that the claim is true, then we have given \( \varphi(n) \) distinct generators of $G$.

Suppose that $G = (a^k)$. Then $a \in (a^k)$, so $a = (a^k)^t$ for some $t \in \mathbb{Z}$. Thus $e = a^{kt-1}$. Since $o(a) = n$, this shows that $n | (kt - 1)$, or $kt - 1 = sn$. But then $sn + kt = 1$ for some $s, t \in \mathbb{Z}$. By class Theorem 7, $\gcd(k, n) = 1$.

Conversely, if $\gcd(k, n) = 1$, then $sn + kt = 1$ for some $s, t \in \mathbb{Z}$. We then have $a = a^s = a^{sn+kt} = e^s(a^k)^t$, i.e., $a \in (a^k)$. Since every element is a power of $a$, every element in $G$ is a power of $a^k$. Thus $G = (a^k)$. \[\square\]

Theorem 8. Let $G$ be a cyclic group of order $n$. For each integer $m \geq 1$ which divides $n$, there are \( \varphi(m) \) elements of order $m$ in $G$.

As a consequence $n = \sum_{m | n} \varphi(m)$ (in the sum we also need $m > 0$).

Proof. Let $G = (a)$ be a cyclic group of order $n$. Note that for any $t$, $o(a^t) = |(a^t)|$. By class theorem 15, a finite cyclic group has one subgroup of order $m$ for each $m$ dividing $n$. The proof shows that if we write $n = ms$, then $|(a^s)| = m$. Since there is only one subgroup of order $m$, every element of order $m$ must generate this subgroup. According to problem 28, the number of generators of a cyclic subgroup of order $m$ is $\varphi(m)$.

Let $m_1, \ldots, m_r$ be the divisors of $n$ (including 1 and $n$) and label $r$ boxes with these numbers. For each of the $n$ elements of $G$, $a^i$, place $a^i$ in the box labeled with $|(a^i)|$. Each element is placed in exactly one box. The box $m_j$ gets $\varphi(m_j)$ elements placed into it (there are $\varphi(m_j)$ elements generating the subgroup of $m_j$ elements). This shows that $n = \varphi(m_1) + \cdots + \varphi(m_r) = \sum_{m | n} \varphi(m)$. \[\square\]