**Exam 2 Solutions Math 641 Fall 2014**

**Definition:** Let $R$ and $S$ be commutative rings with $0 \neq 1$ in each. The ring structure on $R \times S$ is defined by $(a, b) + (a', b') = (a + a', b + b')$ and $(a, b)(a', b') = (aa', bb')$.

1. Let $R = \mathbb{Q}[x]$. Let $I$, $J$, and $K$ be the ideals of $R$ defined by $I = (x - 1)$, $J = (x^2 + x + 1)$, and $K = (x^3 - 1)$. You will prove in this problem that $R/K \cong R/I \times R/J$.

(a) Define $\phi : R \to R/I \times R/J$ by $\phi(f(x)) = (I + f(x), J + f(x))$. Prove that $\phi$ is a ring homomorphism.

(b) Prove that $K \subseteq \ker \phi$.

(c) Prove that $\ker \phi \subseteq K$.

(d) Find $a(x) \in \mathbb{Q}[x]$ and $b(x) \in \mathbb{Q}[x]$ so that $a(x)(x-1)+b(x)(x^2+x+1) = 1$.

(e) Using $(d)$, find $\mu(x) \in \mathbb{Q}[x]$ and $\nu(x) \in \mathbb{Q}[x]$ so that $\phi(\mu(x)) = (I+1, J+0)$ and $\phi(\nu(x)) = (I + 0, J + 1)$.

(f) Using $(e)$, prove that $\phi$ is surjective by finding a formula for $f(x)$ in terms of $p(x)$ and $q(x)$ such that $\phi(f(x)) = (I + p(x), J + q(x))$. Check your work by finding $f(x)$ such that $\phi(f(x)) = (I + 3x^2, J + 6x)$.

Hint:

$$(I + p(x), J + q(x)) = (I + 1, J + 0)(I + p(x), J + p(x))+$$

$$(I + 0, J + 1)(I + q(x), J + q(x)).$$

**Solution:**

(a) $\phi$ preserves addition: $\phi(f(x)+g(x)) = (I+f(x)+g(x), J+f(x)+g(x)) = ((I + f(x)) + (I + g(x)), (J + f(x)) + (J + g(x))) = (I + f(x), J + f(x)) + (I + g(x), J + g(x)) = \phi(f(x)) + \phi(g(x))$.

$\phi$ preserves multiplication: $\phi(f(x)g(x)) = (I + f(x)g(x), J + f(x)g(x)) = ((I+f(x))(I+g(x)), (J+f(x))(J+g(x)) = (I+f(x), J+f(x))(I+g(x), J+g(x)) = \phi(f(x))\phi(g(x))$.

(b) $f(x) \in K \implies f(x) = g(x)(x^3-1) = g(x)(x-1)(x^2+x+1) \implies f(x) \in I$ and $f(x) \in J \implies \phi(f(x)) = (I + f(x), J + f(x)) = (I + 0, J + 0) \implies f(x) \in \ker \phi$.

(c) $f(x) \in \ker\phi \implies (I+f(x), J+f(x)) = (I+0, J+0) \implies f(x) \in I$ and $f(x) \in J \implies f(x) = a(x)(x-1) = b(x)(x^2+x+1) \implies b(1) = 0 \implies b(x) = c(x)(x-1) \implies f(x) = c(x)(x-1)(x^2+x+1) = c(x)(x^3-1) \implies f(x) \in K$.

(d) Using Euclid's Method and Mathematica, I obtained $a(x) = -1-(2/3)x-(1/3)x^2$ and $b(x) = (1/3)x$.

(e) Since $a(x)(x-1) \in I$ and $a(x)(x-1)-1 \in J$, we can set $\nu(x) = a(x)(x-1)$. Since $b(x)(x^2+x+1) \in J$ and $b(x)(x^2+x+1)-1 \in I$, we can set $\mu(x) = b(x)(x^2+x+1)$.

(f) We have $(I+p(x), J+q(x)) = (I+1, J+0)(I+p(x), J+p(x)) + (I+0, J+1)(I+q(x), J+q(x)) = \phi(\mu(x))\phi(p(x)) + \phi(\nu(x))\phi(q(x)) = \phi(\mu(x)p(x) + \nu(x)q(x))$. Therefore we can set $f(x) = \mu(x)p(x) + \nu(x)q(x)$. Setting $p(x) = 3x^2$, $q(x) = 6x$, $\nu(x) = a(x)(x-1) = -\frac{x^3}{3} - \frac{x^2}{3} - \frac{x}{3} + 1$, $\mu(x) = b(x)(x^2+x+1) = \frac{x^3}{3} + \frac{x^2}{3} + \frac{x}{3}$, we obtain $f(x) = 6x - 2x^2 - x^3 - x^4 + x^5$. We have $f(x) - 3x^2 = (x-2)(x-1)x\,(x^2+2x+3) \in I$ and $f(x) - 6x = (x-2)x^2(x^2+x+1) \in J$, as desired.

2. Let $f(x) = 7 + 7x + 7x^2 + 7x^3 + x^4$, $I = (f(x))$, and $E = \mathbb{Q}[x]/I$.

(a) Prove that $E$ is a field.

(b) Prove that $E$ is a field extension of $\mathbb{Q}$. In other words, identify a field $F \subseteq E$ and a ring isomorphism $\phi : \mathbb{Q} \to F$. Prove that $\phi$ has the required properties.

(c) Let $\theta = I + x$ and $g(y) = (I+7) + (I+7)y + (I+7)y^2 + (I+7)y^3 + (I+1)y^4 \in E[y]$. Prove that $\theta$ is a root of $g(y)$ in $E$.

(d) Find $h(y) \in E[y]$ such that $g(y) = ((I+1)y - \theta)h(y)$. Use long division to compute $h(y)$.

(e) Find the multiplicative inverse of $\theta$ in $E$.

**Solution:**

(a) $f(x)$ is irreducible using Eisenstein's Criterion ($p = 7$). Hence $(f(x))$ is a maximal ideal and $\mathbb{Q}[x]/(f(x))$ is a field.

(b) Set $F = \{I + r : r \in \mathbb{Q}\}$, $\phi(r) = I + r$. Then $\phi(r+s) = I + r + s = (I+r) + (I+s) = \phi(r) + \phi(s)$, $\phi(rs) = I + rs = (I+r)(I+s) = \phi(r)\phi(s)$. $\phi$ is clearly surjective. $\phi$ is injective: $\phi(r) = \phi(s)$ implies $I + r = I + s$ implies

$r-s \in I$ implies $r-s = f(x)g(x)$. If $g(x) \neq 0$ then $f(x)g(x)$ has degree $\geq 4$, which contradicts $\deg(r-s) \leq 0$ Therefore $g(x) = 0$, $r-s=0$, $r=s$.

(c) $g(\theta) = (I+7)+(I+7)(I+x)+(I+7)(I+x)^2+(I+7)(I+x)^3+(I+x)^4 = (I+7)+(I+7x)+(I+7x^2)+(I+7x^3)+(I+x^4) = I+7+7x+7x^2+7x^3+x^4 = I+0$ since $7+7x+7x^2+7x^3+x^4-0 \in I$.

(d) Long division yields

$$\frac{(I+1)y^4+(I+7)y^3+(I+7)y^2+(I+7)y+(I+7)}{(I+1)y-(I+x)} =$$

$$(I+1)y^3+(I+x+7)y^2+(I+x^2+7x+7)y+(I+x^3+7x^2+7x+7).$$

Hence

$$(I+7)+(I+7)y+(I+7)y^2+(I+7)y^3+(I+1)y^4 =$$

$$(y-(I+x))((I+1)y^3+(I+x+7)y^2+(I+x^2+7x+7)y+(I+x^3+7x^2+7x+7)).$$

That is, after identifying $I+k$ with $k$ and $I+x^k$ with $\theta^k$, we have

$$7+7y+7y^2+7y^3+y^4 = (y-\theta)(y^3+(\theta+7)y^2+(\theta^2+7\theta+7)y+(\theta^3+7\theta^2+7\theta+7)).$$

Check:

$$(y-\theta)(y^3+(\theta+7)y^2+(\theta^2+7\theta+7)y+(\theta^3+7\theta^2+7\theta+7)) =$$
$$-7\theta-7\theta^2-7\theta^3-\theta^4+7y+7y^2+7y^3+y^4 =$$
$$7+7y+7y^2+7y^3+y^4$$

since

$$\theta^4+7\theta^3+7\theta^2+7\theta = -7.$$

(e) One method is to find $a(x)$ and $b(x)$ in $\mathbb{Q}[x]$ such that $a(x)(7+7x+7x^2+7x^3+x^4)+b(x)x = 1$. This implies $b(\theta)\theta = 1$, hence the inverse of $\theta$ is $b(\theta)$. Another method is to observe that since $\theta^4+7\theta^3+7\theta^2+7\theta+7=0$, we have

$$\theta(-\frac{1}{7}\theta^3-\theta^2-\theta-1) = 1.$$

Either way, the inverse is

$$I-\frac{1}{7}x^3-x^2-x-1.$$