Question 1

Problem a

Proof.

Additive identity :

$0 = 0 + 0\sqrt{3} \in S$

Inverse :

$\forall a + b\sqrt{3} \in S$

$x + a + b\sqrt{3} = 0$

$x = -a - b\sqrt{3} \in S$

Closure :

$\forall a + b\sqrt{3}, c + d\sqrt{3} \in S$

$a + b\sqrt{3} + c + d\sqrt{3} = (a + c) + (b + d)\sqrt{3}$

$a + c \in \mathbb{Z}, b + d \in \mathbb{Z}$

$\Rightarrow (a + c) + (b + d)\sqrt{3} \in S$

Commutative, associative and distributive hold under usual addition

Multiplication :

$x \coloneqq a + b\sqrt{3}$

$y \coloneqq c + d\sqrt{3}$

$xy = (a + b\sqrt{3})(c + d\sqrt{3})$

$xy = (ac + 3bd) + (ad + bc)sqrt3$

$ac + 3bd \in \mathbb{Z}, ad + bc \in \mathbb{Z}$

$\Rightarrow xy \in S$

$\square$

Problem b

Proof.

$$
\begin{aligned}
&x \coloneqq a + b\sqrt{3} \in S \\
&y \coloneqq 1 + \sqrt{3} \in S \\
&xy = 1 \\
&(a + b\sqrt{3})(1 + \sqrt{3}) = 1 \\
&(a + 3b) + (a + b)\sqrt{3} = 1 \\
\Rightarrow &\begin{cases} a + 3b = 1 \\ a + b = 0 \end{cases} \\
\Rightarrow &\begin{cases} a = 0 \\ b = \frac{1}{2} \end{cases} \\
&x = \frac{1}{2}\sqrt{3} \notin S \not\Leftrightarrow x \in S \\
\Rightarrow &S \text{ is not a field}
\end{aligned}
$$

□

Problem c

Proof.

$$
\begin{aligned}
&a + b\sqrt{3} = c + d\sqrt{3} \\
&(a - c) + (b - d)\sqrt{3} = 0 \\
&a, b, c, d \in \mathbb{Z} \\
\Rightarrow &a - c \text{ connot be irrational} \\
&(b - d)\sqrt{3} \text{ cannot be rational} \\
\Rightarrow &\begin{cases} a - c = 0 \\ b - d = 0 \end{cases} \\
\Rightarrow &\begin{cases} a = c \\ b = d \end{cases}
\end{aligned}
$$

□

Problem d

Proof.

$$
\begin{aligned}
&\text{Suppose } u, v \text{ are units}\\
&u \coloneqq a + b\sqrt{3}\\
&v \coloneqq c + d\sqrt{3}\\
&uv = 1\\
&(a + b\sqrt{3})(c + d\sqrt{3}) = 1\\
&(ac + 3bd) + (ad + bc)\sqrt{3} = 1\\
\Rightarrow &\begin{cases} ac + 3bd = 1 \\ ad + bc = 0 \end{cases}\\
&\text{Since } uv = 1, u \text{ is irrational}\\
&\text{Only the conjugate of } u \text{ can produce a rational number}\\
&\overline{u} = a - b\sqrt{3}\\
&\overline{v} = c - d\sqrt{3}\\
&u\overline{u}v\overline{v} = 1\\
&(a + b\sqrt{3})(a - b\sqrt{3})(c + d\sqrt{3})(c - d\sqrt{3}) = 1\\
&(a^2 - 3b^2)(c^2 - 3d^2) = 1\\
&a, b, c, d \in \mathbb{Z}\\
\Rightarrow &a^2 - 3b^2 = \pm 1
\end{aligned}
$$

□

Problem e

Proof.

surjective :

By construction, every matrix in R' has a number in S with the coresponding a and b

injective :

$\forall\phi(a+b\sqrt{3}) = \phi(c+d\sqrt{3})$

$\begin{bmatrix} a & 3b \\ b & a \end{bmatrix} = \begin{bmatrix} c & 3d \\ d & c \end{bmatrix} \in R'$:

$$\begin{cases} a = c \\ 3b = 3d \\ b = d \\ a = c \end{cases}$$

$$\Rightarrow \begin{cases} a = c \\ b = d \end{cases}$$

$\Rightarrow a+b\sqrt{3} = c+d\sqrt{3}$

Addition :

$\phi((a+b\sqrt{3})+(c+d\sqrt{3}))$

$=\phi((a+c)+(b+d)\sqrt{3})$

$= \begin{bmatrix} a+c & 3b+3d \\ b+d & a+c \end{bmatrix}$

$= \begin{bmatrix} a & 3b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 3d \\ d & c \end{bmatrix}$

$=\phi(a+b\sqrt{3})+\phi(c+d\sqrt{3})$

Multiplication :

$\phi((a+b\sqrt{3})(c+d\sqrt{3}))$

$=\phi((ac+3bd)+(ad+bc)\sqrt{3})$

$= \begin{bmatrix} ac+3bd & 3ad+3bc \\ ad+bc & ac+3bd \end{bmatrix}$

$\phi((a+b\sqrt{3}))\phi((c+d\sqrt{3}))$

$= \begin{bmatrix} a & 3b \\ b & a \end{bmatrix} \begin{bmatrix} c & 3d \\ d & c \end{bmatrix}$

$= \begin{bmatrix} ac+3bd & 3ad+3bc \\ ad+bc & ac+3bd \end{bmatrix}$

$=\phi((a+b\sqrt{3})(c+d\sqrt{3}))$

$\Rightarrow\phi$ is a ring homomorphism

$\square$

Question 2

Problem a

$$
\begin{aligned}
&\text{i :}\\
&\text{units are coprime to 15}\\
\Rightarrow &U_{\mathbb{Z}_15} = \{1, 2, 4, 7, 8, 11, 13, 14\}\\
&\text{ii :}\\
&\text{units are coprime to 11}\\
\Rightarrow &U_{\mathbb{Z}_11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}\\
&\text{iii :}\\
&\text{units of } \mathbb{Z} \text{ are } \pm 1\\
&\text{units of } \mathbb{Q} \text{ are } \mathbb{Q}*\\
&\text{units of } \mathbb{Z}_3 \text{ are coprime to 3}\\
\Rightarrow &U_{\mathbb{Z}\times\mathbb{Q}\times\mathbb{Z}_3} = \{x, y, z | x \in \{-1, 1\}, y \in \mathbb{Q}*, z \in \{1, 2\}\}
\end{aligned}
$$

Problem b

$$
\begin{aligned}
&\text{units are the ones having invertibles}\\
&(3^2 - 3^1)(3^2 - 1) = 48\\
\Rightarrow &48 \text{ units}
\end{aligned}
$$

Problem c

Proof.

$$\begin{aligned}
&\text{Id}:\\
&e_R \times e_R = e_R\\
\Rightarrow &e_R \in U\\
&\text{Inverse}:\\
&a \in U\\
&a \times a^{-1} = e_R\\
\Rightarrow &\forall a^{-1}, \exists a : a^{-1} \times a = e_R\\
&\text{Closure}:\\
&\forall a, b, c, d \in U : ac = bd = e_R\\
&acbd = (ab)(cd) = (cd)(ab) = e_R\\
\Rightarrow &ab \in U\\
\Rightarrow &U \text{ is a group}
\end{aligned}$$

□

Problem d

Proof.

$$\begin{aligned}
&\text{Suppose } a \text{ is both unit and zero divisor}\\
&\exists a^{-1}, b \neq 0 : a \times a^{-1} = 1 \wedge ab = 0\\
&a^{-1}ab\\
=&(a^{-1}a)b\\
=&b\\
&a^{-1}ab\\
=&a^{-1}(ab)\\
=&0\\
\Rightarrow &b = 0 \not\Leftrightarrow b \neq 0\\
\Rightarrow &\nexists a \text{ is both unit and zero divisor}
\end{aligned}$$

□

Problem e

Proof.

$$
\begin{aligned}
&a \neq 0, b \neq 0 \\
&ab = 1 \\
&bab = b \\
&babb^{-1} = bb^{-1} = 1 \\
\Rightarrow &ba = 1
\end{aligned}
$$

□

Question 3

Proof.

$$\begin{aligned}
&\text{If there is an isomorphism} \\
&\text{units are mapped to units} \\
&U_{\mathbb{Z}[x]} = \{-1, 1\} \\
&U_{\mathbb{Q}[x]} = \mathbb{Q}* \\
&\nexists \phi : \mathbb{Z}[x] \to \mathbb{Q}[x] : \phi : U_{\mathbb{Z}[x]} \to U_{\mathbb{Q}[x]} \text{ is bijective} \\
\Rightarrow &\nexists \phi : \mathbb{Z}[x] \to \mathbb{Q} \text{ as isomorphism}
\end{aligned}$$

□

Question 4

Problem a

$$
\begin{aligned}
&4 \times 10 \equiv 1 \mod 13 \\
\Rightarrow &10 \times 4x \equiv 20 \mod 13 \\
\Rightarrow &x \equiv 7 mod 13 \\
\Rightarrow &x = 7
\end{aligned}
$$

Problem b

$$
\begin{aligned}
&\gcd(4, 8) = 4 \\
\Rightarrow &\forall k \in \mathbb{Z}_8, \nexists 4k \equiv 2 \mod 8 \\
\Rightarrow &\text{no solution}
\end{aligned}
$$

Problem c

$$
\begin{aligned}
&x^2 + 4x - 2 \equiv x^2 + 4x + 4 \mod 6 \\
&x^2 + 4x - 2 = 0 \Leftrightarrow x^2 + 4x + 4 = 0 \\
&(x + 2)^2 = 0 \\
&x = -2 \\
\Rightarrow &x \equiv -2 \mod 6 \\
&x \equiv 4 \mod 6 \\
\Rightarrow &x = 4
\end{aligned}
$$

Problem d

$$
\begin{aligned}
& x^2 - 1 \equiv 0 \mod 8 \\
& (x-1)(x+1) \equiv 0 \mod 8 \\
& x - 1 \equiv 0, \pm 2, \pm 4 \mod 8 \\
& x \equiv 1, 3, -1, 5, -3 \mod 8 \\
& x + 1 \equiv 0, \pm 4, \pm 2 \mod 8 \\
& x \text{ must be the same in correspondence} \\
\Rightarrow & x \equiv -1, 3, -5, 1, -3 \mod 8 \\
\Rightarrow & x = 1, 3, 5, 7
\end{aligned}
$$

Problem e

$$
\begin{aligned}
& x^2 + 4x + 3 \equiv 0 \mod 15 \\
& (x+1)(x+3) \equiv 0 \mod 15 \\
& x + 1 \equiv 0, \pm 3, \pm 5 \mod 15 \\
& x \equiv -1, 2, -2, 4, -6 \mod 15 \\
& x + 3 \equiv 0, \pm 5, \pm 3 \mod 15 \\
& x \equiv -3, 2, -8, 0, -6 \mod 15 \\
& x \text{ must be the same in correspondence} \\
\Rightarrow & x \equiv -1, 2, -6, -3 \mod 15 \\
\Rightarrow & x = 2, 9, 12, 14
\end{aligned}
$$

Question 5

Problem a

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

Problem b

$$\begin{aligned}&\text{True}:\\&\forall n\geqslant 2:\\&\ \gcd(n,n)=n\\\Rightarrow&n\text{ is not coprime to }n\\&\text{There cannot be }n\text{ positive integers coprime to }n\\\Rightarrow&\phi(n)<n\forall n\geqslant 2\end{aligned}$$

Problem c

$$
\begin{aligned}
&textTrue: \\
&\text{Suppose}: \exists m, \gcd(m,n) \neq 1 : \exists k \in \mathbb{Z}_n : km \equiv 1 \mod n \\
&p \coloneqq \gcd(m,n) \\
\Rightarrow &\exists g, h \in \mathbb{Z} : m = gp, n = hp \\
&km \equiv 1 \mod n \\
\Rightarrow &\exists q \in \mathbb{Z} : km = qn + 1 \\
&kgp = qhp + 1 \\
&p(kg - qh) = 1 \\
\Rightarrow &p = 1 \not\Leftrightarrow \gcd(m,n) \neq 1 \\
\Rightarrow &\text{Units are all numbers coprime to } n
\end{aligned}
$$

Problem d

$$
\begin{aligned}
&\text{True}: \\
&\forall a, b \in U_n \\
&a \times a^{-1} \equiv 1 \mod n \\
\Rightarrow &\exists p \in \mathbb{Z} : a \times a^{-1} \equiv pn + 1 \\
&b \times b^{-1} \equiv 1 \mod n \\
\Rightarrow &\exists q \in \mathbb{Z} : b \times b^{-1} \equiv qn + 1 \\
&a \times a^{-1} \times b \times b^{-1} = a \times b \times a^{-1} \times b^{-1} \\
= &(pn + 1)(qn + 1) \\
= &(pqn + p + q)n + 1 \\
\equiv &1 \mod n \\
\Rightarrow &(a \times b) \times (a^{-1} \times b^{-1}) \equiv 1 \mod n \\
\Rightarrow &\forall a, b \in U_n, a \times b \in U_n
\end{aligned}
$$

Problem e

$$
\begin{aligned}
&\text{True :}\\
&\text{Suppose } \exists a, b \in \mathbb{Z}_n :\\
&\ \gcd(a,n) \neq 1, \gcd(b,n) \neq 1 : ab \equiv 1 \mod n\\
&\exists g : ab = gn + 1\\
&p \coloneqq \gcd(a,n)\\
&\exists k : a = kp\\
&q \coloneqq \gcd(b,n)\\
&\exists l : b = lp\\
&ab = klp^2\\
&\ \gcd(klp^2, n) \geqslant p\\
&\ \gcd(gn+1, n) = 1\\
\Rightarrow &\gcd(ab,n) \geqslant p \not\Leftrightarrow \gcd(ab,n) = 1\\
\Rightarrow &\text{Product of two non-units is a non-unit}
\end{aligned}
$$

Problem f

$$
\begin{aligned}
&\text{True :}\\
&\text{Suppose } \exists a, b \in \mathbb{Z}_n :\\
&b \in U_n, \gcd(a,n) \neq 1, ab \equiv 1 \mod n\\
&\exists g : ab = gn + 1\\
&p \coloneqq \gcd(a,n)\\
&\exists k : a = kp\\
&ab = kpb\\
&\ \gcd(kpb, n) = p\\
&\ \gcd(gn+1, n) = 1\\
\Rightarrow &\gcd(ab,n) = p \not\Leftrightarrow \gcd(ab,n) = 1\\
\Rightarrow &\text{Product of a non-unit and a unit is a non-unit}
\end{aligned}
$$

Question 6

i :

$\forall (a,b) \neq (0,0) \in \mathbb{Z} \times \mathbb{Q}$:

Suppose $\exists n \neq 0 : n(a,b) = (0,0)$

$\Rightarrow (na, nb) = (0,0)$

$$\begin{cases} na = 0 \\ nb = 0 \end{cases}$$

$\Rightarrow a = 0, b = 0 \not\Leftrightarrow (a,b) \neq (0,0)$

$\Rightarrow \text{char}(\mathbb{Z} \times \mathbb{Q}) = 0$

ii :

$\forall (a,b) \neq (0,0) \in \mathbb{Z}_4 \times \mathbb{Z}_5$:

Suppose $\exists n \neq 0 : n(a,b) = (0,0)$

$$\Rightarrow \begin{cases} na \equiv 0 \mod 4 \\ nb \equiv 0 \mod 5 \end{cases}$$

$\Rightarrow n = 20$

$\text{char}(\mathbb{Z}_4 \times \mathbb{Z}_5) = 20$

iii :

$\forall (a,b) \neq (0,0) \in \mathbb{Z}_4 \times \mathbb{Z}_6$:

Suppose $\exists n \neq 0 : n(a,b) = (0,0)$

$$\Rightarrow \begin{cases} na \equiv 0 \mod 4 \\ nb \equiv 0 \mod 6 \end{cases}$$

$\Rightarrow n = 12$

$\text{char}(\mathbb{Z}_4 \times \mathbb{Z}_6) = 12$

Question 7

$$\begin{aligned}
&\mathrm{ord}\mathbb{Z}_{13}^{*} = 12\\
\Rightarrow &\exists a \neq 1 \in \mathbb{Z}_{13}^{*}, \gcd(a,13) = 1 : \mathrm{ord}(a) = 12\\
&a^{13} \equiv a \mod 13\\
\Rightarrow &a^{12} \equiv 1 \mod 13\\
&\forall 1 \leqslant m < n \leqslant 12 \in \mathbb{Z} :\\
&\text{Suppose} a^{m} \mod 13 = a^{n} \mod 13\\
\Rightarrow &a^{m}(a^{n-m} - 1) \equiv 0 \mod 13\\
&a^{n-m} - 1 \equiv 0 \mod 13\\
\Rightarrow &n - m = 12 \not\Leftrightarrow 1 \leqslant m < n \leqslant 12\\
\Rightarrow &\forall 1 \leqslant m < n \leqslant 12 \in \mathbb{Z} : a^{m} \mod 13 \neq a^{n} \mod 13\\
\Rightarrow &\langle a \rangle \text{ generates the whole group}\\
&\mathbb{Z}_{13}^{*} \text{ is cyclic}
\end{aligned}$$

Question 8

$$S \coloneqq \langle m \rangle \text{ is a subring of } \mathbb{Z}_n$$
$$S \text{ must be a subgroup}$$
$$\mathrm{ord}(S) = 2$$
$$\Rightarrow S = \{0, m\}$$
$$m + m \equiv 0 \mod n$$
$$\Rightarrow n = 2m$$
$$S \text{ is a subring}$$
$$\Rightarrow m^2 \mod n \in S$$
$$textcase1 :$$
$$m^2 \equiv 0 \mod n$$
$$\Rightarrow \exists k \in \mathbb{Z}_+ : m^2 = 2km$$
$$m = 2k$$
$$\text{case } 2 :$$
$$m^2 \equiv m \mod n$$
$$\Rightarrow \exists k \in \mathbb{Z}_+ : m^2 = 2km + m$$
$$m = 2k + 1$$
$$\Rightarrow \text{ There is no restriction on } m$$
$$\Rightarrow \forall n = 2m, m \in \mathbb{Z}_+, \mathbb{Z}_n \text{ contains a subring of order } 2 : \langle m \rangle$$

Question 9

$$
\begin{aligned}
&\forall f(x), g(x) \in R:\\
&\Phi(f+g)(x)\\
=&(f+g)'(x)\\
=&f'(x)+g'(x)\\
=&\Phi(f)(x)+\Phi(g)(x)\\
\Rightarrow&\text{homomorphism stands}\\
&\Phi(fg)(x)\\
=&(fg)'(x)\\
=&f'g(x)+fg'(x)\\
&\Phi(f)\Phi(g)(x)=f'g'(x)\\
\Rightarrow&\Phi(fg)x \neq \Phi(f)\Phi(g)x\\
\Rightarrow&\Phi \text{ is not ring homomorphism}
\end{aligned}
$$

Reference

Jeffery Shu