MODEL ANSWERS TO THE FOURTH HOMEWORK

1. 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.
2. (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.
3. 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.
4. It is convenient to introduce the norm, $N(\alpha)$, of any element of $\mathbb{Z}[\sqrt{-5}]$. In fact it is not harder to do the general case $\mathbb{Z}[\sqrt{d}]$, where d is any square-free integer. Given $\alpha = a + b\sqrt{d}$, the norm is by definition

$$N(\alpha) = a^2 - b^2 d.$$

Using the well-known identity,

$$A^2 - B^2 = (A + B)(A - B),$$

note that the norm can be rewritten,

$$N(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = \alpha\bar{\alpha},$$

where $\bar{\alpha}$, known as the conjugate of α, is by definition $a - b\sqrt{d}$. Note that in the case $d < 0$, in fact $\bar{\alpha}$ is precisely the complex conjugate of α. The key property of the norm, which may be checked easily, is that it is multiplicative (this is automatic when $d < 0$). Suppose that $\gamma = \alpha\beta$, then

$$N(\gamma) = N(\alpha)N(\beta).$$

Indeed if $\alpha = a + b\sqrt{d}$ and $\beta = a' + b'\sqrt{d}$, then

$$\gamma = (aa' + bb'd) + (a'b + ab')\sqrt{d},$$

so that

$$\begin{aligned} N(\gamma) &= (aa' + bb'd)^2 - d(a'b + ab')^2 \\ &= (aa')^2 + (bb')^2d^2 - d(a'b)^2 - d(ab')^2. \end{aligned}$$

On the other hand

$$\begin{aligned} N(\alpha)N(\beta) &= (a^2 - b^2d)((a')^2 - (b')^2d) \\ &= (aa')^2 + (bb')^2d^2 - d(a'b)^2 - d(ab)^2 \\ &= N(\gamma). \end{aligned}$$

We first use this to determine the units. Note that if α is a unit, then there is an element β such that $\alpha\beta = 1$. Thus

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1,$$

so that $N(\alpha)$ and $N(\beta)$ are divisors of 1. Thus if $\alpha = a + b\sqrt{d}$ is unit, then $a^2 - b^2d = \pm 1$. Conversely, if the norm of α is ± 1, then $\mp\bar{\alpha}$ is the inverse of α. It follows that the units are precisely those elements whose norm is ± 1.

(a) As $d = -5$, the units are precisely those elements $\alpha = a + b\sqrt{-5}$ such that

$$a^2 + 5b^2 = 1.$$

The only possibilities are $a = \pm 1$, $b = 0$, so that $\alpha = \pm 1$. Suppose that 2 is not irreducible, so that $2 = \alpha\beta$, where α and β are not units. Then

$$4 = N(2) = N(\alpha)N(\beta).$$

As α and β are not units, then $N(\alpha)$ and $N(\beta)$ are greater than one. It follows that $N(\alpha) = N(\beta) = 2$. Suppose that

$$a^2 + 5b^2 = 2.$$

Then $b = 0$ and $a = \pm\sqrt{2}$, not an integer. Thus 2 is irreducible. For 3, the proof proceeds verbatim, with 2 replacing 3. The crucial observation is that one cannot solve

$$a^2 + b^2 = 3.$$

where a and b are integers. For $1 + \sqrt{5}$, observe that its norm is 6, so that α and β are of norm 2 and 3, which we have already seen is impossible.

(b) It suffices to prove that every ascending chain of principal ideals stabilises. But this is clear, since if

$$\langle \alpha \rangle \subset \langle \beta \rangle,$$

then

$$N(\beta) \leq N(\alpha),$$

with equality in one equation if and only if there is equality for the other. Thus a strictly increasing chain of principal ideals is the same thing as a strictly decreasing chain of natural numbers. Thus the set of principal ideals satisfies ACC as the set of natural numbers satisfies DCC.

(c) By (a),

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

are two different factorisations of 6 into irreducibles.

5. (a) Clearly $I + J$ is non-empty. For example it contains $0 = 0 + 0 \in I + J$. Suppose that a and b are in $I + J$. Then $a = i + j$ and $b = k + l$, where i and k are in I and k and l are in J. In this case

$$\begin{aligned} a + b &= (i + j) + (k + l) \\ &= (i + k) + (j + l). \end{aligned}$$

As $i + k \in I$ and $j + l \in J$, it follows that $a + b \in I + J$. Thus $I + J$ is closed under addition. Now suppose $r \in R$. Then

$$\begin{aligned} ra &= r(i + j) \\ &= ri + rj. \end{aligned}$$

As I and J are ideals, $ri \in I$ and $rj \in J$. Thus $ra \in I + J$. Taking $r = -1$, we see that $I + J$ is closed under inverses. Thus $I + J$ is an ideal.

(b) 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. The result follows.

(c) 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 (c) 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 $s_1, s_2, \dots, s_k$ 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 $s_1, s_2, \dots, s_k$. Pick $(x_1, x_2, \dots, x_k) \in \oplus_{i=1}^k R_i$. 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

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

as required.

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

First suppose that we can find such elements $s_1, s_2, \dots, s_k$. 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 $I_1, I_2, \dots, I_k$ are pairwise coprime.

It remains to prove that if $I_1, I_2, \dots, I_k$ are pairwise coprime, we may find $s_1, s_2, \dots, s_k$ 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 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.

9. Say that S has the **cancellation property** if whenever $a+b = a+c$ then $b = c$. This is the natural analogue of the condition that there are no zero divisors in the ring; it is equivalent to saying that S can be embedded in a group.

Say that a and b are **associates** if $a = b + c$ and $a + d = b$ for some c and d.

Say that p is **prime** if whenever $p + c = a + b$ then either $p + d = a$ or $p + d = b$ for some d.

We say that S has **unique factorisation** if every non-zero element a of S, not a unit, is a sum of primes, unique up to re-ordering and associates.

10. First thin out the sequence $v_1, v_2, \dots, v_n$ by discarding any elements which are positive integral linear combinations of the other vectors. The remaining vectors are then all irreducible.

In this case I claim that S has unique factorisation if and only if $v_1, v_2, \dots, v_n$ are independent as vectors in the vector space $\mathbb{Q}^2$. In particular if S has unique factorisation then $n \leq 2$ and if there are two vectors, then neither is a multiple of the other.

Indeed suppose that we don't have unique factorisation. Then there is $v \in \mathbb{Z}^2$ such that,

$$v = \sum a_i v_i = \sum b_i v_i,$$

where $a_i \neq b_i$ for some i and $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ are positive integers. Subtracting one side from the other, exhibits a linear dependence between $v_1, v_2, \dots, v_n$. Conversely, suppose that $v_1, v_2, \dots, v_n$ are linearly dependent. Then we could find rational numbers $c_1, c_2, \dots, c_n$, not all zero, so that

$$\sum c_i v_i = 0.$$

Separating into positive and negative parts, $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ and putting the negative part on the other side, we would have

$$\sum a_i v_i = \sum b_i v_i,$$

for some positive rational numbers $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$. Multiplying through by a highly divisible positive integer, we could clear denominators, so that $a_1, a_2, \dots, a_n$ and $b_1, b_2, \dots, b_n$ are integers. But then unique factorisation fails.

8. Let k be a field and let S be the infinite polynomial ring

$$k[x_1, x_2, \dots].$$

Let I be the ideal generated by $x_1x_2 = x_3x_4x_5$ and $x_4x_5 = x_6x_7x_8$, $x_7x_8 = x_9x_{10}x_{11}$ and so on. Let R be the ring S/I. It is not hard to show that $x_1, x_2, \dots$ are irreducible and that every element is a product of irreducibles.

Consider $a = x_1x_2 \in R$. Then x_1 and x_2 are irreducible and so a is a product of irreducibles. But $x_1x_2 = x_3x_4x_5$, so that a is also a product of x_3, x_4 and x_5. As $x_4x_5 = x_6x_7x_8$ we can keep going and the factorisation algorithm does not terminate starting with a.