1. **Lemma:** By the Division Algorithm, for all integers a, there exist integers r and q where $a = p \cdot q + r$ and $0 \leq r < p$. Thus, it follows that $a \equiv r \pmod{p}$. We claim that if $r = 1$, then $p \mid \Phi_p(a)$. If $r \neq 1$, then $p \mid \Phi_p(a) - 1$.

   Proof:

   For $r = 0$ and since p is a prime, we note that:

   $$\Phi_p(a) - 1 = \frac{a^p - 1}{a - 1} - 1 = (a^{p-1} + a^{p-2} + \cdots + a^1 + 1) - 1 = a^{p-1} + a^{p-2} + \cdots + a^1$$

   It follows that since each term of the sum is in the form a^k for $1 \leq k \leq p - 1$, that $p \mid a^k$ since $p \mid a$, so $p \mid \Phi_p(a) - 1$.

   For $r = 1$, we note that, since p is a prime:

   $$\Phi_p(a) = \frac{a^p - 1}{a - 1} = a^{p-1} + a^{p-2} + \cdots + a^1 + 1$$

   There are p terms in the sum. For $p - 1$ of them, they come in the form a^k for $1 \leq k \leq p - 1$ and $a^k \equiv 1 \pmod{p}$ since $a \equiv 1 \pmod{p}$. Since $1 \equiv 1 \pmod{p}$, the congruence of summing all p terms of the sum is $\Phi_p(a) \equiv p \pmod{p}$. Thus, since $p \mid p$, combining the two gives $p \mid \Phi_p(a)$.

   For $r \neq 0, 1$, we note from Fermat's Little Theorem that $a^{p-1} \equiv 1 \pmod{p}$ as $p \nmid a$, then $\gcd(p, a) = 1$. We then note that:

   $$\Phi_p(a) - 1 = \frac{a^p - 1}{a - 1} - 1 = \frac{a^p - a}{a - 1} = \frac{a(a^{p-1} - 1)}{a - 1}$$

   Since $p \nmid a$ and $p \nmid a - 1$, we get that:

   $$\nu_p(\Phi_p(a) - 1) = \nu_p(a(a^{p-1} - 1)) - \nu_p(a - 1) = \nu_p(a^{p-1} - 1)$$

   We also note that since $\Phi_p(a) - 1$ can be expressed as a sum of powers of a up to $p - 1$ as shown when proving $r = 0$, we note that $\Phi_p(a) - 1$ must be an integer. Since $p \mid a^{p-1} - 1$, we get that $\nu_p(a^{p-1} - 1) \geq 1$, so $\nu_p(\Phi_p(a) - 1) \geq 1$, thus $p \mid \Phi_p(a) - 1$.

   (a) From the Lemma, there are only two possible cases for any given integer a and $\Phi_p(a)$, which is either $p \mid \Phi_p(a) - 1$ or $p \mid \Phi_p(a)$. Thus, if $p \nmid \Phi_p(a)$, then the only other possible case is that $p \mid \Phi_p(a) - 1$.

   (b) We note that from applying the Division Algorithm to a as done in the Lemma, the remainder r of a is either 1 or not 1. If $r \neq 1$, then it follows that $p \mid \Phi_p(a) - 1$, so $p \nmid \Phi_p(a)$. Thus, only when $r = 1$, we get that $p \mid \Phi_p(a)$. Hence, if $p \mid \Phi_p(a)$, we get that $p \mid a - 1$. Since $p \mid a - 1$ and $p > 2$, we apply LTE to get that:

   $$\begin{aligned} \nu_p(\Phi_p(a)) = \nu_p\left(\frac{a^p - 1}{a - 1}\right) &= \nu_p(a^p - 1) - \nu_p(a - 1) \\ &= \nu_p(a - 1) + \nu_p(p) - \nu_p(a - 1) \\ &= 1 \end{aligned}$$

   as desired.

(c) For $m = 2$, we note that 1 is the only divisor d where $\gcd(2, d) = 1$. Thus:

$$\begin{aligned} x^{\phi(2)}\Phi_2(1/x) &= x \cdot (1/x - \zeta_2) \\ &= 1 - x\zeta_2 \\ &= 1 - x(-1) \\ &= x - \zeta_2 \\ &= \Phi_2(x) \end{aligned}$$

For $m > 2$, we note that $\phi(m)$ is equal to the number of k from $1 \leq k \leq m$ where $\gcd(m, k) = 1$. Hence:

$$x^{\phi(m)}\Phi_m(1/x) = \prod_{\substack{1 \leq k \leq m \\ \gcd(m,k)=1}} x \cdot \left(\frac{1}{x} - \zeta_m^k\right) = \prod_{\substack{1 \leq k \leq m \\ \gcd(m,k)=1}} (1 - \zeta_m^k x)$$

We note that if $m/2$ is an integer then $\gcd(m, m/2) \neq 1$. We then note that for every k for $1 \leq k \leq m$ where $\gcd(k, m) = 1$, we get that $\gcd(m - k, m) = 1$ from Proposition 2.15. Since $m/2$ is not part of the k that satisfies $\gcd(m, k) = 1$, we get that the k where $\gcd(m, k) = 1$ can be paired and be split along $m/2$. Thus:

$$\begin{aligned} \prod_{\substack{1 \leq k \leq m \\ \gcd(m,k)=1}} (1 - \zeta_m^k x) &= \prod_{\substack{1 \leq k < m/2 \\ \gcd(m,k)=1}} (1 - \zeta_m^k x) \prod_{\substack{m/2 < i \leq m \\ \gcd(m,i)=1}} (1 - \zeta_m^i x) \\ &= \prod_{\substack{1 \leq k < m/2 \\ \gcd(m,k)=1}} (1 - \zeta_m^k x)(1 - \zeta_m^{m-k} x) \end{aligned}$$

We then expand and refactor them to get:

$$\begin{aligned} \prod_{\substack{1 \leq k < m/2 \\ \gcd(m,k)=1}} (1 - \zeta_m^k x)(1 - \zeta_m^{m-k} x) &= \prod_{\substack{1 \leq k < m/2 \\ \gcd(m,k)=1}} (1 - \zeta_m^k x - \zeta_m^{m-k} x + x^2) \\ &= \prod_{\substack{1 \leq k < m/2 \\ \gcd(m,k)=1}} (x - \zeta_m^k)(x - \zeta_m^{m-k}) \\ &= \prod_{\substack{1 \leq k < m/2 \\ \gcd(m,k)=1}} (x - \zeta_m^k) \prod_{\substack{m/2 < i \leq m \\ \gcd(m,i)=1}} (x - \zeta_m^i) \\ &= \prod_{\substack{1 \leq k \leq m \\ \gcd(m,k)=1}} (x - \zeta_m^k) \\ &= \Phi_m(x) \end{aligned}$$

as desired.

(d) For $m \geq 2$, we prove by induction that $\Phi_{p^k}(1) = p$ for all $k \in \mathbb{N}$ for any prime p.
For $k = 1$, we get that:

$$\Phi_p(1) = \frac{1^p - 1}{1 - 1} = 1^{p-1} + 1^{p-2} + \cdots + 1 = p(1) = p$$

We assume by strong induction that for $1 \leq i \leq m$ that $\Phi_{p^i}(1) = p$. For $k = m + 1$, we get that from Proposition 6.3 and that all of its divisors are $1, p, p^2, \ldots, p^m, p^{m+1}$ that:

$$
\begin{aligned}
1^{p^{m+1}} - 1 &= \Phi_1(1) \cdot \Phi_p(1) \cdots \Phi_{p^m}(1) \cdot \Phi_{p^{m+1}}(1) \\
\frac{1^{p^{m+1}} - 1}{1-1} &= \Phi_p(1) \cdot \Phi_{p^2}(1) \cdots \Phi_{p^m}(1) \cdot \Phi_{p^{m+1}}(1)
\end{aligned}
$$

By the induction hypothesis, we get that:

$$
\begin{aligned}
1^{p^{m+1}-1} + 1^{p^{m+1}-2} + \cdots + 1^1 + 1 &= p^m \cdot \Phi_{p^{m+1}}(1) \\
p^{m+1}(1) &= p^m \cdot \Phi_{p^{m+1}}(1) \\
\Phi_{p^{m+1}}(1) &= p
\end{aligned}
$$

Thus, for all $k \in \mathbb{N}$ and for any prime p, we get that $\Phi_{p^k}(1) = p$.

We perform induction again for $m \geq 2$, but this time, we state the induction hypothesis as:

$$
\Phi_m(1) = \begin{cases} p & \text{if } m = p^k \text{ for some prime } p \text{ and } k \in \mathbb{N} \\ 1 & \text{otherwise} \end{cases}
$$

The case where $m = p^k$ for some p and $k \in \mathbb{N}$ is proven by our earlier induction. We concern ourselves with the otherwise case. The smallest otherwise case is when $m = 6$, and we show that:

$$
\begin{aligned}
\Phi_6(1) &= \frac{1^6 - 1}{\Phi_1(1) \cdot \Phi_2(1) \cdot \Phi_3(1)} \\
&= \frac{1^5 + 1^4 + 1^3 + 1^2 + 1^1 + 1}{2 \cdot 3} \\
&= \frac{6}{6} = 1
\end{aligned}
$$

We now assume by strong induction that for i where $6 \leq i \leq m$ that the induction hypothesis holds. For the case m, if m can be expressed by a perfect prime power then it is proven. However, if m is not, we first show that:

$$
x^m - 1 = \prod_{d \mid m} \Phi_d(x)
$$

Thus:

$$
\begin{aligned}
\frac{1^m - 1}{1-1} &= \prod_{\substack{d \mid m \\ d \neq 1}} \Phi_d(1) \\
1^{m-1} + 1^{m-2} + \cdots + 1^1 + 1 &= \prod_{\substack{d \mid m \\ d \neq 1}} \Phi_d(1) \\
m &= \prod_{\substack{d \mid m \\ d \neq 1}} \Phi_d(1)
\end{aligned}
$$

We then note that if for some prime p and $\nu_p(m) \geq 1$, we get that $p^1, p^2, \ldots, p^{\nu_p(m)}$ are all divisors of m. We also then note that $\Phi_{p^1}(1), \Phi_{p^2}(1), \ldots, \Phi_{p^{\nu_p(m)}}(1)$ are all equal to p from our earlier induction, so multiplying them all gives us $p^{\nu_p(m)}$. This means isolating the divisors expressible as p^k for some prime p and some integer k and multiplying their $\Phi_{p^k}(1)$ gives us the prime factorization of m, which equals m. Thus:

$$m = \prod_{\substack{p \\ p|m}} p^{\nu_p(m)} \prod_{\substack{d|m \\ d\neq 1 \\ d\neq p^k}} \Phi_d(1)$$

$$1 = \prod_{\substack{d|m \\ d\neq 1 \\ d\neq p^k \\ d\neq m}} \Phi_d(1) \cdot \Phi_m(1)$$

The product outside of $\Phi_m(1)$ must all equal 1 as all of its remaining divisors d are $d < m$, which means their product is equal to 1. Thus:

$$1 = 1 \cdot \Phi_m(1) = \Phi_m(1)$$

This completes the induction, and we proved our desired result for $\Phi_m(1)$ for any $m \in \mathbb{N}$.

2. (a) We assume it to be true. From Proposition 6.3 and since m is a divisor of itself, we see that:

$$x^m - 1 = \Phi_m(x) \cdot \prod_{\substack{d|m \\ d \neq m}} \Phi_d(x)$$

Thus, we get that $\Phi_m(69) = 420 \mid 69^m - 1$, so there exists an integer q where $69^m - 1 = 420q = 3(140)q$, so $3 \mid 69^m - 1$. This is a contradiction because $3 \mid 69$, so $3 \mid 69^m$. Thus, the statement is false.

(b) We assume that there does exist such an integer a where $23 \mid \Phi_{69}(a)$.

If $a \equiv 1 \pmod{23}$, then we can apply LTE to $a^{69} - 1$ as 23 is an odd prime and $23 \nmid 1$, $23 \mid a - 1$. Thus:

$$\begin{aligned} \nu_{23}(a^{69} - 1) &= \nu_{23}(a - 1) + \nu_{23}(69) \\ &= \nu_{23}(a - 1) + 1 \end{aligned}$$

From Proposition 6.3, we see that

$$\Phi_{69}(a) = \frac{a^{69} - 1}{\Phi_3(a) \cdot \Phi_{23}(a) \cdot \Phi_1(a)}$$

We also note that since 23 is a prime:

$$\begin{aligned} \Phi_{23}(a) &= \frac{a^{23} - 1}{a - 1} \\ \Phi_{23}(a) \cdot \Phi_1(a) &= a^{23} - 1 \end{aligned}$$

Thus, we then apply LTE on $a^{23} - 1$ to get that:

$$\begin{aligned} \nu_{23}(\Phi_{69}(a)) &= \nu_{23}(a^{69} - 1) - \nu_{23}(a^{23} - 1) - \nu_{23}(\Phi_3(a)) \\ &= \nu_{23}(a - 1) + 1 - (\nu_{23}(a - 1) + 1) - \nu_{23}(\Phi_3(a)) \\ &= -\nu_{23}(\Phi_3(a)) \end{aligned}$$

This implies that $\nu_{23}(\Phi_{69}(a)) = -\nu_{23}(\Phi_3(a)) \leq 0$. Thus, $23 \nmid \Phi_{69}(a)$, so $a \not\equiv 1 \pmod{23}$.

If $a \equiv 0 \pmod{23}$, then $23 \nmid a^{69} - 1$ as $23 \mid a^{69}$. However, as mentioned in a), $\Phi_{69}(a) \mid a^{69} - 1$ from Proposition 6.3, which should imply $23 \mid a^{69} - 1$ if $23 \mid \Phi_{69}(a)$. This is a contradiction, so $a \not\equiv 0 \pmod{23}$.

This leaves that $a \not\equiv 0, 1 \pmod{23}$. By Fermat's Little Theorem, we get that $a^{22} \equiv 1 \pmod{23}$. Since 23 is a prime and $23 \nmid a$, they are coprime. Thus, from Proposition 5.7, we get that $o_{23}(a) \mid 22$. Thus, $o_{23}(a)$ must be either 1, 2, 11, or 22. However, 1 is ruled out because that implies $a \equiv 1 \pmod{23}$. This means $23 \nmid a^{69} - 1$ because if it did then $a^{69} \equiv 1 \pmod{23}$, so $o_{23}(a) \mid 69$, which is not possible given its options. However, we assumed $23 \mid \Phi_{69}(a)$ and $\Phi_{69}(a) \mid a^{69} - 1$, so $23 \mid a^{69} - 1$, a contradiction.

All possible congruences that a can be to mod 23 result in a contradiction. This means that the integer a does not exist, so the statement is false.

(c) We note that for a given $m > 2$, we use our result from c) to show that:

$$\Phi_m(x) = \prod_{\substack{1 \le k \le m/2 \\ \gcd(m,k)=1}} (x - \zeta_m^k)(x - \zeta_m^{m-k})$$

We expand them to get a similar result as in 1c), where

$$\begin{aligned}\Phi_m(x) &= \prod_{\substack{1 \le k \le m/2 \\ \gcd(m,k)=1}} x^2 - (\zeta_m^k + \zeta_m^{m-k})x + 1 \\ &= \prod_{\substack{1 \le k \le m/2 \\ \gcd(m,k)=1}} x^2 - 2\cos(2k\pi/m)x + 1\end{aligned}$$

Thus, we also note that:

$$(x-1)^2 \le x^2 - 2\cos(2k\pi/m)x + 1 \le (x+1)^2$$

Since our product was splitting $\phi(m)$ into ordered pairs of $(k, m-k)$, we note that there exist $\phi(m)/2$ terms in the product. Thus, we get that:

$$(x-1)^{2\cdot\phi(m)/2} \le \prod_{\substack{1 \le k \le m/2 \\ \gcd(m,k)=1}} x^2 - 2\cos(2k\pi/m)x + 1 \le (x+1)^{2\cdot\phi(m)/2}$$

$$(x-1)^{\phi(m)} \le \Phi_m(x) \le (x+1)^{\phi(m)}$$

We now apply this result to $\Phi_{69}(420)$ and $\Phi_{420}(69)$. We first evaluate $\phi(69)$ and $\phi(420)$ using Exercise 5.1.

$$\begin{aligned}\phi(69) &= \phi(23)\cdot\phi(3) \\ &= (23-1)(3-1) \\ &= 44 \\ \phi(420) &= \phi(2^2)\phi(3)\phi(5)\phi(7) \\ &= (4-2)(3-1)(5-1)(7-1) \\ &= 96\end{aligned}$$

We then apply the result to get that:

$$\begin{aligned}(419)^{44} \le \Phi_{69}(420) \le (421)^{44} \\ (68)^{96} \le \Phi_{420}(69) \le (70)^{96}\end{aligned}$$

We note that $96 \cdot \ln(68) > 44 \cdot \ln(421)$, so $68^{96} > 421^{44}$, thus $\Phi_{420}(69) > \Phi_{69}(420)$. This is opposite of what was stated. Thus, the statement is false.

3. (a) Assume that this ring homomorphism $f : \mathbb{R} \to \mathbb{Q}$ exists. We note that $f(1) + f(1) = 2$, so $f(2) = 2$. Thus, we note that $f(\sqrt{2})^2 = f(2) = 2$ or $f(\sqrt{2})^2 = 2$, but there does not exist a number in $\mathbb{Q}$ that can satisfy the value for $f(\sqrt{2})$, which leads to a contradiction.

   (b) Assume this ring homomorphism $f : \mathbb{Q} \to \mathbb{Z}$ exists. Then, we see that $f(1) = 1$, so $f(1) + f(1) = f(2) = 2$. We then note that $f(1/2) \cdot f(2) = f(1) = 1$, but that also implies $f(1/2) \cdot 2 = 1$. There does not exist a number in $\mathbb{Z}$ that satisfies the value for $f(1/2)$, which leads to a contradiction.

   (c) Since $a \geq b$, we note that $a - b \geq 0$. Thus, since $a - b$ is non-negative, we denote a non-negative number $x = \sqrt{a - b}$. We then note that $g(a) = g(b) + g(a - b) = g(b) + g(x)^2$. Since $g(x)^2$ must be non-negative, we get that $g(a) - g(b) \geq 0$, which implies $g(a) \geq g(b)$ as desired.

   (d) Let $r \in \mathbb{Q}$ be arbitrary. There exist integers p and q where $r = p/q$. Since g is a ring homomorphism, we note that $g(1) - g(1) = 0$, so $g(0) = 0$, which gives $g(1) + g(-1) = 0$, thus $g(-1) = -1$. Thus, if $p < 0$, we add $g(-1)$ to itself $-p$ times. If $p > 0$, we add $g(1)$ to itself p times. If $p = 0$, then $g(0) = p = 0$. In all cases, we get that $g(p) = p$, and doing the same with q will yield $g(q) = q$. Since $g(1/q) \cdot g(q) = 1$, we get that $g(1/q) = 1/g(q) = 1/q$. Hence, we get that $g(p) \cdot g(1/q) = p \cdot 1/q$ or $g(p/q) = g(r) = p/q = r$ as desired.

4. (a) Since addition and multiplication is defined coordinate-wise, we get the following given two arbitrary $(r_n)_{n=1}^{\infty}$ and $(\hat{r}_n)_{n=1}^{\infty}$ in R:

$$(r_n)_{n=1}^{\infty} + (\hat{r}_n)_{n=1}^{\infty} = (r_n + \hat{r}_n)_{n=1}^{\infty}$$
$$(r_n)_{n=1}^{\infty} \cdot (\hat{r}_n)_{n=1}^{\infty} = (r_n \cdot \hat{r}_n)_{n=1}^{\infty}$$

Thus, we get that $\pi_j((1)_{n=1}^{\infty}) = 1$ because the series is entirely composed of it regardless of j. Meanwhile, for addition, we get that:

$$\begin{aligned}\pi_j((r_n)_{n=1}^{\infty}) + \pi_j((\hat{r}_n)_{n=1}^{\infty}) &= r_j + \hat{r}_j \\ &= \pi_j((r_n + \hat{r}_n)_{n=1}^{\infty}) \\ &= \pi_j((r_n)_{n=1}^{\infty} + (\hat{r}_n)_{n=1}^{\infty})\end{aligned}$$

Meanwhile, for multiplication, we get that:

$$\begin{aligned}\pi_j((r_n)_{n=1}^{\infty}) \cdot \pi_j((\hat{r}_n)_{n=1}^{\infty}) &= r_j \cdot \hat{r}_j \\ &= \pi_j((r_n \cdot \hat{r}_n)_{n=1}^{\infty}) \\ &= \pi_j((r_n)_{n=1}^{\infty} \cdot (\hat{r}_n)_{n=1}^{\infty})\end{aligned}$$

Thus, π_j satisfies all the conditions for a ring homomorphism, thus it is one.

(b) Since φ_{j+1} and f_j are ring homomorphisms, we get that:

$$\begin{aligned}\varphi_{j+1}(1_S) &= 1 \\ f_j(1) &= 1 \\ f_j(\varphi_{j+1}(1_S)) &= 1\end{aligned}$$

For addition and multiplication, we denote arbitrary $s, \hat{s} \in S$. For addition we get that:

$$\begin{aligned}f_j(\varphi_{j+1}(\hat{s} + s)) &= f_j(\varphi_{j+1}(\hat{s}) + \varphi_{j+1}(s)) \\ &= f_j(\varphi_{j+1}(\hat{s})) + f_j(\varphi_{j+1}(s))\end{aligned}$$

Meanwhile, for multiplication, we get that:

$$\begin{aligned}f_j(\varphi_{j+1}(\hat{s} \cdot s)) &= f_j(\varphi_{j+1}(\hat{s}) \cdot \varphi_{j+1}(s)) \\ &= f_j(\varphi_{j+1}(\hat{s})) \cdot f_j(\varphi_{j+1}(s))\end{aligned}$$

Thus, we showed that $f_j \circ \varphi_{j+1}$ satisfies all the properties for a ring homomorphism, thus it is one.

(c) We define $\varphi : S \to R$ as:

$$\varphi(s) = (\varphi_j(s))_{j=1}^{\infty}$$

We verify that $\varphi(s) \in R$ by showing that for any $j \in \mathbb{N}$, since $\varphi_j(s) = f_j \circ \varphi_{j+1}(s)$, we get that $f_j(\varphi_{j+1}(s)) = \varphi_j(s)$. We now show that it is also a ring homomorphism.

To start, we first show that:

$$\begin{aligned}
\varphi(1_S) &= (\varphi_j(1_S))_{j=1}^{\infty} \\
&= (1)_{j=1}^{\infty}
\end{aligned}$$

For what follows, we denote arbitrary $s, \hat{s} \in S$. For addition, we get that:

$$\begin{aligned}
\varphi(s) + \varphi(\hat{s}) &= (\varphi_j(s))_{j=1}^{\infty} + (\varphi_j(\hat{s}))_{j=1}^{\infty} \\
&= (\varphi_j(s) + \varphi_j(\hat{s}))_{j=1}^{\infty} \\
&= (\varphi_j(s + \hat{s}))_{j=1}^{\infty} \\
&= \varphi(s + \hat{s})
\end{aligned}$$

For multiplication, we get that:

$$\begin{aligned}
\varphi(s) \cdot \varphi(\hat{s}) &= (\varphi_j(s))_{j=1}^{\infty} \cdot (\varphi_j(\hat{s}))_{j=1}^{\infty} \\
&= (\varphi_j(s) \cdot \varphi_j(\hat{s}))_{j=1}^{\infty} \\
&= (\varphi_j(s \cdot \hat{s}))_{j=1}^{\infty} \\
&= \varphi(s \cdot \hat{s})
\end{aligned}$$

Thus, we showed that φ satisfies all the conditions for a ring homomorphism, thus it is one. We note that $\pi_j((\varphi_j(s))_{n=1}^{\infty}) = \varphi_j(s)$. Hence, we proved the existence of a $\varphi : S \to R$ where $\pi_j \circ \varphi = \varphi_j$.