**Math 235 (Fall 2009): Assignment 8 Solutions**

**4.a**: It is easy to see the function is bijective. The remaining part is computational.

**4.b**: We can easily check that $f(xi) = f(x)f(i)$, $f(xj) = f(x)f(j)$ and $f(xk) = f(x)f(k)$ for any $x \in \mathbb{R}$. By definition of the product, it follows that $f(\alpha\beta) = f(\alpha)f(\beta)$ for every $\alpha, \beta \in \mathbb{H}$.

Since $f$ is bijective, it follows that the defining properties of a ring hold in $\mathbb{H}$. For instance, let us see why the product is associative. Let $\alpha, \beta, \gamma \in \mathbb{H}$. Then, $f((\alpha\beta)\gamma) = f(\alpha\beta)f(\gamma) = (f(\alpha)f(\beta))f(\gamma) = f(\alpha)(f(\beta)f(\gamma)) = f(\alpha)f(\beta\gamma) = f(\alpha(\beta\gamma))$. Since $f$ is injective, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

**4.c**: $\mathbb{H}$ is a division ring because $\left\{ \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix} : z_1, z_2 \in \mathbb{C} \right\}$ is a division ring (in fact, the inverse of $\begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix}$ is $\frac{1}{(|z_1||z_2|)^2} \begin{pmatrix} \overline{z_1} & -z_2 \\ \overline{z_2} & z_1 \end{pmatrix}$ ).

**7**: Suppose $(x, y) = (f(x, y))$ for some $f(x, y) \in \mathbb{C}[x, y]$. In particular, $f(x, y)|x$ (because $x \in (f(x, y))$). Hence, $deg_x(f) = 0$ or $1$ and $deg_y(f) = 0$. Similarly, $deg_y(f) = 0$ or $1$ and $deg_x(f) = 0$. Thus $deg_x(f) = 0 = deg_y(f)$, i.e., $f(x, y) \in \mathbb{C}$. Clearly $f \neq 0$. So, $(f(x, y)) = \mathbb{C}[x, y]$. So it suffices to prove $(x, y) \subsetneq \mathbb{C}[x, y]$.

If $(x, y) = \mathbb{C}[x, y]$, then there are polynomials $a(x, y), b(x, y) \in \mathbb{C}[x, y]$ such that $1 = xa(x, y)+yb(x, y)$. Let $c(x, y) := 1 = xa(x, y)+yb(x, y)$. Hence, $1 = c(0, 0) = 0$. Contradiction!

**16**: Since $-2 = 3$ is not a square in $\mathbb{F}_5$, $x^2 + 2$ does not have a root in $\mathbb{F}_5[x]$ and, hence, is irreducible. Thus, $(x^2 + 2)$ is a maximal ideal (why?). Therefore, the quotient is a field.

Now let us compute the expressions. Everything follows from the fact that $x^2 = -2 = 3$ in the quotient ring.

$x^2 + x = 3 + x$ and $x^3 + 1 = 3x + 1$. Hence, $(x^2 + x)(x^3 + 1) = (x + 3)(3x + 1) = 3x^2 + 10x + 3 = 3x^2 + 3 = 3 \cdot 3 + 3 = 12 = 2$. Thus $(x^2 + x)(x^3 + 1) - (x + 1) = -x - 1 + 2 = 4x + 1$.

$x^2 + 3 = 3 + 3 = 1$. So, $(x^2 + 3)^{-1} = 1$. Hence, $\frac{x^2-1}{x^2+3} = 3 - 1 = 2$.

What are the roots of $t^2+2 = t^2-3$ in the quotient ring? We will use the fact that any element in the quotient ring can be written uniquely as a polynomial of the form $ax+b$, where $a, b \in \mathbb{F}_5$. Let $t = ax+b$. Then $t^2 = a^2x^2+2abx+b^2 = 2abx+b^2+3a^2$. Hence, $t^2 = 3$ iff $ab = 0$ and $b^2 + 3a^2 = 3$. Since 3 is not a square in $\mathbb{F}_5$, $a$ can't be zero (why?). Hence, $b = 0$. Thus, $3a^2 = 3$, i.e., $a^2 = 1$. Hence, the roots are $x$ and $-x = 4x$.

What are the roots of $t^2+3 = t^2-2$ in the quotient ring? Since 2 is not a square in $\mathbb{F}_5$, $t$ has to be of the form $ax$ with $3a^2 = 2$ by the same reasoning as above. Hence, the roots are $2x$ and $-2x = 3x$.

**17**: Since $x^3 + x + 1$ does not have roots in $\mathbb{F}_2$, it is an irreducible polynomial in $\mathbb{F}_2[x]$.

Now let us compute the expressions. Everything follows from the fact that $x^3 = x + 1$ in the quotient ring.

$x^3+1 = x$. So, $(x^2+x)(x^3+1) = (x^2+x)x = x^3+x^2 = x^2+x+1$. Hence, $(x^2+x)(x^3+1) - (x+1) = x^2$.

$x^2+3 = x^2+1$. We want to find $ax^2+bx+c$ such that $(x^2+1)(ax^2+bx+c) = 1$. But $(x^2+3)(ax^2+bx+c) = cx^2+ax+(b+c)$. Hence $a = c = 0$ and $b = 1$. Thus, $(x^2+3)^{-1} = x$.

$x^2-1 = x^2+1$. Therefore, $\frac{x^2+1}{x^2+3} = (x^2+1)x = 1$.

What are the roots of $t^3+t^2+1$ in the quotient ring? Let $t = ax^2+bx+c$. Then $t^3+t^2+1 = b(1+c)x^2+(a+b+ac+bc)x+(a+ab+b+1)$ (we used the fact that $\alpha = \alpha^2$ in $\mathbb{F}_2$). This allows us to conclude that the roots are $x+1$, $x^2+1$ and $x^2+x+1$.

What are the roots of $t^3+1$ in the quotient ring? Let $t = ax^2+bx+c$. Then $t^3+1 = (a+bc)x^2+(ac+bc+b)x+(a+b+c+ab+1)$. We conclude the only root is 1.

**18.a**: One can see that 2 is not a square in $\mathbb{F}_{19}$. Hence, $x^2-2$ is irreducible in $\mathbb{F}_{19}[x]$. Thus $L$ is a field.

**18.b**: Let $t = ax+b$. Then $t^2-t+2 = a(2b-1)x+(b^2-b+2a^2+2)$. We conclude that the roots are $7x+10$ and $12x+10$.

**18.c**: We just show that it does not have a root in any of the fields. For $\mathbb{F}_{19}$, there are only 19 possibilities. For the quotient ring, we use the same technique we have been using for the other exercises.

**18.d**: $x^{19} = x\cdot(x^3)^6 = x\cdot 2^6 = (2^2)^3x = (4\cdot 4^2)x = (4\cdot(-3))x = -12x = 7x$. Hence $x^{19}-x = 6x$.