MODEL ANSWERS TO THE SECOND HOMEWORK

1. Chapter 4, §3: 1. I contains 0 as $0 \cdot a = 0$, so I is not empty. Suppose that r and s are in I. Then $0 = ra$ and $0 = sa$. In this case

$$(r+s)a = ra + sa = 0 + 0 = 0.$$

Thus $r + s \in I$. Finally suppose $r \in I$ and $x \in R$. Then

$$(rx)a = x(ra) = 0,$$

so that $rx \in I$. 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 ϕ is surjective, $b = \phi(a)$ for some $a \in R$. Then

$$\begin{aligned}\phi(1)b &= \phi(1)\phi(a)\\ &= \phi(1 \cdot a)\\ &= \phi(a)\\ &= b.\end{aligned}$$

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

$$\begin{aligned}x + y &= (a + b) + (c + d)\\ &= (a + c) + (b + d).\end{aligned}$$

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

$$\begin{aligned}rx &= r(a + b)\\ &= ra + rb.\end{aligned}$$

Thus $rx \in I + J$ and so $I + J$ is an ideal.
6. $I \cap J$ is an additive subgroup, as I and J are additive subgroups. Suppose that $r \in R$ and $a \in I \cap J$. As $a \in I$ and I is an ideal, $ra \in I$. Similarly $ra \in J$. But then $ra \in I \cap J$ and $I \cap J$ is an ideal.

9. (a) Suppose that a and $b \in A$. Then $a' = \phi(a)$, $b' = \phi(b) \in A'$. Thus

$$\begin{aligned}\phi(a+b) &= \phi(a) + \phi(b)\\ &= a' + b' \in A',\end{aligned}$$

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

$$\psi\colon A \longrightarrow A'$$

by $\psi(a) = \phi(a)$. Then ψ is clearly a surjective ring homomorphism. By definition $K \subset A$ and so it is clear that the kernel of ψ 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

$$\begin{aligned}\phi(ra) &= \phi(r)\phi(a)\\ &= r'a' \in A',\end{aligned}$$

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

$$\phi\colon R \longrightarrow \mathbb{Z}_p$$

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 ϕ is a surjective ring homomorphism. Moreover the kernel is clearly I. Thus the result follows by the Isomorphism Theorem.
15. Suppose that $a \in R$. Then $a \in IJ$ if and only if a has the form $i_1j_1 + i_2j_2 + \cdots + i_kj_k$, where $i_1, i_2, \ldots, i_k$ and $j_1, j_2, \ldots, j_k$ are in I and J respectively. It is therefore clear that IJ is closed under addition and it is clear that IJ is non-empty. Thus IJ is an additive subgroup. Suppose that $r \in R$ and $a \in I$. Then

$$\begin{aligned}ra &= r(i_1j_1 + i_2j_2 + \cdots + i_kj_k)\\ &= (ri_1)j_1 + (ri_2)j_2 + \ldots (ri_k)j_k.\end{aligned}$$

As $ri_p \in I$, for all all p, it follows that ra is in IJ. Similarly ar is in IJ, and so IJ is an ideal.
18. Under addition, the set $R \oplus S$, with addition defined componentwise, is equal to the set $R \times S$, with addition defined componentwise. We have already seen that this is a group, in 100A. It remains to check that we have a ring. It is easy to see that multiplication is associative

and that $(1,1)$ plays the role of the identity; in fact just mimic the relevant steps of the proof given in 100A that we have a group under addition.
Finally it remains to check the distributive law. Suppose that $x = (a,b)$, $y = (c,d)$, and $z = (e,f) \in R \oplus S$. Then

$$\begin{aligned} x(y+z) &= (a,b)\left((c,d)+(e,f)\right) \\ &= (a,b)(c+e,d+f) \\ &= (a(c+e),b(d+f)) \\ &= (ac+ae,bd+bf) \\ &= (ac+ae,bd+bf) \\ &= (ac,bd)+(ae,bf) \\ &= (a,b)(c,d)+(a,b)(e,f) \\ &= xy+xz. \end{aligned}$$

Thus the distributive law holds.
Define a map $\phi\colon R \oplus S \longrightarrow S$ be sending (r,s) to s. As we saw in 100A, this is a group homomorphism, of the underlying additive groups. It remains to check what happens under multiplication, but the proof is obviously the same as checking addition. Thus ϕ is a ring homorphism.
The kernel is obviously

$$I = \{\,(r,0) \mid r \in R\,\}.$$

In particular I is an ideal. Consider the map $\psi\colon R \longrightarrow R \oplus S$ such that $\psi(r) = (r,0)$. This is obviously a bijection with I and it was checked in 100A that it is a group homomorphism. It is easy to see that in fact ψ is also a ring homomorphism.
The rest follows by symmetry.
Finally, in terms of what comes next in the homework, I claim that $R \oplus S$ is both the direct sum and product in the category of rings.
The categorical product of R and S, denoted $R \times S$ is an object together with two morphisms $p\colon R \times S \longrightarrow R$ and $q\colon R \times S \longrightarrow S$ that are universal amongst all such morphisms, in the following sense.
Suppose that there are morphisms $f\colon T \longrightarrow R$ and $g\colon T \longrightarrow S$. Then there is a unique morphism $T \longrightarrow R \times S$ which makes the following

diagram commute,

$$\begin{tikzcd}
 & R \\
T \arrow[ur, "f"] \arrow[r, dashed] \arrow[dr, "g"'] & R \times S \arrow[u, "p"'] \arrow[d, "q"'] \\
 & S
\end{tikzcd}$$

A direct sum is precisely the same as a product, except we switch the arrows. That is, the direct sum $R \oplus S$ satisfies the following universal property. There are ring homomorphisms, $a\colon R \longrightarrow R \oplus S$ and $b\colon S \longrightarrow R \oplus S$ such that given any pair of ring homomorphisms $c\colon R \longrightarrow T$ and $d\colon S \longrightarrow T$ there is a unique ring homomorphism $f\colon R \oplus S \longrightarrow T$ such that the following diagram commutes,

$$\begin{tikzcd}
R \arrow[d, "a"] \arrow[dr, "c"] & \\
R \oplus S \arrow[r, dashed, "f"] & T \\
S \arrow[u, "b"] \arrow[ur, "d"'] &
\end{tikzcd}$$

The reader is invited to prove that $R \oplus S$ does indeed satisfy the universal properties of both the direct sum and the product.

19. (a) This was already proved in homework one.

Another, slightly more sophisticated, way to solve this problem is as follows. Matrices in R correspond to linear maps

$$\phi\colon R^2 \longrightarrow R^2$$

such that the vector $e_2 = (0, 1)$ is an eigenvalue of ϕ, that is, $\phi(e_2) = ce_2$ for some scalar c. With this description of R, it is very easy to see that R is an additive subgroup of 2×2 matrices and that it is closed under multiplication.

(b) I is clearly non-empty and closed under addition, so that I is an additive subgroup. Now suppose $A \in R$ and $B \in I$, so that

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \qquad B = \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} 0 & ad \\ 0 & 0 \end{pmatrix},$$

and

$$BA = \begin{pmatrix} 0 & cd \\ 0 & 0 \end{pmatrix}.$$

Thus both AB and BA are in I. It follows that I is an ideal.
Again, another way to see this is to state that I corresponds to all transformations ϕ of R^2, such that $\phi(e_1) = be_2$ and e_2 is in the kernel of ϕ. The fact that I is an ideal then follows readily.
(c) Define a map

$$\phi\colon R \longrightarrow F \oplus F$$

by sending

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

to the vector $(a, c) \in F \oplus F$. We first check that ϕ is a ring homomorphism. It is not hard to see that ϕ respects addition, so that if A and B are in R then $\phi(A + B) = \phi(A) + \phi(B)$. We check multiplication. We use the notation as in (1). Then

$$\begin{aligned} \phi(AB) &= (aa', bb') \\ &= (a, b)(a', b') \\ &= \phi(A)\phi(B). \end{aligned}$$

Thus ϕ is certainly a ring homomorphism. It is also clearly surjective and the kernel is equal to I (thereby providing a different proof that I is an ideal). The result follows by the Isomorphism Theorem.
20. The fact that the map ϕ is a ring homomorphism follows immediately from the universal property of $R \oplus S$. Now suppose that $r \in \operatorname{Ker} \phi$. Then $r + I = I$, so that $r \in I$ and similarly $r \in J$. Thus $r \in I \cap J$. Thus $\operatorname{Ker} \phi \subset I \cap J$. The reverse inclusion is just as easy to prove. Thus $\operatorname{Ker} \phi = I \cap J$.
22. (a) Clearly a multiple of mn is a multiple of m and a multiple of n so that $I_{mn} \subset I_m \cap I_n$. Now suppose that $a \in I_m \cap I_n$. Then $a = bm$ and $a = cn$. As m and n are coprime, by Euclid's algorithm, there are two integers r and s such that

$$1 = rm + sn.$$

Multiplying by a, we have

$$\begin{aligned} a &= rma + sna \\ &= (rc)mn + (sb)mn \\ &= (rc + sb)mn. \end{aligned}$$

Thus $a \in I_{mn}$ and so $I_{mn} = I_m \cap I_n$.

(b) Apply (20) to $R = \mathbb{Z}$. It follows that there is a ring homomorphism

$$\phi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n,$$

such that $I_m \cap I_n = I_m n$ is the kernel Thus, by the Isomorphism Theorem, there is an injective ring homomorphism

$$\psi\colon \mathbb{Z}/I_{mn} \longrightarrow \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n.$$

23. By 20 (b) we already know that there is an injective ring homomorphism from one to the other. On the other hand, both sides have cardinality mn. It follows that the given ring homomorphism is in fact an isomorphism.

2. **Bonus Problems** 26. Let $f_i\colon S \longrightarrow R$ be the projection of S onto the ith (counting left to right and then top to bottom), for $i = 1$, 2, 3 and 4. Denote by J_i the projection of I to R, via f_i. Suppose that $a \in J_1$, so that there is a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in I.$$

Multiplying on the left and right by

$$B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

we see that

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I.$$

Now multiply by

$$B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

on the left to conclude that

$$\begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix} \in I.$$

Thus $a \in J_3$. By symmetry, we conclude that $J_i = J$ is independent of i and as I is an additive subgroup, that I consists of all matrices with entries in J. It remains to prove that J is an ideal. It is clear that J is an additive subgroup. On the other hand if $a \in J$ and $r \in R$, then

$$A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I$$

and

$$B = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \in S.$$

Thus

$$BA = \begin{pmatrix} ra & 0 \\ 0 & 0 \end{pmatrix} \in I,$$

and so $ra \in J$. Similarly $ar \in J$ and so J is indeed an ideal.

27. Denote by m the product of the primes $p_1, p_2, \dots, p_n$. Then we want to know the number of solutions of $x^2 = x$ inside the ring $R = \mathbb{Z}_m$. By repeated application of the Chinese Remainder Theorem,

$$\mathbb{Z}_m \simeq \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \mathbb{Z}_{p_3} \oplus \dots \oplus \mathbb{Z}_{p_n}.$$

As multiplication is computed component by component on the RHS, solving the equation $x^2 = x$, is equivalent to solving the n equations $x^2 = x$ in the n rings $\mathbb{Z}_{p_i}$ and taking the product. Now $x = 0$ is always a solution of $x^2 = x$. So if m is prime and $x \neq 0$, $x^2 = x$, then multiplying by the inverse of x, we have $x = 1$. Thus, prime by prime, there are two solutions, making a total of 2^n solutions in R.