MATH 235 Assignment 7 Solutions

1.1: $x^2 - 3$ is quadratic and hence is irreducible over $\mathbb{Q}/\mathbb{R}$ iff it has no roots in the corresponding fields. But $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$ and since $\sqrt{3}$ lies in $\mathbb{R}$ but not $\mathbb{Q}$ we conclude $x^2 - 3$ is irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{R}[x]$.

1.2: As above, it suffices to check for roots of $x^2 + x - 2$ in the two corresponding fields. It is easy to see however that both 1 and -2 satisfy the equation over the rationals. Hence $\overline{1}$ and $\overline{-2}$ also satisfy the equation over $\mathbb{F}_3$ and $\mathbb{F}_7$. Hence the polynomial is not irreducible over either field.

2: Using the rational root test, we conclude that the only possible rational roots that $2x^4 + 4x^3 - 5x^2 - 5x + 2$ could possibly have lie in the set $\{\pm 1, \pm 2, \pm 1/2\}$. Checking these 6 values explicitly, we conclude that the only rational root is -1.

3: We would like to prove that the only ideals of $\mathbb{Z} \times \mathbb{Z}$ are the sets of the form $<(a,b)>= \{(a \cdot x, b \cdot y) : x, y \in \mathbb{Z}\}$ for any $a, b \in \mathbb{Z}$. It is easy to see that each of the above sets is in fact an ideal, because multiplication and addition are pointwise operations in this ring and $(a), (b)$ are both ideals of $\mathbb{Z}$. Suppose now that $I \lhd \mathbb{Z} \times \mathbb{Z}$ is some arbitrary ideal. Consider the 2 projection maps $\pi_j : I \to \mathbb{Z}$, $\pi_j((x_1, x_2)) = x_j$ for $j = 1, 2$. It is easy to see that the image $\pi_j(I)$ is necessarily an ideal of $\mathbb{Z}$, for example, $z \cdot \pi_1(x, y) = \pi_1(zx, 1y)$ and $(zx, 1y)$ lies in I if (x, y) does because I is an ideal. It follows that the image $\pi_1(I) = (a)$ and $\pi_2(I) = (b)$ for some $a, b \in \mathbb{Z}$. We claim that this implies $I =< (a, b) >$. Indeed, if $(x, y) \in I$, then $x \in (a)$ and $y \in (b)$, say $x = ar_1$ and $y = br_2$. Then $(x, y) = (a, b)(r_1, r_2)$ and so $(x, y) \in< (a, b) >$. Since $\exists\ z \in I$ st. $\pi_1(z) = a$, this implies $(1, 0) \cdot z = (a, 0) \in I$. Likewise $(0, b) \in I$ and hence the sum $(a, b) \in I$. This suffices to show $I =< (a, b) >$.

4.1: We need to check the ideal axioms on the set $I \cap J$. Assume $x, y \in I \cap J$ and $r \in R$ are arbitrary elements. First, it is clear that 0 lies in $I \cap J$ since it necessary lies in I and J as they are ideals. Second, $-x$ and $x + y$ lie in $I \cap J$ because x and y both lie in I and J by assumption and again, they are ideals so they must contain $-x$ and $x + y$. Finally $r \cdot x$ and $x \cdot r$ lies in $I \cap J$ for the same reason.

4.2: Again we argue similarly and check the ideal axioms on $I + J$ by using the fact that I and J are ideals. It is clear that 0 lies in $I + J$. If $x = i_1 + j_1$ and $y = i_2 + j_2$, then $-x = (-i_1) + (-j_1)$ and $x + y = (i_1 + i_2) + (j_1 + j_2)$ both lie in $I + J$. Finally $r \cdot x = (r \cdot i_1) + (r \cdot j_1)$ and $x \cdot r = (i_1 \cdot r) + (j_1 \cdot r)$ using the distributive law of rings, and so $I + J$ is also closed under multiplication by R.

4.3: By definition, $(a) + (b) = \{na + mb : n, m \in \mathbb{Z}\}$ is the set of all $\mathbb{Z}$ linear combinations of a and b. From work done earlier in the course, we know that all such combinations are necessarily divisible by $\mathrm{GCD}(a, b)$ and also that the $\mathrm{GCD}(a, b)$ can be written as such a linear combination. It follows that $(a) + (b) = (\mathrm{GCD}(a, b))$. Consider now the ideal $I = (a) \cap (b)$. If $x \in I$ then x is divisible by both a and b, and hence by their LCM. On the other hand the least common multiple lies in both (a) and (b) and hence in I. It follows that $I = (\mathrm{LCM}(a, b))$.

5: Let $I \lhd M_2(\mathbb{F})$ be a non-trivial (2-sided) ideal. We will show that I contains the identity matrix. Since I is non-trivial, in particular it contains a non-zero element m and let us say that we have

$$m := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Since m is non-trivial, one of the a_{ij}s must be non-zero. Without loss of generality we will assume a_{11} is non-zero (we can always multiply the matrix in such a way as to permute the rows and columns until we get a non-zero element in this position. Since I is an ideal, that matrix must also be in I). We can then do some simple matrix multiplication to show that

$$m' := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix}$$

must lie in I. Likewise the matrix

$$m'' := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a_{11} \end{pmatrix}$$

also lies in I. Hence the sum $m' + m''$ lies in I but this is clearly invertible as a_{11} is (because it is non-zero and $\mathbb{F}$ is a field). Hence I contains an invertible element and therefore contains the identity element since it is an ideal. Therefore I is the whole ring.

6.1: It is trivial to see that 0 and 1 are both in $\mathbb{Z}[\sqrt{3}]$. If $x = a + b\sqrt{3}$ and $y = c + d\sqrt{3}$ then $x + y = (a + c) + (b + d)\sqrt{3}$ and $xy = (ac + 3bd) + (ad + bc)\sqrt{3}$ both of which clearly lie in $\mathbb{Z}[\sqrt{3}]$.

6.2(a): Note that $\sqrt{3}$ lies in the set but $\sqrt{3} \times \sqrt{3} = 3$ does not. Hence the set is not an ideal.

6.2(b): Let $c + d\sqrt{3}$ be an arbitrary element of $\mathbb{Z}[\sqrt{3}]$ and let $2a + 2b\sqrt{3}$ be an arbitrary element of our set. Then their product is $2(ac + 3bd) + 2(ad + bc)\sqrt{3}$ which also lies in the set in question. Hence the set is closed under multiplication by $\mathbb{Z}[\sqrt{3}]$ and it is easy to show that it satisfies the other necessary properties of an ideal. Hence the set is an ideal and in fact it is easy to see that it is the ideal generated by 2.

6.2(c): Again it is obvious that the set satisfies the necessary properties except possibly closure under multiplication by $\mathbb{Z}[\sqrt{3}]$ so we check this. Let $c+d\sqrt{3}$ be an arbitrary element of $\mathbb{Z}[\sqrt{3}]$ and let $(2a+15b)+(5a+2b)\sqrt{3}$ be an arbitrary element of our set. Then their product is $(2ac+15bc+15ad+6bd)+(5ac+2bc+2ad+15bd)\sqrt{3} = (2(ac+3bd)+15(bc+ad))+(5(ac+3bd)+2(bc+ad))\sqrt{3}$. This is of the desired form so we conclude the set is an ideal. We claim that in fact it is the ideal $(2+5\sqrt{3})\mathbb{Z}[\sqrt{3}]$. It is easy to see that this set contains the ideal because it contains the generator (just set $a = 1, b = 0$). On the other hand, $(2+5\sqrt{3})(a+b\sqrt{3}) = 2a+15b+(5a+2b)\sqrt{3}$, which is the form of every element in our set.

7.1: This set is a subring. Indeed one can check directly that the product of two *upper triangular matrices* is again of the same form. Since the set also contains the 0 and identity matrix and is obviously closed under addition, we are done.

7.2: The set $\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \text{ in } \mathbb{C} \right\}$ is not a subring of $M_2(\mathbb{C})$ because it does not contain the identity matrix. One should note however that the set is in fact a ring, with the multiplicative identity element $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. This is an interesting example of when one ring is contained in another, but is not a subring because either the additive or multiplicative identity is different. Try to think of other examples where this could happen.

7.3: This set is a subring. The only non-trivial matter to check is that it is closed under multiplication. Indeed we have

$$\begin{pmatrix} a & b \\ 0 & \overline{a} \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & \overline{c} \end{pmatrix} = \begin{pmatrix} ac & ad + b\overline{c} \\ 0 & \overline{ac} \end{pmatrix}.$$

7.4: This is a subring for the same reasons as 7.1.

7.5: This is not a subring. Indeed it is not closed under multiplication. For example,

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} i & 1 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} i & 1-2i \\ 0 & -i \end{pmatrix}.$$