This exam contains 8 pages (including this cover page) and 7 questions. The total of points one can obtain is 28. Questions 6 and 7 are considered as BONUS problems.

This is NOT an open book and notes exam. Phones and calculators are NOT allowed. Show all your work (no work = no credit). Write neatly. Simplify your answers.

### Grade Table (for teacher use only)

<table>
<thead>
<tr>
<th>Question</th>
<th>Points</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Total:</td>
<td>28</td>
<td>28/20</td>
</tr>
</tbody>
</table>

Good luck !!!
1. (4 points) (a) Give the definition of the following notions: ring and field. (b) Show that $\mathbb{Q}(\sqrt{7})$ is a field. You may use the fact that $\mathbb{Q}(\sqrt{7}) \subset \mathbb{R}$ and $\mathbb{R}$ is a ring.

(a) A ring $R$ equipped with two operations "+" and "\cdot" is the set $R$ such that $(R, +)$ is an Abelian group and the following four ring axioms are satisfied, for any elements $a, b, c$ in $R$:

1. $(R, +)$ is an Abelian group
2. Closure: $a + b \in R$
3. Associativity: $a(bc) = (ab)c$
4. Distributivity: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$

A field $F$ is a ring such that it satisfies the following:

4. $F$ is commutative
5. $F$ has unity
6. Every nonzero element in $F$ is a unit.

(b) We know that $\mathbb{R}$ is a ring! We only need to show that $\mathbb{Q}(\sqrt{7}) \subset \mathbb{R}$ is a subring of $\mathbb{R}$ such that every element has an inverse in $\mathbb{Q}(\sqrt{7})$. Let $x = a + b\sqrt{7}$, and $y = c + d\sqrt{7}$, with $x, y \in \mathbb{Q}(\sqrt{7})$.

- **Closure under addition**: $x + y = (a + c) + (b + d)\sqrt{7} \in \mathbb{Q}(\sqrt{7})$
  since $a + c$ and $b + d$ are in $\mathbb{Q}$.
- **Closure under multiplication**: $x \cdot y = (a + b\sqrt{7})(c + d\sqrt{7}) = ac + ad\sqrt{7} + bc\sqrt{7} + bd\sqrt{7} \in \mathbb{Q}(\sqrt{7})$, since $ac + bd$ and $ad + bc$ are both in $\mathbb{Q}$. 
- additive identity: 0 = 0 + 0 \cdot \sqrt{7} \in \mathbb{Q}(\sqrt{7})
- multiplicative identity: 1 = 1 + 0 \cdot \sqrt{7} \in \mathbb{Q}(\sqrt{7})
- additive inverse: -a - b\sqrt{7} is in \mathbb{Q}(\sqrt{7}), since -a, b \in \mathbb{Q}.

\[ \frac{-a}{a^2 - 7b^2} + \frac{-b}{a^2 - 7b^2} e \in \mathbb{Q}. \]

Thus \( \mathbb{Q}(\sqrt{7}) \) is a field. \( \Box \)
2. (4 points) Find all units, zero-divisors, idempotents and nilpotents in $\mathbb{Z}_{12}$.

**Units:** \( \{1, 5, 7, 11\} \) in $\mathbb{Z}_{12}$

Indeed, 1 divides itself, so 1 is always a unit. Next, \( 5 \cdot 5 = 25 = 1 \pmod{12} \), \( 7 \cdot 7 = 49 = 1 \pmod{12} \), and \( 11 \cdot 11 = 121 = 1 \pmod{12} \).

**Zero-Divisors:** \( \{2, 3, 4, 6, 8, 9, 10\} \) in $\mathbb{Z}_{12}$

Indeed, \( 2 \cdot 6 = 12 = 0 \pmod{12} \). Also, we have \( 8 \cdot 9 = 72 = 0 \pmod{12} \), and \( 10 \cdot 6 = 60 = 0 \pmod{12} \).

**Idempotents:** \( \{0, 1, 4, 9\} \) in $\mathbb{Z}_{12}$

Indeed, one can check that \( 0^2 = 0 \), \( 1^2 = 1 \), \( 2^2 = 4 \), \( 3^2 = 9 \), \( 4^2 = 16 = 4 \pmod{12} \), \( 5^2 = 25 = 1 \pmod{12} \), \( 6^2 = 36 = 0 \pmod{12} \), \( 7^2 = 49 = 1 \pmod{12} \), \( 9^2 = 81 = 9 \pmod{12} \), \( 10^2 = 100 = 4 \pmod{12} \), and \( 11^2 = 121 = 1 \pmod{12} \).

**Nilpotents:** \( \{0, 6\} \) in $\mathbb{Z}_{12}$

Clearly, 0 is nilpotent, and \( 6^2 = 36 = 0 \pmod{12} \).
3. (4 points) (a) Find all prime and maximal ideals in the ring \( \mathbb{Z}_{12} \). (b) Find all ring homomorphisms from \( \mathbb{Z}_{12} \) to \( \mathbb{Z}_{12} \).

(a) The positive divisors of 12 are 1, 2, 3, 4, 6, 12. So, the ideals in \( \mathbb{Z}_{12} \) are

\[
\begin{align*}
(1) &= \mathbb{Z}_{12}, \\
(2) &= \{0, 2, 4, 6, 8, 10\}, \\
(3) &= \{0, 3, 6, 9\}, \\
(4) &= \{0, 4, 8\}, \\
(6) &= \{0, 6\} \text{ and } (12) = \{0\} \quad \text{(trivial ideal)}
\end{align*}
\]

Clearly, (1) and (12) are improper ideals. Also, we have

\[
\begin{align*}
(12) &= (6) \\
(12) &= (6) \\
(12) &= (6) \\
(12) &= (6)
\end{align*}
\]

This implies that (2) and (3) are prime and maximal ideals.

(b) Any ring homomorphism \( \phi: \mathbb{Z}_{12} \to \mathbb{Z}_{12} \) satisfies the following conditions:

(i) \( \phi(a+b) = \phi(a) + \phi(b), \quad \forall a, b \in \mathbb{Z}_{12} \)

(ii) \( \phi(ab) = \phi(a) \cdot \phi(b), \quad \forall a, b \in \mathbb{Z}_{12} \)

From (i), we know that \( \phi(a) = a \cdot \phi(1) \), and from (ii) \( \phi(1) = \phi^2(1) \), which implies that \( \phi^2(1) - \phi(1) = 0 \) in \( \mathbb{Z}_{12} \).

Denote \( \phi(1) = x \), and thus \( x^2 = x \) in \( \mathbb{Z}_{12} \). We need to find the idempotents in \( \mathbb{Z}_{12} \). This implies that \( x \in \{0, 1, \hat{1}, \hat{2}\} \). Therefore, the ring homomorphisms from \( \mathbb{Z}_{12} \) to \( \mathbb{Z}_{12} \) are given by
\( \phi(a) = 0 \pmod{12}, \)
\( \phi(a) = a \pmod{12} \)
\( \phi(a) = 4a \pmod{12} \)
\( \phi(a) = 9a \pmod{12}, \) and we are done. \( \square \)
4. (4 points) Let \((\mathbb{C}, +, \cdot)\) be the ring of complex numbers, and \((\mathbb{S}, +, \cdot)\) be the ring of two by two complex matrices together with matrix addition and multiplication. Here \(\mathbb{S}\) denotes the set \(\mathbb{S} = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{C} \right\}\). Show that the map \(\phi : \mathbb{C} \to \mathbb{S}\) defined by
\[
\phi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}
\]
is a ring homomorphism.

Let \(z_1 = a + b \cdot i\) and \(z_2 = c + d \cdot i\) be two complex numbers. Since
\[
\phi(z_1 + z_2) = \phi(a + b \cdot i + c + d \cdot i) = \phi(a + c + (b + d) \cdot i) =
\begin{bmatrix} a + c & b + d \\ -b - d & a + c \end{bmatrix} =
\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \phi(a + b \cdot i) + \phi(c + d \cdot i) = \phi(z_1) + \phi(z_2).
\]

Also,
\[
\phi(z_1 z_2) = \phi((a + bi)(c + di)) = \phi(ac - bd + (ad + bc) \cdot i) = \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix} =
\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \phi(a + bi) \cdot \phi(c + di) = \phi(z_1) \cdot \phi(z_2).
\]

Therefore, the map \(\phi : \mathbb{C} \to \mathbb{S}\), \(\phi(a + b \cdot i) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\) is an homomorphism. \(\Box\)
5. (4 points) Show that the rings \( \mathbb{Q}(\sqrt{2}) \) and \( \mathbb{Q}(\sqrt{3}) \) are not isomorphic.

Assume that there exists an isomorphism, \( \phi: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3}) \). Note that any homomorphism between the fields \( \mathbb{Q} \) and \( \mathbb{Q} \) fixes \( \mathbb{Q} \) pointwise. In other words, \( \phi(x) = x \), for all \( x \in \mathbb{Q} \).

Since \( \phi \) fixes the elements of \( \mathbb{Q} \), we have

\[
2 = \phi(2) = \phi((\sqrt{2})^2) = \phi(\sqrt{2})^2 = (a + b\sqrt{3})^2,
\]

since \( \phi(\sqrt{2}) = a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3}) \) for some \( a, b \in \mathbb{Q} \).

This implies that

\[
2 = \phi(2) = a^2 + 3b^2 + 2ab\sqrt{3}, \text{ which will give us}
\]

\[
\begin{cases}
  a^2 + 3b^2 = 2 \\
  2ab = 0
\end{cases}
\]

From the second equality, we have \( a = 0 \) or \( b = 0 \). If \( a = 0 \), then \( 3b^2 = 2 \), and \( b = \pm \sqrt{\frac{2}{3}} \notin \mathbb{Q} \), contradiction. Hence \( a \neq 0 \) and \( b = 0 \). But, in this case \( 2 = a^2 \), which implies \( a = \pm \sqrt{2} \notin \mathbb{Q} \), contradiction again!

Therefore, there does not exist an isomorphism \( \phi: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3}) \) and we are done. \( \square \)
6. (4 points) An element $a$ in a ring $R$ is called **idempotent** if $a^2 = a$ for all $a \in R$.

(a) Prove that the only idempotents in an integral domain are 0 and 1.

(b) If the ring $R$ is commutative and $a \in R$ is an idempotent, then show that $1 - a$ is also an idempotent.

(a) Let us consider the element $a$ in $R$ such that $a^2 = a$. Then $a^2 - a = 0$ or $a(a-1) = 0$. Since there are no zero divisors in an integral domain, it follows that $a = 0$ or $a - 1 = 0$, or equivalently $a = 0$ or $a = 1$.

(b) Let $a \in R$ be an idempotent, i.e. $a^2 = a$. Now, we compute

\[
(1-a)^2 = 1 - 2a + a^2 = 1 - 2a + a = 1 - 2a + a = 1 - a. 
\]

Thus, $1-a$ is also an idempotent. $\square$
7. (4 points) Let \( R = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} ; a, b \in \mathbb{Q} \right\} \). One can prove that \( R \) with the usual matrix addition and multiplication is a ring. Consider \( J = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} ; b \in \mathbb{Q} \right\} \) be a subset of the ring \( R \).

(a) Prove that the subset \( J \) is an ideal of the ring \( R \);

(b) Prove that the quotient ring \( R/J \) is isomorphic to \( \mathbb{Q} \).

(a) Let \( \alpha = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} \) and \( \beta = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \) be arbitrary elements in \( J \), with \( a, b \in \mathbb{Q} \). Then, since we have

\[
\alpha + \beta = \begin{bmatrix} 0 & a+b \\ 0 & 0 \end{bmatrix} \in J,
\]

the subset \( J \) is an additive group. Now, consider the elements

\[
\gamma = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in J \quad \text{and} \quad \delta = \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix} \in J.
\]

Then, we have

\[
\gamma \delta = \begin{bmatrix} 0 & ac \\ 0 & 0 \end{bmatrix} \in J \quad \text{and} \quad \delta \gamma = \begin{bmatrix} 0 & ca \\ 0 & 0 \end{bmatrix} \in J.
\]

Thus, each element of \( J \) multiplied by an element of \( R \) is still in \( J \). Hence \( J \) is an ideal of the ring \( R \).

(b) Consider the map \( \phi : R \to \mathbb{Q} \) defined by

\[
\phi \left( \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \right) = a, \quad \text{for} \quad \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in R.
\]

Firstly, we show that \( \phi \) is a ring homomorphism.
We have $\phi([1,0,0]) = 1$. Thus $\phi$ maps the unity element of $R$ to the unity element of $Q$.

Now, take
\[
\begin{bmatrix}
a & b \\
0 & a
\end{bmatrix}, \begin{bmatrix}
c & d \\
0 & c
\end{bmatrix} \in R.
\]

Then, we have
\[
\phi\left(\begin{bmatrix}
a & b \\
0 & a
\end{bmatrix} + \begin{bmatrix}
c & d \\
0 & c
\end{bmatrix}\right) = \phi\left(\begin{bmatrix}
a+c & b+d \\
0 & a+c
\end{bmatrix}\right) = a+c = \phi\left(\begin{bmatrix}
a & b \\
0 & a
\end{bmatrix}\right) + \phi\left(\begin{bmatrix}
c & d \\
0 & c
\end{bmatrix}\right),
\]

and
\[
\phi\left(\begin{bmatrix}
a & b \\
0 & a
\end{bmatrix} \cdot \begin{bmatrix}
c & d \\
0 & c
\end{bmatrix}\right) = \phi\left(\begin{bmatrix}
ac & ad+bc \\
0 & ac
\end{bmatrix}\right) = ac = \phi\left(\begin{bmatrix}
a & b \\
0 & a
\end{bmatrix}\right) \cdot \phi\left(\begin{bmatrix}
c & d \\
0 & c
\end{bmatrix}\right).
\]

It follows that $\phi : R \to Q$ is a ring homomorphism.

Next, we determine the kernel of $\phi$. We claim that $\text{Ker } \phi = \{0\}$.

If $g = \begin{bmatrix}
a & b \\
0 & a
\end{bmatrix} \in \text{Ker } \phi$, then we have $0 = \phi(g) = \phi\left(\begin{bmatrix}
a & b \\
0 & a
\end{bmatrix}\right) = a$. So $g = \begin{bmatrix}
0 & 0 \\
0 & 0
\end{bmatrix} \in \{0\}$. 

and hence \( \ker \phi \subset J \). On the other hand, if \( B = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \in J \), then it follows from the definition of \( \phi \) that \( \phi(B) = 0 \). Thus, \( J \subset \ker \phi \). Putting these two inclusions together yields \( J = \ker \phi \). Next, let us observe that the homomorphism \( \phi \) is onto.

Indeed, just take for any \( a \in \mathbb{Q} \), \( \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in \mathbb{R} \); then we have

\[
\phi \left( \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \right) = a.
\]

Therefore, \( \phi : \mathbb{R} \to \mathbb{Q} \) is a surjective homomorphism with kernel \( J \). By the first isomorphism theorem,

\[
\mathbb{R} / J \cong \mathbb{Q}
\]

and we are done. \( \square \)