Patrick,

The problems you are asking about that I put on the review sheet are for your "general mathematical education" and a way to prepare for the exam by looking at problems that are somewhat *harder* than the ones you'll actually be seeing. In other words, if you can do those, you'll not have any difficulty with the exam because you'll really understand everything. The actual exam will be closer to the practice problems.

On 4.10 A, what you are saying is not quite correct. (You need to review what it means for something to be a subgroup of the integers under addition – see Definition 4.18.) The set $\langle a \rangle \cap \langle b \rangle$ is the set of integers that are simultaneously multiples of a and multiples of b. That means it is the set of all integers x such that $x = sa = tb$ for some integers s, t. So you had the definition more or less correct. However, to show that that is a subgroup of $\mathbf{Z}$, you need to show first that if you take $x_1, x_2 \in \langle a \rangle \cap \langle b \rangle$, then the sum $x_1 + x_2 \in \langle a \rangle \cap \langle b \rangle$ as well. This is true because you have $x_1 = s_1 a = t_1 b$ and $x_2 = s_2 a = t_2 b$ for some integers s_1, t_1, s_2, t_2. So

$$\begin{aligned} x_1 + x_2 &= s_1 a + s_2 a = (s_1 + s_2)a \quad \text{and} \\ x_1 + x_2 &= t_1 b + t_2 b = (t_1 + t_2)b. \end{aligned}$$

This shows $x_1 + x_2 \in \langle a \rangle \cap \langle b \rangle$. Then, you also need to show that $-x_1 \in \langle a \rangle \cap \langle b \rangle$. But this follows too since $-x_1 = (-s_1)a = (-t_1)b$, so $-x_1$ is also a multiple of both a and b.

Now, by Theorem 4.20, we know that $\langle a \rangle \cap \langle b \rangle = m\mathbf{Z}$ for some (unique) positive integer m. I'm calling it m rather than d in the theorem because this m is going to be the least common multiple of a, b.

Then for part B what you need to show is:

1. m is a common multiple of a and b – that is, $a|m$ and $b|m$
2. If n is any other common multiple of a and b, then $m|n$ (so m is the smallest number that is a common multiple of a, b).

Statement 1 follows directly from the definition of $\langle a \rangle \cap \langle b \rangle$. m is in that subgroup so it is a multiple of a and a multiple of b. Statement 2 is proved like this: If $a|n$ and $b|n$, then $n = sa = tb$ for some integers s, t. But that is equivalent to saying that $n \in \langle a \rangle \cap \langle b \rangle$. Hence $m|n$ since m divides everything in $\langle a \rangle \cap \langle b \rangle$.

For part C, use the suggestion: Assume $ab = md$ (for any two integers m, d – not necessarily the lcm and gcd yet). We want to show that d is a common divisor of a and b if and only if m is a common multiple of a and b.

$\Rightarrow$: If $d|a$ and $d|b$ then we can write $a = ds$ and $b = dt$ for some integers s, t. But then $(ds)(dt) = md$, so $dst = m$. This shows $(ds) = a$ divides m and $(dt) = b$ divides m. Hence m is a common multiple of a, b.

$\Leftarrow$: Conversely, if m is a common multiple of a, b, then we have $m = as$ and $m = bt$ for some integers s, t. Substituting the first one into the equation $ab = md$ we get $ab = asd$ so

$b = sd$ and $d|b$. Similarly, if we substitute the second one in to $ab = md$, we get $ab = btd$ so $a = td$, which says $d|a$.

Now to prove that $ab = \gcd(a, b)\mathrm{lcm}(a, b)$, we can argue like this. ab is clearly a common multiple of a, b, so it is in the subgroup $\langle a\rangle \cap \langle b\rangle$. That shows that $\mathrm{lcm}(a, b)$ divides the product ab and we have an equation $ab = \mathrm{lcm}(a, b) \cdot q$ for some integer q. But what we proved above (the "suggestion") shows that q must then be a common divisor of a, b. Arguing by contradiction, suppose that $q \neq d = \gcd(a, b)$. Then from the properties of $d = \gcd(a, b)$ we know that $q|d$, or $d = qs$ for some integer $s > 1$. If we multiply s on both sides of the equation $ab = \mathrm{lcm}(a, b) \cdot q$, we get $abs = \mathrm{lcm}(a, b)d$. But d divides a so $a = dr$ for some integer r and we get $(dr)bs = \mathrm{lcm}(a, b)d$ so $rbs = \mathrm{lcm}(a, b)$. Similarly $b = dt$ for some t so we get $a(dt)s = \mathrm{lcm}(a, b)d$, so $ats = \mathrm{lcm}(a, b)$. But now we have a contradiction because of the factor $s > 1$ on the left side of both of these equations. The number $rb = at$ is also a common multiple of a, b and it's smaller than $rbs = ats$ since $s > 1$. Hence the other factor q in the equation $ab = \mathrm{lcm}(a, b) \cdot q$ must equal $d = \gcd(a, b)$.