Homework 7 Solutions

1. (a) Since I, J are ideals of R, they are (additive) subgroups of R, so $I \cap J$ is a subgroup of R.

   Next let $r \in R$ and $a \in I \cap J$. Then $ra \in RI \subset I$ and $ra \in RJ \subset J$, so $ra \in I \cap J$. Since $r \in R$ is arbitrary, we have $R(I \cap J) \subset I \cap J$.

   Therefore $I \cap J$ is an ideal of R.

   (b) Let $c_1, c_2 \in I + J$. By definition, $c_1 = a_1 + b_1$ and $c_2 = a_2 + b_2$ for some $a_1, a_2 \in I$ and $b_1, b_2 \in J$. Then

   $$c_1 + c_2 = a_1 + b_1 + a_2 + b_2 = (a_1 + a_2) + (b_1 + b_2) \in I + J.$$

   Next let $r \in R$ and $c \in I + J$. By definition, $c = a + b$ for some $a \in I, b \in J$. Now $rc = ra + rb$ satisfies $ra \in rI \subset I$ and $rb \in rJ \subset J$ so $rc \in I + J$.

   Therefore $I + J$ is an ideal of R.

   (c) Let $c, c' \in IJ$. By definition, $c_1 = \sum a_i b_i$ and $c' = \sum a_i' b_i'$ for some $a_i, a_i' \in I$ and $b_i, b_i' \in J$. Then

   $$c + c' = \sum a_i b_i + \sum a_i' b_i' \in IJ.$$

   Next let $r \in R$ and $c \in IJ$. By definition, $c = \sum a_i b_i$ for some $a_i \in I$ and $b_i \in J$. Then

   $$rc = r \sum a_i b_i = \sum (ra_i) b_i.$$

   Since $ra_i \in rI \subset I$, we see that $rc \in IJ$.

   Therefore IJ is an ideal of R.

2. Suppose that $I \subset J$. Then $a \in I \subset J = (b)$ so $a = cb$ for some $c \in R$. Therefore, b divides a.
   Conversely, suppose that b divides a. This means that $a = cb$ for some $c \in R$. So $a \in I \subset J = (b)$. For any $r \in R$, $ra \in R(b) = (b)$ so $(a) = Ra \subset (b)$.

   The ring homomorphism $f : \mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ has kernel (12). By the correspondence theorem, the ideals of $\mathbb{Z}/12\mathbb{Z}$ correspond to the ideals of $\mathbb{Z}$ that contain (12). By our work above, the ideals of $\mathbb{Z}$ containing (12) must be $(1),(2),(3),(4),(6),(12)$. Under the correspondence, the ideals of $\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ are therefore given by $(\bar{1}),(\bar{2}),(\bar{3}),(\bar{4}),(\bar{6}),(\bar{0})$.

3. **Finding the kernel.** After a linear change of variables, we can instead work with the ring homomorphism

$$\begin{aligned} \psi : \mathbb{C}[x,y] &\to \mathbb{C}[t] \\ x &\mapsto t \\ y &\mapsto t^3 \end{aligned}$$

We claim that $\ker \psi = (x^3 - y)$. (This implies that $\ker \phi = ((x+1)^3 - y - 1)$.) The inclusion $\ker \psi \supset (x^3 - y)$ is clear. For the reverse inclusion, let $f \in \ker \psi$, so that $f(t,t^3) = 0$.

Consider $f(x,y)$ and $x^3 - y$ as polynomials in y. Since $-y + x^3$ has unit leading coefficient -1, we can divide $f(x,y)$ by $-y + x^3$, giving us:

$$f(x,y) = q(x,y)(-y + x^3) + r(x,y)$$

for some $q(x,y), r(x,y) \in \mathbb{C}[x,y]$ with $\deg_y r(x,y) < \deg_y(-y + x^3) = 1$, so $r(x,y) = r(x)$. Upon evaluation our equality becomes

$$0 = f(t,t^3) = q(t,t^3) \cdot 0 + r(t)$$

so $r(t) = 0$ so $r(x) = 0$. Therefore $f \in (x^3 - y)$ so $\ker \psi \subset (x^3 - y)$.

Showing any ideal containg $\ker \phi$ is generated by two elements.

Again it suffices to show that any ideal containg $\ker \psi$ is generated by two elements. Let I be an ideal of $\mathbb{C}[x,y]$ containing $\ker \psi$. By the correspondence theorem, its image $\psi(I)$ is an ideal of $\mathbb{C}[t]$. Since any ideal of $\mathbb{C}[t]$ is principal, $\psi(I) = (f(t))$ for some $f(t) \in \mathbb{C}[t]$.

We claim that $I = (f(x), x^3 - y)$.

$\underline{I \supset (f(x), x^3 - y)}$. By the correspondence theorem, $I = \psi^{-1}((f(t)))$ and since $f(x)$ is a preimage of $f(t) \in (f(t))$ and $x^3 - y$ is a preimage of $0 \in (f(t))$, the inclusion $I \supset (f(x), x^3 - y)$ holds.

$\underline{I \subset (f(x), x^3 - y)}$. Let $g(x, y) \in I$ be given. Since

$$g(t, t^3) = \psi(g(x, y)) \in \psi(I) = (f(t)),$$

we can write $g(t, t^3) = h(t)f(t)$ for some $h(t) \in \mathbb{C}[t]$. This implies that

$$g(x, y) - h(x)f(x) \in \ker \psi = (x^3 - y)$$

and so

$$g(x, y) \in (x^3 - y) + h(x)f(x) \subset (x^3 - y, f(x)).$$

Since $g \in I$ is arbitrary, we deduce that $I \subset (f(x), x^3 - y)$.

4. Any ideal of $\mathbb{Z}[i]$ contains 0, which is an integer.

5. (a)

   (b) View the ideal $(2+i)$ as a lattice in $\mathbb{Z}[i]$ and note that the quotient has 5 elements. As a result, $\frac{\mathbb{Z}[i]}{(2+i)}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ as a group. Since $\mathbb{Z}/5\mathbb{Z}$ is a cyclic group, the multiplication structure on it is uniquely determined. Therefore any ring with 5 elements must be isomorphic to $\mathbb{Z}/5\mathbb{Z}$, so $\frac{\mathbb{Z}[i]}{(2+i)}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ as rings.

6. (a) We claim that $\ker f = (x, y)$. Clearly $\ker f \supset (x, y)$ since $f(x) = f(y) = 0$. Conversely let

$$g(x, y) = \sum_{i,j \geq 0} a_{ij} x^i y^j$$

   be an element in $\ker f$. This means that $f(g) = g(0, 0) = a_{00} = 0$. Therefore

$$g(x, y) = \left(\sum_{i>0, j=0} a_{ij} x^{i-1} y^j \right) x + \left(\sum_{i \geq 0, j>0} a_{ij} x^i y^{j-1} \right) y \subset (x, y).$$

   This shows that $\ker f \subset (x, y)$.

   (b) We claim that $\ker f = (x^2 - 4x + 5)$. Since $\mathbb{R}[x]$ is a ring with division algorithm, its ideals are all principal, so $\ker f = (g)$ for some $g \in \mathbb{R}[x]$. Clearly g is not constant or linear since $2 + i$ is not in $\mathbb{R}$. Since $x^2 - 4x + 5$ is the polynomial of smallest degree which has $2 + i$ as a root, we can take g to be $x^2 - 4x + 5$.

   Here's another way to say the above. To show that $\ker f = (x^2 - 4x + 5)$, note that the inclusion $\ker f \supset (x^2 - 4x + 5)$ is clear. For the converse, let $g(x) \in \ker f$, so we get $g(2+i) = 0$.

Now by the division algorithm,

$$g(x) = q(x)(x^2 - 4x + 5) + r(x)$$

for some $q(x), r(x) \in \mathbb{R}[x]$ with $\deg r(x) < 2$. Plugging in $2+i$ to this equality gives

$$0 = g(2+i) = q(2+i) \cdot 0 + r(2+i)$$

Since $2+i$ is not in $\mathbb{R}$ and $r(x)$ is either a constant or a linear polynomial over $\mathbb{R}$, we must have $r(x) = 0$. Therefore,

$$g(x) = q(x)(x^2 - 4x + 5) \in (x^2 - 4x + 5).$$