MATH 235: Assignment 4 solutions

1. Observe that the identity matrix $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$ belongs to the set R by setting $a = c = 1$ and $b = 0$. Furthermore we have

$$\begin{aligned} -\left(\begin{smallmatrix}a & b\\ 0 & c\end{smallmatrix}\right) &= \left(\begin{smallmatrix}-a & -b\\ 0 & -c\end{smallmatrix}\right) \\ \left(\begin{smallmatrix}a & b\\ 0 & c\end{smallmatrix}\right) + \left(\begin{smallmatrix}a' & b'\\ 0 & c'\end{smallmatrix}\right) &= \left(\begin{smallmatrix}a+a' & b+b'\\ 0 & c+c'\end{smallmatrix}\right) \\ \left(\begin{smallmatrix}a & b\\ 0 & c\end{smallmatrix}\right) \cdot \left(\begin{smallmatrix}a' & b'\\ 0 & c'\end{smallmatrix}\right) &= \left(\begin{smallmatrix}aa' & ab'+bc'\\ 0 & cc'\end{smallmatrix}\right). \end{aligned}$$

Thus R is closed under addition, multiplication and additive inverses. It follows that R is a subring of $M_2(F)$. An example of a non-trivial ideal in R is the set

$$I := \{\left(\begin{smallmatrix}0 & b\\ 0 & c\end{smallmatrix}\right) \quad | \quad b, c \in F\}.$$

The ring R/I is isomorphic to the field F. Indeed the element $\overline{\left(\begin{smallmatrix}a & b\\ 0 & c\end{smallmatrix}\right)} \in R/I$ is uniquely determined by a since it is equal to $\overline{\left(\begin{smallmatrix}a & 0\\ 0 & 0\end{smallmatrix}\right)}$ and is not equal to 0 unless $a = 0$. This gives a bijective map from R/I to F and it is clear from the multiplication and addition formulas above (recall multiplication and addition in a quotient ring is inherited from the original ring) that this map is a ring homomorphism, hence an isomorphism.

2. Let $R \subset \mathbb{Z}$ be a subring of $\mathbb{Z}$. Suppose $R \neq \mathbb{Z}$. Then there exists an element $x \in \mathbb{Z}\backslash R$. We can assume $x > 0$ because R contains 0 and R is closed under additive inverses (hence either R contains both $-x$ and x or it contains neither). Then the set $S := \{n \in \mathbb{N} \quad | \quad n \notin R\}$ is a non-empty subset of $\mathbb{N}$ as it contains x. Thus S contains a minimal element x'. The element $x' - 1$ lies in $\mathbb{N}$ (note $x' \neq 0$) and since it doesn't lie in S (by minimality) it must lie in R. But R is also a subring so it contains 1. But then $x' = (x' - 1) + 1$ must lie in R, which is a contradiction. Therefore $R = \mathbb{Z}$.

3a) A ring homomorphism $\varphi : R \to R'$ must send the additive and multiplicative identities of R to the respective identities of R'. Thus $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ must have $\varphi(1) = \overline{1}$ for any such homomorphism. But then for $k \in \mathbb{N}$ we have

$$\varphi(k) = \varphi(1 + \ldots + 1) = \varphi(1) + \ldots + \varphi(1) = \overline{1} + \ldots + \overline{1} = \overline{k}$$

(where the second equality comes from the fact that φ is a ring homomorphism). Furthermore, we have

$$\overline{0} = \varphi(0) = \varphi(k - k) = \varphi(k) + \varphi(-k) = \overline{k} + \varphi(-k)$$

so that $\varphi(-k) = \overline{-k}$. Since the value of φ is already determined for every value of $\mathbb{Z}$, it is unique. Since φ is the quotient map, it is necessarily a homomorphism.

b) Suppose ψ is a ring homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}$. Then $\psi(\overline{1}) = 1$ and $\psi(\overline{0}) = 0$. But if we add together n ones, we get $\overline{1} + \ldots + \overline{1} = \overline{n} = 0$ and therefore

$$0 = \psi(\overline{0}) = \psi(\overline{1} + \ldots + \overline{1}) = \psi(\overline{1}) + \ldots + \psi(\overline{1}) = 1 + \ldots 1 = n$$

which is clearly a contradiction (unless of course $n = 0$ in which case $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}$ and we have the identity map). Hence no such ψ exists (when $n \neq 0$).

c) From (a) we know that there is a unique morphism φ from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ and also a unique morphism ψ from $\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$. If $\tau : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is a group homomorphism, then it follows from uniqueness that $\psi = \tau \circ \varphi$. From this we can conclude that the kernel of φ must be contained in the kernel of ψ if such a τ exists. But the kernels of these maps are the ideals (n) and (m) respectively. The ideal (m) contains the ideal (n) iff m divides n. We conclude that if τ exists, m must divide n. On the other hand, if m divides n, then the element $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ generates a non-trivial I of $\mathbb{Z}/n\mathbb{Z}$, and the quotient by this ideal is isomorphic to $\mathbb{Z}/m\mathbb{Z}$ as can be seen from the first isomorphism theorem applied to the composition of maps

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})/I.$$

Therefore if $m|n$ we have a map between the two rings. Hence a ring homomorphism exists iff $m|n$.

4. Suppose the ideal $(3, 1+\sqrt{-5})$ was principle, so it could be generated by a single element $a + b\sqrt{-5}$. Then we can write

$$\begin{aligned} 3 &= (a+b\sqrt{-5})(c+d\sqrt{-5}) \\ 1+\sqrt{-5} &= (a+b\sqrt{-5})(c'+d'\sqrt{-5}) \end{aligned}$$

Recall the norm map $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ sending $c+d\sqrt{-5}$ to c^2+5d^2 is multiplicative. Hence from the two equalities above, we get that $a^2 + 5b^2 = N(a + b\sqrt{-5})$ divides 9 and 6 (the norm of 3 and $1+\sqrt{-5}$ respectively). Hence it divides $\mathrm{GCD}(9, 6) = 3$. The only way $a^2 + 5b^2$ could divide 3 is if $b = 0$ and $a = \pm 1$, which would mean the ideal $(3, 1+\sqrt{-5}) = (a + b\sqrt{-5}) = (1)$. This means 1 lies in the ideal, so that

$$1 = 3(c+d\sqrt{-5}) + (1+\sqrt{-5})(c'+d'\sqrt{-5}) = (3c - 5d' + c') + (3d + d' + c')\sqrt{-5}$$

for some choice of $c, c', d, d' \in \mathbb{Z}$. But that means $c' = -(3d + d')$ and so

$$1 = 3c - 6d' - 3d$$

which obviously has no solutions in the integers since the RHS is divisible by 3. Therefore no such $a + b\sqrt{-5}$ exists.

5. Observe that the norm map gives $N(5) = 25$ and $N(1 - 8i) = 65$, so if $(5, 1 - 8i)$ is principally generated by $(a + bi)$, we must have $N(a + bi)$ dividing $\mathrm{GCD}(25, 65) = 5$. Up to units, there are only 2 elements of norm 5, namely $1 + 2i$ and $1 - 2i$, so the ideals generated by these two elements are the only possibilities (if the generator had norm 1 it would be a unit and so the ideal would be the whole ring which is not the case by an argument similar to the one given in problem 4). Since $(1 + 2i)(1 - 2i) = 5$, both ideals contain 5. However $\frac{1-8i}{1+2i} = -3 - 2i$ lies in the Gaussian integers while $\frac{1-8i}{1-2i} = \frac{17-6i}{5}$ does not. Therefore the ideal $(1 + 2i)$ contains the ideal $(5, 1 - 8i)$. Since we can write

$$1 + 2i = 5(2i) + 1 - 8i,$$

the ideal $(5, 1 - 8i)$ also contains $(1 + 2i)$ and hence these two ideals are equal.

6. By theorem 22.1.2 of the notes, the given ring is a field so long as the polynomial $x^4 + x + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$. This was proved in an earlier assignment, however to briefly recall note that $x^4 + x + 1$ has no roots in $\mathbb{Z}/2\mathbb{Z}$ and hence if it were not irreducible, it must be the product of two irreducible quadratics over

$\mathbb{Z}/2\mathbb{Z}$. However there is only 1 such quadratic, namely x^2+x+1 and its square is x^4+x^2+1. Thus x^4+x+1 is irreducible.

7. We want to find a polynomial $p(x)$ such that $p(x)\cdot(x^2+1) \equiv 1 \mod x^4+x+1$. This can be done by Euclid's algorithm on $\mathbb{Z}/2\mathbb{Z}[x]$:

$$\begin{aligned} x^4+x+1 &= (x^2+1)(x^2+1)+x \\ x^2+1 &= (x)(x)+1. \end{aligned}$$

Now working backwards:

$$\begin{aligned} 1 &= x^2+1-x(x) \\ &= x^2+1-x(x^4+x+1-(x^2+1)(x^2+1)) \\ &= (x^2+1)(1+x+x^3)-x(x^4+x+1). \end{aligned}$$

Therefore $[x^2+1]^{-1} = [1+x+x^3]$.

8. φ certainly sends the identity element of R_1 (the constant polynomial 1) to the identity element of R_2 (the function which sends every element of F to 1). Suppose f and g are 2 polynomials in $F[x]$. Then for $a \in F$,

$$\varphi(f+g)(a) = (f+g)(a) = f(a)+g(a) = \varphi(f)(a)+\varphi(g)(a)$$

so $\varphi(f+g) = \varphi(f)+\varphi(g)$. Likewise

$$\varphi(f\cdot g)(a) = (f\cdot g)(a) = f(a)\cdot g(a) = \varphi(f)(a)\cdot\varphi(g)(a).$$

Hence φ is a ring homomorphism.

9. Suppose $p(x) \in F[x]$ is in the kernel of φ. Then for all $a \in F$, $p(a) = 0$. If $p(x)$ is non-zero then the number of distinct roots of p is bounded by the degree of p and in particular is finite. Hence $p(a) = 0$ for only finitely many a if $p \neq 0$. If $F = \mathbb{Q}, \mathbb{R}$ or in fact any field with infinitely many elements, it follows that $p(x)$ lies in the kernel of φ iff $p(x) = 0$. Thus in such a case, φ is injective. These remarks also show why φ fails to be surjective. Consider the map from $F \to F$ that takes the value 1 at 0, but takes the value 0 everywhere else. If F has infinitely many elements, then this map takes the value 0 infinitely many times. But it is not the zero map because it takes the value 1. Hence it could not lie in the image of φ.

10. Assume $F = \mathbb{Z}/p\mathbb{Z}$. The polynomial $x^p - x$ factors as $\prod_{a\in F}(x-a)$ and hence takes the value 0 at every point of F. Thus it lies in the kernel of φ and hence in this case φ is not injective. In fact the kernel of the map is equal to the ideal generated by $x^p - x$ in $F[x]$. This is because if $f \in F[x]$ satisfies $f(a) = 0$, then $f = (x-a)f'$ for unique $f' \in F[x]$. Since the polynomial $(x-a)$ does not take the value 0 anywhere other than a, it follows that if $f(a) = 0$ for all $a \in F$, we must have $f = \left(\prod_{a\in F}(x-a)\right)\tilde{f}$ for some unique $\tilde{f} \in F[x]$.
To show surjectivity, observe that for every $a \in F$, it suffices to construct a polynomial that takes the value 1 at a and 0 everywhere else. Indeed suppose we have such polynomials $p_a(x)$, and suppose $g : F \to F$ is an arbitrary function that takes the value b_a at a. Then $g = \varphi(\sum_{a\in F} b_a \cdot p_a(x))$. Given $a \in F$, we construct p_a as

follows. First note that the polynomial

$$\prod_{\substack{c \in F \\ c \neq a}} (x - c)$$

takes the value 0 at every element of F except a, and is non-zero at a (in fact by Wilson's theorem it takes the value -1 at a). Hence multiplying the polynomial by -1 gives the desired p_a (note p_a is of course non-unique).