1) Let R be a commutative ring [with $1 \neq 0$] and let

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \; : \; a, b \in R \right\}.$$

[So, diagonal 2×2 matrices with entries in R.]

(a) Prove that S is a ring.

(b) Prove that R is *not* a domain.

Proof. First, note that $S \subseteq M_2(R)$ [where $M_2(R)$ is the set of 2×2 matrices with entries in R]. So, suffices to show that S is a *subring* of $M_2(R)$.

We have $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$ [and I is the 1 of $M_2(R)$]. Also, if $\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix}, \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \in S$, then

$$\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & 0 \\ 0 & b_1 - b_2 \end{bmatrix} \in S$$

and

$$\begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & b_1 b_2 \end{bmatrix} \in S.$$

Hence, S is a subring of $M_2(R)$.

Note that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in S \setminus \{0\}$ but

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0.$$

So, S is not a domain. $\square$

2) Is $\mathbb{C}$ the field of fractions of $\mathbb{R}$? [Justify your answer!]

Solution. **No!** Since $\mathbb{R}$ is already a field, we have that its field of fraction is itself. [Or, i is not a quotient of two real numbers, as these quotients are real, and i is not.] $\square$

3) Prove that if R is a domain, then $U(R[x]) = U(R)$. [Remember, $U(R)$ is the set of units of R. So, what you need to prove it that the units of the polynomial ring are the constant polynomials which are units of R.]

Proof. First, not that if $a \in U(R)$, then there exists $b \in R$ such that $ab = 1$. Since $a, b \in R[x]$ [as $R \subseteq R[x]$], as have that $a \in U(R[x])$. [So $U(R) \subseteq U(R[x])$.]

Now, let $f \in U(R[x])$. Then, there is $g \in R[x]$ such that $f \cdot g = 1$. Then, $\deg(f \cdot g) = \deg(1) = 0$. Since R is a domain, we have that $\deg(f \cdot g) = \deg(f) + \deg(g)$. So, $\deg(f) + \deg(g) = 0$. Thus, $\deg(f) = \deg(g) = 0$, and hence $f, g \in R$. Since their product is 1, we have that f [and g] is in $U(R)$. [So, $U(R[x]) \subseteq U(R)$. Since we also have the other inclusion, we have equality.] $\square$

4) Let F be a field having $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ as a subfield. Prove that for all $a \in F$ we have that $a + a = 0$ [i.e., $a = -a$].

Proof. In $\mathbb{F}_2$ we have $1 + 1 = 0$. Since $\mathbb{F}_2$ is a subfield of F, we have that $1 + 1 = 0$ in F also. [They have the same 1 and same addition.] Now let $a \in F$. Then

$$a + a = a(1 + 1) = a \cdot 0 = 0.$$

$\square$

5) Let F be a finite field with n elements and $a \in F \setminus \{0\}$. Prove that there is $k \in \{1, 2, \ldots, n\}$ such that $a^k = 1$. [**Hint:** Consider the set $S = \{1, a, a^2, a^3, \ldots, a^n\} \subseteq F$. How many *distinct* elements can S have?]

Proof. Since $S \subseteq F$, and F has n elements, we have that S has at most n elements. So, there are $i, j \in \{0, 1, 2, \ldots, n\}$, with $i < j$, such that $a^i = a^j$ [otherwise, S would have $n + 1$ elements].
Since $a \neq 0$, we have an inverse a^{-1}. Then,

$$(a^{-1})^i \cdot a^i = a^{-i} \cdot a^i = a^{-i+i} = a^0 = 1,$$

and

$$(a^{-1})^i \cdot a^j = a^{-i} \cdot a^j = a^{j-i}.$$

But, since $a^j = a^i$, we then have $a^{j-i} = 1$. So, $k = j - i \in \{1, , \ldots, n\}$ and $a^k = 1$. $\square$