§9. Construction of fields \( F_4 \) and \( F_8 \).

Let’s begin with the following new terminology yet to be officially introduced.

**Definition (Finite fields).** A field \( F \) is called a **finite field**, if \( F \) contains only finitely many elements.

- So, much of what we have seen in our last lecture (in “Review of Lectures – V”) was about finite fields. We learned that, if \( F \) is a finite field, then the number of elements contained in \( F \) is a prime power \( q \). For each prime power \( q \), there exists a finite field having \( q \) elements and its isomorphism type is unique, we write it as \( F_q \). If \( q = p \) is a prime, then \( F_p \) is called the **prime field of characteristic \( p \)**. We already know the structure of the prime field of characteristic \( p \) for an arbitrary prime number \( p \). On the other hand, we have not seen yet the structure of finite fields \( F_q \) which are not prime fields, namely, those \( F_q \) where \( q \) is not a prime.

- For example, we have not seen yet the structure of each of

\[ F_4, \quad F_8, \quad \text{and} \quad F_{16}. \]

All you were told was they exist. Today, we will ‘construct’ \( F_4, F_8, \) and \( F_{16} \). Our method is probably not what you see in your abstract algebra textbook, if you own one of those in your bookshelves. Most abstract algebra textbooks offer the following construction of each of \( F_4, F_8, F_{16}, \cdots \), as follows: First construct one single field \( \overline{F}_2 \) called ‘the algebraic closure of the prime field of characteristic 2’.

The authors of those books go on and say that \( F_4, F_8, F_{16}, \cdots \), are all subfields of \( \overline{F}_2 \), defined by certain ‘algebraic equations’, or more specifically:

- \( F_4 \) is the subset consisting of elements of \( \overline{F}_2 \) satisfying \( x^4 = x \),
F_8 is the subset consisting of elements of \( \overline{\mathbb{F}_2} \) satisfying \( x^8 = x \),
and so on. From the most rigorous standpoint, this makes perfect sense. However, the drawback is, you have to go through the existence of the algebraic closure \( \overline{\mathbb{F}_2} \). Yes, it is viable to prove the existence of the algebraic closure \( \overline{F} \) of an arbitrary field \( F \) in an introductory abstract algebra course. Actually, that proof itself has nothing to do with the notion of finite fields. Unfortunately, digesting that proof does not really help understanding the rest of the subject. (Believe me, in many areas of mathematics, there are certain basic theorems and results which you need to rely on throughout, and yet their proofs do not fairly represent the flavor of the subject, understanding those proofs really don’t help your understanding of the subject as a whole. This is one of those things.)

So, I choose a different approach. Our method does not cover all cases but it gives you a concrete picture, and it reflects the flavor of the subject of finite fields.

**Construction of \( \mathbb{F}_4 \).**

Out of the blue, consider

\[ \sigma = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}. \]

We regard this as a matrix with entries in \( \mathbb{F}_2 \). Let’s calculate \( \sigma^2 \). Here, once again, entries of this matrix are in \( \mathbb{F}_2 \). So, squaring the matrix means you do it in a usual fashion, and once you get \( 2 \) then you replace it with \( 0 \). Let’s go:

\[
\sigma^2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + 1 \cdot 1 & 1 \cdot 1 + 1 \cdot 0 \\ 1 \cdot 1 + 0 \cdot 1 & 1 \cdot 1 + 0 \cdot 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.
\]
So far so good. But then, you got 2 in one out of the four entries. Remember, you identify it with 0. So, the final outcome:

\[ \sigma^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}. \]

Now, why is this important? Yes it is important. You may not see it immediately, but I have to ask you to trust my words. Let’s do \( \sigma^3 \), and see what happens.

\[
\sigma^3 = \sigma^2 \sigma = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}
= \begin{bmatrix} 0 \cdot 1 + 1 \cdot 1 & 0 \cdot 1 + 1 \cdot 0 \\ 1 \cdot 1 + 1 \cdot 1 & 1 \cdot 1 + 1 \cdot 0 \end{bmatrix}
= \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.
\]

So far so good. But here, once again, you got 2 in one out of the four entries. Remember, you identify it with 0. So, the final outcome:

\[ \sigma^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \]

Okay. Now, isn’t this the identity matrix, which we usually denote as \( I \)? Yes. So, we have just got three different matrices:

\( \sigma, \quad \sigma^2 \quad \text{and} \quad \sigma^3 = I. \)

Now, finally, let’s add the zero matrix to this list:

\[ O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}. \]
So, we have got four matrices altogether: \( O; \sigma; \sigma^2; \text{ and } \sigma^3 = I. \)

Here, somehow let’s denote \( O \) as 0. Also let’s denote \( I \) as 1. So, once again, our four matrices:

\[
\begin{align*}
0 & \quad 0 & \quad 0 & \quad 0 \\
0 & \quad 0 & \quad 0 & \quad 0 \\
1 & \quad 1 & \quad 1 & \quad 1 \\
0 & \quad 0 & \quad 0 & \quad 0 \\
\end{align*}
\]

\[
\begin{align*}
0 & \quad 1 & \quad \sigma & \quad \sigma^2 \\
0 & \quad 1 & \quad \sigma & \quad \sigma^2 \\
1 & \quad 0 & \quad \sigma & \quad \sigma^2 \\
0 & \quad 1 & \quad \sigma & \quad \sigma^2 \\
\end{align*}
\]

Claim. This set \( \{ 0, 1, \sigma, \sigma^2 \} \) forms a field, consisting of \( 4 = 2^2 \) elements, with respect to the matrix addition and multiplication. Hence this is \( \mathbb{F}_4 \). In short,

\[
\mathbb{F}_4 = \left\{ 0, 1, \sigma, \sigma^2 \right\}
\]

\[
= \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\}.
\]

- The addition and the multiplication tables (below \( \sigma^2 \) is denoted as \( \tau \)):
• Construction of $\mathbb{F}_8$.

Next, we will construct $\mathbb{F}_8$. Once again, out of the blue, consider

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

We regard this as a matrix with entries in $\mathbb{F}_2$. Let’s calculate $\sigma^2$. Here, once again, entries of this matrix are in $\mathbb{F}_2$. So, squaring the matrix means you do it in a usual fashion, and once you get 2 then you replace it with 0. Let’s go:

$$\sigma^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$ 

So far so good. We don’t have to do anything with it, because there is no 2 here. Next,

$$\sigma^3 = \sigma^2 \sigma = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$ 

Once again, we don’t have to do anything with it, because there is no 2 here. Now, next

$$\sigma^4 = \sigma^3 \sigma = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$
Now 2 appeared in one out of the nine entries. What are we supposed to do then? Yes, as you remember, you identify it with 0. So, the final outcome:

\[
\sigma^4 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.
\]

This is important. Next,

\[
\sigma^5 = \sigma^4 \sigma = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 1 & 1 & 2 \end{bmatrix}.
\]

Again, substitute 2 with 0:

\[
\sigma^5 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}.
\]

Good. Now, how far do we have to go? Actually, two more steps. Please just bear with me.

\[
\sigma^6 = \sigma^5 \sigma = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \end{bmatrix}.
\]
Substitute 2 with 0:
\[
\sigma^6 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.
\]

One more step, just bear with me:
\[
\sigma^7 = \sigma^6 \sigma = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}
\]
\[
= \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.
\]

Substitute 2 with 0, as usual:
\[
\sigma^7 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.
\]

Okay, what is this? Yes, this is the identity matrix \( I \). So, \( \sigma^7 = I \).

To summarize our result:
\[
\sigma = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \sigma^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \quad \sigma^3 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix},
\]
\[
\sigma^4 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \quad \sigma^5 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}, \quad \sigma^6 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix},
\]
\[
\sigma^7 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I.
\]