Solutions to Assignment # 2

1 a) We need to see that $(S,+)$ is an abelian group. $+$ is both associative and commutative since $+$ in R is. The constant function 0 is 0 in S and for $f \in S$, $(-f)(r) = -f(r)$ is the additive inverse.

Multiplication is associative since it is in R and distributivity holds both on the left and right because it does in R.

b) We need to see that P is closed under $+, \cdot$ and $-$.

If $f, g \in P$ say $f(x) = a_n x^n + \cdots + a_0$, $g(x) = b_m x^m + \cdots + b_0$ where $a_0 \cdots a_n, b_0 \cdots b_m \in R$ then $f+g$ is also defined by a polynomial as is fg and $-f$. So P is a subring of S.

c) If R is finite then the total number of functions from R to R is finite so both S and P are finite. However, $R[x]$ which is the collection of all poly. over R is infinite even if R is finite. The issue is that elements of $R[x]$ are treated formal as poly. and not as functions. The relationship between $R[x]$ and P is captured by:

$$R[x] \overset{\rho}{\twoheadrightarrow} P$$
$$f \longmapsto f(x), \text{ the function.}$$

and so $P \cong R[x] / \ker(\rho)$.

2. There are 4 diagonal solutions to the equation $x^2 = I$ over $M_2(\mathbb{C})$; I, $-I$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

Let $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. If P is any invertible 2×2 matrix

then $P^{-1}AP$ is also a solution. To see there are infinitely many such solutions, thinking geometrically,

let $P(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, a rotation of the plane by θ.

$P^{-1}(\theta) = P(-\theta)$ and A is reflection in the x-axis.

So $P^{-1}(\theta)\, A\, P(\theta) = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ -\sin 2\theta & -\cos 2\theta \end{pmatrix}$

and there are infinitely many different values of θ making these matrices distinct.

3. We need to show first of all that $F[[X]]$ is a ring.

$(F[[X]], +)$ is an abelian group: This is clear as

$(F[[X]], +) \cong (F^{\mathbb{N}}, +)$ where $F^{\mathbb{N}}$ is the set of all functions from $\mathbb{N}$ to F with coordinate-wise addition. The latter is an abelian group.

Multiplication is associative:

If $f = \sum_{i=0}^{\infty} f_i X^i$, $g = \sum_{i=0}^{\infty} g_i X^i$ and $h = \sum_{i=0}^{\infty} h_i X^i$

then $$(fg)h = \left(\sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} f_j g_{i-j} \right) X^i \right) \sum_{i=0}^{\infty} h_i X^i$$

$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} \left(\sum_{k=0}^{j} f_k g_{j-k} \right) h_{i-j} \right) X^i$$

$$= \sum_{i=0}^{\infty} \left(\sum_{j+k+l=i} f_j g_k h_l \right) X^i$$

and $$f(gh) = \sum_{i=0}^{\infty} f_i X^i \left(\sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} g_j h_{i-j} \right) X^i \right)$$

$$= \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} f_j \left(\sum_{k=0}^{i-j} g_k h_{i-j-k} \right) X^i \right)$$

$$= \sum_{i=0}^{\infty} \left(\sum_{j+k+l=i} f_j g_k h_l \right) X^i$$

So $f(gh) = (fg)h$

Multiplication is clearly commutative and has a 1 (the unit is $1+0\cdot X+0\cdot X^2+\cdots$).

To see distributivity, with f, g and h ~~as~~ as on page 3

$$f(g+h) = \sum_{i=0}^{\infty}\left(\sum_{j=0}^{i} f_j\,(g_{i-j}+h_{i-j})\right)X^i$$

$$= \sum_{i=0}^{\infty}\left(\sum_{j=0}^{i} f_j\,g_{i-j} + \sum_{j=0}^{i} f_j\,h_{i-j}\right)X^i$$

$$= fg + fh.$$

Finally, to see that $F[[X]]$ is an integral domain, suppose $f = \sum_{i=0}^{\infty} f_i X^i$ and $g = \sum_{i=0}^{\infty} g_i X^i$, both $\neq 0$.

Let i be least s.t. $f_i \neq 0$ and j least s.t. $g_j \neq 0$. The coeff. of X^{i+j} in fg is

$$\underbrace{f_0 g_{i+j} + f_1 g_{i+j-1} + \cdots}_{0} + \underbrace{f_i g_j}_{\neq 0} + \underbrace{f_{i+1} g_{j-1} + \cdots + f_{i+j} g_0}_{0}$$

So $fg \neq 0$ and $F[[X]]$ is an integral domain.

4, ~~a~~ Suppose $f, g : G \to G$ are endomorphisms.

a) $(f+g)(u-v) = f(u-v) + g(u-v)$

$= f(u) + g(u) - f(v) - g(v)$

$= (f+g)(u) - (f+g)(v)$

for all $u, v \in G$ so $f+g$ is an endomorphism.

b) $f(g(u-v)) = f(g(u) - g(v))$

$= f(g(u)) - f(g(v))$

so $f \circ g$ is an endomorphism.

c) $(End(G), +)$ is an abelian group: $+$ is associative and commutative since $+$ on G is. 0 is the zero map on G.

For $-f$ we check that if $f : G \to G$ is an endomorphism then $(-f)(u) = -f(u)$ is also an endo.

$$(-f)(u-v) = -(f(u-v))$$
$$= -(f(u) - f(v))$$
$$= -f(u) - (-f(v))$$

so $-f$ is ~~an~~ an endo.

Composition of functions is always associative and the identity map on G is 1.

To see distributivity, suppose $f, g, h : G \to G$ are endomorphisms.

$$f \circ (g+h)(u) = f(g(u) + h(u))$$
$$= (f \circ g)(u) + (f \circ h)(u) \quad \text{for all } u \in G$$

so $f \circ (g+h) = f \circ g + f \circ h$.

and $$(f+g) \circ h(u) = (f+g)(h(u))$$
$$= f \circ h(u) + g \circ h(u) \quad \text{for all } u \in G$$

so $(f+g) \circ h = f \circ h + g \circ h$ and we have distributivity.

5. To see that C forms a subring of $\mathbb{Q}^{\mathbb{N}}$, we need to show closure under $+$, $-$ and $\cdot$

$+$: If $\langle a_i : i \in \mathbb{N} \rangle$ and $\langle b_i : i \in \mathbb{N} \rangle$ are two Cauchy sequences. Fix k. There is an M

so that 1) for all $i, j \geq M$, $|a_i - a_j| \leq \frac{1}{2k}$.

and 2) for all $i, j \geq M$, $|b_i - b_j| \leq \frac{1}{2k}$.

Then for all $i, j \geq M$

$$|(a_i + a_j) - (b_i + b_j)| \leq |a_i - b_j| + |a_j - b_j|$$

$$\leq \frac{1}{2k} + \frac{1}{2k} = \frac{1}{k}.$$

$-$: If $\langle a_i : i \in \mathbb{N} \rangle$ is a Cauchy sequence then for a fixed k, there is M s.t. for all $i, j \geq M$ $|a_i - a_j| \leq \frac{1}{k}$. So $|(-a_i) - (-a_j)| = |a_j - a_i|$

$$= |a_i - a_j| \leq \frac{1}{k}.$$

for all $i, j \geq M$.

$\cdot$: We first show that Cauchy sequences are bounded.

If $\langle a_i : i \in \mathbb{N} \rangle \in C$, consider $k = 1$. There is M s.t. for all $i, j \geq M$, $|a_i - a_j| \leq 1$.

So for all $i \geq M$, $|a_i| \leq |a_M| + 1$. Let

$L = \max \{ |a_0|, \ldots |a_{M-1}|, |a_M| + 1 \}$ and we have

$|a_i| \leq L$ for all i.

Now pick $\langle a_i : i \in \mathbb{N} \rangle, \langle b_i : i \in \mathbb{N} \rangle \in C$; Choose $L \geq 1$ s.t. $|a_i| \leq L$ for all i and $|b_i| \leq L$ for all i.

Now ~~for~~ fixed k, choose M s.t. for all $i, j \geq M$ we have

(1) $|a_i - a_j| \leq \frac{1}{2kL}$ and (2) $|b_i - b_j| \leq \frac{1}{2kL}$

For $i, j \geq M$ we have.

$$|a_i b_i - a_j b_j| = |a_i b_i - a_i b_j + a_i b_j - a_j b_j|$$
$$\leq |a_i| |b_i - b_j| + |a_i - a_j| |b_j|$$
$$\leq L \cdot \frac{1}{2kL} + \frac{1}{2kL} \cdot L$$
$$= \frac{1}{k}.$$

So C is a subring of $\mathbb{Q}^{\mathbb{N}}$.

$\varphi: C \to \mathbb{R}$ is surjective : ~~Re~~ for any $r \in \mathbb{R}$, choose a sequence of rationals a_i for $i \in \mathbb{N}$ s.t. $\lim_{i \to \infty} a_i = r$.

That φ is a homomorphism follows from the fact that sums and products of bounded limits are limits of their sums and products.

$I = \ker(\varphi)$ is the set of all Cauchy sequences which tend to zero so we have $C/I \cong \mathbb{R}$.