2004 (2) MATH 338 ALGEBRA IIIB
ASSIGNMENT S2 SOLUTIONS

Question 1 **(a)** $1 = \frac{1}{1}$ and p does not divide 1 so $1 \in R$. From

$$\frac{m}{n} + \frac{r}{s} = \frac{ms+nr}{ns}, \quad \frac{m}{n}\frac{r}{s} = \frac{mr}{ns}$$

and the fact that $p \mid ns$ implies $p \mid n$ or $p \mid s$, we see that R is closed under + and $\times$.

(b) From the fact that $\frac{m}{n}, \frac{r}{s} \in p^k R$, $\frac{m}{n} + \frac{r}{s} = \frac{ms+nr}{ns}$ and $p^k \mid m$, $p^k \mid r$ imply $p^k \mid ms + rn$ we see that $p^k R$ is closed under addition. If $\frac{r}{s} \in R$ and $\frac{m}{n} \in p^k R$ then $p^k \mid m$ implies $p^k \mid mr$ so that $\frac{m}{n}\frac{r}{s} = \frac{mr}{ns} \in p^k R$; so $p^k R$ is an ideal of R.

(c) Let ϕ be the ring morphism $\mathbf{Z} \xrightarrow{\text{unique}} R \xrightarrow{\text{canon.}} R / p^k R$ taking n to $n + p^k R$. Then $\ker\phi = \left\{ n \in \mathbf{Z} \,\middle|\, n \in p^k R \right\} = p^k R$. Take any $\frac{m}{n} \in R$; so p does not divide n. So n and p^k have greatest common divisor 1; so there exist integers a and b with $1 = an + bp^k$. Then $\frac{m}{n} - ma = \frac{m(1-an)}{n} = \frac{mbp^k}{n} \in p^k R$. So $\frac{m}{n} + p^k R = \phi(ma) \in \operatorname{im}\phi$. So ϕ is surjective. By the First Isomorphism Theorem, $R / p^k R = \operatorname{im}\phi \cong \mathbf{Z} / \ker\phi = \mathbf{Z}_{p^k}$.

Question 2 **(a)** $C(\mathbf{R})$ is a subring of $\mathbf{R}^{\mathbf{R}}$ since 1 is continuous and a sum and a product of continuous functions is continuous.

(b) Suppose f and g lie in $M = \left\{ f \in C(\mathbf{R}) \,\middle|\, f(1) = 0 \right\}$. Then $(f+g)(1) = f(1) + g(1) = 0$ so $f + g \in M$. If $h \in C(\mathbf{R})$ and $f \in M$ then $(hf)(1) = h(1)f(1) = h(1)0 = 0$ so $hf \in M$. So is an ideal of $C(\mathbf{R})$. Suppose N is an ideal of $C(\mathbf{R})$ strictly containing M. Then there is some h in N which is not in M. Then $h(1) \neq 0$. Take any $g \in C(\mathbf{R})$. Put $f = g - \frac{g(1)}{h(1)}h$. Then $f(1) = g(1) - \frac{g(1)}{h(1)}h(1) = 0$. So f is in M. So, since N is an ideal, $g = f + \frac{g(1)}{h(1)}h \in N$. So $N = C(\mathbf{R})$. So M is maximal.

Question 3

(a) $(a_1, \ldots, a_m) \in R_1 \times \ldots \times R_m$ is invertible iff there exists $(b_1, \ldots, b_m) \in R_1 \times \ldots \times R_m$ such that $(a_1b_1, \ldots, a_mb_m) = (1, \ldots, 1)$ iff $a_1 \in R_1, \ldots, a_m \in R_1$ are all invertible. It follows that $(R_1 \times \ldots \times R_m)^\times = R_1^\times \times \ldots \times R_m^\times$.

(b) By the Chinese Remainder Theorem, $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \ldots \times \mathbf{Z}_{p_m^{\alpha_m}}$. So the result follows from Part (a).

(c) From the definition of ϕ we see that $\phi(n) = \#\mathbf{Z}_n^\times$ since an integer is invertible modulo n iff it is relatively prime to n. Clearly the positive integers less than or equal to p^α and **not** relatively prime to p^α are $p, 2p, 3p, \ldots, p^{\alpha-1}p$; so $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. So

$$\phi(n) = \phi(p_1^{\alpha_1}) \ldots \phi(p_m^{\alpha_m}) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \ldots \left(p_m^{\alpha_m} - p_m^{\alpha_m - 1}\right) = n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_m}\right).$$

Question 4 (a) Put L = $\{ab^{-1} \mid b \notin P\}$. Then we have $\lambda : D \longrightarrow L$ defined by $\lambda(a) = a1^{-1}$ which is in L since $1 \notin P$. Clearly λ is a ring morphism. If $a \notin P$ then $\lambda(a) = a$ has inverse $1a^{-1} \in L$. So λ inverts all $a \notin P$. Suppose $f : D \longrightarrow R$ is a ring morphism which inverts all $a \notin P$. Define $g : L \longrightarrow R$ by $g(ab^{-1}) = f(a)f(b)^{-1}$ (since f(b) is invertible as $b \notin P$). The following calculations show that g is a ring morphism:

$$g(ab^{-1} + cd^{-1}) = g((ad+bc)b^{-1}d^{-1}) = f(ad+bc)f(bd)^{-1} = (f(a)f(d) + f(b)f(c))f(b)^{-1}f(d)^{-1}$$

$$= f(a)f(b)^{-1} + f(c)f(d)^{-1} = g(ab^{-1}) + g(cd^{-1}),$$

$$g(ab^{-1}cd^{-1}) = g(acb^{-1}d^{-1}) = f(ac)f(bd)^{-1} = f(a)f(c)f(b)^{-1}f(d)^{-1} = 1.1^{-1} = 1,$$

$$g(1) = g(1.1^{-1}) = f(1)f(1)^{-1} = 1.1^{-1} = 1.$$

Also $(g \circ \lambda)(a) = g(a) = f(a)$, so $g \circ \lambda = f$. Moreover, g is unique with $g \circ \lambda = f$ since $g(ab^{-1}) = g(a)g(b)^{-1}$. By the universal property of D_P we see that D_P is isomorphic to L.

(b) Suppose D is a PID. Let A be an ideal of D_P. Then $\lambda^{-1}(A)$ is an ideal of D. So $\lambda^{-1}(A) = \langle a \rangle$ for some a in D. I claim that $A = \langle \lambda(a) \rangle$. Clearly $\lambda(a) \in A$; so $\langle \lambda(a) \rangle \subseteq A$. Take $cd^{-1} \in A$. Then $\lambda(c) = c = (cd^{-1})d \in A$. So $c \in \lambda^{-1}(A) = \langle a \rangle$. So $c = ea$ for some e in D. Then $cd^{-1} = ead^{-1} \in \langle a \rangle$. So $\langle \lambda(a) \rangle = A$.

Question 5 Suppose D is a Euclidean domain. Let A be an ideal of D. If A is non-zero, we have $a \in A$ with $a \neq 0$. Clearly $\langle a \rangle \subseteq A$. To prove $A \subseteq \langle a \rangle$ take $b \in A$. If $b = 0$ then $b = 0a \in \langle a \rangle$. So suppose $b \neq 0$. There exist q and r in D with $b = aq + r$ and $r = 0$ or $\delta(r) < \delta(a)$. So $r = b - aq \in A$. Suppose a was chosen with $\delta(a)$ least. Then $\delta(r) < \delta(a)$ is impossible. So $r = 0$. So $b = aq \in \langle a \rangle$, as required.

Bonus: See Beachy.