Homework 2
MAS4301
Carson Mulvey

NB 2.3 We claim that all subgroups of $\mathbb{Z}$ take form $\langle a \rangle$ for some nonnegative integer a. In other terms, subgroups of $\mathbb{Z}$ are also cyclic. We will prove this by contradiction.

Suppose there exists a subgroup H of $\mathbb{Z}$ that does not take the above form. Then for any choice of positive integer $a \in H$, $H \neq \langle a \rangle$ (the case of $a = 0$ does not have to be checked, since $H \neq \{0\}$). Thus, for any choice of a, there exists $b \in H$ such that $b \notin \langle a \rangle$. This implies that $b \neq 0$.

Then, since H is a subgroup, H is closed under the group operation, so for any $n, m \in \mathbb{Z}$, we know that $na + mb \in H$. We also know that for nonzero $a, b \in \mathbb{Z}$, there exist $n, m \in \mathbb{Z}$ such that $\gcd(a, b) = na + mb$ Letting n and m be as such, we see that $\gcd(a, b) \in H$. Again, since H is closed under the group operation, $n \cdot \gcd(a, b) \in H$ for all $n \in \mathbb{Z}$.

However, since all linear combinations of a and b can be expressed as $n \cdot \gcd(a, b)$ for some $n \in \mathbb{Z}$, all elements of H take this form. Thus $H = \langle \gcd(a, b) \rangle$, which contradicts the assumption that H does not take the form described above. Thus, all subgroups of $\mathbb{Z}$ must take the form described above. $\square$

Other infinite cyclic groups are "essentially the same" as $\mathbb{Z}$, which lets us conclude that subgroups of infinite cyclic groups are also cyclic.

NB 2.4 We will prove by contradiction. Suppose that $\mathbb{R}$ *is* cyclic. Then there exists $a \in \mathbb{R}$ such that $\{na \mid n \in \mathbb{Z}\} = \mathbb{R}$. However, for any choice of a, we see that $\frac{1}{2} \cdot a$ is in $\mathbb{R}$ but *not* in $\{na \mid n \in \mathbb{Z}\}$. This forms a contradiction, so we conclude that $\mathbb{R}$ is not cyclic. $\square$

For all $a \in Q$, we also have $\frac{1}{2} \cdot a$ in $\mathbb{Q}$. Thus, the same argument made above can be made for $\mathbb{Q}$, replacing instances of $\mathbb{R}$ with $\mathbb{Q}$.

3.2 In Q, we have $\langle \frac{1}{2} \rangle = \{\dots, -\frac{3}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, \dots\} = \{\frac{k}{2} \mid k \in \mathbb{Z}\}$.
In Q^*, we have $\langle \frac{1}{2} \rangle = \{\dots, 8, 4, 2, 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots\} = \{\frac{1}{2^k} \mid k \in \mathbb{Z}\}$.

3.10 There are 2 subgroups of D_4: $\{R_0, R_{180}, H, V\}$ and $\{R_0, R_{90}, R_{180}, R_{270}\}$.

3.18 Let G be a group, and let element $a \in G$ satisfy $a^6 = e$. By the definition of order, $|a| \leq 6$. Particularly, $a^6 = e$ holds iff $|a|$ divides 6, so we have $|a| \in \{1, 2, 3, 6\}$.

3.28 Let G be a group containing elements a and b such that $|a| = |b| = 2$ and $ab = ba$. We claim that $H = \{e, a, b, ab\}$ is a subgroup of G of order 4.

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Using the Cayley table above, we see that H is closed under the group operation. Additionally, Since $a^2 = b^2 = e$, we have $a^{-1} = a$ and $b^{-1} = b$. Along with $e^{-1} = e$ and $(ab)^{-1} = b^{-1}a^{-1} = ba = ab$, we see that H is closed under taking inverses. Thus, H is a subgroup of G, and has order 4. $\square$

3.32 Since $\gcd(2^{50}, 3^{50}) = 1$, there exists $n, m \in \mathbb{Z}$ such that $2^{50} \cdot n + 3^{50} \cdot m = 1$. Let n, m be as such. Since H is closed under the group operation of addition, $2^{50} \cdot n + 3^{50} \cdot m = 1 \in H$. Since $1 \in H$, which is a generator for $\mathbb{Z}$, it follows that $H = \mathbb{Z}$.

3.34 Let there be a group G with subgroups H and K. We claim that $H \cap K$ is a subgroup of G. We will follow the definition of a subgroup as given in class (Two-Step Subgroup Test in the textbook).

Consider arbitrary elements $a, b \in H \cap K$. We see that $a, b \in H$, and because H is a subgroup of G, it follows that $ab \in H$. Similarly, since $a, b \in K$ and K is a subgroup of G, we have that $ab \in K$. Thus $ab \in H \cap K$, so $H \cap K$ is closed under the group operation.

Now consider an arbitrary element $a \in H \cap K$. Since $a \in H$ and H is a subgroup of G, $a^{-1} \in H$. Similarly, since $a \in K$ and K is a subgroup of G, $a^{-1} \in K$. Thus $a^{-1} \in H \cap K$, so $H \cap K$ is closed under taking inverses.

Because $H \cap K$ is closed under the group operation and inverses, we conclude that $H \cap K$ is a subgroup of G by the definition of a subgroup. $\square$