1. If 0 and 0' are both zeros in \( R \) then, by the existence of zero axiom applied twice,
\[
0 = 0 + 0' = 0'.
\]
If 1 and 1' are both multiplicative identity elements in \( R \) then, by the defining condition for existence of a multiplicate identity element applied twice,
\[
1 = 1 \cdot 1' = 1'.
\]
If \( b \) and \( c \) are both negatives of \( a \in R \), then, by the zero axiom, the negatives axiom and associativity,
\[
b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c.
\]
If \( b \) and \( c \) are both multiplicative inverses of \( a \in R \), then, by the multiplicative identity condition, the multiplicative inverses condition and associativity,
\[
b = b \cdot 1 = b \cdot (a \cdot c) = (b \cdot a) \cdot c = 1 \cdot c = c.
\]

\*2. (a) Let \( a \in R \). By the zero axiom and one half of distributivity,
\[
a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.
\]
Now using the existence of negatives axiom, the previous observation, associativity and the zero axiom, we have
\[
0 = -(a \cdot 0) + a \cdot 0 = -(a \cdot 0) + (a \cdot 0 + a \cdot 0) = (-a \cdot 0 + a \cdot 0) + a \cdot 0 = 0 + a \cdot 0 = a \cdot 0.
\]
Similarly, using the other half of distributivity, we have 0 = 0 \cdot a.

(b) Let \( a, b \in R \). By part (a), commutativity of addition, distributivity and the negatives and zero axioms, we have
\[
ab + a(-b) = a(-b) + ab = a((-b) + b) = a \cdot 0 = 0
\]
and
\[
ab + (-a)b = (-a)b + ab = ((-a) + a)b = 0 \cdot b = 0.
\]
By uniqueness of the negative of \( ab \), we have
\[
-(ab) = a(-b) = (-a)b.
\]
Thus also
\[
(-a)(-b) = -(a(-b)) = -(-(ab)) = ab,
\]
since, by uniqueness, every element is the negative of its negative.

Let \( R \) be a nontrivial ring with identity, so \( R \) contains at least two elements, so must contain something nonzero, say \( a \neq 0 \). If 1 = 0 then, by part (a),
\[
a = a \cdot 1 = a \cdot 0 = 0,
\]
contradicting that \( a \neq 0 \). Hence 1 \neq 0.
3. Let $F$ be a field, so certainly $F$ is a nontrivial commutative ring with identity. Let $a, b \in F$ and suppose that $ab = 0$. If $a \neq 0$, then, by the definition of a field, the element $a$ possesses a multiplicative inverse $a^{-1}$ in $F$. By ring axioms and part (a) of the previous exercise,

$$b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0.$$  

This shows that either $a = 0$ or $b = 0$, and completes the proof that $F$ is an integral domain.

Let $R$ be a nontrivial commutative ring with identity. Suppose first that $R$ is an integral domain. Let $a, b, c \in R$ such that $a \neq 0$ and $ab = ac$. Then

$$a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-ac) = ab + (-ab) = 0.$$  

By definition of an integral domain, we can deduce that $b - c = b + (-c) = 0$, so that $b = b + 0 = b + ((-c) + c) = (b + (-c)) + c = 0 + c = c$, verifying cancellativity.

Conversely, suppose that $R$ is cancellative and $a, b \in R$ with $ab = 0$. If $a \neq 0$ then $ab = 0 = a \cdot 0$, by part (a) of the previous exercise, so that $b = 0$, by cancellativity. This shows either $a = 0$ or $b = 0$, verifying that $R$ is an integral domain.

4. Let $S$ be a subring of a ring $R$, so $S$ is nonempty and closed under addition, multiplication and taking negatives. Any ring axiom that uses universal quantifiers only will automatically hold in $S$ with respect to the operations inherited from $R$, because all elements of $S$ are elements of $R$. It remains only to check the axioms that use an existential quantifier. Since $S$ is nonempty we can choose some $a \in S$. Because $S$ is closed under addition and taking negatives, we have $-a \in S$ and

$$0 = a + (-a) \in S.$$  

Hence the ring axiom for existence of zero holds also in $S$, using the zero from $R$, as all elements of $S$ are elements of $R$. The ring axiom for existence of negatives now also holds immediately, because $S$ is closed under taking negatives from $R$.

5. Let $S$ be nonempty subset of a ring $R$. Suppose first that $S$ is a subring, so $S$ is closed under addition, taking negatives and multiplication. Let $a, b \in S$. Then, by definition of subtraction and the closure properties of $S$, we have

$$a - b = a + (-b) \in S.$$  

This verifies that $S$ is closed under subtraction and multiplication.

Conversely, suppose that $S$ is closed under subtraction and multiplication. Because $S$ is nonempty there exists some $c \in S$. Then $0 = c + (-c) = c - c \in S$, because $S$ is closed under subtraction. Let $a, b \in S$. Then $-b = 0 + (-b) = 0 - b \in S$, again because $S$ is closed under subtraction. This shows that $S$ is closed under taking negatives. Also

$$a + b = a + (-(-b)) = a - (-b) \in S,$$

again because $S$ is closed under subtraction. Thus $S$ is also closed under addition. This completes the proof that $S$ is a subring of $R$.  

6. Clearly all of the sets are nonempty. We check that $S_1$ is closed under subtraction and multiplication. Let
\[ \alpha = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \quad \text{and} \quad \beta = \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \]
be any elements of $S_1$, where $a, b, c, d, e, f \in \mathbb{R}$. Then
\[ \alpha - \beta = \begin{bmatrix} a - d & b - e \\ 0 & c - f \end{bmatrix} \quad \text{and} \quad \alpha \beta = \begin{bmatrix} ad & ae + bf \\ 0 & cf \end{bmatrix} \]
are both clearly elements of $S_1$, verifying that $S_1$ is closed under subtraction and multiplication. The verifications for $S_3$, $S_5$ and $S_6$ are similar, so that $S_1$, $S_3$, $S_5$ and $S_6$ are subrings of $\text{Mat}_2(\mathbb{R})$. Put
\[ \alpha = \beta = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} . \]
Then $\alpha, \beta \in S_2, S_4$. But
\[ \alpha \beta = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin S_2, S_4. \]
Hence neither $S_2$ nor $S_4$ is closed under multiplication, so that neither can be subrings of $\text{Mat}_2(\mathbb{R})$.

Both $S_1$ and $S_3$ have a multiplicative identity element, which is the usual $2 \times 2$ identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. The subring $S_5$ also has a multiplicative identity element, which is $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. In $S_6$ the product of any two elements is the zero matrix, so no element of $S_6$ can fix all others by multiplication, because certainly $S_6$ contains nonzero matrices. Hence $S_6$ has no multiplicative identity element.

7. Observe that, in $S$,
\[ 0 = 0\phi - 0\phi = (0 + 0)\phi - 0\phi = (0\phi + 0\phi) - 0\phi = 0\phi + (0\phi - 0\phi) = 0\phi + 0 = 0\phi . \]
If $a \in R$ then, by the previous observation, again in $S$,
\[ a\phi + (-a)\phi = (-a)\phi + a\phi = (-a + a)\phi = 0\phi = 0 , \]
so that $-(a\phi) = (-a)\phi$ in $S$.

*8. Define a mapping $\phi : C \to \mathbb{C}$ by $a + bx \mapsto a + bi$, where $i = \sqrt{-1}$, and $a, b \in \mathbb{R}$. This is clearly a bijection, so it suffices to check that $\phi$ preserves addition and multiplication. Let $\alpha, \beta \in C$, say
\[ \alpha = a + bx \quad \text{and} \quad \beta = c + dx , \]
for some $a, b, c, d \in \mathbb{R}$. Then, using addition of polynomials,
\[ \alpha + \beta = (a + c) + (b + d)x , \]
which coincides immediately with its remainder after division by \( x^2 + 1 \) (since it is already a linear polynomial). Hence

\[
(\alpha + \beta) \phi = (((a + c) + (b + d)x) \phi = (a + c) + (b + d)i = (a + bi) + (c + di) = \alpha \phi + \beta \phi,
\]

which verifies that \( \phi \) preserves addition. Multiplication of polynomials and some rearrangement yield

\[
\alpha \beta = ac + (ad + bc)x + bdx^2 = bd(x^2 + 1) + ac - bd + (ad + bc)x,
\]

leaving a remainder of \( ac - bd + (ad + bc)x \) after division by \( x^2 + 1 \), the product of \( \alpha \) and \( \beta \) in \( C \). Hence

\[
(\alpha \beta) \phi = (ac - bd + (ad + bc)x) \phi = (ac - bd) + (ad + bc)i = (a + bi)(c + di) = (\alpha \phi)(\beta \phi),
\]

which verifies that \( \phi \) preserves multiplication. This completes the proof that \( \phi \) is an isomorphism.

**9.** The addition tables are the same in both cases, because addition of linear polynomials yields linear polynomials, which coincide automatically with their remainders after division by a quadratic:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>( x )</th>
<th>( 1 + x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>( x )</td>
<td>( 1 + x )</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>( 1 + x )</td>
<td>( x )</td>
</tr>
<tr>
<td>( x )</td>
<td>( x )</td>
<td>( 1 + x )</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( 1 + x )</td>
<td>( 1 + x )</td>
<td>( x )</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

In case (a), when \( p(x) = x^2 + 1 \) we have the following multiplication table:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>( x )</th>
<th>( 1 + x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>( x )</td>
<td>( 1 + x )</td>
</tr>
<tr>
<td>( x )</td>
<td>0</td>
<td>( x )</td>
<td>1</td>
<td>( 1 + x )</td>
</tr>
<tr>
<td>( 1 + x )</td>
<td>0</td>
<td>( 1 + x )</td>
<td>( 1 + x )</td>
<td>0</td>
</tr>
</tbody>
</table>

The multiplicative identity element of \( R \) is the constant polynomial 1, but \( R \) fails to be a field because the last line of the table does not contain 1, so that \( 1 + x \) is nonzero but does not have a multiplicative inverse.
In case (b), when \( p(x) = x^2 + x + 1 \) we have the following multiplication table:

<table>
<thead>
<tr>
<th>.</th>
<th>0</th>
<th>1</th>
<th>( x )</th>
<th>( 1 + x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>( x )</td>
<td>( 1 + x )</td>
</tr>
<tr>
<td>( x )</td>
<td>0</td>
<td>( x )</td>
<td>( 1 + x )</td>
<td>1</td>
</tr>
<tr>
<td>( 1 + x )</td>
<td>0</td>
<td>( 1 + x )</td>
<td>1</td>
<td>( x )</td>
</tr>
</tbody>
</table>

Now every nonzero row contains the multiplicative identity element 1, so all nonzero elements have multiplicative inverses. Hence, in this case, \( R \) is a field with 4 elements.

*10 If \( R \) is any ring then the identity mapping that fixes all elements of \( R \) is clearly an isomorphism, so that \( R \cong R \), verifying that \( \cong \) is reflexive.

Suppose that \( R \) and \( S \) are rings and \( R \cong S \). Then there exists an isomorphism \( \phi : R \to S \). In particular, \( \phi \) is a bijection so the inverse mapping \( \phi^{-1} : S \to R \) exists and is also a bijection. We check that \( \phi^{-1} \) is a ring homomorphism. Let \( a, b \in S \). Then \( a = x\phi \) and \( b = y\phi \) for some \( x, y \in R \), since \( \phi \) is onto. Then

\[
(a + b)\phi^{-1} = (x\phi + y\phi)\phi^{-1} = ((x + y)\phi)\phi^{-1} = x + y = a\phi^{-1} + b\phi^{-1},
\]

and

\[
(ab)\phi^{-1} = ((x\phi)(y\phi))\phi^{-1} = ((xy)\phi)\phi^{-1} = xy = (a\phi^{-1})(b\phi^{-1}),
\]

which verifies that \( \phi^{-1} \) preserves addition and multiplication. Hence \( \phi^{-1} : S \to R \) is an isomorphism, so \( S \cong R \), verifying that \( \cong \) is symmetric.

Suppose that \( R, S \) and \( T \) are rings and \( R \cong S \) and \( S \cong T \). Then there exist isomorphisms \( \alpha : R \to S \) and \( \beta : S \to T \). In particular, \( \alpha \) and \( \beta \) are bijections, so the composite \( \alpha\beta : R \to T \) is a bijection. We check that \( \alpha\beta \) is a ring homomorphism. Let \( a, b \in R \). Then

\[
(a + b)\alpha\beta = (a\alpha + b\alpha)\beta = (a\alpha)\beta + (b\alpha)\beta = a(\alpha\beta) + b(\alpha\beta),
\]

and

\[
(ab)\alpha\beta = ((a\alpha)(b\alpha))\beta = ((a\alpha)\beta)((b\alpha)\beta) = (a(\alpha\beta))(b(\alpha\beta)),
\]

which verifies that \( \alpha\beta \) preserves addition and multiplication. Hence \( \alpha\beta : R \to T \) is an isomorphism, so \( R \cong T \), verifying that \( \cong \) is transitive.