Exercises.

1. Let $\mathbb{F}$ be the field $\mathbb{F} = \mathbb{F}_5 = \mathbb{Z}_5$.

   (a) Find the multiplicative inverse of the elements $1, 2, 3, 4$ of $\mathbb{F}$.

   (b) Compute the following in $\mathbb{F}^3$:

   $$\text{(a)} \begin{pmatrix} 2 \\ 4 \\ 1 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix} \quad \text{(b)} \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix} + \begin{pmatrix} 4 \\ 0 \\ 3 \end{pmatrix} \quad \text{(c) } 4 \cdot \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} \quad \text{(d) } 3 \cdot \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix}$$

   (c) Find a nonzero vector $\begin{pmatrix} a \\ b \\ c \end{pmatrix} \in \mathbb{F}^3$ such that

   $$a \begin{pmatrix} 0 \\ 3 \\ 1 \end{pmatrix} + b \begin{pmatrix} 4 \\ 0 \\ 3 \end{pmatrix} + c \begin{pmatrix} 3 \\ 4 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

   (Remember that in this entire problem, $\mathbb{F} = \mathbb{Z}_5$! You might want to mimic row reduction that you have done in an earlier linear algebra class).

Solution to Question 1.

(a) In $\mathbb{F}_5$, we have

$$\begin{aligned} 1 \cdot 1 &= 1, \\ 2 \cdot 3 &= 1, \\ 4 \cdot 4 &= 1. \end{aligned}$$

Hence,

$$\begin{aligned} 1^{-1} &= 1, \\ 2^{-1} &= 3, \\ 3^{-1} &= 2, \\ 4^{-1} &= 4. \end{aligned}$$

(b) (a) $\begin{pmatrix} 2 \\ 4 \\ 1 \end{pmatrix} + \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$, (b) $\begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix} + \begin{pmatrix} 4 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix}$,

(c) $4 \cdot \begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$, (d) $3 \cdot \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \\ 2 \end{pmatrix}$.

(c) By performing row reduction

$$\begin{bmatrix} 0 & 4 & 3 \\ 3 & 0 & 4 \\ 1 & 3 & 4 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 3 & 4 \\ 0 & 4 & 3 \\ 3 & 0 & 4 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 3 & 4 \\ 0 & 4 & 3 \\ 0 & 1 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 3 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{bmatrix}.$$

Therefore,

$$\begin{aligned} b &= -2c = 3c, \\ a &= -3b - 4c = 2b + c = 2c. \end{aligned}$$

Any vector of the form $c \cdot \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}$ works.

2. Let $\mathbb{R}^{n\times n}$ denote the $n \times n$ matrices with coefficients in $\mathbb{R}$, for $n \geq 1$. This set has two natural operations, matrix addition $+$ and matrix multiplication $\cdot$. For which n is $\mathbb{R}^{n\times n}$ with these operations a field? (Remember to justify your answers! If it is a field, prove it, if not, give a reason).

   Solution to Question 2.

   - For $n = 1$, $\mathbb{R}^{1\times 1} \simeq \mathbb{R}$. So it is a field.
   - Assume $n \geq 2$. If $\mathbb{R}^{n\times n}$ is a field, then the matrix $\mathbf{0}$ is the 0 element in the field. Let $\mathbb{E}_{ij}$ be the matrix in $\mathbb{R}^{n\times n}$ with the (i, j)-entry equals 1 and all other entries are 0. Then $\mathbf{E}_{11} \cdot \mathbf{E}_{22} = \mathbf{0}$. However, we know that neither $\mathbf{E}_{11}$ nor $\mathbf{E}_{22}$ is $\mathbf{0}$. Therefore, $\mathbb{R}^{n\times n}$ is not a field for $n \geq 2$.

3. Let $\mathbb{F}$ be a field. The **characteristic** of $\mathbb{F}$ is defined to be the smallest positive integer p such that $1+1+\cdots+1=0$, where there are p 1's in this formula. If no such sum is 0, then we say the characteristic of $\mathbb{F}$ is 0.

   (a) Find the characteristics of the fields $\mathbb{R}, \mathbb{C}, \mathbb{Z}_p$.

   (b) If $\mathbb{F}$ is a finite field, show that the characteristic p of $\mathbb{F}$ is not zero.

   (c) If $\mathbb{F}$ is a finite field, show that the characteristic p of $\mathbb{F}$ is a prime number.

Solution to Question 3.

(a) char $\mathbb{R}=0$. Reason: If not, assume char $\mathbb{R}=n>0$. This means

$$0<n=\sum_n 1=0,$$

which is a contradiction. This reasoning implies that for any field $\mathbb{F}$ containing $\mathbb{Z}$, char $\mathbb{F}=0$. In particular, char $\mathbb{R}$ and char $\mathbb{C}$ are 0.
char $\mathbb{Z}_p=p$ by the definition of $\mathbb{Z}_p$ and that of characteristic.

(b) Assume the cardinality $|\mathbb{F}|=n$. Let $e_i=\sum_i \mathbf{1}_{\mathbb{F}}=i\cdot\mathbf{1}_{\mathbb{F}}$. Because there are only n elements in $\mathbb{F}$, so among $e_1,\ldots,e_{n+1}$ there must be two identical elements. Assume WLOG that $e_j=e_k$ and $j<k$. Then $(k-j)\cdot\mathbf{1}=0$. So the characteristic is not 0. From the reasoning, we've actually shown that

$$0<\text{char }\mathbb{F}\leq|\mathbb{F}|.$$

(c) Assume char $\mathbb{F}=n>0$. If n is not prime, then $n=p\cdot q$ with $p,q<n$. By the definition of characteristic, $p\mathbf{1}_{\mathbb{F}}\neq\mathbf{0}_{\mathbb{F}}$ and $q\mathbf{1}_{\mathbb{F}}\neq\mathbf{0}_{\mathbb{F}}$. Since we have distribution law in $\mathbb{F}$,

$$p\mathbf{1}_{\mathbb{F}}\cdot q\mathbf{1}_F=pq\mathbf{1}_F=n\mathbf{1}_F=\mathbf{0}_{\mathbb{F}}.$$

This makes a contridiction. So n must be prime.

4. In this problem we will investigate fields with 4 elements.

   (a) If $\mathbb{F}_4$ is a field with exactly 4 elements, what must the characteristic be? (justify your answer, of course! But you may use without proof statements from the previous problem).

   (b) Find a field $\mathbb{F}_4$ that has 4 elements. Write down the addition and multiplication tables of this field. Remember that two of your elements are 0 and 1!

   (c) Find all fields with 4 elements (i.e. write down all possible addition and multiplication tables. Your first two elements should be 0 and 1).

Solution to Question 4.

(a) Recall in Question 3, we've shown that

$$0 < \operatorname{char} \mathbb{F} \leq |\mathbb{F}|,$$

and that char $\mathbb{F}$ is prime. So char $\mathbb{F}$ can only be 2 or 3.
If char $\mathbb{F} = 3$, then we may assume $\mathbb{F}_4 = \{0, 1, 2, a\}$, where a is distinct from $0, 1, 2$. Now $a + 1 \in \mathbb{F}_4$. So either $a + 1 = 0, 1, 2$ or $a + 1 = a$. However $a + 1 = a$ implies $0 = 1$. $a + 1 = 0, 1, 2$ implies $a = 2, 0, 1$, respectively. All these cases are impossible. So char $\mathbb{F}_4 \neq 3$.
Hence, char $\mathbb{F}_4 = 2$.

(b) Notice that char $\mathbb{F}_4 = 2$, so $1 + 1 = 0$. Let a be an element in $\mathbb{F}_4$ distinct from 0 and 1. Then $a + 1$ is also in $\mathbb{F}_4$. Because

$$a + 1 = 0 \implies a = 1,$$
$$a + 1 = 1 \implies a = 0,$$

and

$$a + 1 = a \implies 1 = 0,$$

so $a + 1$ is distinct from 0, 1 and a. Hence,

$$\mathbb{F}_4 = \{0, 1, a, a + 1\}.$$

(c) The addition table is

$+$	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

For the multiplication, we know for all $x \in \mathbb{F}_4$,

$$0 \cdot x = 0, \qquad 1 \cdot x = x.$$

Since $a \cdot a \in \mathbb{F}_4$, it must be one of the 4 elements. Because

$$\begin{aligned} &a \cdot a = 0 \implies a = 0, \\ &a \cdot a = 1 \implies (a+1)^2 = 0 \implies a = 1, \\ &a \cdot a = a \implies a = 1, \end{aligned}$$

so $a \cdot a$ must be $a+1$. The only possible multiplication table is If there is another field

$\cdot$	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
$a+1$	0	$a+1$	1	a

.

$\mathbb{F}_4' = \{0, 1, b, b+1\}$ with 4 elements, it must have the same multiplication table with b in place of a. So the map $\varphi : \mathbb{F}_4 \to \mathbb{F}_4'$ defined by

$$\begin{aligned} \varphi(0) &= 0, \qquad & \varphi(1) &= 1, \\ \varphi(a) &= b, \qquad & \varphi(a+1) &= b+1 \end{aligned}$$

is an isomorphism between fields. Hence, there is only one such field up to isomorphism.

5. Show that $\mathbb{C}$ is a vector space over the field $\mathbb{R}$. More generally, if $\mathbb{F} \subset \mathbb{K}$ are both fields (with addition, multiplication, 0, 1, in $\mathbb{F}$ induced from the same operations/elements on $\mathbb{K}$), is $\mathbb{K}$ a vector space over $\mathbb{F}$? (for this one case, you should either provide a counter-example or a one or two line reason, no proof is required this time).

Solution to Question 5.

$\mathbb{C}$ is a vector space over $\mathbb{R}$. This is because for all $a, b \in \mathbb{R}$ and $z_1, z_2 \in \mathbb{C}$, we know $az_1 + bz_2 \in \mathbb{C}$, and by the distribution law,

$$(a+b)z_1 = az_1 + bz_1,$$
$$a(z_1 + z_2) = az_1 + az_2.$$

The reason can be applied to any $\mathbb{F} \subset \mathbb{K}$ if we replace $\mathbb{R}$ with $\mathbb{F}$ and $\mathbb{C}$ with $\mathbb{K}$. Hence we may say, in general, if $\mathbb{F}$ is a subfield of $\mathbb{K}$, then $\mathbb{K}$ is a vector space over $\mathbb{F}$.