Homework #9 Solutions

Handout, #1 As suggested, we induct on m. When $m = 1$ we must prove the following statement: if $p_1, q_1, \ldots, q_n \in D$ ($n \in \mathbb{Z}^+$) are primes and $p_1 = q_1 q_2 \cdots q_n$ then $n = 1$. So, suppose we have the stated hypotheses and assume that $n \geq 2$. Since p_1 is prime and divides $q_1 \cdots q_n$ it divides q_1(without loss of generality). So $q_1 = ap_1$ for some $a \in D$. But then the irreducibility of q_1 implies that a is a unit (since p_1 is not). Therefore we have

$$\begin{aligned} p_1 &= (ap_1)q_2 \cdots q_n \\ &= p_1 a q_2 \cdots q_n. \end{aligned}$$

As we are working in a domain we can cancel p_1 from both sides to obtain $1 = aq_2 \cdots q_n$, implying that q_2 is a unit. As q_2 is prime this is a contradiction and we conclude therefore that our assumption that $n \geq 2$ is false. Thus, $n = 1$ and $p_1 = q_1$.

We now prove the induction step. Let $m \in \mathbb{Z}^+$ be at least 2 and assume that the statement of the problem is true for $m - 1$ and any $n \in \mathbb{Z}^+$. Let $p_1, \ldots, p_m, q_1, \ldots, q_n \in D$ ($n \in \mathbb{Z}^+$) be primes with $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$. Since p_m is prime and divides $q_1 \cdots q_n$ it divides q_n (without loss of generality). Since p_m and q_n are both primes (and hence irreducible) we may argue as above and conclude that p_m and q_n are associate. Writing $q_n = ap_m$ for some unit $a \in D$ we have

$$\begin{aligned} p_1 \cdots p_m &= q_1 q_2 \cdots q_{n-1}(ap_m) \\ &= (aq_1)q_2 \cdots q_{n-1} p_m. \end{aligned}$$

Since D is a domain we can cancel p_m to obtain $p_1 \cdots p_{m-1} = (aq_1)q_2 \cdots q_{n-1}$. Since aq_1 is also prime, the induction hypothesis implies that $m - 1 = n - 1$ and (after reordering) p_1 is associate to aq_1 and p_i is associate to q_i for $i = 2, \ldots, m - 1$. But this means that $m = n$ and p_i is associate to q_i for every i. That is, the statement of the exercise is true for $m \geq 2$ if it is true for $m - 1$.

Finally, mathematical induction allows us to conclude that the statement of the exercise holds for all $m\imath n\mathbb{Z}^+$.

Handout, #2 a. We use the ideal test. First, $I \neq \emptyset$ since $0 \in I_1 \subset I$. Let $a, b \in I$ and $r \in R$. Then there are $i, j \in \mathbb{Z}^+$ so that $a \in I_i$ and $b \in I_j$. Without loss of generality we can assume that $i \leq j$. Then $I_i \subset I_j$ so that $a \in I_j$. Since I_j is an ideal, $a - b \in I_j \subset I$ and $ra \in I_j \subset I$. Since $a, b \in I$ and $r \in R$ were arbitrary, this proves that I is an ideal.
b. If R has an identity and each I_j is proper then $1 \notin I_j$ for *every* $j \in \mathbb{Z}^+$. It follows that $1 \not{\imath}tI$ and therefore that $I \neq R$, i.e. I is a proper ideal.

p 335, #38 The ideals

$$I_n = \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n\text{times}} \oplus 0 \oplus 0 \oplus \cdots$$

work.

p 340, #24 We start by noticing $13 = 3^2 + 2^2 = (3+2i)(3-2i)$. Since $N(3+2i) = N(3-2i) = 13$ is prime, both $3+2i$ and $3-2i$ are irreducible in $\mathbb{Z}[i]$, and so we have found the desired factorization.

Now we note that
$$\frac{5+i}{1+i} = \frac{(5+i)(1-i)}{(1+i)(1-i)} = \frac{6-4i}{2} = 3-2i$$
so that $5+i = (1+i)(3-2i)$. We have already seen that $3-2i$ is irreducible and $1+i$ is, too, since $N(1+i) = 2$. So, we're finished.

p 347, #6 The given set of vectors is linearly dependent over *any* field since
$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} - 2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

p 348, #8 If $\{v_1, v_2, \ldots, v_n\}$ is linearly dependent in a vector space V over F then there exist $a_1, a_2, \ldots, a_n \in F$, not all zero, so that $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$. By reordering we can assume that $a_1 \neq 0$. Then we have $a_1v_1 = -a_2v_2 - \cdots - a_nv_n$ and multiplying both sides by a_1^{-1} yields $v_1 = (-a_1^{-1}a_2)v_2 + \cdots + (-a_1^{-1}a_n)v_n$, proving that v_1 is a linear combination of $v_2, v_3, \ldots, v_n$.

p 348, #16 We see that
$$\begin{aligned} V &= \left\{ \begin{pmatrix} a & b \\ b & c \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{Q} \right\} \\ &= \left\{ a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{Q} \right\} \\ &= \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \end{aligned}$$
which proves that V is a vector space. We claim that

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$
is a basis for V. According to what we've already done, it suffices to show that this set is linearly independent. Suppose that $a, b, c \in \mathbb{Q}$ satsify
$$a\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + c\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Then, after adding the matrices on the left, we have

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

which implies $a = b = c = 0$. This proves that the three matrices in question are linearly independent and completes the exercise.

p 348, #18 We have

$$\begin{aligned} P &= \{(a, b, c) \mid a, b, c \in \mathbb{R}, a = 2b + 3c\} \\ &= \{(2b + 3c, b, c) \mid b, c \in \mathbb{R}\} \\ &= \{b(2, 1, 0) + c(3, 0, 1) \mid b, c \in \mathbb{R}\} \\ &= \langle (2, 1, 0), (3, 0, 1) \rangle \end{aligned}$$

which proves that P is a subspace of $\mathbb{R}^3$. To prove that the set $\{(2, 1, 0), (3, 0, 1)\}$ is a basis for P it therefore suffices to prove that this set is linearly independent over $\mathbb{R}$. So let $b, c \in \mathbb{R}$ and suppose

$$b(2, 1, 0) + c(3, 0, 1) = (0, 0, 0).$$

Then

$$(2b + 3c, b, c) = (0, 0, 0)$$

which implies $b = c = 0$ and proves that the vectors in question are linearly independent.

p 349, #24 We first deal with $U \cap W$. This set is nonempty since $0 \in U$ and $0 \in W$ implies $0 \in U \cap W$. Given $u, v \in U \cap W$, $u + v \in U$ and $u + v \in W$ since both U and W are subspaces of V. Therefore $u + v \in U \cap W$. Furthermore, if $a \in F$ then $au \in U$ and $au \in W$, again because both U and W are subspaces of V. It follows from the subspace test mentioned in class that $U \cap W$ is a subspace of V.

We now turn to $U + W$. As above, this set is nonempty since $0 \in U$ and $0 \in W$ implies $0 = 0 + 0 \in U + W$. Let $x, y \in U + W$. Then there exist $u_1, u_2 \in U$ and $w_1, w_2 \in W$ so that $x = u_1 + w_1$ and $y = u_2 + w_2$. Thus

$$x + y = (u_1 + w_1) + (u_2 + w_2) = (u_1 + u_2) + (w_1 + w_2) \in U + W$$

since the fact that U and W are subspaces implies $u_1 + u_2 \in U$ and $w_1 + w_2 \in W$. Moreover, if $a \in F$ then

$$ax = a(u_1 + w_1) = au_1 + aw_1 \in U + W$$

since, again, $au_1 \in U$ and $aw_1 \in W$. As above, this proves that $U + W$ is a subspace of V.