1[2.3.6]) Find all the generators of the following cyclic groups:

$$(\mathbb{Z}/6\mathbb{Z},+),((\mathbb{Z}/5\mathbb{Z})^\times,\cdot),(2\mathbb{Z},+),((\mathbb{Z}/11\mathbb{Z})^\times,\cdot)$$

$\rightarrow \mathbb{Z}/6\mathbb{Z} = \langle 1\rangle = \langle 5\rangle$.

$\rightarrow (\mathbb{Z}/5\mathbb{Z})^\times = \langle 2\rangle$

$\rightarrow 2\mathbb{Z} = \langle 2\rangle = \langle -2\rangle$

$\rightarrow (\mathbb{Z}/11\mathbb{Z})^\times = \langle\rangle$

***

2[2.3.7]) Show that a finite group of even order has to have at least one element of order 2.

Proof
It has been proven in a previous homework problem that if a group has finite, even order then there exists $a \in G$ such that $a^2 = \mathbb{1}_G$ but $a \neq \mathbb{1}_G$. This is equivalent to saying that $o(a) = 2$, proving the above claim.

Let G be a finite group of even order. Thus, we can write $G = \{\mathbb{1}_G, g_2, \ldots, g_{2n}\}$. We prove in a problem below that $o(x) = o(x^{-1})$. Consider the set of all elements in G such that $o(x) > 2$. Then this set has even order since x and x^{-1} have the same order. We also know that $o(\mathbb{1}) = 1$, implying that the set of G has an odd number of elements that are not $\mathbb{1}_G$. It then follows that there must be at least one element in G which has order 2 since there are an odd number of nonidentity elements in G along with the previous observations.

■

3[2.3.11]) Let G be a group, and let $x \in G$. How are $o(x)$ and $o(x^{-1})$ related? Prove your assertion

$\rightarrow$ We claim that $o(x^{-1}) = o(x)$.

Proof
Observe that $o(x) = \min\{m \in \mathbb{Z}^+ | x^m = \mathbb{1}\}$ and that $(x^{-1})^m = (x^m)^{-1}$. Thus, if $x^m = \mathbb{1}_G$, then $(x^{-1})^m = (x^m)^{-1} = \mathbb{1}_G^{-1} = \mathbb{1}_G$, and $o(x^{-1}) = \min\{m \in \mathbb{Z}^+ | (x^{-1})^m = \mathbb{1}\} = \min\{m \in \mathbb{Z}^+ | (x^m)^{-1} = \mathbb{1}\} = \min\{m \in \mathbb{Z}^+ | x^m = \mathbb{1}\} = o(x)$.

■

4[2.4.4]) Let $H = \{2^n | n \in \mathbb{Z}\}$, and let $\cdot$ denote ordinary multiplication. Show that $(H, \cdot)$ is isomorphic to $(\mathbb{Z}, +)$.

Proof
Consider $\varphi : \mathbb{Z} \to H$ such that $\varphi(n) = 2^n$. It is obvious that this function is bijective since if $2^n = 2^m$ then $n = m$ and $\varphi(\mathbb{Z}) = H$ by definition. We now prove that φ is homomorphic. Observe that $\varphi(n+m) = 2^{n+m}$ and $\varphi(n)\varphi(m) = 2^n 2^m$. It is clear then that $\varphi(n+m) = \varphi(n)\varphi(m)$.

■

5[2.4.14]) Let G and H be groups, and let $\phi : G \to H$ be a group homomorphism. For $x \in G$, prove that $\phi(x^{-1}) = \phi(x)^{-1}$.

Proof
Recall that $\phi(\mathbb{1}_G) = \mathbb{1}_H$. Notice that $x^{-1}x = \mathbb{1}_G$, meaning that $\phi(x^{-1}x) = \phi(x^{-1})\phi(x) = \mathbb{1}_H$ or $\phi(x^{-1}) = \phi(x)^{-1}$.

■

6[2.6.4]) Let G be a group, and let H and K be subgroups of G. Show that $H \cap K$ is a subgroup of G.

Proof
Notice that $\mathbb{1} \in H \cap K$ since $\mathbb{1} \in H$ and $\mathbb{1} \in K$, meaning that $H \cap K$ is nonempty. Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$, implying $ab \in H$ and $ab \in K$ and $ab \in H \cap K$. Finally, suppose that $a \in H \cap K$. Then $a \in H$ and $a \in K$, which means that $a^{-1} \in H$ and $a^{-1} \in K$ and $a^{-1} \in H \cap K$.

■

7[2.6.9]) Let G be a group, and assume that a and b are two elements of order 2 in G. If $ab = ba$, then what can you say about $\langle a, b \rangle$?

$\to$ We can write $G = \langle a, b | a^2 = b^2, ab = ba \rangle = \{\mathbb{1}_G, a, b, ab\}$.

8[2.6.12]) Let $G = \langle x, y \mid x^7 = y^3 = \mathbb{1}, yxy^{-1} = \mathbb{1} \rangle$. What is $|G|$? Find a familiar group that is isomorphic to G.

$\to$ Notice that the relation $yxy^{-1} = \mathbb{1}$ reduces to $x = y^{-1}y = \mathbb{1}$, so we can write $G = \{\mathbb{1}, y, y\}$. It is clear then that this group is isomorphic to the additive group $\mathbb{Z}/3\mathbb{Z}$. This may be observed with the function from $\varphi : \mathbb{Z}/3\mathbb{Z} \to G$ such that $\varphi(\bar{n}) = y^n$.

9[2.6.19]) Let G and H be groups, and let $\theta : G \to H$ be a homomorphism. The set $\{x \in G | \theta(x) = \mathbb{1}\}$ is called the *kernel* of θ and is denoted by $\ker(\theta)$. Show that $\ker(\theta)$ is a subgroup of G.

Proof
Notice that $\mathbb{1}_G \in \ker(\theta)$ since $\theta(\mathbb{1}_G) = \mathbb{1}_H$, meaning that $\ker(\theta)$ is nonempty. Next,

suppose that $a, b \in \ker(\theta)$, then $\theta(a) = \theta(b) = \mathbb{1}_H$. Thus, $\theta(ab) = \theta(a)\theta(b) = \mathbb{1}_H\mathbb{1}_H = \mathbb{1}_H$, implying that $ab \in \ker(\theta)$. Now, suppose that $a \in \ker(\theta)$. We then have that $\theta(a^{-1}a) = \theta(a^{-1})\theta(a) = \theta(a^{-1})\mathbb{1}_H = \theta(a^{-1})$. It is also known that $\theta(a^{-1}a) = \theta(\mathbb{1}_G) = \mathbb{1}_H$, implying that $\theta(a^{-1}) = \mathbb{1}_H$.

■

10[2.6.20]) Let G and H be groups, and let $\theta : G \to H$ be a homomorphism. Let K be a subgroup of H. The set of elements of G that are mapped into K are denoted by $\theta^{-1}(K)$. In other words,

$$\theta^{-1}(K) = \{g \in G \mid \theta(g) \in K\}$$

Is $\theta^{-1}(K)$ necessarily a subgroup of G?

Proof

Obviously $\mathbb{1}_G \in \theta^{-1}(K)$, so it is nonempty. If $a, b \in \theta^{-1}(K)$, then $\theta(a), \theta(b) \in K$. Hence, because θ is a homomorphism $\theta(ab) = \theta(a)\theta(b) \in K$ since K is closed under multiplication. Thus, $ab \in \theta^{-1}(K)$. Similarly, if $a \in K$, then $\theta(a^{-1}a) = \theta(a^{-1})\theta(a) = \mathbb{1}_H$ or $\theta(a^{-1}) = \theta(a)^{-1}$. Notice that $\theta(a^{-1}) = \theta(a)^{-1} \in K$ since $\theta(a) \in K$.

■