MS321 Algebra, tutorial 4, question 3

3. Prove that the intersection of two subgroups of a group is also a subgroup. If m and n are positive integers which cyclic subgroup of $\mathbb{Z}$ is $m\mathbb{Z} \cap n\mathbb{Z}$?

We'll start with the first part. Note that this was part of an exam question in 2012 and 2017. First we collect the definitions we need. The intersection of two sets is the set of elements in both sets. In mathematical notation,

$$A \cap B = \{x \mid (x \in A) \text{ and } (x \in B)\}.$$

A subgroup of a group G is a non-empty subset, H, of G which is closed under products and inverses. In mathematical notation, $H \subseteq G$ satisfies
(0) $H \neq \emptyset$,
(1) $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$ and
(2) $h \in H \Rightarrow h^{-1} \in H$.
Recall that we saw that we could replace (0) by $e \in H$. ($H \neq \emptyset$ means $h \in H$. (2) gives $h^{-1} \in H$ and (1) gives $e = hh^{-1} \in H$.)
Now suppose G is a group with subgroups H and K. We want to show that $H \cap K$ satisfies (0), (1) and (2).
Proof of (0): Since $H < G$, $e \in H$. Since $K < G$, $e \in K$. Thus $e \in H$ and $e \in K$. This means $e \in H \cap K$ so that $H \cap K \neq \emptyset$.
Proof of (1): Suppose $g_1, g_2 \in H \cap K$. In particular, $g_1, g_2 \in H$. Since $H < G$, $g_1 g_2 \in H$. We also have $g_1, g_2 \in K$. Since $K < G$, $g_1 g_2 \in K$. Thus $g_1 g_2 \in H$ and $g_1 g_2 \in K$. This means $g_1 g_2 \in H \cap K$.
Proof of (2): Suppose $g \in H \cap K$. In particular, $g \in H$. Since $H < G$, $g^{-1} \in H$. We also have $g \in K$. Since $K < G$, $g^{-1} \in K$. Thus $g^{-1} \in H$ and $g^{-1} \in K$. This means $g^{-1} \in H \cap K$.

Moving on to the second part, we recall that $\mathbb{Z}$ is cyclic so that all its subgroups are of the form

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

for some k which we can take to be non-negative. By the first part, the intersection of any two subgroups of this type is a subgroup and hence of the same type. Thus

$$m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z},$$

and the question is: what magic combination of the numbers m and n gives the number l? We try a few cases.

$$2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$$

$$3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$$
$$(12)\mathbb{Z} = \{\ldots, -36, -24, -12, 0, 12, 24, 36, \ldots\}$$
$$(18)\mathbb{Z} = \{\ldots, -36, -18, 0, 18, 36, 54, \ldots\}$$

$$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}, \quad (18)\mathbb{Z} \cap (12)\mathbb{Z} = (36)\mathbb{Z}.$$

Baed on this, we expect $l = \text{lcm}(m, n)$. So define $l = \text{lcm}(m, n)$ and prove $m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z}$. This involves showing that $m\mathbb{Z} \cap n\mathbb{Z} \subseteq l\mathbb{Z}$ and $l\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$.

$m\mathbb{Z} \cap n\mathbb{Z} \subseteq l\mathbb{Z}$: Every element of $m\mathbb{Z}$ is a multiple of m. Every element of $n\mathbb{Z}$ is a multiple of n. Thus every element of $m\mathbb{Z} \cap n\mathbb{Z}$ is a common multiple of m and n and must be a multiple of l by definition of lcm.

$l\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$: l is a common multiple of m and n so we can write $l = am$ and $l = bn$. Now if $x \in l\mathbb{Z}$, $x = kl$. However this means

$$x = kl = kam \in m\mathbb{Z} \quad \text{and} \quad x = kl = kbn \in n\mathbb{Z},$$

which is what we want.