MODEL ANSWERS TO THE THIRD HOMEWORK

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 $a^2 + b^2$.

Chapter 4, §4: 2. It is proved in example 2 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, 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

$$\phi\colon \mathbb{Z}[i] \longrightarrow \mathbb{Z} \oplus \mathbb{Z},$$

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 $9 = 3 \times 3$.

Chapter 4, §4: 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 before, the key point to establish is that if 5 does not divide at least one of a or 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.

Chapter 4, §4: 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. The rest follows as in example 2.

2. We are told that I is an ideal. Suppose that J is any ideal of R. To show that I is maximal it suffices to show that ever ideal J of R not contained in I is equal to R.

As J is not contained in I there is an element $a \in R$ such that $a \in J$ whilst $a \notin I$. By assumption, a is then a unit of R, so that there is an element $b \in R$ such that $ab = 1$. Then $1 = ba \in J$. Let c be an arbitrary element of R. Then $c = c \cdot 1 \in J$. Thus $J = R$. It follows that I is the unique maximal ideal.

3. (i) Replacing S by the image of ϕ, we may as well assume that ϕ is surjective. Let ψ denote the composition of ϕ and the natural map from S to S/J. Then the kernel of ψ is I. Thus I is an ideal of R. Moreover by the Isomorphism Theorem,

$$\frac{R}{I} \simeq \frac{S}{J}.$$

As J is prime, S/J is an integral domain. Thus R/I is also an integral domain and so I is prime.

(ii) The key point is to exhibit an ideal of a ring that is prime but not maximal. For example take the zero ideal in $\mathbb{Z}$. Consider the natural inclusion

$$\phi\colon \mathbb{Z} \longrightarrow \mathbb{Q},$$

which is easily seen to be a ring homomorphism. Then the zero ideal J of $\mathbb{Q}$ is maximal as $\mathbb{Q}$ is a field. But the inverse image I of J is the zero ideal of $\mathbb{Z}$ which is not maximal, as $\mathbb{Z}$ is not a field.

4. Suppose that p is prime and that $p = ab$, for a and b two elements of R. Certainly $p|(ab)$, so that either $p|a$ or $p|b$. Suppose $p|a$. Then $a = pc$. We have $p = ab = p(bc)$. Cancelling, $bc = 1$ so that b is a unit. Thus p is irreducible.

5. (a) Note that $\langle 1 \rangle = R$. Indeed given $r \in R$, $r = r \cdot 1 \in \langle 1 \rangle$. Thus an ideal K is the whole of R if and only if it contains 1.

(b) We want to prove

$$IJ = I \cap J.$$

One inclusion is clear. If $a \in IJ$, then a is a sum of terms of the form ij. Each term is clearly in i, as $i \in I$ and $j \in R$ and I is an ideal. Thus $a \in I$. By symmetry $a \in J$. It follows that that $a \in I \cap J$.
Now suppose that $a \in I \cap J$. Now $1 = i + j$. In this case,

$$\begin{aligned} a &= a \cdot 1 \\ &= a(i+j) \\ &= ai + aj. \end{aligned}$$

Now $a \in J$ and so $ai \in IJ$. Similarly $a \in I$ and so $aj \in IJ$. Thus $a \in IJ$.
6. By 5 (b) and an obvious induction, it suffices to prove that $I = I_1$ and

$$J_k = \prod_{a=2}^{k} I_a$$

are coprime. We proceed by induction on k. The case $k = 2$ is part of our assumption. By induction then, we can write

$$1 = i + j,$$

where $j \in J_{k-1}$. On the other hand, as I and I_k are coprime, we may write

$$1 = a + b,$$

where $a \in I$ and $b \in I_k$. Now multiply these two equations,

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= (i+j)(a+b) \\ &= ia + ib + ja + jb. \end{aligned}$$

Now the first two terms are elements of I and the last two are elements of J_k. The result follows.
7. (a) Let

$$\phi_i \colon R \longrightarrow R_i$$

be the natural map. Then ϕ_i is a ring homomorphism. ϕ is the map derived from the universal property of the direct sum; as such it is automatically a ring homomorphism.
(b) I claim first that ϕ is surjective if and only if there are elements $s_1, s_2, \ldots, s_k$ of R such that

$$\phi_b(s_a) = \delta_{ab},$$

where δ_{ab} is defined in the standard way as

$$\delta_{ab} = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{otherwise.} \end{cases}$$

One direction is clear. Otherwise suppose we can find such $s_1, s_2, \ldots, s_k$. Pick $(x_1, x_2, \ldots, x_k) \in \oplus_{i=1}^k R_i$. Then each $x_a = t_a + I_a$. Set

$$s = \sum_a t_a s_a.$$

It suffices to prove that $\phi_a(s) = t_a + I_a$, that is, to prove this result coordinate by coordinate. But

$$\begin{aligned}\phi_a(s) &= \phi_a(\sum_b t_b s_b) \\ &= \sum_b \phi_a(t_b)\phi_a(s_b) \\ &= \sum_b \delta_{ab}(t_b + I_a) \\ &= t_a + I_a,\end{aligned}$$

as required.

So it suffices to prove that $I_1, I_2, \ldots, I_k$ are pairwise coprime if and only if we can find $s_1, s_2, \ldots, s_k$ as above.

First suppose that we can find such elements $s_1, s_2, \ldots, s_k$. Pick two indices a and b and let $I = I_a$, $J = I_b$ and $s = s_a$. Then $s + I = 1 + I$ and $s + J = 0 + J = J$. It follows that there are elements i and j of I and J such that $s + i = 1$ and $s = j$. In this case $1 - i = j$, so that $1 = i + j$. Hence I and J are coprime. As a and b are arbitrary, it follows that if ϕ is surjective then $I_1, I_2, \ldots, I_k$ are pairwise coprime.

It remains to prove that if $I_1, I_2, \ldots, I_k$ are pairwise coprime, we may find $s_1, s_2, \ldots, s_k$ with the given properties. By symmetry we may assume that $a = 1$. Set $I = I_1$ and $J = \cap_{a=2}^k I_a$. Then we have already seen that I and J are coprime. Thus there are i and j in I and J such that $1 = i + j$. Let $s = j$. As $j \in J$, $\phi_b(s_a) = 0$, if $b > 1$. As $s = 1 - i$, $\phi(s) = 1$. The result follows.

(c) The kernel is clearly equal to the intersection of the ideals. By 2, this is the same as the product.

8. Follows immediately from the Isomorphism Theorem and what we proved. There are two places that the book asks the reader to prove versions of the Chinese Remainder Theorem. The first is on page 147. The relevant questions are 20, 21, 22, 23 and 24. 20 follows from our version (GCRT). 21 is a special case of 23. 22 is a special case of the GCRT. 23 follows from the our version, by taking $R = \mathbb{Z}$, $I = \langle m \rangle$ and $J = \langle n \rangle$. 24 is equivalent to saying that ϕ is surjective.

The second is on page 165. The relevant question is 17. As $R = F[x]$ is a UFD, if $p(x)$ is prime it is certainly irreducible. As R is also a

Euclidean domain, if $p(x)$ and $q(x)$ have no common factor (for example if $p(x)$ is prime and $p(x)$ does not divide $q(x)$) then we may find r and s such that

$$1 = r(x)p(x) + s(x)q(x).$$

Thus the ideals $\langle p_a(x) \rangle$ are pairwise coprime and the result follows by the GCRT.

Challenge Problems: (Just for fun)

9. (i) It is clear that R is a group under addition, isomorphic to the group $R \oplus R$.
$1 = 1 + 0\epsilon$ plays the role of 1. Suppose that $a + b\epsilon$, $c + d\epsilon$ and $e + f\epsilon$ are three elements of K. We have

$$\begin{aligned}(a + b\epsilon)((c + d\epsilon)(e + f\epsilon)) &= (a + b\epsilon)(ce + (cf + de)\epsilon) \\ &= ace + (bcf + ade)\epsilon,\end{aligned}$$

and

$$\begin{aligned}((a + b\epsilon)((c + d\epsilon))(e + f\epsilon) &= (ac + (bc + ad)\epsilon)(e + f\epsilon) \\ &= ace + (bcf + ade)\epsilon,\end{aligned}$$

so that multiplication is associative. Distributivity is checked similarly.
(ii) Define a function

$$\phi \colon K[x] \longrightarrow R$$

by sending

$$a + bx + \ldots \qquad \text{to} \qquad a + b\epsilon.$$

ϕ is clearly surjective and it is easy to check that ϕ is a ring homomorphism.
Note that the kernel of ϕ is $\langle x^2 \rangle$. Thus the resilt follows by the first isomorphism theorem.
10. Let $p \in \mathbb{N}$ be a prime.
(i) If a is an integer then consider a^2 modulo 4. As

$$0^2 = 2^2 = 0 \qquad \text{and} \qquad 1^2 = 3^2 = 1$$

a^2 modulo 4 is either 0 or 1. Thus $a^2 + b^2$ is either 0, 1 or 2 modulo 4. In particular if p is a sum of two squares then it is not congruent to 3 modulo 4.
(ii)

$$2 = 1 + 1 = 1^2 + 1^2.$$

(iii) It is clear that

$$(x, y, z) \longrightarrow (x, z, y)$$

is an involution of S.

Now we check the second function is an involution of S. Suppose that $(x, y, z) \in S$. Then x, y and z are natural numbers and $x^2 + 4yz = p$. It is clear that either

$$x \leq y - z \qquad \text{or} \qquad y - z < x < 2y \qquad \text{or} \qquad 2y \leq x.$$

Suppose that $x = y - z$. Then

$$(y - z)^2 + 4yz = (y + z)^2 \neq p$$

as p is not a square. Similarly if $x = 2y$ then

$$x^2 + 4yz = 4y(y + z) \neq p$$

as p is not even. Thus we at least get a function

$$S \longrightarrow \mathbb{Z}^3.$$

Suppose that $x < y - z$. Then $y - x - z > 0$ and

$$\begin{aligned}(x + 2z)^2 + 4z(y - x - z) &= x^2 + 4xz + 4z^2 + 4yz - 4xz - 4z^2 \\ &= x^2 + 4yz \\ &= p.\end{aligned}$$

Thus $(x + 2z, z, y - x - z) \in S$. Now suppose that $y - z < x < 2y$. Then $2y - x > 0$, $x - y + z > 0$ and

$$\begin{aligned}(2y - x)^2 + 4y(x - y + z) &= 4y^2 - 4xy + x^2 + 4xy - 4y^2 + 4yz \\ &= x^2 + 4xz \\ &= p.\end{aligned}$$

Thus $(2y - x, y, x - y + z) \in S$. Finally suppose that $2y < x$. Then $x - 2y > 0$, $x - y + z > 0$ and

$$\begin{aligned}(x - 2y)^2 + 4y(x - y + z) &= x^2 - 4xy + 4y^2 + 4xy - 4y^2 + 4yz \\ &= x^2 + 4yz \\ &= p.\end{aligned}$$

Thus $(x - 2y, x - y + z, y) \in S$. Thus we get a function

$$\phi \colon S \longrightarrow S.$$

Now check that applying ϕ twice is the identity. Suppose that $x < y - z$. Then

$$(x + 2z) > 2z.$$

Thus

$$\begin{aligned}\phi^2(x,y,z) &= \phi(x+2z, z, y-x-z)\\ &= (x+2z-2z, x+2z+z+y-x-z, z)\\ &= (x,y,z).\end{aligned}$$

Now suppose that $y - z < x < 2y$. Then

$$2y - x > y - (x - y + z) \qquad \text{and} \qquad 2y > 2y - x.$$

Thus

$$\begin{aligned}\phi^2(x,y,z) &= \phi(2y-x, y, x-y+z)\\ &= (2y-(2y-x, y.2y-x-y+x-y+z)\\ &= (x,y,z).\end{aligned}$$

Finally suppose that $2y < x$. Then

$$x - 2y < (x - y + z) - y.$$

Thus

$$\begin{aligned}\phi^2(x,y,z) &= \phi(x-2y, x-y+z, y)\\ &= (x-2y+2y, y, x-y+z-(x-2y)-y)\\ &= (x,y,z).\end{aligned}$$

It follows that ϕ is indeed an involution.
(iv) Suppose that ϕ fixes (x, y, z), so that

$$\phi(x,y,z) = (x,y,z).$$

The definition of ϕ breaks S into three regions. We already saw that ϕ switches the first and third region. Thus we must be in the middle region $y - z < x < 2y$. In this case we would have $z = x - y + z$ so that $x = y$. Therefore

$$x^2 + 4yz = x(x + 4z) = p.$$

As p is prime, $x = 1$ and $4z + 1 = p$. By assumption $p = 4k + 1$, for some natural number k, so that $z = k$. In this case $(1, 1, k)$ is fixed by ϕ.
Thus ϕ has one fixed point. Thus S has an odd number of elements, since the other elements of S come in pairs (formally, the group $\mathbb{Z}_2$ acts on S via ϕ. The cardinality of an orbit is one or two. There is one orbit of cardinality 1, corresponding to $(1, 1, k)$ and all other orbits have cardinality 2).

As S has an odd number of orbits, the first involution must also have at least one fixed point. Thus we may find $(a, b, c) \in S$ such that

$$(a, b, c) = (a, c, b).$$

In this case

$$\begin{aligned} p &= a^2 + 4bc \\ &= a^2 + 4b^2 \\ &= a^2 + (2b)^2 \end{aligned}$$

is a sum of two squares.

11. Let $p \in \mathbb{N}$ be a prime. Suppose first that p is a sum of two squares

$$\begin{aligned} p^2 &= a^2 + b^2 \\ &= (a + bi)(a - bi). \end{aligned}$$

Note that $a + bi$ is invertible if and only if $a - bi$ is invertible. Thus neither $a + bi$ nor $a + bi$ is invertible and so p is a prime element of the Gaussian integers.

Thus we may assume that p is congruent to 3 modulo 4 and that p is not a sum of two squares.

We just mimic the construction in the book and the lecture notes. Let I be the set of Gaussian integers R of the form $a+bi$ where both a and b are divisible by p.

It is clear that I is an ideal and $I \neq R$. We first follow the book. Suppose that $I \subset J$ is an ideal, not equal to I. Then we can find $a + bi \in J$ but not in I. It follows that p does not divide at least one of a or b.

Therefore p does not divide $c = a^2 + b^2$. As

$$c = (a + bi)(a - bi),$$

it follows that c belongs to J but not to I. As c is coprime to p we may find x and y such that

$$1 = xc + yp.$$

As $p \in I \subset J$, it follows that $1 \in J$. Thus $J = R$ and so I is maximal. In particular I is prime.

Instead we can follow the lecture notes. We sketch the details. Suppose that $(a + bi)(c + di) \in I$ but $a + bi \notin I$. As

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$

p divides

$$(ja + b)c - (jb - a)d \qquad \text{and} \qquad (ja + b)d + (jb - a)c,$$

and p divides

$$(a+jb)c-(b-ja)d \qquad \text{and} \qquad (a+jb)d+(b-ja)c,$$

and the other way around with j switched between a and b.
By assumption p does not divide both a and b. In this case p divides a but not b, or vice-versa, or the same is true replacing the pair (a,b) by one of (a,b), or $(ja+b, ja-b)$ or $(a+jb, jb-a)$ for $2 \leq j \leq k+1$. Now finish as in the lecture notes.