MATH 113 Assignment 8 Partial solutions

1. We know from class that if R is an integral domain, then the polynomial ring $R[x]$ is also. Since $\mathbb{Q}$ is an integral domain, so is $\mathbb{Q}[\sqrt{2}]$ and $(\mathbb{Q}[\sqrt{2}])[\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ by applying that general result twice.

The other way is to try to explicitly show that a product of two nonzero elements in the ring cannot multiply to zero. But no one succeeded doing it this way.

2. Recall that Kerϕ is an ideal of F (many forgot to say this explicitly). But since F is a field, it has only the zero ideal $\langle 0\rangle$ and F as ideals. These correspond to ϕ being one to one, and to ϕ being the zero homomorphism, respectively.

3. Let $f(x) = a_n x^n + \cdots$ have degree n. If $n = 1$ we are clearly done. Proceed by induction. Suppose that the desired conclusion holds when $n = k > 1$. Now consider the case where $f(x)$ has degree $n = k + 1$. Suppose f has infinitely many roots, let a one of them. By the factor theorem $x - a$ divides $f(x)$ giving, say $g(x)$. Notice that $g(x)$ has degree $k = k + 1 - 1$ but still has infinitely many roots, contradicting the induction hypothesis. Thus the result follows.

4. Almost everyone found that $\mathrm{irr}(\sqrt{\frac{1}{3}} + \sqrt{7}, \mathbb{Q}) = x^4 - \frac{2}{3}x^2 - \frac{62}{9}$ (note that by definition, we normalize to make the answer a *monic* polynomial). We know from class that this polynomial is irreducible over $\mathbb{Q}$ if and only if $9x^4 - 6x^2 - 62$ is irreducible over $\mathbb{Z}$. Now apply Eisenstein's criterion with $p = 2$ to conclude that the latter assertion holds.

There is every another way to prove irreducibility, that might prove useful in the future (Eisentsein works better and faster in this particular case). Notice that the quartic polynomial that we are dealing with can be *explicitly solved* by setting $z = x^2$ and using the quadratic formula. Thus you can determine explicitly the roots and write the polynomial as $(x - a)(x - b)(x - c)(x - d)$. Now, if the polynomial were reducible over the rationals, it must have a linear or quadratic polynomial factor with rational coefficients. Moreover, that factor must be a product of some of the linear polynomials in the factorization. Now verify that isn't the case!

5. Since $2 = (i - 1)(i + 1)$ we get (a). For (b), let us run through the thought process: we know that each coset is of the form $a+bi+\langle 1+i\rangle$ for some $a, b \in \mathbb{Z}$. The idea is that to identify the different cosets, we would like to write down a *canonical* or "distinguished" coset representative $a + bi$ for each coset.

As it turns out, this isn't so bad. By part (a), since $2 \in J = \langle i + 1\rangle$, so is $2i$. Now, given a coset representative $a + bi$ for some coset, we can get other coset representatives by adding and subtracting 2 and $2i$. Thus, we can always convert a "random" coset representative to one of the following four possibilities $0 + 0i, 1 + 0i, 0 + 1i, 1 + 1i$. Now $0 + 0i$ and $1 + 1i$ both lie in J and correspond to the coset $0 + J$. In fact, 1 and i are in the same coset: since $i - 1 = (i + 1) - 2$ and $i + 1$ and 2 are in J. Thus we need only pick one or the other, say $1 + J$ is a *possible* coset. I say "possible" because we should check that $1 \notin J$.

We J is a principal ideal, and every element is of the form $(c+di)(1+i) = (c - d) + (c + d)i$. So if $1 \in J$ then there are integers c, d such that $c - d = 1$ and $c + d = 0$. It is easy to check this doesn't happen. Hence $1 \notin J$. Hence we have two cosets, which we can express as $0 + J$ and $1 + J$.

Thus $\mathbb{Z}[i]/J$ is a two element ring, and it is easy to see that it is isomorphic to $\mathbb{Z}_2$. This is part (c).