Algebra 1 Assignment 5 Solutions

Problem 1 We preform long division:

$$
\begin{array}{r|l}
3x^4 - 2x^3 + 6x^2 - x + 2 & x^2 + x + 1 \\
-(3x^4 + 3x^3 + 3x^2) & \\ \hline
 & 3x^2 - 5x + 8 \\
-5x^3 + 3x^2 - x + 2 & \\
-(-5x^3 - 5x^2 - 5x) & \\ \hline
8x^2 + 4x + 2 & \\
-(8x^2 + 8x + 8) & \\ \hline
-4x - 6 &
\end{array}
$$

And we find that $q(x) = x^2 + x + 1, r(x) = -4x - 6$.

Problem 2 Same thing, only recall that in $\mathbb{Z}_2[x]$, $a = -a$ and $2 * a = a + a = 0$. We find $q(x) = x^3 + x^2 + 1, r(x) = 0$.

Problem 3 Let $f : \mathbb{Z}[x] \to \mathbb{Z}$ be the map that sends a ploynomial $p(x) = a_0 + a_1x + \dots a_mx^m$ to $f(p) = a_0$. To show: f is a homomorphism.
Proof:

- The unit and zero elements in $\mathbb{Z}[x]$ are respectively 1 and 0. $f(1) = 1$ and $f(0) = 0$.
- Let $q(x) = b_0+b_1x+\dots$ and $p(x) = a_0+a_1x+\dots$. Then $p(x)+q(x) = (b_0+a_0)+(b_1+a_1)x+(b_2+p_2)x^2+\dots$. We get $f(p+q) = a_0+b_0 = f(p)+f(q)$.
- Let $p(x)$ and $q(x)$ be as above. We have that $p(x)q(x) = (a_0b_2) + (a_0b_1 + b_0a_1)x + \dots$. It follows that $f(pq) = a_0b_0 = f(p)f(q)$.

So f is a homomorphism.$\square$

Problem 4 We perform the Euclidian algorithm (notice that at each step I can replace the remainders by their monic representative):

$$
\begin{array}{rcll}
x^4 - x^3 - x^2 + 1 & = & (x^3 - 1)(x - 1) & +(-x^2 + x) \\
x^3 - 1 & = & (x^2 - x)(x + 1) & +\boxed{x - 1} \\
x^2 - x & = & (x - 1)x & +0
\end{array}
$$

And we find $\gcd(x^4 - x^3 - x^2 + 1, x^3 - 1) = x - 1$.

Problem 5 Again ...

$$x^4 + 3x^2 - 2x + 4 = (x^2 + 1)(x^2 + 3x - 1) + \underbrace{-5x - 5}_{=0 \text{ in } \mathbb{Z}_5[x]}$$

So in fact $x^2 + 1$ divides $x^4 + 3x^2 - 2x + 4$ so the gcd is $x^2 + 1$.

Problem 6 Let $x, y \in \mathbb{C}$ we define

$$M(x, y) = \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix}$$

We want to show that the set $H = \{M(z_1, z_2) \in M_2(\mathbb{C}) | z_1, z_2 \in \mathbb{C}\}$ is a subring of $M_2(\mathbb{C})$. To save work it is useful to have the following identities for complex conjugation: for all $\alpha, \beta \in \mathbb{C}$:

$$\begin{aligned} \overline{\alpha\beta} &= \bar{\alpha}\bar{\beta} \quad (1) \\ \overline{\alpha + \beta} &= \bar{\alpha} + \bar{\beta} \quad (2) \\ \bar{\bar{\alpha}} &= \alpha \quad (3) \\ \alpha\bar{\beta} &= \overline{\bar{\alpha}\beta} \quad (4) \end{aligned}$$

Proving $(1), (2), (3)$ is straightforward (write $\alpha = a + bi, \beta = c + di$ and expand both sides). And (4) is a consequence of (1) and (3). Moreover these identities almost immediately show that the map $f : \mathbb{C} \to \mathbb{C}$ where $f(x) = \bar{x}$ is a an isomorphism, the fact that f is bijective follows from (3).

Let's now check that H is a subring of $R = M_2(\mathbb{C})$ (this is only a sketch of a proof, but all the steps should be straightforward, using the identities you shouldn't have to write out stuff like $z_1 = a_1 + b_1 i, z_2 = \ldots$):

- $M(1, 1) \in H$ is the identity element in R.
- $M(0, 0) = 0_R$
- $M(z_1, z_2) + M(w_1, w_2) = M(z_1 + w_1, z_2 + w_2)$ (use identity (2)). So H is closed under addition.
- $M(z_1, z_2) + M(-z_1, -z_2) = 0_R$ (again, by identity (2)). So every element in H has its additive inverse in H.
- $$M(a, b) * M(c, d) = \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -\bar{b}c - \bar{d}\bar{a} & -\bar{b}d + \bar{a}\bar{c} \end{pmatrix} = A$$

  Using identities $(2), (3)$ and (4) on the lower entries gives

  $$A = M(ac - b\bar{d}, ad + b\bar{c}) \in H$$

  So H is closed under multiplication.

So H is a subring of R. I'll also point out right now that in general using the result from the last item $M(c, d) * M(a, b) = M(ca - d\bar{b}, cb - d\bar{a}) \neq M(a, b) * M(c, d)$. Because in general $ca - d\bar{b} \neq ac - b\bar{d}$. Therefore H is not a commutative ring.

Problem 7 We must show that every nonzero element in H has a multiplicative inverse. That is, using notation from the previous excercise, that for any matrix $M(a, b) \in H$ where $a, b \neq 0$, there is a matrix $M(x, y) \in H$ such that:

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} x & y \\ -\bar{y} & \bar{x} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

This means that the equations for the matrix coefficients have a solution i.e. we can find x, y such that:

$$\begin{array}{rrcl} e_1(x,y) = & ax - b\bar{y} & = & 1 \\ e_2(x,y) = & ay + b\bar{x} & = & 0 \\ e_3(x,y) = & -\bar{b}x - \bar{a}\bar{y} & = & 0 \\ e_4(x,y) = & -\bar{b}y + \bar{a}\bar{x} & = & 1 \end{array}$$

We now try to solve for x and y. Either a or b is not zero. I'll only do the case where $a \neq 0$ (the other case is the same). $a \neq 0$ so $\bar{a} \neq 0$ so we can divide $e_3(x, y)$ by $\bar{a}$. We write:

$$e_3'(x,y) = \frac{b}{\bar{a}} e_3(x,y) = (-b\bar{b}/\bar{a})x - b\bar{y} = 0$$

Computing $e_1(x, y) - e_3'(x, y)$ gives us:

$$1 = ax - b\bar{y} - \underbrace{\big((-b\bar{b}/\bar{a})x - b\bar{y}\big)}_{=0} = \frac{a\bar{a} - b\bar{b}}{\bar{a}} x \Rightarrow x = \frac{\bar{a}}{a\bar{a} - b\bar{b}}$$

We can then substitute this value of x back into $e_3(x, y)$ and easily solve for $\bar{y}$ and then for y. So there exist solutions $x = x_0, y = y_0$ for $e_1(x, y) = 1$ and $e_3(x, y) = 0$. And noting that by using our identities from the previous problem,

$$e_2(x_0, y_0) = -\overline{e_3(x_0, y_0)} = -\bar{0} = 0$$

and

$$e_4(x_0, y_0) = \overline{e_1(x_0, y_0)} = \bar{1} = 1$$

We have that the x_0, y_0 we found are solutions to the entire system of equations. So this system of equations has a solution so $M(a, b)$ is invertible. Since $M(a, b) \in H$ was arbitrary we may infer that H is a non-commutative ring in which every non-zero element is invertible.