Question 1

Problem a

$$\begin{aligned}&\text{False :}\\&a^{p-1} \equiv 1 \mod p \Leftrightarrow \gcd(a,p) = 1 \wedge \varphi(p) = p-1\end{aligned}$$

Problem b

$$\begin{aligned}&\text{True :}\\&\forall n \geqslant 2, \gcd(n,n) = n \neq 1\\&\varphi(n) = \#(p) : p \leqslant n, \gcd(p,n) = 1\\\Rightarrow&\varphi(n) < n\end{aligned}$$

Problem c

$$\begin{aligned}&\text{False :}\\&\mathbb{Z} \text{ is not closed in multiplication}\\\Rightarrow&\mathbb{Z} \text{ cannot be a kernel for ring homomorphism}\end{aligned}$$

Problem d

$$
\begin{aligned}
&\text{True :}\\
&(R,+,\times) \text{ is commutative}\\
&\forall x,y \in R : (x+I)\times(y+I) = x\times y + I = y\times x + I = (y+I)\times(x+I)\\
\Rightarrow &R/I \text{ is commutative}
\end{aligned}
$$

Problem e

$$
\begin{aligned}
&\text{True :}\\
&1 \in I\\
&\forall r \in R : r\times 1 = r \in I\\
\Rightarrow &R \subseteq I\\
&I \text{ is an ideal of } R\\
\Rightarrow &I \subseteq R\\
\Rightarrow &I = R
\end{aligned}
$$

Question 2

Problem a

$$
\begin{aligned}
&x^6 + 3x^5 + x + 1 \\
=&x^4(x^2 + 2x - 1) + x^5 + x^4 + x + 1 \\
=&x^4(x^2 + 2x - 1) + x^3(x^2 + 2x - 1) - x^4 - x^3 + x + 1 \\
=&x^4(x^2 + 2x - 1) + x^3(x^2 + 2x - 1) - x^2(x^2 + 2x - 1) + 3x^3 - x^2 + x + 1 \\
=&x^4(x^2 + 2x - 1) + x^3(x^2 + 2x - 1) - x^2(x^2 + 2x - 1) + 3x(x^2 + 2x - 1) - 7x^2 + 4x + 1 \\
\equiv&(x^4 + x^3 - x^2 + 3x)(x^2 + 2x - 1) + 4x + 1 \mod 7 \\
\Rightarrow& q(x) = x^4 + x^3 - x^2 + 3x, r(x) = 4x + 1
\end{aligned}
$$

Problem b

$$
\begin{aligned}
&x^6 + 3x^5 + x + 1 \\
=&5x^4(3x^2 + 2x - 1) - 14x^6 - 7x^5 + 5x^4 + x + 1 \\
\equiv&5x^4(3x^2 + 2x - 1) + 5x^4 + x + 1 \mod 7 \\
=&5x^4(3x^2 + 2x - 1) + 4x^2(3x^2 + 2x - 1) - 7x^4 - 8x^3 + 4x^2 + x + 1 \\
\equiv&5x^4(3x^2 + 2x - 1) + 4x^2(3x^2 + 2x - 1) - x^3 + 4x^2 + x + 1 \mod 7 \\
=&5x^4(3x^2 + 2x - 1) + 4x^2(3x^2 + 2x - 1) - 5x(3x^2 + 2x - 1) + 14x^3 + 14x^2 - 4x + 1 \\
\equiv&5x^4(3x^2 + 2x - 1) + 4x^2(3x^2 + 2x - 1) - 5x(3x^2 + 2x - 1) - 4x + 1 \mod 7 \\
=&(5x^4 + 4x^2 - 5x)(3x^2 + 2x - 1) - 4x + 1 \\
\Rightarrow& q(x) = 5x^4 + 4x^2 - 5x, r(x) = -4x + 1
\end{aligned}
$$

Problem c

$$
\begin{aligned}
&x^4+5x^3-3x^2\\
=&9x^2(5x^2-x+2)-44x^4+14x^3-21x^2\\
\equiv&9x^2(5x^2-x+2)+3x^3+x^2 \mod 11\\
=&9x^2(5x^2-x+2)+5x(5x^2-x+2)-22x^3+6x^2-10x\\
\equiv&9x^2(5x^2-x+2)+5x(5x^2-x+2)+6x^2+x \mod 11\\
=&9x^2(5x^2-x+2)+5x(5x^2-x+2)+10(5x^2-x+2)-44x^2+11x-20\\
\equiv&9x^2(5x^2-x+2)+5x(5x^2-x+2)+10(5x^2-x+2)+2 \mod 11\\
=&(9x^2+5x+10)(5x^2-x+2)+2\\
\Rightarrow&q(x)=9x^2+5x+10, r(x)=2
\end{aligned}
$$

Question 3

Problem a

Proof.

$$
\begin{aligned}
&p(0) = 0^2 + 0 + 1 \equiv 1 \mod 5\\
&p(1) = 1^2 + 1 + 1 \equiv 3 \mod 5\\
&p(2) = 2^2 + 2 + 1 \equiv 2 \mod 5\\
&p(3) = 3^2 + 3 + 1 \equiv 3 \mod 5\\
&p(4) = 4^2 + 4 + 1 \equiv 1 \mod 5\\
\Rightarrow &p(x) \text{ is irreducable in } \mathbb{Z}_5\\
&p(0) = 0^2 + 0 + 1 \equiv 1 \mod 29\\
&p(1) = 1^2 + 1 + 1 \equiv 3 \mod 29\\
&p(2) = 2^2 + 2 + 1 \equiv 2 \mod 29\\
&p(3) = 3^2 + 3 + 1 \equiv 13 \mod 29\\
&p(4) = 4^2 + 4 + 1 \equiv 21 \mod 29\\
&p(5) = 5^5 + 5 + 1 \equiv 2 \mod 29\\
&\vdots\\
&p(28) = 28^+ 28 + 1 \equiv 1 \mod 29\\
\Rightarrow &\nexists n \in \mathbb{Z}_2 9 : p(n) \equiv 0 \mod 29
\end{aligned}
$$

□

Problem b

Proof.

$$
\begin{aligned}
&f(x) = x^3 - a \\
&f(0) \equiv -a \mod 7 \\
&f(1) \equiv 1 - a \mod 7 \\
&f(2) \equiv 1 - a \mod 7 \\
&f(3) \equiv -1 - a \mod 7 \\
&f(4) \equiv 1 - a \mod 7 \\
&f(5) \equiv -1 - a \mod 7 \\
&f(6) \equiv -1 - a \mod 7 \\
&-a : \\
&a = 0 \implies -a \equiv 0 \mod 7 \\
&1 - a : \\
&a = 1 \implies 1 - a \equiv 0 \mod 7 \\
&-1 - a : \\
&a = -1 \implies -1 - a \equiv 0 \mod 7 \\
\Rightarrow &f(x) \text{ is reducable if } a = 0, \pm 1
\end{aligned}
$$

□

Problem c

$$
\begin{aligned}
&f(x) = x^5 + 1 \\
&f(0) \equiv 1 \mod 2 \\
&f(1) \equiv 0 \mod 2 \\
\Rightarrow &x - 1 \text{ is a factor} \\
&x^5 + 1 \equiv (x-1)(x^4 + x^3 + x^2 + x + 1) \mod 2 \\
&g(x) = x^4 + x^3 + x^2 + x + 1 \\
&g(0) \equiv 1 \mod 2 \\
&g(1) \equiv 1 \mod 2 \\
\Rightarrow &g(x) \text{ is irreducable} \\
\Rightarrow &x^5 + 1 \equiv (x+1)(x^4 + x^3 + x^2 + x + 1) \mod 2
\end{aligned}
$$

Question 4

Proof.

$$\begin{aligned}
&\phi : F \to R\\
&F, \{0\} \text{ are the only ideal in } F\\
&\Rightarrow \ker(\phi) = \{0\} \vee F\\
&\phi \text{ is not injective}\\
\Rightarrow &\ker(\phi) \neq \{0\}\\
\Rightarrow &\ker(\phi) = F\\
&\phi \text{ is trivial}
\end{aligned}$$

□

Question 5

Problem a

Proof.

$$
\begin{aligned}
&\phi(0) = 0 \in \phi[N] \\
&\forall r, s \in N \\
&r^{-1} \in N \\
&\phi(r)^{-1} = \phi(r^{-1}) \in \phi[N] \\
&r' \coloneqq \phi(r), s' \coloneqq \phi(s) \\
&\phi(r), \phi(s) \in \phi[N] \\
&\phi(r) + \phi(s) = \phi(r + s) \\
&r + s \in N \\
\Rightarrow &\phi(r + s) \in \phi[N] \\
&\phi(r) + \phi(s) \in \phi[N] \\
&\forall a \in R, \phi(a) \in \phi[R] \\
&\phi(a)\phi(r) = \phi(ar) \\
&N \text{ is an ideal} \\
&ar \in N \\
\Rightarrow &\phi(ar) \in \phi[N] \Rightarrow \qquad \phi[N] \text{ is an ideal of } \phi[R]
\end{aligned}
$$

□

Problem b

Proof.

$$
\begin{aligned}
&f : \mathbb{Z} \to \mathbb{Q} \\
&3\mathbb{Z} \text{ is an ideal in } \mathbb{Z} \\
&1 \notin 3\mathbb{Z} \implies 1 \notin f(3\mathbb{Z}) \\
&\frac{1}{3} \in \mathbb{Q} \\
&\frac{1}{3} \times 3 = 1 \in f(3\mathbb{Z}) \\
&1 \in f(3\mathbb{Z}) \not\Leftrightarrow 1 \notin f(3\mathbb{Z}) \\
\Rightarrow &f(3\mathbb{Z}) \text{ is not an ideal in } \mathbb{Q}
\end{aligned}
$$

□

Problem c

$$
\begin{aligned}
&0 \in N' \\
&\text{Only 0 maps to 0} \\
\Rightarrow &0 \in \phi^{-1}[N'] \\
&\forall r, s \in N' \\
&r^{-1} \in N' \\
\Rightarrow &\phi^{-1}(r^{-1}) \in \phi^{-1}[N'] \\
&r' \coloneqq \phi^{-1}(r), s' \coloneqq \phi^{-1}(s) \\
&\phi(r') = r, \phi(s') = s \\
&r', s' \in phi^{-1}[N'] \\
&\phi(r' + s') = \phi(r') + \phi(s') = r + s \in N' \\
\Rightarrow &r' + s' \in \phi^{-1}[N'] \\
&\forall a \in R \\
&\phi(ar') = \phi(a)r \\
&N' \text{ is an ideal}, \phi(a) \in \phi[R] \\
\Rightarrow &\phi(a)r \in N' \\
\Rightarrow &ar' \in \phi^{-1}[N'] \\
\Rightarrow &\phi^{-1}N' \text{ is an ideal in } R
\end{aligned}
$$

Question 6

Problem a

Proof.

$$
\begin{aligned}
&0 \in I, 0 \in J \\
\Rightarrow &0 \in I \cap J \\
&\forall a, b \in I \cap J \\
\Rightarrow &a, b \in I \wedge a, b \in J \\
&a^{-1} \in I, a^{-1} \in J \\
\Rightarrow &a^{-1} \in I \cap J \\
&a + b \in I, a + b \in J \\
\Rightarrow &a + b \in I + J \\
&\forall c \in R \\
&ac \in I, ac \in J \\
\Rightarrow &ac \in I \cap J \\
\Rightarrow &I \cap J \text{ is an ideal} \\
&K \text{ is a ideal contained in both } I \text{ and } J \\
&K \subset I \wedge K \subset J \\
\Rightarrow &K \subset I \cap J \\
&K \text{ is arbitrary} \\
\Rightarrow &I \cap J \text{ is the biggest ideal contained in } I \text{ and J}
\end{aligned}
$$

□

Problem b

$0 \in I, 0 \in J$

$\rightarrow 0 + 0 = 0 \in I + J$

$\forall a, b \in I, c, d \in J$

$a + c \in I + J$

$a^{-1} \in I, c^{-1} \in J$

$\Rightarrow a^{-1} + c^{-1} \in I + J$

$a^{-1} + c^{-1} = (a + c)^{-1}$

$(a + c)^{-1} \in I + J$

$a + c \in I + J, b + d \in I + J$

$(a + c) + (b + d) = (a + b) + (c + d)$

$a + b \in I, c + d \in J$

$\Rightarrow (a + b) + (c + d) \in I + J$

$a + c \in I + J, r \in R$

$r(a + c) = ra + rc$

$ra \in I, rc \in J$

$\Rightarrow ra + rc \in I + J$

$\Rightarrow I + J$ is an ideal

Let K be an ideal containing I and J

K is additively closed

$\Rightarrow I + J \subseteq K$ since this is the requirement for two ideals to be additively closed

$\Rightarrow I + J$ is the smallest ideal

Question 7

Problem a

$$
\begin{aligned}
&\forall n \in \mathbb{Z}_+, 0^n = 0\\
\Rightarrow &0 \in N\\
&\forall a, b \in N, \exists n, m \in \mathbb{Z}_+ : a^n = b^m = 0\\
&(-a)^n = (-1)^n \times a^n = -1^n \times 0 = 0\\
\Rightarrow &-a \in N\\
&(a+b)^{m+n} = \sum_k^{m+n} \binom{m+n}{k} a^k b^{m+n-k}\\
&\forall k \leqslant m+n : \begin{cases} k < n : b^{m+n-k} = 0 \\ k \geqslant n : a^k = 0 \end{cases}\\
\Rightarrow &\forall k \leqslant m+n \binom{m+n}{k} a^k b^{m+n-k} = 0\\
\Rightarrow &(a+b)^{m+n} = 0\\
&a+b \in N\\
&(ab)^n = a^n b^n\\
&a^n = 0\\
\Rightarrow &(ab)^n = 0\\
&ab \in N
\end{aligned}
$$

Problem b

Suppose $a + N$ is nilpotent

$\Rightarrow \exists n \in \mathbb{Z}_+ : (a + N)^n = 0 + N$

$(a + N)^n = a^n + N = 0 + N$

$\Rightarrow a^n$ is nilpotent

$\exists m : a^{nm} = a^{mn} = 0$

$\Rightarrow a$ is nilpotent

$a \in N$

$\Rightarrow a + N = 0 + N$

Question 8

Problem a

$$\begin{aligned}
&\text{Possible :}\\
&R = \langle 2\mathbb{Z}, +, \times\rangle\\
&\text{multiplication identity is } 1\\
&1 \notin 2\mathbb{Z}
\end{aligned}$$

Problem b

$$\begin{aligned}
&\text{Possible :}\\
&R = \langle \mathbb{Z}_6, +_6, \times_6\rangle\\
&1 \in \mathbb{Z}_6\\
&2 \times 3 \equiv 0 \mod 6\\
&2 \neq 0 \mod 6, 3 \neq 0 \mod 6
\end{aligned}$$

Problem c

$$\begin{aligned}
&\text{Possible :}\\
&R = \langle M_{2\times 2}(\mathbb{R}), +, \times\rangle\\
&\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} \neq \begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\\
&\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_{2\times 2}(\mathbb{R}) \text{ is the unit}
\end{aligned}$$

Problem d

$$\begin{aligned}
&\text{Possible :}\\
&R = \langle \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, +, \times \rangle\\
&\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\\
&\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin R
\end{aligned}$$

Problem e

$$\begin{aligned}
&\text{Not Possible :}\\
&R \text{ is a field}\\
\Rightarrow &\forall r, s \neq 0 \in R, \exists s \in R : rs \neq 0\\
&R \text{ is an integral domain}
\end{aligned}$$

Problem f

$$\begin{aligned}
&\text{Possible :}\\
&R = \langle \mathbb{Z}, +, \times \rangle\\
&\forall m, n \neq 0 \in R, mn \neq 0\\
&\forall p \in R, \nexists q \in R : pq = 1\\
\Rightarrow &R \text{ is not a field}
\end{aligned}$$

Problem g

$$
\begin{aligned}
&\text{Not Possible :}\\
&R \text{ is a finite integral domain}\\
&\forall n \in R :\\
&n^m \in R\\
&R \text{ is finite}\\
\Rightarrow &\exists p, q \in \mathbb{Z} : n^p = n^q\\
\Rightarrow &n^{p-q} = 1 \leftarrow \text{cancellation}\\
\Rightarrow &n^{p-q-1} \times n = 1\\
&n \text{ has an inverse}\\
\Rightarrow &R \text{ is a field}
\end{aligned}
$$

Reference

Jeffery Shu