Article 4: Construction of Finite Fields

Debadatta Kar

June 22, 2025

1 Introduction

Finite fields always show up in the order p^k where p is a prime number and k is some positive integer. The fields of order p are isomorphic to the finite field $\mathbb{Z}_p$ where addition and multiplication are modulo p. Finite fields of order p^k are constructed from $\mathbb{Z}_p$ with some treatment of algebra. Often, a finite field F of order q is denoted as $F(q)$ or F_q. We also call them Galois Field in the name of Évariste Galois, a French mathematician. So it's very common to denote F_q as $G(q)$ as well. In this article, we will show a way to construct a finite field of order $q = p^k$ using elements of F_p.

2 Prime order Fields

In this setting, we can construct the Cayley table for any field of order p.

Example 2.1. *Consider the field F_3. So we have elements $\{0, 1, 2\}$, and now we will construct the Cayley table to see addition and multiplication.*
For addition, we have the table as follows:

$+$	*0*	*1*	*2*
0	*0*	*1*	*2*
1	*1*	*2*	*0*
2	*2*	*0*	*1*

For multiplication, we have the table as follows:

$\times$	*0*	*1*	*2*
0	*0*	*0*	*0*
1	*0*	*1*	*2*
2	*0*	*2*	*1*

If we begin doing it considering a field of order p^k for some $k > 1$ we will fail in producing a similar table. For instance, we can check it for F_4
The addition table look good.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

However, the multiplication table is not appealing, 2 does not have a multiplicative inverse!!

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Result 2.2. *If F_p is a field and $f(x)$ is irreducible in the polynomial ring $F[x]$ then the $\frac{F_p[x]}{f(x)}$ is a field and the order of this field is $p^{\deg(f(x))}$*

The above result directly applies to the construction of a field of order p^k by choosing an irreducible polynomial of order k and the field F_p.

3 Construction of Finite Field of Order p^k

We will go by taking a simple case of constructing F_4, and then we will construct F_9.

3.1 Constructing F_4

The base field is F_2. We will go for the SageMath implementation for the quick construction of F_4 instead of doing it manually.

```
#1 Define the finite field with 2 elements (GF(2))
F2 = GF(2)
#2 Define the polynomial ring over Z with variable x
F2X.<x> = PolynomialRing(F2, 'x')
#3 Generate an initial random polynomial of degree 2
a = F2X.random_element(2)
#4 Loop until an irreducible polynomial is found
#The loop continues as long as 'a' is NOT irreducible.
while not a.is_irreducible():
#5 Generate a new random polynomial (of degree 2)
    a = F2X.random_element(2)
# Print the found irreducible polynomial and its degree
print(f"Found irreducible polynomial: {a}")
print(f"Degree: {a.degree()}")
```

The above program constructs the polynomial ring $F_2[x]$ and then randomly picks elements,which happen to be polynomials and specifically of degree 2, which has been restricted to it. Then top of it, the program checks the irreducibility using the function $'is\_irreducible()'$. The point it gives a true value the program terminates by outputting the irreducible polynomial it checked for.
On termination of this program, we got the irreducible polynomial $x^2 + x + 1$.
We will now design the set $\frac{F_2[x]}{<x^2+x+1>}$ and construct the caley table for verification.
The elements of this field are all polynomials in $F_2[x]$ of degree ≤ 1. More precisely the elements of the field are $\{0, 1, x, 1 + x\}$.
The addition table is as below and it is addition modulo $x^2 + x + 1$:

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

The multiplication table is as below and it is multiplication modulo $x^2 + x + 1$:

$\times$	0	1	x	$1 + x$
0	0	0	0	0
1	0	1	x	$1 + x$
x	0	x	$1 + x$	1
$1 + x$	0	$1 + x$	1	x

For the computation of $x(1 + x)$ we have,

$$x(1 + x) = x^2 + x \equiv 1 \pmod{x^2 + x + 1}$$

For the computation of $(x + x)^2$ we have,

$$(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1 \equiv x \pmod{x^2 + x + 1}$$

and finally, the field is ready after construction and verification.

3.2 Constructing F_9

We would mimic the same approach here as well. The base field is F_3, so we just need to change the base field, and the degree of the polynomial would be again 2 as $3^2 = 9$, which is the order of F_9.

```
#1 Define the finite field with 3 elements (GF(3))
F3 = GF(3)
#2 Define the polynomial ring over F3 with variable x
F3X.<x> = PolynomialRing(F3, 'x')
#3 Generate an initial random polynomial of degree 2
a = F3X.random_element(2)
#4 Loop until an irreducible polynomial is found
#The loop continues as long as 'a' is NOT irreducible.
while not a.is_irreducible():
#5 Generate a new random polynomial (of degree 2)
    a = F3X.random_element(2)
# Print the found irreducible polynomial and its degree
print(f"Found irreducible polynomial: {a}")
print(f"Degree: {a.degree()}")
```

On termination of this program, we got the irreducible polynomial $2x^2 + 2$.
We will now design the set $K_9 = \frac{F_3[x]}{<2x^2+2>}$ and construct the caley table for verification.
The elements of this field are all polynomials in $F_3[x]$ of degree ≤ 1. More precisely, the elements of the field are $\{0, 1, 2, x, 2x, 1 + x, 2 + x, 1 + 2x, 2 + 2x\}$.

References

[1] Lidl R, Niederreiter H, *Finite Fields*, 2nd ed. Cambridge University Press; 1996