MODEL ANSWERS TO THE THIRD HOMEWORK

1. Chapter 4, §3: 5. $I$ and $A$ are additive subgroups, and the intersection of subgroups is a subgroup, so that $I \cap A$ is an additive subgroup of $R$, whence of $A$.
   Now suppose that $a \in A$ and $i \in I \cap A$. Then $a \in R$ and $I$ is an ideal of $R$, so that $ai \in I$. On the other hand, $A$ is a subring of $R$, so that $ai \in A$ as $i$ and $a$ are in $A$. Thus $ai \in I \cap A$. It follows that $I \cap A$ is an ideal.

6. As in the previous question, $I \cap J$ is an additive subgroup, as both $I$ and $J$ are. 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.

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

$$ra = r(i_1j_1 + i_2j_2 + \cdots + i_kj_k)$$
$$= (ri_1)j_1 + (ri_2)j_2 + \cdots (ri_k)j_k.$$ 

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

\[
x(y + z) = (a, b) ((c, d) + (e, f)) \\
= (a, b)(c + e, d + f) \\
= (a(e + c), b(d + f)) \\
= (ac + ae, bd + bf) \\
= (ac + ae, bd + bf) \\
= (ac, bd) + (ae, bf) \\
= (a, b)(c, d) + (a, b)(e, f) \\
= xy + xz.
\]

Thus the distributive law holds.

Define a map \( \phi: R \oplus S \rightarrow S \) 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 \( \phi \) is a ring homomorphism. The kernel is obviously

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

In particular \( I \) is an ideal. Consider the map \( \psi: R \rightarrow R \oplus S \) 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 \( \psi \) 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. Both the direct sum and the product are defined in terms of universal properties. I define the product first.

The categorical product of \( R \) and \( S \), denoted \( R \times S \) is an object together with two morphisms \( p: R \times S \rightarrow R \) and \( q: R \times S \rightarrow S \) that are universal amongst all such morphisms, in the following sense.

Suppose that there are morphisms \( f: T \rightarrow R \) and \( g: T \rightarrow S \). Then there is a unique morphism \( T \rightarrow R \times S \) which makes the following
A direct sum is precisely the same as a product, except where we switch the arrows. That is, the direct sum \( R \oplus S \) satisfies the following universal property. There are ring homomorphisms, \( a: R \to R \oplus S \) and \( b: S \to R \oplus S \) such that given any pair of ring homomorphisms \( c: R \to T \) and \( d: S \to T \) there is a unique ring homomorphism \( f: R \oplus S \to T \) such that the following diagram commutes,

\[
\begin{array}{ccc}
R & \xrightarrow{a} & R \oplus S \\
\downarrow{c} & & \downarrow{f} \\
R \oplus S & \xrightarrow{f} & T \\
\downarrow{b} & & \downarrow{d} \\
S & \xrightarrow{d} & T
\end{array}
\]

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) As \( R \) is a subset of the \( 2 \times 2 \) matrices, it suffices to check that \( R \) is non-empty (clear as \( R \) contains the zero matrix), closed under addition and inverses (easy check) and closed under multiplication. Suppose \( A \) and \( B \) are two matrices in \( R \). Then

\[
A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad B = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}
\]

for some \( a, b, c, a', b' \) and \( c' \in \mathbb{R} \). Then

\[
AB = \begin{pmatrix} aa' & ab' + a'b \\ 0 & cc' \end{pmatrix}.
\]

Thus \( AB \in R \) and \( R \) is indeed a ring.

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

\[
\phi: \mathbb{R}^2 \to \mathbb{R}^2
\]
such that the vector $e_2 = (0, 1)$ is an eigenvalue of $\phi$, that is $\phi(e_2) = ce_2$.

With this description of $R$, it is very easy to see that $R$ is an additive subgroup of $2 \times 2$ 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

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

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 $\phi$ of $\mathbb{R}^2$, such that $\phi(e_1) = be_2$ and $e_2$ is in the kernel of $\phi$. The fact that $I$ is an ideal then follows readily.

(c) Define a map

$$\phi: R \rightarrow F \oplus F$$

by sending

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

to the vector $(a, c) \in F \oplus F$. We first check that $\phi$ is a ring homomorphism. It is not hard to see that $\phi$ 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

$$\phi(AB) = (aa', bb')$$

$$= (a, b)(a', b')$$

$$= \phi(A)\phi(B).$$

Thus $\phi$ 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 $\phi$ is a ring homomorphism follows immediately from the universal property of $R \oplus S$. Now suppose that $r \in \text{Ker } \phi$. Then $r + I = I$, so that $r \in I$ and similarly $r \in J$. Thus $r \in I \cap J$. Thus $\text{Ker } \phi \subset I \cap J$. The reverse inclusion is just as easy to prove. Thus $\text{Ker } \phi = I \cap J$.

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

$$a = rma + sna = (rc)mn + (sb)mn = (rc + sb)mn.$$ 

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

$$\phi: \mathbb{Z} \rightarrow \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n,$$

such that $I_m \cap I_n = I_{mn}$ is the kernel. Thus, by the Isomorphism Theorem, there is an injective ring homomorphism

$$\psi: \mathbb{Z}/I_{mn} \rightarrow \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$$

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. Chapter 4, §4: 1. Note that if 3 does not divide $a$, then either $a$ is congruent to 1 or 2 modulo 3. Either way $a^2$ is congruent to $1 = 1^2 = 2^2$ modulo three. In this case $a^2 + b^2$ is congruent to either $1 = 1 + 0$ or $2 = 1 + 1$, modulo three. Thus 3 does not divide $a^2 + b^2$.

2. It is proved in example that $M$ is maximal so that $R/M$ is a field and so it suffices to prove that $R/M$ has cardinality 9. There are two ways, essentially equivalent, ways to proceed. The first is to observe that $a + bi$ and $c + di$ generate the same left coset if and only if $(a-c) + (b-d)i \in I$, that is 3 divides $a-c$ and 3 divides $b-d$. In turn, this is equivalent to saying that $a$ and $c$ (respectively $b$ and $d$) have the same residue modulo 3. As there are 3 residues modulo three, namely 0, 1 and 2, there are $9 = 3 \times 3$ left cosets, and $R/M$ has cardinality 9.

The second way to proceed is to define a map

$$\phi: \mathbb{Z}[i] \rightarrow \mathbb{Z} \oplus \mathbb{Z},$$

by sending $a + bi$ to $(a, b)$. It is easy to check that this map is a group homomorphism (and just as easy to see that it is not a ring homomorphism). Under this correspondence, $I$ corresponds to $3\mathbb{Z} \oplus 3\mathbb{Z}$ and so the cardinality of $R/M$ is equal to the cardinality of

$$\frac{\mathbb{Z} \oplus \mathbb{Z}}{3\mathbb{Z} \oplus 3\mathbb{Z}} \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3.$$
which, as before, is $9 = 3 \times 3$.

7. First note that, as $\sqrt{2}$ is irrational, then

$$a + b\sqrt{2} = c + d\sqrt{2},$$

if and only if $a = c$ and $b = d$. Indeed if $b = d$, then this is clear. Otherwise, we can solve for $\sqrt{2}$ to obtain

$$\sqrt{2} = \frac{a - c}{d - b} \in \mathbb{Q},$$

a contradiction. Thus the fact that $R/M$ has 25 elements follows, as in 2.

It remains to prove that $M$ is maximal. Given two integers $a$ and $b$, consider $a^2 - 2b^2$. As in 2 and 7, the key point to establish is that if 5 does not divide either $a$ of $b$ then it does not divide $a^2 - 2b^2$. The squares modulo 5 are 0, 1 and 4, and multiplying by three we get 0, 3 and 2. If we take the sum of one number from the first list and one number from the second, as before, the only way to get a number congruent to zero modulo 5, is to pick zero from both. The rest follows as in example 2.

8. Take $I$ to be the set of all Gaussian integers of the form $a + bi$, where both $a$ and $b$ are divisible by 7. The key point is that if 7 does not divide $a$, then 7 does not divide $a^2 + b^2$. Indeed the squares modulo seven are 0, 1, 2 and 4, as can be seen by squaring 0, 1, 2 and 3 (for the rest observe that $a^2 = (-a)^2 = (7 - a)^2$, modulo seven). If a pair of these sum to a number divisible by 7, then both of these numbers must be 0, whence the result. The rest follows as in example 2.

3. **Bonus Problems**

26. Let $f_i : S \to R$ be the projection of $S$ onto the $i$th (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

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

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$
on the left to conclude that
\[
\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \in I.
\]
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 \( p_1, p_2, \ldots, p_n \). 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,
\[
\mathbb{Z}_m \cong \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \mathbb{Z}_{p_3} \oplus \cdots \oplus \mathbb{Z}_{p_n}.
\]
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 \( R \).