Proposition (2.2.20) Let $G$ be a group, $a \in G$.

(i) If $o(a) = \infty$, $\varphi: \mathbb{Z} \to \langle a \rangle$, $\varphi(k) = a^k$ is an isomorphism.

(ii) If $o(a) = n < \infty$, $\varphi: \mathbb{Z}_n \to \langle a \rangle$, $\varphi([k]) = a^k$ is an isomorphism.

Proof: See Goodman for (i). For (ii), first we check $\varphi$ is well defined. If $[k] = [k']$, $k = k' + qn$, $q \in \mathbb{Z}$, and using $a^n = e$ we find $a^k = a^{k' + qn} = a^{k'} (a^n)^q = a^{k'} e^q = a^{k'} = a^k$.

Bijectivity: We know $\langle a \rangle = \{a^0, a^1, \ldots, a^{n-1}\}$ and $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and $\varphi([k]) = a^k$, so this works.

Lastly $\varphi([k] + [l]) = \varphi([k+l]) = a^{k+l} = a^k a^l = \varphi([k]) \varphi([l])$.

Now one way to get at the structure of a group is to look at all its subgroups.

Example/Exercise: $S_3 = \text{Sym}\{1, 2, 3\} = \{e, (12), (23), (13), (123), (132)\}$.

The subgroups are $\langle (12) \rangle = \{e, (12)\}$, $\langle (23) \rangle$, $\langle (13) \rangle$, $\langle (123) \rangle = \{e, (123), (132)\}$ as well as the trivial subgroup $\{e\}$ and the whole group $S_3$.

We visualize this as a "lattice"

$S_3$

$\langle (12) \rangle$ $\langle (23) \rangle$ $\langle (13) \rangle$ $\langle (123) \rangle$

$\{e\}$

Edges indicate containment relations.

We will investigate cyclic groups today, using the examples of $\mathbb{Z}$ and $\mathbb{Z}_n$ as our "models", since every cyclic group is isomorphic to one of these models by prop. 2.2.20.
Subgroups of \((\mathbb{Z}_+):\) for \(d \in \mathbb{Z}\), \(<d> = \{dk | k \in \mathbb{Z} \} = d \cdot \mathbb{Z}
\]

**Proposition (2.2.21)** (a) Let \(H \leq \mathbb{Z}\). Then either \(H = \{0\}\) or there is a unique \(d \in \mathbb{N}\) such that \(H = <d>\). 
(b) For \(d \in \mathbb{N}\), \(<d> \cong \mathbb{Z}\)
(c) For \(a, b \in \mathbb{N}\), \(<a> \leq <b> \iff b \mid a\).

**Proof.** We prove (c) first: If \(b \mid a\), then \(a = nb\) so
\(<b> = \{kb | k \in \mathbb{Z}\} = \{knb | k \in \mathbb{Z}\} = \{ka | k \in \mathbb{Z}\} = <a>\).

If \(<a> \leq <b>\), then \(a \in <b>\), so \(a = kb\) for some \(k \in \mathbb{Z}\), so \(b \mid a\).

This proves uniqueness in (a), for if \(d_1, d_2 \in \mathbb{N}\) and \(<d_1> = <d_2>\), then \(d_1 \mid d_2\) and \(d_2 \mid d_1\), so \(d_1 = d_2\).

To show existence in (a): If \(H = \{0\}\) we are done, so assume \(H \neq \{0\}\). Then \(\exists a \in H\), \(a \neq 0\). So \(a \in H\) and \(-a \in H\). One of \(a\) or \(-a\) is positive, so \(H \cap \mathbb{N} \neq \emptyset\). Let \(d\) be the smallest element of \(H \cap \mathbb{N}\).

We claim \(H = <d>\): Since \(d \in H\), \(<d> \leq H\). Now let \(h \in H\) be any element. Then \(h = qd + r\) for some \(r\) in the range \(0 \leq r < d\). Then \(r = h - qd \in H\) and \(r < d\), so by minimality of \(d\) we have \(r = 0\). Thus \(h = qd \in <d>\) and \(H \leq <d>\) as well. So \(H = <d>\).

To see (b), note \(kd = ld \Rightarrow k = l\) (since \(d \neq 0\)) so \(o(d) = \infty\), and \(<d> \cong \mathbb{Z}\). \(\Box\)

Thus, every subgroup of \(\mathbb{Z}\) is either trivial or infinite cyclic.

Now consider \((\mathbb{Z}_n, +)\): \(<[b]> = \{[kb] | k \in \mathbb{Z} \}\).

**Proposition (2.2.23+2.2.28)** Let \(n \in \mathbb{N}\), \(b \in \mathbb{Z}\), \(b \neq 0\), \(d = \gcd(b, n)\).

Then in \(\mathbb{Z}_n\):
(1) \(<[b]> = <[d]> \leq \mathbb{Z}_n>\)
(2) \(\circ([b]) = n/d\)

Hence \([b]\) is a generator of \(\mathbb{Z}_n\) iff \(d = 1\), i.e., \(\gcd(b, n) = 1\).
Proof: (1) Write \( d = sb + t u \), \( s, t \in \mathbb{Z} \). Then \([d] = [sb]\) in \(\mathbb{Z}_n\), so \([d] \in \langle [b] \rangle\) and \(\langle [d] \rangle \leq \langle [b] \rangle\).
Since \( d \mid b \), can write \( b = kd \), so \([b] = [kd] \in \langle [d] \rangle\), so \(\langle [b] \rangle \leq \langle [d] \rangle\). So these subgroups are equal.
(2) Since \(\langle [b] \rangle = \langle [d] \rangle\), \( o([b]) = o([d]) \). Now \( o([d]) = k \) where \( k \) is the smallest \( k \in \mathbb{N} \) such that \([kd] = [0]\). Equivalently, the smallest \( k \in \mathbb{N} \) such that \( n \mid kd \).
Since \( d \mid n \), \( \frac{n}{d} \) is an integer and \( \frac{n}{d} \cdot d = n \). Clearly no smaller integer works, so \( k = \frac{n}{d} \).

Proposition (2.2.24) Let \( H \leq \mathbb{Z}_n \). then \( H = \{ [0] \} \) or \( \exists \ d, 0 \leq d < n \) such that \( H = \langle [d] \rangle \).
Proof: If \( H = \{ [0] \} \), we're done, so suppose \( H \neq \{ [0] \} \). Let \( d \in \{ 1, 2, \ldots, n-1 \} \) be the smallest such that \([kd] \in H \). then \( \langle [d] \rangle \leq H \). For any \([b] \in H \), write \( b = kd + r \), \( 0 \leq r < d \).
Thus \([r] = [b] - [kd] \in H \). By minimality of \( d \), \( r = 0 \), so \([b] = [kd] \in \langle [d] \rangle \). thus \( H \leq \langle [d] \rangle \). Hence \( H = \langle [d] \rangle \).

So every subgroup of \( \mathbb{Z}_n \) is finite cycle (possibly trivial)
Also, the order of \( \langle [b] \rangle \) is \( n \div \gcd(b,n) \), and so the order divides \( n \).

Corollary (2.2.25+2.2.26) Any subgroup of \( \mathbb{Z}_n \) is cyclic with order dividing \( n \). Conversely, for each \( q \in \mathbb{N} \), \( q \mid n \), there is a unique subgroup \( H \) with \( q \) elements, namely \( H = \langle \frac{n}{q} \rangle \). For any two subgroups \( H, H' \), we have \( H \leq H' \iff |H| \mid |H'| \).

Notation: \( |H| \) = number of elements of \( H \), also called order of \( H \).
Example of subgroups of $\mathbb{Z}_{12}$

$\mathbb{Z}_{12}$ \hspace{1cm} \text{order} = 12

order = 6 \langle [2] \rangle \quad \langle [3] \rangle \quad \text{order} = 4

order = 3 \langle [4] \rangle \quad \langle [6] \rangle \quad \text{order} = 2

\langle [0] \rangle \quad \text{order} = 1