MAT235 Assignment 9 Solutions

1: As noted in the hint, we first consider the total number of squares in $\mathbb{F}^\times$, where $|\mathbb{F}| = q^n$ for some prime q and positive integer n. Clearly the set $S := \{x^2 | x \in \mathbb{F}^\times\}$ runs through all such square, we consider the cardinality of S.

If $x^2 = y^2$ then $(x-y)(x+y) = 0$ and so $x = \pm y$. If $q = 2$, then $\pm 1 = 1$ and so $x^2 = y^2$ iff $x = y$. It follows that $|S| = |\mathbb{F}^\times|$ when q=2 and so the statement in the problem is vacuous as there are no non-square elements.

Otherwise q is an odd prime and $-1 \neq 1$, so every element in S is a square of two distinct elements in $\mathbb{F}^\times$, hence $|S| = |\mathbb{F}^\times|/2$. Suppose now that a is a non-square. Then $a \cdot x$ runs through all elements of $\mathbb{F}^\times$ as x does and attains each value exactly once because $\mathbb{F}$ is a field. On the other hand, if x is a square, say $x = z^2$, then $a \cdot x$ could not be a square, for if it was then we would have

$$a \cdot z^2 = t^2 \Rightarrow a = (tz^{-1})^2$$

contradicting the fact that a is not a square. But since there are $|S| = |\mathbb{F}^\times|/2$ squares, there must also be the same number of non-squares. Hence by comparing cardinalities it follows by the bijective nature of the map that sends y to $a \cdot y$ that every non-square can be written as $a \cdot x$ for some square x. Hence if b is a non-square, $a \cdot b = a^2 \cdot x$ for some square x and therefore $a \cdot b$ must be a square.

5 (a): Suppose there was a ring homorphism φ between $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}$. Then $\varphi(\overline{1}) = 1$. Since we have a ring homomorphism, $\varphi(\overline{2}) = \varphi(\overline{1}) + \varphi(\overline{1}) = 2$ and likewise for 3 and 4. But we can continue this, since $\varphi(\overline{0}) = \varphi(\overline{4}) + \varphi(\overline{1}) = 4 + 1 = 5$ and $\varphi(\overline{1}) = \varphi(\overline{0}) + \varphi(\overline{1}) = 5 + 1 = 6 \neq 1$. Hence we have a contradiction, and so no such map exists.

5 (b): The exact same argument as above shows that any such ring homomorphism would have to send $\overline{1} \in \mathbb{Z}/5\mathbb{Z}$ to both $\overline{1}$ and $\overline{6} \in \mathbb{Z}/7\mathbb{Z}$. Since these two elements are distinct in the latter ring, we conclude no such homomorphism exists.

5 (c): Suppose they were isomorphic under $\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$. Then $\varphi(x) + \varphi(x) = \varphi(x + x) = \varphi((\overline{0}, \overline{0})) = \overline{0}$. But if φ was an isomorphism, this would imply every element in $\mathbb{Z}/4\mathbb{Z}$ satisfies $y + y = \overline{0}$ which is clearly false.

5 (d): There is an obvious homomorphism from $\mathbb{Z}/4\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$, namely the quotient map which merely sends and integer mod 4 to the same integer mod 2 (equivalently taking the quotient by the ideal $(\overline{2}) \lhd \mathbb{Z}/4\mathbb{Z}$, see proposition 22.0.10 in the notes). The map sending $\overline{0}$ to $(\overline{0}, \overline{0})$ and $\overline{1}$ to $(\overline{1}, \overline{1})$ is a ring homomorphism from $\mathbb{Z}/2\mathbb{Z}$ into $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Composing these two maps gives the desired ring homomorphism.

5 (e): Arguments like those in (a) and (b) show that no ring homomorphism exists from $\mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/4\mathbb{Z}$. It follows that no map can exist from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ to $\mathbb{Z}/4\mathbb{Z}$ because the restriction of the map to the subring $\{(\overline{0}, \overline{0}), (\overline{1}, \overline{1})\}$ would be a ring homomorphism with domain isomorphic to $\mathbb{Z}/2\mathbb{Z}$, contradicting the above.

6 (a): Recall from assignment 7 question (4) that the sum of two ideals is also an ideal. We use this to prove via induction that $(a_1, \ldots, a_n)$ is an ideal. If $n = 1$ then the result is trivial and the case $n = 2$ follows from the aforementioned question. Assume inductively we have proved the claim for $n = k$, and consider the ideal $(a_1, \ldots, a_{k+1})$. Let $I = (a_1, \ldots, a_k)$ which is an ideal by inductive assumption and it is easy to see that $(a_1, \ldots, a_{k+1}) = I + (a_{k+1})$ which is an ideal according to assignment 7 question (4).

6 (b)(i): Suppose $(2, x)$ was generated by $a \in \mathbb{Z}[x]$. Note that 1 is not in $(2, x)$, for if it were, then there would be $r_1, r_2 \in \mathbb{Z}[x]$ st. $1 = 2r_1 + x \cdot r_2$. But substituting $x = 0$ into the equation we see that 1 must be the product of 2 and the constant term of r_1, which is impossible since the coefficients of r_1 lies in $\mathbb{Z}$. It follows that a is not a unit. Since a generates $(2, x)$, there exists $y \in \mathbb{Z}[x]$ st. $ay = 2$ and so a must be ± 2 by above. But then $a \times p(x)$ for any $p(x) \in \mathbb{Z}[x]$ must be a polynomial with even coefficients, so $x \notin (a)$. This is a contradiction and therefore no such a exists. The fact that $\mathbb{Z}[x]$ is not a PID follows trivially.

6 (b)(ii): Consider the two maps $g : \mathbb{Z}[x] \to \mathbb{Z}$ and $h : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, where $g(p(x)) = p(0)$ and h is just that natural quotient map $h(y) = \overline{y}$. Let $f = h \circ g$. It is clear that the kernel of g are all polynomials who are zero at zero, ie. the ideal (x) and likewise the kernel of h is (2). It follows easily that the kernel of f contains $(2, x)$. On the other hand, if $p(x)$ lies in the kernel of f, then $p(0)$ must be divisible by 2, say $p(0) = 2m$. But then $p(x) - 2m$ has a zero at zero, and so is of the form $x \cdot r(x)$. Therefore $p(x) = 2m + x \cdot r(x)$, showing that $(2, x) \supseteq Ker(f)$. Thus the two sets are equal.

8: There are obviously no isomorphisms between $\mathbb{R}^4$ and either of the other 2 rings because $\mathbb{R}^4$ is a commutative ring while the other 2 are not, and it is a simple exercise to prove that commutativity of multiplication is preserved by isomorphisms. To show that the real quaternions and $M_2(R)$ are not isomorphic, observe that $\mathbb{H}$ is a division ring, so in particular all of its non-zero elements are units. On the other hand any matrix with determinant zero does not have an inverse and so could not possibly be in the image of a ring homomorphism from $\mathbb{H}$ because ring homomorphisms send units to units (make sure you understand why). Since there are non-zero real 2 by 2 matrices with zero determinant, this completes the proof.

10: We first show R is a subring of $M_3(\mathbb{F})$. Clearly both the 1 and 0 elements lie in R and it is obvious that R is closed under addition. It remains to show R is closed under multiplication. Indeed we have

$$\begin{pmatrix} a_{11} & a_{12} & a_{23} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ 0 & b_{22} & b_{23} \\ 0 & 0 & b_{33} \end{pmatrix}$$
$$= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} + a_{12}b_{22} & a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33} \\ 0 & a_{22}b_{22} & a_{22}b_{23} + a_{23}b_{33} \\ 0 & 0 & a_{33}b_{33} \end{pmatrix}.$$

Turning to the set I, we have that I is clearly closed under addition and contains 0, so it suffices to show closure under R multiplication:

$$\begin{pmatrix} a_{11} & a_{12} & a_{23} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \cdot \begin{pmatrix} 0 & b_{12} & b_{13} \\ 0 & 0 & b_{23} \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a_{11}b_{12} & a_{11}b_{13} + a_{12}b_{23} \\ 0 & 0 & a_{22}b_{23} \\ 0 & 0 & 0 \end{pmatrix}$$

&

$$\begin{pmatrix} 0 & b_{12} & b_{13} \\ 0 & 0 & b_{23} \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} & a_{23} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} = \begin{pmatrix} 0 & a_{22}b_{12} & a_{23}b_{12} + a_{33}b_{13} \\ 0 & 0 & a_{33}b_{23} \\ 0 & 0 & 0 \end{pmatrix}.$$

Now we consider the map $f : R/I \to \mathbb{F}^3$, $f(A) = (a_{11}, a_{22}, a_{33})$, where A is the matrix $\begin{pmatrix} a_{11} & a_{12} & a_{23} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix}$. This map is clearly well defined modulo I. Furthermore it preserves addition and sends the multiplicative identity of R/I to the respective identity of $\mathbb{F}^3$. The map is certainly surjective, and also injective because any two matrices with the same diagonal differ by an element of I and hence are in the same residue class of R/I. It remains to show this map also respects multiplication, which follows from the fact that

$$\begin{pmatrix} a_{11} & a_{12} & a_{23} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ 0 & b_{22} & b_{23} \\ 0 & 0 & b_{33} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & * & * \\ 0 & a_{22}b_{22} & * \\ 0 & 0 & a_{33}b_{33} \end{pmatrix}.$$

11 (a): If $d \in \mathbb{Z}$ were the square of a rational number, say $d = (\frac{a}{b})^2$ with $(a, b) = 1$, then $d \cdot b^2 = a^2$ and so by the fundamental theorem of arithmetic, any primes dividing b also divide a. Since $(a, b) = 1$, it follows that $b = \pm 1$. Hence any integer is the square of a rational number iff it is the square of an integer.

11 (b): The only non-routine thing to prove is that every non-zero element is invertible. Indeed $\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-b^2d} = \frac{a}{a^2-b^2d} - \frac{b}{a^2-b^2d}\sqrt{d}$. By (a) the denominator is never zero so this is a well defined element of $\mathbb{Q}[\sqrt{d}]$.

11 (c): Let $f : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}[x]/(x^2 - d)$ be the map that sends $a + b\sqrt{d}$ to $\overline{a + bx}$. The map is surjective, as every element of the range can be written in the form $\overline{a + bx}$ for some $a, b \in \mathbb{Q}$, because $\overline{x^2} = d$. It is easy to see that f preserves addition and the multiplicative identity, and also f preserves multiplication using the fact that $\overline{x^2} = \overline{d}$ in the range. It remains to show f is injective, but this is also obvious because every element in $\mathbb{Q}[\sqrt{d}]$ has a unique representation of the form $a + b\sqrt{d}$ and $\overline{a + bx} = \overline{c + ex}$ iff $a + bx = c + ex + (x^2 - d) \cdot p(x)$ for some $p(x) \in \mathbb{Q}[x]$ iff $p(x) = 0$ and $a = c$ and $b = e$ by degree considerations.

11 (d): Suppose $f : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$ is a ring isomorphism. Then $0 = f(0) = f((\sqrt{2})^2 - 2) = f(\sqrt{2})^2 - f(2) = f(\sqrt{2})^2 - 2$ and hence there must be an element in $\mathbb{Q}[\sqrt{3}]$ whose square is 2. Let $a + b\sqrt{3}$ be such an element, so that $2 = (a + b\sqrt{3})^2 = (a^2 + b^2 3) + 2ab\sqrt{3}$ for rational a, b. It follows that $0 = 2ab$ and $2 = a^2 + 3b^2$. There are thus 2 cases, either $a = 0$ or $b = 0$. When $b = 0$, we have $2 = a^2$, contradicting (a). If $a = 0$ then $2 = 3b^2 \Rightarrow 6 = (3b)^2$ again contradicting (a). Hence no such f exists.