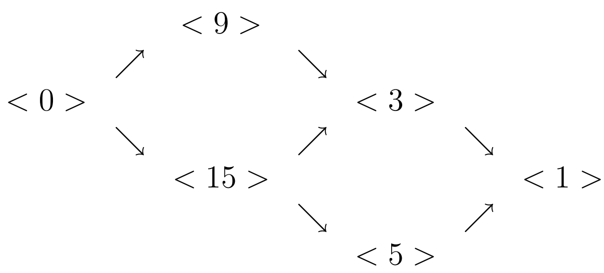
Homework Four Solutions

- (2.3.1) Find all subgroups of $\mathbb{Z}/45\mathbb{Z}$, giving a generator for each. Describe the containments between these subgroups.



- (2.3.3) Find all generators for $\mathbb{Z}/48\mathbb{Z}$.

  Recall that x being a generator is equivalent to $gcd(x, 48)$ equaling one. Thus we have:

$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47.$$

- (2.3.18) Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to H such that $1 \mapsto h$.

  Define $\phi(\mathbb{Z}/n\mathbb{Z}) \to H$ by $\phi(1) = h$. Thus extending by linearity we have $\phi(a) = h^a$. To see that ϕ is well defined, suppose that $a \cong b \bmod n$. Then $n|(a-b)$, that is, $nx = (a-b)$ for some x, and we have $h^a h^{-b} = h^{a-b} = h^{nx} = 1_H$ and thus multiplying on the right by h^b give us $h^a = h^b$. Thus ϕ is indeed well defined. It is straightforward to see that ϕ is a homomorphism, as $\phi(x+y) = h^{x+y} = h^x h^y = \phi(x)\phi(y)$. Uniqueness is clear since if $\phi(1) = h$ and $\psi(1) = h$ then $\phi(n) = h^n = \psi(n)$ for all n, and hence $\phi = \psi$.

- (2.3.19) Show that if H is any group and h is an element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.

  Again note that if $\phi(1) = h$ then $\phi(n) = h^n$. ϕ is a homomorphism as before since $\phi(x+y) = h^{x+y} = h^x h^y = \phi(x)\phi(y)$. Uniqueness is as before since if $\phi(1) = h = \psi(1)$ then $\phi(n) = h^n = \psi(n)$ for all n, so $\phi = \psi$.

- (2.3.25) Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem (ex. 19, section 1.7, the fourth problem on homework three) to prove that the same is true for any finite group of order n.

  Suppose that $G =< g >$ is of order n, and let $\phi : G \to G$ be given by $\phi(x) = x^k$. If $gcd(k, n) = 1$ then there are integers a and b such that $1 = an + bk$. Then $g^1 = g^{an+bk} = (g^n)^a (g^b)^k = (g^b)^k$. Thus $\phi(g^b) = g^1$, and hence $\phi(g^y b) = g^y$ for any y.

  For H any group of order n, let $h \in H$. Then $h^1 = h^{an+bk} = (h^n)^a (h^b)^k = (h^b)^k$, so $\phi(h^b) = h$. (Lagrange gives us that $h^n = 1$ for any $h \in H$).