MODEL ANSWERS TO HWK #9

1. It is proved in example 18.12 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, 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

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

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 $9 = 3 \times 3$.

2. (i) This set is clearly non-empty, and if a, b, c and d are integers then

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

so that R is closed under addition, and

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2},$$

so that it is closed under multiplication as well. Thus R is a subring of the real numbers.

(ii) Note that if a, b, c and d are divisible by 5 then $a+b$ and $c+d$ are divisible by 5, so that M is closed under addition, and it is easy to see that it is closed under inverses. Similarly if a and b are divisible by 5 then $ac+2bd$ and $ad+bc$ are divisible by 5 as well and so M is an ideal.

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 question 1.

It remains to prove that M is maximal. Given two integers a and b, consider $a^2 - 2b^2$. 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 $3 = -2 \mod 5$ we get 0, 3 and 2. If we take the sum of one number from the first list and one number from the second, the only way to get a number congruent to zero modulo 5, is to pick zero from both. The rest follows as in example 18.12.

3. 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 18.12.

4. 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.

5. (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.
6. (i) $a|b$ if and only if $b = ac$, for some $c \in R$. Suppose that $\langle b \rangle \subset \langle a \rangle$. 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 $r = qb = (qc)a$. 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.
7. 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.
8. As d' divides a and b, by the universal property of d, $d'|d$. By symmetry d divides d'. But then d and d' are associates.
9. It is convenient to introduce the norm, $N(\alpha)$, of any element α 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. 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

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

On the other hand

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

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 $a^2 - b^2 d = \pm 1$. 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.

(i) 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 mutatis mutandis, with 2 replacing 3. The crucial observation is that one cannot solve

$$a^2 + 5b^2 = 3.$$

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.

(ii) 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 gives rise to a strictly decreasing chain of natural numbers. Thus the set of principal ideals satisfies the ACC as the set of natural numbers satisfies the DCC.

(iii) By (i),

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

are two different factorisations of 6 into irreducibles.

10. (i) As R is a UFD, we may factor a and b as

$$a = up_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \qquad \text{and} \qquad b = vp_1^{n_1} p_2^{n_2} \cdots p_k^{n_k},$$

where $p_1, p_2, \dots, p_k$ are primes, $m_1, m_2, \dots, m_k$ and $n_1, n_2, \dots, n_k$ are natural numbers, possibly zero, and u and v are units. Define

$$m = p_1^{o_1} p_2^{o_2} \cdots p_k^{o_k}$$

where o_i is the maximum of m_i and n_i. It follows easily that $a|m$ and $b|m$.

Now suppose that $a|m'$ and $b|m'$. Then, possibly enlarging our list of primes, we may assume that

$$m' = wp_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

where w is a unit and $r_1, r_2, \dots, r_k$ are positive integers. As $a|m'$, $r_i \geq m_i$. Similarly as $b|m'$, $r_i \geq n_i$. It follows that $r_i \geq o_i = \max(m_i, n_i)$. Thus m is indeed an lcm of a and b. Uniqueness of lcms' up to associates, follows as in the proof of uniqueness of gcd's.

(ii) It suffices to prove this result for one choice of gcd d and one choice of lcm m. Pick d as in class (that is, take the minimum exponent) and take m as above (that is, the maximum exponent). In this case I claim that $dm = ab$. It suffices to check this prime by prime, in which case this becomes the simple rule,

$$m + n = \max(m, n) + \min(m, n)$$

where m and n are integers.

11. Same definition as for rings.

12. I claim that S has unique factorisation if and only if $v_1, v_2, \dots, v_n$ are independent as vectors in $\mathbb{Q}^2$. 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, $a_1, a_2, \ldots, a_n$ 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.