Problem 1 [3pts] Define a ring R.

We say R is a ring iff R is a set equipt with two binary operations $(+)$ and $(\cdot)$ such that

(1.) $\langle R, + \rangle$ forms an abelian group

(2.) $(\cdot)$ obeys distributive laws that follow: for all $a, b, c \in R$

(i.) $a \cdot (b + c) = a \cdot b + a \cdot c$

(ii) $(a + b) \cdot c = a \cdot c + b \cdot c$

(3.) $\langle R, \cdot \rangle$ is associative; $a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in R$.

Problem 2 [15pts] Prove either a, b or c of the following:

a. If R is a ring with additive identity 0, then for any $a, b \in R$ we have

1. $0a = a0 = 0$
2. $a(-b) = (-a)b = -(ab)$

b. Every **finite** integral domain is a field.

c. An element $a \in F$ is a zero of $f(x) \in F[x]$ iff if $x - a$ is a factor of $f(x)$ in $F[x]$.

See text.

Problem 3 [4pts] Is $f(x) = x^3 + 3x^2 - 8$ irreducible over $\mathbb{Q}$? Is $f(x)$ irreducible over $\mathbb{R}$ (you may use calculus to answer this).

Use Eisenstein criteria $p = 3$. Notice $1 \not\equiv 0 \mod(3)$ and $-8 \not\equiv 0 \mod(3^2)$ however $3 \equiv 0 \mod(3)$. Hence $f(x) = x^3 + 3x^2 - 8$ irred. over $\mathbb{Q}$ by Eisenstein's Criteria.

Every cubic has a zero over $\mathbb{R}$. Observe $f(x)$ is continuous. Furthermore, $f(0) = -8$ while $f(2) = 8 + 12 - 8 = 12$. Thus, by mean value Th^{m}, $\exists\, c \in (0, 2)$ s.t. $f(c) = 0$. This demonstrates $f(x)$ will factor over $\mathbb{R}$.

Problem 5 [4pts] Let F be a field. If $f(x) \in F[x]$ is a polynomial of degree 5 such that $f(x)$ has no irreducible factors of degree 3 or 4 then **is $f(x)$ is irreducible ?** If this is only sometimes true explain when and why with an example or two.

If $f(x)$ is irreducible it does not factor thus it will be irreducible (and have no irred. factors of degree 3 or 4). Take $f(x) = x^5 + 4$ in $\mathbb{Q}[x]$, this is irred. by Eisenstein's Criteria (take $p = 3$).

However, it is possible to have $f(x) = x^5$ and this has no irreducible factors of degree 3 or 4 yet it is clearly <u>not</u> irreducible. $f(x) = f_1(x) f_2(x) f_3(x) f_4(x) f_5(x)$ where $f_i(x) = x \quad \forall\, i = 1, 2, 3, 4, 5$. That is $f(x)$ can be <u>factored</u>. (this works for any field F)

Problem 4 [4pts] Let R be a ring with unity 1 and $r \in R$. Show that r cannot be both a zero divisor and a unit.

Suppose $r \in R$ is a <u>unit</u>, it follows $\exists\, r^{-1} \in R$ such that $rr^{-1} = r^{-1}r = 1$. Additionally, suppose r is a <u>zero divisor</u>, then $\exists\, b \in R$ such that $b \neq 0$ and $r \neq 0$ yet $br = 0$. Consider,

$$rr^{-1} = 1 \implies brr^{-1} = b \implies 0r^{-1} = b$$
$$\implies 0 = b$$

This is a contradiction with $b \neq 0$. Hence r cannot be both a unit and a zero divisor.

Problem 5 [4pts] Let R be a ring where $a^2 = a$ for each $a \in R$. Show that R is commutative. *Hint:* For all $a, b \in R$, $(a+b)^2 = (a+b)$ and $(a+a)^2 = a+a$.

Proof: Let $a, b \in R$. Observe $(a+b), (a+a) \in R$ since $(+)$ is closed. Since we assume $x^2 =$ for each $x \in R$ it follows,

$$(a+a)^2 = a+a \Rightarrow a^2+a+a+a^2 = a+a$$
$$\Rightarrow a^2+a^2 = 0$$
$$\Rightarrow a+a = 0$$
$$\Rightarrow \underline{a = -a} \quad \text{likewise } \underline{b = -b}.$$

Consider then,

$$(a+b)^2 = a+b \Rightarrow a^2+ab+ba+b^2 = a+b$$
$$\Rightarrow a+ab+ba+b = a+b$$
$$\Rightarrow ab+ba = 0$$
$$\Rightarrow ab = -ba = ba$$

Thus $\forall a, b \in R$, $ab = ba$. <u>R is commutative</u>.

Problem 6 [4pts] Let $\phi : R \to S$ be a homomorphism from a ring R to a ring S. Also, suppose T is a subring of R. Prove that $\phi[T]$ is a subring of S.

Let $a, b \in \phi[T]$ then $\exists x, y \in T$ such that $\phi(x) = a$ and $\phi(y) = b$. Moreover, since $T < R$, $(y-x) \in T$. Observe that since ϕ is a homomorphism,

$$\phi(y) - \phi(x) = \phi(y-x) \in \phi[T] \quad (\text{using } (y-x) \in T)$$

Hence, $(b-a) \in \phi[T]$. We also have $xy \in T$ since $T < R$. Consider then that

$$\phi(x)\phi(y) = \phi(xy) \in \phi[T].$$

Finally $\phi(0) = 0$ thus $\phi[T] \neq \emptyset$. Thus we have found $a, b \in \phi[T] \Rightarrow ab, (b-a), 0 \in \phi[T]$

Hence $\phi[T] < S$ by subring test.

Problem 7 [8pts] Consider the following questions in $\mathbb{Z}_9$,

a. Write out the multiplication table for $\mathbb{Z}_9$

b. List all members of $U(\mathbb{Z}_9)$

c. List all zero divisors in $\mathbb{Z}_9$

d. Is $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ a unit in $M_2(\mathbb{Z}_9)$.

a.)

$\cdot$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

b.) $\boxed{U(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}}$

We can see from table $1^{-1} = 1$, $2^{-1} = 5$, $4^{-1} = 7$
$5^{-1} = 2$, $7^{-1} = 4$, $8^{-1} = 8$.

c.) Since $3 \cdot 6 = 0$ we find $\boxed{\text{3 and 6 are zero divisors}}$

d.)
$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} = (4-6)^{-1} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$$
$$= (-2)^{-1} \begin{bmatrix} 4 & 7 \\ 6 & 1 \end{bmatrix}$$
$$= 7^{-1} \begin{bmatrix} 4 & 7 \\ 6 & 1 \end{bmatrix} = 4 \begin{bmatrix} 4 & 7 \\ 6 & 1 \end{bmatrix} = \begin{bmatrix} 16 & 28 \\ 24 & 4 \end{bmatrix}$$
$$= \begin{bmatrix} 7 & 1 \\ 6 & 4 \end{bmatrix}$$

Clearly $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 7 & 1 \\ 6 & 4 \end{bmatrix} \overset{*}{=} \begin{bmatrix} 19 & 9 \\ 45 & 19 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $\therefore$ $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ is unit.

Problem 8 [2pts] Is $\mathbb{Q}$ isomorphic to $\mathbb{Z}$? Why or why not?

Suppose $\psi : \mathbb{Q} \longrightarrow \mathbb{Z}$ was a bijection. Notice

$\psi(xx^{-1}) = \psi(x)\psi(x^{-1}) = \psi(1) = 1 \quad \therefore \psi(x)^{-1} = \psi(x^{-1})$

We know ψ takes units to units. We find $\nexists\ \psi$ since the number of units in $\mathbb{Z}$ is two, yet $\mathbb{Q}$ has ∞ly many units. (there are other arguments)

Problem 9 [4pts] Is $M_2(\mathbb{Z}_2)$ isomorphic to $\mathbb{Z}_{16}$? Why or why not?

If these were isomorphic they would have the same characteristic. Notice

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \therefore \quad \mathrm{char}(M_2(\mathbb{Z}_2)) = 2.$$

$$\underbrace{1 + 1 + \cdots + 1}_{16} = 16 = 0 \quad \therefore \quad \mathrm{char}(\mathbb{Z}_{16}) = 16.$$

Or, we could count units and compare,

$$\mathcal{U}(\mathbb{Z}_{16}) = \{1, 3, 5, 7, 9, 11, 13, 15\} \qquad \underline{8 \text{ units in } \mathbb{Z}_{16}}$$

In contrast,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad \underline{6 \text{ units in } M_2(\mathbb{Z}_2)}.$$

Thus $M_2(\mathbb{Z}_2) \not\cong \mathbb{Z}_{16}$. (same idea as Problem 8)

Finally, $\exists\, a, b \in M_2[\mathbb{Z}_2]$ such that $ab \neq ba$ (see ✱) yet $\nexists\ x, y \in \mathbb{Z}_{16}$ such that $xy \neq yx$.

Isomorphism preserves commutivity $\therefore$ these are not isomorphic. To be precise if $\psi : M_2(\mathbb{Z}_2) \longrightarrow \mathbb{Z}_{16}$,

$$\psi(ab) = \underbrace{\psi(a)\psi(b) = \psi(b)\psi(a)}_{\text{in } \mathbb{Z}_{16} \text{ we can commute}} = \psi(ba)$$

(✱) Note $a = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ has

$$ab = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \text{ whereas } ba = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

oops. I meant to put $\mathbb{R}\times\mathbb{R}$ so you'd see to use the product ring construction.

Problem 10 [4pts] Is $\mathbb{R}^2$ isomorphic to real diagonal matrices in $D \subset M_2(\mathbb{R})$? Why or why not? Here

$$D = \{A \in M_2(\mathbb{R}) \mid A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \; a, b \in \mathbb{R}\}$$

should be given the usual ring structure for matrices.

Let $\varphi(a,b) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Observe $\varphi^{-1}\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = (a,b)$ and if $A = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \in D$ clearly $\varphi(x,y) = A \therefore \varphi$ is a bijection. $M_2(\mathbb{R})$ is a ring w.r.t matrix operations, On the other hand, $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$ is a <u>product ring</u> where

$$(a,b) + (c,d) = (a+c, b+d)$$
$$(a,b)\cdot(c,d) = (ac, bd)$$

$\forall (a,b), (c,d) \in \mathbb{R}\times\mathbb{R}$. We seek to show φ preserves the ring structure, let $(a,b), (c,d) \in \mathbb{R}\times\mathbb{R}$

$$\varphi((a,b)+(c,d)) = \varphi((a+c, b+d)) = \begin{pmatrix} a+c & 0 \\ 0 & b+d \end{pmatrix}$$

$$\varphi((a,b)) + \varphi((c,d)) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a+c & 0 \\ 0 & b+d \end{pmatrix}$$

Thus $\underline{\varphi((a,b)+(c,d)) = \varphi((a,b)) + \varphi((c,d))}$. Moreover,

$$\varphi((a,b)\cdot(c,d)) = \varphi((ac, bd)) = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}.$$

$$\varphi((a,b))\cdot\varphi((c,d)) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}.$$

Thus $\underline{\varphi((a,b))\cdot\varphi((c,d)) = \varphi((a,b)\cdot(c,d))}$.

We find φ is a ring isomorphism.

Problem 11 [4pts] List all of the monic polynomials of degree 2 in $\mathbb{Z}_3[x]$. Circle all of the irreducible polynomials in your list.

Looking for $f(x) = x^2 + bx + c$ where $b, c \in \mathbb{Z}_3$

	$f_i(0)$	$f_i(1)$	$f_i(2)$
$f_1(x) = x^2$	0	1	1
$f_2(x) = x^2 + 1$	1	2	2
$f_3(x) = x^2 + 2$	2	0	0
$f_4(x) = x^2 + x$	0	2	0
$f_5(x) = x^2 + 2x$	0	0	2
$f_6(x) = x^2 + x + 1$	1	0	1
$f_7(x) = x^2 + x + 2$	2	1	2
$f_8(x) = x^2 + 2x + 1$	1	1	0
$f_9(x) = x^2 + 2x + 2$	2	2	1

No zeros $\Rightarrow$ no factors $(x - \alpha)$ $\Rightarrow$ irreducible.

Problem 12 [4pts] Suppose a ring R is isomorphic to $2\mathbb{Z}$ and another ring T is isomorphic to $3\mathbb{Z}$. Show that R is not isomorphic to T. (Do not assume that $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.)

<u>Idea</u>: use my diagramatic argument from homework piggy-backed onto the isomorphisms given implicitly by this problem. Suppose $R \underset{\varphi}{\approx} T$, $2\mathbb{Z} \underset{\psi_R}{\approx} R$, $3\mathbb{Z} \underset{\psi_T}{\approx} T$,

$$2\mathbb{Z} \xleftrightarrow{\psi_R} R \xleftrightarrow{\varphi} T \xleftrightarrow{\psi_T} 3\mathbb{Z}$$

Notice it follows $\psi_T \circ \varphi \circ \psi_R : 2\mathbb{Z} \to 3\mathbb{Z}$ is an isomorphism since ψ_T, ψ_R are given and we are assuming φ is isomorphism.

But, we can prove $2\mathbb{Z} \not\approx 3\mathbb{Z} \Rightarrow \varphi$ an isomorphism does not exist and hence $R \not\approx T$.

Let me redo the hwk. problem here.

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\gamma_2"] \arrow[d, "\pi_2"'] & 2\mathbb{Z} \arrow[r, "\psi_R"] & R \arrow[r, "\phi"] & T \arrow[r, "\psi_T"] & 3\mathbb{Z} & \mathbb{Z} \arrow[l, "\gamma_3"'] \arrow[d, "\pi_3"] \\
\mathbb{Z}/\mathrm{Ker}\,\gamma_2 \arrow[ur, dashed, "\psi_2"'] \arrow[rrr, "\underbrace{\psi_3^{-1} \circ \psi_T \circ \phi \circ \psi_R \circ \psi_2}_{\text{Composition of isomorphisms if } R \underset{\phi}{\approx} T.}"'] & & & & & \mathbb{Z}/\mathrm{Ker}\,\gamma_3 \arrow[ul, dashed, "\psi_3"]
\end{tikzcd}$$

This would show $\mathbb{Z}_2 \approx \mathbb{Z}_3$ which is clearly false.