§8. Finite fields $\mathbb{F}_q$.

- We have defined the notion of a field, and already know the real number field $\mathbb{R}$; the complex number field $\mathbb{C}$, and the rational number field $\mathbb{Q}$, are representative examples of fields. Today I want to introduce a different type of a field, namely, a finite field, which is — as the name suggests — a field that contains only finitely many elements. The goal is to develop a geometry over such a field, called finite geometry. For that matter, I need to first go over some general properties of a field. There is one extremely important fact concerning an arbitrary field which I did not necessarily emphasize before:

"the notion of vector spaces can be defined over any field $F$.”

In other words, we can do linear algebra over any field $F$. In particular, matrices with entries in $F$ makes sense. The truth is, the notion of a vector space strictly hinges on the notion of a field. It is only with the specification of a field $F$ as a “base field” that the notion of a vector space makes sense. So, once again, a vector space is “defined over” each field $F$. So, it is always good to be meticulous and call it an “$F$-vector space”. This also means that, in retrospect, what you have learned in your ‘Elementary Linear Algebra’ class (Math 290 in our course listings) was the linear algebra over $\mathbb{R}$. What you used to call it a vector space was indeed something to be called an $\mathbb{R}$-vector space. The fact of the matter is, we can replace $\mathbb{R}$ with any field $F$ and 80% (anecdotally) of the results remain valid over the field $F$. The other 20% is the aspect of linear algebra which only makes sense over $\mathbb{R}$ and/or $\mathbb{C}$. Those are the part called ‘spectral theory’. There is some subtlety in this 20%. Proofs of many facts in linear algebra stated over $\mathbb{R}$ which do not hold true over an arbitrary field resort to $\mathbb{C}$. Proof of the fact that “a symmetric matrix whose entries are in $\mathbb{R}$ is diagonalizable within $\mathbb{R}$” is such an example.* This is natural, considering that eigenvalues of a matrix whose entries are in $\mathbb{R}$ can be non-real, but they are always in $\mathbb{C}$. Now, on the other hand, please don’t be misled: I did not say that what holds true over $\mathbb{R}$ holds true over $\mathbb{C}$. For example, the statement “a symmetric matrix over $\mathbb{C}$ is diagonalizable within $\mathbb{C}$” is false.

*This fact is non-trivial. You learn the statement without proof in elementary linear algebra.
• Cram session. General properties of a field $F$.

So let’s start with a cram session on general properties of an arbitrary field $F$. We will make a frequent reference to the field axioms, so let me reproduce the field axioms here*

**Field Axioms.**

(i) $\alpha + \beta = \beta + \alpha$,  
(ii) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$,  
(iii) $\alpha + 0 = \alpha$,  
(iv) $\alpha + (-\alpha) = 0$,  
(v) $\alpha \beta = \beta \alpha$,  
(vi) $(\alpha \beta) \gamma = \alpha (\beta \gamma)$,  
(vii) $(\alpha + \beta) \gamma = \alpha \gamma + \beta \gamma$,  
(viii) $\alpha \cdot 1 = \alpha$,  
(ix) for $\alpha \neq 0$, there is $\alpha^{-1}$ such that $\alpha \alpha^{-1} = 1$.  
(x) $0 \neq 1$.

First, some notational remarks.

**Notation.** In a field $F$, taking into account axiom (ii), we may write the quantity  

$$(\alpha_1 + \alpha_2) + \alpha_3$$

as  

$$\alpha_1 + \alpha_2 + \alpha_3.$$  

*The numbering of the axioms are different from “Review of Lectures – IV”, but as a whole this is the same set of axioms as given in “Review of Lectures – IV”.

2
Also, taking into account axiom (vi), we may write the quantity

\[(\alpha_1 \alpha_2)^3\]

as

\[\alpha_1 \alpha_2 \alpha_3.\]

Now we may write the quantities

\[\left(\alpha_1 + \alpha_2 + \alpha_3\right) + \alpha_4, \quad \text{and} \quad \left(\alpha_1 \alpha_2 \alpha_3\right) \alpha_4,\]

as

\[\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4, \quad \text{and} \quad \alpha_1 \alpha_2 \alpha_3 \alpha_4,\]

respectively. We may write

\[\left(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4\right) + \alpha_5, \quad \text{and} \quad \left(\alpha_1 \alpha_2 \alpha_3 \alpha_4\right) \alpha_5,\]

as

\[\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5, \quad \text{and} \quad \alpha_1 \alpha_2 \alpha_3 \alpha_4 \alpha_5,\]

respectively, and so on.

**Definition (The element 2 of F).** 2 ∈ F is defined as

\[2 = 1 + 1.\]

* Here I want to draw your attention. What I just did was, to “define” 2 as 1 + 1. This kind of proclamation is typical of ‘modern mathematics’, namely, I proclaim that 2 = 1 + 1 should be the definition, not a fact. Indeed, if you claim this is a fact, then you have to throw the definition of 2, which you can’t. That’s because 2 is defined as 1 + 1 but no other way. All this is contrary to how we were taught in schools, where 2 = 1 + 1 is a ‘fact’.*

---

*‘Modern’ as in ‘post 19th century’. For a long time in the history of human civilization, 2 = 1 + 1 was regarded as a ‘fact’. I cannot pinpoint when exactly mathematicians realized that 2 = 1 + 1 was the definition, not a fact. Georg Cantor (1845-1928) and Giuseppe Peano (1858–1932), among others, are the two names that come to my mind, of mathematicians who addressed axiomatic foundations of the number system (I can find this out).
• Here let me make another important remark:

\[ 2 \text{ may or may not equal } 0. \]

Indeed, this may throw you off, but for some fields \( F \), \( 2 \) indeed equals \( 0 \). It is just that, in the real number field \( \mathbb{R} \), we have \( 2 \neq 0 \). See Remark 1 (on page 18).

**Definition (The element 3 of \( F \)).** \( 3 \in F \) is defined as

\[ 3 = 2 + 1. \]

Alternatively, \( 3 \in F \) is defined as

\[ 3 = 1 + 1 + 1. \]

• This is the same deal once again. \( 3 = 2 + 1 \) (or equivalently \( 3 = 1 + 1 + 1 \)) is not a fact, but rather it is a definition. And also,

\[ 3 \text{ may or may not equal } 0. \]

Indeed, for some fields \( F \), \( 3 \) indeed equals \( 0 \). It is just that, in the real number field \( \mathbb{R} \), we have \( 3 \neq 0 \).

**Exercise 1.** Prove that, on a field \( F \),

\[ 2 = 0 \quad \text{and} \quad 3 = 0 \]

cannot happen at once.

**Exercise 2.** Define 4, 5, 6, 7, 8, and 9 as elements of a field \( F \).

• The following basic facts hold for any field \( F \).
Below I am going to prove six formulas (Formula 1 through Formula 6), relying on the field axioms as duplicated in page 1. Axiom numbers I cite in the proofs below are consistent with those listed in page 1.

**Formula 1.** In a field \( F \),

\[
0 + 0 = 0.
\]

*Proof.* Substitute \( \alpha = 0 \) in axiom (iii), to obtain \( 0 + 0 = 0 \). This completes the proof of Formula 1.

**Formula 2.** Let \( F \) be a field. Let \( \alpha \in F \).

(1) \[ \alpha = 1 \alpha. \]

(2) \[ \alpha + \alpha = 2 \alpha. \]

(3) \[ \alpha + \alpha + \alpha = 3 \alpha. \]

*Proof.* (1) is simply a paraphrase of axiom (viii), taking into account the axiom (v).

(2) From (1), we have \( \alpha = 1 \alpha \). Hence

\[
\alpha + \alpha = 1 \cdot \alpha + 1 \cdot \alpha.
\]

By axiom (vii), this is rewritten as

\[
\alpha + \alpha = (1 + 1) \cdot \alpha.
\]

Since \( 1 + 1 = 2 \) by definition, we obtain

\[
\alpha + \alpha = 2 \alpha.
\]
(3) We now have \( \alpha + \alpha = 2\alpha \), and \( \alpha = 1\alpha \). Hence by axiom (vii),

\[
\alpha + \alpha + \alpha = (\alpha + \alpha) + \alpha = 2\alpha + 1\alpha = (2 + 1)\alpha.
\]

Since \( 2 + 1 = 3 \) by definition, we obtain

\[
\alpha + \alpha + \alpha = 3\alpha.
\]

Now the proof of Formula 2 is complete.

**Notation (positive integer powers of elements).**

In a field \( F \), define \( \alpha^2, \alpha^3, \ldots \) as

\[
\alpha^2 = \alpha\alpha, \quad \alpha^3 = \alpha^2\alpha = \alpha\alpha\alpha, \quad \ldots.
\]

**Formula 3.** Let \( F \) be a field. Let \( \alpha \in F \).

(1) \quad 1 \cdot 1 = 1.

(2) \quad 0 \cdot \alpha = 0.

(3) \quad 0 \cdot 1 = 0.

(4) \quad 0 \cdot 0 = 0.

(5) \quad (\alpha - 1)\alpha = -\alpha.

(6) \quad \alpha - 0 = 0.

(7) \quad -\alpha = 0.

(8) \quad (\alpha - 1)(\alpha - \alpha) = \alpha.

(9) \quad (\alpha - 1) = 1.
**Proof.**  
(1) Substitute $\alpha = 1$ in axiom (viii), to obtain $1 \cdot 1 = 1$.

(2) By axiom (vii),

$$0 \cdot \alpha + 0 \cdot \alpha = (0 + 0) \cdot \alpha.$$ 

Since $0 + 0 = 0$, we may simplify the last quantity as $0 \cdot \alpha$. Hence the above identity reads

$$0 \cdot \alpha + 0 \cdot \alpha = 0 \cdot \alpha.$$ 

By axiom (iv), there exists an element $-(0 \cdot \alpha) \in F$ such that

$$0 \cdot \alpha + (- (0 \cdot \alpha)) = 0.$$ 

Thus, add $-(0 \cdot \alpha) \in F$ to the both sides of the identity $0 \cdot \alpha + 0 \cdot \alpha = 0 \cdot \alpha$ which we have already established above, and

$$0 \cdot \alpha + 0 \cdot \alpha + (- (0 \cdot \alpha)) = 0 \cdot \alpha + (- (0 \cdot \alpha)).$$

The right-hand side is simplified as 0. Similarly, the left-hand side is simplified as $0 \cdot \alpha + 0$, which is further simplified to $0 \cdot \alpha$, by axiom (iii). To conclude,

$$0 \cdot \alpha = 0.$$ 

(3) and (4) are special cases of (2), namely, the cases $\alpha = 1$ and $\alpha = 0$.

(5) By axiom (iv), we have $1 + (-1) = 0$. Hence

$$\left(1 + (-1)\right) \cdot \alpha = 0 \cdot \alpha.$$ 

By (2), the right-hand side is simplified as 0. Thus

$$\left(1 + (-1)\right) \cdot \alpha = 0.$$ 

Use axiom (v) to rewrite the left-hand side of the above identity as \(1 \alpha + (-1) \alpha\). Thus

\[1 \alpha + (-1) \alpha = 0.\]

Note that, by Formula 2 (1), \(1 \alpha = \alpha\). Thus the same identity is

\[\alpha + (-1) \alpha = 0.\]

By axiom (i), this is the same as

\[(-1) \alpha + \alpha = 0.\]

By axiom (iv), there exists an element \(-\alpha \in F\) such that

\[\alpha + (-\alpha) = 0.\]

Thus, add \(-\alpha \in F\) to the both sides of the identity \((-1) \alpha + \alpha = 0\) which we have already established above, and

\[(-1) \alpha + \alpha + (-\alpha) = 0 + (-\alpha).\]

The right-hand side is simplified as \(-\alpha\), by axiom (iii). The left-hand side is simplified as \((-1) \alpha + 0\), which is further simplified to \((-1) \alpha\), by axiom (iii). To conclude,

\[(-1) \alpha = -\alpha.\]

(6) In (5), substitute \(\alpha = 0\):

\[(-1) 0 = -0.\]
By the axiom (v), this is rewritten as

\[ 0 \cdot (-1) = -0. \]

By (2), the left-hand side is simplified as 0. Hence \( 0 = -0 \).

(7) By axiom (iv), we have

\[-\alpha + \left( -\left( -\alpha \right) \right) = 0.\]

Or, the same to say,

\[ \left( -\left( -\alpha \right) \right) + (-\alpha) = 0.\]

Add \( \alpha \) to the both sides, and

\[ \left( -\left( -\alpha \right) \right) + (-\alpha) + \alpha = 0 + \alpha.\]

Or, the same to say

\[ \left( -\left( -\alpha \right) \right) + \alpha + (-\alpha) = 0 + \alpha.\]

The right-hand side is simplified as \( \alpha \), by axiom (iii), whereas the left-hand side is simplified as \( \left( -\left( -\alpha \right) \right) + 0 \), which is further simplified as \( -\left( -\alpha \right) \), by axiom (iii). To conclude,

\[-\left( -\alpha \right) = \alpha.\]
(8) In (5), substitute $\alpha$ with $-\alpha$:

\[
(-1)(-\alpha) = -(-\alpha).
\]

By (7), the right-hand side is simplified as $\alpha$. Hence

\[
(-1)(-\alpha) = \alpha.
\]

(9) is a special case of (8), namely, the case $\alpha = 1$. Note that the notation $\left( -1 \right)^2$ means \( (-1)(-1) \).

Now the proof of Formula 3 is complete.

**Exercise 3.** In a field $F$, prove the following.

(1) \( (-\alpha)^2 = \alpha^2 \).  
(2) \( (-\alpha)^3 = -\alpha^3 \).  
(3) \( (-1)^3 = -1 \).

**Exercise 4.** In a field $F$, prove the following.

(1) \( (\alpha + \beta)(\gamma + \delta) = \alpha \gamma + \alpha \delta + \beta \gamma + \beta \delta \).

(2) \( (\alpha + \beta)^2 = \alpha^2 + 2\alpha \beta + \beta^2 \).

**Notation.** In a field $F$, we often write $\alpha - \beta$ to mean $\alpha + (-\beta)$. For example,

\[
\alpha - \alpha = 0.
\]
Exercise 5. In a field $F$, prove the following.

(1) $- (\alpha + \beta) = (- \alpha) + (- \beta)$.

(2) $(- \alpha)(- \beta) = \alpha \beta$.

(3) $(\alpha - \beta)(\gamma - \delta) = \alpha \gamma - \alpha \delta - \beta \gamma + \beta \delta$.

(4) $(\alpha - \beta)^2 = \alpha^2 - 2 \alpha \beta + \beta^2$.

Formula 4. Let $F$ be a field. Let $\alpha \in F$ be such that $\alpha \neq 0$. Then

$$\alpha^{-1} \neq 0.$$ 

Moreover

(1) $1^{-1} = 1$.

(2) $\left(\alpha^{-1}\right)^{-1} = \alpha$.

(3) $(- \alpha)^{-1} = - \alpha^{-1}$.

(4) $(- 1)^{-1} = -1$.

Proof. (1) By axiom (ix), we have

$$1 \cdot 1^{-1} = 1.$$ 

By Formula 2 (1), the left-hand side is simplified as $1^{-1}$. Hence

$$1^{-1} = 1.$$ 

11
First, we need to verify that \( \alpha^{-1} \neq 0 \). Indeed, if \( \alpha^{-1} = 0 \), then multiply \( \alpha \) to the both sides of the identity \( \alpha^{-1} = 0 \), and obtain

\[ \alpha \cdot \alpha^{-1} = \alpha \cdot 0. \]

By the axiom (v), this is the same as

\[ \alpha \cdot \alpha^{-1} = 0 \cdot \alpha. \]

By Formula 3 (2), the right-hand side is simplified as 0. Meanwhile, by axiom (iv), the left-hand side is simplified as 1. Hence we obtain

\[ 1 = 0. \]

This contradicts axiom (x). This way we have verified that \( \alpha^{-1} \neq 0 \). In particular, the element \( \left( \alpha^{-1} \right)^{-1} \) makes sense. By axiom (ix), we have

\[ \alpha^{-1} \cdot \left( \alpha^{-1} \right)^{-1} = 1. \]

Multiply \( \alpha \) to the both sides of the above identity, and obtain

\[ \alpha \cdot \alpha^{-1} \cdot \left( \alpha^{-1} \right)^{-1} = \alpha \cdot 1. \]

By axiom (viii), the right-hand side is simplified as \( \alpha \). Meanwhile, by axiom (viii), the left-hand side is simplified as \( 1 \cdot \left( \alpha^{-1} \right)^{-1} \), which is further simplified as \( \left( \alpha^{-1} \right)^{-1} \). Hence we obtain

\[ \left( \alpha^{-1} \right)^{-1} = \alpha. \]
(3) By axiom (ix),

\[ (-\alpha) (-\alpha)^{-1} = 1. \]

Now, multiply \((-1)\) to the both sides:

\[ (-1) (-\alpha) (-\alpha)^{-1} = (-1) \cdot 1. \]

By axiom (viii), the right-hand side is simplified as \(-1\). Meanwhile, by Formula 3 (8), the left-hand side is simplified as \(\alpha \cdot (-\alpha)^{-1}\). Thus,

\[ \alpha \cdot (-\alpha)^{-1} = -1. \]

By the axiom (v), the above identity is the same as

\[ (-\alpha)^{-1} \cdot \alpha = -1. \]

Multiply \(\alpha^{-1}\) to the both sides:

\[ (-\alpha)^{-1} \cdot \alpha \cdot \alpha^{-1} = (-1) \cdot \alpha^{-1}. \]

By Formula 3 (5), the right-hand side is simplified as \(-\alpha^{-1}\), whereas the left-hand side is simplified as \((-\alpha)^{-1} \cdot 1\), which is further simplified as \((-\alpha)^{-1}\). To conclude,

\[ (-\alpha)^{-1} = -\alpha^{-1}. \]
In (3), substitute $\alpha = 1$:

$$(-1)^{-1} = -1^{-1}.$$  

By (1), the right-hand side is simplified as $-1$, thus

$$(-1)^{-1} = -1.$$  

Now the proof of Formula 4 is complete.

The next formula may look familiar. It is called “the integral domain property of a field”. We learned that it is true for $\mathbb{C}$. Now we can prove that the same is true for any field.

**Formula 5 (Integral domain property of a field).**

Let $F$ be a field. Let $\alpha, \beta \in F$ be such that $\alpha \neq 0$, $\beta \neq 0$. Then

$$\alpha \beta \neq 0.$$  

Moreover,

$$\left(\alpha \beta\right)^{-1} = \alpha^{-1} \beta^{-1}.$$  

**Proof.** First we prove $\alpha \beta \neq 0$, by assuming $\alpha \neq 0$ and $\beta \neq 0$. Let us assume

$$\alpha \neq 0, \quad \beta \neq 0, \quad \text{and} \quad \alpha \beta = 0,$$  

to derive a contradiction. Indeed, then $\beta^{-1}$ exists. Multiply $\beta^{-1}$ to the both sides of the identity $\alpha \beta = 0$, and obtain

$$\left(\alpha \beta\right) \beta^{-1} = 0 \cdot \beta^{-1}. $$
By Formula 3 (2), the right-hand side is simplified as 0. Meanwhile, by axiom (vi), the left-hand side is rewritten as \( \alpha (\beta \beta^{-1}) \), which is simplified as \( \alpha \cdot 1 \), which is further simplified as \( \alpha \). Thus the above identity is simplified as

\[
\alpha = 0.
\]

This contradicts the assumption \( \alpha \neq 0 \). To conclude, we obtain \( \alpha \beta \neq 0 \), under the assumption \( \alpha \neq 0 \), and \( \beta \neq 0 \).

Now, under the same assumption \( \alpha \neq 0 \), and \( \beta \neq 0 \), we will prove that \( (\alpha \beta)^{-1} \) equals \( \alpha^{-1} \beta^{-1} \). For this matter, observe

\[
\left( \alpha \beta \right) \left( \beta^{-1} \alpha^{-1} \right) = \alpha \left( \beta \beta^{-1} \right) \alpha^{-1}
\]

\[
= \alpha \cdot 1 \cdot \alpha^{-1}
\]

\[
= \alpha \alpha^{-1}
\]

\[
= 1.
\]

In short,

\[
\left( \alpha \beta \right) \left( \beta^{-1} \alpha^{-1} \right) = 1.
\]

Multiply \( (\alpha \beta)^{-1} \) to the both sides, and obtain

\[
\left( \alpha \beta \right)^{-1} \left( \alpha \beta \right) \left( \beta^{-1} \alpha^{-1} \right) = \left( \alpha \beta \right)^{-1} \cdot 1.
\]

15
By axiom (ix), the right-hand side is simplified as \( (\alpha \beta)^{-1} \). Meanwhile, by the axiom (v), the left-hand side is rewritten as

\[
(\alpha \beta)(\alpha \beta)^{-1} (\beta^{-1} \alpha^{-1}),
\]

which is simplified as \( 1 \cdot (\beta^{-1} \alpha^{-1}) \), which is further simplified as \( \beta^{-1} \alpha^{-1} \). Hence

\[
\beta^{-1} \alpha^{-1} = (\alpha \beta)^{-1}.
\]

By the axiom (v), the left-hand side can be written as \( \alpha^{-1} \beta^{-1} \). To conclude,

\[
\alpha^{-1} \beta^{-1} = (\alpha \beta)^{-1}.
\]

Now the proof of Formula 5 is complete.

**Formula 6.** Let \( F \) be a field. Let \( \alpha \in F \) be such that \( \alpha \neq 0 \). Then

\[
\alpha^2 \neq 0.
\]

Moreover,

\[
(\alpha^2)^{-1} = (\alpha^{-1})^2.
\]

**Proof.** This is a special case of Formula 5, namely, the case \( \beta = \alpha \).

So there is nothing to prove.
Notation (raising the power of $-2$ to elements).

In a field $F$, let $\alpha \in F$ be such that $\alpha \neq 0$. Define $\alpha^{-2}$ as

$$\alpha^{-2} = \left(\alpha^2\right)^{-1} = \left(\alpha^{-1}\right)^2.$$

**Exercise 6.** In a field $F$, for an element $\alpha \neq 0$, define $\alpha^{-3}, \alpha^{-4}, \alpha^{-5}, \ldots$. Establish an equivalent counterpart of Formula 5 for each of these negative powers.

**Notation.** In a field $F$, for two elements $\alpha, \beta \in F$, with $\beta \neq 0$, we often write

$$\frac{\alpha}{\beta}$$

to mean $\alpha \beta^{-1}$. In particular, we write

$$\frac{1}{\beta}$$

to mean $\beta^{-1}$.

**Exercise 7.** In a field $F$, prove the following (1) through (9):

(1) $\frac{\alpha}{1} = \alpha$.

(2) If $\beta \neq 0$, and $\delta \neq 0$, then

$$\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta + \beta\gamma}{\beta\delta}.$$

(3) If $\beta \neq 0$, and $\delta \neq 0$, then

$$\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta}.$$
(4) If \( \beta \neq 0 \), and \( \delta \neq 0 \), then
\[
\frac{1}{\beta} \cdot \frac{1}{\delta} = \frac{1}{\beta \delta}.
\]

(5) If \( \alpha \neq 0 \), and \( \beta \neq 0 \), then
\[
\left( \frac{\alpha}{\beta} \right)^{-1} = \frac{\beta}{\alpha}.
\]

(6) If \( \beta \neq 0 \), then
\[
\left( \frac{1}{\beta} \right)^{-1} = \beta.
\]

(7) If \( \beta \neq 0 \), \( \gamma \neq 0 \), and \( \delta \neq 0 \), then
\[
\frac{\alpha}{\beta} \div \frac{\gamma}{\delta} = \frac{\alpha \delta}{\beta \gamma}.
\]

(8) If \( \beta \neq 0 \), then
\[
-\frac{\alpha}{\beta} = \frac{-\alpha}{\beta} = \frac{\alpha}{-\beta}.
\]

(9) If \( \beta \neq 0 \), and \( \delta \neq 0 \), then
\[
\frac{\alpha}{\beta} - \frac{\gamma}{\delta} = \frac{\alpha \delta - \beta \gamma}{\beta \delta}.
\]

**Remark.** It is important to note that, the above formulas (Formulas 1 through 6) are obtained by assuming the Field Axioms (i) through (x) and nothing else. We have never used anything else, no matter how common sense it is, but strictly the Field Axioms (i) through (x), and also what we can deduce from the Field Axioms (i) through (x).

It is important to emphasize that Formulas 1 through 6 are valid for an arbitrary field \( F \), We just knew the fact that Formulas 1 through 6 are valid for the real number field \( \mathbb{R} \).
I would like to remind you:

\[ 1 \neq 0 \]

was a part of the field axioms. So, this is true for any field \( F \). On the other hand,

\[ 2 \neq 0 \]

was not a part of the field axioms. Here, recall that 2 is the notation for \( 1 + 1 \). This was the definition of 2. Now, you don’t find this \( 2 \neq 0 \) in the list of field axioms. The question is, does this follow from the field axioms? The answer is, no, it does not. So in other words, there can potentially be a field satisfying the property

\[ 2 = 0. \]

As odd as it may sound, there indeed exists such a field \( F \) (Example 1 below). Note that,

\[ 2 = 0 \]

is equivalent to

\[ 1 = -1. \]

The next example is surprisingly simple:
Example 1 (the prime field of characteristic 2). Let \( \mathbb{F}_2 \) denote the set consisting of two elements 0 and 1. Thus

\[
\mathbb{F}_2 = \{0, 1\}.
\]

Define the addition and multiplication on \( \mathbb{F}_2 \) as follows:

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

<table>
<thead>
<tr>
<th>( \cdot )</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

These tables should read

\[
\begin{align*}
0 + 0 &= 0, & 0 + 1 &= 1, \\
1 + 0 &= 1, & 1 + 1 &= 0, \\
0 \cdot 0 &= 0, & 0 \cdot 1 &= 0, \\
1 \cdot 0 &= 0, & 1 \cdot 1 &= 1.
\end{align*}
\]

Everything looks ‘normal’, well, except

\[
1 + 1 = 0.
\]

But the truth of the matter is, if you define the addition and multiplication this way, over the set \( \mathbb{F}_2 \) which just consists of 0 and 1, then all the ten axioms in the set of field axioms are satisfied. So, this \( \mathbb{F}_2 \) is a field. This field is very important in mathematics, and there is a name for it:

\[
\mathbb{F}_2 = \text{the prime field of characteristic 2}.
\]
I leave it as your own exercise to verify that the above $\mathbb{F}_2$ indeed satisfies all the ten field axioms.

- Next, I will show you an example of a field in which $2 \neq 0$ but $3 = 0$.

**Example 2 (the prime field of characteristic 3).**

Let $\mathbb{F}_3$ denote the set consisting of three elements $0$, $1$ and $2$. Thus
\[
\mathbb{F}_3 = \{0, 1, 2\}.
\]
Define the addition and multiplication on $\mathbb{F}_3$ as follows:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\cdot$</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

These tables should read

\[
\begin{align*}
0 + 0 &= 0, & 0 + 1 &= 1, & 0 + 2 &= 2, \\
1 + 0 &= 1, & 1 + 1 &= 2, & 1 + 2 &= 0, \\
2 + 0 &= 2, & 2 + 1 &= 0, & 2 + 2 &= 1, \\
0 \cdot 0 &= 0, & 0 \cdot 1 &= 0, & 0 \cdot 2 &= 0, \\
1 \cdot 0 &= 0, & 1 \cdot 1 &= 1, & 1 \cdot 2 &= 2, \\
2 \cdot 0 &= 0, & 2 \cdot 1 &= 2, & 2 \cdot 2 &= 1.
\end{align*}
\]
Well, everything looks ‘normal’, except

\[ 1 + 2 = 0, \quad 2 + 1 = 0, \quad 2 + 2 = 1, \]

and also

\[ 2 \cdot 2 = 1. \]

But once again, the truth of the matter is, if you define the addition and multiplication this way, over the set \( \mathbb{F}_3 \) which just consists of 0, 1 and 2, then all the ten axioms in the set of field axioms are satisfied. So, this \( \mathbb{F}_3 \) is a field. This field too is very important in mathematics, and there is a name for it:

\[ \mathbb{F}_3 = \text{the prime field of characteristic 3}. \]

I leave it as your own exercise to verify that the above \( \mathbb{F}_3 \) indeed satisfies all the ten field axioms.

- Now, where is this going? Yes, you see some pattern here. Namely, in \( \mathbb{F}_3 \) as in Example 2 above, how you add and multiply numbers is simply as follows:

  “In \( \mathbb{F}_3 \), you first do the arithmetic in a usual way. If the outcome of addition is 3 then read it as 0. Indeed, \( \mathbb{F}_3 \) carries only 0, 1 and 2 as its elements. So, whenever you get 3 out of the usual arithmetic, you just automatically substitute it with 0.

  Likewise, if the outcome of addition or multiplication of two elements in \( \mathbb{F}_3 \) is 4, then read it as 1. Indeed, once again, \( \mathbb{F}_3 \) carries only 0, 1 and 2 as its elements. So whenever you get 4 you just automatically substitute it with 1. There is nothing more.”

In other words, in \( \mathbb{F}_3 \), the usual arithmetic holds, but there is one additional feature that \( \mathbb{F}_3 \) carries, namely,

3 is identified with 0, and 4 is identified with 1.
Hence also

5 is identified with 2, 6 is identified with 0,
7 is identified with 1, 8 is identified with 2,
9 is identified with 0, and so forth.

Now, in retrospect, in \( \mathbb{F}_2 \) as in Example 1 above, the same concept applies. Namely, in \( \mathbb{F}_2 \) the usual arithmetic holds, but there is one additional feature, namely, 2 is identified with 0.

- Now, you can stretch these and say you can construct \( \mathbb{F}_4 \) in a similar fashion perhaps? That’s a very good guess, but that is very subtle. So, please listen carefully. I’ll say three things.

1. The field \( \mathbb{F}_4 \) exists.
2. The field \( \mathbb{F}_4 \) consists of four elements.
3. The field \( \mathbb{F}_4 \) is \( \{0, 1, 2, 3\} \), with the addition and multiplication

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\]

\[
\begin{array}{c|cccc}
\cdot & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 0 & 2 \\
3 & 0 & 3 & 2 & 1 \\
\end{array}
\]
What’s wrong with these tables? Oh, Student A:

**Student A.** “Yes, this last pair of tables may appear a legitimate arithmetic rule to make the set \( \{0, 1, 2, 3\} \) a field. However, it has one crucial drawback. namely, if you look at the multiplication table carefully, you see 2 times 2 equals 0. That is not allowed in any field. It violates ‘the Integral Domain Property’ of fields which you emphasized as important in the last class.”

— Excellent. Yes, you are exactly right. The integral domain property was highlighted in our previous set of notes “Review of Lectures – IV” as Formula 5. Due to the very reason you cited, namely,

\[
2 \cdot 2 = 0,
\]

is included in the multiplication table, you cannot say that the set \( \{0, 1, 2, 3\} \) whose arithmetic dictated by the above tables is a field. Good grief.

But then you remember that in the above I still said that the field \( \mathbb{F}_4 \) exists, and it consists of four elements. Then what is \( \mathbb{F}_4 \)? Yes I would like to tell you that. But before that, let me do \( \mathbb{F}_5 \) first.

**Example 3 (the prime field of characteristic 5).**

Let \( \mathbb{F}_5 \) denote the set consisting of five elements 0, 1, 2, 3 and 4. Thus

\[
\mathbb{F}_5 = \{0, 1, 2, 3, 4\}.
\]

Define the addition and multiplication on \( \mathbb{F}_5 \) as follows:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
In short, in $\mathbb{F}_5$, the usual arithmetic holds, but there is one additional feature that $\mathbb{F}_5$ carries, namely,

- $5$ is identified with $0$,
- $6$ is identified with $1$,
- $7$ is identified with $2$,
- $8$ is identified with $3$,
- $9$ is identified with $4$, and so forth.

This field is equally very important in mathematics as $\mathbb{F}_2$ and $\mathbb{F}_3$, and there is a name for it:

\[ \mathbb{F}_5 = \text{the prime field of characteristic 5} \]

I leave it as your own exercise to verify that the above $\mathbb{F}_5$ indeed satisfies all the ten field axioms.

- Now, a question.

**Question.** Does a field $\mathbb{F}_6$ exist?

The answer is ‘no’.

**Question.** Does a field $\mathbb{F}_7$ exist?

The answer is ‘yes’. It is called the prime field of characteristic 7.
**Question.** Does a field \( \mathbb{F}_8 \) exist?

The answer is ‘yes’. However, it is not a prime field.

**Question.** Does a field \( \mathbb{F}_9 \) exist?

The answer is ‘yes’. However, it is not a prime field.

**Question.** Does a field \( \mathbb{F}_{10} \) exist?

The answer is ‘no’.

**Question.** Does a field \( \mathbb{F}_{11} \) exist?

The answer is ‘yes’. It is called \underline{the prime field of characteristic 11}.

**Question.** Does a field \( \mathbb{F}_{12} \) exist?

The answer is ‘no’.

**Question.** Does a field \( \mathbb{F}_{13} \) exist?

The answer is ‘yes’. It is called \underline{the prime field of characteristic 13}.

**Question.** Does a field \( \mathbb{F}_{14} \) exist?

The answer is ‘no’.

**Question.** Does a field \( \mathbb{F}_{15} \) exist?

The answer is ‘no’.

And you can keep throwing the same question about \( \mathbb{F}_N \) with a larger \( N \), and I can keep answering the questions, but it is endless. But there is a simple fact that is governing this.
Key Facts about finite fields.

(1) A field consisting of \( N \) number of elements **exists**, if \( N \) is either a **prime number**, or a **prime power**.

(2) A field consisting of \( N \) number of elements **does not exist**, if \( N \) is neither a prime number nor a prime power.

Here, \( p \) being a **prime number** means \( p \) is an integer, such that \( p \geq 2 \), and moreover no smaller positive integers other than 1 divides \( p \). Also, a **prime power** means a positive integer power of a prime number.

Thus,

\[
p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \cdots
\]

are the first few prime numbers. Also,

\[
q = 4 \ (= 2^2), \ 8 \ (= 2^3), \ 16 \ (= 2^4), \ 32 \ (= 2^5), \ 64 \ (= 2^6),
\]

\[
9 \ (= 3^2), \ 27 \ (= 3^3), \ 81 \ (= 3^4), \ 243 \ (= 3^5),
\]

\[
25 \ (= 5^2), \ 125 \ (= 5^3), \ 625 \ (= 5^4), \ 3125 \ (= 5^5),
\]

\[
49 \ (= 7^2), \ 343 \ (= 7^3), \ 2401 \ (= 7^4),
\]

\[
121 \ (= 11^2), \ 1331 \ (= 11^3),
\]

\[
169 \ (= 13^2), \ 2197 \ (= 13^3),
\]

\[
289 \ (= 17^2),
\]

\[
361 \ (= 19^2), \ \cdots
\]

are examples of prime powers.
• The proof of the above key facts (1), (2) belong to ‘abstract algebra’. Let’s not do the proof of this fact in this class. Let’s leave it to an ‘abstract algebra’ course. But I just want you to memorize those two statements. Next, two remarks are in order concerning the usage:

**Remark about the terms ‘prime power’**.

We often include prime numbers as members of the set of prime powers. Thus, you can say 2 is a prime power, even though 2 is indeed a prime number. Similarly, 3 is a prime power, even though 3 is indeed a prime number, 5 is a prime power, even though 5 is indeed a prime number, and so on.

**Remark about the terms ‘prime’**.

We often refer to prime numbers as **primes**. So, in what follows I may say “let \( p \) be a prime”, and it certainly means “let \( p \) be a prime number”.

• The next thing is very important.

**Theorem–Definition.** Let \( p \) be a **prime**. Suppose a field \( F \) has \( p \) number of elements. Then such an \( F \) is denoted as \( \mathbb{F}_p \), and it is called the prime field of characteristic \( p \). You may write elements of \( F = \mathbb{F}_p \) as

\[
\mathbb{F}_p = \{ 0, 1, 2, 3, \ldots, p - 1 \}.
\]

The addition and the multiplication rules of \( F = \mathbb{F}_p \), are the ‘usual’ ones, except the following: If the result of addition/multiplication is a number which exceeds \( p - 1 \), then you subtract a suitable integer multiple of \( p \) from the result so as to make the outcome number being in the set \( \{ 0, 1, 2, 3, \ldots, p - 1 \} \), and that outcome number is the result of addition/multiplication of the given two numbers in \( \mathbb{F}_p \).
Example 4  (the prime field of characteristic 7).

The field $F_7$, the prime field of characteristic 7, consists of seven elements:

$$F_7 = \{0, 1, 2, 3, 4, 5, 6\},$$

with the addition and multiplication defined as follows:

<table>
<thead>
<tr>
<th>$+$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\cdot$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<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>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Exercise 1. Describe $F_{11}$ in a similar fashion.

[Answer] $F_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. 

29
<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9</td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>1</td>
<td>4</td>
<td>7</td>
<td>10</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>2</td>
<td>6</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>0</td>
<td>5</td>
<td>10</td>
<td>4</td>
<td>9</td>
<td>3</td>
<td>8</td>
<td>2</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>0</td>
<td>6</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>9</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>0</td>
<td>7</td>
<td>3</td>
<td>10</td>
<td>6</td>
<td>2</td>
<td>9</td>
<td>5</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>0</td>
<td>8</td>
<td>5</td>
<td>2</td>
<td>10</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>0</td>
<td>9</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>10</td>
<td>8</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>0</td>
<td>10</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
Exercise 2. Does a field having

(1) 4,  (2) 6,  (3) 8,  (4) 9,  (5) 12,
(6) 16,  (7) 20,  (8) 23,  (9) 24,  (10) 25,
(11) 31,  (12) 36,  (13) 48,  (14) 49,  (15) 64,
(16) 71,  (17) 81,  (18) 99,  (19) 100,  (20) 101,
(21) 111,  (22) 121,  (23) 125,  (24) 144,

number of elements exist? Is it a prime field? If it is a prime field, then give its official name.

\[
\text{Answers: } (1) \text{ exists, not a prime field. } (2) \text{ does not exist.}
\]

\[
(3) \text{ exists, not a prime field. } (4) \text{ exists, not a prime field.}
\]

\[
(5) \text{ does not exist. } (6) \text{ exists, not a prime field.}
\]

\[
(7) \text{ does not exist. } (8) \text{ exists, it is the prime field of characteristic 23.}
\]

\[
(9) \text{ does not exist. } (10) \text{ exists, not a prime field.}
\]

\[
(11) \text{ exists, it is the prime field of characteristic 31. } (12) \text{ does not exist.}
\]

\[
(13) \text{ does not exist. } (14) \text{ exists, not a prime field.}
\]

\[
(15) \text{ exists, not a prime field. } (16) \text{ exists, it is the prime field of characteristic 71.}
\]

\[
(17) \text{ exists, not a prime field. } (18) \text{ does not exist.}
\]

\[
(19) \text{ does not exist. } (20) \text{ exists, it is the prime field of characteristic 101.}
\]

\[
(21) \text{ does not exist. } (22) \text{ exists, not a prime field.}
\]

\[
(23) \text{ exists, not a prime field. } (24) \text{ does not exist.}
\]

* Now, as for fields whose number of elements are not primes, their structure is a little more complicated.
The standard textbooks adopt the following approach: Namely, first construct a
certain field, which itself carries infinitely many elements, called \( \mathbb{F}_p \), which yet has
the property that it contains all the fields whose number of elements are \( p \)-to-some
power, simultaneously. This is abstract, and suitable for ‘abstract algebra’ course.
I choose a different approach. My approach does not cover all cases, yet it is concrete
and is easier to understand. First, let me give the following theorem:

**Theorem.** Let \( q \) be a prime power. Then a field having \( q \) number of elements is
“unique up to isomorphisms”, namely, suppose \( F_1 \) and \( F_2 \) are both fields having
\( q \) number of elements, then there exists a bijective mapping

\[
\varphi : F_1 \longrightarrow F_2
\]

satisfying the properties:

(Isom1) \[
\varphi \left( \alpha + \beta \right) = \varphi \left( \alpha \right) + \varphi \left( \beta \right),
\]

(Isom2) \[
\varphi \left( \alpha \beta \right) = \varphi \left( \alpha \right) \varphi \left( \beta \right), \quad \text{and}
\]

(Isom3) \[
\varphi \left( 1 \right) = 1.
\]

In a plain language, the existence of such a \( \varphi \) simply means that \( F_1 \) and \( F_2 \)
carry the exact identical structure as fields. That is, \( F_1 \) and \( F_2 \) are replicas of
each other. So, in that sense, a field having \( q \) number of elements is unique.

In case you wonder how come \( \varphi \left( 0 \right) = 0 \) is not included in the list of (Isom1)
through (Isom3), this is actually something you can prove out of (Isom1), so it is not
necessary to include it in the list (it would be redundant). Indeed, in (Isom1), set
\( \alpha = 0 \), and \( \beta = 0 \). Then the entire line of (Isom1) reads

\[
\varphi \left( 0 \right) = \varphi \left( 0 \right) + \varphi \left( 0 \right).
\]

By adding \( -\varphi \left( 0 \right) \) to the both sides you obtain \( \varphi \left( 0 \right) = 0 \).

If this was an abstract algebra course I would say a few more things about this
notion of ‘isomorphism’, but let’s not worry about it for now. The bottom line is, once
again, for each prime power \( q \), the field having \( q \) number of elements is ‘essentially’
unique.
• **Usage.** ‘Unique up to isomorphisms’.

Still, please know that ‘unique up to isomorphisms’ is a more meticulous way of saying it, and is considered as more formal and more preferable mathematically. For the rest of the semester, I will be in the situations where I must utter these words: ‘unique up to isomorphisms’. Sometimes I say it as ‘whose isomorphism type is unique’. Know that it is just a jargon for ‘essentially unique’. The precise meaning of it is given in the above. Now, if this was an abstract algebra course I would give a proof of this Theorem. But let’s not worry about the proof of this Theorem. So, in any case, the following notation makes sense:

**Notation (being consistent with Theorem above).**

Let $q$ be a prime power. Then unique field (up to an isomorphism) having $q$ number of elements is denoted as

\[
\mathbb{F}_q
\]

**Caution.** If $q$ is **not** a prime, then we **do not** say $\mathbb{F}_q$ is a prime field. **Only** when $q = p$ is a prime, we say $\mathbb{F}_q = \mathbb{F}_p$ is a prime field.

**Theorem–Definition.** Let $q$ be a prime power, not necessarily a prime. Thus there exist a prime $p$ and a positive integer $n$ such that $q = p^n$. Let $F = \mathbb{F}_q$ be the unique field (up to an isomorphism) having $q$ number of elements, as defined above. Then the smallest positive integer $\ell$ such that

\[
1 + 1 + \cdots + 1 = 0
\]

inside $F$ is equal to $p$. In this regard, the prime $p$ is called **the characteristic** of the field $F = \mathbb{F}_q$. We write

\[
\text{char } \mathbb{F}_q = p.
\]

**Exercise 3.** Find the characteristic of each of the following fields:

- $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{11}$, $\mathbb{F}_{16}$, $\mathbb{F}_{25}$, $\mathbb{F}_{31}$,
- $\mathbb{F}_{32}$, $\mathbb{F}_{49}$, $\mathbb{F}_{64}$, $\mathbb{F}_{81}$, $\mathbb{F}_{121}$, $\mathbb{F}_{125}$, $\mathbb{F}_{169}$.
\[ \text{[Answers]} : \quad \text{char } F_2 = 2. \quad \text{char } F_3 = 3. \quad \text{char } F_4 = 2. \quad \text{char } F_8 = 2. \]
\[ \text{char } F_{11} = 11. \quad \text{char } F_{16} = 2. \quad \text{char } F_{17} = 17. \quad \text{char } F_{25} = 5. \]
\[ \text{char } F_{31} = 31. \quad \text{char } F_{32} = 2. \quad \text{char } F_{49} = 7. \quad \text{char } F_{64} = 2. \]
\[ \text{char } F_{81} = 3. \quad \text{char } F_{121} = 11. \quad \text{char } F_{125} = 5. \quad \text{char } F_{169} = 13. \]

- \( F_q = F_{p^n} \) contains the prime field \( F_p \) as a ‘subfield’.

Once again, let \( q \) be a prime power, and let \( F_q \) be the unique field (up to isomorphisms) having \( q \) number of elements. Since \( F_q \) (or any field for that matter) contains 1, it makes sense to consider

\[
\underbrace{1 + 1 + \cdots + 1}_\ell
\]

inside the same field \( F_q \). This is an element of \( F_q \). We denote this element of \( F_q \) by \( \ell \) (by abuse of notation). Now, let me paraphrase the ‘theorem part’ of Theorem–Definition above: If \( p \) is the prime such that \( q = p^n \) using some positive integer \( n \), then

\[
1 = 1,
2 = 1 + 1,
3 = 1 + 1 + 1,
4 = 1 + 1 + 1 + 1,
\vdots
p - 1 = 1 + 1 + \cdots + 1
\]

are all non-zero, whereas

\[
p = 1 + 1 + \cdots + 1 + 1
\]

equals 0.
Example. In each of the characteristic 2 fields

\[ F_4 = F_{2^2}; \quad F_8 = F_{2^3}; \quad F_{16} = F_{2^4}; \quad F_{32} = F_{2^5}; \quad F_{64} = F_{2^6}; \quad \ldots, \]

\[ 1 = 1 \neq 0, \]

but

\[ 2 = 1 + 1 = 0. \]

We know that the same is true for the prime field \( F_2 \) of characteristic 2.

Example. In each of the characteristic 3 fields

\[ F_9 = F_{3^2}; \quad F_{27} = F_{3^3}; \quad F_{81} = F_{3^4}; \quad F_{243} = F_{3^5}; \quad \ldots, \]

\[ 1 = 1 \neq 0, \]

\[ 2 = 1 + 1 \neq 0, \]

but

\[ 3 = 1 + 1 + 1 = 0. \]

We know that the same is true for the prime field \( F_3 \) of characteristic 3.

Example. In each of the characteristic 5 fields

\[ F_{25} = F_{5^2}; \quad F_{125} = F_{5^3}; \quad F_{625} = F_{5^4}; \quad F_{3125} = F_{5^5}; \quad \ldots, \]

\[ 1 = 1 \neq 0, \]

\[ 2 = 1 + 1 \neq 0, \]

\[ 3 = 1 + 1 + 1 \neq 0, \]

\[ 4 = 1 + 1 + 1 + 1 \neq 0, \]

but

\[ 5 = 1 + 1 + 1 + 1 + 1 = 0. \]

We know that the same is true for the prime field \( F_5 \) of characteristic 5.
In view of this, it makes sense to isolate the subset of $\mathbb{F}_q$ consisting of elements which are of form

$$1 + 1 + \cdots + 1.$$ 

Then it is true (by Theorem–Definition above) that that subset consists precisely of $p$ elements, where $p$ is the prime such that $q$ is written as $q = p^n$ for some positive integer $n$. We may write that subset as

$$\{0, 1, 2, 3, \cdots, p-1\}.$$ 

**Theorem.** Let $q$ be a prime power, thus $q = p^n$ for some prime number $p$ and a positive integer $n$. Then the subset

$$L = \{0, 1, 2, 3, \cdots, p-1\} \subseteq \mathbb{F}_q$$

of $\mathbb{F}_q$ is a field by itself, with respect to the addition and the multiplication of $\mathbb{F}_q$. The subset $L$, regarded as a field, is isomorphic to $\mathbb{F}_p$.

- So, in short, if $q = p^n$, $p$ is a prime and $n$ is a positive integer, then the field $\mathbb{F}_q$ contains a subset $L$ consisting of the sums of replicas of 1, which forms a field by itself. Moreover, $L$ and $\mathbb{F}_p$ have an identical structure as fields. So $L = \mathbb{F}_p$.

This may actually remind you of the fact that the real number field $\mathbb{R}$ contained the subset $\mathbb{Q}$ consisting of all rational numbers, and $\mathbb{Q}$ formed a field by itself. Now, I want to officially call the subset $L = \mathbb{F}_p$ of $\mathbb{F}_q$ ‘the prime subfield’ of $\mathbb{F}_q$. Also, I want to officially call the subset $\mathbb{Q}$ of $\mathbb{R}$ ‘the prime subfield’ of $\mathbb{R}$. For that matter, I need to officially define the notion of a ‘subfield’ of a field. So, let’s tentatively go back to an arbitrary field, containing either finite or infinite number of elements.

**Definition (subfield).** Let $F$ be an arbitrary field. Let $L$ be its subset: $L \subseteq F$. Suppose $L$ satisfies

(Sub-F1) $\alpha + \beta \in L$ whenever $\alpha \in L$, $\beta \in L$,

(Sub-F2) $-\alpha \in L$ whenever $\alpha \in L$,

(Sub-F3) $\alpha \beta \in L$ whenever $\alpha \in L$, $\beta \in L$,

(Sub-F4) $\alpha^{-1} \in L$ whenever $\alpha \in L$, and $\alpha \neq 0$,

(Sub-F5) $1 \in L$. 

36
These five axioms are altogether called the subfield axioms. Under these assumptions, \( L \) forms a field by itself, with respect to the addition and the multiplication of \( F \). We say that \( L \) is a subfield of the field \( F \).

- The following is probably the most basic example of a subfield of a field.

**Example.** The rational number field \( \mathbb{Q} \) is a subfield of the real number field \( \mathbb{R} \).

- So far I have not addressed what kind of subfields \( \mathbb{R} \) carries, other than \( \mathbb{Q} \). Are there many subfields which \( \mathbb{R} \) carries, or only a few? The answer is, ‘plenty’. You perhaps remember that I said in a couple of lectures ago that ‘number theory’ is one outstanding branch of mathematics. There is one major (indeed major-major) subdiscipline of number theory called ‘algebraic number theory’. A (significantly) oversimplified version of what ‘algebraic number theory’ is all about (which still captures the spirit):

  “Algebraic number theory is about subfields of \( \mathbb{R} \) (and about subfields of \( \mathbb{C} \), the complex number field, which we haven’t defined yet), which are in a ‘modest size’ (‘finite dimensional’ over \( \mathbb{Q} \) as a ‘vector space’). Those fields are called algebraic number fields. Thus, algebraic number theory is a study of algebraic number fields.”

- Now, an alert student might ask:

**Student X.** “Isn’t \( \mathbb{Q} \) an example of an algebraic number field, by definition? If so, then at least a part of algebraic number theory studies just rational numbers? That doesn’t sound difficult or exciting.”

That’s a good point. One part of what you are saying is right: Namely, the part algebraic number theory studies \( \mathbb{Q} \). Now, as for the part ‘therefore it is not exciting’, let me say this: You remember that a couple of lectures ago (in “Review of Lectures – III”), I cited one outstanding problem in mathematics which had remained unsettled for three centuries, and had finally been settled recently (in 1995), called ‘Fermat’s last theorem’. That theorem is about \( \mathbb{Q} \). The statement of ‘Fermat’s last theorem’ is made only with reference to the field \( \mathbb{Q} \). You don’t have to know anything else but just the field \( \mathbb{Q} \). Yet the proof of ‘Fermat’s last theorem’ (by Wiles and Taylor) is indeed ‘super-duper’, only the greatest minds in number theory can decipher and understand. Many consider this breakthrough as the most monumental achievement in all pure mathematics to date.
Let’s move back to our original theme, namely, fields consisting of finite number of elements. In the above I highlighted as a theorem the fact that $\mathbb{F}_q$ contains one distinguished subset consisting of sums of replicas of 1 which forms a field by itself. Now, using the term ‘subfields’ which I just introduced, I can paraphrase it:

**Theorem paraphrased.** Let $q$ be a prime power, thus $q = p^n$ for some prime number $p$ and a positive integer $n$. Then the subset

$$\{ 0, 1, 2, 3, \ldots, p - 1 \} \subseteq \mathbb{F}_q$$

forms a subfield of $\mathbb{F}_q$, which is isomorphic to $\mathbb{F}_p$.

**Definition.** The subfield

$$\{ 0, 1, 2, 3, \ldots, p - 1 \} \subseteq \mathbb{F}_q$$

is called the prime subfield of $\mathbb{F}_q$.

- **Recap.**
  1. If a field has only a finite number of elements, say $q$ number of elements, then $q$ is a prime power.

  2. Conversely, let $q$ be an arbitrary prime power. Then there exists a field having $q$ number of elements. It is unique up to isomorphisms, and is denoted $\mathbb{F}_q$.

  3. If $p$ is a prime, then $\mathbb{F}_p$ is called the prime field of characteristic $p$.

  4. Let $q$ be a prime power. Suppose $p$ is the prime such that $q$ is written as $q = p^n$ using some positive integer $n$. Then $\mathbb{F}_q$ contains a distinguished subfield which is isomorphic to $\mathbb{F}_p$, called the prime subfield of $\mathbb{F}_q$.

  5. In 4, the prime subfield of $\mathbb{F}_q$ is nothing else but the subset of $\mathbb{F}_q$ consisting of the sums of replicas of 1 inside $\mathbb{F}_q$. We define the characteristic of $\mathbb{F}_q$ as $p$, write $\text{char} \mathbb{F}_q = p$. In particular, if $p$ is a prime, then $\text{char} \mathbb{F}_p = p$.

So far so good?