Comments on Problem Set 4

1. Chapter 12, Exc. 2.8 (division with remainder in $\mathbb{Z}[i]$)

It is simplest to do the division in $\mathbb{C}$, then take a nearby Gauss integer. For example,

$$
\frac{4 + 36i}{5 + i} = \frac{(4 + 36i)(5 - i)}{26} = \frac{56 + 176i}{26} = (2 + \frac{4}{26}) + (7 - \frac{6}{26})i
$$

So $4 + 36i = (2 + 7i)(5 + i) + r$, where the remainder $r$ is $4 + 36i - (2 + 7i)(5 + i) = 1 + 4i$.

2. Chapter 11, Exc. 8.1 (principal ideals in $\mathbb{Z}[x]$ that are maximal)

The answer is that no maximal ideal of $\mathbb{Z}[x]$ is a principal ideal. You are expected to prove this, of course.

3. Chapter 11, Exc. 9.12 (polynomials without common zeros)

I assigned this so that you would learn that the Nullstellensatz is useful. To write 1 as a combination of $f_1, f_2, f_3$, one can use repeated division with remainder, as in the Euclidean algorithm.

For example, since $f_1$ is monic in $t$, one can use it to divide $f_3$. The remainder is $g = f_3 - tf_1 = 4tx^2 + 2t + 1$. Then one can divide $g$ by $f_2$, obtaining remainder $h = g - xf_2 = 2t + 4x + 1$. We replace $f_3$ by $\frac{1}{2}h$, which is linear and monic in $t$. Then one can use $h$ to divide $f_1$ and $f_2$, etc.

However, substituting back at the end is a big pain. Sorry.

4. Chapter 11, Exc. 6.8 (Chinese Remainder Theorem)

(a) For any ideals $I$ and $J$, it is true that $IJ \subset I$ and $IJ \subset J$. So $IJ \subset I \cap J$. Suppose that $I + J = R$. Then we can write $1 = r + s$ with $r \in I$ and $s \in J$. If $x \in I \cap J$, $rx$ is in $IJ$ and $sx$ is in $JI = IJ$. Therefore $x = xa + xb$ is in $IJ$. So $I \cap J \subset IJ$.

(b) Writing $x = rx + sx$, where $r + s = 1$, $r \in I$ and $s \in J$, does the trick.

(c) Let $R_1 = R/I$ and $R_2 = R/J$. The kernel of the map $\pi = (\pi_1, \pi_2) : R \to R_1 \times R_2$ that sends an element $x$ to the pair $(x_1, x_2)$ of its residues is $I \cap J$, which is equal to $IJ = 0$. Therefore $\pi$ is injective. Let $(\overline{a}, \overline{b})$ be an element of $R_1 \times R_2$, and let $a, b$ be elements that map to $\overline{a}, \overline{b}$. With $1 = r + s$ as above, $(1, 1) = \pi(1) = \pi(s) + \pi(r) = (\pi_1(s), 0) + (0, \pi_2(r))$. So $\pi(s) = (1, 0)$ and $\pi(r) = (0, 1)$. Then $\pi(sa + rb) = (\pi_1(a), 0) + (0, \pi_2(b)) = (\overline{a}, \overline{b})$.

(d) In $R_1 \times R_2$, the idempotents that describe the product decomposition are $(1, 0)$ and $(0, 1)$. The inverse images of these elements in $R$ are the idempotents $r$ and $s$. 

1
5. Chapter 11, Exc. M.3 (maximal ideals in a ring of sequences)

The map that sends a sequence \( a = (a_1, a_2, \ldots) \) to \( a_i \) is a homomorphism \( R \rightarrow \mathbb{R} \). Its kernel \( \mathfrak{m}_i \), is the set of sequences \( a \) such that \( a_i = 0 \). It is a maximal ideal. The only other maximal ideal is \( \mathfrak{M} \), the kernel of the homomorphism to \( \mathbb{R} \) that sends a sequence \( a \) to its limit.

Let \( M \) be any maximal ideal. If \( M \neq \mathfrak{m}_i \), then because \( M \) is maximal, \( M \not\subset \mathfrak{m}_i \). So there is a sequence \( a \in M \) with \( a_i \neq 0 \). Let \( e_i \) be the sequence that is identically zero except for a 1 in position \( i \). Then the sequence \( e_ia \), which is in the ideal \( M \), is zero except for position \( i \), its entry in that position is \( a_i \), and it is an element of \( M \). Since we can multiply elements of \( M \) by \( a_i^{-1} \), \( e_i \) is an element of \( M \).

Using the elements \( e_i \), we can construct any element of \( R \) whose limit is zero. Thus \( M \) contains the set of such sequences. They form the ideal \( \mathfrak{M} \). So \( \mathfrak{m}_1, \mathfrak{m}_2, \ldots \) and \( \mathfrak{M} \) are the only maximal ideals.

6. Chapter 12, Exc. M.4. (ring generated by \( \sin x \) and \( \cos x \))

There are various ways to do this, but it seems simplest to begin by allowing complex coefficients, to study the ring \( \mathbb{C}[\cos t, \sin t] \).

Let \( S \) denote the ring \( \mathbb{C}[x, y]/(x^2 + y^2 - 1) \). When we change variables in \( S \) to \( u = x + iy, \ v = x - iy \), the equation \( x^2 + y^2 - 1 \) becomes \( uv = 1 \), or \( v = u^{-1} \). The ring \( S \) is isomorphic to the Laurent Polynomial Ring \( \mathbb{C}[u, u^{-1}] \). We identify \( S \) with that ring. The corresponding change of variables in \( \mathbb{C}[\cos t, \sin t] \) is \( e^{it} = \cos t + i \sin t, \ e^{-it} = \cos t - i \sin t \).

So \( \mathbb{C}[\cos t, \sin t] = \mathbb{C}[e^{it}, e^{-it}] \).

You will be able to check that the substitution \( u = e^{it} \) defines an isomorphism \( S = \mathbb{C}[u, u^{-1}] \rightarrow \mathbb{C}[e^{it}, e^{-it}] \). Therefore the ideal of complex polynomial relations among \( \cos t, \sin t \) is generated by \( e^{it}e^{-it} - 1 \), which is equal to \( \cos^2 t + \sin^2 t - 1 \). Then the same is true for the real polynomial relations. This proves (a).

In \( S \), every nonzero element of \( S \) can be written uniquely in the form \( u^k f(u) \), where \( k \) can be positive or negative, and \( f(u) \) is a polynomial in \( u \) whose constant coefficient isn't zero. This makes it easy to prove that \( S \) is a principal ideal domain and therefore a unique factorization domain, hence (c) is true.

(d) We write an element of \( S \) in the form \( s = u^k f(u) \), as above. If \( s \) is a unit, its inverse also has that form, say \( s^{-1} = u^\ell g(u) \), so that \( u^{k+\ell} f(u)g(u) = 1 \). Since the polynomials \( f \) and \( g \) aren't divisible by \( u \), neither is \( fg \). Therefore \( fg = 1 \) and \( k + \ell = 0 \). So \( f \) and \( g \) are scalars. The units of \( S \) are \( cu^k \) with \( c \in \mathbb{C} \) not zero, and \( k \in \mathbb{Z} \).

The units in \( R = \mathbb{R}[x, y]/(f) \) are units in \( S \) too. Since \( u^k \) isn't in \( R \) when \( k \neq 0 \), the units of \( R \) are the nonzero real scalars.

(b) In \( R \), we have the equation \( x^2 = (y + 1)(y - 1) \). When we show that \( x \) is an irreducible element of \( R \) that doesn't divide \( y + 1 \), it will follow that the two sides of the equation are inequivalent factorizations.
In $S$, $x = \frac{1}{2}(u + u^{-1}) = \frac{1}{2}u^{-1}(u^2 + 1) = \frac{1}{2}u^{-1}(u+i)(u-i)$, and $y+1 = \frac{1}{2}(u - u^{-1})+1 = \frac{1}{2}u^{-1}(u^2 + u + 1)$. The term $\frac{1}{2}u^{-1}$ is a unit that can be ignored. Since $u+1$ doesn’t divide $u^2 + u + 1$, $x$ doesn’t divide $y+1$ in $S$ or in $R$. The two factors $u+i, u-i$ of $x$ are irreducible elements of $\mathbb{C}[u, u^{-1}]$. They can’t be made real by multiplying by a unit. So $x$ is irreducible in $R$. 