MODEL ANSWERS TO THE SECOND HOMEWORK

1. Chapter 4, §2: 2. If \(ab = ac\) then \(0 = ab - ac = a(b - c)\). As \(R\) is an integral domain, and \(a \neq 0\), it follows that \(b - c = 0\), so that \(b = c\).

3. See model answers to question 40.

8. (a) Denote by \(na\), \(a\) added to itself \(n\) times. Then if \([n]\) denotes \(1\) added to itself \(n\) times, it is easy to see, but somewhat tedious to prove, that \(na = [n]a\). Now as \(F\) is finite, there is an integer \(n\) (for example the order of \(F\)) such that \(na = 0\). It follows, as \(F\) is an integral domain, that \([n] = 0\). Suppose that \(n = xy\). Then \([n] = [x][y] = 0\) and as \(F\) is an integral domain, either \([x] = 0\) or \([y] = 0\). In this case, it follows that if \(p\) is the smallest positive integer such that \([p] = 0\) then \(p\) is prime. But then \(pa = [p]a = 0\), for every \(a \in R\).

(b) Suppose that the order of \(F\) is \(q\) and that \(q\) is not coprime to \(p\). Pick a prime \(r\) that divides \(q\). Then by Sylow’s Theorems there is a subgroup of order \(r\).

Chapter 4, §3: 1. \(I\) contains \(a = 1 \cdot 1\), so \(I\) is not empty. Suppose that \(r\) and \(s\) are in \(I\). Then \(r = xa\) and \(s = ya\) for some \(x\) and \(y\) in \(R\). In this case \(r + s = xa + ya = (x + y)a\). Finally suppose \(r \in I\) and \(y \in R\). Then \(r = xa\) and \(yr = y(xa) = (yx)a \in I\). Thus \(I\) is an ideal.

2. Let \(a \in R\), \(a \neq 0\). Then \(I = \langle a \rangle\) is an ideal of \(R\), and \(I \neq \{0\}\) as \(a = 1 \cdot a \in R\). As the only ideals in \(R\) are \(\{0\}\) and \(R\), it follows that \(I = R\). But then \(1 \in I\) and so there is an element \(b \in R\) such that \(1 = ba \in I\). But then \(a\) is invertible and as \(a\) is arbitrary, \(R\) is a field.

3. As the unit element is unique, it suffices to prove that \(\phi(1)\) acts as a unit. Suppose that \(b \in R'\). As \(\phi\) is surjective, \(b = \phi(a)\) for some \(a \in R\). Then

\[
\phi(1)b = \phi(1)\phi(a) \\
= \phi(1 \cdot a) \\
= \phi(a) \\
= b.
\]

4. As \(0 \in I\) and \(0 \in J\), it follows that \(0 = 0 + 0 \in I + J\). In particular \(I + J\) is non-empty. Suppose that \(x \in I + J\) and \(y \in I + J\). Then \(x = a + b\) and \(y = c + d\), where \(a\) and \(c\) are in \(I\) and \(b\) and \(d\) are in \(J\).
Then
\[ x + y = (a + b) + (c + d) \]
\[ = (a + c) + (b + d). \]
As \( a + c \in I \) and \( b + d \in J \), it follows that \( x + y \in I + J \). Now suppose that \( x \in I + J \) and \( r \in R \). Then
\[ rx = r(a + b) \]
\[ = ra + rb. \]
Thus \( rx \in I + J \) and so \( I + J \) is an ideal.

9. (a) Suppose that \( a \) and \( b \in A \). Then \( a' = \phi(a), b' = \phi(b) \in A' \). Thus
\[ \phi(a + b) = \phi(a) + \phi(b) \]
\[ = a' + b' \in A', \]
as \( A' \) is closed under addition. Thus \( a + b \in A \) and \( A \) is closed under addition. Similarly \( A \) is closed under multiplication and \( A \) is non-empty, as it contains 0 for example. Thus \( A \) is a subring.

(b) Define \( \psi : A \longrightarrow A' \) by \( \psi(a) = \phi(a) \). Then \( \psi \) is clearly a surjective ring homomorphism. By definition \( K \subset A \) and so it is clear that the kernel of \( \psi \) is \( K \). Now apply the Isomorphism Theorem.

(c) Suppose \( r \in R \) and \( a \in A \). Let \( a' = \phi(a) \) and \( r' = \phi(r) \). Then \( a' \in A' \). Thus
\[ \phi(ra) = \phi(r)\phi(a) \]
\[ = r'a' \in A', \]
as we are assuming that \( A' \) is a left ideal. Thus \( ra \in A \) and so \( A \) is a left ideal.

12. Define a map \( \phi : R \longrightarrow \mathbb{Z}_p \) by the rule
\[ \phi(a/b) = [a][b]^{-1}. \]
Note that \( [b] \neq 0 \) as \( b \) is coprime to \( p \) and so taking the inverse of \( [b] \) makes sense. It is easy to check that \( \phi \) is a surjective ring homomorphism. Moreover the kernel is clearly \( I \). Thus the result follows by the Isomorphism Theorem.