Solutions to Assignment 1.

1. The only additive subgroups of \( \mathbb{Z}_{12} \) are
   
   \[ \{0\}, \{0,6\}, \{0,4,8\}, \{0,3,6,9\}, \{0,2,4,6,8,10\}, \mathbb{Z}_{12}, \]
   
   and each of these is an ideal of \( \mathbb{Z}_{12} \). In fact, they are the principal ideals \((0),(6),(4),(3),(2),(1)\), respectively. Since every ideal of \( \mathbb{Z}_{12} \) is an additive subgroup of \( \mathbb{Z}_{12} \), this accounts for all the ideals.

2. \( S \subseteq R \) by definition, and \( S \neq \emptyset \) since \( 0 \in S \). If \( x, y \in S \), then \( a(x-y) = ax - ay = 0 - 0 = 0 \) so \( x-y \in S \), and \( a(xy) = (ax)y = 0y = 0 \) so \( xy \in S \). Hence \( S \) is a subring of \( R \).

   Now assume \( R \) is commutative, and let \( r \in R, x \in S \). Then \( a(rx) = a(xr) = (ax)r = 0r = 0 \), so \( rx \in S \) and \( xr \in S \). Hence \( S \) is an ideal of \( R \).

3. Let \( R, S, T \) be rings and let \( \sigma : R \rightarrow S \), \( \tau : S \rightarrow T \) be ring homomorphisms. If \( a, b \in R \), then \( (\tau\sigma)(a + b) = \tau(\sigma(a + b)) = \tau(\sigma(a) + \sigma(b)) = \tau(\sigma(a)) + \tau(\sigma(b)) = (\tau\sigma)(a) + (\tau\sigma)(b) \), so \( \tau\sigma \) preserves addition. Similarly, \( \tau\sigma \) preserves multiplication, so \( \tau\sigma : R \rightarrow T \) is also a ring homomorphism.

4. (a) Let \( x, y \in \mathbb{Z}_5 \). Then \( \sigma(x + y) = 6(x + y) = 6x + 6y = \sigma(x) + \sigma(y) \) and \( \sigma(xy) = 6xy = 36xy = (6x)(6y) = \sigma(x)\sigma(y) \) in \( \mathbb{Z}_{30} \) (this works because \( 36 \equiv 6 \pmod{30} \)). Hence \( \sigma \) is a ring homomorphism.

   (b) \( \tau \) is not is a ring homomorphism, since it does not preserve multiplication. For example, \( \tau(1 \times 1) = \tau(1) = 2 \), but \( \tau(1)\tau(1) = 4 \).

5. (a) First we show that \( \varphi \) is well-defined. If \( a + n\mathbb{Z}, b + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} \) and \( a + n\mathbb{Z} = b + n\mathbb{Z} \), then \( a \equiv b \pmod{n} \). Since \( m \mid n \) it follows that \( a \equiv b \pmod{m} \) and hence \( a + m\mathbb{Z} = b + m\mathbb{Z} \), as required.
Also

\[ \varphi((a + n\mathbb{Z}) + (b + n\mathbb{Z})) = \varphi((a + b) + n\mathbb{Z}) = (a + b) + m\mathbb{Z} \]
\[ = (a + m\mathbb{Z}) + (b + m\mathbb{Z}) = \varphi(a + m\mathbb{Z}) + \varphi(b + m\mathbb{Z}), \]

so \( \varphi \) preserves addition. Similarly, \( \varphi \) preserves multiplication, so \( \varphi \) is a homomorphism.

Now \( a + n\mathbb{Z} \in \ker \varphi \iff \varphi(a + n\mathbb{Z}) = m\mathbb{Z} \iff a + m\mathbb{Z} = m\mathbb{Z} \iff a \in m\mathbb{Z} \iff m \mid a \). This shows us that

\[ \ker \varphi = \{a + n\mathbb{Z} \mid m \mid a\} = \{n\mathbb{Z}, m + n\mathbb{Z}, 2m + n\mathbb{Z}, \ldots, (k-1)m + n\mathbb{Z}\}, \]

where \( k \in \mathbb{Z} \) such that \( n = mk \). Clearly, \( \text{im} \ varphi = \mathbb{Z}/m\mathbb{Z} \).

(b) In this case, the map is not well defined unless \( n = m \). If \( n \neq m \) then \( n = mk \) with \( k \in \mathbb{Z} \) and \( k > 1 \). Now \( 1 + m\mathbb{Z} = (m+1) + m\mathbb{Z} \).

However, \( \varphi(1 + m\mathbb{Z}) = 1 + n\mathbb{Z} \neq (m+1) + n\mathbb{Z} = \varphi(m+1 + m\mathbb{Z}) \).

6. Let \( \sigma : \mathbb{Z}_5 \to \mathbb{Z}_{30} \) be as in question 11(a). Then \( \sigma(1) = 6 \) is not the identity of \( \mathbb{Z}_{30} \). (But 6 is the identity for the subring \( \text{im} \sigma = \{0, 6, 12, 18, 24\} \) of \( \mathbb{Z}_{30} \) – try it!!)

7. (a) Let \( J = \varphi(I) \). Obviously \( J \subseteq \text{im} \varphi \). As \( 0 \in I \) and \( \varphi(0) = 0 \), it follows that \( 0 \in J \) and hence \( J \neq \emptyset \). Now suppose \( a, b \in J \). Then there are \( i, j \in I \) such that \( \varphi(i) = a \) and \( \varphi(b) = j \). Hence \( b - a = \varphi(j) - \varphi(i) = \varphi(j - i) \). As \( j - i \in I \) it follows that \( b - a \in J \).

Now suppose \( s \in \text{im} \varphi \) and \( a \in J \). Then there is \( i \in I \) such that \( \varphi(i) = a \) and an \( r \in R \) such that \( \varphi(r) = s \). Hence \( sa = \varphi(r) \varphi(i) = \varphi(r i) \). Since \( I \) is an ideal in \( R \) it follows that \( ri \in I \) and thus \( sa \in J \). Similarly \( as \in J \), so \( J \) is an ideal of \( \text{im} \varphi \).

(b) Clearly \( \varphi^{-1}(I) \subseteq R \). Since \( I \) is an ideal of \( \text{im} \varphi \) it follows that \( 0 \in I \). Since \( \varphi(0) = 0 \in I \) we have that \( 0 \in \varphi^{-1}(I) \) and thus \( \varphi^{-1}(I) \neq \emptyset \). Now suppose \( a, b \in \varphi^{-1}(I) \). Thus there are \( i, j \in I \) such that \( \varphi(a) = i \) and \( \varphi(b) = j \). Then \( \varphi(b - a) = \varphi(b) - \varphi(a) = j - i \in I \) and therefore \( b - a \in \varphi^{-1}(I) \). Finally suppose \( r \in R \) and \( a \in \varphi^{-1}(I) \). Then there is an \( i \in I \) such that \( \varphi(a) = i \).

As \( \varphi(ra) = \varphi(r) \varphi(a) = \varphi(r)i \in I \) it follows that \( ra \in \varphi^{-1}(I) \). Similarly \( ar \in \varphi^{-1}(I) \), so \( \varphi^{-1}(I) \) is an ideal of \( R \).