1. We are told that $I$ is an ideal. Suppose that $J$ is any ideal of $R$, not equal to the whole of $R$. I claim that $J \subset I$. Suppose not. Then 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 $J = R$, a contradiction. It follows easily that $I$ is the unique maximal ideal.

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

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

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 

$$\phi: \mathbb{Z} \rightarrow \mathbb{Q},$$

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. (a) $a \mid b$ if and only if $b = ac$, for some $c \in R$. Suppose that $(b) \subset \langle a \rangle$. Then $b \in \langle a \rangle$, so that $b = ac$ for some $c \in R$. Now suppose that $b = ac$. Pick $r \in \langle b \rangle$. Then $r = qb$, for some $q \in R$. But then $r = q b = (qc)a$. Thus $r \in \langle a \rangle$ and so $\langle b \rangle \subset \langle a \rangle$.

(b) Immediate from (a), as two subsets $A$ and $B$ are equal if and only if $A \subset B$ and $B \subset A$.

(c) Clear, as $R = \langle 1 \rangle$ and an element $a$ of $R$ is an associate of $1$ if and only if it is a unit.

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. 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
\[
N(\alpha) = a^2 - b^2d.
\]
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 \( \alpha \), is by definition \( a - b\sqrt{d} \). Note that in the case \( d < 0 \), in fact \( \bar{\alpha} \) is precisely the complex conjugate of \( \alpha \). The key property of the norm, which may be checked easily, is that it is multiplicative. 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
\[
N(\gamma) = (aa' - bb'd)^2 + d(a'b - ab')^2
= (aa')^2 + (bb')^2d^2 + d(a'b)^2 + d(ab'0^2).
\]
On the other hand
\[
N(\alpha)N(\beta) = (a^2 + b^2d)((a')^2 + (b')^2d)
= (aa')^2 + (bb')^2d^2 + d(a'b)^2 + d(ab'0^2).
= N(\gamma).
\]
We first use this to determine the units. Note that if \( \alpha \) is a unit, then there is an element \( \beta \) 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 \( \alpha \) is \( \pm 1 \), then \( \mp \bar{\alpha} \) is the inverse of \( \alpha \). It follows that the units are precisely those elements whose norm is \( \pm 1 \).
(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 \( \alpha \) and \( \beta \) are not units. Then
\[
4 = N(2) = N(\alpha)N(\beta).
\]
As $\alpha$ and $\beta$ 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 $\alpha$ and $\beta$ 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.

6. 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.

7. First thin out the sequence $v_1, v_2, \ldots, v_n$ 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 $v_1, v_2, \ldots, v_n$ 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
different 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 $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are positive integers. Subtracting one side from the other, exhibits a linear dependence between $v_1, v_2, \ldots, v_n$. Conversely, suppose that $v_1, v_2, \ldots, v_n$ are linearly dependent. Then we could find rational numbers $c_1, c_2, \ldots, c_n$, not all zero, so that

$$\sum c_i v_i = 0.$$ 

Separating into positive and negative parts, $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ 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 $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$. Multiplying through by a highly divisible positive integer, we could clear
denominators, so that $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ are integers. But then unique factorisation fails.

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

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

Let $I$ be the ideal generated by $x_1 x_2 = x_3 x_4 x_5$ and $x_4 x_5 = x_6 x_7 x_8$, $x_7 x_8 = x_9 x_{10} x_{11}$ and so on. Let $R$ be the ring $S/I$. It is not hard to show that $x_1, x_2, \ldots$ are irreducible and that every element is a product of irreducibles.

Consider $a = x_1 x_2 \in R$. Then $x_1$ and $x_2$ are irreducible and so $a$
is a product of irreducibles. But $x_1 x_2 = x_3 x_4 x_5$, so that $a$ is also a product of $x_3, x_4$ and $x_5$. As $x_4 x_5 = x_6 x_7 x_8$ we can keep going and the factorisation algorithm does not terminate starting with $a$. 