Fundamental Theorem on Cyclic groups.

A group that is generated by one element is called *cyclic*. The one element group which consists only of the unit e is cyclic. The group $\mathbb{Z}$ of integers with addition is cyclic.

The group $\mathbb{Z}_n$ of integers $modn$ is cyclic.An infinite cyclic group is *isomorphic* to $\mathbb{Z}$. a finite cyclic group is isomorphic to $\mathbb{Z}_n$

Subgroups of cyclic groups are cyclic:

The subgroups H of $\mathbb{Z}$ are $n\mathbb{Z}$ where n is the smallest non-negative element in $H.$Thus the subgroups of $\mathbb{Z}$ are:

$\{0\} = 0\mathbb{Z}, \mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \ldots$

If G is a cyclic group of order n then the subgroups of G correspond to the non-negative divisors d of $n.$The divisor d of n generates a unique subgroup of order $\frac{n}{d}$. Take for example a cyclic group of order $12.$Say $\mathbb{Z}_{12}$. The divisors of 12 are $1,2,3,4,6,12$

$<[1]>$ is the whole group $\mathbb{Z}_{12}$, $<[2]>$ has 6 elements, $<[3]>$ has 4 elements, $<[6]>$ has two elements, $<[12]>=<0>$ has one element. G

In general, $[k]$ generates in $\mathbb{Z}_n$ the same subgroup as $[(k,n)]$. For example $[8]$ generates in $\mathbb{Z}_{12}$ the same subgroup as $[(8,12)] = [4]$ which is $\{[4],[8],[12] = [0]\}$. If k and n are relatively prime then $[k]$ generates in $\mathbb{Z}_n$ the whole group $[1] = \mathbb{Z}_n$.

This is Theorem 5.5 in the book. you should study it.

The direct product of cyclic groups is cyclic if the orders of the factors are relatively prime. This is theorem 6.1 which you should study. The key is the following. Let $G = G_1 \times G_2$ be the direct product of two groups. Let $(g_1,g_2) \in G.$ Then $(g_1,g_2)^n = (e_1,e_2)$ iff $g_1^n = e_1, g_2^n = e_2$.That is $o(g_1)|n, o(g_2)|n$ That is n is a multiple of the least common multiple of $o(g_1)$ and $o(g_2)$.But $o(g_1,g_2)$ is the smallest n such that $(g_1,g_2)^n = (e_1,e_2)$.Thus $o(g_1,g_2) = \operatorname{lcm}((o(g_1),o(g_2)))$.Only if $o(g_1)$ and $o(g_2)$ are relatively prime we have that (g_1,g_2) generate $G_1 \times G_2$ if g_1 generates G_1 and g_2 generates G_2.

Practice test 2:

1. Which of the direct products are cyclic? Explain your answers.
   - a. $\mathrm{Z}_2 \times \mathrm{Z}_3 \times \mathrm{Z}_5$. Answer: cyclic, orders are pairwise prime.
   - b. $\mathrm{Z}_2 \times \mathrm{Z}_2$. Answer: not. Each element has order 2, none cannot generate a group of order 4. It is Klein four group$V$
   - c. $\mathrm{Z} \times \mathrm{Z}$. Not cyclic. The only possible generator would be $(1,1)$ which cannot generate any element where one component is 0
2. Calculate the order of (8,6,4) in $\mathrm{Z}_{18} \times \mathrm{Z}_9 \times \mathrm{Z}_8$. Answer $o(8) = \frac{18}{(8,18)} = \frac{18}{2} = 9, o(6) = \frac{9}{(6.9)} = \frac{9}{(6,9)} = \frac{9}{3} = 3, o(4) = \frac{8}{(4,8)} = \frac{8}{4} = 2\ o(8,6,4) = \operatorname{lcm}(9,3,2) = 18$
3. Let $f : A \to B$ and $g : B \to C$ be maps such that $g \circ f : A \to C$ is injective (i.e., one-to-one). Prove that f must be injective. Answer:
   Assume that $f(x_1) = f(x_2)$.Then $g(f(x_1) = g(f(x_2))$. But then $x_1 = x_2$ because $g \circ f$ is injective. Thus f is injective.
4. Find for the function $f : \mathrm{N} \to \mathrm{N}$, where $f(n) = 2n, n = 1,2,\ldots$, some function

$g : \mathrm{N} \to \mathrm{N}$ such that $g \circ f$ is the identity on N.
Can you find some h such that $f \circ h$ is the identity on N?Answer: $g(m) = \frac{m}{2}$ if m is even,$g(m) = 1$ (or any number)if m is odd. Then $gf(n) = g(2n) = n$ for any n. There is no h such that $f \circ h = id$ because this would make f surjective which is not the case.

5. Find the right cosets of the subgroup $< (1,1) >$ in $Z_2 \times Z_4$ Answer: $< (1,1) >= \{(1,1),(0,2),(1,3),(0,0)\} \ = H,$ $\mathbb{Z}_2 \times \mathbb{Z}_4 = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3)\}, H + (0,0) = H = \{(0,0),(1$
$H + (0,1) = \{(0,1),(1,2),(0,3),(1,0)\}$. There are two cosets, the coset H for $(0,0)$and the coset $H + (0,1)$.

6. Let $\mathbf{G}$ be any group and $x \in \mathbf{G}$. Let σ be the map $\sigma : y \mapsto xyx^{-1}$. Prove that this map is bijective. Answer: Assume that $\sigma(y_1) = \sigma(y_2)$ then $xy_1x^{-1} = xy_2x^{-1}$. This yields $y_1 = y_2$ by left and right cancellation. Let $z \in G$.Then $z = x(x^{-1}zx)x^{-1}$ shows that σ is surjective..

7. **a**. Let R be an equivalence relation on the set S, and let $s \in S$. How is the equivalence class of s under R defined? Answer: $[s] = \{t|sRt\}$

b. Let R be the equivalence relation on the set R of real numbers where $r \sim s$ iff $|r|= |s|$. What is the equivalence class of r? Answer: $[r] = \{r,-r\}$

8. **a**. Find the order of the following permutation in S_{10}:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 2 & 1 & 7 & 8 & 6 & 10 & 9 \end{pmatrix}$$

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 2 & 1 & 7 & 8 & 6 & 10 & 9 \end{pmatrix} = (1,3,5)(2,4)(6,7,8)(9,1), \mathrm{lcm}(3,2) = 6.$The order is 6.

b. Is this permutation even or odd? Answer: This permutation is even as a product of even permutation.

9. Let p be a prime and G a group whose order is p. Prove that G is cyclic. Answer: The order of any element x different from e in G is a divisor of the order of G which is a prime p.Thus it is p.

10. Let G be a group and let H and K be subgroups of G where $|H|$ and $|K|$ are relatively prime. Prove that $H \cap K = \{e\}$. Answer: Let $x \in H \cap K$.Then $o(x)$ divides $o(H) = |H|$ as well as $o(x)$ divides $o(K) = |K|$. But $|H|$ and $|K|$ are relatively prime. Thus $o(x) = 1$ which is the same as $x = e$